Oracle® Communications

Diameter Signaling Router

DSR Security Guide

Release 8.5.1

F51015-01

December 2021

Oracle Communications Diameter Signaling Router Security Guide, Release 8.5.0.1.0

CAUTION: Use only the Upgrade procedure included in the Upgrade Kit.

Before upgrading any system, please access My Oracle Support (MOS) (https://support.oracle.com) and review any Technical Service Bulletins (TSBs) that relate to this upgrade.

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 My Oracle Support (MOS) in Appendix B.

Table of Contents

1. Introduction 9
1.1 Audience 9
1.2 References 9
1.3 Acronyms 9
2. Oracle Communications Diameter Singling Router Security Overview 10
2.1 Basic Security Considerations 10
2.2 Access the Oracle Communications Diameter Signaling Router System 11
2.3 Overview of Oracle Communications Diameter Signaling Router Security 12
2.4 Overview of Oracle Communications Diameter Signaling Router Security 12
3. Implement Oracle Communications Diameter Signaling Router Security 13
3.1 Oracle Communications Diameter Signaling Router Web GUI Standard Features 13
3.1.1 User Administration 13
3.1.1.1 Establish GUI Groups and Group Privileges 14
3.1.1.2 Create GUI Users and Assign to Groups 15
3.1.2 GUI User Authentication 16
3.1.2.1 GUI Passwords 16
3.1.2.2 Change Passwords for all DSR Administrative Accounts 16
3.1.2.3 Set Up Password Complexity 16
3.1.2.4 Set Up Password Aging Parameters 16
3.1.2.5 Restrict Concurrent GUI Logins 17
3.1.2.6 External Authentication 17
3.1.2.7 LDAP Authentication for GUI Users 17
3.1.2.8 System Single Sign-On for GUI Users 17
3.1.2.9 Set Password Strength Minimum Digit Characters 18
3.1.2.10 Set Password Strength Minimum Uppercase Characters 18
3.1.2.11 Set Password Strength Minimum Special Characters 19
3.1.2.12 Set Password Strength Minimum Lowercase Characters 19
3.1.2.13 Set Deny for Failed Password Attempts 20
3.1.2.14 Set Minimum Password Length 21
3.1.3 GUI Login and Welcome Banner Customization 21
3.1.4 SSH Security Hardening Procedures 21
3.1.4.1 Set SSH Client Alive Count 21
3.1.4.2 Disable SSH Access via Empty Passwords 22

3.1.4.3 Enable SSH Warning Banner 22
3.1.4.4 Do not allow SSH Environment Options 23
3.1.4.5 Generate passphrase protected RSA SSH Key for ‘admusr’ User Account 23
3.1.4.6 Set SSH LogLevel to INFO 24
3.1.4.7 Enable SSH IgnoreRhosts 25
3.1.4.8 Disable SSH X11 Forwarding 25
3.1.4.9 Disable SSH HostbasedAuthentication 25
3.1.4.10 Set SSH LoginGraceTime to 1m 26
3.1.4.11 Disable diffie-hellman-group1-sha1 Key Exchange(Kex) algorithm ..... **Error! Bookmark not defined.**
3.1.5 Services Hardening Procedures 27
3.1.5.1 Uninstall tftp-server Package 27
3.1.5.2 Disable xinetd Service 27
3.1.5.3 Uninstall xinetd Service 27
3.1.5.4 Disable ntpdate Service 28
3.1.6 SNMP Configuration 28
3.1.6.1 Select Versions 29
3.1.6.2 Community Names/Strings 29
3.1.7 SNMPv3 on PMAC 29
3.1.7.1 Enable SNMPv3 Support on PMAC 29
3.1.7.2 Configure SNMPv3 Security Model and Trap Servers 29
3.1.8 Authorized IPs 29
3.1.9 Certificate Management 30
3.1.9.1 Create a New Certificate for WebLogic and Tomcat Servers 30
3.1.10 SFTP Administration 34
3.2 Host Intrusion Detection System (HIDS) 35
3.2.1 Host Intrusion Detection System (HIDS) overview 35
3.2.2 Determine Host Intrusion Detection System (HIDS) Status 35
3.2.3 Initialize Host Intrusion Detection System (HIDS) 37
3.2.4 Enable or Disable Host Intrusion Detection System (HIDS) 39
3.2.5 Suspend or Resume Host Intrusion Detection System (HIDS) 41
3.2.6 Run On-Demand Host Intrusion Detection System (HIDS) Security Check 43
3.2.7 Update Host Intrusion Detection System (HIDS) Baseline 46
3.2.8 Delete Host Intrusion Detection System (HIDS) Baseline 48

3.2.9 Host Intrusion Detection System (HIDS) Alarms 50
3.3 Oracle Communications Diameter Signaling Router OS Standard Features 52
3.3.1 Configure NTP Servers 53
3.3.1.1 Configure NTP for the Host OS of the Application guest VM (TVOE) 53
3.3.2 Set the Time on the TVOE Host 54
3.3.3 Configure Password Settings for OS Users 55
3.3.4 Configure Other Session and Account Settings for OS Users 56
3.3.5 Update the TPD-Provd Cipher List 57
3.3.6 Operational Dependencies on Platform Account Passwords 57
3.3.7 Update the SELinux mode to ‘permissive’ 58
3.4 Other Optional Configurations 58
3.4.1 Require Authentication for Single User Mode 58
3.4.2 Change OS User Account Passwords 59
3.4.3 Change Login Display Message 59
3.4.4 Force iLO to Use Strong Encryption 60
3.4.5 Set Up rsyslog for External Logging 61
3.4.6 Add sudo Users 61
3.4.7 Report and Disable Expired OS User Accounts 63
3.5 Ethernet Switch Considerations 63
3.5.1 Configure SNMP in Switches 63
3.5.2 Configure Community Strings 64
3.5.3 Configure Traps 64
3.6 Security Logs and Alarms 64
3.7 Optional IPsec Configuration 65
3.7.1 IPsec Overview 65
3.7.1.1 Encapsulate Security Payload 65
3.7.1.2 Internet Key Exchange 65
3.7.2 IPsec Process 66
3.7.3 Pre-requisite Steps for Setting Up IPsec 66
3.7.4 Set up IPsec 66
3.7.5 IPsec IKE and ESP Elements 67
3.7.6 Add an IPsec Connection 68
3.7.7 Edit an IPsec Connection 69
3.7.8 Enable and Disable an IPsec Connection 70

3.7.9 Delete an IPsec Connection 71
3.8 Firewall Configuration Changes 71
3.8.1 Iptables 71
3.8.2 TCP Wrappers....71
3.9 Internal Web Services 72
3.9.1 Changing the Internal Web Service Passwords 72
3.9.1.1 Changing the TPD Web Service Password 72
3.9.1.2 Changing the Configuration Web Services Password 73
3.9.2 Changing the Internal Web Service Certificates and Key Material 74
3.10 Update MySQL Password 77
3.10.1 Updating the MySQL Password....77

Appendix A. Secure Deployment Checklist....77

Appendix B. My Oracle Support (MOS)....78

List of Tables

Table 1. Acronyms 9
Table 2. Predefined User and Group....14
Table 3. IPsec IKE and ESP Elements....67

List of Figures

Figure 1. Oracle Communications Diameter Signaling Router Login Page....11
Figure 2. Oracle Communications Diameter Signaling Router Home Page 12
Figure 3. Oracle Communications Diameter Signaling Router Generic DSR Deployment Model for a Generic Model of the Deployment Strategy 13
Figure 4. Global Action and Administration Permissions 15
Figure 5. NTP Configuration (GUI) 53

List of Procedures

Procedure 1. Set Password Strength Minimum Digit Characters....18
Procedure 2. Set Password Strength Minimum Uppercase Characters....18
Procedure 3. Set Password Strength Minimum Special Characters 19
Procedure 4. Set Password Strength Minimum Lowercase Characters....19
Procedure 5. Set Deny for Failed Password Attempts....20

