

**Oracle® Communications  
EAGLE Application Processor**

Security Guide

Release 16.2

**E87672 Revision 1**

August 2017

Oracle Communications EAGLE Application Processor Security Guide, Release 16.2

Copyright © 2000, 2017, Oracle and/or its affiliates. All rights reserved.

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 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 installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. 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 and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon 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, Opteron, the AMD logo, and the AMD Opteron 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.

# Table of Contents

<b>Chapter 1: Introduction.....</b>	<b>7</b>
Overview.....	8
Scope and Audience.....	8
Documentation Admonishments.....	8
My Oracle Support (MOS).....	9
Emergency Response.....	9
Related Publications.....	10
Customer Training.....	10
Locate Product Documentation on the Oracle Help Center Site.....	10
<b>Chapter 2: EPAP Security Overview.....</b>	<b>11</b>
Basic Security Considerations.....	12
Understanding the EPAP Environment.....	12
Recommended Deployment Configurations.....	12
EPAP SSL Certificate Security.....	14
Root User Is Disabled for SSH Login.....	14
<b>Chapter 3: Implementing EPAP Security.....</b>	<b>15</b>
User and Group Administration.....	16
User Authentication.....	17
Modifying System Defaults.....	18
SNMP Configuration.....	18
Authorized IP Addresses.....	18
Installing an SSL Certificate For a Provisionable Interface With Customized Parameters.....	19
Installing an SSL Certificate For a Provisionable Interface From a Trusted Certificate Authority.....	22
Installing an SSL Certificate For a Backup Provisionable Interface With Customized Parameters.....	26
Installing an SSL Certificate For a Backup Provisionable Interface From a Trusted Certificate Authority.....	29
Installing an SSL Certificate For a VIP With Customized Parameters.....	32
Installing an SSL Certificate For a VIP From a Trusted Certificate Authority.....	34

<b>Appendix A: Secure Deployment Checklist.....</b>	<b>38</b>
<b>Appendix B: Secure Turnover to Customer.....</b>	<b>39</b>
Secure Turnover Process.....	40
<b>Glossary.....</b>	<b>41</b>

# List of Figures

Figure 1: Generic EPAP Deployment Model.....	13
----------------------------------------------	----

# List of Tables

Table 1: Admonishments.....	8
Table 2: EPAP UI Logins.....	16

# Chapter 1

## Introduction

---

### Topics:

- *Overview.....8*
- *Scope and Audience.....8*
- *Documentation Admonishments.....8*
- *My Oracle Support (MOS).....9*
- *Emergency Response.....9*
- *Related Publications.....10*
- *Customer Training.....10*
- *Locate Product Documentation on the Oracle Help Center Site.....10*

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

## Overview

This document provides guidelines and recommendations for configuring the Oracle Communications EAGLE Application Processor (EPAP) 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.





## Scope and Audience

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

## 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: Admonishments**

Icon	Description
 DANGER	Danger: (This icon and text indicate the possibility of <i>personal injury</i> .)
 WARNING	Warning: (This icon and text indicate the possibility of <i>equipment damage</i> .)
 CAUTION	Caution: (This icon and text indicate the possibility of <i>service interruption</i> .)
 TOPPLE	Topple: (This icon and text indicate the possibility of <i>personal injury and equipment damage</i> .)



## My Oracle Support (MOS)

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

Call the CAS 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:

1. Select **2** for New Service Request
2. Select **3** for Hardware, Networking and Solaris Operating System Support
3. Select one of the following options:
  - For Technical issues such as creating a new Service Request (SR), Select **1**
  - For Non-technical issues such as registration or assistance with MOS, Select **2**

You will be connected to a live agent who can assist you with MOS registration and opening a support ticket.

MOS is available 24 hours a day, 7 days a week, 365 days a year.

## Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at 1-800-223-1711 (toll-free in the US), or by calling the Oracle Support hotline for your local country from the list at <http://www.oracle.com/us/support/contact/index.html>. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

## 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.

## Customer Training

Oracle University offers training for service providers and enterprises. Visit our web site to view, and register for, Oracle Communications training:

<http://education.oracle.com/communication>

To obtain contact phone numbers for countries or regions, visit the Oracle University Education web site:

[www.oracle.com/education/contacts](http://www.oracle.com/education/contacts)

## 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.

# Chapter 2

## EPAP Security Overview

---

### Topics:

- *Basic Security Considerations.....12*
- *Understanding the EPAP Environment.....12*
- *Recommended Deployment Configurations.....12*
- *EPAP SSL Certificate Security.....14*
- *Root User Is Disabled for SSH Login.....14*

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

## 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 EPAP 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 EPAP security features.** See *Implementing EPAP 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>

## Understanding the EPAP Environment

The EPAP platform, coupled with the Provisioning Database Application (PDBA), facilitates and maintains the database required by EPAP-related features. See the *Glossary* for a list of EPAP-related features. The EPAP serves two major purposes:

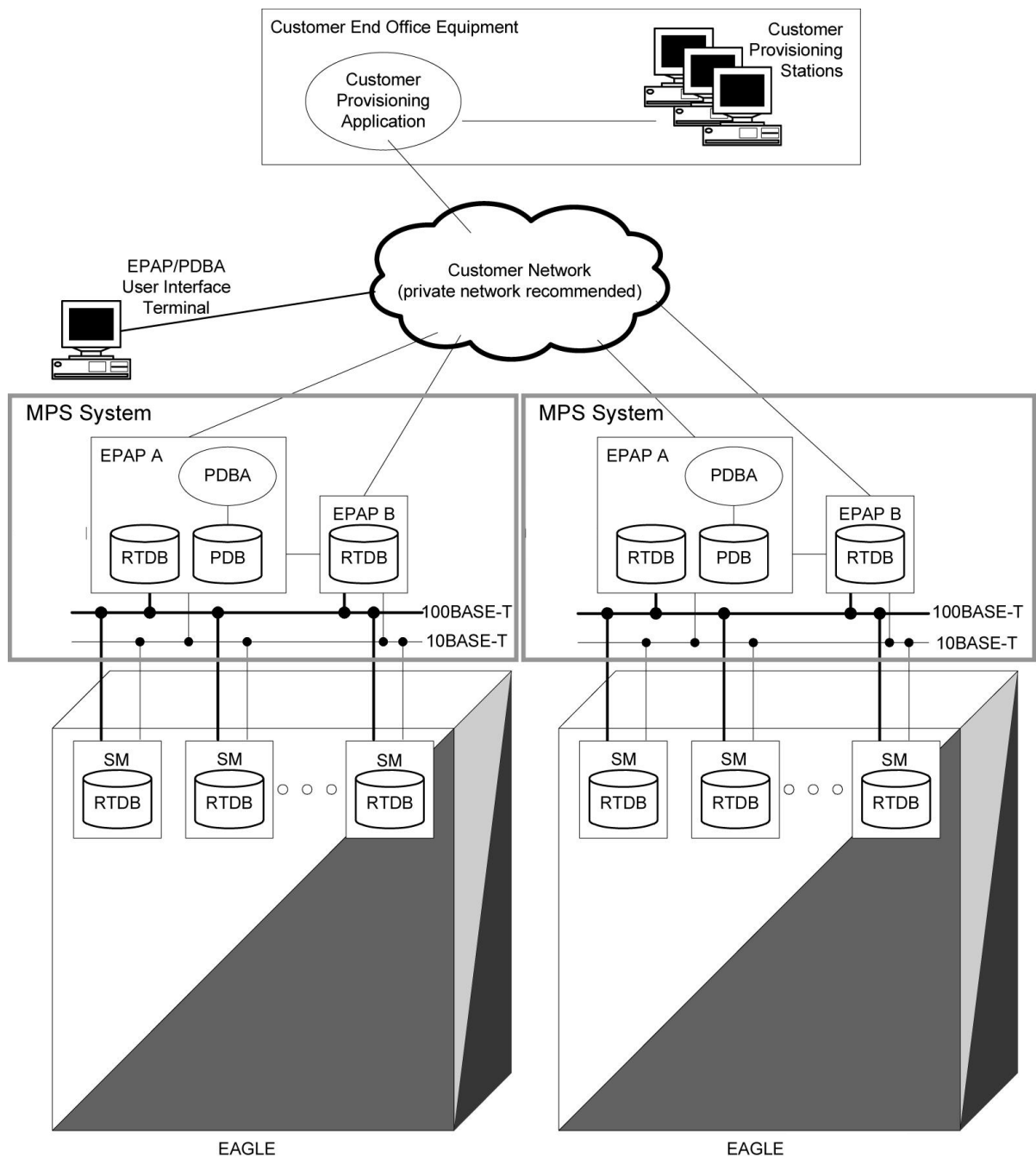
- Accept and store data provisioned by the customer
- Update customer provisioning data and reload databases on the Service Module cards in the Multi Purpose Server (MPS)

The MPS hardware platform supports high speed provisioning of large databases for the EAGLE. The MPS is composed of hardware and software components that interact to create a secure and reliable platform. MPS supports the EPAP.

During normal operation, information flows through the EPAP and PDBA with no intervention. Each EPAP has a graphical user interface that supports maintenance, debugging, and platform operations. The EPAP user interface includes a PDBA user interface for configuration and database maintenance.

## Recommended Deployment Configurations

The EPAP is deployed in the central office of the carrier and service provider, co-located with the EAGLE STP. The customer network should be secured via firewall, and making the EPAP provisioning network its own private network or VLAN is further recommended where possible. For a generic model of the deployment strategy, see *Figure 1: Generic EPAP Deployment Model*.



**Figure 1: Generic EPAP Deployment Model**

In addition to the firewalls, the EPAP system provides additional security capabilities that include application-specific remote IP address control.

## EPAP SSL Certificate Security

Currently, EPAP uses self-signed SSL certificates. You can install an X.509 certificate for a provisionable or backup provisionable interface with customized parameters, install an SSL certificate for a provisionable or backup provisionable interface from a trusted Certificate Authority (CA), install an SSL certificate for a Virtual IP (VIP) with customized parameters, and install an SSL certificate for a Virtual IP (VIP) from a trusted Certificate Authority (CA). For more information, see the following procedures:

- [\*Installing an SSL Certificate For a Provisionable Interface With Customized Parameters\*](#)
- [\*Installing an SSL Certificate For a Provisionable Interface From a Trusted Certificate Authority\*](#)
- [\*Installing an SSL Certificate For a Backup Provisionable Interface With Customized Parameters\*](#)
- [\*Installing an SSL Certificate For a Backup Provisionable Interface From a Trusted Certificate Authority\*](#)
- [\*Installing an SSL Certificate For a VIP With Customized Parameters\*](#)
- [\*Installing an SSL Certificate For a VIP From a Trusted Certificate Authority\*](#)

These procedures are devised to be executed on the EPAP 16.2 system deployed on TPD 7.4, on E5-APP-B-01/02 hardware.

## 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.

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.

# Chapter 3

## Implementing EPAP Security

---

### Topics:

- *User and Group Administration.....16*
- *User Authentication.....17*
- *Modifying System Defaults.....18*
- *SNMP Configuration.....18*
- *Authorized IP Addresses.....18*
- *Installing an SSL Certificate For a Provisionable Interface With Customized Parameters.....19*
- *Installing an SSL Certificate For a Provisionable Interface From a Trusted Certificate Authority.....22*
- *Installing an SSL Certificate For a Backup Provisionable Interface With Customized Parameters.....26*
- *Installing an SSL Certificate For a Backup Provisionable Interface From a Trusted Certificate Authority.....29*
- *Installing an SSL Certificate For a VIP With Customized Parameters.....32*
- *Installing an SSL Certificate For a VIP From a Trusted Certificate Authority.....34*

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

## User and Group Administration

The EPAP 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 2: EPAP UI Logins](#).

**Table 2: EPAP UI Logins**

Login Name	Access Granted
epapmaint	Maintenance menu and all submenus
epapdatabase	Database menu and all submenus
epapdebug	Debug menu and all submenus
epapplatform	Platform menu and all submenus
uiadmin	User Administration menu
epapall	All of the above menus
epapconfig	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 terminate active sessions and modify system defaults.

### 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. EPAP users can fall into one of the following default groups:

- maint
- database
- platform
- debug
- pdba
- 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 > Groups** menu allows administrator access to group functions to add, modify, delete, and retrieve a group. For more information, see *Groups* under *User Administration Menu* in *Administration 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 > Users** menu to add the user.

The **User Administration > Users** menu can also be used to modify, delete, and retrieve user accounts, and to reset passwords. For more information, see *Users* under *User Administration Menu* in *Administration Guide*.

## User Authentication

Users are authenticated using login credentials. Each user that is allowed access to the UI is assigned a unique username. This username and associated password must be provided during login.

### Password Restrictions

Before beginning to use EPAP for provisioning, the EPAP software must be configured and initialized. During configuration, default password restrictions such as password aging and minimum password size can be changed via the **EPAP Configuration > Security** menu. For more information, see *Security* under *EPAP Configuration Menu* in *Administration Guide*.

