TIBCO LogLogic®

Security Event Manager (SEM)

Installation Guide

Software Release: 3.6.0

March 2013

Two-Second Advantage®

Important Information

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

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

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

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

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

Contents

List of Figures

Preface

About This Guide

This guide is intended as a step by step guide to the initial configuration of the Security Management Platform and its connection to the Web Console - the web-based graphical user interface.

There are three phases to the installation of the SMP:

- Phase 1 - Initial Installation of the SMP
    - Formatting the hard drive
    - Installing the TIBCO LogLogic® software and components
    - Creating the database
- Phase 2 - Configuration of the SMP
    - Configuring the Internet Protocol (IP) address of the SMP
    - Setting a hostname
    - Assigning a super-administrative password
- Phase 3 - Configuration of the Web Console
    - Connecting to a web browser
    - Examining the security certificate
    - Logging into the Web Console and viewing the alerts

This guide also explains how to apply a patch on a standard server.

Note that SEM Log Source Package (SEM LSP) - that contains log parsers for supported logs - can be installed on SEM and SEM EVA 3.6.0.

Please refer to SEM Log Source Package Release Notes for more information.

The installation procedure should take 45-50 minutes.

Audience

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

Related Documentation

Documentation	Content
Administration Guide	This guide explains how to configure the various functions of the Security Event Manager Solution in an advanced manner.
Concepts Guide	This guide gives an overview of: Regulatory Compliance through its three underlying domains: regulation, standards and technical reporting. Taxonomy. How logs are converted into user-oriented messages. Correlation. Encryption of logs.
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.
User Guide	This guide explains how to use and configure the various functions and modules provided in the Web Console application.

Technical Support Information

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.

LogLogic provides timely and comprehensive customer support and technical assistance from highly knowledgeable, experienced engineers who can help you maximize the performance of your 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 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 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 LogLogic Technical Publications team.

Conventions

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

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

IMPORTANT! Highlights key considerations to keep in mind.

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

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

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

```
username: system
```

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

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

```
LogLogic_home_directory\upgrade\
```

- Straight brackets signal options in command line syntax.

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

Chapter 1 - Recommendation and Requirements

Recommendation

Packaging

Please be aware that we package our servers in a cardboard box sealed with a special tape. The adhesive security tape, printed with our logo, is designed to show unauthorized broaching of a package. Should someone try to peel it away, the tape cannot be resealed to the box surface, furnishing evidence that it was tampered with.

Please contact our support at your earliest convenience if you find any problems with the delivery of your equipment.

Physical Security

Most corporation information system departments have well-established security policies, which include the implementation of server computers in a secure area that is not accessible to unauthorized personnel. It is extremely important that the SMP server be placed in a secure environment, since physical access to a server can bring forth a host of security threats. An individual with physical access to a server can, for example, disrupt service, or even damage or steal data.

Here are some important guidelines for securing your data center:

1. Install the server in a locked, environmentally controlled data center with restricted access to the server.

2. Restrict access to the smallest number of people necessary for the operation of the data center.

3. Install security cameras to monitor activity on a 24-hour basis.

4. Keep keyboards away from cameras, windows or unauthorized personnel.

5. Security also applies to backup procedures, equipment, and storage media. Keep all backup tapes (or other media) in a secure environment where you can maintain strict physical control of them.

6. The workstation from which you can access the Web Console must be located in a secure and protected environment where only authorized personnel can access.

Logical Security

To protect your server from intruders using non-authorized protocols or a connection from a non-authorized machine, you should use filtering devices.

No applications except those provided by TIBCO LogLogic® must be installed on the Security Management Platform.

Requirements

Configuration Worksheet

An example configuration worksheet is provided at the end of this guide and will prove a useful record should you need to reconfigure at a later stage. Before you begin the installation, please fill in your specific network details in lines 1-7, as you will need this information during the installation process, and they will be required throughout this guide.

Hardware

To perform a correct installation, 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 equipment units.
- the following appliances, either:
    - SEM 1065

or

    - SEM 3065

or

    - SEM 4065

TIBCO LogLogic® new (H4) Appliances (H4) come with an embedded SD card that contains an image of the Appliance software. This new feature will facilitate reimaging the Appliance in case of critical hardware or software failure. For instructions on how to use the backup image for recovery, please contact TIBCO LogLogic® support through the online support portal-

https://support.tibco.com/esupport/loglogic.htm

or email TIBCO LogLogic® support-

ll-support@tibco.com

Software

This guide covers the configuration of the SMP. Any other software referred to in this guide is assumed to be in its default configuration.

Chapter 2 - Installing SEM

[If No Appliance] Deploy SEM EVA Virtual Machine

TIBCO LogLogic® Security Event ManagerEnterprise Virtual Appliance (SEM EVA) can be deployed on VMware solutions.

For further details on VMware compatible software and requirements, please read carefully SEM EVA release notes.

To deploy SEM EVA:

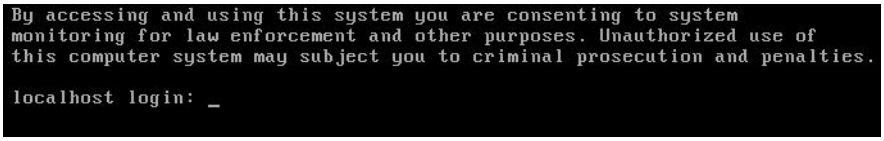
1. Download the *.ova file from https://download.tibco.com/tibco/.

2. Open your virtual machine editor and import the *.ova file.

3. Launch the file to start configuring the virtualized SEM.

This displays the login prompt:

Figure 1 Login prompt



Note: The keyboard is automatically set to US/UK (or QWERTY) by EVA to enter the login and password.

4. Follow the procedure described in the following chapter.

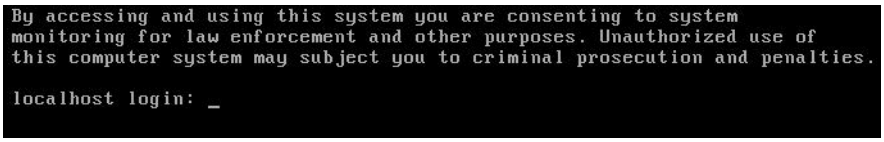
Initialize SEM

Set the Hostname and IP Configuration

1. Turn on the power.

This displays the login prompt:

Figure 2 Login prompt



2. For the `localhost login` prompt, enter **`admin`**, and then press **Return**.

3. For the `Password` prompt, enter the default password i.e. **`logapp`** and then press **Return**.

The TIBCO LogLogic® `licence agreement` is displayed.

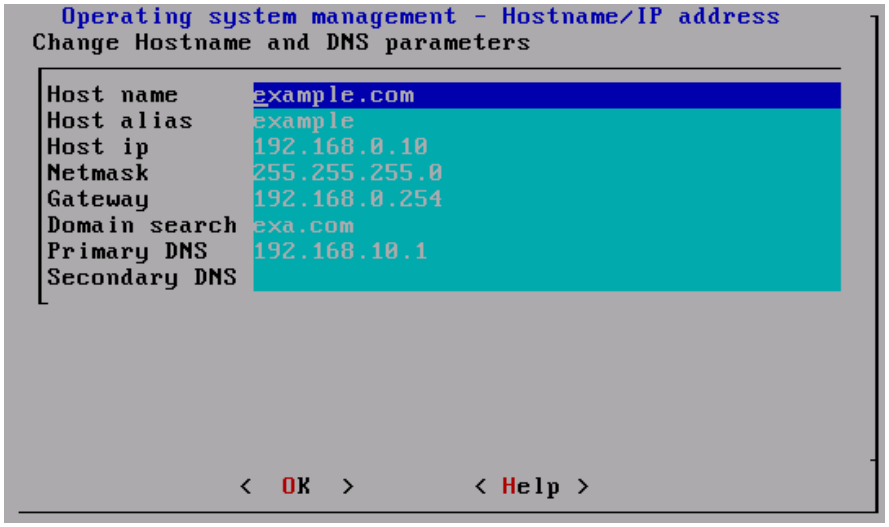
4. Use the up and down arrows on the keyboard to view the entire licence, and then select **`Continue`**.