Procedure 6. Set Minimum Password Length 21
Procedure 7. Set SSH Client Alive Count.....21
Procedure 8. Disable SSH Access via Empty Passwords 22
Procedure 9. Set SSH Warning Banner 22
Procedure 10. Do not allow SSH Environment Options.....23
Procedure 11. Generate passphrase protected RSA SSH Key for ‘admusr’ User Account.....23
Procedure 12. Set SSH LogLevel to INFO 24
Procedure 13. Enable SSH IgnoreRhosts 25
Procedure 14. Disable SSH X11 Forwarding 25
Procedure 15. Disable SSH HostbasedAuthentication 25
Procedure 16. Set SSH LoginGraceTime to 1m 26
Procedure 17. Disable diffie-hellman-group1-sha1 Key Exchange (Kex) algorithm .....**Error! Bookmark not defined.**
Procedure 18. Uninstall tftp-server Package 27
Procedure 19. Disable xinetd Service 27
Procedure 20. Uninstall xinetd Service.....28
Procedure 21. Disable ntpdate Service 28
Procedure 14. HIDS Status.....35
Procedure 15. Initialize HIDS 37
Procedure 16. Enable or Disable HIDS 39
Procedure 17. Suspend or Resume HIDS.....41
Procedure 18. Suspend or Resume HIDS.....43
Procedure 19. Update HIDS.....46
Procedure 20. Delete HIDS.....48
Procedure 21. View HIDS Alarms 51
Procedure 22. Configure NTP for the Host OS of the Application Guest VM 53
Procedure 23. Configure Password Settings for OS Users 55
Procedure 24. Don’t Allow Usernames to be Embedded in Passwords.....55
Procedure 25. Configure Session Inactivity for OS Users 56
Procedure 26. Lock OS User Accounts After Too Many Failed Login Attempts.....56
Procedure 27. Lock Inactive OS User Accounts.....57
Procedure 28. Update SELinux mode on the server 58
Procedure 29. Require Authentication for Single User Mode.....58
Procedure 30. Change OS User Account Passwords.....59
Procedure 31. Change Login Display Message.....59

Procedure 32. Force iLO to Use Strong Encryption....60
Procedure 33. Set Up rsyslog for External Logging....61
Procedure 34. Require admusr to Enter a Password to Run Commands Using sudo....62
Procedure 35. Report and Disable Expired OS User Accounts....63
Procedure 36. Report and Disable Expired OS User Accounts....63
Procedure 37. Add an IPsec Connection....68
Procedure 38. Edit an IPsec Connection....69
Procedure 39. Enable/Disable an IPsec Connection....70
Procedure 40. Delete an IPsec Connection....71
Procedure 41. Update TPD Web Service Password on Active NO....72
Procedure 42. Update TPD Web Service Password on PMAC....73
Procedure 43. Update Configuration Web Service Password on Active NO....73
Procedure 44. Update Configuration Web Service Password on IDIH....74
Procedure 45. Create and Distribute a Combined Certificate/Key PEM File....75
Procedure 46. Install a Combined PEM File on Each Distinct <hostname>....75
Procedure 47. Update MySQL Password on Active NO....77

1. Introduction

This document provides guidelines and recommendations for configuring the Oracle Communications Diameter Signaling Router (DSR) to enhance the security posture of the system. The recommendations herein are optional and should be considered along with your organization's approved security strategies. Additional configuration changes that are not included in this document 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 Diameter Signaling Router documentation set. See My Oracle Support (MOS).

[1] Operation, Administration, and Maintenance (OAM) Guide

[2] Alarms, KPIs, and Measurements Reference

[3] DSR C-Class Hardware and Software Installation Procedure 1/2 Guide

[4] DSR C-Class Hardware and Software Installation Procedure 2/2 Guide

[5] DSR Upgrade Procedure

[6] PMAC Configuration Guide

[7] DSR VNFM Installation and User Guide

1.3 Acronyms

An alphabetized list of acronyms used in the document.

Table 1. Acronyms

Acronym	Definition
CLI	Command Line Interface
CSR	Customer Service Request
DSR	Diameter Signaling Router
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
MMI	Machine to Machine Interface

Acronym	Definition
MP	Message Processor
NOAMP	Network Operation, Administration, Maintenance, and Provisioning
OAM	Operation, Administrations, and Maintenance
OCH	Oracle Communications Help Center
OS	Operating System
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

2. Oracle Communications Diameter Singling Router Security Overview

This chapter provides an overview of Oracle Communications Diameter Signaling Router (DSR) security.

2.1 Basic Security Considerations

These 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 Diameter Signaling Router software upgrades.
- **Limit privileges**. Users should be assigned to the proper user group and reviewed periodically to determine relevance to current work requirements. See User Administration, for more information.
- **Monitor system activity**. Establish who should access which system components, and how often, and monitor those components. See Host Intrusion Detection System (HIDS) and Security Logs and Alarms, for more information.
- **Configure software securely**. For example, use secure protocols such as TLS and strong passwords. See GUI Passwords and Oracle Communications Diameter Signaling Router OS Standard Features, for more information.
- **Change default passwords**. The initial installation of the DSR system software uses default passwords. These should be changed at installation time. (See Change Passwords for all DSR Administrative Accounts and Changing the Internal Web Service Passwords, for more information.)
- **Obtain and install X**.509 web certificates for GUI and MMI access. The DSR system ships with a self-signed certificate that should be replaced before the system is put into operation. See Certificate Management, for more information.
- **Learn and use the Oracle Communications Diameter Signaling Router security features**. See Section 3 Implement Oracle Communications Diameter Signaling Router Security and Section 3.7 Optional IPsec Configuration for more information.
- **Keep up to date on security information**. Oracle regularly issues security alerts for important vulnerability fixes. It is advisable to install the applicable security patches as soon as possible. See

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

2.2 Access the Oracle Communications Diameter Signaling Router System

There are four ways a user can access the Oracle Communications Diameter Signaling Router system.

1. **Web browser GUI** – The client access to the Oracle Communications Diameter Signaling Router GUI for remote administration requires a web browser supporting a TLS 1.1 or TLS 1.2 enabled session to Oracle Communications Diameter Signaling Router. (See for a list of supported TLS Ciphers.) This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. When a user accesses the Oracle Communications Diameter Signaling Router system via the GUI interface, the Log In screen displays. Type the **Username** and **Password** credentials, and click **Log In** to access the GUI.

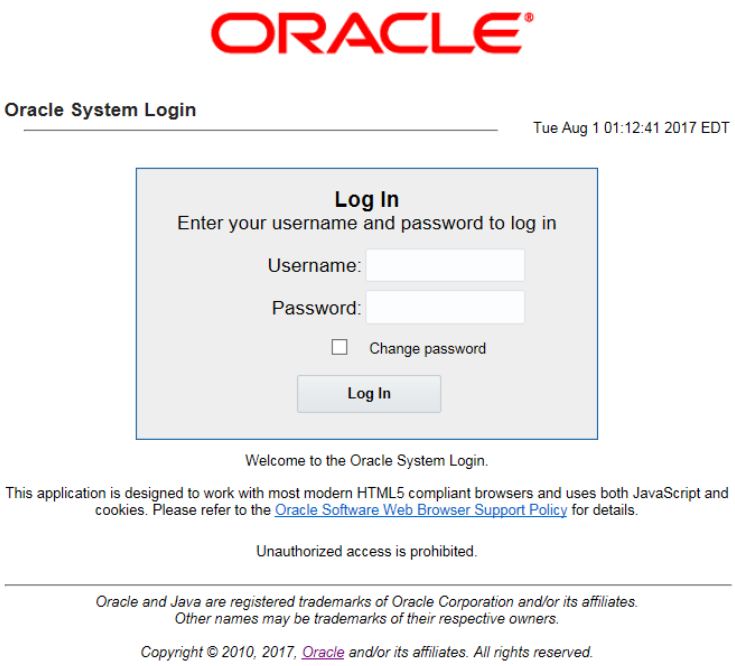


Figure 1. Oracle Communications Diameter Signaling Router Login Page

When successfully logged in, the Oracle Communications Diameter Signaling Router home page displays. To logout, click the upper-right corner link labelled **Logout** or select the bottom menu item.