The UI addresses security concerns with various restrictions and controls. In many cases, the frequency or severity of these checks is configurable by the administrator at both a user-specific and system-wide level. For information about modifying system-wide defaults, see *Modify Defaults* under *User Administration Menu* in *Administration Guide*. For information about user-specific settings, see *Users* under *User Administration Menu* in *Administration Guide*.

For information about topics such as password complexity, password aging, and password reuse, see *Change Password* under *EPAP Graphical User Interface Menus* in *Administration Guide*.

### Changing Default Passwords

As a security measure, passwords for the EPAP UI login names, the OS root, and the OS admusr 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 of the EPAP GUI main menu provides all EPAP 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 appuser user 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 epapconfig uses the option provided in the EPAP Configuration Menu. Linux PAM rules are not applicable while changing the password for the epapconfig user. Only the configured minimum password length applies.

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

## Modifying System Defaults

The **User Administration > Modify System Defaults** screen enables the administrator to manage system defaults. Use this screen to control settings such as maximum failed login attempts before disabling a user account, maximum account inactivity, maximum password age, and minimum password length. For more information, see *Modify Defaults* under *User Administration Menu* in *Administration Guide*.

## SNMP Configuration

EPAP can use the industry-standard Simple Network Management Protocol (SNMP) interface to send alarms as trap messages to an OCEEMS. EPAP sends SNMPv2c only, SNMPv3 only, or both SNMPv2c and SNMPv3 traps to the OCEEMS if the configurable parameter SNMP Alarm Feed is set to **ON**. EPAP also supports GET and SET of the `resyncVar` MIB element.

The active EPAP server provides a single interface to SNMP data for the EPAP pair. For network configurations using the Stand-Alone PDBI feature, the PDBI provides its own SNMP interface directly with SNMP managers. The application sends SNMP traps to SNMP managers that are registered to receive traps.

### Community Names / Strings

The default community names configured for Read and Write in the `snmpd.conf` file are `epapRdSnmp` and `epapWrSnmp`. You should change the default community names to prevent unauthorized access. Always use different names for the Read community and Write community.

For more information about configuring community names, see *Configure SNMP Agent Community* in *Administration Guide*.

## Authorized IP Addresses

The **User Administration > Authorized IP** menu enables you to add, remove, and list authorized IP addresses (IPv4 and/or IPv6), and to change the IP address authorization status. The IP addresses are authorized for both GUI and server access. For more information, see *EPAP Security Enhancements*, and *Authorized IPs* under *User Administration Menu*, in *Administration Guide*.

The PDBA maintains a list of IP addresses that are allowed to connect through the PDBI. Any connect request coming from an IP address that is not in the list is rejected. Each IP address in the list has either **READ** or **READ/WRITE** permission. The **PDBA > Authorized IP List** menu enables you to add, modify, remove, and list the IP addresses authorized to connect to the PDBA through the PDB. For more information, see *Authorized IP List* under *PDBA Menu* in *Administration Guide*.

## 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 EPAP A as admusr.
2. Execute the following commands to determine the IP configuration for which the certificate files were generated.

```
[admusr@mps-A ~]$ sudo openssl verify /usr/TKLC/plat/etc/ssl/server.crt
[admusr@mps-A ~]$ sudo openssl verify /usr/TKLC/plat/etc/ssl/server_dual.crt
```

Sample output for the above commands:

```
[admusr@mps-A ~]$ sudo openssl verify /usr/TKLC/plat/etc/ssl/server.crt
/usr/TKLC/plat/etc/ssl/server.crt: CN = 10.250.51.149
error 18 at 0 depth lookup:self signed certificate
OK
```

The EPAP network configuration can be IPv4, IPv6, or dual stack (both IPv4 and IPv6), and you need to determine which certificate file corresponds to which network configuration:

- Both certificate files have the same IP address (either IPv4 or IPv6)
  - The server.crt file has the certificate for IPv4 and the server\_dual.crt file has the certificate for IPv6
  - The server.crt file has the certificate for IPv6 and the server\_dual.crt file has the certificate for IPv4
3. Sign the certificate files on the EPAP A server according to the determined network configuration information:
    - If both certificate files have been generated for the same IP address (either IPv4 or IPv6), sign both certificate files with that IP address by using the following commands:

```
[admusr@mps-A ~]$ 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=<EPAP A GUI IP address >" -newkey rsa:<RSA Key Management>
-keyout /usr/TKLC/plat/etc/ssl/server.key -out /usr/TKLC/plat/etc/ssl/server.crt
```

```
[admusr@mps-A ~]$ sudo /usr/bin/openssl req -x509 -nodes -days <No of days to
certify the certificate for, after which the certificate shall expire> -subj
"/CN=<EPAP A GUI IP address >" -newkey rsa:<RSA Key Management> -keyout
/usr/TKLC/plat/etc/ssl/server_dual.key -out /usr/TKLC/plat/etc/ssl/server_dual.crt
```

- If the server.crt file has the certificate for EPAP IPv4 and the server\_dual.crt file has the certificate for EPAP IPv6, sign the certificate files by using the following commands:

```
[admusr@mps-A ~]$ 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=<EPAP A GUI IPv4 IP address >" -newkey rsa:<RSA Key Management>
-keyout /usr/TKLC/plat/etc/ssl/server.key -out /usr/TKLC/plat/etc/ssl/server.crt
```

```
[admusr@mps-A ~]$ sudo /usr/bin/openssl req -x509 -nodes -days <No of days to
certify the certificate for, after which the certificate shall expire> -subj
```

```
"/CN=<EPAP A GUI IPv6 IP address >" -newkey rsa:<RSA Key Management> -keyout
/usr/TKLC/plat/etc/ssl/server_dual.key -out /usr/TKLC/plat/etc/ssl/server_dual.crt
```

- If the server.crt file has the certificate for EPAP IPv6 and the server\_dual.crt file has the certificate for EPAP IPv4, sign the certificate files by using the following commands:

```
[admusr@mps-A ~]$ 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=<EPAP A GUI IPv6 IP address >" -newkey rsa:<RSA Key Management>
-keyout /usr/TKLC/plat/etc/ssl/server.key -out /usr/TKLC/plat/etc/ssl/server.crt
```

```
[admusr@mps-A ~]$ sudo /usr/bin/openssl req -x509 -nodes -days <No of days to
certify the certificate for, after which the certificate shall expire> -subj
"/CN=<EPAP A GUI IPv4 IP address >" -newkey rsa:<RSA Key Management> -keyout
/usr/TKLC/plat/etc/ssl/server_dual.key -out /usr/TKLC/plat/etc/ssl/server_dual.crt
```

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

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

6. Open the EPAP A and B GUIs using https and install the SSL certificates.
  - For IPv4, use the following commands:

```
https://<EPAP A GUI IPv4 IP>
https://<EPAP B GUI IPv4 IP>
```