5. On the next window, select **`YES`** to accept the licence. This displays the **Keyboard Type** window.

6. Select your required keyboard type, and then select `OK`.

The next step requires you to enter the hostname (FQDN) and IP configuration for the appliance. In the example shown below, the hostname is `example.exaprotect.com`:

Figure 3 Configure TCP/ IP window



7. Enter your hostname (FQDN) details, record them on line 1 of your configuration worksheet.

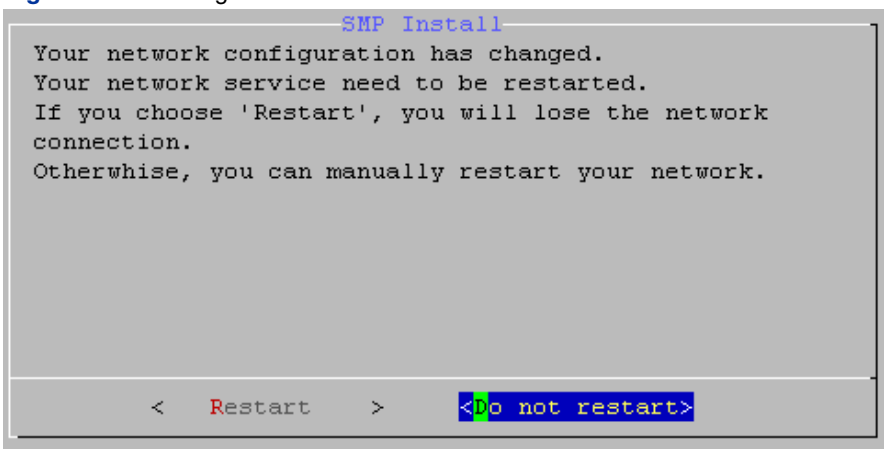
8. Using the Tab key to navigate around the window, enter the **`IP address`**, **`Netmask`**, **`Default gateway`**, **`domain search`**, and **`Primary and Secondary nameserver`** details for your SMP. Record your specific IP details in lines 2-5 of your configuration worksheet.

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

9. Press the Tab key until `OK` is highlighted, and then press **Return**.

The following warning screen is displayed.

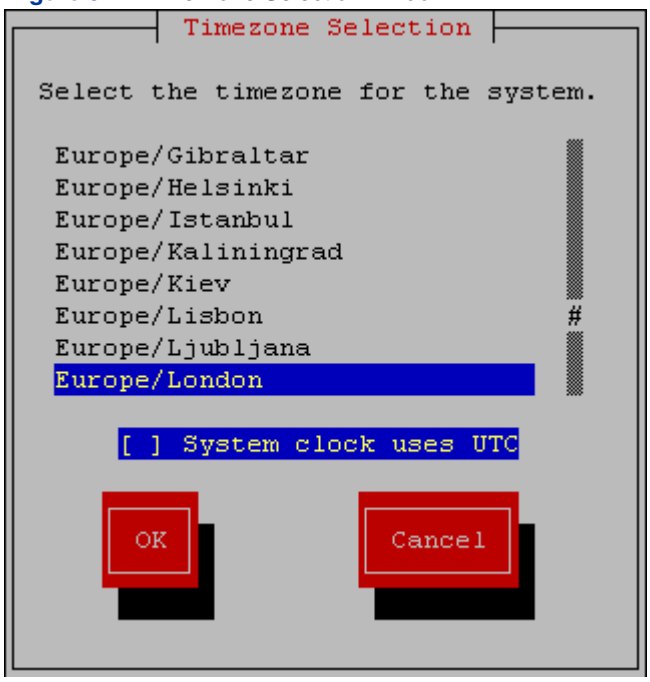
Figure 4 Warning screen



10. Select **Restart**.

This restarts the networking software and then displays the **Timezone Selection** window:

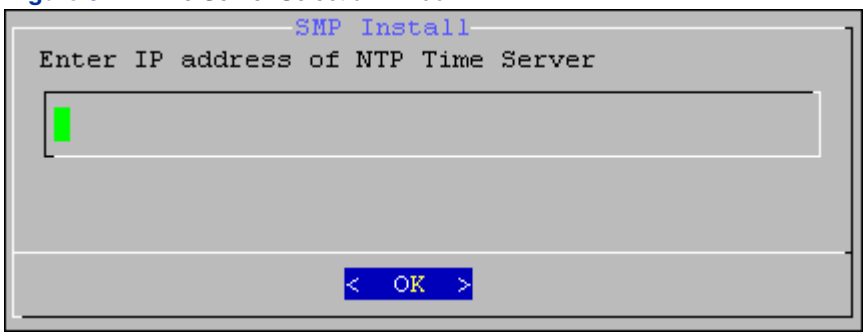
Figure 5 Time Zone Selection window



11. Using the Up and Down keys, select your timezone, and then press **Return**.

This displays the Time Server window:

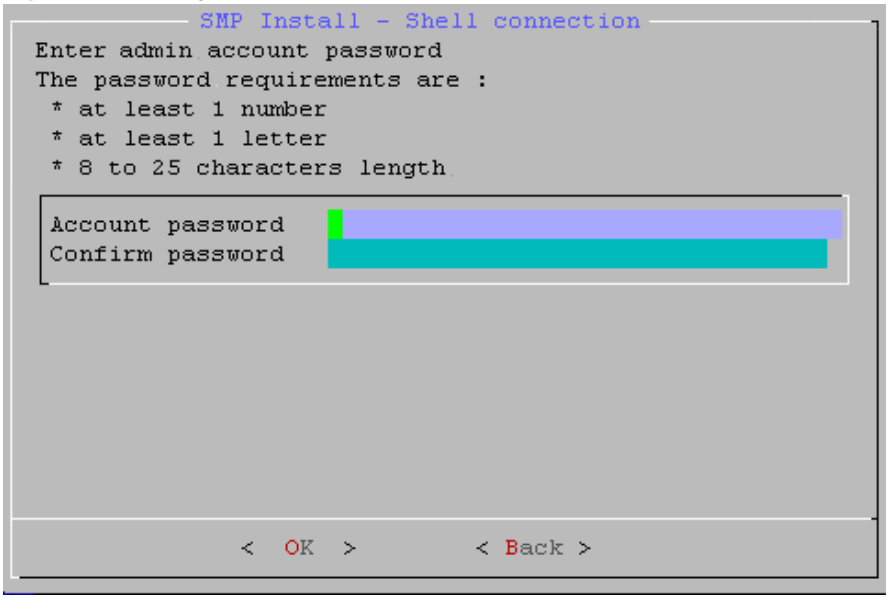
Figure 6 Time Server Selection window



12. Enter the IP address of your Network Time Protocol (NTP) Server, and then press **Return**. Please contact your network administrators to obtain details of the NTP Server.

The software currently has a default password, the next step is to create your new unique administration password:

Figure 7 Change password

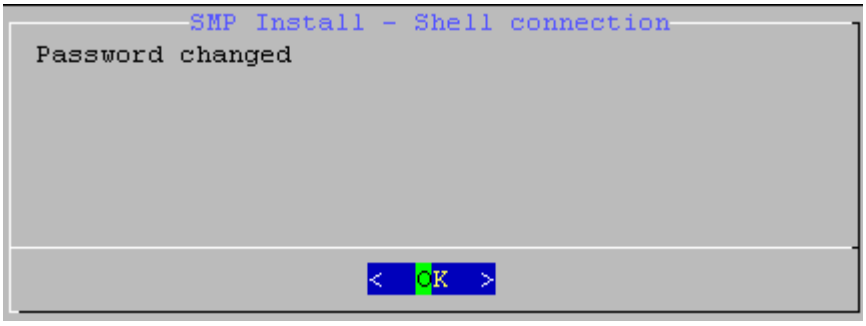


13. Enter a new password, and then press **Return**.

> **Note:** You must enter a password at least 8 characters long that includes at least one number and one letter.

14. Re-enter your password, and then press Return. You will see a confirmation window showing that the password has been changed.

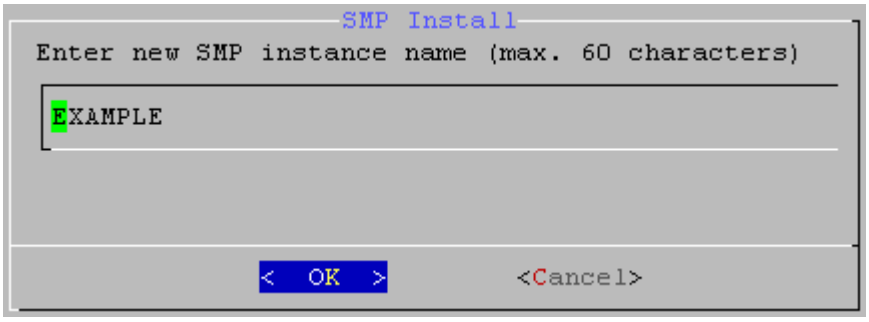
Figure 8 Password Confirmation window



Set the Instance Name and the Certificate Fingerprint

The next step consists of entering the name of the SMP instance.

