Oracle® Communications

User Data Repository
Security Guide

Release 12.10

F45854-01

August 2021

ORACLE®

Oracle Communications User Data Repository Security Guide, Release 12.10

F45854-01

CAUTION: Use only the Installation procedure included in the Install Kit.
Before installing any system, please access My Oracle Support (MOS) (https://support.oracle.com) and review any Technical Service Bulletins (TSBs) that relate to this procedure.

My Oracle Support (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.

See more information on MOS in the Appendix section.

Oracle Communications User Data Repository Security Guide

Table of Contents

Oracle Communications User Data Repository Security Guide

List of Figures

List of Tables

Oracle Communications User Data Repository Security Guide

1 Introduction

This document provides guidelines and recommendations for configuring the Oracle Communications User Data Repository to enhance the security of the system. The recommendations herein are optional and should be considered along with your organizations approved security strategies. 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.

1.1 Audience

This Guide is intended for administrators responsible for product and network security.

1.2 References

The following references capture the source material used to create this document. These documents are included in the Oracle Communications User Data Repository documentation set. See Appendix C.

[1]   *Operations, Administration, and Maintenance (OAM) User's Guide*

[2]   *Alarms, KPIs, and Measurements Reference*

[3]   *Installation and Configuration Guide*

[4]   *Enhanced Subscriber Profile Repository User's Guide*

[5]   *REST Provisioning Interface Specification*

[6]   *Bulk Import/Export File Specification*

[7]   *SOAP Provisioning Interface Specification*

1.3 Glossary

This section lists terms and acronyms specific to this document.

Table 1. Glossary

Acronym/Term	Definition
CLI	Command Line Interface
CSR	Customer Service Request
ESP	Encapsulating Security Payload
GUI	Graphical User Interface
HIDS	Host Intrusion Detection System
IKE	Internet Key Exchange
IPsec	Internet Protocol security
IV	Initialization Vector
KPI	Key Performance Indicator
LDAP	Lightweight Directory Access Protocol
MP	Message Processor

Table 1. Glossary

Acronym/Term	Definition
NOAMP	Network Operation, Administration, Maintenance, and Provisioning
OAM	Operation, Administrations and Maintenance
OS	Operating System
PSO	Pools Spanning Oracle Communication User Data Repository systems
REST	Representational State Transfer. A type of Northbound provisioning interface.
SFTP	Secure File Transfer Protocol
SOAM	System Operation, Administration, and Maintenance
SOAP	Simple Object Access Protocol
SNMP	Simple Network Management Protocol
SSO	Single Sign On
TLS	Transport Layer Security
UDR	User Data Repository
Ud Interface	The Ud Interface is an access protocol as defined in 3GPP TS 29.335. It defines a logical connection between a Front-End (FE) and a User Data Repository (UDR). The Ud Interface consists connections using LDAP to perform CRUD operations on subscriber data (Create/Delete/Update/Read), and connections using SOAP for publish/subscribe interface in order to request notifications when subscriber data stored in the UDR changes, and to receive those notifications when the data is changed.
Ud Client	A Ud Client is a Front-End (FE) that uses the Ud Interface to access subscriber data from a User Data Repository (UDR)
Ud Server	A Ud Server is a User Data Repository (UDR) that has a Ud Interface to allow external Front-Ends to access subscriber data via LDAP and SOAP, according to the Ud Interface specification

2 Oracle Communications User Data Repository Security Overview

This chapter provides an overview of Oracle Communications User Data Repository security.

2.1 Basic Security Considerations

The following principles are fundamental to using any application securely:

- **Keep software up to date.** Consider upgrading to the latest maintenance release. Consult with your Oracle support team to plan for Oracle Communications User Data Repository software upgrades.

- **Limit privileges.** Users should be assigned to the proper user group and 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.

- **Configure software securely.** For example, use secure protocols such as TLS and strong passwords.

- **Learn about and use of the Oracle Communications User Data Repository security features.** See Section 3 "*Implementing Oracle Communications User Data Repository Security*" for more information.

- **Keep up to date on security information.** Oracle regularly issues Security Alerts for vulnerability fixes deemed too critical. It is advisable to install the applicable security patches as soon as possible. See the Security Alerts page at the following link.

  http://www.oracle.com/technetwork/topics/security/alerts-086861.html#SecurityAlerts

2.2 Accessing the Oracle Communications User Data Repository system

There are four ways a user can access the Oracle Communications User Data Repository system.

1. Web browser GUI – The client access to the Oracle Communications User Data Repository GUI for remote administration requires a web browser supporting a TLS 1.2 enabled session to Oracle Communications User Data Repository. This application supports the use of Microsoft® Internet Explorer 8.0, 9.0 or 10.0, and both cookies and java script must be enabled. When a user accesses the Oracle Communications User Data Repository system via the GUI interface, the following screen is presented. On the Log In screen, enter the Username and Password credentials, then click **Log In** to access the GUI.

Figure 1. Oracle Communications User Data Repository Login Page

Oracle Communications User Data Repository Security Guide

When successfully logged in, the Oracle Communications User Data Repository home page appears as shown below. To log out, the user can click the upper-right corner link labelled **Logout** or select the bottom menu item.

Figure 2. Oracle Communications User Data Repository Home Page
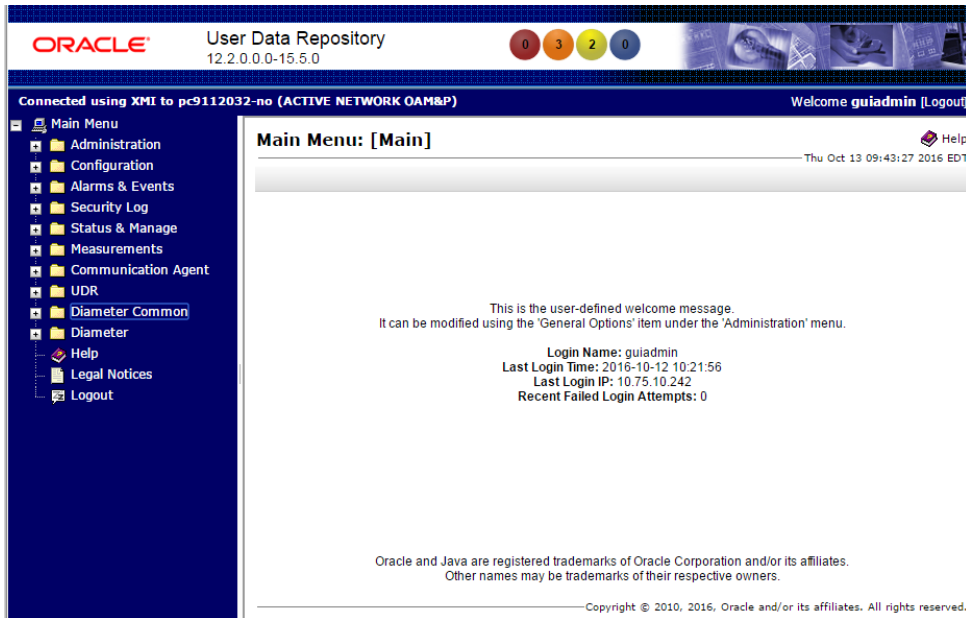
2. CLI via SSH client - Normal login access is remote through network connections. The client access to the command line interface (CLI) is with an SSH capable client such as PUTTY, SecureCRT or similar client using the default administrative login account. SSH login is supported on the distinct management interface. To log out, enter the command, "logout" and press the **Enter** key.

3. Local access is supported by a hardware connection of a monitor and a key board. The local access supports CLI only. When successfully logged in, a command line prompt containing userid @host name followed by a $ prompt appears.

4. There is no requirement to add additional users, but adding users is supported.

5. iLO Web GUI access: Proliant Server iLO provides Web GUI access from an Internet Explorer session using the URL, **https://<iLO IP Address>/.** Using a supported web browser, log in to iLO as an administrator user by providing username and password.

2.3 Overview of Oracle Communications User Data Repository Security

Oracle Communications User Data Repository is developed with security in mind and is delivered with a standard configuration that includes Linux operating system security hardening best practices. These practices include the following security objectives:

- Attack Surface Reduction
- Attack Surface Hardening
- Vulnerability Mitigation

3 Implementing Oracle Communications User Data Repository Security

This chapter explains security-related configuration settings that may be applied to Oracle Communications User Data Repository.

3.1 Oracle Communications User Data Repository Web GUI Standard Features

This section explains the security features of the Oracle Communications User Data Repository software that are available to the Administrative User through the Graphical User Interface (GUI) using a compatible web browser.

3.1.1 User Administration

There is a pre-defined user and group that are delivered with the system for setting up the groups and users by the customer. The following are details of this pre-defined user.

Table 2. Predefined User and Group

User	Group	Description
guiadmin	**admin**	Full access (read/write privileges) to all functions including administration functions

The *User Administration* page enables the administrator to perform functions such as adding, modifying, enabling, or deleting user accounts. 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. After three consecutive, unsuccessful login attempts, a user account is disabled. The number of failed login attempts before an account is disabled is a value that is configured through **Administrations> Options**. The customer can set this value to 0-10, with a default of 3. If the customer sets the value to 0, the user account will never be disabled for unsuccessful login attempts.

Each user is also assigned to one or more groups. A user must have user/group administrative privileges to view or make changes to user accounts or groups.

For more details on user administration, see the Users Administration section in [1] *Operations, Administration, and Maintenance (OAM) User's Guide.*

3.1.1.1 Establishing GUI Groups and Group Privileges

Each GUI user is assigned to one or more groups. Permissions to a set of functions are assigned to the group. The permissions determine the functions and restrictions for the users belonging to that group. The *Groups Administration* page enables you to create, modify, and delete user groups.

The permissions in this page are grouped into the below sections

- Global Action Permissions
- Administration Permissions
- Configuration Permissions
- Alarms & Events Permissions
- Security Log Permissions
- Status & Manage Permissions
- Measurements Permissions
- Communication Agent Configuration Permissions
- Communication Agent Maintenance Permissions

Oracle Communications User Data Repository Security Guide

- Diameter Configuration Permissions
- Diameter Maintenance Permissions
- Diameter Diagnostics Permissions
- Diameter Mediation Permissions
- Diameter AVP Dictionary Permissions
- UDR Configuration Permissions
- UDR SEC Permissions
- UDR Maintenance Permissions

For more details on the permissions available for the above groups, please see the section Group Administration in the [1] *Operations, Administration, and Maintenance (OAM) User's Guide* and the [4] *Enhanced Subscriber Profile Repository User's Guide.*

For non-administrative users, a group with restricted authority is essential. To prevent non-administrative users from setting up new users and groups, be sure that User and Group in the Administration Permissions section are unchecked (see Figure 3.

Figure 3. Global Action and Administration Permissions

Permissions:

Resource	View	Insert	Edit	Delete	Manage
Global Action Permissions	☐	☐	☐	☐	☐
Administration Permissions	☐	☐	☐	☐	☐
General Options	☐		☐		
Users	☐	☐	☐	☐	☐
Groups	☐	☐	☐	☐	
Sessions	☐			☐	
Certificate Management	☐	☐	☐	☐	
Authorized IPs	☐	☐	☐	☐	
SFTP Users	☐	☐	☐	☐	
Software Versions	☐				
Software Upgrade	☐		☐		☐
Remote LDAP Authentication	☐	☐	☐	☐	
Remote SNMP Trapping	☐		☐		
Remote Export Server	☐	☐	☐	☐	☐
DNS Configuration	☐		☐		

3.1.1.2   Creating GUI Users and Assigning to Groups

Prior to adding a User, determine to which user group the user should be assigned based on the user's operational role. The group assignment determines the functions that a user may access. A user must have user/group administrative privileges to view or make changes to user accounts or groups. The administrative user can set up or change user accounts and groups, enable or disable user accounts, set password expiration intervals, and change user passwords.