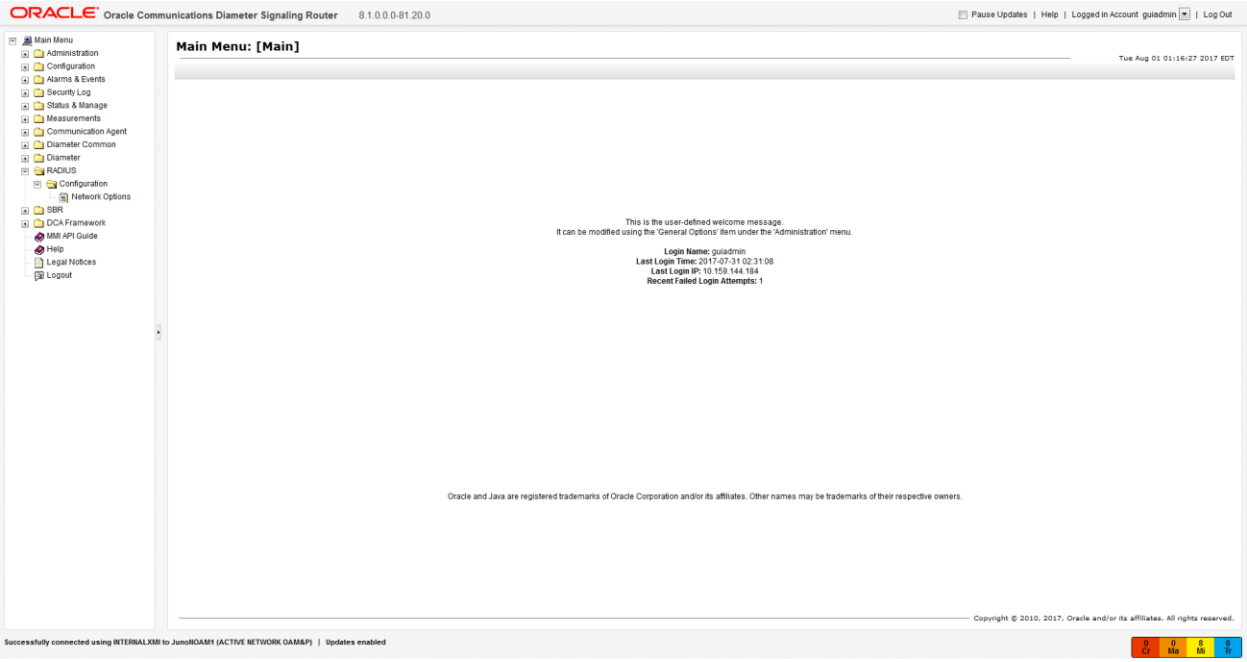


Figure 2. Oracle Communications Diameter Signaling Router Home Page

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. (See for a list of supported SSH Ciphers/MACs.) SSH login is supported on the distinct management interface. To logout, enter the command, logout, and press **Enter**.

3. **Local access may be supported by a hardware connection of a monitor and a keyboard**. Local access supports CLI only. When successfully logged in, a command line prompt containing userid@host name followed by a $ prompt displays. There is no requirement to add additional users, but adding users is supported. This is not supported on all hardware.

   - iLO/ILOM Web GUI access – Proliant Server iLO or Oracle ILOM provides web GUI access from a web browser using the URL, https://<iLO/ILOM IP Address>/. Using a supported web browser, log into iLO/ILOM as an administrator user by providing a username and password.

2.3 Overview of Oracle Communications Diameter Signaling Router Security

Oracle Communications Diameter Signaling Router 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

2.4 Overview of Oracle Communications Diameter Signaling Router Security

Oracle Communications Diameter Signaling Router is deployed in carrier's and service provider's core networks and provides critical signaling routing functionality for 4G, LTE, and IMS networks. The solution is based on Linux servers and is highly scalable to accommodate a wide range of capacities to address

networks of various sizes. A DSR node is comprised of a suite of servers and related Ethernet switches that create a cluster of servers operating as a single Network Element. It is assumed that firewalls are established to isolate the core network elements from the internet and from partner networks (Figure 3).

In addition to the firewalls mentioned above, DSR provides additional security capabilities including Access Control Lists (ACL) functionality at the demarcation switch, VLAN, or physical separation of administrative and signaling traffic, and IP Tables functionality at the servers for local firewalling.

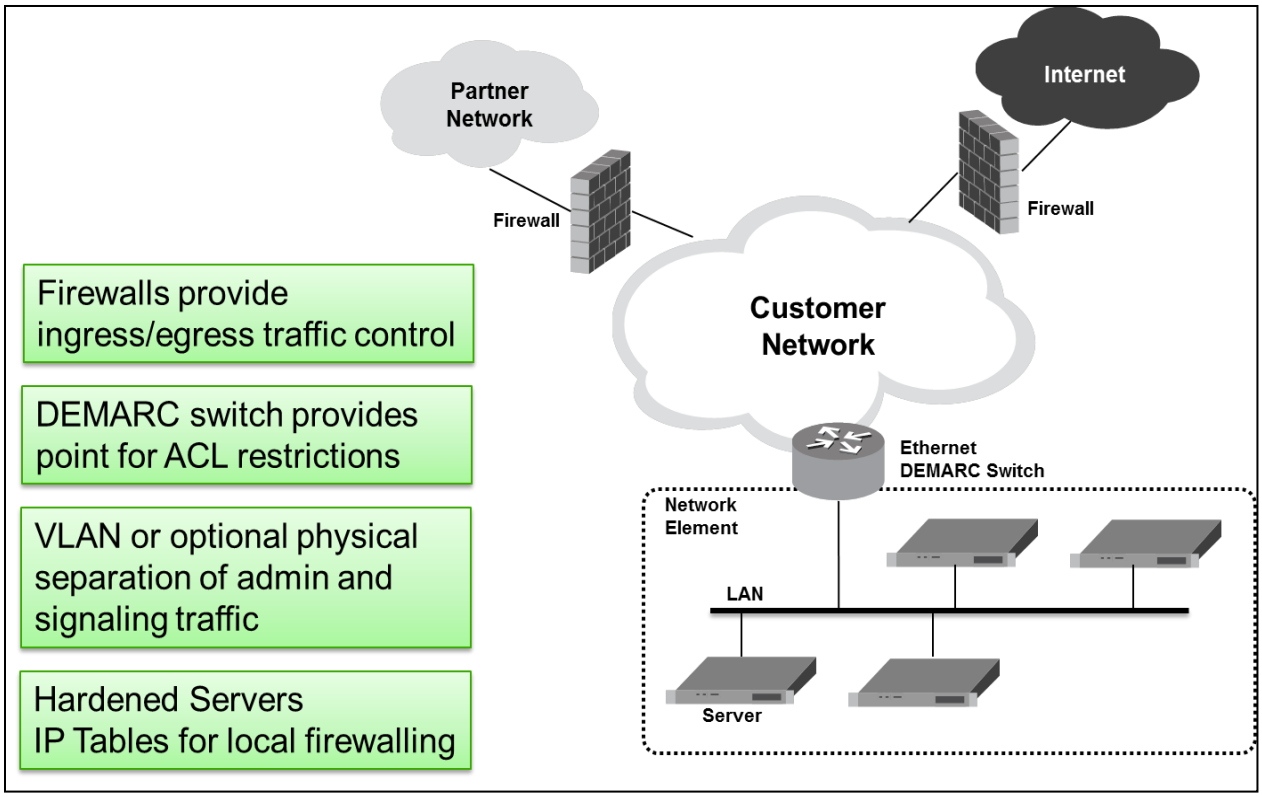


Figure 3. Oracle Communications Diameter Signaling Router Generic DSR Deployment Model for a Generic Model of the Deployment Strategy

3. Implement Oracle Communications Diameter Signaling Router Security

This chapter explains security-related configuration settings that may be applied to Oracle Communications Diameter Signaling Router.

3.1 Oracle Communications Diameter Signaling Router Web GUI Standard Features

This section explains the security features of the Oracle Communications Diameter Signaling Router 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 delivered with the system for setting up the groups and users by the customer. The following are details for 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 is never 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 in [1] Operation, Administration, and Maintenance (OAM) Guide.

3.1.1.1 Establish 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 these 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
- Diameter Configuration Permissions
- Diameter Maintenance Permissions
- Diameter Diagnostics Permissions
- Diameter Mediation Permissions
- Diameter Troubleshooting with IDIH Permissions
- Diameter AVP Dictionary Permissions

For more details on the permissions available for the above groups, please see the section Group Administration in the [1] Operation, Administration, and Maintenance (OAM) 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 4).

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 SNMP Trapping	☐	☐	☐	☐	☐
Remote LDAP Authentication	☐	☐	☐	☐	
Remote Export Server	☐	☐	☐	☐	☐
DNS Configuration	☐	☐	☐	☐	

Figure 4. Global Action and Administration Permissions

3.1.1.2 Create GUI Users and Assign to Groups

Before adding a user, determine which user group the user should be assigned based on the user's operational role. The group assignment determines the functions 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.