Figure 9 Enter New Instance Name



An instance consists of:

- the configuration of which logs and supported products to monitor
- the collected events
- the rules and scenarios to apply to the collected events
- a console server (the Web Console Web GUI):

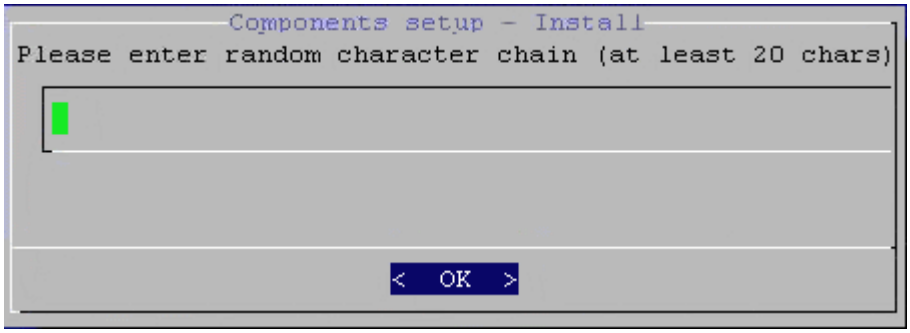
The name of your SMP instance will default to the hostname that you created earlier, in this case "EXAMPLE". The name of the SMP instance will be displayed on the Web Console login window. Record the instance name in line 7 of the configuration worksheet.

Caution: The instance name cannot be changed once created.

1. Accept the suggested SMP instance name, or enter a new one, and then press **Return**.

The **Components Setup** screen is displayed. This screen will allow you to to enter a random chain character in order to generate cryptographically secure keys.

Figure 10 Enter a Random Character Chain



2. Enter any characters (at least 20 characters) in the field and select **OK**.

At this point, the information store is populated. When this has completed the Certificate Fingerprint and the URL, for you to connect to the SMP is displayed.

Figure 11 Certificate Fingerprint and URL Information

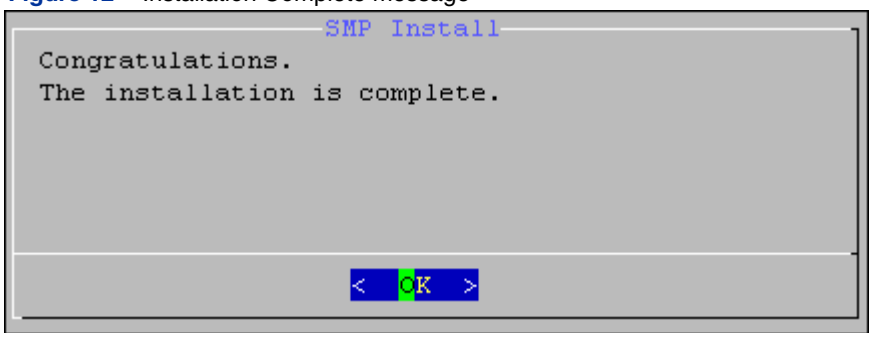
Note: Record the URL, displayed at the top of the screen, in line 9 of your worksheet. You will need this URL address to connect to the Web Console.

3. Using the Up and Down keys on your keyboard, scroll through the window until the **SHA1** certificate fingerprint is displayed.

> **Note:** Record the SHA1 Certificate fingerprint in line 8 of your configuration worksheet. This will be required later for verification purposes. This fingerprint is used to verify the Web Console connection later in the setup process.

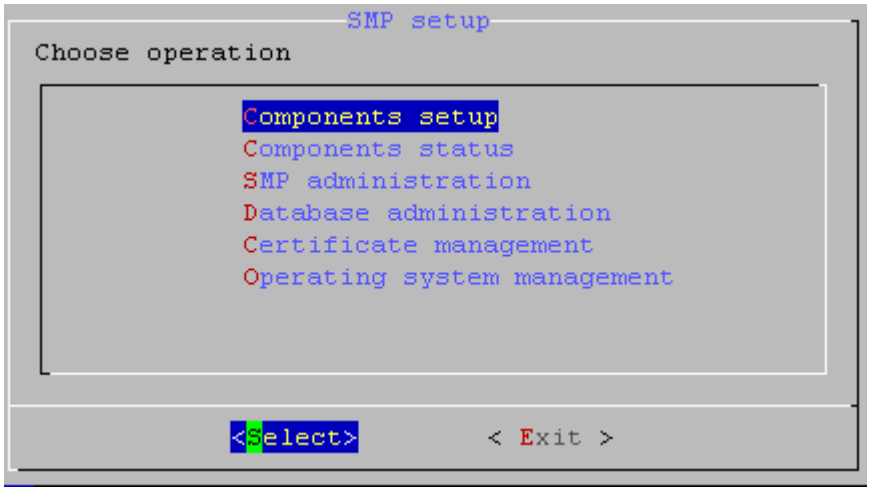
4. Press **Return**. The installation is now complete and a confirmation window is displayed:

Figure 12 Installation Complete message



5. Press **Return** to display the main SMP window.

Figure 13 SMP Main Setup window



6. If at this point you would like to make any changes to your instance setup, select the required menu item, and then choose **Select**. If you are happy with your instance setup, choose **Exit**.

Configure the Web Console

This section deals with the initial configuration of the Web Console (Web Console). The Web Console provides the visual interface to processed alerts, and displays the organization's current security status. Alerts are enriched with business information, allowing priorities to be set according to the business importance of the asset.

This section describes the initial setup of the Web Console. For further information on how to use the Web Console, please refer to the Web Console ***User Guide***.

1. On a networked PC, start your web browser.

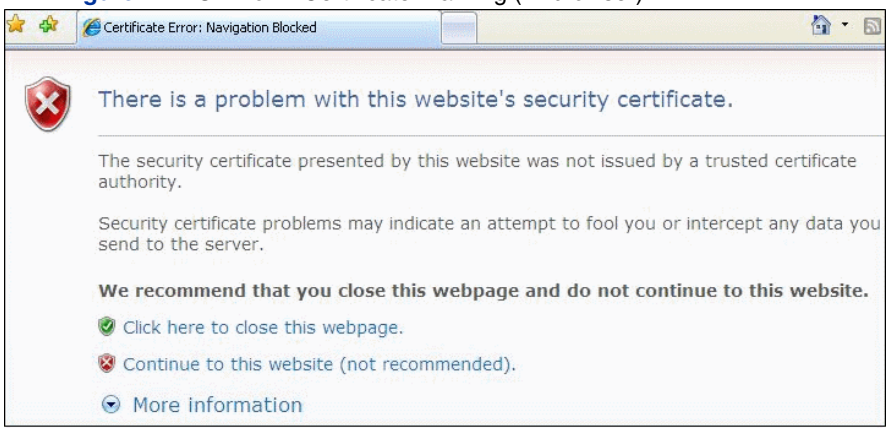
2. Enter your specific URL: this is recorded in line 9 of your configuration worksheet (see Table 1 "Configuration Worksheet").

This displays a Certificate Authenticity Warning which varies according to your web browser. The Internet Explorer and the Firefox procedures are described below.

On Internet Explorer

The following message will be displayed:

Figure 14 Unknown Certificate Warning (IE browser)



1. Click **Continue to this website (not recommended)**.

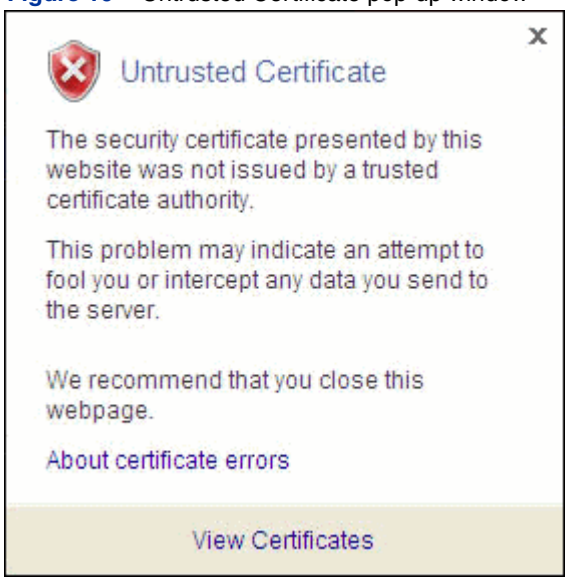
The Welcome screen is displayed. However in the menu bar, the following information is displayed:

Figure 15 Certificate Error in menu bar

2. Click on this error message.

The following pop-up window is displayed:

Figure 16 Untrusted Certificate pop-up window



3. Click **View Certificates** and then **Install Certificate**.

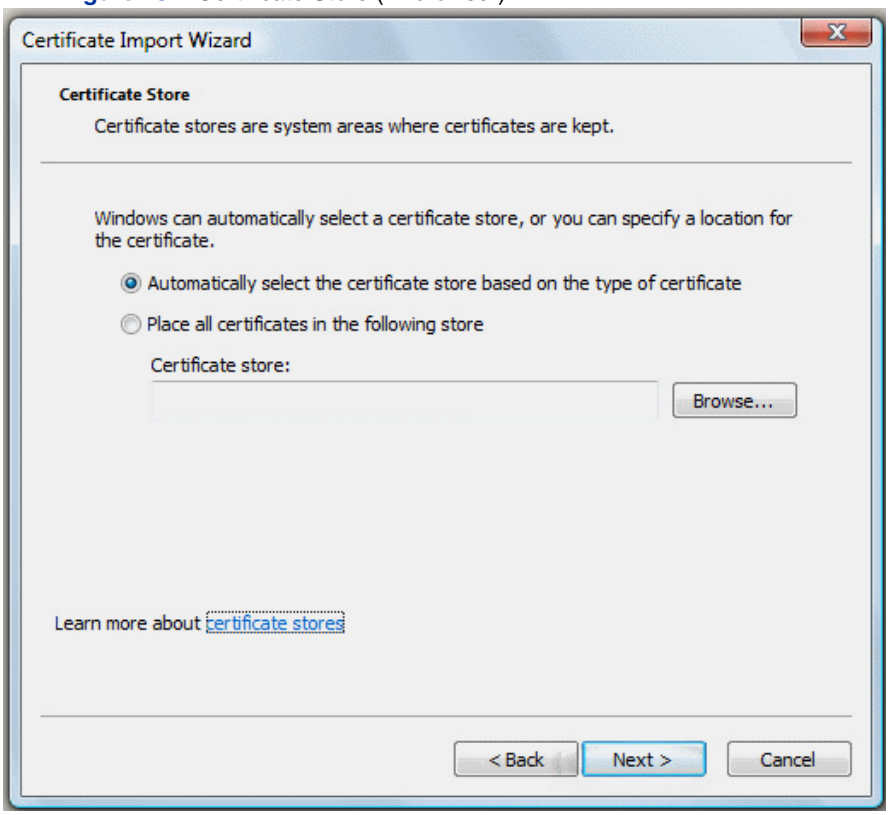
A **Certificate Import Wizard** opens.

Figure 17 Certificate Import Wizard (IE browser)

4. Click **Next**.

5. In the following window, ensure that the **Automatically select the certificate store...** radio button is selected and click **Next**.

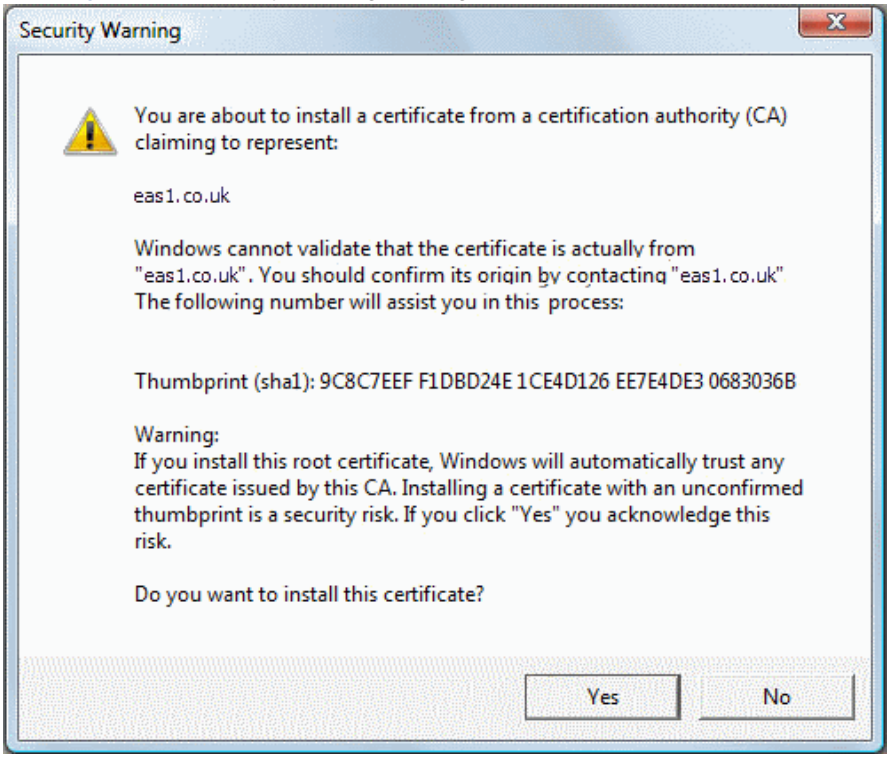
Figure 18 Certificate Store (IE browser)



6. Click **Finish** to complete the certificate importation.

A Security Warning message opens.

Figure 19 Security Warning message (IE browser)



7. Check that the fingerprint (referred to as a ***thumbprint***) matches the fingerprint of the SMP (recorded in line "8. Certificate Fingerprint" of the configuration worksheet). If it does match, click **Yes** and the certificate will be imported.

Figure 20 Successful Certificate Import (IE browser)

8. Click **OK** to validate.

On Firefox

Figure 21 Unknown Certificate Warning (Firefox browser)

To verify your SSL connection to the Web Console, you will need to check the Certificate to make sure that the SHA1 fingerprint is the same as you recorded (see line "8. Certificate Fingerprint" of your configuration worksheet) during the installation of the SMP.

1. Click **Add Exception...**. This displays the **Add Security Exception** window.

2. Click **Get Certificate.**

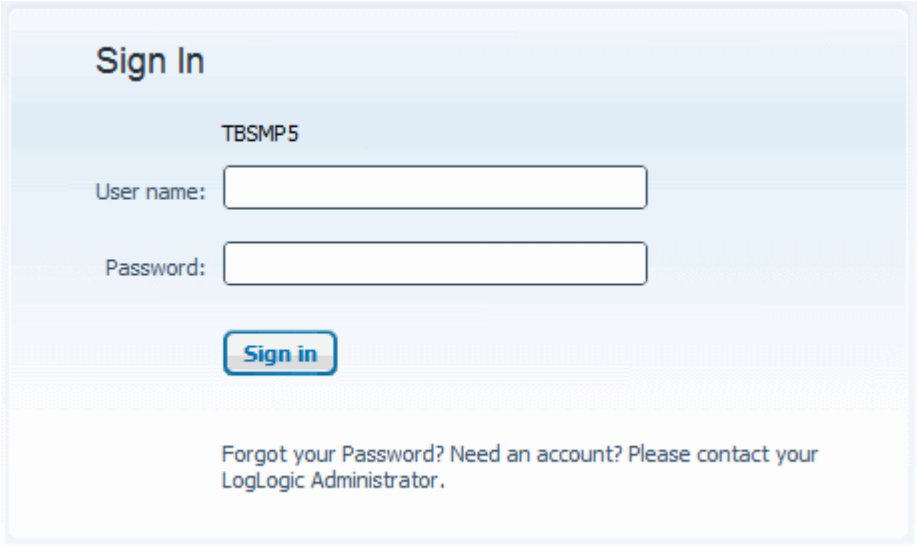
3. Click on the **View...** button to make sure that the SHA1 Fingerprint matches the one that you recorded during your SMP installation. When you have verified this, click **Close**.