- For IPv6, use the following commands:

```
https://[<EPAP A GUI IPv6 IP>]
https://[<EPAP B GUI IPv6 IP>]
```

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

- a. Check the value of EPAP\_IP\_VERSION, and then access the **EPAP Configuration Menu**:

```
[admusr@mps-A ~]$ uiEdit | grep -i EPAP_IP_VERSION
"EPAP_IP_VERSION" is set to "IPv4v6"

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

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

```
/-----EPAP 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 | PDB Configuration Menu
-----
 9 | Security
-----
10 | SNMP Configuration
-----
11 | Configure Alarm Feed
-----
12 | Configure Query Server
-----
13 | Configure Query Server Alarm Feed
-----
14 | Configure SNMP Agent Community
-----
15 | Mate Disaster Recovery
-----
 e | Exit
-----
\
Enter Choice: 2

```

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

```

/----Configure Network Interfaces Menu----\
| 1 | Configure Provisioning Network
| 2 | Configure Sync Network
| 3 | Configure DSM Network
| 4 | Configure Backup Provisioning Network
| 5 | Configure Static NAT Addresses
| 6 | Configure Provisioning VIP Addresses
| e | Exit
\
Enter Choice: 1

```

d. On the **Configure Provisioning Network Menu**, choose option 1 if the EPAP\_IP\_VERSION is IPv4, option 2 if the EPAP\_IP\_VERSION is IPv6, or options 1 and 2 in succession if the EPAP\_IP\_VERSION is IPv4v6.

- Enter 1 for **IPv4 Configuration**:

•

```

/-----Configure Provisioning Network Menu-----\
| 1 | IPv4 Configuration |
|-----|
| 2 | IPv6 Configuration |
|-----|
| e | Exit |
\-----/

Enter Choice: 1

EPAP software and PDBA are running. Stop them? [N]: Y
Verifying connectivity with mate...
EPAP A provisioning network IP Address [192.168.61.45]:
EPAP B provisioning network IP Address [192.168.61.46]:
EPAP provisioning network netmask [255.255.255.0]:
EPAP provisioning network default router [192.168.61.250]:

```

- Press **Enter** to reconfigure the network with the same configuration.
- Enter 2 for **IPv6 Configuration**:

```

/-----Configure Provisioning Network Menu-----\
| 1 | IPv4 Configuration |
|-----|
| 2 | IPv6 Configuration |
|-----|
| e | Exit |
\-----/

Enter Choice: 2

EPAP software and PDBA are running. Stop them? [N]: Y
Verifying connectivity with mate...
EPAP A provisioning network IPv6 Address [2606:B400:605:B80B:200:17FF:FE0F:2884]:
EPAP B provisioning network IPv6 Address [2606:B400:605:B80B:200:17FF:FE0F:2F2C]:
EPAP provisioning network IPv6 prefix [64]:
EPAP provisioning network IPv6 default router [FE80:0000:0000:0000:0226:98FF:FE1A:9AC1]:

```

- Press **Enter** to reconfigure the network with the same configuration.
- e. If you need assistance, contact [My Oracle Support \(MOS\)](#).

## 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 EPAP A and B servers, create a new **certificate** directory (`/var/TKLC/epap/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/epap/free/certificate
[admusr@mps-A ~]$ sudo chmod 777 /var/TKLC/epap/free/certificate
[admusr@mps-A ~]$ cd /var/TKLC/epap/free/certificate

```

2. On EPAP A, execute the following commands to determine the IP configuration for which the certificate files were generated.

```
[admsr@mps-A certificate]$ sudo openssl verify /usr/TKLC/plat/etc/ssl/server.crt
[admsr@mps-A certificate]$ sudo openssl verify
/usr/TKLC/plat/etc/ssl/server_dual.crt
```

Sample output of the above commands:

```
[admsr@mps-A certificate]$ sudo openssl verify /usr/TKLC/plat/etc/ssl/server.crt
/usr/TKLC/plat/etc/ssl/server.crt: CN = 10.250.51.149
error 18 at 0 depth lookup:self signed certificate
OK
```

The EPAP network configuration can be IPv4, IPv6, or dual stack (both IPv4 and IPv6), and you need to determine which certificate file corresponds to which network configuration:

- Both certificate files have the same IP address (either IPv4 or IPv6)
  - The server.crt file has the certificate for IPv4 and the server\_dual.crt file has the certificate for IPv6
  - The server.crt file has the certificate for IPv6 and the server\_dual.crt file has the certificate for IPv4
3. Based on the determined network configuration information, generate certificate signing request (CSR) and private key files for the EPAP A server by using the appropriate commands from within the certificate directory.

**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.

- If both certificate files have been generated for the same IP address (either IPv4 or IPv6), enter the following commands:

```
[admsr@mps-A certificate]$ 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=<EPAP GUI IP address, e.g, 1.1.1.1>/emailAddress=xxx@yyy.com"
```

```
[admsr@mps-A certificate]$ sudo /usr/bin/openssl req -newkey rsa:2048 -nodes
-keyout server_dual.key -out server_dual.csr -subj "/C=US/ST=New
York/L=Brooklyn/O=Example Brooklyn Company/OU=Example Org Unit/CN=<EPAP GUI IP
address, e.g, 1.1.1.1>/emailAddress=xxx@yyy.com"
```

- If the server.crt file has the certificate for EPAP IPv4 and the server\_dual.crt file has the certificate for EPAP IPv6, enter the following commands:

```
[admsr@mps-A certificate]$ 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=<EPAP GUI IPv4 IP address, e.g, 1.1.1.1>/emailAddress=xxx@yyy.com"
```

```
[admsr@mps-A certificate]$ sudo /usr/bin/openssl req -newkey rsa:2048 -nodes
```

```
-keyout server_dual.key -out server_dual.csr -subj "/C=US/ST=New
York/L=Brooklyn/O=Example Brooklyn Company/OU=Example Org Unit/CN=<EPAP GUI IPv6
IP address, e.g, 1.1.1.1>/emailAddress=xxx@yyy.com"
```

- If the server.crt file has the certificate for EPAP IPv6 and the server\_dual.crt file has the certificate for EPAP IPv4, enter the following commands:

```
[admusr@mps-A certificate]$ 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=<EPAP GUI IPv6 IP address, e.g, 1.1.1.1>/emailAddress=xxx@yyy.com"
```

```
[admusr@mps-A certificate]$ sudo /usr/bin/openssl req -newkey rsa:2048 -nodes
-keyout server_dual.key -out server_dual.csr -subj "/C=US/ST=New
York/L=Brooklyn/O=Example Brooklyn Company/OU=Example Org Unit/CN=<EPAP GUI IPv4
IP address, e.g, 1.1.1.1>/emailAddress=xxx@yyy.com"
```

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

```
[admusr@mps-A certificate]$ ls -lrt
-rw-r--r-- 1 root root 1679 May 21 11:08 server.key
-rw-r--r-- 1 root root 968 May 21 11:08 server.csr
-rw-r--r-- 1 root root 1675 May 21 11:09 server_dual.key
-rw-r--r-- 1 root root 968 May 21 11:09 server_dual.csr
```

4. Generate certificate signing request (CSR) and private key files for the EPAP B server in the same way (steps 2 - 3), using the files serverB.csr and serverB\_dual.csr for EPAP B.

