Oracle® Communications

EAGLE LNP Application Processor Security Guide



Release 11.1
G63366-01
October 2026

Oracle Communications EAGLE LNP Application Processor Security Guide, Release 11.1

G63366-01

Copyright © 2000, 2026, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Oracle customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

Contents

1 Introduction

1.1 Overview 1
1.2 Scope and Audience 1
1.3 Documentation Admonishments 1
1.4 Manual Organization 2
1.5 Related Publications 2
1.6 Locate Product Documentation on the Oracle Help Center Site 2

2 ELAP Security Overview

2.1 Basic Security Considerations 1
2.2 Overview of ELAP Security 1
2.3 Root User Is Disabled for SSH Login 2

3 Implementing ELAP Security

3.1 ELAP Support for HTTPS on GUI 1
3.2 User and Group Administration 1
3.3 User Authentication 3
3.4 Modifying System Defaults 4
3.5 Authorized IP Addresses 4
3.6 Secure File Transfer Protocol 4
3.7 Installing an SSL Certificate For a Provisionable Interface With Customized Parameters 4
3.8 Installing an SSL Certificate For a Provisionable Interface From a Trusted Certificate Authority 6
3.9 Installing an SSL Certificate For a VIP With Customized Parameters 9
3.10 Installing an SSL Certificate For a VIP From a Trusted Certificate Authority 11

A Configuring IPSec for Secure Packet Transmission between All Hosts

Copyright © 2000, 2026, Oracle and/or its affiliates.

B Secure Deployment Checklist

B.1 ELAP Firewall Port Assignments B-1

C Secure Turnover to Customer

C.1 Secure Turnover Process C-1

Copyright © 2000, 2026, Oracle and/or its affiliates.

My Oracle Support

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support can assist you with My Oracle Support registration.

Call the Customer Access Support main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

- For Technical issues such as creating a new Service Request (SR), select **1**.
- For Non-technical issues such as registration or assistance with My Oracle Support, select **2**.
- For Hardware, Networking and Solaris Operating System Support, select **3**.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

Copyright © 2000, 2026, Oracle and/or its affiliates.

What's New in This Guide

This section introduces the documentation updates for Release 11.1 in Oracle Communications EAGLE LNP Application Processor Security Guide.

Release 11.1 - G63366-01, October 2026

There are no updates to this guide in this release.

Copyright © 2000, 2026, Oracle and/or its affiliates.

1 Introduction

This chapter contains general information such as an overview of the manual, how to get technical assistance, and where to find additional information.

1.1 Overview

This document provides guidelines and recommendations for configuring the Oracle Communications EAGLE **LNP** Application Processor (**ELAP**) to enhance the security of the system. The recommendations herein are optional and should be considered along with the approved security strategies of your organization. Additional configuration changes that are not included herein are not recommended and may hinder the product's operation or Oracle's capability to provide appropriate support.

1.2 Scope and Audience

This guide is intended for administrators that are responsible for product and network security.

1.3 Documentation Admonishments

Admonishments are icons and text throughout this manual that alert the reader to assure personal safety, to minimize possible service interruptions, and to warn of the potential for equipment damage.

Table 1-1 Admonishments

Icon	Description
	Danger: (This icon and text indicate the possibility of *personal injury*.)
	Warning: (This icon and text indicate the possibility of *equipment damage*.)
	Caution: (This icon and text indicate the possibility of *service interruption*.)
	Topple: (This icon and text indicate the possibility of *personal injury* and *equipment damage*.)

Copyright © 2000, 2026, Oracle and/or its affiliates.

1.4 Manual Organization

This manual contains the following chapters:

- Introduction contains general information such as an overview of the manual, how to get technical assistance, and where to find more information.
- ELAP Security Overview describes basic security considerations and provides an overview of ELAP security.
- Implementing ELAP Security explains ELAP security features.
- Secure Deployment Checklist contains a security checklist to help secure ELAP.
- Secure Turnover to Customer describes the secure turnover process to ensure the security of delivered systems.

1.5 Related Publications

For information about additional publications related to this document, refer to the Oracle Help Center site. See Locate Product Documentation on the Oracle Help Center Site for more information on related product publications.

1.6 Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, http://docs.oracle.com. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at http://www.adobe.com.

1. Access the Oracle Help Center site at http://docs.oracle.com.
2. Click `Industries`.
3. Under the Oracle Communications subheading, click the `Oracle Communications documentation` link.

   The Communications Documentation page appears. Most products covered by these documentation sets will appear under the headings "Network Session Delivery and Control Infrastructure" or "Platforms."
4. Click on your Product and then the Release Number.

   A list of the entire documentation set for the selected product and release appears.
5. To download a file to your location, right-click the PDF link, select `Save target as` (or similar command based on your browser), and save to a local folder.

Copyright © 2000, 2026, Oracle and/or its affiliates.

2
ELAP Security Overview

This chapter describes basic security considerations and provides an overview of ELAP security.

2.1 Basic Security Considerations

The following principles are fundamental to using any application securely:

- **Keep software up to date.** This includes the latest product release and any patches that apply to it. Consult with your Oracle support team to plan for ELAP software upgrades.
- **Limit privileges as much as possible.** Users should be given only the access necessary to perform their work. User privileges should be reviewed periodically to determine relevance to current work requirements.
- **Monitor system activity.** Establish who should access which system components, and how often, and monitor those components.
- **Install software securely.** For example, use firewalls, secure protocols such as **SSL**, and strong passwords.
- **Learn about and use the ELAP security features.** See Implementing ELAP Security for more information.
- **Keep up to date on security information.** Oracle regularly issues security-related patch updates and security alerts. You must install all security patches as soon as possible. See the "Critical Patch Updates and Security Alerts" Web site: http://www.oracle.com/technetwork/topics/security/alerts-086861.html

2.2 Overview of ELAP Security

The main functions of the ELAP are:

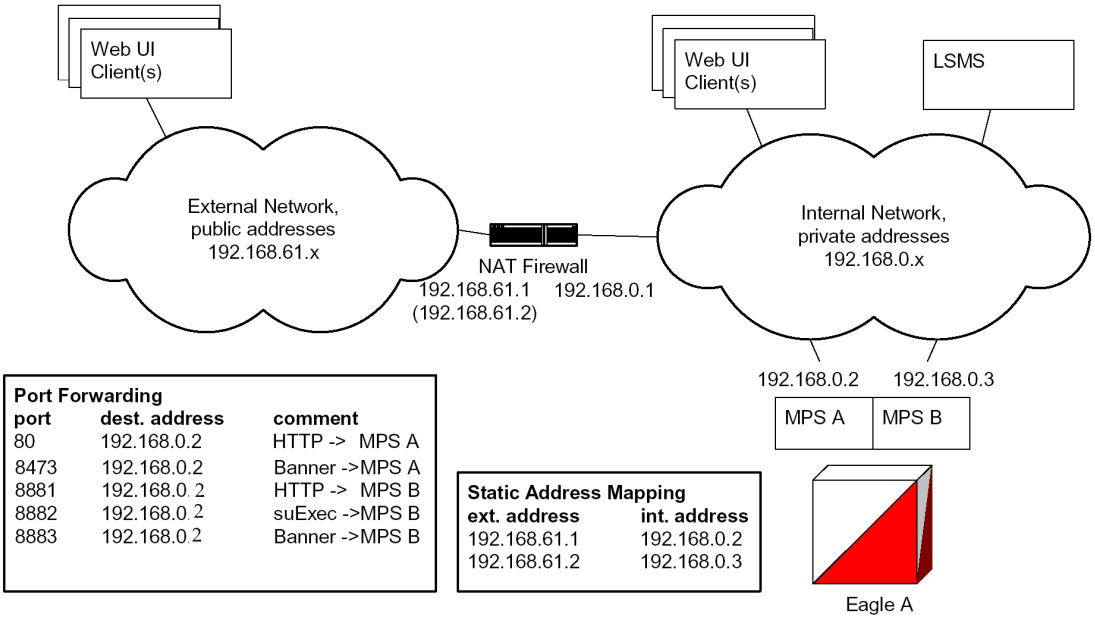
- Accept and store data provisioned by the customer from LSMS over the provisioning network
- Update and reload provisioning data to the EAGLE Service Module cards

The Multi-Purpose Server (**MPS**) hardware platform supports high-speed provisioning of large databases for the EAGLE. The MPS system is composed of hardware and software components that interact to create a secure and reliable platform.

As shown in Figure 2-1, the MPS supports two types of network address translation (**NAT**), Port Forwarding and Static Address Mapping. In both cases, the MPS will have private IP addresses that are not available outside of the firewall-protected internal network. The firewall will translate particular addresses and port numbers to the internal addresses for the MPS.

Copyright © 2000, 2026, Oracle and/or its affiliates.

Figure 2-1 Generic ELAP Deployment Model



> **Note**
>
> The addresses in Figure 2-1 are examples. Addresses are not restricted to particular classes/ranges. Port assignments are shown in ELAP Firewall Port Assignments.

The ELAP provides two user interfaces (UIs):

- Text-based UI
- Graphical UI (GUI)

Before you can use the GUI, you must use the text-based UI to initialize and configure the ELAP software. For information, see *ELAP Initialization and First Configuration* and *ELAP Software Configuration* in *Administration and LNP Feature Activation Guide*.

> **Note**
>
> After a fresh installation of ELAP, the GUI is accessible via the HTTPS protocol only, which supports encryption of data exchanged between the web server and the browser. For more information, see *ELAP Support for HTTPS on GUI* in *Administration and LNP Feature Activation Guide*.

For more information about the overall design and functions of the ELAP, see the *ELAP Functional Description* in *Administration and LNP Feature Activation Guide*.

2.3 Root User Is Disabled for SSH Login

The root user can log in through the serial interface for installation of the application. The root user will not have the permission to log in as an **SSH** user.

Copyright © 2000, 2026, Oracle and/or its affiliates.

To login as an **SSH** user, the user admusr is provided. The admusr can run all commands, and when root permissions are required `sudo` can be used along with admusr.

Copyright © 2000, 2026, Oracle and/or its affiliates.

3
Implementing ELAP Security

This chapter explains security related configuration settings that may be applied to the ELAP.

3.1 ELAP Support for HTTPS on GUI

The *ELAP Support for HTTPS on GUI* feature enables the use of the HTTPS protocol, which supports encryption of data exchanged between the web server and the browser. After a fresh installation of ELAP, the GUI is accessible via HTTPS only; the HTTP protocol is disabled since there is no encryption. For more information, see *ELAP Support for HTTPS on GUI* in *Administration and LNP Feature Activation Guide*.

3.2 User and Group Administration

The ELAP user interface (**UI**) comes pre-defined with UI users to provide a seamless transition to the GUI. For instance, there is a pre-defined user that is used to access the **User Administration** menu, as shown in Table 3-1.

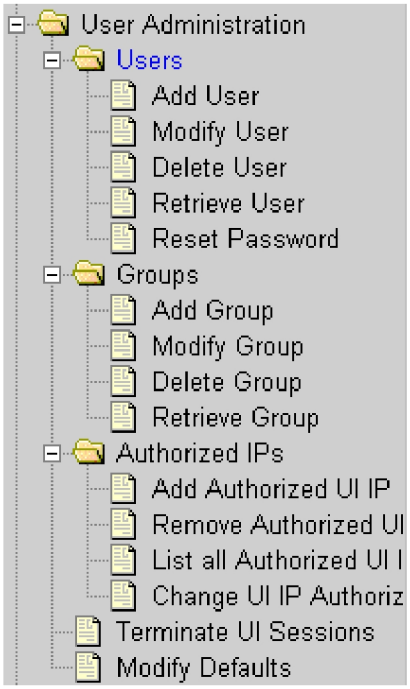
Table 3-1 ELAP UI Logins

Login Name	Access Granted
elapmaint	Maintenance menu and all submenus
elapdatabase	Database menu and all submenus
elapdebug	Debug menu and all submenus
elapplatform	Platform menu and all submenus
uiadmin	User Administration menu
elapall	All of the above menus
elapconfig	Configuration menu and all submenus (text-based UI)

The **User Administration** menu is used to set up and perform administrative functions for users and groups, and also to maintain an authorized IP address list, terminate active sessions, and modify system defaults.