4. Tick the **Permanently store this exception** checkbox.

5. Click **Confirm Security Exception**.

6. The Web Console Welcome screen is displayed:

Figure 22 Web Console Welcome screen



7. In the **Login** field enter `superadmin`.

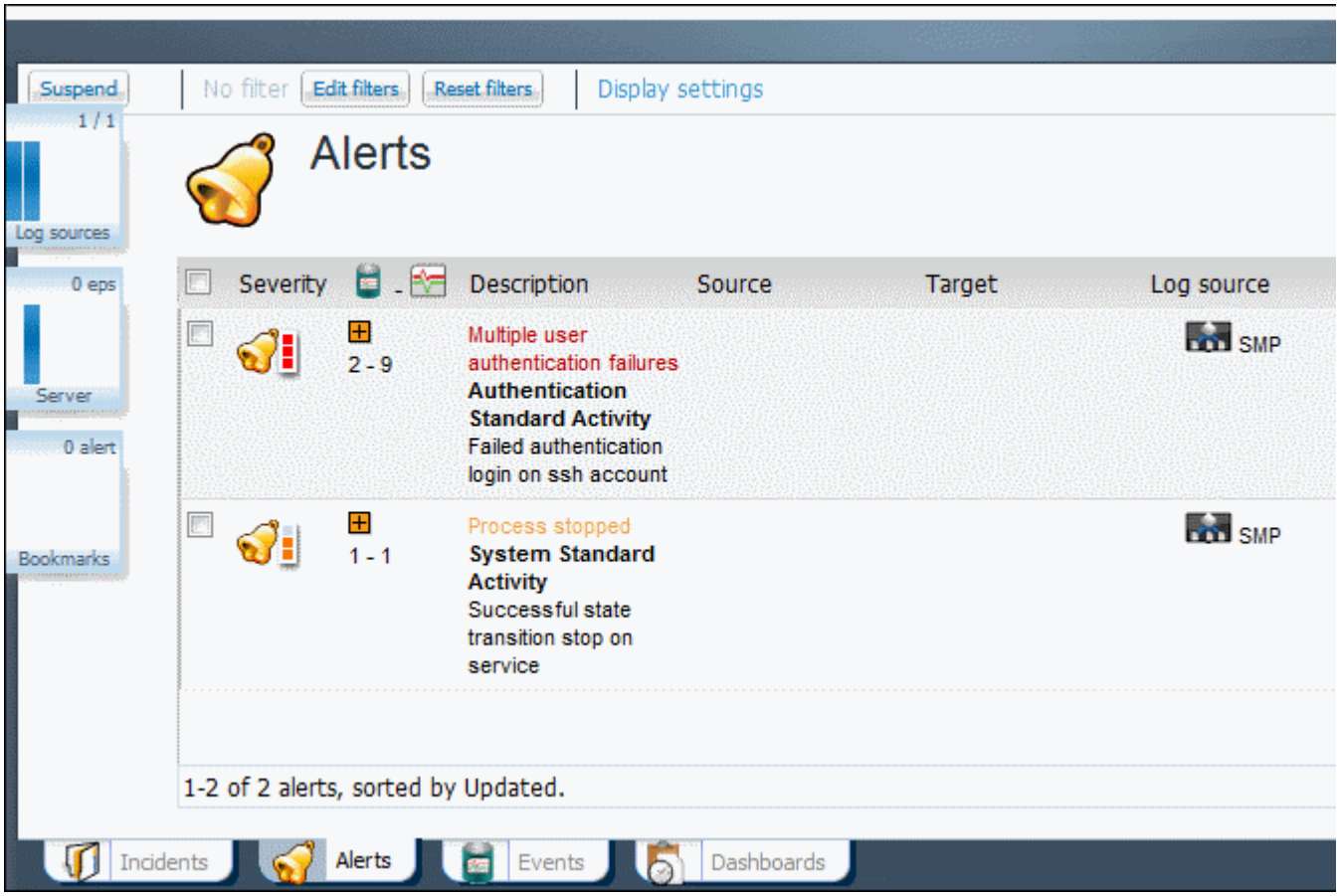
8. In the **Password** field enter `admin`.

> **Note:** This password is only for use with the Web Console; it is a separate account from the one created for use with the SMP command line interface.

9. Click **Log in**.

The monitoring window is displayed:

Figure 23 Monitoring window



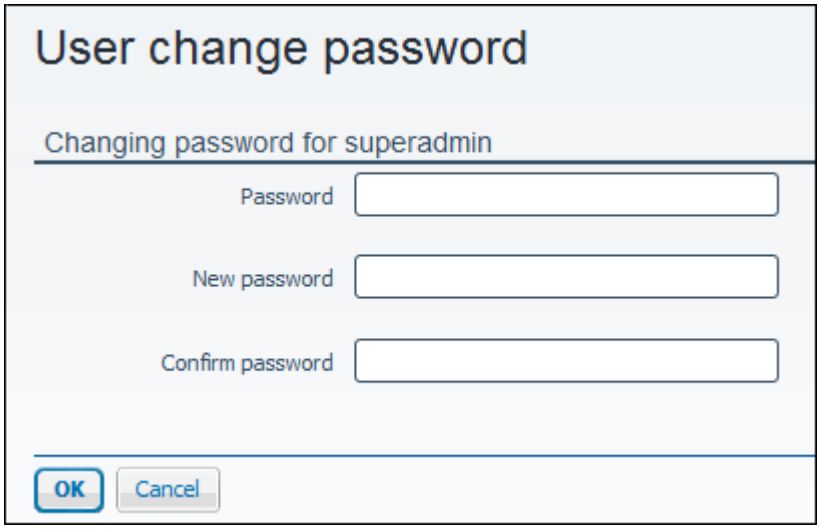
The **Monitoring** window provides a real-time view of the current security alerts, events or incidents, color coded to reflect severity and priority, and is the main screen of the Web Console. Each element can be explored through an intuitive drill-down interface to display its component events and enriched information about these events, including the original event log files.

The first alert shown in your screen shows your first login.

10. On the top right hand side of the Monitoring screen, click the link displaying the current logged-in user (i.e. `superadmin`). The page corresponding to this user account opens.

11. Click **Change the password**. The **Changing Password for Superadmin** window opens to let you change the superadmin password.

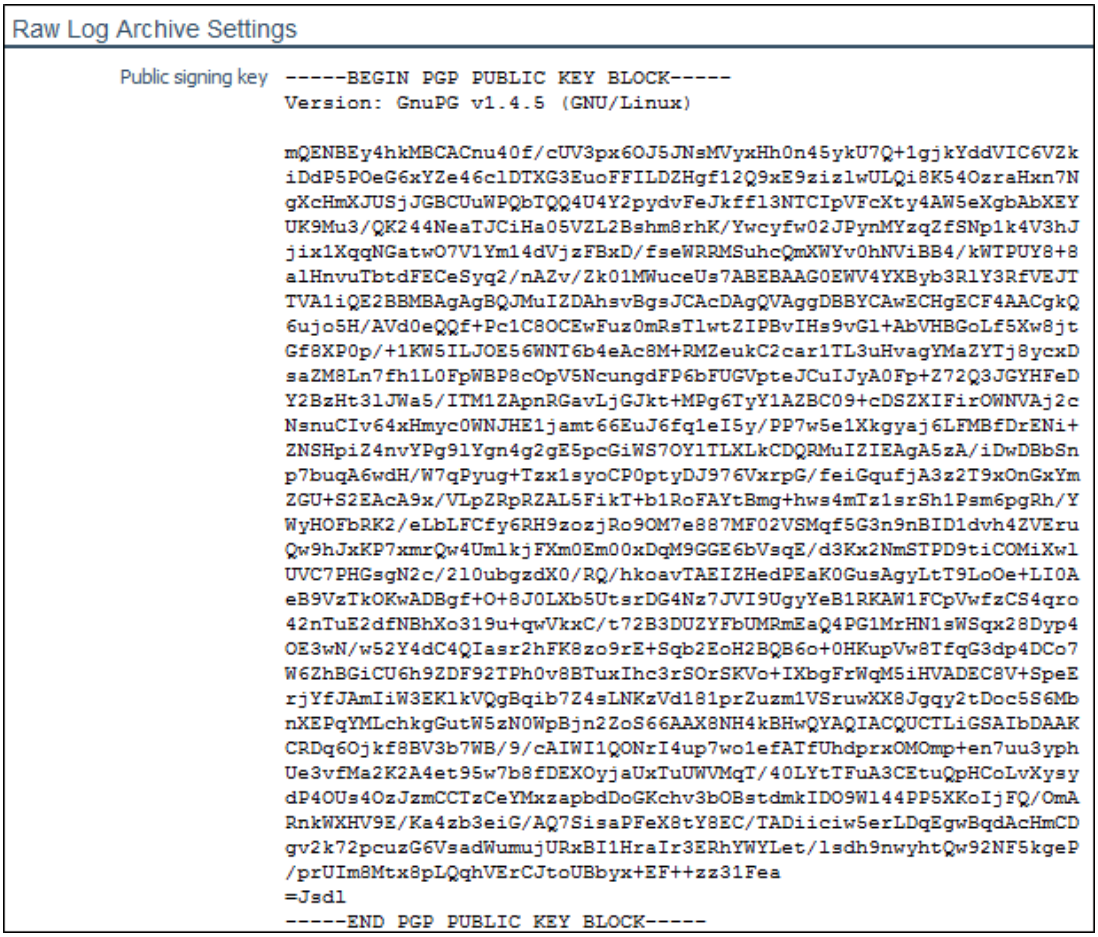
Figure 24 Change the superadmin Password



12. Set the new password and click **OK** to validate.

13. Now go to **Log Management > Archiving > Settings**. The following window is displayed:

Figure 25 Raw Log Archive Settings



The **Raw Log Archive Settings** screen contains the public key which allows to check if the archive has been signed by TIBCO LogLogic®.

14. Copy and paste the Public Signing Key in order to register it at a Trusted Third-Party or store it in a safe location.

The initial configuration of the Web Console is now complete.

Re-image SEM Appliance

This section covers the initial configuration of the SMP typically carried out at the factory by TIBCO LogLogic®. These instructions must be followed in case you have to reimage the appliance.