The following files will be generated on the EPAP B server:

```
[admusr@mps-B certificate]$ ls -lrt
-rw-r----- 1 root root 1679 May 21 11:02 server.key
-rw-r----- 1 root root 968 May 21 11:02 serverB.csr
-rw-r----- 1 root root 1679 May 21 11:02 server_dual.key
-rw-r----- 1 root root 968 May 21 11:02 serverB_dual.csr
```

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



8. Open the EPAP A and B GUIs using https and install the SSL certificates.

- For IPv4, use the following commands:

```
https://<EPAP A GUI IPv4 IP>  
https://<EPAP B GUI IPv4 IP>
```

- For IPv6, use the following commands:

```
https://[<EPAP A GUI IPv6 IP>]  
https://[<EPAP B GUI IPv6 IP>]
```

9. Verify that the EPAP A and B GUIs opened successfully with the installed certificate.
10. If the EPAP GUI does not open, follow these steps on the EPAP 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/sslcert/ca.crt
```

to:

```
SSLCertificateChainFile /etc/httpd/conf/sslcert/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 EPAP A and B GUIs open successfully.

## Installing an SSL Certificate For a Backup Provisionable Interface With Customized Parameters

Perform the following steps to install an SSL certificate for a backup prov interface with customized parameters:

1. Log in to EPAP A as admusr.
2. Switch to the root user as "su -".
3. Change the directory to `/usr/TKLC/plat/etc/ssl/`.
4. Execute the following command to list the files in the directory `/usr/TKLC/plat/etc/ssl/`.

Sample output for the previous command:

```
[admusr@mps-A ssl]$ ls -ltrh server_bkprov*  
-rw-r----- 1 root epap 1.7K May 23 06:33 server_bkprov_v4.key  
-rw-r----- 1 root epap 1.1K May 23 06:33 server_bkprov_v4.crt
```

The EPAP network configuration can be IPv4, IPv6, or dual stack (both IPv4 and IPv6), and you need to determine which certificate file corresponds to which network configuration:

- Both certificate files are present in the `/usr/TKLC/plat/etc/ssl/` directory
  - The `server_bkprov_v4.crt` certificate file is present in the `/usr/TKLC/plat/etc/ssl/` directory
  - The `server_bkprov_v6.crt` certificate file is present in the `/usr/TKLC/plat/etc/ssl/` directory
5. Exit from the root user:

```
[admusr@mps-A ssl]$ exit  
logout
```

6. Sign the certificate files on the EPAP A server according to the determined certificate file information:
  - If both certificate files have been generated for the same IP address (either IPv4 or IPv6), sign both certificate files with that IP address by using the following commands:

```
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=<EPAP  
A Backup Prov IPv4 address >" -newkey rsa:<RSA Key Management> -keyout  
/usr/TKLC/plat/etc/ssl/server_bkprov_v4.key -out  
/usr/TKLC/plat/etc/ssl/server_bkprov_v4.crt
```

```
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=<EPAP  
A Backup Prov IPv6 address >" -newkey rsa:<RSA Key Management> -keyout  
/usr/TKLC/plat/etc/ssl/server_bkprov_v6.key -out  
/usr/TKLC/plat/etc/ssl/server_bkprov_v6.crt
```

- If the `server_bkprov_v4.crt` file is generated because the backup prov is configured for EPAP IPv4, sign the certificate files by 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=<EPAP  
A Backup Prov IPv4 address >" -newkey rsa:<RSA Key Management> -keyout  
/usr/TKLC/plat/etc/ssl/server_bkprov_v4.key -out  
/usr/TKLC/plat/etc/ssl/server_bkprov_v4.crt
```

- If the server\_bkprov\_v6.crt file is generated because the bakcup prov is configured for EPAP IPv6, sign the certificate files by 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=<EPAP
A Backup Prov IPv6 address >" -newkey rsa:<RSA Key Management> -keyout
/usr/TKLC/plat/etc/ssl/server_bkprov_v6.key -out
/usr/TKLC/plat/etc/ssl/server_bkprov_v6.crt
```

7. Sign the certificate files on the EPAP B server in the same way.
8. Restart the httpd service on both the EPAP A and B servers by using the following commands:

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

9. Open the EPAP A and B GUIs using https and install the SSL certificates.

- For IPv4, use the following commands:

```
https://<EPAP A GUI IPv4 IP>
https://<EPAP B GUI IPv4 IP>
```

- For IPv6, use the following commands:

```
https://[<EPAP A GUI IPv6 IP>]
https://[<EPAP B GUI IPv6 IP>]
```

10. Verify that the certificates installed successfully and the EPAP A and B GUIs opened successfully.
11. If the EPAP GUI does not open, on the EPAP A and B servers, follow these steps to reconfigure the IP addresses on EPAP through the epapconfig menu. This will re-install the SSL certificates with the default parameters.

- a. Check the value of EPAP\_IP\_VERSION, and then access the **EPAP Configuration Menu**:

```
[admusr@mps-A ~]$ uiEdit | grep -i "EPAP_A_BACKUP_PROV_NETWORK_IP_ADDRESS"
"EPAP_A_BACKUP_PROV_NETWORK_IP_ADDRESS" is set to "10.75.136.41"

[admusr@mps-A ~]$ uiEdit | grep -i "EPAP_B_BACKUP_PROV_NETWORK_IP_ADDRESS_V6"
"EPAP_B_BACKUP_PROV_NETWORK_IP_ADDRESS_V6" is set to "
2606:b400:605:b912:200:17ff:fe0e:bf88"

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

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

```
/-----EPAP 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 | PDB Configuration Menu
-----
 9 | Security
-----
10 | SNMP Configuration
-----
11 | Configure Alarm Feed
-----
12 | Configure Query Server
-----
13 | Configure Query Server Alarm Feed
-----
14 | Configure SNMP Agent Community
-----
15 | Mate Disaster Recovery
-----
 e | Exit
-----
\
Enter Choice: 2

```

- c. Enter choice 1 to **Configure Provisioning Network**:

```

/-----Configure Network Interfaces Menu-----\
| 1 | Configure Provisioning Network
|-----|
| 2 | Configure Sync Network
|-----|
| 3 | Configure DSM Network
|-----|
| 4 | Configure Backup Provisioning Network
|-----|
| 5 | Configure Static NAT Addresses
|-----|
| 6 | Configure Provisioning VIP Addresses
|-----|
| e | Exit
\-----/
Enter Choice: 1

```

- d. On the **Configure Provisioning Network Menu**, choose option 1 if the EPAP\_IP\_VERSION is IPv4, option 2 if the EPAP\_IP\_VERSION is IPv6, or options 1 and 2 in succession if the EPAP\_IP\_VERSION is IPv4v6.

- Enter 1 for **IPv4 Configuration**:

```

/-----Configure Provisioning Network Menu-----\
| 1 | IPv4 Configuration |
|-----|-----|
| 2 | IPv6 Configuration |
|-----|-----|
| e | Exit |
\-----\

Enter Choice: 1

```

```

EPAP software and PDBA are running. Stop them? [N]: Y
Verifying connectivity with mate...
EPAP A backup provisioning network IP Address [10.75.136.41]:
EPAP B backup provisioning network IP Address [10.75.136.42]:
EPAP backup provisioning network netmask [255.255.255.0]:
EPAP backup provisioning network default router [10.75.136.1]:

```

- Press **Enter** to reconfigure the network with the same configuration.
- e. If you need assistance, contact [My Oracle Support \(MOS\)](#).

## Installing an SSL Certificate For a Backup Provisionable Interface From a Trusted Certificate Authority

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

1. Log in as the admusr user on both the EPAP A and B servers, create a new **certificate** directory (`/var/TKLC/epap/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/epap/free/certificate
[admusr@mps-A ~]$ sudo chmod 777 /var/TKLC/epap/free/certificate
[admusr@mps-A ~]$ cd /var/TKLC/epap/free/certificate

```

2. Switch to the root user as "su -".
3. Change the directory to `/usr/TKLC/plat/etc/ssl/`.
4. Execute the following command to list the files in the directory `/usr/TKLC/plat/etc/ssl/`.

Sample output for the previous command:

```

[admusr@mps-A ssl]$ ls -ltrh server_bkprov*
-rw-r----- 1 root epap 1.7K May 23 06:33 server_bkprov_v4.key
-rw-r----- 1 root epap 1.1K May 23 06:33 server_bkprov_v4.crt

```

5. The EPAP Backup prov network configuration can be IPv4, IPv6, or dual stack (both IPv4 and IPv6), and you need to determine which certificate file corresponds to which network configuration:

- Both certificate files are present in the `/usr/TKLC/plat/etc/ssl/` directory
- The `server_bkprov_v4.crt` certificate file is present in the `/usr/TKLC/plat/etc/ssl/` directory
- The `server_bkprov_v6.crt` certificate file is present in the `/usr/TKLC/plat/etc/ssl/` directory

6. Exit from the root user:

```
[admusr@mps-A ssl]$ exit
logout
```

7. Based on the determined network configuration information, generate certificate signing request (CSR) and private key files for the EPAP A server by using the appropriate commands from within the `certificate` directory.

**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.

- If both certificate files have been generated for the same IP address (either IPv4 or IPv6), enter the following commands:

```
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_bkprov_v4.key -out server_bkprov_v4.csr -subj "/C=US/ST=New
York/L=Brooklyn/O=Example Brooklyn Company/OU=Example Org Unit/CN=<EPAP Backup
Prov IPv4 address>/emailAddress=xxx@yyy.com"
```

```
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_bkprov_v6.key -out server_bkprov_v6.csr -subj
"/C=US/ST=New York/L=Brooklyn/O=Example Brooklyn Company/OU=Example Org
Unit/CN=<EPAP Backup Prov IPv6 address>/emailAddress=xxx@yyy.com"
```

- If the `server_bkprov_v4.crt` file is generated because the backup prov is configured for EPAP IPv4, sign the certificate files by 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 > -newkey rsa:2048
-nodes -keyout server_bkprov_v4.key -out server_bkprov_v4.csr -subj "/C=US/ST=New
York/L=Brooklyn/O=Example Brooklyn Company/OU=Example Org Unit/CN=<EPAP Backup
Prov IPv4 address>/emailAddress=xxx@yyy.com"
```

- If the `server_bkprov_v6.crt` file is generated because the backup prov is configured for EPAP IPv6, sign the certificate files by 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 > -newkey rsa:2048
-nodes -keyout server_bkprov_v6.key -out server_bkprov_v6.csr -subj "/C=US/ST=New
York/L=Brooklyn/O=Example Brooklyn Company/OU=Example Org Unit/CN=<EPAP Backup
Prov IPv6 address>/emailAddress=xxx@yyy.com"
```

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

```
[admusr@mps-A certificate]$ ls -lrt
-rw-r----- 1 root root 1679 May 21 11:08 server_bkprov_v4.key
-rw-r----- 1 root root 968 May 21 11:08 server_bkprov_v4.csr
```

```
-rw-r----- 1 root root 1675 May 21 11:09 server_bkprov_v6.key
-rw-r----- 1 root root 968 May 21 11:09 server_bkprov_v6.csr
```

8. Generate certificate signing request (CSR) and private key files for the EPAP B server in the same way (steps 1- 7), using the files serverB\_bkprov\_v4.csr and serverB\_bkprov\_v6.csr for EPAP B.

The following files will be generated on the EPAP B server:

```
[admusr@mps-B certificate]$ ls -lrt
-rw-r----- 1 root root 1679 May 21 11:02 server_bkprov_v4.key
-rw-r----- 1 root root 968 May 21 11:02 serverB_bkprov_v4.csr
-rw-r----- 1 root root 1679 May 21 11:02 server_bkprov_v6.key
-rw-r----- 1 root root 968 May 21 11:02 serverB_bkprov_v6.csr
```