Copyright © 2000, 2026, Oracle and/or its affiliates.

Figure 3-1 User Administration Menu



Establishing Groups and Group Privileges

Each user is assigned to a group, and permissions to a set of functions are assigned to the group. The permissions determine the functions and restrictions for the users belonging to the group. ELAP users can fall into one of the following default groups:

- maint
- database
- platform
- debug
- admin
- readonly

The readonly group is the default group for new users. The readonly group contains only actions that view status and information.

The **User Administration**, and then **Groups** menu allows administrator access to group functions to add, modify, delete, and retrieve a group. For more information, see *Groups Menu* under *User Administration Menu* in *Administration and LNP Feature Activation Guide*.

Creating Users and Assigning to Groups

Each user that is allowed access to the user interface is assigned a unique username. This username and associated password must be provided during login.

Prior to adding a user, determine which group the user should be assigned based on their operational role. The group assignment determines the functions that a user can access. After determining the proper group for a user, use the **User Administration**, and then **Users** menu to add the user.

Copyright © 2000, 2026, Oracle and/or its affiliates.

In addition to the group permissions that apply to a user, the administrator can set other user-specific permissions or restrictions for a specific user when adding the user. The **User Administration**, and then **Users** menu can also be used to modify, delete, and retrieve user accounts, and to reset passwords. For more information, see *Users Menu* under *User Administration Menu* in *Administration and LNP Feature Activation Guide*.

3.3 User Authentication

Users are authenticated through a unique username and password when logging in to the UI. The following rules govern passwords:

- Must be at least eight characters in length
- Must include at least one alpha character
- Must include at least one numeric character
- Must not contain three or more of the same alphanumeric character in a row
- Must not contain three or more consecutive ascending or descending alphanumeric characters in a row
- Must not contain the user account name or its reverse
- Must contain at least one of the following special punctuation characters: question mark (?), period (.), exclamation point (!), comma (,), or semi-colon(;)
- Must not use blank, null, or default passwords

The system administrator can change password-related default settings, such as maximum password age and password reuse limit. For information, see Modifying System Defaults.

Changing Default Passwords

As a security measure, the passwords for the default ELAP UI users (for example, uiadmin) and operating system users (for example, root) must be changed from their default values to user-defined values. For more information, see Secure Turnover to Customer.

Changing User Passwords

The **Change Password** screen available from the ELAP GUI main menu provides all ELAP users with the capability to change their password. To change the password, the current password must be entered, then the new password is entered. The new password is confirmed by retyping the new password and clicking the Set Password button.

Password Change for System Users

The elapdev and appuser users can use the passwd command provided by the operating system. If changing a password using the passwd command, then the Linux PAM credit rules are used.

The system user elapconfig uses the option provided in the ELAP Configuration Menu. Linux PAM rules are not applicable while changing the password for the elapconfig user. Only the configured minimum password length applies.

> **Note**
>
> If the password for the appuser or elapconfig user is changed by the root user, the appuser or elapconfig user will be prompted to change the password again.

Copyright © 2000, 2026, Oracle and/or its affiliates.

Resetting a User Password

The **User Administration**, and then **Users**, and then **Reset Password** screen enables the system administrator to select a username and change the associated password.

3.4 Modifying System Defaults

The **User Administration**, and then **Modify Defaults** screen enables the administrator to manage system defaults. Following are examples of the system defaults that you can modify from this screen:

- Maximum failed user login attempts before disabling a user account
- Maximum number of days that a user account can be inactive until it is automatically disabled
- Maximum number of days before a user password must be changed
- Number of unique passwords required before a previously used password can be reused

For a complete list and more information, see *Modify System Defaults* under *User Administration Menu* in *Administration and LNP Feature Activation Guide*.

3.5 Authorized IP Addresses

ELAP security functions limit access to the ELAP GUI to specific IP addresses. The specified allowed IP addresses are kept in an ELAP list that can be added to, deleted from, and retrieved only by an authorized user. These functions also allow an authorized user to use the GUI to toggle authorized IP address checking to be on or off. The **User Administration**, and then **Authorized IPs** menu enables you to add, remove, and list authorized UI IP addresses, and to change the UI IP address authorization status.

For more information, see *ELAP Security Functions* and *Authorized IP Address Menu* under *User Administration Menu* in *Administration and LNP Feature Activation Guide*.

3.6 Secure File Transfer Protocol

The ELAP supports secure File Transfer Protocol (**FTPS**) sessions with external servers for transfer of various files from the ELAP. The authentication process requires a self-signed digital certificate (user name & password only) for authenticating the sessions. The transfer of files is driven from the external server.

3.7 Installing an SSL Certificate For a Provisionable Interface With Customized Parameters

Perform the following steps to install a certificate with customized parameters:

1. Log in to ELAP as admusr.
2. Sign the certificate files on the ELAP A server:

```
sudo /usr/bin/openssl req –x509 -sha<SHA Hash>-nodes -days <No of days to
certify the certificate for, after which the certificate shall expire> –
subj "/CN=<ELAP A GUI IPv4 IP address >" -newkey rsa:<RSA Key Management> -
```


Copyright © 2000, 2026, Oracle and/or its affiliates.

```
keyout /usr/TKLC/plat/etc/ssl/server.key -out /usr/TKLC/plat/etc/ssl/
server.crt
```

3. Sign the certificate files on the ELAP B server in the same way.
4. Restart the httpd service on both the ELAP A and B servers by using the following commands:

```
[admusr@mps-A ~]$ sudo service httpd restart
[admusr@mps-B ~]$ sudo service httpd restart
```

5. Open the ELAP A and B GUIs using https and install the SSL certificates. Use the following commands to open the ELAP A and ELAP B GUI using the IP:

```
https://<ELAP A GUI IP>
https://<ELAP B GUI IP>
```