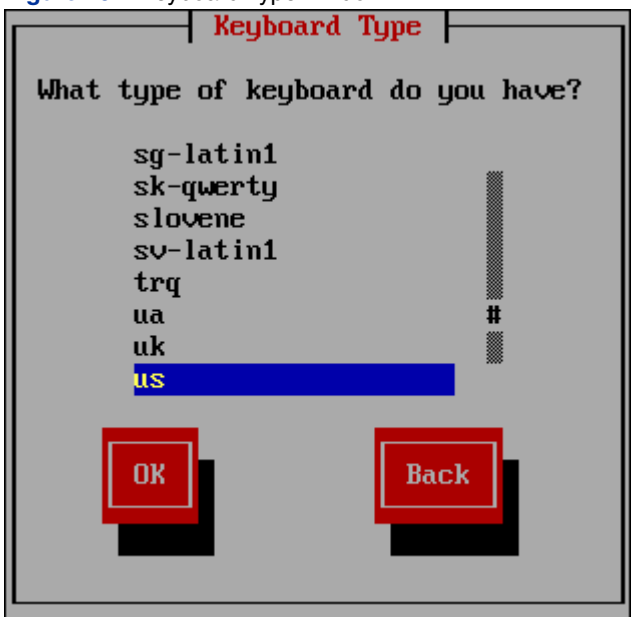
1. Ensure that a monitor and keyboard are connected to the SMP appliance.

On the appliance, switch on the power, and insert the TIBCO LogLogic® CD. The appliance will begin the boot process from the CD.

2. Press **Return** to start the software installation process.

After the initial boot process has completed, the Keyboard Type window is displayed:

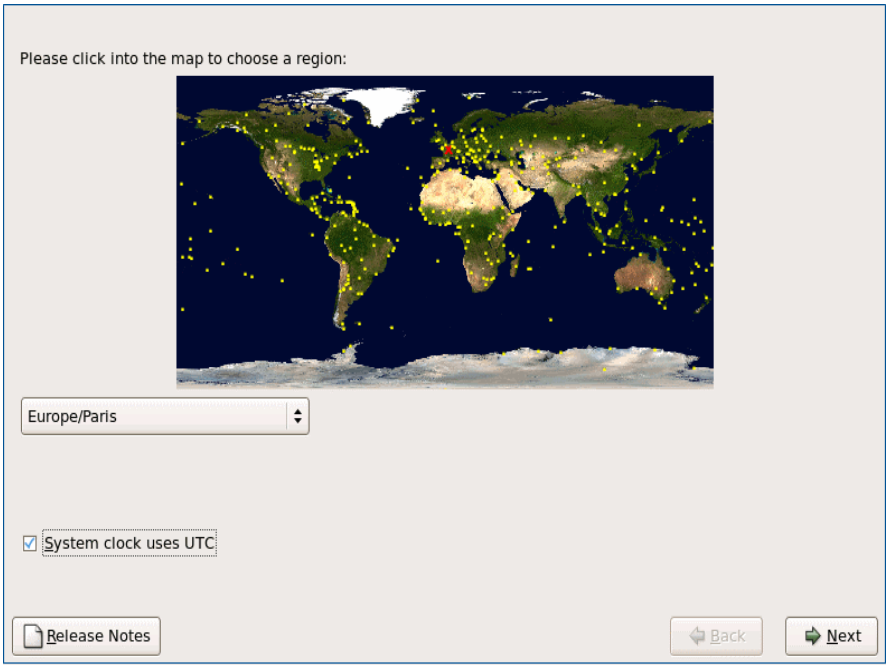
Figure 26 Keyboard Type window



3. Using the Up and Down arrows on your keyboard, select your keyboard type, and then select **OK**.

The **Time Zone** screen is displayed.

Figure 27 Time Zone



4. Select the relevant time zone in the drop-down list.

5. If you want the system clock to be set on the GMT time standard, check the **System clock uses UTC** box, then click **Next**.

The SMP software is copied and installed onto the appliance. During this process you will see a Package Installation window.

Installation covers the following processes:

- the hard drive is formatted and the file system created
- drivers are installed
- the Linux operating system is installed
- the SMP software and components are installed
- the database is created

When the installation of the software is complete, the media is ejected from the appliance, and the appliance reboots from the hard drive.

> **Note:** The Reboot screen that is displayed is set by default on `LogLogic-SEM` (i.e. multi-processing mode). Do not change this configuration.

On completion of the boot process, the login prompt is displayed:

Figure 28 Login prompt

```
By accessing and using this system you are consenting to system
monitoring for law enforcement and other purposes. Unauthorized use of
this computer system may subject you to criminal prosecution and penalties.

localhost login: _
```

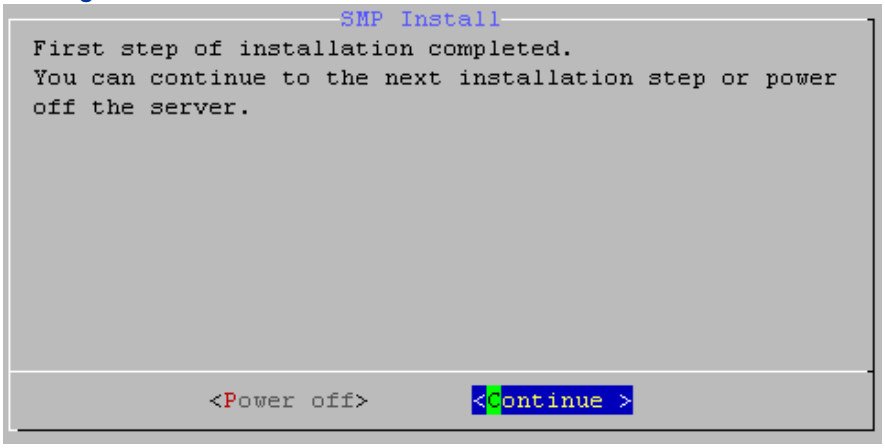
6. For the `localhost login` prompt, enter **`admin`**, and then press **Return**.

7. For the `Password` prompt, enter the default password i.e. **`logapp`** and then press **Return**.

The database file system and the database are then created. This phase usually takes more than one hour (it can take several hours for large disks).

When the database has been installed, the following window will be displayed:

Figure 29 SMP Install window



8. Phase 1 is the configuration performed at the TIBCO LogLogic® factory. The appliance is delivered to customers ready to perform Phase 2.

- If you are not going to continue with the configuration, select **`power off`**. When it displays the message `Power Down`, switch off the power.
- If you are going to continue with configuration, select **`Continue`** and continue with Phase 2.

9. Please follow the procedure described in chapter "Initialize SEM".

Chapter 3 - Updating SEM

For an optimal use of TIBCO LogLogic® Security Event Manager, it is recommended to update your SEM server, i.e. the appliance as well as the standard content, which is regularly enhanced to best meet your requirements. The updated standard content is detailed in the SEM Release Notes, section “Standard Content”.

The objective of this chapter is to learn how to apply a patch on a standard server to install new SMP Packages.

In order to migrate from a version to another one, you must apply all the intermediary versions or patches of Security Event Manager.

Examples:

To go from v3.3.1 to v3.6.0, you must apply v3.3.2, v3.4, v3.5, v3.5.1, v3.5.2 and 3.6.0.

List of all SEM versions:

- SEMv3.0
- SEM v3.1
- SEM v3.2
- SEM v3.3
- SEM v3.3.1
- SEM v3.3.2
- SEM v3.4
- SEM v3.5
- SEM v3.5.1
- SEM v3.5.2
- SEM v3.6.0

For more information, please contact our technical support at ll-support@tibco.com.

Caution: As an administrator, you should be aware that your current TIBCO LogLogic® version is fully functional, but it may be altered as fixes are implemented following bug discoveries. Therefore, it is highly important that you carefully read the e-mail notifications concerning SMP updates and download the available patches on the TIBCO LogLogic® website.

Updating the SMP

Downloading the Files for Update

You can get the updates files by accessing the download website.

To connect to the update site:

1. Go to https://download.tibco.com/tibco/
2. Enter your credentials.
3. Click on the files you want to download and save them on your disk.

4. Check the downloaded TIBCO LogLogic® packages integrity with the provided digest.

Activating the "Root" Connection on SMP Server

Now that the *.rpm files have been downloaded, you must prepare their installation on the server. To do so, you must first activate the "root" connection on the SMP server.

1. Open an SSH console.
2. With either a remote or local connection, identify yourself as `admin`.
3. In the **Operating System Management** submenu, use the **Up** and **Down** arrows to highlight **Shell Connection** and then click **Return**.
4. For more information about the "root" connection, please refer to the SEM ***Administration Guide*** (see SMP Advanced Configuration section).

Copying the *.rpm Files to the Server

Caution: The process of copying *.rpm files to the server must be secured.

There are two ways to copy the files you have just saved on your disk to the server:

- Copying and pasting the files with WinSCP, for example.
- Transferring files using a USB key.