The Insert User page displays these elements:

- User Name
- Group
- Authentication Options
- Access Allowed
- Maximum Concurrent Logins
- Session Inactivity Limit
- Comment

For more details on these elements, refer to the Administration chapter in the [1] Operation, Administration, and Maintenance (OAM) Guide.

The user administration page lets users perform these actions:

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

For details on how to perform these actions, refer to the Administration chapter in the [1] Operation, Administration, and Maintenance (OAM) 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] Operation, Administration, and Maintenance (OAM) 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 a way to set passwords: through the user interface from the Users Administration page. For more detailed steps on performing these two methods, refer to the Administration chapter in [1] Operation, Administration, and Maintenance (OAM) Guide.

3.1.2.2 Change Passwords for all DSR Administrative Accounts

The System Installation procedure creates these default accounts:

- **guiadmin** – for Oracle Communications Diameter Signaling Router Application GUI
- **root** – for CLI
- **admusr** – for CLI

This procedure also conveys 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] Operation, Administration, and Maintenance (OAM) Guide for Passwords in the Administration chapter.

For changing the OS account passwords of a CLI account, see Section 3.4.2 Change OS User Account Passwords.

3.1.2.3 Set 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: numeric, 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 on the **Administration > General Options** screen.

3.1.2.4 Set 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] Operation, Administration, and Maintenance (OAM) 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.

These elements are required to configure an LDAP server:

- 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] Operation, Administration, and Maintenance (OAM) 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] Operation, Administration, and Maintenance (OAM) 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. ☐	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/$/ dcredit=-1/" /etc/pam.d/system-auth`
	`$ 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. ☐	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/$/ ucredit=-2/" /etc/pam.d/system-auth`
	`$ sudo sed -i --follow-symlinks "/pam_cracklib.so/ s/$/ ucredit=-2/" /etc/pam.d/password-auth`

Procedure 2. Set Password Strength Minimum Uppercase Characters	

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. ☐	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/$/ ocredit=-2/" /etc/pam.d/system-auth`
	`$ 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`

Procedure 4. Set Password Strength Minimum Lowercase Characters	

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`

Procedure 5. Set Deny for Failed Password Attempts	

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 Diameter Signaling Router 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 administrative 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`

Procedure 7. Set SSH Client Alive Count	

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:
	`$ sudo sed -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:

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`

Procedure 9. Set SSH Warning Banner	

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:
	`$ sudo sed -i '/PermitUserEnvironment/c\PermitUserEnvironment no' /etc/ssh/sshd_config`

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

3.1.4.5 Generate passphrase protected RSA SSH Key for 'admusr' User Account

Execute the below procedure to generate a passphrase protected 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 passphrase protected RSA SSH Key for 'admusr' User Account	

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

2.	Stop the apwSoapServer process : `$ sudo pm.set off apwSoapServer`

Procedure 11. Generate passphrase protected RSA SSH Key for 'admusr' User Account	

3. ☐	Go to .ssh directory and remove the old DSA keys if they exist :
	`$ cd /home/admusr/.ssh`
	`$ sudo rm -rf id_dsa id_dsa.pub`

4. ☐	Generate new RSA key using below command :
	`$ ssh-keygen -t rsa -b 4096`
	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_rsa** will be used :
	`$ Enter file in which to save the key (/home/admusr/.ssh/id_rsa):`
	You will be prompted to enter the passphrase. Insert the passphrase :
	`$ Enter passphrase (empty for no passphrase):`
	You will be asked to confirm the passphrase. Insert passphrase again :
	`$ Enter same passphrase again:`
	
	A password protected RSA key will be generated successfully.

5.	Start the apwSoapServer process : `$ sudo pm.set on apwSoapServer`
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' account will 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. The procedure include procedures specified in Section 3.9.1.1 Changing the TPD Web Services Password and Section and Section 3.9.1.2 Changing the Configuration Web Services Password.

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	

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

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

7. ☐	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`

8. ☐	Check in the 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`

Procedure 15. Disable SSH HostbasedAuthentication	
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 and gss-group1-sha1- Key Exchange (Kex) algorithms, and set the moduli (key length) longer than 1024 bits

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

Procedure 17. Disable diffie-hellman-group1-sha1 and gss-group1-sha1- Key Exchange (Kex) algorithms, and set the moduli (key length) longer than 1024 bits	

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`

Procedure 17. Disable diffie-hellman-group1-sha1 and gss-group1-sha1- Key Exchange (Kex) algorithms, and set the moduli (key length) longer than 1024 bits	
4. ☐	Execute the below command to 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] Operation, Administration, and Maintenance (OAM) 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 checkbox on this page.

The SNMP Trapping page provides the following functionalities:

- Add an SNMP manager
- View SNMP settings
- Update SNMP settings
- Delete the SNMP manager

For more details on these actions, refer to the [1] Operation, Administration, and Maintenance (OAM) Guide.

3.1.6.1 Select 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 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 PMAC server 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 displays 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] Operation, Administration, and Maintenance (OAM) Guide, Authorized IPs section for more details on how to enable this feature.

3.1.9 Certificate Management

The Certificate Management feature allows the user to configure digital security certificates for securing Oracle Communications Diameter Signaling Router web sessions, user authentication thru secure LDAP over TLS, and secure Single Sign-On authentication across a defined zone of Oracle Communications Diameter Signaling Router 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 then later import the signed certificate into the Oracle Communications Diameter Signaling Router. This feature lets the user generate a Certificate Report of individual or all (wildcard) defined certificates.

For details on Certificate Management feature see Certificate Management chapter in [1] Operation, Administration, and Maintenance (OAM) Guide.

3.1.9.1 Create a New Certificate for WebLogic and Tomcat Servers

The procedures in this section allow you to create customized certificates and replace the default Appworks certificate provided by DSR.

3.1.9.1.1 Creating Keystore and Certificate Signing Request

1. Log in to the application VM of IDIH using SSH.
2. Execute the `sudo su - tekelec` command to change the user to tekelec.
3. Execute the following command to change the directory to the Weblogic domain (nsp):

   ```
   cd /usr/TKLC/xIH/bea/user_projects/domains/tekelec/nsp
   ```

4. Execute the following commands to take a backup of the existing key and trust stores:

   ```
   cp idih.jks idih_bkp.jks
   cp idih-trust.jks idih-trust-bkp.jks
   ```

5. Execute the following command to create a keystore and a private key using the genkeypair or genkey command:

   ```
   keytool -genkeypair -alias <alias_name> -keyalg RSA -keysize 1024 -
   dname "CN=<ServerName>, OU=GTI, O=<CompanyName>, L=<City>,
   ST=<State>,C=<Country> " -keypass <key_password> -keystore
   <server_keystore>.jks -storepass <store_password>
   ```

   Where,

   - `<alias_name>` indicates the alias for the keystore.
   - `<ServerName>` indicates the server name.
   - `<CompanyName>` indicates your company name.
   - `<City>` indicates your city name.
   - `<State>` indicates your state name.
   - `<Country>` indicates your country name.
   - `<key_password>` indicates the password.
   - `<server_keystore>` indicates keystore name.
   - `<store_password>` indicates the store password.

In the aforementioned command, Common Name (CN) can be a domain name/DNS Name/machine name or any other name. The CN must match your machine name or hostname. This allows the hostname verification to complete.

The system generates a private and public key pair.

6. To create a Certificate Signing Request (CSR), execute the following command:

```
keytool -certreq -v -alias <alias_name> -file <csr-for-myserver>.pem -
keypass <key_password> -storepass <store_password> -keystore
<server_keystore>.jks
```

Where,

- `<alias_name>` indicates the alias that was used during the creation of keystore.
- `<csr-for-myserver>` indicates a file name for the CSR file.
- `<key_password>` indicates the keystore password that was provided during the keystore creation.
- `<store_password>` indicates the store password that was provided during the keystore creation.
- `<server_keystore>` indicates the JKS file name that was generated during the keystore creation.

The system creates the csr-for-myserver.pem file. The file is sent to a Certificate Authority (CA) to create a signed public key certificate.

3.1.9.1.2 Importing Certificate

1. When the CA returns the signed public key with the intermediate and root certificates, execute the following command to import the intermediate and root certificates into your Keystore:

```
keytool -importcert -v -noprompt -trustcacerts -alias
<alias_for_root_certificate> -file <root_certificate_file> -keystore
<server_keystore>.jks -storepass <store_password>
```

Where,

- `<alias_for_root_certificate>` indicates an alias for the root certificate.
- `root_certificate_file` indicates the file name of the root certificate issued by CA.
- `server_keystore` indicates the JKS file name that was generated during the Keystore creation.
- `store_password` indicates the store password that was provided during the Keystore creation.