6. Verify that the certificates installed successfully and the ELAP A and B GUIs opened successfully.
7. If the ELAP GUI does not open, on the ELAP A and B servers, follow these steps to reconfigure the network on ELAP through the elapconfig menu. This will re-install the SSL certificates with the default parameters.

```
[admusr@mps-A ~]$sudo su – elapconfig


 /-------ELAP Configuration Menu--------\
/----------------------------------------\
|  1 | Display Configuration             |
|----|-----------------------------------|
|  2 | Configure Network Interfaces Menu |
|----|-----------------------------------|
|  3 | Set Time Zone                     |
|----|-----------------------------------|
|  4 | Exchange Secure Shell Keys        |
|----|-----------------------------------|
|  5 | Change Password                   |
|----|-----------------------------------|
|  6 | Platform Menu                     |
|----|-----------------------------------|
|  7 | Configure NTP Server              |
|----|-----------------------------------|
|  8 | Mate Disaster Recovery
|----|-----------------------------------|
|  e | Exit                              |
\----------------------------------------/
Enter Choice: 2
```

   a. Enter choice **2** to access the Configure Network Interfaces Menu:
   b. Enter choice 1 to Configure Provisioning Network:

```
 /----Configure Network Interfaces Menu--\
/----------------------------------------\
|  1 | Configure Provisioning Network    |
```


Copyright © 2000, 2026, Oracle and/or its affiliates.

```
|----|----------------------------------|
|  2 | Configure DSM Network            |
|----|----------------------------------|
|  3 | Configure Forwarded Ports        |
|----|----------------------------------|
|  4 | Configure Status NAT Addresses   |
|----|----------------------------------|
|  e | Exit                             |
\-------------------------------------/
Enter Choice: 1
ELAP software is running. Stop it? [N]: Y
ELAP A provisioning network IP Address [10.75.141.47]:
ELAP B provisioning network IP Address [10.75.141.48]:
ELAP provisioning network netmask [255.255.255.128]:
ELAP provisioning network default router [10.75.141.1]:
ELAP local provisioning Virtual IP Address [10.75.141.49]:
```

c. Select **Enter** to reconfigure the network with the same configuration.

d. Contact My Oracle Support to re-run the procedure.

8. Copy key and cert files for the `tpdProvd` process running on Port `20000`.

```
cp /usr/TKLC/plat/etc/ssl/server.key /usr/TKLC/plat/etc/ssl/server.pem
cp /usr/TKLC/plat/etc/ssl/server.crt /usr/TKLC/plat/etc/ssl/server.cert
```

9. Restart the `tpdProvd` process by killing the existing process and letting it restart.

```
ps -eaf | grep tpdProvd
Output:
tpdProvd 13468     1  0 03:42 ?        00:00:04 /usr/TKLC/plat/bin/tpdProvd
kill -9 <pid>
Example: kill -9 13468
Run ps again to check process is restarted
ps -eaf | grep tpdProvd
Output:
tpdProvd  9090     1  3 04:09 ?        00:00:00 /usr/TKLC/plat/bin/tpdProvd
```

10. Repeat Steps 8 and 9 on LSMS B, as well.

3.8 Installing an SSL Certificate For a Provisionable Interface From a Trusted Certificate Authority

Perform the following steps to install an SSL certificate from a trusted Certificate Authority (CA):

1. Log in as the admusr user on both the ELAP A and B servers, create a new `certificate` directory (`/var/TKLC/ELAP/free/certificate`), provide permissions to the new directory, and change to the new directory:

```
[admusr@mps-A ~]$ pwd
/home/admusr
[admusr@mps-A ~]$ sudo mkdir /var/TKLC/elap/free/certificate
```


Copyright © 2000, 2026, Oracle and/or its affiliates.

```
[admusr@mps-A ~]$ sudo chmod 777 /var/TKLC/elap/free/certificate
[admusr@mps-A ~]$ cd /var/TKLC/elap/free/certificate
```

2. Generate a certificate signing request (CSR) and private key files for the ELAP A server using the following commands from the certificate directory:

```
sudo /usr/bin/openssl req -x509 -sha<SHA Hash>-nodes -days <No of days to
certify the certificate for, after which the
certificate shall expire>-newkey rsa:2048 -nodes –keyout server.key
–out server.csr -subj "/C=US/ST=New York/L=Brooklyn/O=Example Brooklyn
Company/OU=Example Org Unit/CN=<ELAP GUI IPv4 IP address, e.g,
1.1.1.1>/emailAddress=xxx@yyy.com"
```

   The commands should generate the following files on the ELAP A server:

```
[admusr@mps-A certificate]$ ls –lrt
-rw-r----- 1 root root 1679 Jul 13 11:08 server.key
-rw-r----- 1 root root 968 Jul 13 11:08 server.csr
```

3. Generate certificate signing request (CSR) and private key files for the ELAP B server in the same way (steps 2 - 3), using the file serverB.csr for ELAP B.
   The following files will be generated on the ELAP B server:

```
[admusr@mps-B certificate]$ ls –lrt
-rw-r----- 1 root root 1679 Jul 13 11:02 server.key
-rw-r----- 1 root root 968 Jul 13 11:02 serverB.csr
```

4. Send the generated CSR files (server.csr and serverB.csr) to the CA. The CA will provide signed certificate (server.crt and serverB.crt) files in return.
5. Copy the appropriate files to the appropriate `ssl` directory, and rename (in the B server only) as needed:
   a. On the ELAP A server, copy the two files generated through the openssl commands (server.key and server.csr) and the file provided by the CA for the ELAP A server (server.crt) to the `/usr/TKLC/plat/etc/ssl` directory.
   b. On the ELAP B server, copy the two files generated through the openssl commands (server.key and serverB.csr) and the file provided by the CA for the ELAP B server (serverB.crt) to the `/usr/TKLC/plat/etc/ssl` directory.
   c. After copying serverB.crt to the `/usr/TKLC/plat/etc/ssl` directory on the ELAP B server, rename it to server.crt.
6. Restart the httpd service on both the ELAP A and B servers by using the following commands:

```
[admusr@mps-A certificate]$ sudo service httpd restart
[admusr@mps-B certificate]$ sudo service httpd restart
```

7. Open the ELAP A and B GUIs using https and install the SSL certificate. Use the following commands to open the ELAP A and B GUIs:

```
https://<ELAP A GUI IP>
https://<ELAP B GUI IP>
```


Copyright © 2000, 2026, Oracle and/or its affiliates.