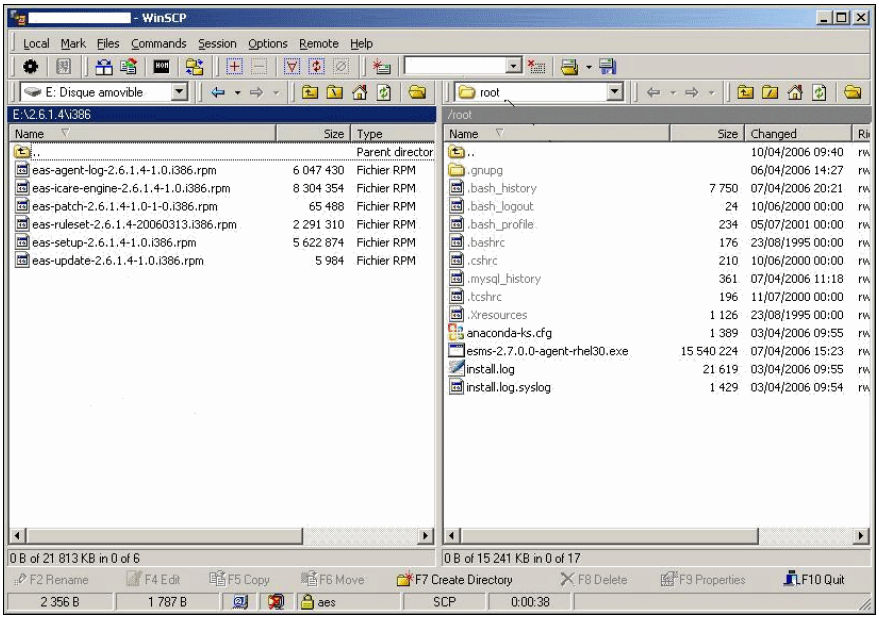
Copying the *.rpm Files via the Network Using the SCP Function

We will describe the way to copy the *.rpm files using the WinSCP software (downloadable at http://winscp.net) as a reference. Please note you must work on a Windows machine to use it.

Make sure you have enough free space on your file system before copying the *.rpm files. Otherwise, you will get an error message.

1. Open WinSCP on the machine where the *.rpm files have been downloaded.
2. Connect as "root" user to access SMP server in WinSCP.
3. Copy the files. Make sure the /tmp folder is displayed in the corresponding field.

Figure 30 WinSCP Interface



4. Open a shell as “root” user on the SMP server.

5. Enter the following command to apply the update:

```
yum --nogpgcheck --disablerepo=* localinstall *.rpm
```

6. Enter the following command to delete the *.rpm files:

```
rm -f /tmp/*.rpm
```

7. Restart the machine to take the modification into account.

> **Caution:** Do not forget to deactivate the “root” connection at the end of the procedure.

Transferring the *.rpm Files from a USB Key to the Server

> **Caution:** Make sure your USB key is compatible with the Operating System.

1. Plug the USB key on the SMP server.

2. Open a shell as “root” user.

3. Enter the following command to mount the USB key:

```
mount /mnt/flash.
```

This command can vary according to the RedHat version you use.

4. Enter the following command to copy the files from the USB key to the tmp folder:

```
yum --nogpgcheck --disablerepo=* localinstall /mnt/flash/*.rpm
```

5. Unmount the USB key.

6. Unplug the USB key.

> **Caution:** Do not forget to deactivate the “root” connection at the end of the procedure.

Deactivating the “Root” Connection on SMP Server

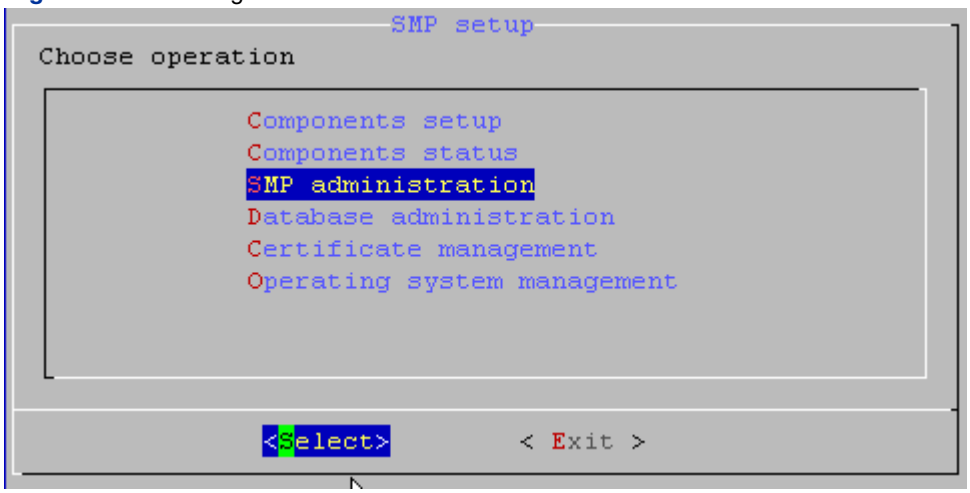
Now, the deactivation of the “root” account is required. Please refer to the ***Administration Guide*** for more information.

Updating the Server

Once you are finished with the update procedure, you must connect either in SSH mode or Console mode. You will need the admin account and a password.

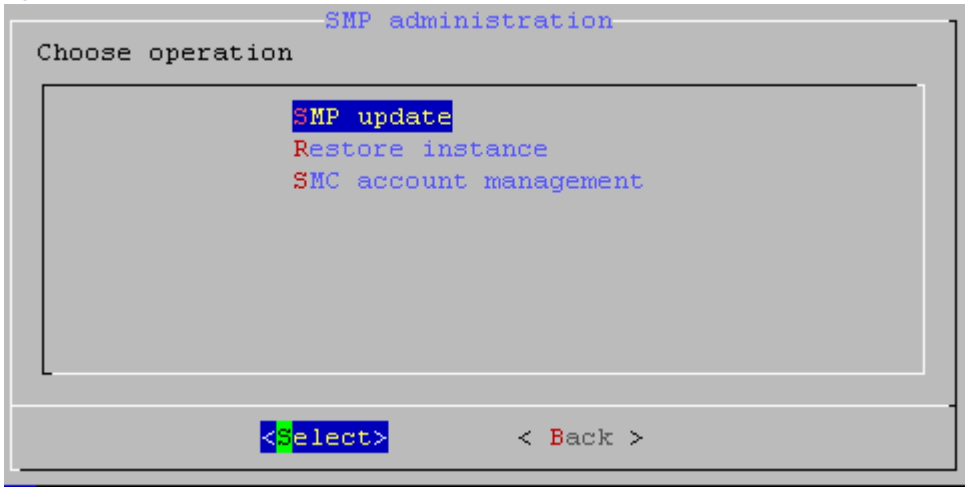
1. To open the SMP **Administration** menu, go to the main menu and select SMP **Administration**.

Figure 31 Choosing SMP Administration



The SMP Administration submenu is displayed:

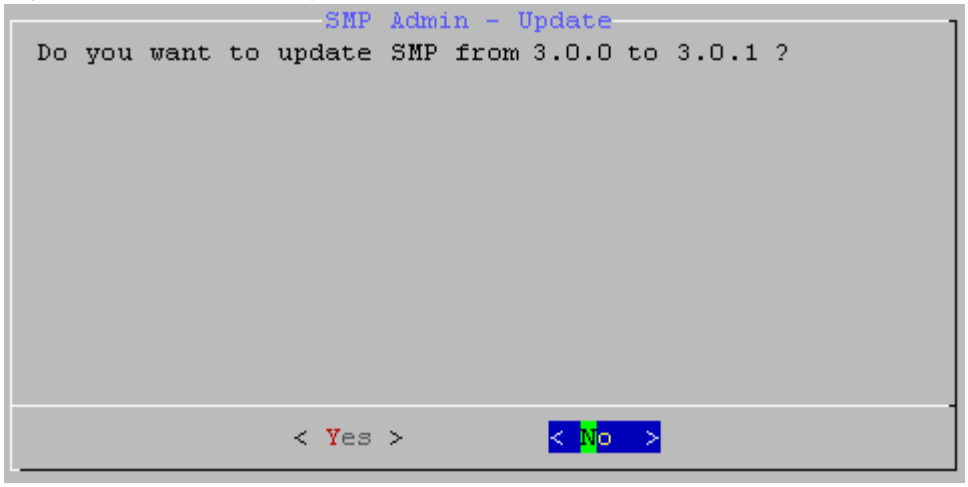
Figure 32 The SMP Administration submenu



2. Select SMP **Update.**

A screen asking you to confirm your choice is displayed. By default, the **No** option is selected.