2. Import the public certificate into the Keystore using the private key alias.
3. To obtain the certificate, do one of the following:
   - From the CA's website, download the root CA and intermediate CA if available.
   - Double-click the certificate file, and then go to the **Certification Path** tab.

     The first certificate in the list is the root CA and the second one is the intermediate CA if available. If you highlight the root CA, and then click **View Certificate**, it opens the Root CA certificate. Then, you can go to the **Details** tab and click <Copy to file>. Select Base 64 as the format and save the file. Repeat the same steps to copy the intermediate CA to a file.

4. When you obtain root CA, intermediate, and certificate files, if you have an intermediate CA, edit it and copy all the content.
5. Edit the certificate file and paste the intermediate at the bottom of the server certificate.

   Skip this step if you do not have an intermediate CA.
6. Repeat the same step for the root CA and paste it at the end of the previously added certificate.

   The following is a sample certificate:

```
-------BEGIN CERTIFICATE---------
dfsfsdfdf
sfsdfwehdfhdf <---------certificate
dgdfgfgfdg
--------END CERTIFICATE-----------
-------BEGIN CERTIFICATE---------
hghjgfjgj
sfsdfwejjhdfhdf <---------intermediate
dgdfgiuiyuiuiyufgfdg
--------END CERTIFICATE-----------
-------BEGIN CERTIFICATE---------
dfsfsmbvmvbmdfdf
sfsdetetrtyrfwehdfhdf <---------root CA
dgdfgnbnbvnvbfgfdg
--------END CERTIFICATE-----------
```

7. Execute the following command to import the certificate:

```
keytool -importcert -v -alias <alias_name> -file <mycert> -keystore
<server_keystore>.jks -keypass <key_password> -storepass
<store_password>
```

   Where,

   - `<alias_name>` indicates the alias that was used during the creation of Keystore.
   - `<mycert>` indicates the file name of the certificate issued by CA.
   - `<server_keystore>` indicates the JKS file name that was generated during the Keystore creation.
   - `<key_password>` indicates the Keystore password that was provided during the Keystore creation.
   - `<store_password>` indicates the store password that was provided during the Keystore creation.
8. Execute the following command to check whether the Keystore creation is complete:

```
keytool -list -v -keystore <server_keystore>.jks -storepass
<store_password>
```

9. Execute the following command to import the root CA of your signed certificate to the Trust KeyStore file:

```
keytool -alias server_cert -import -file rootcacert.cer -keystore
trustkeystore.jks -storepass <Password>
```

3.1.9.1.3 Configuring Keystore on WebLogic

1. Log in to the WebLogic Server Administration Console using your login credentials.
2. In the left navigation pane, click **Environment** > **Servers**.
3. In the **Customize this table** section, in the **Name** column, click **nsp(admin)**.

   nsp(admin) is the server for which the identity and trust keystores configuration is performed.
4. In the **Settings for nsp** section, click **Configuration** > **Keystores**.
5. To edit or modify the existing settings of the Keystore configuration, in the left navigation pane, click **Lock & Edit**.
6. In the **Keystores** section, edit the following fields as required:
   - **Custom Identity Keystore**: Enter the fully qualified path to the identity Keystore.
   - **Custom Identity Keystore Type**: Enter the type of Keystore.
     This attribute is a Java KeyStore (JKS). The default value is JKS.
   - **Custom Identity Keystore Passphrase**: Enter the password required for reading or writing to the Keystore, for example, weblogic1234.
   - **Custom Trust Keystore**: Enter the fully qualified path to the trust Keystore.
   - **Custom Trust Keystore Passphrase**: Enter the passphrase of the custom trust Keystore.
   - **Confirm Custom Trust Keystore Passphrase**: Re-enter the passphrase of the custom trust Keystore.
7. Click **Save**.
8. In the **Settings for nsp** section, click **Configuration** > **SSL**.
9. In the **Identity** section, edit the following fields as required:
   - **Private Key Alias**: Enter the fully qualified path to the identity Keystore.
   - **Private Key Passphrase**: Enter the same password used for the creation of Keystore, for example, weblogic1234.
   - **Confirm Private Key Passphrase**: Re-enter the same password used in the **Private Key Passphrase** field**.**
10. Click **Save**.
11. In the left navigation pane, click **Activate Changes**.
12. Restart WebLogic by logging in to app server using admusr, and then execute the following command:

```
sudo service xih-apps restart
```

3.1.9.1.4 Creating Keystore in the Tomcat Server

1. Log in to the IDIH App VM using SSH as an admusr user.
2. Execute the following command to change the directory to conf folder of Tomcat:

   ```
   cd /usr/share/tomcat6/conf
   ```

3. Execute the following command to take a backup of the existing jks file:

   ```
   cp idih.jks idih-bkp.jks
   ```

4. Execute the following command to copy the Keystore that was created for the WebLogic server into the Tomcat configuration folder:

   ```
   cp /usr/TKLC/xIH/bea/user_projects/domains/tekelec/nsp/<JKS file
   created for WebLogic in the previous step> .
   ```

   ```
   sudo chown tomcat:root <JKS file created for WebLogic in the previous
   step>
   ```

3.1.9.1.5 Modifying the Tomcat File Configuration

1. Execute the following command to edit the `server.xml` file and update keystoreFile and keystorePass fields:

   ```
   sudo vim server.xml
   ```

2. Modify the following tag in the server.xml file and ensure that the keystoreFile field is updated with the latest jks file name and keystorePass with its corresponding password.

   ```
   <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"

                  maxThreads="150" scheme="https" secure="true"

                  clientAuth="false" sslProtocol="TLS"

                  keystoreFile="conf/<JKS file created for WebLogic in the
                  previous step>.jks"

                  keystorePass="<Password used during the creation of
                  keystore>" />
   ```

3. Execute the `sudo service tomcat6 restart` command to restart the Tomcat server.

3.1.10 SFTP Administration

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

The transfer of files is driven from the external server. See section SFTP Users Administration in [1] Operation, Administration, and Maintenance (OAM) Guide.

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.

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 results in an alarm being raised or cleared is logged here (for example, file tampering alarm, Syscheck process alarm, Samhain process alarm).
- **admin.log** – Any HIDS command executed has the output logged here either for successful or error 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 does not 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. The Customers can view active alarms on the Oracle Communications Diameter Signaling Router GUI by navigating to **Alarms & Events > View Active**.

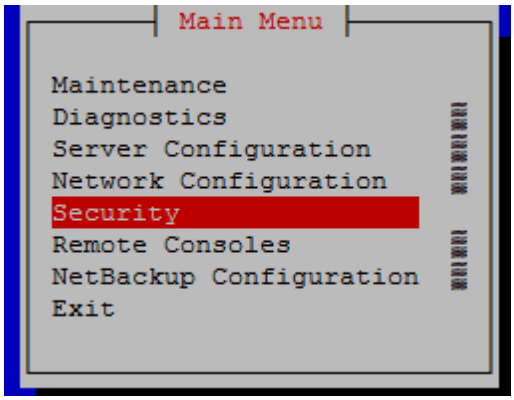
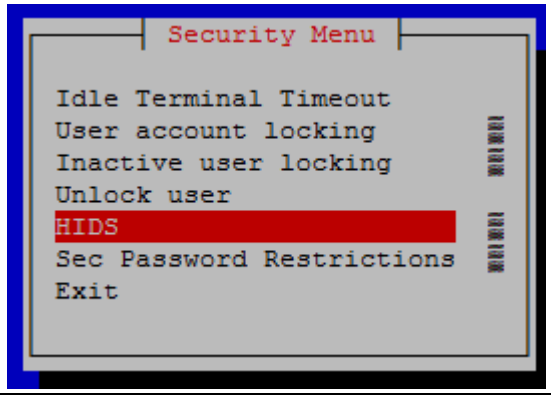
3.2.2 Determine Host Intrusion Detection System (HIDS) Status