8. Verify that the ELAP A and B GUIs opened successfully with the installed certificate.
9. If the ELAP GUI does not open, follow these steps on the ELAP A and B servers:
   a. Open the `/etc/httpd/conf.d/ssl.conf` file:

      ```
      [admusr@mps-A certificate]$ sudo vi /etc/httpd/conf.d/ssl.conf
      ```

   b. Edit `/etc/httpd/conf.d/ssl.conf` and un-comment the appropriate code:
      - If the CA provides ca.crt (CA intermediate certificate), change from:

        ```
        #SSLCertificateChainFile /etc/httpd/conf/ssllcrt/ca.crt
        ```

        to:

        ```
        SSLCertificateChainFile /etc/httpd/conf/ssllcrt/ca.crt
        ```

      - If the CA provides CA certificate(s), change from:

        ```
        #SSLCACertificatePath /etc/httpd/conf/ca-cert
        #SSLCACertificateFile /usr/share/ssl/certs/ca-bundle.crt
        ```

        to:

        ```
        SSLCACertificatePath /etc/httpd/conf/ca-cert
        SSLCACertificateFile /usr/share/ssl/certs/ca-bundle.crt
        ```

   c. Make sure that these files (CA certs) are copied to the right path on both servers, as mentioned in `/etc/httpd/conf.d/ssl.conf`.
   d. Restart the httpd service using the following command on both servers:

      ```
      [admusr@mps-A certificate]$ sudo service httpd restart
      [admusr@mps-B certificate]$ sudo service httpd restart
      ```

   e. Verify that the ELAP A and B GUIs open successfully.
10. Copy key and cert files for the `tpdProvd` process running on Port `20000`.

    ```
    cp /usr/TKLC/plat/etc/ssl/server.key /usr/TKLC/plat/etc/ssl/server.pem
    cp /usr/TKLC/plat/etc/ssl/server.crt /usr/TKLC/plat/etc/ssl/server.cert
    ```

11. Restart the `tpdProvd` process by killing the existing process and letting it restart.

    ```
    ps -eaf | grep tpdProvd
    Output:
    tpdProvd 13468     1  0 03:42 ?        00:00:04 /usr/TKLC/plat/bin/tpdProvd
    kill -9 <pid>
    Example: kill -9 13468
    Run ps again to check process is restarted
    ps -eaf | grep tpdProvd
    Output:
    tpdProvd  9090     1  3 04:09 ?        00:00:00 /usr/TKLC/plat/bin/tpdProvd
    ```

12. Repeat Steps 10 and 11 on LSMS B, as well.

Copyright © 2000, 2026, Oracle and/or its affiliates.

3.9 Installing an SSL Certificate For a VIP With Customized Parameters

Perform the following steps to install an SSL certificate for a Virtual IP (VIP) with customized parameters:

1. Log in to ELAP A as admusr.
2. Change the directory to `/usr/TKLC/plat/etc/ssl/`.
3. Execute the following command to list the files in the directory `/usr/TKLC/plat/etc/ssl/`.
   Sample output for the previous command:

   ```
   [root@Natal-a ssl]# ls -ltrh server_vip*
   -rw-r----- 1 root elap 1.7K Jul 15 04:27 server_vip.key
   -rw-r----- 1 root elap 1.1K Jul 15 04:27 server_vip.crt
   ```

   The certificate file server_vip.crt is present in the directory `/usr/TKLC/plat/etc/ssl/`. Continue with the next step to sign the certificate after exiting from the root user.
4. Sign the certificate on the ELAP A server according to the information determined in Step 1 using the following command:

   ```
   sudo /usr/bin/openssl req –x509 -sha<SHA Hash>-nodes -days <No of days to
   certify the certificate for, after which the certificate shall expire> –
   subj "/CN=<ELAP A VIP IPv4 address >" -newkey rsa:<RSA Key Management> -
   keyout /usr/TKLC/plat/etc/ssl/server_vip.key -out /usr/TKLC/plat/etc/ssl/
   server_vip.crt
   ```

5. Sign the certificate files on the ELAP B server in the same way.
6. Restart the httpd service on both the ELAP A and B servers by using the following commands:

   ```
   [admusr@mps-A ~]$ sudo service httpd restart
   [admusr@mps-B ~]$ sudo service httpd restart
   ```

7. Open the GUI using VIP IPv4 IP using https and install the SSL certificate using the following command:

   ```
   https://<ELAP A VIP IP>
   ```

8. Verify that the certificate installed successfully and the GUI opened successfully.
9. If the ELAP GUI does not open on the ELAP A server, follow these steps to reconfigure the VIP IP addresses on ELAP through the elapconfig menu. This will re-install the SSL certificates with the default parameters:

   ```
   [admusr@mps-A ~]$ sudo su – elapconfig
   ```


Copyright © 2000, 2026, Oracle and/or its affiliates.