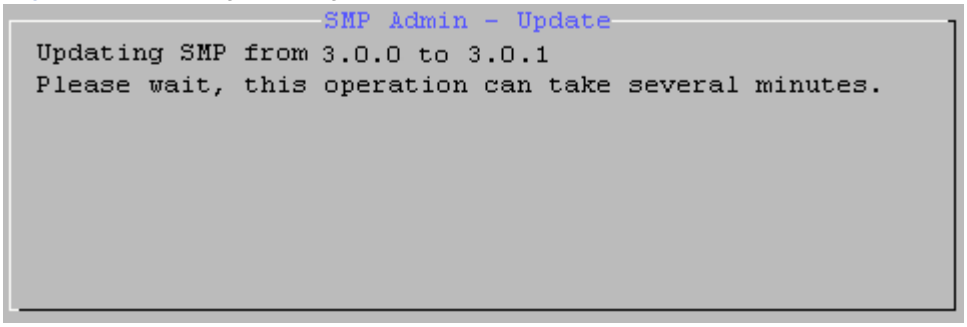
Figure 33 No is selected by default



3. Select the **Yes** option to start the updating process

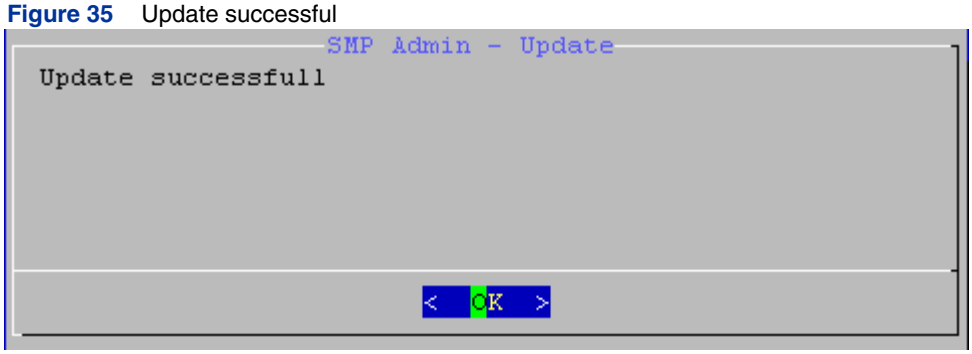
4. A screen is displayed to show you the updating progress.

Figure 34 Updating is in progress



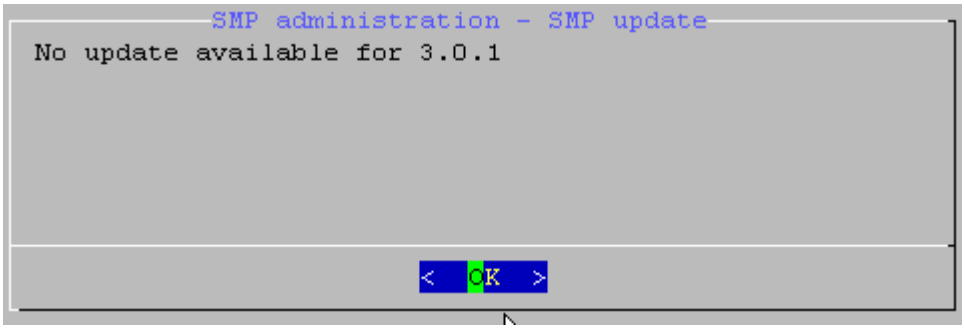
Once the update is finished, a message is displayed indicating that the update was successful.

Figure 35 Update successful



Note that if there is no available update, the following message will be displayed:

Figure 36 No available updates



Once the update installation starts, the server and the database will be stopped.

If you want to check that the update was successful, go to the Connection page: the version number should have changed.

Chapter 4 - LogLogic iDRAC Configuration

Beginning with H4 gear, LogLogic appliances will include the Dell iDRAC utility for more convenient low-level LogLogic appliance administration.

The iDRAC interface is available by local console, and also web interface. The web interface is enabled by default on all LogLogic appliances, and relies on the iDRAC designated interface being connected to the network infrastructure. If that interface is left disconnected, the iDRAC interface will not be accessible remotely, but will still be accessible in the local console.

By default on LogLogic appliances, the labeled iDRAC network interface will have an assigned static IPv4 address of 192.168.0.120/24. By connecting the iDRAC network interface to a network infrastructure, the iDRAC web interface will become available via HTTPS, at https://192.168.0.120 as well as telnet and SSH to the same default IP. Following are instructions on how to change that network connectivity from the local console.

Setting Up iDRAC IP Using iDRAC Settings Utility

To set up the iDRAC7 IP address:

1. Turn on the managed system.

2. Press **<F2>** during Power-on Self-test (POST).

3. In the **System Setup Main Menu** page, Select **iDRAC Settings**, using Down arrow key and press **Enter** key.

The **iDRAC Settings page** is displayed.

4. Select **Network** and press **Enter** key.

5. The **Network** page is displayed.

6. Specify the following settings:

- Network Settings
- Common Settings
- IPv4 Settings
- IPv6 Settings
- IPMI Settings
- VLAN Settings

7. Go back to the iDRAC settings page and press **Esc** key.

8. A pop up window is displayed with message "**Settings have changed. Do you want to save the changes?**" and two options "**Yes**" and "**No**".

9. Select "**Yes**" using arrow keys and press **Enter** key.

10. Press **Esc** key to go back to **System Setup Main Menu** and press **Esc** key to exit

11.A pop up window is displayed with message "**Are you sure you want to exit and reboot?**" and two options "**Yes**" and "**No**".

12. Select "**Yes**" using arrow keys and press **Enter** key.

13. The network information is saved and the system reboots.

It is also possible to configure iDRAC7 IP information remotely using the iDRAC web interface.

Disable iDRAC remote connectivity

The iDRAC remote connectivity feature can be disabled from the local console so it will not respond even if connected to a network interface-

To disable the iDRAC7 network interface:

1. Turn on the managed system.
2. Press **<F2>** during Power-on Self-test (POST).
3. In the **System Setup Main Menu** page, Select **iDRAC Settings**, using Down arrow key and press Enter key.

   The **iDRAC Settings** page is displayed.
4. Select **Network** and press **Enter** key.

   The **Network** page is displayed.
5. Specify the following settings:
   - Network Settings
6. Select "**Enable NIC**" using arrow keys and press **Enter** key.
   - Two options are displayed
   - Select **Disabled** using arrow keys and press **Enter** key.
7. Go back to the **iDRAC settings** page and press **Esc** key.
8. A pop up window is displayed with message "**Settings have changed. Do you want to save the changes?**" and two options "**Yes**" and "**No**".
9. Select "**Yes**" using arrow keys and press **Enter** key.
10. Press **Esc** key to go back to **System Setup Main Menu** and press **Esc** key to exit.
11. A pop up window is displayed with message "**Are you sure you want to exit and reboot**?" and two options "**Yes**" and "**No**".
12. Select "**Yes**" using arrow keys and press **Enter** key.
13. The network information is saved and the system reboots.

It is also possible to disable iDRAC7 network connectivity information remotely using the iDRAC web interface.

Logging in to the iDRAC console

The iDRAC console supports several variations for logging in- Local User, Active Directory, and LDAP. Active Directory and LDAP authentication will not be discussed, as those methods are documented by Dell.

It is important to know that by default, LogLogic appliances will have a Local User account with the user name root and password calvin. It is advisable to change those credentials if iDRAC will be used over the network. Users accessing iDRAC locally at the console do not use the credentials.

To configure local users in the iDRAC7 local console:

1. Turn on the managed system.
2. Press **<F2>** during Power-on Self-test (POST).

3. In the **System Setup Main Menu** page, select **iDRAC Settings**, using Down arrow key and press **Enter** key.

The **iDRAC Settings** page is displayed.

4. Go to **User Configuration** using arrow keys and press **Enter** key

- A page with all **User configuration fields** is displayed

5. Configure the following fields-

- User Name
- Lan User Privilege
- Serial Port User Privilege
- Change Password

6. Go back to the i**DRAC settings** page and press Esc key.

7. A pop up window is displayed with message "**Settings have changed. Do you want to save the changes?**" and two options "**Yes**" and "**No**".

8. Select "**Yes**" using arrow keys and press **Enter** key.

9. Press **Esc** key to go back to **System Setup Main Menu** and press **Esc** key to exit.

10.A pop up window is displayed with message "**Are you sure you want to exit and reboot?**" and two options "**Yes**" and "**No**".

11. Select "**Yes**" using arrow keys and press **Enter** key.

12. The network information is saved and the system reboots.

It is also possible to configure users and change information using the iDRAC web interface.

Appendix A - Configuration Worksheet

Please use this worksheet to record your own unique configuration details.

Table 1 Configuration Worksheet

Item	Value
1. FQDN of the Security Management Platform	e.g. example.loglogic.com
2. IP address	e.g. 192.168.0.101
3. Netmask	e.g. 255.255.255.0
4. Default Gateway	e.g. 192.168.0.1
5. Primary nameserver	e.g. 192.168.0.1
6. Administrative Password	
7. Instance name	e.g. EXAMPLE
8. Certificate Fingerprint	e.g.61:B2:9E:BE:E0:19:A5:D6:5F:F5:10:29:B1:8B:10:0D:A5
9. Web Console URL	e.g. https://example.loglogic.com