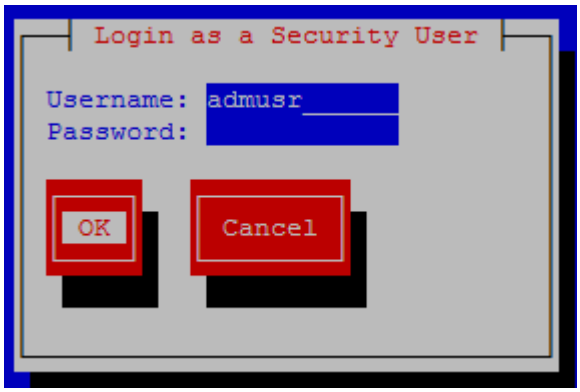
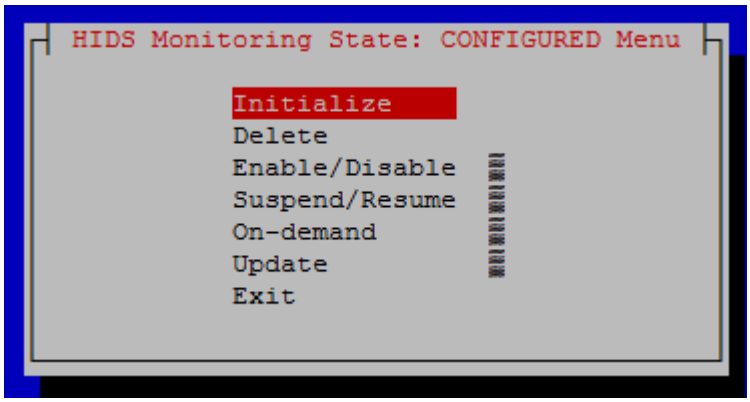
The HIDS status for the server is displayed along the top of the HIDS menu window.

Procedure 14. HIDS Status		

1. ☐	Log in to server	Log in as **admusr** on the server.
		`Login: admusr`
		`Password: <current admin user password>`

2. ☐	Open platcfg menu	Open the **platcfg** menu by entering this command: `$ sudo su - platcfg`

Procedure 14. HIDS Status		
3. ☐	Select Security	Select **Security** from the menu and press **Enter**. 
4. ☐	Select HIDS	Select **HIDS** from the menu and press **Enter**. 

Procedure 14. HIDS Status		
5. ☐	Check HIDS status	1. Type the **Username** and **Password** for a user that is part of the **secgrp** group.  ***Note:*** By default, **admusr** is part of the **secgrp** group. 2. Click **OK** and press **Enter**. The HIDS menu displays and the HIDS Monitoring State is listed on the top of the window. 
6. ☐	Exit	Select **Exit** in each of the menus until a command prompt is reached.

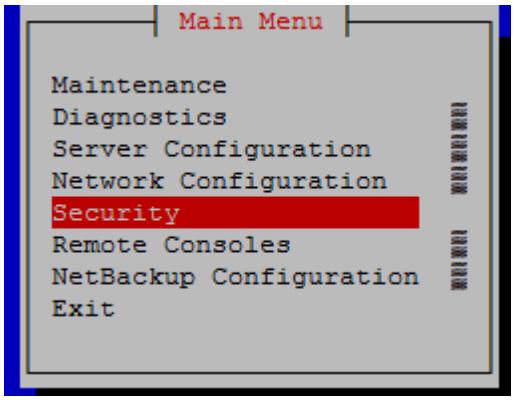
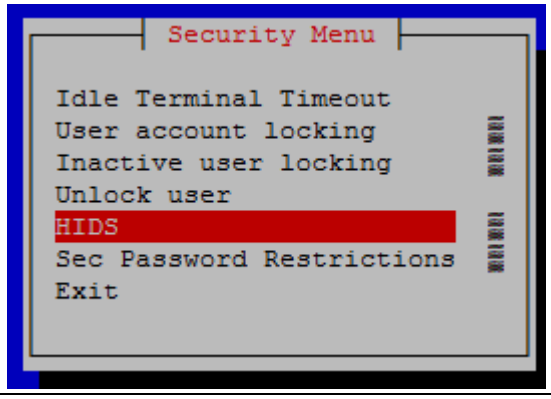
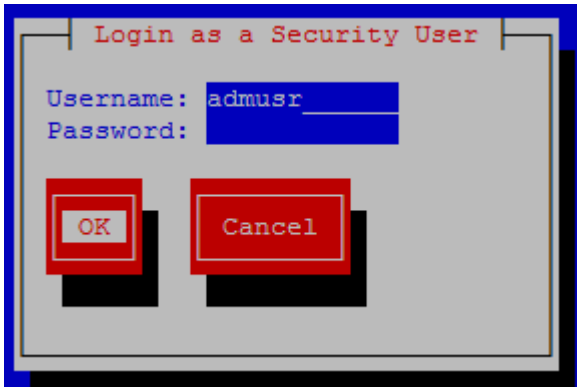
3.2.3 Initialize Host Intrusion Detection System (HIDS)

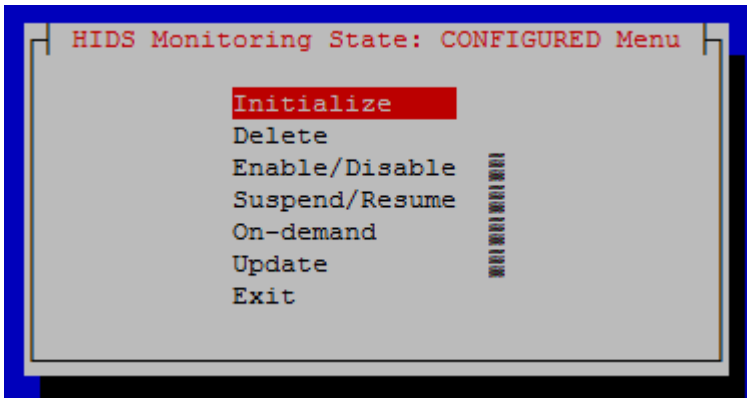
The Host Intrusion Detection System (HIDS) feature must be initialized before enabling HIDS for the first time on a system.

Procedure 15. Initialize HIDS		

1. ☐	Log in to server	Log in as **admusr** on the server.
		`Login: admusr`
		`Password: <current admin user password>`

2. ☐	Open platcfg menu	Open the **platcfg** menu by entering this command: `$ sudo su - platcfg`

Procedure 15. Initialize HIDS		
3. ☐	Select Security	Select **Security** from the menu and press **Enter**. 
4. ☐	Select HIDS	Select **HIDS** from the menu and press **Enter**. 
5. ☐	Check HIDS status	1. Type the **Username** and **Password** for a user that is part of the **secgrp** group.  ***Note:*** By default, **admusr** is part of the **secgrp** group. 2. Click **OK** and press **Enter**.

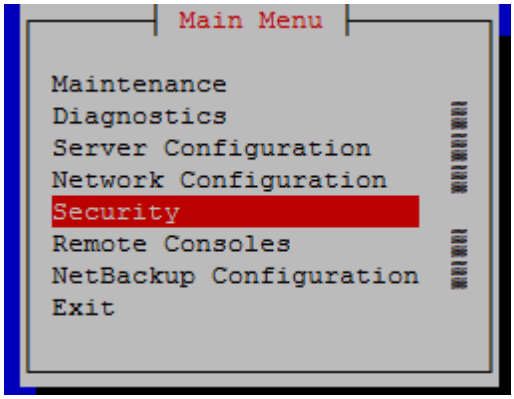
Procedure 15. Initialize HIDS		
6. ☐	Initialize HIDS	1. Select **Initialize** and press **Enter**.  2. Select **Yes** and press **Enter**. 3. After the HIDS baseline successfully initialized message displays, press any key to continue.
7. ☐	Exit	Select **Exit** in each of the menus until a command prompt is reached.