Oracle Communications User Data Repository Security Guide

The Insert User page displays the following elements:

1. UserName
2. Group
3. Authentication Options
4. Access Allowed
5. Maximum Concurrent Logins
6. Session Inactivity Limit
7. Comment

For more details on these elements, please refer to the Administration chapter in the [1] *Operations, Administration, and Maintenance (OAM) User's Guide.*

The user administration page lets users perform the below actions:

- Add a New User
- View User Account Information
- Update User Account Information
- Delete a User
- Enable/Disable a User Account
- Changing a User's Assigned Group
- Generate a User Report
- Change Password

For details on how to perform these actions, please refer to the Administration chapter in the [1] *Operations, Administration, and Maintenance (OAM) User's Guide*.

3.1.2   GUI User Authentication

Users are authenticated using either login credentials or Single Sign-On. See the Passwords section under Administration in the OAM guide for more details on password setup. Single sign-on (SSO) can be configured to work either with or without a shared LDAP authentication server. If an LDAP server is configured, SSO can be configured to require remote (LDAP) authentication for SSO access on an account by account basis. See LDAP Authentication in the [1] *Operations, Administration, and Maintenance (OAM) User's Guide* for more details.

3.1.2.1   GUI Passwords

Password configuration, such as setting passwords, password history rules, and password expiration, occurs in Administration. The application provides two ways to set passwords: through the user interface from the *Users Administration* page, and at the Oracle Communications User Data Repository Login page. For more detailed steps on performing these two methods, please refer to the *Administration* chapter in the [1] *Operations, Administration, and Maintenance (OAM) User's Guide*.

3.1.2.2   Changing Passwords for All Oracle Communications User Data Repository Administrative Accounts

The System Installation procedure will create the following default accounts:

- **guiadmin** – for Oracle Communications User Data Repository Application GUI
- **root** – for CLI
- **admusr** – for CLI

Oracle Communications User Data Repository Security Guide

This procedure will also convey the passwords for the accounts created. As a security measure, these passwords must be changed.

To change the default password of an account created for web GUI access, See the [1] *Operations, Administration, and Maintenance (OAM) User's Guide* for "Passwords" in the "Administration" chapter.

For changing the OS account passwords of a CLI account, please see Section 3.4.1 "*Changing OS User Account Passwords*"

3.1.2.3 Setting up Password Complexity

A valid password must contain from 8 to 16 characters. A password must contain at least three of the four types of characters: numerics, lower case letters, upper case letters, or special characters (! @ # $ % ^ & * ? ~). A password cannot be the same as the Username or contain the Username in any part of the password (for example, Username=jsmith and password=$@jsmithJS would be invalid). A password cannot be the inverse of the Username (for example, Username=jsmith and password=$@htimsj would be invalid). By default, a user cannot reuse any of the last three passwords. This feature can be configured with the required setting for the "MaxPasswordHistory" field in the **Administration > General Options** page.

3.1.2.4 Setting up Password Aging Parameters

Password expiration is enforced the first time a user logs in to the user interface. During initial user account setup, the administrative user grants the user a temporary password, and optionally forces a change of password on first login. The user is redirected to a page that requires the user to enter the old password and then enter a new password twice.

The user interface provides two forms of password expiration:

- The password expiration can be forced when a new user logs in for the first time with a temporary password granted by the administrator.
- The administrative user can configure password expiration on a system-wide basis.

By default, password expiration occurs after 90 days.

See the section **Configuring the Expiration of Password** in the [1] *Operations, Administration, and Maintenance (OAM) User's Guide*, Administration chapter.

3.1.2.5 Restrict Concurrent GUI Logins

The *Insert User* page has "Maximum Concurrent Logins" field; the value in this field indicates the maximum concurrent Logins per user per server. This feature cannot be enabled for users belonging to the Admin group. The range in this field is 0 to 50.

The *User Administration* page has a "Concurrent Logins Allowed" field. The value in this field is the concurrent number of logins allowed.

Note: Restrictions on number of concurrent login instances for OS users can be provided by contacting Oracle technical support.

3.1.2.6 External Authentication

Users can be authenticated remotely where an external LDAP server is used to perform authentication.

3.1.2.7 LDAP Authentication for GUI Users

Use this feature to configure, update, or delete LDAP authentication servers. This feature is available under the **Remote Servers** option. If multiple LDAP servers are configured, the first available server in the list is used to perform authentication. Secondary servers are only used if the first server is unavailable.

Below are the elements required to configure an LDAP server:

Oracle Communications User Data Repository Security Guide

- Hostname
- Account Domain Name
- Account Domain Name Short
- Port
- Base DN
- Password
- Account Filter Format
- Account Canonical Form
- Referrals
- Bind Requires DN

See the *LDAP Authentication* section in the [1] *Operations, Administration, and Maintenance (OAM) User's Guide* for more details.

3.1.2.8   System Single Sign-On for GUI Users

Single Sign-On allows the user to log into multiple servers within a zone by using a shared certificate among the subject servers within the zone. Once a user has successfully authenticated with any system in the SSO domain, the user can access other systems in the SSO zone without the need to re-enter authentication credentials. When two zones in the SSO domain exchange certificates, a trusted relationship is established between the zones, as well as between all systems grouped into the zone, expanding the authenticated login capability to servers in both zones. For details on configuring single sign-on zones, please see the section *Certificate Management* in the [1] *Operations, Administration, and Maintenance (OAM) User's Guide*.

3.1.2.9   Set Password Strength Minimum Digit Characters

Execute the below procedure for each and every server in the topology:

Procedure 1.Set Password Strength Minimum Digit Characters

1.	Login as admusr on the server.
	
	```login: admusr```
	```Password: <current admin user password>```

2.	Check out the file system-auth and password-auth:
	
	```$ sudo rcstool co /etc/pam.d/system-auth```
	```$ sudo rcstool co /etc/pam.d/password-auth```

3.	Execute the below commands
	
	```$ sudo sed -i --follow-symlinks "/pam_cracklib.so/ s/$/ dcredit=-1/" /etc/pam.d/system-auth```
	```$ sudo sed -i --follow-symlinks "/pam_cracklib.so/ s/$/ dcredit=-1/" /etc/pam.d/password-auth```

4.	Check in the file `system-auth` and `password-auth`:
	
	`$ sudo rcstool ci/etc/pam.d/system-auth`
	
	`$ sudo rcstool ci/etc/pam.d/password-auth`

3.1.2.10 Set Password Strength Minimum Uppercase Characters

Execute the below procedure for each and every server in the topology:

Procedure 2.Set Password Strength Minimum Uppercase Characters	

1.	Login as admusr on the server.
	
	`login: admusr`
	
	`Password: <current admin user password>`

2.	Check out the file `system-auth` and `password-auth`:
	
	`$ sudo rcstool co /etc/pam.d/system-auth`
	
	`$ sudo rcstool co /etc/pam.d/password-auth`

3.	Execute the below commands:
	
	`$ sudo sed -i --follow-symlinks "/pam_cracklib.so/ s/$/ ucredit=-2/" /etc/pam.d/system-auth`
	
	`$ sudo sed -i --follow-symlinks "/pam_cracklib.so/ s/$/ ucredit=-2/" /etc/pam.d/password-auth`

4.	Check in the file `system-auth` and `password-auth`:
	
	`$ sudo rcstool ci/etc/pam.d/system-auth`
	
	`$ sudo rcstool ci/etc/pam.d/password-auth`

3.1.2.11 Set Password Strength Minimum Special Characters

Execute the below procedure for each and every server in the topology:

Procedure 3.Set Password Strength Minimum Special Characters	

1.	Login as admusr on the server.
	
	`login: admusr`
	
	`Password: <current admin user password>`

2.	Check out the file `system-auth` and `password-auth`:
	
	`$ sudo rcstool co /etc/pam.d/system-auth`
	
	`$ sudo rcstool co /etc/pam.d/password-auth`

3.	Execute the below commands:
	
	`    $ sudo sed -i --follow-symlinks "/pam_cracklib.so/ s/$/`
	`ocredit=-2/" /etc/pam.d/system-auth`
	
	`    $ sudo sed -i --follow-symlinks "/pam_cracklib.so/ s/$/`
	`ocredit=-2/" /etc/pam.d/password-auth`

4.	Check in the file `system-auth` and `password-auth`:
	
	`    $ sudo rcstool ci/etc/pam.d/system-auth`
	
	`    $ sudo rcstool ci/etc/pam.d/password-auth`

3.1.2.12   Set Password Strength Minimum Lowercase Characters

Execute the below procedure for each and every server in the topology:

Procedure 4.Set Password Strength Minimum Lowercase Characters	

1.	Log in as admusr on the server.
	
	`    login: admusr`
	`    Password: <current admin user password>`

2.	Check out the file `system-auth` and `password-auth`:
	
	`    $ sudo rcstool co /etc/pam.d/system-auth`
	
	`    $ sudo rcstool co /etc/pam.d/password-auth`

3.	Execute the below commands:
	
	`    $ sudo sed -i --follow-symlinks "/pam_cracklib.so/ s/$/`
	`lcredit=-2/" /etc/pam.d/system-auth`
	
	`    $ sudo sed -i --follow-symlinks "/pam_cracklib.so/ s/$/`
	`lcredit=-2/" /etc/pam.d/password-auth`

4.	Check in the file `system-auth` and `password-auth`:
	
	`    $ sudo rcstool ci/etc/pam.d/system-auth`
	
	`    $ sudo rcstool ci/etc/pam.d/password-auth`

3.1.2.13   Set Deny for Failed Password Attempts

Execute the below procedure for each and every server in the topology:

Procedure 5.Set Deny for Failed Password Attempts
1. Log in as admusr on the server. `    login: admusr`

	`Password: <current admin user password>`

2.	Check out the files `system-auth` and `password-auth`:
	
	`$ sudo rcstool co /etc/pam.d/system-auth`
	
	`$ sudo rcstool co /etc/pam.d/password-auth`

3.	Execute below commands:
	
	`$ sudo sed -i --follow-symlinks`
	`"/^auth.*sufficient.*pam_unix.so.*/i auth required`
	`pam_faillock.so preauth silent deny=5 unlock_time=604800`
	`fail_interval=900" /etc/pam.d/system-auth`
	
	`$ sudo sed -i --follow-symlinks`
	`"/^auth.*sufficient.*pam_unix.so.*/a auth [default=die]`
	`pam_faillock.so authfail deny=5 unlock_time=604800`
	`fail_interval=900" /etc/pam.d/system-auth`
	
	`$ sudo sed -i --follow-symlinks`
	`"/^account.*required.*pam_unix.so/i account required`
	`pam_faillock.so" /etc/pam.d/system-auth`
	
	`$ sudo sed -i --follow-symlinks`
	`"/^auth.*sufficient.*pam_unix.so.*/i auth required`
	`pam_faillock.so preauth silent deny=5 unlock_time=604800`
	`fail_interval=900" /etc/pam.d/password-auth`
	
	`$ sudo sed -i --follow-symlinks`
	`"/^auth.*sufficient.*pam_unix.so.*/a auth [default=die]`
	`pam_faillock.so authfail deny=5 unlock_time=604800`
	`fail_interval=900" /etc/pam.d/password-auth`
	
	`$ sudo sed -i --follow-symlinks`
	`"/^account.*required.*pam_unix.so/i account required`
	`pam_faillock.so" /etc/pam.d/password-auth`

4.	Check in the files `system-auth` and `password-auth`:
	
	`$ sudo rcstool ci/etc/pam.d/system-auth`
	
	`$ sudo rcstool ci/etc/pam.d/password-auth`

3.1.2.14   Set Minimum Password Length

Execute the below procedure for each and every server in the topology:

	Procedure 6.Set Minimum Password Length

1.	Log in as admusr on the server.
	
	`login: admusr`
	
	`Password: <current admin user password>`

2.	Check out the file `password-auth`: `$ sudo rcstool co /etc/pam.d/password-auth`

3.	Execute the below command:
	
	`$ sudo sed -i --follow-symlinks "/pam_cracklib.so/ s/$/`
	`minlen=14/" /etc/pam.d/password-auth`

4.	Check in the file `password-auth`: `$ sudo rcstool ci/etc/pam.d/password-auth`

3.1.3   GUI Login and Welcome Banner Customization

When logged in to the Oracle Communications User Data Repository GUI as an administrator user, the *Options* page under *Administration* enables the administrative user to view a list of global options.