a. Enter choice **2** to access the Configure Network Interfaces Menu:

```
 /-------ELAP Configuration Menu--------\
/----------------------------------------\
|  1 | Display Configuration             |
|----|-----------------------------------|
|  2 | Configure Network Interfaces Menu |
|----|-----------------------------------|
|  3 | Set Time Zone                     |
|----|-----------------------------------|
|  4 | Exchange Secure Shell Keys        |
|----|-----------------------------------|
|  5 | Change Password                   |
|----|-----------------------------------|
|  6 | Platform Menu                     |
|----|-----------------------------------|
|  7 | Configure NTP Server              |
|----|-----------------------------------|
|  8 | Mate Disaster Recovery
|----|-----------------------------------|
|  e | Exit                              |
\----------------------------------------/
Enter Choice: 2
```

b. Enter choice **1** to Configure Provisioning Network:

```
 /----Configure Network Interfaces Menu--\
/----------------------------------------\
|  1 | Configure Provisioning Network    |
|----|-----------------------------------|
|  2 | Configure DSM Network             |
|----|-----------------------------------|
|  3 | Configure Forwarded Ports         |
|----|-----------------------------------|
|  4 | Configure Status NAT Addresses    |
|----|-----------------------------------|
|  e | Exit                              |
\----------------------------------------/
Enter Choice: 1
ELAP software is running. Stop it? [N]: Y
ELAP A provisioning network IP Address [10.75.141.47]:
ELAP B provisioning network IP Address [10.75.141.48]:
ELAP provisioning network netmask [255.255.255.128]:
ELAP provisioning network default router [10.75.141.1]:
ELAP local provisioning Virtual IP Address [10.75.141.49]:
```

c. Press **Enter** to reconfigure the network with the same configuration.

d. Contact to re-run the procedure.

Copyright © 2000, 2026, Oracle and/or its affiliates.

3.10 Installing an SSL Certificate For a VIP From a Trusted Certificate Authority

Perform the following steps to install an SSL certificate for a Virtual IP (VIP) from a trusted Certificate Authority (CA):

1. Log in as the admusr user on both the ELAP A and B servers, create a new `certificate` directory (`/var/TKLC/elap/free/`), provide permissions to the new directory, and change to the new directory:

   ```
   [admusr@mps-A ~]$ pwd
   /home/admusr
   [admusr@mps-A ~]$ sudo mkdir /var/TKLC/elap/free/certificate
   [admusr@mps-A ~]$ sudo chmod 777 /var/TKLC/elap/free/certificate
   [admusr@mps-A ~]$ cd /var/TKLC/elap/free/certificate
   ```

2. When the ELAP is configured in IPv4 configuration, log in to ELAP A as admusr.
3. Switch to the root user as "su -".
4. Change the directory to `/usr/TKLC/plat/etc/ssl/`.
5. Execute the following command to list the files in the directory `/usr/TKLC/plat/etc/ssl/`.
   Sample output for the previous command:

   ```
   [root@Natal-a ssl]# ls -ltrh server_vip*
   -rw-r----- 1 root elap 1.7K Jul 15 04:27 server_vip.key
   -rw-r----- 1 root elap 1.1K Jul 15 04:27 server_vip.crt
   ```

   The certificate file server_vip_v4.crt is present in the directory `/usr/TKLC/plat/etc/ssl/`. Continue with the next step to sign the certificate after exiting from the root user.
6. Generate certificate signing request (CSR) and private key files for ELAP A server using the following commands from within the certificate directory.
   The certificate file server_vip_v4.crt is generated since the VIP is configured in IPv4 configuration. Enter the following commands on ELAP A server:

   ```
   sudo /usr/bin/openssl req -x509 -sha<SHA Hash>-nodes -days <No of days to
   certify the certificate for, after which the certificate shall expire>-
   newkey rsa:2048 -nodes –keyout server_vip.key –out server_vip.csr -subj "/
   C=US/ST=New York/L=Brooklyn/O=Example Brooklyn Company/OU=Example Org Unit/
   CN=<ELAP VIP IPv4 address>/emailAddress=xxx@yyy.com"
   ```

> **Note**
>
> The -subj option in the following commands has example fields, which must be replaced with your organization-specific domain information. The /C field is for your country, /ST is for state, /L is for location, /O is for organization, /OU is for organizational unit, and /CN is the common name field, which is the IP address or fully-qualified domain name that you want to use with your certificate.

Copyright © 2000, 2026, Oracle and/or its affiliates.

These commands generate the following files on the ELAP A server:

```
[admusr@mps-A certificate]$ ls –lrt
-rw-r----- 1 root root 1679 Jul 15 11:08 server_vip.key
-rw-r----- 1 root root 968 Jul 15 11:08  server_vip.csr
```

7. Generate certificate signing request (CSR) and private key files for ELAP B server by executing steps 1 to 7. Sign the certificate files on the ELAP B server in the same way. Use the files serverB_vip.csr for ELAP B.
   These commands generate the following files on the ELAP B server:

   ```
   [admusr@mps-B certificate]$ ls –lrt
   -rw-r--r-- 1 root root 1679 May 21 11:02 server_vip_v4.key
   -rw-r--r-- 1 root root 968 May 21 11:02  serverB_vip_v4.csr
   ```

8. Send the generated CSR file (server_vip.csr) to the CA. The CA will provide signed certificate file (server_vip.crt) in return.
9. Copy the appropriate files to the appropriate ssl directory, and rename as needed:
   - On the ELAP A server, copy the two files generated through the openssl commands (server_vip.key, server_vip.csr) and the file provided by the CA (server_vip_v4.crt) to the `/usr/TKLC/plat/etc/ssl` directory.
   - On the ELAP B server, copy the two files generated through the openssl command (server_vip.key, serverB_vip.csr) and the file provided by the CA for the ELAP B server (serverB_vip_v4.crt) to the `/usr/TKLC/plat/etc/ssl` directory.
10. After copying serverB_vip.crt to the `/usr/TKLC/plat/etc/ssl` directory on the ELAP B server, rename it to server _vip.crt.
11. Restart the httpd service on both the ELAP A and B servers by using the following commands:

    ```
    [admusr@mps-A certificate]$ sudo service httpd restart
    [admusr@mps-B certificate]$ sudo service httpd restart
    ```

12. Open the GUI using VIP IPv4 IP using https and install the SSL certificate using the following command:

    ```
    https://<ELAPVIP IP>
    ```

13. Verify that the certificate installed successfully and the GUI opened successfully.
14. If the ELAP GUI does not open, follow these steps on the ELAP A and B servers:
    a. Open the `/etc/httpd/conf.d/ssl.conf` file:

       ```
       [admusr@mps-A certificate]$ sudo vi /etc/httpd/conf.d/ssl.conf
       ```

    b. Edit `/etc/httpd/conf.d/ssl.conf` and un-comment the appropriate code:
       - If the CA provides ca.crt (CA intermediate certificate), change from:

         ```
         #SSLCertificateChainFile /etc/httpd/conf/ssllcrt/ca.crt
         ```


Copyright © 2000, 2026, Oracle and/or its affiliates.

to:

```
SSLCertificateChainFile /etc/httpd/conf/ssllcrt/ca.crt
```

- If the CA provides CA certificate(s), change from:

```
#SSLCACertificatePath /etc/httpd/conf/ca-cert
#SSLCACertificateFile /usr/share/ssl/certs/ca-bundle.crt
```

to:

```
SSLCACertificatePath /etc/httpd/conf/ca-cert
SSLCACertificateFile /usr/share/ssl/certs/ca-bundle.crt
```

c. Make sure that these files (CA certs) are copied to the right path on both servers, as mentioned in `/etc/httpd/conf.d/ssl.conf`.

d. Restart the httpd service using the following command on both servers:

```
[admusr@mps-A certificate]$ sudo service httpd restart
[admusr@mps-B certificate]$ sudo service httpd restart
```

e. Verify that the ELAP A and B GUIs open successfully.

Copyright © 2000, 2026, Oracle and/or its affiliates.

A

Configuring IPSec for Secure Packet Transmission between All Hosts

Perform the following steps to enable IPSec service between nodes, for example, between LSMS and ELAP nodes, and so on.

1. Switch to the root user as "su -".
2. Enable the service to be started and run the command:

   ```
   systemctl enable ipsec
   [admusr@mps-A~]$ systemctl enable ipsec
   [admusr@mps-A~]$ Created symlink /etc/systemd/system/multi-
   user.target.wants/ipsec.service ->
   /usr/lib/systemd/system/ipsec.service
   ```

3. Configure the firewall (if enabled) to allow 500 and 4500/UDP ports for the IKE, ESP, and AH protocols by adding the IPsec service:

   ```
   firewall-cmd --add-service="ipsec"
   firewall-cmd --runtime-to-permanent
   ```

4. Initialize the new NSS database and run the following command as root:

   ```
   ipsec initnss
   ```

   For example:

   ```
   [admusr@mps-A~]$ ipsec initnss
   ```

   ```
   [admusr@mps-A ~]$ Initializing NSS database
   ```

5. Create Host-to-Host VPN Link. Change the directory to `/etc/ipsec.d/`.
6. Create a new file with the name `my_host-to-host.conf`.
7. Edit the file and enter all the details shown below:
   It is mandatory to maintain the gap of one tab between conn mytunnel and auto=start. Similarly, the user needs to make more than one tunnel using “-also” keyword. For example, "conn mytunnel-also".

   ```
   conn mytunnel
       auto=start
       keyexchange=ike
       phase2=esp
       pfs=no
       type=tunnel
       authby=secret
       leftid=(ip address of self linux machine)
       left=(ip address of self linux machine)
   ```


Copyright © 2000, 2026, Oracle and/or its affiliates.

```
    right=(ip address of remote linux machine)
    rightid=(ip address of remote linux machine)
```

If more than one IPSec connection is required, for example, from LSMS to multiple ELAPs, then write as mentioned below:

```
conn mytunnel
    auto=start
    keyexchange=ike
    phase2=esp
    pfs=no
    type=tunnel
    authby=secret
    leftid=(ip address of self linux machine)
    left=(ip address of self linux machine)
    right=(ip address of remote linux machine)
    rightid=(ip address of remote linux machine)


conn mytunnel-also
    auto=start
    keyexchange=ike
    phase2=esp
    pfs=no
    type=tunnel
    authby=secret
    leftid=(ip address of self linux machine)
    left=(ip address of self linux machine)
    right=(ip address of remote linux machine)
    rightid=(ip address of remote linux machine)
```

8. Create a new file with the name ipsec.secrets. Edit the file and enter the following details. Here, pre-shared-key could be any passphrase:

   ```
   siteA-public-IP siteB-public-IP: PSK "pre-shared-key"
   ```

   In case of multiple sites:

   ```
   siteA-public-IP siteB-public-IP: PSK "pre-shared-key"
   siteA-public-IP siteC-public-IP: PSK "corresponding-pre-shared-key"
   ```

9. Edit file /etc/ipsec.conf. Go to line no. 17 and comment the flag oe=off like and save the file:

   ```
   #oe=off
   ```

10. Start the IPsec services and run the command:

    ```
    systemctl start ipsec
    ```

11. If the conf file is modified, restart the IPsec services and run the command:

    ```
    systemctl restart ipsec
    ```


Copyright © 2000, 2026, Oracle and/or its affiliates.

12. To verify the tunnel creations and traffic flow, run the following command:

    ```
    ipsec traffic
    ```

    For example:

    ```
    [admusr@mps-A~]# ipsec traffic 006 #4: "mytunnel", type=ESP,
    add_time=1666264187, inBytes=600, outBytes=544,id='x.x.x.x' 006 #6: "mytunnel-
    also", type=ESP, add_time=1666264189, inBytes=2820, outBytes=2024,id='x.x.x.x'
    ```

13. Follow the same steps at the peer end.

14. Below is the sample site scenario where 1 LSMS and 2 ELAP hosts are connected:
    LSMS Site IP: 10.71.141.10

    ELAP Site A: 10.71.141.20

    ELAP Site B: 10.71.141.21

    Sample Files for LSMS Site (10.71.141.10)

    File - /etc/ipsec.d/my_host-to-host.conf

    ```
    conn mytunnel
        auto=start
        keyexchange=ike
        phase2=esp
        pfs=no
        type=tunnel
        authby=secret
        leftid=10.75.141.10
        left=10.75.141.10
        right=10.75.141.20
        rightid=10.75.141.20

    conn mytunnel-also
        auto=start
        keyexchange=ike
        phase2=esp
        pfs=no
        type=tunnel
        authby=secret
        leftid=10.75.141.10
        left=10.75.141.10
        right=10.75.141.21
        rightid=10.75.141.21
    ```