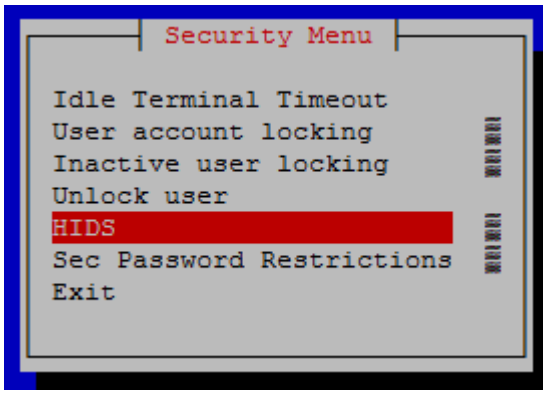
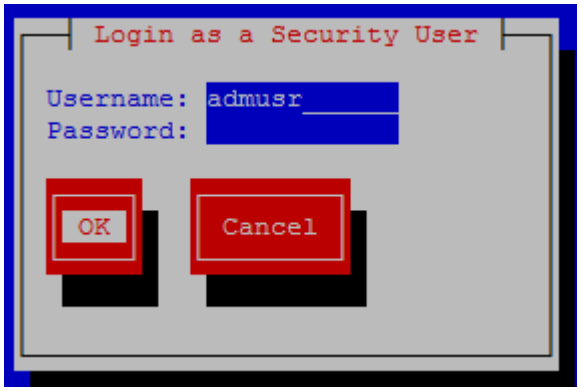
3.2.4 Enable or Disable Host Intrusion Detection System (HIDS)

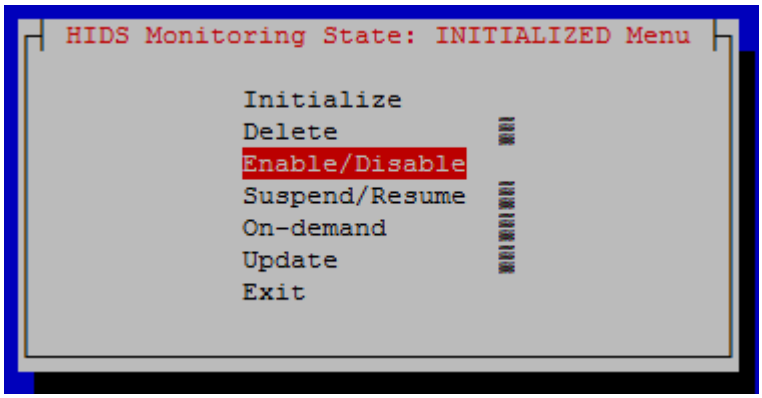
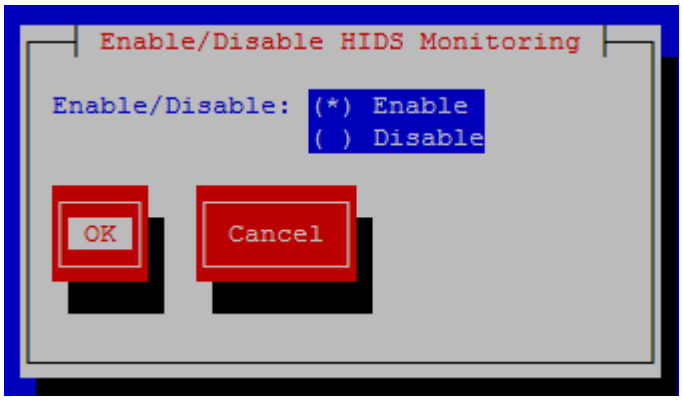
The Host Intrusion Detection System (HIDS) feature must be initialized before enabling HIDS for the first time on a system.

Procedure 16. Enable or Disable HIDS		

1. ☐	Log in to server	Log in as **admusr** on the server.
		`Login: admusr`
		`Password: <current admin user password>`

2. ☐	Open platcfg menu	Open the **platcfg** menu by entering this command: `$ sudo su - platcfg`
3. ☐	Select Security	Select **Security** from the menu and press **Enter**. 

Procedure 16. Enable or Disable HIDS		
4. ☐	Select HIDS	Select **HIDS** from the menu and press **Enter**. 
5. ☐	Check HIDS status	1. Type the **Username** and **Password** for a user that is part of the **secgrp** group.  ***Note:*** By default, **admusr** is part of the **secgrp** group. 2. Click **OK** and press **Enter**.

Procedure 16. Enable or Disable HIDS		
6. ☐	Enable/Disable HIDS	1. Select **Enable/Disable** and press **Enter**.  2. Select either the **Enable** or **Disable** option.  3. Click **OK** and press **Enter**. 4. After the message box that indicates that DB monitoring has been enabled/disabled or a failure message displays, press any key to continue.
7. ☐	Exit	Select **Exit** in each of the menus until a command prompt is reached.

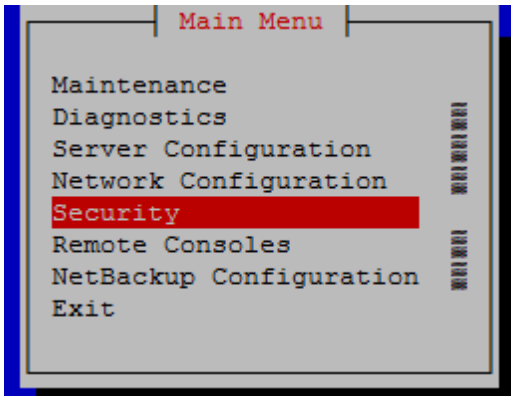
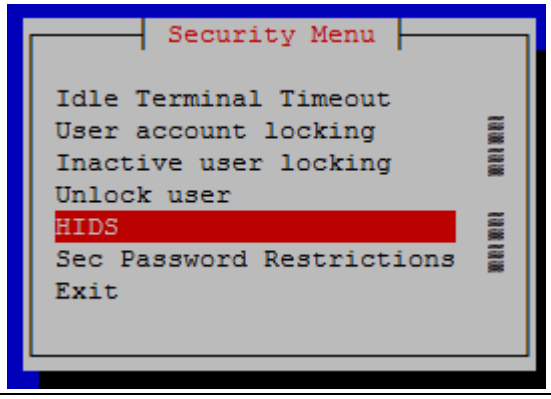
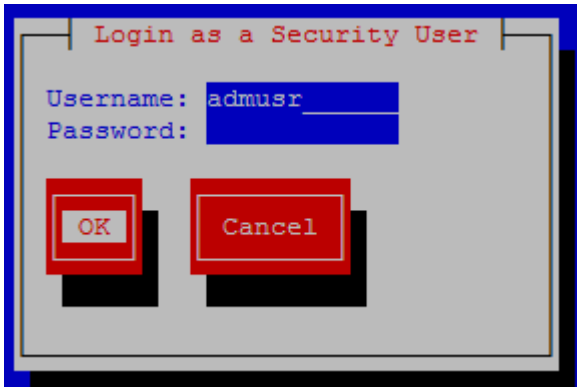
3.2.5 Suspend or Resume Host Intrusion Detection System (HIDS)

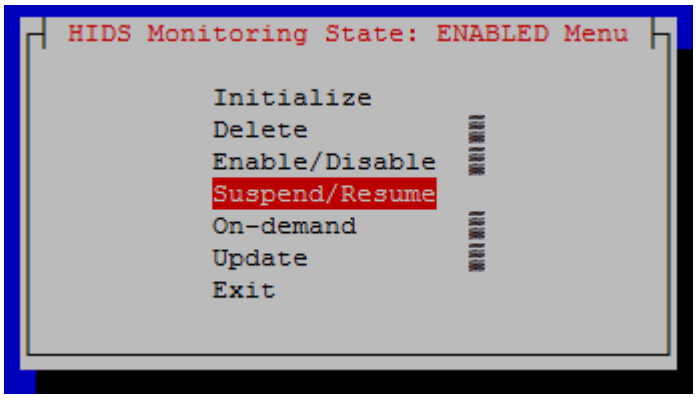
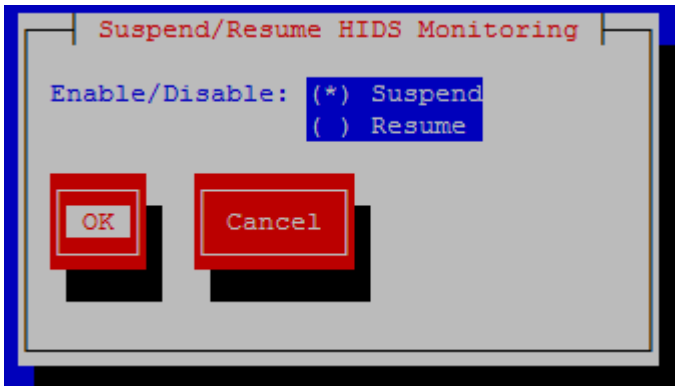
The HIDS monitoring can be temporarily suspended or resumed on a system that has HIDS enabled.

Procedure 17. Suspend or Resume HIDS		

1. ☐	Log in to server	Log in as **admusr** on the server.
		`Login: admusr`
		`Password: <current admin user password>`

2. ☐	Open platcfg menu	Open the **platcfg** menu by entering this command: `$ sudo su - platcfg`

Procedure 17. Suspend or Resume HIDS		
3. ☐	Select Security	Select **Security** from the menu and press **Enter**. 
4. ☐	Select HIDS	Select **HIDS** from the menu and press **Enter**. 
5. ☐	Check HIDS status	1. Type the **Username** and **Password** for a user that is part of the **secgrp** group.  ***Note:*** By default, **admusr** is part of the **secgrp** group. 2. Click **OK** and press **Enter**.