The *LoginMessage* field is the configurable portion of the login message seen on the login screen. The admin user can enter the message in this field as required. Similarly, the *WelcomeMessage* field can be used by the admin user to enter the message seen after successful login.

3.1.4   SSH Security Hardening Procedures

3.1.4.1   Set SSH Client Alive Count

Execute the below procedure for each and every server in the topology:

	Procedure 7.Set SSH Client Alive Count

1.	Log in as admusr on the server.
	
	`login: admusr`
	
	`Password: <current admin user password>`

2.	Check out the file `sshd_config` and grep for variable 'ClientAliveCountMax' in the file using below command:
	
	`$ sudo rcstool co /etc/ssh/sshd_config`
	
	`$ sudo grep^ClientAliveCountMax/etc/ssh/sshd_config`

3.	If no result is returned then execute below command:
	
	    `$ sudo echo "ClientAliveCountMax 0" >>`
	`/etc/ssh/sshd_config`
	
	If some result is returned by executing Step 2, the execute the below command:
	
	    `$ sudosed -i "s/ClientAliveCountMax.*/ClientAliveCountMax`
	`0/g"/etc/ssh/sshd_config`

4.	Check in the file `sshd_config`: `$ sudo rcstool ci/etc/ssh/sshd_config`

3.1.4.2   Disable SSH Access via Empty Passwords

Execute the below procedure for each and every server in the topology:

Procedure 8.Disable SSH Access via Empty Passwords	

1.	Log in as admusr on the server.
	
	    `login: admusr`
	
	    `Password: <current admin user password>`

2.	Check out the file `sshd_config` and grep for variable 'PermitEmptyPasswords' in the file using below command:
	
	    `$ sudo rcstool co /etc/ssh/sshd_config`
	
	    `$ sudo grep PermitEmptyPasswords/etc/ssh/sshd_config`

3.	If no result is returned then execute below command:
	
	    `$ sudo echo "PermitEmptyPasswords no" >>`
	`/etc/ssh/sshd_config`
	
	If some result is returned by executing Step 2, the execute the below command:
	
	    `$ sudo sed -i`
	`'/PermitEmptyPasswords/c\PermitEmptyPasswords no'`
	`/etc/ssh/sshd_config`

4.	Check in the file `sshd_config`: `$ sudo rcstool ci/etc/ssh/sshd_config`

3.1.4.3   Enable SSH Warning Banner

Execute the below procedure for each and every server in the topology:

Oracle Communications User Data Repository Security Guide

Procedure 9.Set SSH Warning Banner	

1.	Log in as admusr on the server.
	
	`login: admusr`
	
	`Password: <current admin user password>`

2.	Check out the file `sshd_config` and grep for variable 'Banner' in the file using below command:
	
	`$ sudo rcstool co /etc/ssh/sshd_config`
	
	`$sudo grep Banner/etc/ssh/sshd_config`

3.	If no result is returned then execute below command:
	
	`$ sudo echo "Banner /etc/issue" >> /etc/ssh/sshd_config`
	
	If some result is returned by executing Step 2, the execute the below command:
	
	`$ sudo sed -i '/Banner/c\Banner \/etc\/issue' /etc/ssh/sshd_config`

4.	Check in the file `sshd_config`: `$ sudo rcstool ci/etc/ssh/sshd_config`

3.1.4.4   Do not allow SSH Environment Options

Execute the below procedure for each and every server in the topology:

Procedure 10.Do not allow SSH Environment Options	

1.	Log in as admusr on the server.
	
	`login: admusr`
	
	`Password: <current admin user password>`

2.	Check out the file `sshd_config` and grep for variable 'PermitUserEnvironment' in the file using below command:
	
	`$ sudo rcstool co /etc/ssh/sshd_config`
	
	`$sudo grep PermitUserEnvironment/etc/ssh/sshd_config`

3.	If no result is returned then execute below command: `$ sudo echo "PermitUserEnvironment  no" >> /etc/ssh/sshd_config` If some result is returned by executing Step 2, the execute the below command:

Release 12.10   **21**   **August 2021**

| | ```
     $ sudo sed -i
'/PermitUserEnvironment/c\PermitUserEnvironment no'
/etc/ssh/sshd_config
``` |
| 4. | Check in the file `sshd_config`:<br><br>```
     $ sudo rcstool ci/etc/ssh/sshd_config
``` |

3.1.4.5   Generate passphraseprotected RSA SSH Key for 'admusr' User Account

Execute the below procedure to generate a passphraseprotected RSA SSH key for 'admusr' User Account.This procedure should be executed on each server in the topology. The order of execution in the topology should be from A -level servers to C -level servers.

Procedure 11.Generate passphraseprotected RSA SSH Key for 'admusr' User Account	
| 1. | Log in as admusr on the server.<br><br>```
     login: admusr

     Password: <current admin user password>
``` |
| 2. | Stop the apwSoapServer process :<br><br>```
     $ sudo pm.set off apwSoapServer
``` |
| 3. | Go to .ssh directory and remove the old DSA keys if they exist :<br><br>```
     $ cd /home/admusr/.ssh

     $ sudo rm —rf id_dsa id_dsa.pub
``` |
| 4. | Generate new RSA key using below command :<br><br>```
     $ ssh-keygen -t rsa -b 4096
```<br><br>You will be prompted to enter the location to save the key. Provide the desired location or it can be left blank. On leaving it blank, default location /home/admusr/.ssh/id_rsawill be used :<br><br>```
     $ Enter file in which to save the key
(/home/admusr/.ssh/id_rsa):
```<br><br>You will be prompted to enter the passphrase. Insert the passphrase :<br><br>```
     $ Enter passphrase (empty forno passphrase):
```<br><br>You will be asked to confirm the passphrase. Insert passphrase again :<br><br>```
     $ Enter same passphrase again:
```<br><br>A password protected RSA key will be generated successfully. |

Oracle Communications User Data Repository Security Guide

5.	Start the apwSoapServer process : `$ sudo pm.set onapwSoapServer`
6.	Wait for 60 seconds. Post 60 Seconds, server will use the generated RSA key.

After executing the procedure, any key based SSH login for 'admusr' accountwill be prompted for passphrase.Setting a passphrase on the key will affect the execution of procedures requiring ssh access using 'admusr' account where the user will be prompted to enter the passphrase for each ssh access.

3.1.4.6   Set SSH LogLevel to INFO
Execute the below procedure for each and every server in the topology:

Procedure 12.Set SSH LogLevel to INFO

1.	Log in as admusr on the server.
	
	    `login: admusr`
	
	    `Password: <current admin user password>`

2.	Check out the file `sshd_config`: `$ sudo rcstool co /etc/ssh/sshd_config`
3.	Execute the below command: `$ sudo sed -i '/LogLevel/c\LogLevel INFO' /etc/ssh/sshd_config`
4.	Check in the file `sshd_config`: `$ sudo rcstool ci/etc/ssh/sshd_config`

3.1.4.7   Enable SSH IgnoreRhosts
Execute the below procedure for each and every server in the topology:

Procedure 13.Enable SSH IgnoreRhosts

1.	Log in as admusr on the server.
	
	    `login: admusr`
	
	    `Password: <current admin user password>`

2.	Check out the file `sshd_config`: `$ sudo rcstool co /etc/ssh/sshd_config`

3.	Execute the below command:
	
	`    $ sudo sed -i '/IgnoreRhosts/c\IgnoreRhosts yes'`
	`/etc/ssh/sshd_config`

4.	Check in the file `sshd_config`: `    $ sudo rcstool ci/etc/ssh/sshd_config`

3.1.4.8   Disable SSH X11 Forwarding

Execute the below procedure for each and every server in the topology:

Procedure 14.Disable SSH X11 Forwarding	

1.	Log in as admusr on the server.
	
	`    login: admusr`
	
	`    Password: <current admin user password>`

2.	Check out the file `sshd_config`: `    $ sudo rcstool co /etc/ssh/sshd_config`

3.	Execute the below commands:
	
	`    $ sudo sed -i '/X11Forwarding yes/s/^/#/g'`
	`/etc/ssh/sshd_config`
	
	`    $ sudo sed -i '/X11Forwarding no/s/^#//g'`
	`/etc/ssh/sshd_config`

4.	Check inthe file `sshd_config`: `    $ sudo rcstool ci/etc/ssh/sshd_config`

3.1.4.9   Disable SSH HostbasedAuthentication

Execute the below procedure for each and every server in the topology:

Procedure 15.Disable SSH HostbasedAuthentication	

1.	Log in as admusr on the server.
	
	`    login: admusr`
	
	`    Password: <current admin user password>`

2.	Check out the file `sshd_config`: `    $ sudo rcstool co /etc/ssh/sshd_config`

3.	Execute the below commands:
	
	`    $ sudo sed -i '/HostbasedAuthentication no/s/^#//g'`
	`/etc/ssh/sshd_config`

4.	Check in the file `sshd_config`: `    $ sudo rcstool ci/etc/ssh/sshd_config`

3.1.4.10   Set SSH LoginGraceTime to 1m

Execute the below procedure for each and every server in the topology:

Procedure 16.Set SSH LoginGraceTime to 1m	

1.	Log in as admusr on the server.
	
	`    login: admusr`
	
	`    Password: <current admin user password>`

2.	Check out the file `sshd_config`: `    $ sudo rcstool co /etc/ssh/sshd_config`

3.	Execute the below commands:
	
	`    $ sudo sed -i '/LoginGraceTime/c\LoginGraceTime 60'`
	`/etc/ssh/sshd_config`

4.	Check in the file `sshd_config`: `    $ sudo rcstool ci/etc/ssh/sshd_config`

3.1.4.11   Disable diffie-hellman-group1-sha1 Key Exchange(Kex) algorithm

Execute the below procedure for each and every server in the topology:

Procedure 17.Disable diffie-hellman-group1-sha1 Key Exchange (Kex) algorithm	

1.	Log in as admusr on the server.
	
	`    login: admusr`
	
	`    Password: <current admin user password>`

2.	Check if "diffie-hellman-group1-sha1" key exchange algorithm is supported: ` $ sudo sshd -T	grep -i diffie-hellman-group1-sha1`
3.	If no result is returned, that means "diffie-hellman-group1-sha1" key exchange algorithm is already disabled and nothing is to be done –skip steps 4 and 5.

	Else, Check out the file `sshd_config`: `$ sudo rcstool co /etc/ssh/sshd_config`
4.	Execute the below commandto disable "diffie-hellman-group1-sha1" key exchange algorithm: `$ sudo sed -i '$ a KexAlgorithms diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1' /etc/ssh/sshd_config`
5.	Check in the file `sshd_config`: `$ sudo rcstool ci /etc/ssh/sshd_config`

3.1.5   Services Hardening Procedures

3.1.5.1   Uninstall tftp-server Package

Execute the below procedure for each and every server in the topology:

Procedure 18.Uninstall tftp-server Package	

1.	Log in as admusr on the server.
	
	    `login: admusr`
	
	    `Password: <current admin user password>`

2.	The tftp-server package can be removed with the following command: `$ sudo yum erase tftp-server`

3.1.5.2   Disable xinetd Service

Execute the below procedure for each and every server in the topology:

Procedure 19.Disable xinetd Service	

1.	Log in as admusr on the server.
	
	    `login: admusr`
	
	    `Password: <current admin user password>`

2.	Disable xinetd for all run levels and Stop xinetd if currently running: `$ sudo yum erase tftp-server`

```
$ sudo /sbin/service xinetd stop
```

This step might fail if the xinetd service is already disabled/stopped.

3.1.5.3   Uninstall xinetd Service

Execute the below procedure for each and every server in the topology:

Procedure 20.Uninstall xinetd Service

1.	Log in as admusr on the server.
	
	```login: admusr```
	
	```Password: <current admin user password>```

2.	Disable xinetd for all run levels and Stop xinetd if currently running: ```$ sudo yum erase xinetd```

3.1.5.4   Disable ntpdate Service

Execute the below procedure for each and every server in the topology:

Procedure 21.Disable ntpdate Service

1.	Log in as admusr on the server.
	