9. Send the generated CSR files (server\_bkprov\_v4.csr, server\_bkprov\_v6.csr, serverB\_bkprov\_v4.csr and serverB\_bkprov\_v6.csr) to the CA. The CA will provide signed certificate files (server\_bkprov\_v4.crt, server\_bkprov\_v6.crt, serverB\_bkprov\_v4.crt, serverB\_bkprov\_v6.crt) in return.
10. Copy the appropriate files to the appropriate ssl directory, and rename as needed:
  - a. On the EPAP A server, copy the four files generated through the openssl commands (server\_bkprov\_v4.key, server\_bkprov\_v6.key, server\_bkprov\_v4.csr, server\_bkprov\_v6.csr) and the two files provided by the CA for the EPAP A server (server\_bkprov\_v4.crt and server\_bkprov\_v6.crt) to the /usr/TKLC/plat/etc/ssl directory.
  - b. On the EPAP B server, copy the four files generated through the openssl commands (server\_bkprov\_v4.key, server\_bkprov\_v6.key, serverB\_bkprov\_v4.csr, serverB\_bkprov\_v6.csr) and the two files provided by the CA for the EPAP B server (serverB\_bkprov\_v4.crt and serverB\_bkprov\_v6.crt) to the /usr/TKLC/plat/etc/ssl directory.
  - c. After copying serverB\_bkprov\_v4.crt and serverB\_bkprov\_v6.crt to the /usr/TKLC/plat/etc/ssl directory on the EPAP B server, rename them to server\_bkprov\_v4.crt and server\_bkprov\_v6.crt, respectively.
11. Restart the httpd service on both the EPAP 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 EPAP A and B GUIs using https and install the SSL certificates.

- For IPv4, use the following commands:

```
https://<EPAP A GUI IPv4 IP>
https://<EPAP B GUI IPv4 IP>
```

- For IPv6, use the following commands:

```
https://[<EPAP A GUI IPv6 IP>]
https://[<EPAP B GUI IPv6 IP>]
```

13. Verify that the EPAP A and B GUIs opened successfully with the installed certificate.
14. If the EPAP GUI does not open, follow these steps on the EPAP 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/sslcert/ca.crt
```

to:

```
SSLCertificateChainFile /etc/httpd/conf/sslcert/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 EPAP A and B GUIs open successfully.

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

Sample output for the previous command:

```
[admusr@mps-A ssl]$ ls -ltrh server_vip_v*
-rw-r----- 1 root epap 1.7K May 25 03:34 server_vip_v4.key
-rw-r----- 1 root epap 1.1K May 25 03:34 server_vip_v4.crt
```



5. Exit from the root user:

```
[admusr@mps-A ssl]$ exit
logout
```

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. Sign the certificate files on the EPAP A server according to the determined network configuration information:

The certificate file `server_vip_v4.crt` is generated, as the VIP is configured in IPv4 configuration. Sign the certificate file 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=<EPAP
A VIP IPv4 address >" -newkey rsa:<RSA Key Management> -keyout
/usr/TKLC/plat/etc/ssl/server_vip_v4.key -out
/usr/TKLC/plat/etc/ssl/server_vip_v4.crt
```

7. Sign the certificate files on the EPAP B server in the same way.
8. Restart the `httpd` service on both the EPAP A and B servers by using the following commands:

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

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

```
https://<EPAP A VIP IPv4 IP>
```

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

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

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

```
/-----EPAP 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 | PDB Configuration Menu |
|---|-----|
```

```

 9 | Security
---|-----
10 | SNMP Configuration
---|-----
11 | Configure Alarm Feed
---|-----
12 | Configure Query Server
---|-----
13 | Configure Query Server Alarm Feed
---|-----
14 | Configure SNMP Agent Community
---|-----
15 | Mate Disaster Recovery
---|-----
  e | Exit
\-----/
Enter Choice: 2

```

b. Enter choice 6 to **Configure Provisioning VIP Addresses**:

```

MPS Side A:  hostname: hvar-A  hostid: 4b0a1a8d
              Platform Version: 6.1.4-7.4.0.0.0_88.37.0
              Software Version: EPAP 162.0.16-0.59464
              Thu May 25 07:06:20 EDT 2017

/-----Configure Provisioning VIP address Menu-----\
| 1 | IPv4 Configuration |
|---|-----|
| 2 | IPv6 Configuration |
|---|-----|
|  e | Exit |
\-----/

Enter Choice: 1

Verifying root connectivity with mate...
EPAP local provisioning Virtual IP Address [10.75.141.28]:
EPAP remote provisioning Virtual IP Address [10.75.141.29]:

```

- c. Press **Enter** to reconfigure the network with the same configuration.
- d. If you need assistance, contact [My Oracle Support \(MOS\)](#).

## 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 EPAP A and B servers, create a new **certificate** directory (`/var/TKLC/epap/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/epap/free/certificate
[admusr@mps-A ~]$ sudo chmod 777 /var/TKLC/epap/free/certificate
[admusr@mps-A ~]$ cd /var/TKLC/epap/free/certificate
```

2. When the EPAP is configured in IPv4 configuration, log in to EPAP 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:

```
[admusr@mps-A ssl]$ ls -ltrh server_vip_v*
-rw-r----- 1 root epap 1.7K May 25 03:34 server_vip_v4.key
-rw-r----- 1 root epap 1.1K May 25 03:34 server_vip_v4.crt
```

6. Exit from the root user:

```
[admusr@mps-A ssl]$ exit
logout
```

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.

7. Generate certificate signing request (CSR) and private key files for EPAP 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 EPAP 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_v4.key -out server_vip_v4.csr -subj "/C=US/ST=New
York/L=Brooklyn/O=Example Brooklyn Company/OU=Example Org Unit/CN=<EPAP 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.

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

```
[admusr@mps-A certificate]$ ls -lrt
-rw-r----- 1 root root 1679 May 21 11:08 server_vip_v4.key
-rw-r----- 1 root root 968 May 21 11:08 server_vip_v4.csr
```

8. Generate certificate signing request (CSR) and private key files for EPAP B server by executing steps 1 to 7. Sign the certificate files on the EPAP B server in the same way. Use the files `serverB_vip_v4.csr` and `serverB_vip_v6.csr` for EPAP B.

These commands generate the following files on the EPAP 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
```

9. Send the generated CSR files (server\_vip\_v4.csr, serverB\_vip\_v4.csr) to the CA. The CA will provide signed certificate files (server\_vip\_v4.crt, serverB\_vip\_v4.crt) in return.
10. Copy the appropriate files to the appropriate ssl directory, and rename as needed:
  - On the EPAP A server, copy the two files generated through the openssl commands (server\_vip\_v4.key, server\_vip\_v4.csr) and the file provided by the CA (server\_vip\_v4.crt) to the /usr/TKLC/plat/etc/ssl directory.
  - On the EPAP B server, copy the two files generated through the openssl command (server\_vip\_v4.key, serverB\_vip\_v4.csr) and the file provided by the CA for the EPAP B server (serverB\_vip\_v4.crt) to the /usr/TKLC/plat/etc/ssl directory.
11. After copying server B\_vip\_v4.crt to the /usr/TKLC/plat/etc/ssl directory on the EPAP B server, rename them to server\_vip\_v4.crt.
12. Restart the httpd service on both the EPAP 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
```

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

```
https://<EPAP A VIP IPv4 IP>
```

14. Verify that the certificate installed successfully and the GUI opened successfully.
15. If the EPAP GUI does not open, follow these steps on the EPAP 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/sslcert/ca.crt
```

to:

```
SSLCertificateChainFile /etc/httpd/conf/sslcert/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 EPAP A and B GUIs open successfully.