    File - /etc/ipsec.d/ipsec.secrets

    ```
    10.75.141.10 10.75.141.20 : PSK "Abc1234"
    10.75.141.10 10.75.141.21 : PSK "Abc1234"
    ```

    Sample Files for ELAP Site A (10.71.141.20)

    File - /etc/ipsec.d/my_host-to-host.conf

    ```
    conn mytunnel
        auto=start
    ```


Copyright © 2000, 2026, Oracle and/or its affiliates.

```
    keyexchange=ike
    phase2=esp
    pfs=no
    type=tunnel
    authby=secret
    leftid=10.75.141.20
    left=10.75.141.20
    right=10.75.141.10
    rightid=10.75.141.10
```

File - /etc/ipsec.d/ipsec.secrets

```
10.75.141.20 10.75.141.10 : PSK "Abc1234"
```

Sample Files for ELAP Site B (10.71.141.21)

File - /etc/ipsec.d/my_host-to-host.conf

```
conn mytunnel
    auto=start
    keyexchange=ike
    phase2=esp
    pfs=no
    type=tunnel
    authby=secret
    leftid=10.71.141.21
    left=10.71.141.21
    right=10.75.141.10
    rightid=10.75.141.10
```

File - /etc/ipsec.d/ipsec.secrets

```
10.71.141.21 10.75.141.10 : PSK "Abc1234"
```


Copyright © 2000, 2026, Oracle and/or its affiliates.

B

Secure Deployment Checklist

Use the following security checklist to help secure ELAP and its components:

- Change default passwords
- Configure ELAP firewall port assignments
- Enable HTTPS and disable HTTP
- Enforce strong password management
- Restrict admin functions to the required administrator groups
- Utilize the Authorized IP addresses feature

B.1 ELAP Firewall Port Assignments

If a firewall is installed in the provisioning network between the MPS systems or between the MPS system(s) and the provisioning system, it must be configured to allow selected traffic to pass. Firewall protocol filtering for the various interfaces is defined in this table (from the perspective of each MPS).

> **Note**
>
> The information in the following table is used for both internal customer network configuration and VPN access for support.

Table B-1 Firewall Requirements

Server Interface	IP Address	TCP/IP Port	Inbound	Outbound	Use/Comments
ELAP Application Firewall Requirements:					
Port 1	Provisioning IP or VIP configured on ELAP	22	Yes	Yes	SSH/SCP/SFTP
Port 1	NTP server IP(s) configured on ELAP	123	Yes	Yes	NTP - Needed for time-sync.
Port 1	Provisioning IP or VIP configured on ELAP	80	Yes	No	APACHE - Needed for ELAP Web-based GUI.
Port 1	Provisioning IP or VIP configured on ELAP	8473	Yes	Yes	GUI server (process) - Needed by ELAP Web-based GUI.

Copyright © 2000, 2026, Oracle and/or its affiliates.

Table B-1 (Cont.) Firewall Requirements

Server Interface	IP Address	TCP/IP Port	Inbound	Outbound	Use/Comments
ELAP Application Firewall Requirements:					
Port 1	Provisioning IP or VIP configured on ELAP	9691	Yes	Yes	Used for HSOPD watcher.
Port 1	Provisioning IP or VIP configured on ELAP	1030	Yes	Yes	Used for bulkdownload between LSMS and ELAP.
Port 1	Provisioning IP or VIP configured on ELAP	7483	Yes	No	Used for download the normal provisioning data from LSMS to ELAP.

Copyright © 2000, 2026, Oracle and/or its affiliates.

C

Secure Turnover to Customer

To ensure security of systems delivered to our customers and to satisfy Oracle policies, all passwords must be owned by the customer once transfer of ownership of systems has occurred.

C.1 Secure Turnover Process

Three key requirements address the fundamental principles of the secure turnover process:

- Oracle default passwords shall not remain on fielded systems.
- Oracle default passwords shall not be revealed to customers.
- Customer installed passwords shall not be known by Oracle.

Goals of the Secure Turnover Process

Following are the goals of the password handoff process:

1. Install the system securely with Oracle internal default passwords (passwords exclusively known and used by Oracle personnel).
2. Change the special account passwords during the installation process to a unique value (meeting password complexity rules required by the system).
3. Provide a non-repudiation process for the customer agent to set all special passwords.

Secure Turnover Procedure

Perform the following steps for secure system turnover:

1. System servers are installed by Oracle personnel using common ISO deliverables and installation procedures. The OS root password, OS admusr password, and the passwords for the default ELAP UI login accounts are from the build process, and are private and known only by Oracle.
2. Following installation, the Oracle installer performs a login to each server OS (real and virtual) as admusr and changes the password to a new unique secure password. The Oracle installer then switches user to root and changes the root password to a new unique password.
3. The Oracle installer uses a web browser to log in to the application on each relevant server using each default ELAP UI login name (such as uiadmin) and changes the password to a new unique password. For a list of the pre-defined ELAP UI login names, see Table 3-1.
4. As a precursor to the official handoff of the system (all servers) to the customer, the Oracle installer ensures that the new unique passwords for root, admusr, and default ELAP UI login accounts have been securely given to the authorized customer agent.
5. The authorized customer agent is instructed to log in to each OS account on each server (real and virtual) and change the password for accounts admusr and root to the authorized operational setting for the customer.

Copyright © 2000, 2026, Oracle and/or its affiliates.

6. The customer agent is instructed to use a web browser to log in to each relevant application server and change the password for the default ELAP UI login accounts to the authorized operational password for the customer.
7. Following the entry of the new passwords by the customer agent, the Oracle installer or authorized Oracle agent attempts to log in to each server using the previously known password. This should result in a failed login attempt verifiable in the server logs.
8. The customer agent again logs in to each OS account and the default ELAP UI login accounts using the new customer passwords to verify success with the new customer passwords.

Copyright © 2000, 2026, Oracle and/or its affiliates.