	```login: admusr```
	
	```Password: <current admin user password>```

2.	The ```ntpdate``` service can be disabled with the following command: ```$ sudo chkconfig ntpdate off```

3.1.6   SNMP Configuration

The application has an interface to retrieve KPIs and alarms from a remote location using the industry-standard Simple Network Management Protocol (SNMP) interface. Only the active Network OAM&P server allows SNMP administration. For more details, see the section *SNMP Trapping* in the [1] *Operations, Administration, and Maintenance (OAM) User's Guide* under the *Administration* chapter.

The Active Network OAM&P server provides a single interface to SNMP data for the entire network and individual servers interface directly with SNMP managers. The application sends SNMP traps to SNMP Managers that are registered to receive traps. IP addresses and authorization information can be viewed and changed using the *SNMP Trapping* page.

For SNMP to be enabled, at least one Manager must be set up. The system allows configuring up to five different Managers to receive SNMP traps and send requests. These could be either a valid IPv4 address or a valid hostname known to the system. The hostname must be unique and is case-insensitive. Up to 20 characters can be entered in the string. Valid

characters are alphanumeric and the minus sign. The hostname must start with an alphanumeric and end with an alphanumeric.

The *Enabled Versions* field in this page lets the user pick the version of SNMP. The traps can be enabled or disabled collectively or independently from individual servers by checking the traps enabled check box in this page.

The *SNMP Trapping* page provides the below functionalities:

- Add an SNMP Manager
- View SNMP settings
- Updating SNMP settings
- Delete SNMP manager

For more details on these actions, please refer to the [1] *Operations, Administration, and Maintenance (OAM) User's Guide.*

3.1.6.1   Selecting Versions

The *Enabled Versions* field in the SNMP Trapping page lets the user pick the version of SNMP. Options are:

- SNMPv2c: Allows SNMP service only to managers with SNMPv2c authentication.
- SNMPv3: Allows SNMP service only to managers with SNMPv3 authentication.
- SNMPv2c and SNMPv3: Allows SNMP service to managers with either SNMPv2c or SNMPv3 authentication. This is the default option.

The recommended option is SNMPv3 for secure operation.

3.1.6.2   Community Names / Strings

When the SNMPv2c is enabled in the *Enabled Versions* field, the SNMPV2c Community Name is a required field. This is the configured Community Name. This string can be optionally changed. The maximum length of the Community Name (String) is 31 characters. It is recommended that customers use unique, hard to guess Community Name values and that they avoid using well known Community Names like "public" and "private".

3.1.7   SNMPv3 on PMAC

3.1.7.1   Enable SNMPv3 Support on PMAC

There are a set of procedures and sub-procedures required to enable overall SNMPv3 protocol support on the PMAC system. There are multiple PMAC Procedures required to complete this:

- Updating the SNMP service on existing remote servers on the PMAC control network.

- Updating the SNMP service on the PMACserver service to support SNMPv3.

- Updating the PMAC messaging system to support SNMPv3.

- Updating the SNMPv3 Security settings.

For more detailed steps on performing these methods, refer to Appendix S in [6] PMAC Configuration Guide.

3.1.7.2 Configure SNMPv3 Security Model and Trap Servers

This procedure configures SNMP Version 3 security model and trap servers. This SNMPv3 support is only for HP 6125G/XLG and Cisco 4948E/E-F switches. For more detailed steps on performing these methods, refer to Procedure 18 & Procedure 19 in [6]PMAC Configuration Guide.

3.1.8 Authorized IPs

IP addresses that have permission to access the GUI can be added or deleted on the *Authorized IPs* page. If a connection is attempted from an IP address that does not have permission to access the GUI, a notification appears on the GUI and access is not granted from that IP address. This feature cannot be enabled until the IP address of the client is added to the authorized IP address table. You must add the IP address of your own client to the list of authorized IPs first before you enable this feature.

Enabling Authorized IPs functionality prevents unauthorized IP addresses from accessing the GUI. See the [1] *Operations, Administration, and Maintenance (OAM) User's Guide, Authorized IPs* section for more details on how to enable this feature.

3.1.9 Enabling IPsec

Internet Protocol Security (IPsec) provides network layer security protocols used for authentication, encryption, payload compression, and key exchange. IPsec provides Host-to-Host encrypted connections or Network-to-Network packet tunneling.

Network traffic between two end-points is encrypted and decrypted by authenticated hosts at the end-points, using a shared private key. The shared private key forms a Security Association that can be automatically changed by Security Policies based on traffic volume, expiry time, or other criteria.

IPsec will work for both IPv4 and IPv6 addresses. Oracle Communications User Data Repository IPsec uses the Encapsulating Security Payload (ESP) protocol for encryption and authentication. ESP also provides authentication of the encrypted packets to prevent attacks by ensuring the packet is from the correct source.

Internet Key Exchange (IKE) is used to exchange secure keys to set up IPsec security associations. See Section 3.7 "*Optional IPsec Configuration*" for more details on how to enable IPsec.

3.1.10 Certificate Management

The Certificate Management feature allows the user to configure digital security certificates for securing Oracle Communications User Data Repository web sessions, user authentication thru secure LDAP over TLS, and secure Single Sign-On authentication across a defined zone of Oracle Communications User Data Repository servers. The feature supports certificates based on host name or fully qualified host name.

This feature allows users to build certificate signing requests (CSRs) for signing by a known certificate authority and importing into the Oracle Communications User Data Repository. This feature lets the user generate a Certificate Report of individual or all defined certificates.

For details on Certificate Management feature see Certificate Management chapter in [1] *Operations, Administration, and Maintenance (OAM) User's Guide.*

3.1.11 SFTP Administration

 Oracle Communications User Data Repository supports SFTP sessions with external servers for transfer of various files from Oracle Communications User Data Repository. The authentication process requires a digital certificate for authenticating the sessions.

Oracle Communications User Data Repository Security Guide

The transfer of files is driven from the external server. Please see section *SFTP Users Administration* in [1] *Operations, Administration, and Maintenance (OAM) User's Guide*.

3.1.12 Remote Import/Export

Oracle Communications User Data Repository supports transferring import and export files over secure channels (rsync over SSH) to/from a user configured server. The customer configures whether they want the remote import and/or remote export features enabled, remote host's IP address, user name, import directory and export directory, and performs SSH Key Exchanges between the primary NOAMP server and the remote host server.

The transfer of files is driven from the primary NOAMP server. For more information regarding the configuration options, please see *Provisioning Options* in [4] *Enhanced Subscriber Profile Repository User's Guide*.

3.1.13 Command Log Export

Oracle Communications User Data Repository supports exporting provisioning command logs and transferring the exported logs to a remote server on a regular basis while the feature is enabled. The command log export is enabled and disabled using *Main Menu: UDR → Configuration → Command Log Export Options* GUI screen. When enabled, a log file is generated every time the export is triggered and is transferred to the remote command log export host server over secure channels (scp over SSH) to a user configured server. The customer configures the remote command log export host's IP address, user name, export directory, and performs SSH Key Exchanges between the primary NOAMP server and the remote command log export host server.

The transfer of files is driven from the primary NOAMP server. For more information regarding the configuration options, please see *Provisioning Options* in [4] *Enhanced Subscriber Profile Repository User's Guide*.

3.1.14 Provisioning Security

The Oracle Communications User Data Repository provisioning interface supports both SOAP and REST interfaces. Only IP addresses that are configured by the user in the Provisioning Connections Whitelist are allowed to connect to the primary provisioning site's NOAMP server and execute commands. Please see *Provisioning Connections* in [4] *Enhanced Subscriber Profile Repository User's Guide* for more information.

The customer also configures what type of provisioning interfaces are enabled – SOAP and/or REST. The customer can also configure whether the REST interface runs in secure mode (using TLS) or unsecure mode (plain text). The customer can also configure whether the SOAP interface runs in secure mode (using TLS) or unsecure mode (plain text). For more information regarding the configuration options, please see Provisioning Options in [4] Enhanced Subscriber Profile Repository User's Guide.

The secure REST interface uses SSL certificates and public/private key pairs as described in [5] *REST Provisioning Interface Specification*. These REST certificates are not certified.

The secure SOAP interface also uses SSL certificates and public/private key pairs as described in [7] *SOAP Provisioning Interface Specification*. These SOAP certificates are not certified

For both REST and SOAP provisioning interfaces, the customer can configure their IP address to use Internet Protocol Security (IPsec) to provide secure connections. For more information regarding IPsec, please see section 3.7 "*Optional IPsec Configuration*".

Oracle Communications User Data Repository supports authentication of the username and password received in the header of the SOAP request to validate the identity of the user who generated the request when the *SOAP Username/Password Authentication* feature is enabled. Any requests that do not match valid users shall be rejected. The username/password provided in the SOAP Header will be ignored when the *SOAP Username/Password Authentication* feature is disabled and the

request will be processed. The *SOAP Username/Password Authentication* feature can be enabled and disabled on the *Main Menu: UDR -> Configuration -> Provisioning Options* GUI screen. When this authentication feature is enabled, the customer should use IPSec provisioning connections to encrypt the user names and passwords on the incoming connections, as described in section 3.7. For more information regarding storing the username and password in the SOAP Header, please see [7] *SOAP Provisioning Interface Specification*.

3.1.15 Security for Pools Spanning Oracle Communications User Data Repository systems

Oracle Communications User Data Repository allows customers to provision subscribers that are members of a pool that is stored on a different Oracle Communications User Data Repository system within the customer's network. This feature is called Pools Spanning Oracle Communications User Data Repository (PSO). To use the PSO feature, the customer must configure a unique UDR Name and unique UDR ID for each Oracle Communications User Data Repository system on the customer's network. These unique UDR Name/UDR ID combinations must be configured identically across all Oracle Communications User Data Repository systems on the customer's network.

On every Oracle Communications User Data Repository system in the customer's network that uses the PSO feature, the customer must also configure Communication Agent connections to each of the remote Oracle Communications User Data Repository NOAMP servers by using the *Main Menu: UDR → Communication Agent → Configuration → Remote Servers* GUI screen. This information includes unique remote server name, remote server IP address, remote server mode (always set to "server"), and NOAMP server groups to connect to the remote server. The user must select the NOAMP server groups from both the primary site and the possible geo-redundant site. So, if the remote Oracle Communications User Data Repository contains 4 NOAMP servers, 4 entries must be added on the local host.

The customer can configure their NOAMP IP addresses to use Internet Protocol Security (IPsec) to provide secure connections. For more information regarding IPsec, please see section 3.7 "*Optional IPsec Configuration*".

3.1.16 Ud Client

Oracle Communications User Data Repository Ud Client feature supports having an LDAP and a SOAP interface to communicate with an external Ud Server to retrieve subscriber profile data to populate Oracle Communication User Data Repository's (UDR) subscriber Profile. Ud Client is essentially a gateway into an Ud Server where subscriber data is stored and mastered. The Ud Client feature allows UDR access to externally stored subscriber data so that it can provide it to other network elements such as PCRF. Operations requiring this data are transparent; the data is presented as if it were stored and managed by UDR.

Oracle Communication User Data Repository's Ud Client has two interfaces: LDAP and SOAP. LDAP is used for reading subscriber profile data, and SOAP is used for the publish/subscribe interface to be notified when requested subscriber data is changed.

The Ud client interface on the NOAMP can be configured into either the XSI or XMI network, depending on accessibility and connectivity to the centralized database that hosts the Ud server interface.On every Oracle Communications User Data Repository system in the customer's network that uses the Ud Client feature, the customer must enable the Ud Client feature, configure if the Ud SOAP interface is enabled and configure whether or not to send SOAP Subscribe requests on the *Main Menu: UDR -> Configuration -> Ud Client -> Ud Client Options* GUI screen. The customer must also configure all of the LDAP and SOAP Hosts' IP addresses, Ports and Type (WAN/LAN) on the *Main Menu: UDR -> Configuration -> Ud Client -> Ud Remote Server* GUI screen.

The customer can configure their NOAMP IP addresses to use Internet Protocol Security (IPsec) to provide secure connections. For more information regarding IPsec, please see section 3.7 "*Optional IPsec Configuration*".

3.2   Host Intrusion Detection System (HIDS)

This section explains the Host Intrusion Detection System (HIDS) security feature available to the Platform Administrator through the Linux Command Line Interface (CLI). The platcfg utility of the OS is used for configuring this feature.

3.2.1   Host Intrusion Detection System (HIDS) overview

The Host Intrusion Detection System (HIDS) feature monitors a server for malicious activity by periodically examining file system changes, logs, and monitoring auditing processes. The HIDS feature monitors TPD and TVOE log files, and ensures that HIDS and syscheck processes are running. For maximum effectiveness, the HIDS feature should be enabled on all NOAMP, SOAM and MP servers/VMs, as well all virtual hosts (TVOE servers).

The files that are considered to be protected log files and are therefore monitored by the HIDS monitoring feature are:
- All files in /var/TKLC/log/hids
- /var/log/messages
- /var/log/secure
- /var/log/cron

The log files created are:
- alarms.log – Any HIDS functionality that will result in an alarm being raised or cleared will be logged here (i.e. file tampering alarm, Syscheck process alarm, Samhain process alarm)
- admin.log – Any HIDS command executed will have the output logged here either for successful or errored commands. This includes attempts to run commands as a non HIDS administrator.
- hids.log – Logs any other information such as state changes and when Samhain runs but doesn't find any file tampering errors.

No other system resources (files, processes, actions, etc) are monitored by HIDS.

HIDS alarms are standard TPD alarms with the alarmEventType set to **securityServiceOrMechanismViolation**. The HIDS alarms are propagated through normal COMCOL channels ultimately resulting in SNMP traps being sent to the customer's SNMP management system, if configured. Customers can view active alarms in the platcfg GUI as shown in Figure 6. Platcfg Alarm Screen. The Customers can view active alarms on the Oracle Communications User Data Repository GUI on the *Main Menu: Alarms & Events -> View Active* GUI screen as shown in Figure 4. UDR View Active Alarm Screen and Figure 5. UDR View Active Alarm Report Screen.

3.2.2   Determine Host Intrusion Detection System (HIDS) Status

The HIDS status for the server is displayed along the top of the HIDS menu window.

1. Log in as **admusr** on the server

    Login: admusr
    Password: <current admin user password>

2. Open the platcfg menu by entering the following command.

    $sudo su - platcfg

3. Select **Security** from the menu and press **Enter**.

4. Select **HIDS** from the menu and press **Enter**.

5. Enter the **Username** and **Password** for a user that is part of the **secgrp** group. (Note: By default, **admusr** is part of the **secgrp** group.)

6. The HIDS menu will be displayed and the HIDS Monitoring State is listed on the top of the window, as illustrated below:

```
HIDS Monitoring State: CONFIGURED Menu
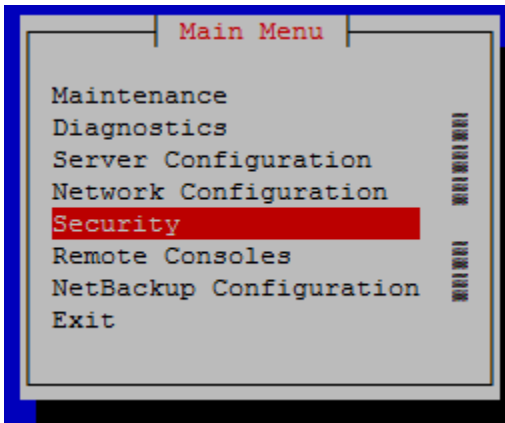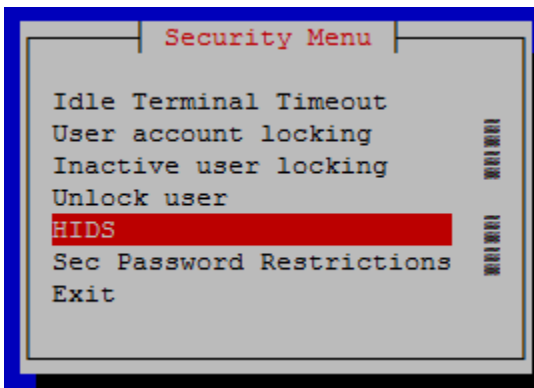
            Initialize
            Delete
            Enable/Disable
            Suspend/Resume
            On-demand
            Update
            Exit
```

7. Select **Exit** in each of the menus until a command prompt is reached.

3.2.3   Initialize Host Intrusion Detection System (HIDS)

The Host Intrusion Detection System (HIDS) feature must be initialized prior to enabling HIDS for the first time on a system.

8. Log in as **admusr** on the server

   Login: admusr
   Password: <current admin user password>

9. Open the platcfg menu by entering the following command.

   $ sudo su - platcfg

10. Select **Security** from the menu and press **Enter**.

```
                Main Menu
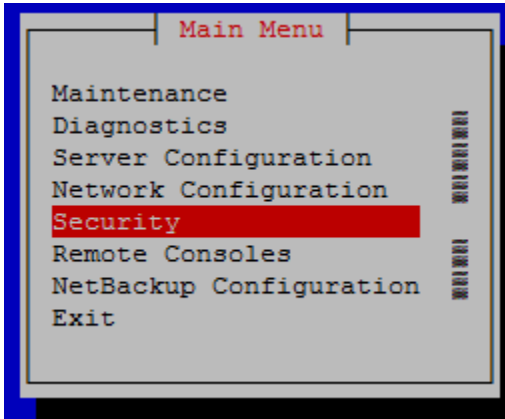
        Maintenance
        Diagnostics
        Server Configuration
        Network Configuration
        Security
        Remote Consoles
        NetBackup Configuration
        Exit
```

11. Select **HIDS** from the menu and press **Enter**.

12. Enter the **Username** and **Password** for a user that is part of the **secgrp** group. (Note: By default, **admusr** is part of the **secgrp** group.)

13. Select **Initialize** and press **Enter**.

14. Select **Yes** and press **Enter.**

15. After the message box that says "HIDS baseline successfully initialized" appears, press any key to continue.

16. Select **Exit** in each of the menus until a command prompt is reached.

3.2.4   Enable or Disable Host Intrusion Detection System (HIDS)

The Host Intrusion Detection System (HIDS) feature must be initialized prior to enabling HIDS for the first time on a system.

17. Log in as **admusr** on the server

   Login: admusr

Oracle Communications User Data Repository Security Guide

Password: <current admin user password>

18. Open the platcfg menu by entering the following command.

    $ sudo su - platcfg

19. Select **Security** from the menu and press **Enter**.

20. Select **HIDS** from the menu and press **Enter**.

21. Enter the **Username** and **Password** for a user that is part of the **secgrp** group. (Note: By default, **admusr** is part of the **secgrp** group.)

22. Select **OK** and press **Enter.**

23. Select **Enable/Disable** and press **Enter**.

Release 12.10   **36**   **August 2021**

24. Select either the **Enable** or **Disable** option.

25. Select **OK** and press **Enter.**

26. After the message box that indicates that DB monitoring has been enabled/disabled or a failure message appears, press any key to continue.

27. Select **Exit** in each of the menus until a command prompt is reached.

3.2.5   Suspend or Resume Host Intrusion Detection System (HIDS)

The HIDS monitoring can temporarily by suspended or resumed on a system that has HIDS enabled.

28. Log in as **admusr** on the server

    Login: admusr
    Password: <current admin user password>

29. Open the platcfg menu by entering the following command.

    $ sudo su - platcfg

30. Select **Security** from the menu and press **Enter**.

31. Select **HIDS** from the menu and press **Enter**.

32. Enter the **Username** and **Password** for a user that is part of the **secgrp** group. (Note: By default, **admusr** is part of the **secgrp** group.)

33. Select **OK** and press **Enter.**
34. Select **Suspend/Resume** and press **Enter**.

35. Select either the **Suspend** or **Resume** option.

36. Select **OK** and press **Enter.**

37. After the message box that indicates that DB monitoring has been suspended/resumed or a failure message appears, press any key to continue.

38. Select **Exit** in each of the menus until a command prompt is reached.

3.2.6   Run On-Demand Host Intrusion Detection System (HIDS) Security Check

The HIDS tests run periodically. A user can force an immediate run of the HIDS tests by using the **On-demand** HIDS menu.

39. Log in as **admusr** on the server

   Login: admusr
   Password: <current admin user password>

40. Open the platcfg menu by entering the following command.

   $ sudo su - platcfg

41. Select **Security** from the menu and press **Enter**.

42. Select **HIDS** from the menu and press **Enter**.

43. Enter the **Username** and **Password** for a user that is part of the **secgrp** group. (Note: By default, **admusr** is part of the **secgrp** group.)

44. Select **On-demand** and press **Enter**.

45. Select **Yes** and press **Enter.**

46. After the message box that indicates the success/fail result appears, press any key to continue. If an error exists, a screen similar to the below screen will be displayed:

Note: This alarm can also been seen when viewing alarms in the platcfg system, as described in section 3.2.9: View Host Intrusion Detection System (HIDS) Alarms, and shown in Figure 6. Platcfg Alarm Screen.

Note 2: This alarm is also propagated through normal COMCOL channels ultimately resulting in the alarm being accessible on the Oracle Communications User Data Repository's GUI in the Main Menu: Alarm & Events -> View Active GUI screen, as shown in step 48.

47. Select **Exit** in each of the menus until a command prompt is reached.

48. (Optional) Log onto Oracle Communications User Data Repository GUI and open the Main Menu: Alarms & Events -> View Active GUI screen to view details for the HIDS error. Examples of screens from the current error are listed below:

Figure 4. UDR View Active Alarm Screen

Oracle Communications User Data Repository Security Guide

Main Menu: Alarms & Events -> View Active

Filter* ▼   Tasks ▼   Graph* ▼

NO_SG   SO_SG

Seq #	Event ID	Timestamp	Severity	Product	Process	NE	Server	Type	Instance
	Alarm Text		**Additional Info**						
97	32349	2016-06-02 14:52:04.063 EDT	**MAJOR**	TPD	cmplat alarm	SO_UDR	pc9112032-so-a	PLAT	
	File Tampering		GN_WARNING/WRN Platform detected an error condition [cmplatalarm.cxx:194] ... More...						
17	10300	2016-05-30 15:55:58.567 EDT	**MINOR**	OAM	audit	SO_UDR	pc9112032-so-a	DB	
	SNMP Trapping Not Configured		No SNMP trap configuration found for this site!						

Figure 5. UDR View Active Alarm Report Screen

3.2.7   Update Host Intrusion Detection System (HIDS) Baseline

The HIDS **Update** menu is used to update the checksums on all files or specific files in the HIDS baseline, which can clear HIDS alarms associated with the updated files.

49. Log in as **admusr** on the server

Login: admusr
Password: <current admin user password>

50. Open the platcfg menu by entering the following command.

$ sudo su - platcfg

51. Select **Security** from the menu and press **Enter**.

52. Select **HIDS** from the menu and press **Enter**.

53. Enter the **Username** and **Password** for a user that is part of the **secgrp** group. (Note: By default, **admusr** is part of the **secgrp** group.)

54. Select **OK** and press **Enter.**

55. Select **Update** and press **Enter**.

56. Select file's baseline to update.

57. Select **OK** and press **Enter.**

58. After the message box that indicates the success/fail result appears, press any key to continue.

59. Select **Exit** in each of the menus until a command prompt is reached.

3.2.8   Delete Host Intrusion Detection System (HIDS) Baseline

The HIDS **Delete** menu can be used for permanently disabling HIDS or for backing out of a product upgrade.

60. Log in as **admusr** on the server

   Login: admusr
   Password: <current admin user password>

61. Open the platcfg menu by entering the following command.

   $ sudo su - platcfg

62. Select **Security** from the menu and press **Enter**.

63. Select **HIDS** from the menu and press **Enter**.