# Appendix

# A

## Secure Deployment Checklist

---

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

- Change default passwords
- Set strong password restrictions
- Restrict admin functions to the required administrator groups
- Change the default community names in `snmpd.conf`
- Utilize the Authorized IP addresses feature

# Appendix B

## Secure Turnover to Customer

---

### Topics:

- [Secure Turnover Process.....40](#)

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.

## 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 EPAP 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 EPAP UI login name (such as uiadmin) and changes the password to a new unique password.
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 EPAP 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.
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 EPAP 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 EPAP UI login accounts using the new customer passwords to verify success with the new customer passwords.



## E

EPAP

EAGLE Application Processor

EPAP-related features

Features that require EPAP connection and use the Real Time Database (RTDB) for lookup of subscriber information.

- ANSI Number Portability Query (AINPQ)
- ANSI-41 AnalyzedInformation Query – no EPAP/ELAP (ANSI41 AIQ)
- Anytime Interrogation Number Portability (ATI Number Portability, ATINP)
- AINPQ, INP, G-Port SRI Query for Prepaid, GSM MAP SRI Redirect, IGM, and ATINP Support for ROP
- A-Port Circular Route Prevention (A-Port CRP)
- Equipment Identity Register (EIR)
- G-Flex C7 Relay (G-Flex)
- G-Flex MAP Layer Routing (G-Flex MLR)
- G-Port SRI Query for Prepaid
- GSM MAP SRI Redirect to Serving HLR (GSM MAP SRI Redirect)
- GSM Number Portability (G-Port)
- IDP A-Party Blacklist
- IDP A-Party Routing
- IDP Relay Additional Subscriber Data (IDPR ASD)
- IDP Relay Generic Routing Number (IDPR GRN)
- IDP Service Key Routing (IDP SK Routing)

## E

- IDP Screening for Prepaid
- INAP-based Number Portability (INP)
- Info Analyzed Relay Additional Subscriber Data (IAR ASD)
- Info Analyzed Relay Base (IAR Base)
- Info Analyzed Relay Generic Routing Number (IAR GRN)
- Info Analyzed Relay Number Portability (IAR NP)
- INP Circular Route Prevention (INP CRP)
- IS41 Mobile Number Portability (A-Port)
- IS41 GSM Migration (IGM)
- MNP Circular Route Prevention (MNPCR)
- MO-based GSM SMS NP
- MO-based IS41 SMS NP
- MO SMS Generic Routing Number (MO SMS GRN)
- MO- SMS B-Party Routing
- MO SMS IS41-to-GSM Migration
- MT-based GSM SMS NP
- MT-based GSM MMS NP
- MT-based IS41 SMS NP
- MTP Routed Messages for SCCP Applications (MTP Msgs for SCCP Apps)
- MTP Routed Gateway Screening Stop Action (MTPRTD GWS Stop Action)
- Portability Check for MO SMS
- Prepaid IDP Query Relay (IDP Relay, IDPR)
- Prepaid SMS Intercept Phase 1 (PPSMS)
- Service Portability (S-Port)
- S-Port Subscriber Differentiation
- Triggerless ISUP Framework Additional Subscriber Data (TIF ASD)

## E

- Triggerless ISUP Framework Generic Routing Number (TIF GRN)
- Triggerless ISUP Number Portability (TIF NP)
- Triggerless ISUP Framework Number Substitution (TIF NS)
- Triggerless ISUP Framework SCS Forwarding (TIF SCS Forwarding)
- Triggerless ISUP Framework Simple Number Substitution (TIF SNS)
- Voice Mail Router (V-Flex)

## I

IPv4

Internet Protocol version 4

Identifies an Internet Protocol version 4 address composed of 4 bytes in a dotted decimal format (for example, nnn.nn.nnn.nn).

IPv6

Internet Protocol version 6

Identifies an Internet Protocol version 6 address composed of 8 groups of colon-separated 4 hexadecimal digits.

## M

MIB

Management Information Database

A database of network management information that is used and maintained by the SNMP protocol.

MPS

Multi-Purpose Server

The Multi-Purpose Server provides database/reload functionality and a variety of high capacity/high speed offboard database functions

**M**

for applications. The MPS resides in the General Purpose Frame.

Messages Per Second

A measure of a message processor's performance capacity. A message is any Diameter message (Request or Answer) which is received and processed by a message processor.

**O**

OCEEMS

Oracle Communications EAGLE Element Management System

An optional product in the Oracle Communications EAGLE product family that consolidates real-time element management functions at a centralized point within the signaling network.

**P**

PDB

Provisioning Database

PDBA

Provisioning Database Application

There are two Provisioning Database Applications (PDBAs), one in EPAP A on each EAGLE. They follow an Active/Standby model. These processes are responsible for updating and maintaining the Provisioning Database (PDB).

PDBI

Provisioning Database Interface

The interface consists of the definition of provisioning messages only. The customer must write a client application that uses the PDBI request/response messages to communicate with the PDBA.

**S**

## S

SNMP	<p>Simple Network Management Protocol.</p> <p>An industry-wide standard protocol used for network management. The SNMP agent maintains data variables that represent aspects of the network. These variables are called managed objects and are stored in a management information base (MIB). The SNMP protocol arranges managed objects into groups.</p>
SSH	<p>Secure Shell</p> <p>A protocol for secure remote login and other network services over an insecure network. SSH encrypts and authenticates all EAGLE IPUI and MCP traffic, incoming and outgoing (including passwords) to effectively eliminate eavesdropping, connection hijacking, and other network-level attacks.</p>
SSL	<p>Secure Socket Layer (SSL) is an industry standard protocol for clients needing to establish secure (TCP-based) SSL-enabled network connections</p>
STP	<p>Signal Transfer Point</p> <p>The STP is a special high-speed switch for signaling messages in SS7 networks. The STP routes core INAP communication between the Service Switching Point (SSP) and the Service Control Point (SCP) over the network.</p> <p>Spanning Tree Protocol</p>

## U

	<b>U</b>
UI	User Interface
	<b>V</b>
VLAN	Virtual Local Area Network
	A logically independent network. A VLAN consists of a network of computers that function as though they were connected to the same wire when in fact they may be physically connected to different segments of a LAN. VLANs are configured through software rather than hardware. Several VLANs can co-exist on a single physical switch.