```
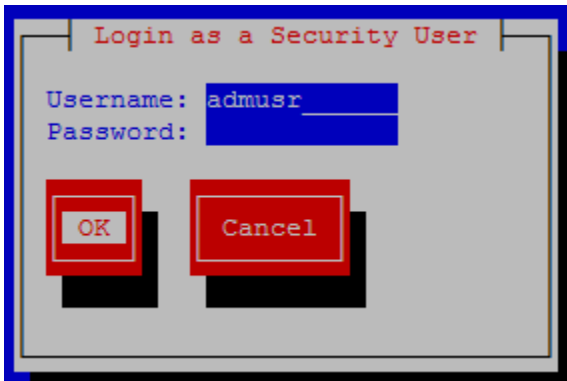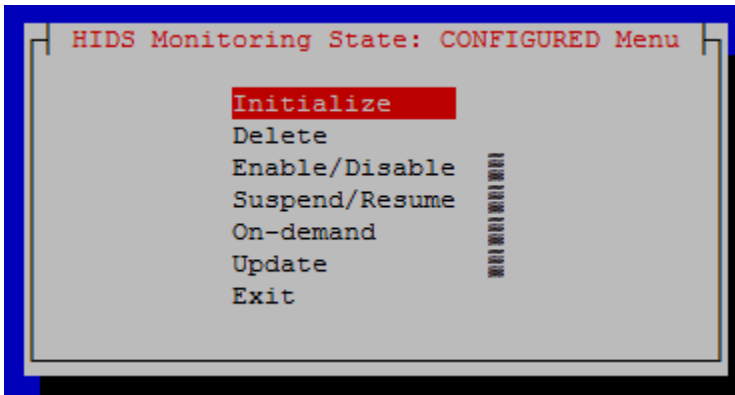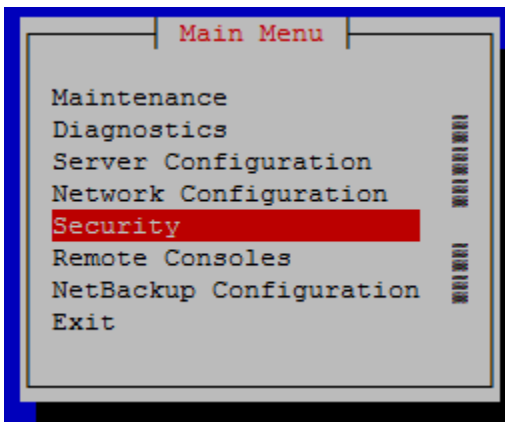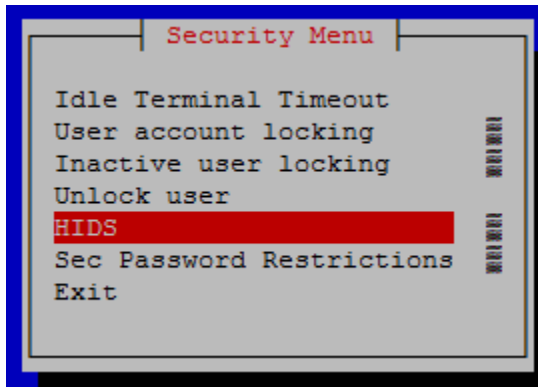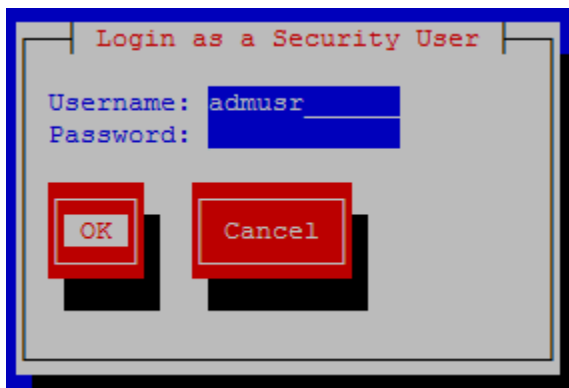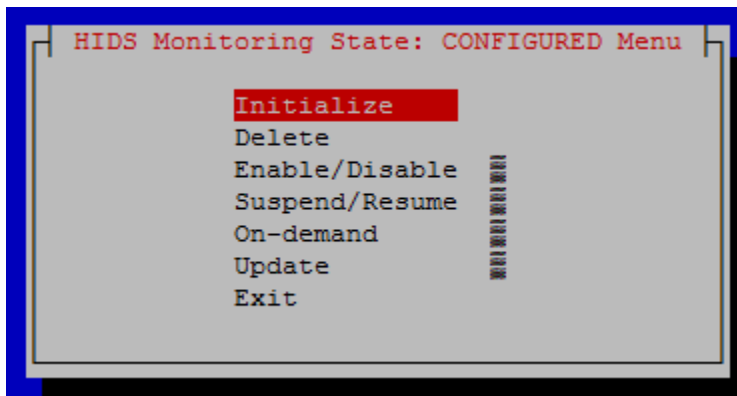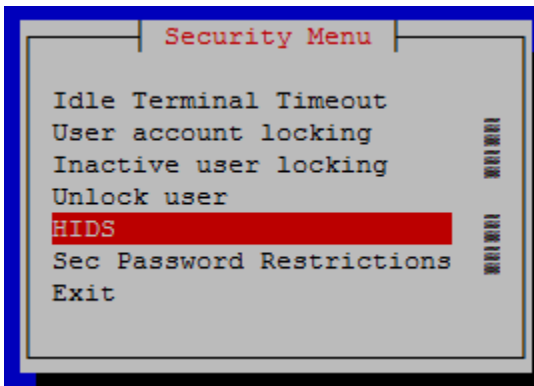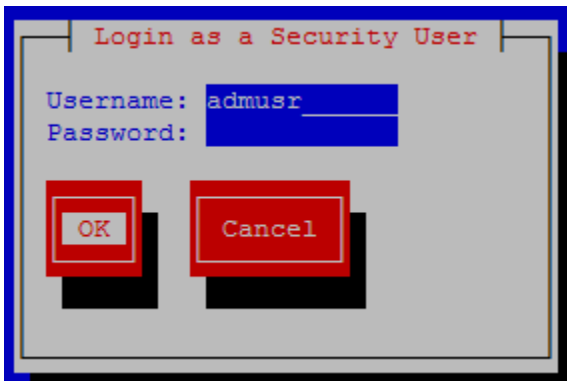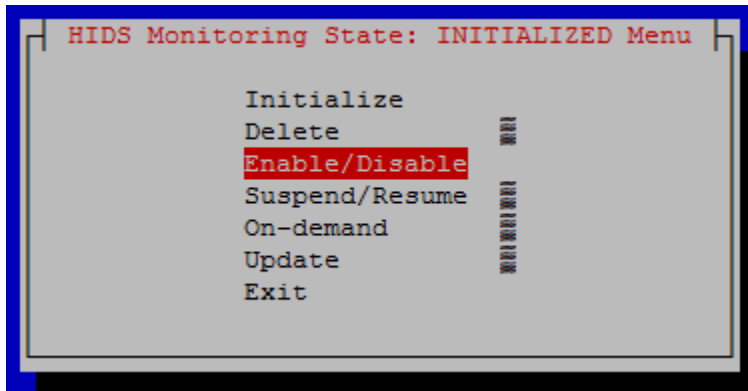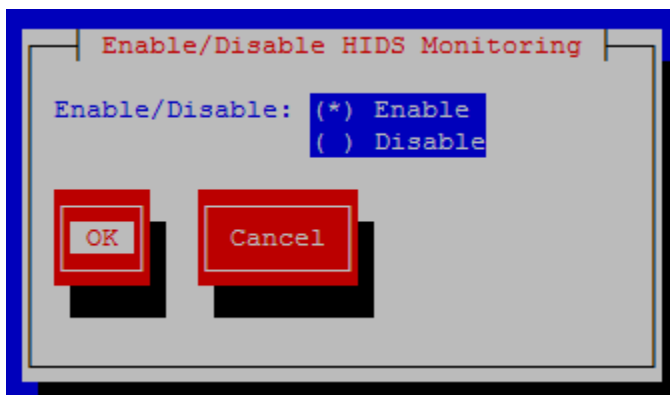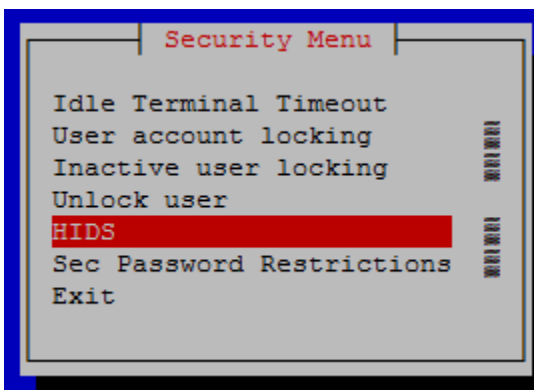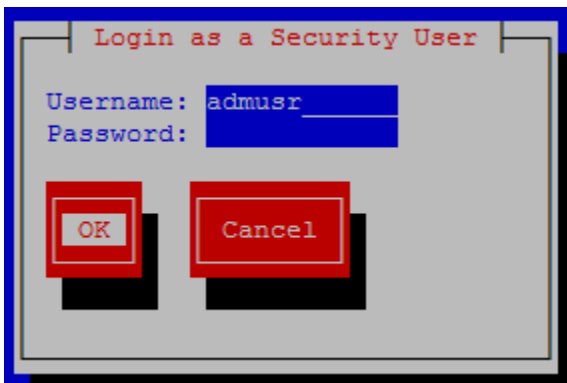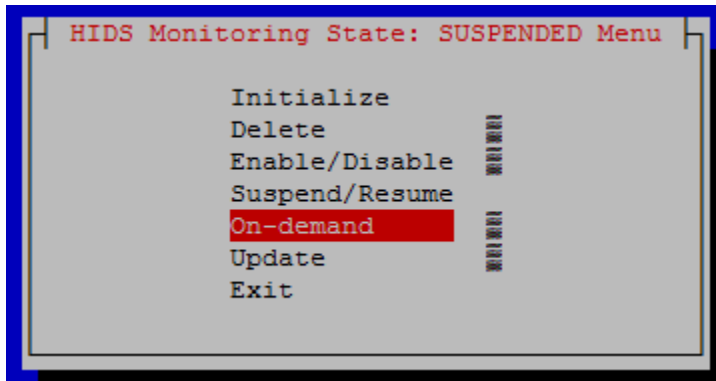┌────┤ Security Menu ├────┐
│                         │
│  Idle Terminal Timeout  │
│  User account locking   ▓│
│  Inactive user locking  ▓│
│  Unlock user            │
│  HIDS                   ▓│
│  Sec Password Restrictions ▓│
│  Exit                   │
│                         │
│                         │
└─────────────────────────┘
```

64. Enter the **Username** and **Password** for a user that is part of the **secgrp** group. (Note: By default, **admusr** is part of the **secgrp** group.)

```
┌────┤ Login as a Security User ├────┐
│                                     │
│  Username: admusr_____             │
│  Password:                          │
│                                     │
│   ┌──────┐      ┌──────────┐        │
│   │  OK  │      │  Cancel  │        │
│   └──────┘      └──────────┘        │
│                                     │
│                                     │
└─────────────────────────────────────┘
```

65. Select **OK** and press **Enter.**

66. Select **Delete** and press **Enter**.

```
┌─┤ HIDS Monitoring State: SUSPENDED Menu ├─┐
│                                            │
│              Initialize                    │
│              Delete              ▓│
│              Enable/Disable                │
│              Suspend/Resume        ▓│
│              On-demand              │
│              Update                 ▓│
│              Exit                   │
│                                            │
└────────────────────────────────────────────┘
```

67. Select **Yes** and press **Enter.**

68. After the message box that indicates the success/fail result appears, press any key to continue.

69. Select **Exit** in each of the menus until a command prompt is reached.

3.2.9   View Host Intrusion Detection System (HIDS) Alarms

HIDS alarms can be viewed using multiple methods. HIDS alarms are standard TPD alarms with the alarmEventType set to **securityServiceOrMechanismViolation**. The HIDS alarms are propagated through normal COMCOL channels ultimately

resulting in SNMP traps being sent to the customer's SNMP management system, if configured. The multiple ways to view the alarms include:

- Customers can view current, previously cleared, and how alarms were cleared in the /var/TKLC/logs/hids/alarms.log file.

- Customers can view active alarms on the Oracle Communications User Data Repository GUI on the *Main Menu: Alarms & Events -> View Active* GUI screen as shown in Figure 4. UDR View Active Alarm Screen and Figure 5. UDR View Active Alarm Report Screen.

- Customers can view active active alarms on the platcfg GUI, including HIDS alarms, by using the below steps:

  70. Log in as **admusr** on the server

     Login: admusr
     Password: <current admin user password>

  71. Open the platcfg menu by entering the following command.

     $ sudo su - platcfg

  72. Select **Diagnostics** from the menu and press **Enter**.

  73. Select **Alarm Manager** from the menu and press **Enter**.

  74. Select **Show Alarm Status** from the menu and press **Enter**.

75. After the message box that indicates the success/fail result appears, press any key to continue. If an error exists, a screen similar to the below screen will be displayed:

Figure 6. Platcfg Alarm Screen

76. Select **Exit** in each of the menus until a command prompt is reached.

3.3   Oracle Communications User Data Repository OS Standard Features

This section explains the security features of Oracle Communications User Data Repository available to the Platform Administrator through the Linux Command Line Interface (CLI). The platcfg utility of the OS is used for configuring these features.

3.3.1   Configure Password Expiry for OS Users

Use the below procedure to configure password expiry:

1. Log in as **admusr** on the server

    Login: admusr
    Password: <current admin user password>

2. Open the platcfg menu by entering the following command.

    $ sudo su - platcfg

3. Select **Security** from the menu and press **Enter**.

4. Fill out the following settings:

   Maximum number of days a password may be used: 99999

 5. Select **OK** and press **Enter.**

 6. Select **Exit** in each of the menus until a command prompt is reached.

3.3.2 Configuring minimum time before OS password can be changed

Procedure to configure minimum time before password can be changed:

 7. Log in as **admusr** on the server

   Login: admusr
   Password: <current admin user password>

 8. Open the platcfg menu by entering the following command.

   $ sudo su - platcfg

 9. Select **Security** from the menu and press **Enter**.

 10. From the menu select **Sec Password Restrictions** option

 11. Select **Global Password Restrictions for New Users**.

 12. Fill out the following settings:

   Minimum number of days allowed between password changes: 0

 13. Select **OK** and press **Enter.**

 14. Select **Exit** in each of the menus until a command prompt is reached.

3.3.3 Configuring Password Length for OS Users

Procedure to configure password length:

 1. Log in as **admusr** on the server

   Login: admusr
   Password: <current admin user password>

 2. Open the platcfg menu by entering the following command.

   $ sudo su - platcfg

 3. Select **Security** from the menu and press **Enter**.

 4. From the menu select **Sec Password Restrictions** option

 5. Select **Global Password Restrictions for New Users**. And in the menu displayed, fill out the field *Minimum acceptable size for the new password*. Select **OK** and press **Enter**

 6. Select exit in each of the menus until a command prompt is reached.

3.3.4 Configuring Session Inactivity for OS users

This procedure sets the idle time allowed before a session times out for OS users.

 1. Log in as **admusr** on the server

   Login: admusr
   Password: <current admin user password>

 2. Open the platcfg menu by entering the following command.

   $ sudo su – platcfg

3.   Select **Security** from the menu and press **Enter**.

4.   Select **Idle Terminal Timeout** option in the security menu and enter the desired value in minutes for the *Idle Terminal Timeout* field.

5.   Select **OK** and press **Enter.**

6.   Select **Exit** in each of the menus until a command prompt is reached.

3.3.5   Locking OS user accounts after a specified number of failed login attempts

This procedure sets the number of failed login attempts allowed before locking OS user accounts.

1.   Log in as admin user on the server

   login: admusr
   Password: <current admin user password>

2.   Open the platcfg menu by entering the following command.

   $ sudo su - platcfg

3.   Select **Security** from the menu and press **Enter**.

4.   Select **User account Locking** from the menu and press **Enter**

5.   Fill out the following settings:

   Feature: ( ) disable (*) enable
   Deny after # of attempts: <max tries>
   Fail interval in minutes: <interval minutes>
   Unlock time in minutes: <unlock time>

6.   Select **OK** and press **Enter.**

7.   Select **Exit** in each of the menus until a command prompt is reached.

3.4   Other Optional Configurations

The features explained in this section do not provide a GUI. This requires the administrator to issue the Linux commands provided in the instructions.

3.4.1   Changing OS User Account Passwords

All OS accounts that need to change the respective default passwords shall use the following procedure.

Procedure to Change Default Passwords

1.   Log in as **admusr** on the source server.

   login: admusr
   Password: <current admin user password>

2.   Change the passwords for each of the accounts being changed:

   $ sudo passwd <user account>
   Changing password for user <user account>.
   New UNIX password: <new password - will not display>
   Retype new UNIX password: <new password - will not display>
   passwd: all authentication tokens updated successfully.

3.   Repeat step 2 for all accounts that are being changed.

3.4.2   Changing Login Display Message

1. Use this procedure to change the Login Display Message.Log in as **admusr** on the source server.

    login: admusr
    Password: <current admin user password>

2. Create a backup copy of sshd_config

    $ sudo cd /etc/ssh
    $ sudo cp sshd_config sshd_config.bak

3. Edit the sshd configuration file.

    $ sudo rcstool co sshd_config
    $ sudo vi sshd_config

    Uncomment and edit the following line:

    $ Banner /some/path

    To this:

    Banner /etc/ssh/sshd-banner

    Save and exit the *vi* session.

4. Edit the banner file.

    $ sudo vi sshd-banner

    Add and format the desired text. Save and exit the *vi* session

5. Restart the sshd service.

    $ sudo service sshd restart

6. Test the change. Repeat steps 4 & 5 until the message is formatted correctly.

    $ sudo ssh <current server name>

    Verify message line feeds are formatted correctly.

    $ exit

7. Check the files into rcs to preserve changes during upgrades

    $ sudo rcstool init /etc/ssh/sshd-banner
    $ sudo rcstool ci sshd_config

3.4.3   Setting Up rsyslog for External Logging

1. Use this procedure to set up rsyslog for external logging to a central server from NOAMs and SOAMs. Log in as admin user on the server:

    login: admusr
    Password: <current admin user password>

2. Enable remote logging:

    $sudo syslog_config --remote=<IP of remote host to log to>

3. Repeat on all necessary NOAMs and SOAMs

Note: The following restrictions exist:

- Only OS level log events will be forwarded, such as /var/log/messages and /var/log/secure content
- Application level logging is not included and should be accessed through the *Main Menu: Administration -> Remote Servers -> Data Export* GUI screen
- Remote logging is over a non-secure communication channel that is not encrypted

3.4.4   Adding Sudo Users

Privileged operations by new OS users can be accomplished through a configuration of the "sudo" capability. The configuration supports very granular authorization to an individual OS user for certain desired commands.
The syntax of the configuration file can be somewhat tedious and editing mistakes could leave a system without needed access. For this reason, details of the configuration rules are available through Oracle Technical Network (OTN) or by opening a ticket with Oracle technical support.

3.4.5   Reporting and Disabling Expired OS User Accounts

Procedure to Report and Disable Expired User Accounts

1. Log in as admin user on the source server.

   login: admusr
   Password: <current admin user password>

2. Run the report of expired users.

   $ sudo lastlog -b <N>

   Note: This command will display the users who have not logged in over N number of days. It will also show the users that have never logged in. To filter those users out of the display use the following command:

   $ sudo lastlog -b <N> | grep -v Never

3. Disable the user accounts identified by the lastlog report

   $ sudo passwd -l <user acct>

   Repeat this step for each user account you want to disable.

4. To re-enable an account:

   $ sudo passwd -u <user acct>

   Repeat this step for each user account you want to re-enable.

3.5   Ethernet Switch Considerations

This section describes security related configuration changes that could be made to the demarcation Ethernet switches.

3.5.1   Configuring SNMP in Switches

It is essential that all switches have been configured successfully using the procedures in [3] *Installation and Configuration Guide*:

- Configure Cisco 3020 switch (netConfig) and/or
- Configure HP 6120XG switch (netConfig) and/or
- Configure Cisco 4948/4948E/4948E-F (netConfig)
1. Log in to the server as root user and list all the configured switches using the below command.

 # netConfig --repo listDevices

2. Refer to application documentation to determine which switches to add/remove the community string, making a note of the DEVICE NAME of each switch. This will be used as <switch_name>.

3. For any given switch by switch name, display SNMP community information using the below command:

 # netConfig getSNMP --device=<switch_name>

4. For any given switch by switch name, display its SNMP trap information using the below command

#netConfig listSNMPNotify --device=<switch_name>

Note: If the reply indicates "Could not lock device", enter the following command to clear the lock in order to proceed:

 # netConfig --wipe --device=<switch_name>

(reply "y" if prompted)

3.5.2   Configuring Community Strings

1. To ADD a community string to ANY switch by switch name, use below command with appropriate switch name

#netConfig addsSNMP –device=<switch name> community=<community string> uauth=RO

2. To DELETE a community string to ANY switch by switch name, use appropriate switch name in the below command

#netConfig deleteSNMP --device=<switch_name> community=<community_string>

3.5.3   Configuring Traps

1. To ADD a trap server, use below command with appropriate switch name:

#netConfig addSNMPNotify --device=<switch_name> host=<snmp_server_ip> version=2c auth=<community_string> [traplvl=not-info]

2. To DELETE a trap server, use the below command with appropriate switch name:

#netConfig deleteSNMPNotify --device=<switch_name> host=<snmp_server_ip> version=2c auth=<community_string> [traplvl=not-info]

Note: traplvl=not-info in the command is needed only in case of the 6120 switch. The switches 4948 or 3020 do not need this field in the above commands.

3.6   Security Logs and Alarms

The *Security Log* page in the GUI allows you to view the application historical security logs from all configured Security logs that are displayed in a scrollable, optionally filterable table. The security logs can also be exported to file management area in .csv format. For more details, see the *Security Log* chapter in [1] *Operations, Administration, and Maintenance (OAM) User's Guide*.

Application Alarms and Events are unsolicited messages used in the system for trouble notification and to communicate the status of the system to Operations Services. The application merges unsolicited alarm messages and unsolicited informational messages from all servers in a network and notifies you of their occurrence. Security alarms enable a network manager to detect security events early and take corrective action to prevent degradation in the quality of service.

Alarms provide information pertaining to a system's operational condition that a network manager may need to act upon. Alarms can have these severities:

- Critical
- Major
- Minor
- Cleared

See chapters *Alarms and Events* and *Security Log* in [2] *Alarms, KPIs, and Measurements Reference* and [1] *Operations, Administration, and Maintenance (OAM) User's Guide* for more details.

OS-level logging is captured in

- **/var/log/messages** - general system messages
- **/var/log/secure** – security related messages
- **/var/log/httpd** (directory) – apache webserver logging

3.7 Optional IPsec Configuration

This section describes security related to configuration changes that are required to use Internet Protocol Security (IPsec). Customers are NOT required to configure IPsec.

3.7.1 IPsec Overview

Internet Protocol Security (IPsec) provides network layer security protocols used for authentication, encryption, payload compression, and key exchange. IPsec provides Host-to-Host encrypted connections or Network-to-Network packet tunneling.

Network traffic between two end-points is encrypted and decrypted by authenticated hosts at the end-points, using a shared private key. The shared private key forms a Security Association that can be automatically changed by Security Policies based on traffic volume, expiry time, or other criteria.

IPsec will work for both IPv4 and IPv6 on the Diameter Sh interface. The provisioning interface only supports IPsec on IPv4.

Note: Oracle Communications User Data Repository supports IPsec with an SCTP/IPv6 configuration.

3.7.1.1 Encapsulating Security Payload

Oracle Communications User Data Repository IPsec uses the Encapsulating Security Payload (ESP) protocol for encryption and authentication. The ESP protocol uses encryption algorithms to encrypt either the packet payload or the entire packet, depending on whether IPsec is configured to use transport mode or tunnel mode. When IPsec is in transport mode, the packet payload is encrypted and the IP header is not encrypted. When IPsec is in tunnel mode, the packet payload and the original IP header are both encrypted and a new IP header is added.

ESP also provides authentication of the encrypted packets to prevent attacks by ensuring the packet is from the correct source.

Many encryption algorithms use an initialization vector (IV) to encrypt. The IV is used to make each message unique. This makes it more difficult for cryptanalysis attempts to decrypt the ESP.

The supported ESP encryption and authentication algorithms are described in Table 3. IPsec IKE and ESP Elements.

3.7.1.2 Internet Key Exchange

Internet Key Exchange (IKE) is used to exchange secure keys to set up IPsec security associations. There are two versions of IKE: IKEv1 and IKEv2. The following main differences exist between IKEv1 and IKEv2:

- IKEv1
  - Security associations are established in in 8 messages

      o   Does not use a Pseudo Random Function

- IKEv2
  - o   Security associations are established in in 4 messages
  - o   Uses an increased number of encryption algorithms and authentication transformations
  - o   Uses a Pseudo Random Function

The encryption algorithms and authentication transformations that are supported for IKE are described in Table 3. IPsec IKE and ESP Elements.

3.7.2 IPsec Process

When an IPsec connection is configured, Security Polices are created using the IPsec connection configuration files. IPsec uses Security Policies to define whether a packet should be encrypted or not. The Security Policies help determine whether an IPsec procedure is needed for a connection. The Security Polices do not change over time.

After the Security Policies exist and initial network connectivity has been made, the Internet Key Exchange (IKE) process occurs.

IKE operates in two phases.

1. Phase 1 acts as an initial handshake and creates the IKE security associations, which are used to determine how to set up an initial secure connection to begin the IPsec security association negotiation.

2. In phase 2, the keys are exchanged and the IPsec Security Associations are created. After the IPsec security Associations exist, the IPsec connection setup process is complete. IPsec now knows how to encrypt the packets.

IPsec uses Security Associations to determine which type of encryption algorithm and authentication transportation should be used when creating an IPsec packet, and to apply the correct decryption algorithm when a packet is received. Because security associations change with time, a lifetime parameter is used to force the security associations to expire so that IPsec must renegotiate them.

An IPsec connection can be set up on a virtual IP, which can be used for HA. However, when a switchover occurs and the VIP is added on the new box a SIGHUP is sent to the iked daemon on the newly active box, so that the VIP is under iked management. Also, the switchover will not occur until the security associations have expired and the renegotiation can begin.

3.7.3 Pre-requisite Steps for Setting Up IPsec

These steps must run once on the active NOAMP server prior to configuring IPsec.

1. Log in as root on the active NOAMP server
2. On the active NOAMP server using the below commands

   **iadd -xu -fallowPgmChg -fname -fvalue LongParam **
   <<'!!!'
   Yes|cm.ha.enableIpsecWhack|1
   !!!

3.7.4 Setting Up IPsec

Adding an IPsec connection also configures it. An existing IPsec connection can be edited or deleted, and an IPsec connection can be started (enabled) and stopped (disabled) without having to fully delete the connection.

IPsec setup needs to be performed on each MP that can control the connection.

Note: IPsec should not be enabled on a live connection. Disable a connection before enabling IPsec.

The following steps refer to procedures for setting up a new IPsec connection:

1. Open platcfg
2. Add and configure an IPsec connection. See Section 3.7.6 "*Adding an IPsec Connection*".
3. Select an IKE version.
   a. Complete the IKE configuration for the IPsec connection.
   b. Complete the ESP configuration for the IPsec connection.
   c. Complete the IPsec connection configuration entries.
   d. Wait for the connection to be added.
4. Enable the IPsec connection. See Section 3.7.8 "*Enabling and Disabling an IPsec Connection*".
5. Log out of platcfg
6. Restart IPsec service by using the below command.

   # service ipsec restart

3.7.5   IPsec IKE and ESP Elements

Table 3 describes IPsec IKE and ESP configuration elements and provides default values if applicable

Table 3. IPsec IKE and ESP Elements

Description	Valid Values	Default
Internet Key Exchange Version	ikev1, ikev2	ikev2
IKE Configuration		
IKE Encryption	aes128_cbc, aes192_cbc, aes256_cbc, 3des_cbc, hmac_md5	aes128_cbc hmac_md5
IKE Authentication	hmac_sha1, aes_xcbc, hmac_md5	hmac_md5
Pseudo Random Function. This is used for the key exchange only for ikev2	hmac_sha1, aes_xcbc (ikev2)	-
Diffie-Hellman Group The group number is used to generate the group (group - set of numbers with special algebraic properties) that is used to select keys for the Diffie-Hellman algorithm. The larger the group number, the larger the keys used in the algorithm.	2, 14 (ikev2) 2 (ikev1)	2 (IKEv1) 14 (IKEv2)
IKE SA Lifetime Lifetime of the IKE/IPsec security associations. A correct lifetime value would be <hours/mins/secs>. Example: 3 mins. **Note:** If a connection goes down, it will not reestablish until the lifetime expires. If the lifetime is set to 60 minutes and a failure causing a switchover of a VIP is required, the switchover will not occur until the 60 minutes expire. The recommendation is to set the lifetime to the lowest possible time that will not impact network connectivity, such as 3-5 minutes.	Number of time units	60
Lifetime Units	hours, mins, secs	mins

Table 3. IPsec IKE and ESP Elements

Description	Valid Values	Default
Perfect Forward Secrecy This is an algorithm used to ensure that if one of the private keys is compromised the other keys are not compromised.	yes, no	yes
ESP Configuration		
ESP Authentication Algorithm used to authenticate the encrypted ESP	hmac_sha1, hmac_md5	hmac_sha1
Encryption Algorithm Algorithm used to encrypt the actual IPsec packets	aes128_cbc, aes192_cbc, aes256_cbc, 3des_cbc	aes128_cbc

3.7.6   Adding an IPsec Connection

Procedure to add an IPsec connection:

1. Log in as **admusr** on the server

    Login: admusr
    Password: <current admin user password>

2. Open the platcfg menu by entering the following command.

    $ sudo su - platcfg

3. Select **Network Configuration**.

4. Select **IPsec Configuration**.

5. Select **IPsec Connections**.

6. Select **Edit**.

7. Select **Add Connection**.

8. Select the Internet Key Exchange Version: either **IKEv1** or **IKEv2**.

9. Complete the *IKE Configuration* fields for the desired connection, then click **OK**.

    The fields are described in Table 3. IPsec IKE and ESP Elements.

10. Select the desired ESP Encryption algorithm, then click **OK**.

    The fields are described Table 3. IPsec IKE and ESP Elements.

11. Complete the Add Connection fields for the desired connection.

    a.   Enter the **Local Address**.

    b.   Enter the **Remote Address**.

    c.   Enter the **Pass Phrase**.

    d.   Select the **Mode**.

12. Click **OK**.

    Wait for the connection to be added.

    When the connection has been successfully added, the **Internet Key Exchange Version** Menu appears.

13. Select **Exit** in each of the menus until a command prompt is reached.

3.7.7   Editing an IPsec Connection

Procedure to edit an IPsec connection:

1. Log in as **admusr** on the server

    Login: admusr
    Password: <current admin user password>

2. Open the platcfg menu by entering the following command.

    $ sudo su - platcfg

3. Select **Network Configuration**.

4. Select **IPsec Configuration**.

5. Select **IPsec Connections**.

6. Select **Edit.**

7. Select **Edit Connection**.

8. Select **IPsec connection** to edit.

9. View the IPsec connection's current configuration.

10. Select **Edit.**

11. Select either **IKEv1** or **IKEv2**.

12. Complete the *IKE Configuration* fields if needed, then click **OK.**

    The fields are described in Table 3. IPsec IKE and ESP Elements.

13. Select the desired *ESP Configuration* fields, then click **OK**.

    The fields are described in Table 3. IPsec IKE and ESP Elements.

14. Complete the Add Connection fields for the desired connection.
    a. Enter the **Local Address**.
    b. Enter the **Remote Address**.
    c. Enter the **Pass Phrase**.
    d. Select the **Mode**.

15. Click **OK**.

16. Select **Yes** to restart the connection.

    When the connection has been successfully updated, the **Internet Key Exchange Version** Menu appears.

17. Select **Exit** in each of the menus until a command prompt is reached.

3.7.8   Enabling and Disabling an IPsec Connection

Procedure to enable or disable an IPsec connection:

1. Log in as **admusr** on the server

    Login: admusr
    Password: <current admin user password>

2. Open the platcfg menu by entering the following command.

    $ sudo su - platcfg

3. Select **Network Configuration**.

4. Select **IPsec Configuration**.

5. Select **IPsec Connections**.

6. Select **Edit.**

7. Select **Connection Control**.

8. Select **IPsec connection** to enable or disable.

9. Select **Enable** or **Disable.**

10. Click **OK** to enable or disable the selected IPsec connection.

11. Select **Exit** in each of the menus until a command prompt is reached.

3.7.9   Deleting an IPsec connection

Procedure to delete an IPsec connection:

1. Log in as **admusr** on the server

   Login: admusr
   Password: <current admin user password>

2. Open the platcfg menu by entering the following command.

   $ sudo su - platcfg

3. Select **Network Configuration**.

4. Select **IPsec Configuration**.

5. Select **IPsec Connections**.

6. Select **Edit**.

7. Select **Delete Connection**.

8. Select IPsec connection to delete.

9. Click **Yes** to confirm the delete.

10. Wait for the connection to be deleted.

   When the IPsec connection has been successfully deleted, the **Connection Action** Menu appears.

11. Select **Exit** in each of the menus until a command prompt is reached.

3.8   Firewall Configuration Changes

3.8.1   Iptables

UDR comes with various IP tables rules preconfigured and dynamically adjusts IP table rules as new diameter peers are defined. In general, we do not recommend making any IP table rule adjustments without prior consultation with UDR product support.

3.8.2   TCP Wrappers

UDR does not use TCP wrappers. Customers wishing to add TCP wrapper rules (`hosts.allow / hosts.deny`) must take care to ensure that management and signaling traffic is not impacted. In general, we do not recommend making any TCP Wrapper rule adjustments without prior consultation with UDR product support.

3.9   Update MySQL Password

3.9.1   Updating the MySQL Password

Use the following procedure to change the MySQL password. Execute the below procedure only from Active NO:

Procedure 22.Update MySQL Password on Active NO	

1.	Log in as admusr on the source server.
	
	`login: admusr`
	
	`Password: <current admin user password>`

2.	To update password for default user :
	
	Reset the MySQL default user password by running:
	
	`$ /usr/TKLC/appworks/bin/resetMysqlPassword`
	
	You are prompted to provide a password:
	
	`Enter password:<enter the new password>`
	
	`Enter Password Again: <re-enter the new password>`
	
	To update password for root user :
	
	Reset the MySQL root password by running:
	
	`$ /usr/TKLC/appworks/bin/resetMysqlPassword root`
	
	You are prompted to provide a password:
	
	`Enter password:<enter the new password>`
	
	`Enter Password Again: <re-enter the new password>`

3.	The command copies the new password to each reachable server in the topology, and flushes client password caches.

This update command synchronizes the MySQL password on all reachable servers in the topology. Any servers added to the topology after running this command are automatically configured to use the new password. No server in the topology should be rebooting while the password is being changed. If any servers were not reachable when this command is run, run the command again later when those servers are reachable. Note -The resetMysqlPassword script should be run only after all the servers in the topology have been upgraded to DSR 8.5 or later.

Appendix A. Secure Deployment Checklist

The following security checklist lists guidelines to help you secure Oracle Communications User Data Repository and its components.

- Change default passwords
- Utilize LDAP for authentication purposes
- Use TLS or IPSEC
- Enforce strong password management
- Restrict admin functions to the required few administrator groups
- Configure community strings and traps explained in Section 3.4 "*Other Optional Configurations*"
- Change provisioning options to only enable secure REST provisioning in Section 3.1.14 "*Provisioning Security*"

Appendix B.   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.

Appendix C. 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.