Procedure 17. Suspend or Resume HIDS		
6. ☐	Suspend/Resume HIDS	1. Select **Suspend/Resume** and press **Enter**.  2. Select either the **Suspend** or **Resume** option.  3. Click **OK** and press **Enter**. 4. After the message box that indicates that DB monitoring has been suspended/resumed or a failure message displays, press any key to continue.
7. ☐	Exit	Select **Exit** in each of the menus until a command prompt is reached.

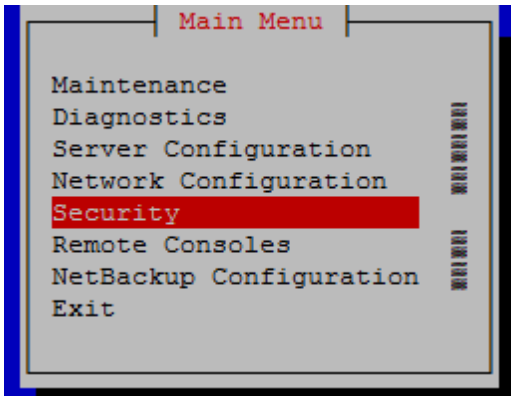
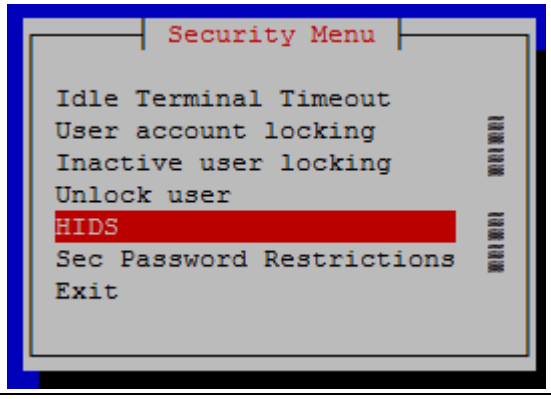
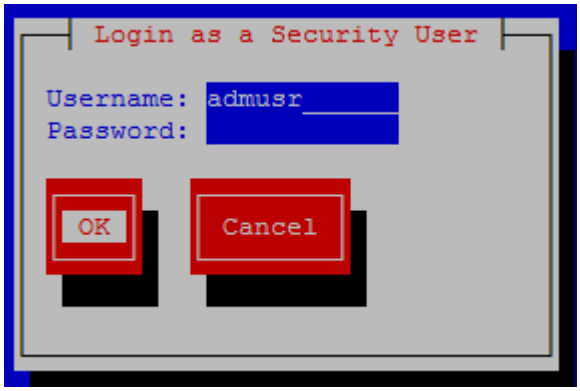
3.2.6 Run On-Demand Host Intrusion Detection System (HIDS) Security Check

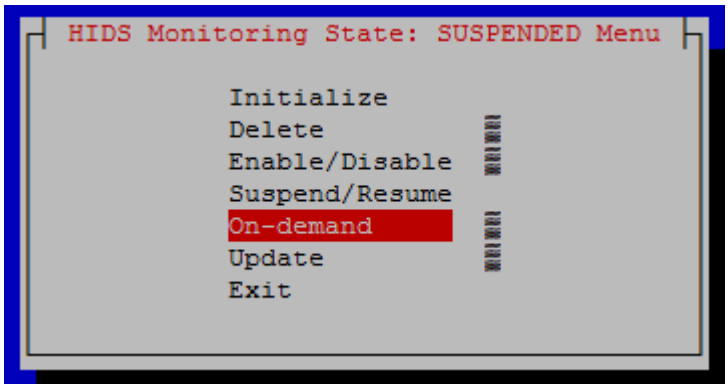
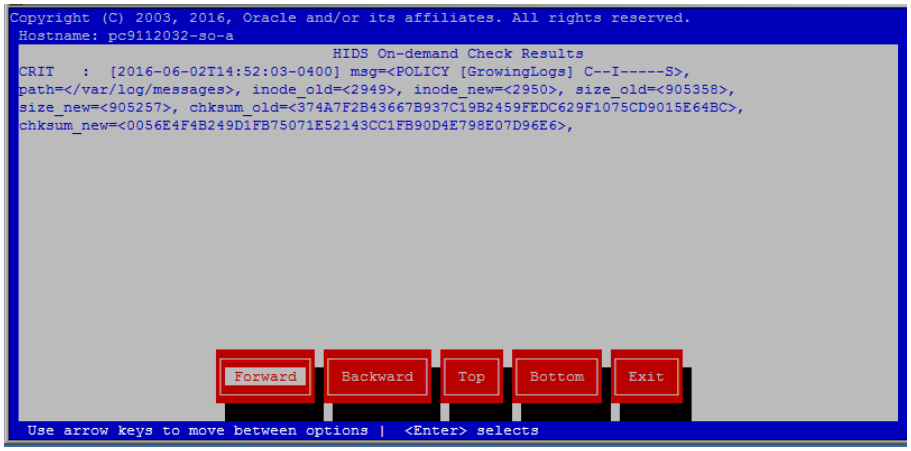
The HIDS tests run periodically. A user can force an immediate run of the HIDS tests by using the **On-demand** HIDS menu.

Procedure 18. Suspend or Resume HIDS		

8. ☐	Log in to server	Log in as **admusr** on the server.
		`Login: admusr`
		`Password: <current admin user password>`

9. ☐	Open platcfg menu	Open the **platcfg** menu by entering this command: `$ sudo su - platcfg`

Procedure 18. Suspend or Resume HIDS		
10. ☐	Select Security	Select **Security** from the menu and press **Enter**. 
11. ☐	Select HIDS	Select **HIDS** from the menu and press **Enter**. 
12. ☐	Check HIDS status	1. Type the **Username** and **Password** for a user that is part of the **secgrp** group.  ***Note:*** By default, **admusr** is part of the **secgrp** group. 2. Click **OK** and press **Enter**.

Procedure 18. Suspend or Resume HIDS		
13. ☐	On-demand HIDS	1. Select **On-demand** and press **Enter**.  2. Click **Yes** and press **Enter.** 3. After the message box that indicates the success/fail result displays, press any key to continue. If an error exists, a screen similar to the following screen displays:  This alarm can also been seen when viewing alarms in the platcfg system, as described in section 3.2.9: Host Intrusion Detection System (HIDS) Alarms. This alarm is also propagated through normal COMCOL channels ultimately resulting in the alarm being accessible on the Oracle Communications Diameter Signaling Router GUI by navigating to **Alarm & Events > View Active**, as shown in step 15.
14. ☐	Exit	Select **Exit** in each of the menus until a command prompt is reached.

Procedure 18. Suspend or Resume HIDS		
15. ☐	View HIDS error (Optional)	Log into the DSR GUI and navigate to **Alarms & Events > View Active** to view details for the HIDS error. Examples of screens from the current error follow:

Main Menu: Alarms & Events -> View Active

Thu Jun 02 15:14:41 2016 EDT

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!						

Main Menu: Alarms & Events -> View Active [Report]

Thu Jun 02 15:15:21 2016 EDT

```
                    Main Menu: Alarms & Events -> View Active [Report]
                                Thu Jun 02 15:15:21 2016 EDT
_____________________________________________________________________________

      TIMESTAMP: 2016-06-02 14:52:04.063 EDT
NETWORK_ELEMENT: SO_UDR
         SERVER: pc9112032-so-a
        SEQ_NUM: 97
   EVENT_NUMBER: 32349
       SEVERITY: MAJOR
        PRODUCT: TPD
        PROCESS: cmplatalarm
           TYPE: PLAT
       INSTANCE:
           NAME: File Tampering
          DESCR: File Tampering
       ERR_INFO:
   GN_WARNING/WRN Platform detected an error condition [cmplatalarm.cxx:194]
  ^^ Additional details captured in /var/TKLC/log/syscheck/fail_log or
/var/TKLC/log/arse/alarm.log (timestamp: 1464893524) [cmplatalarm.cxx:198]
  ^^ [6114:cmplatalarm.cxx:200]
         NSECS: 1572917444489037368
            ID: 0
_____________________________________________________________________________
```

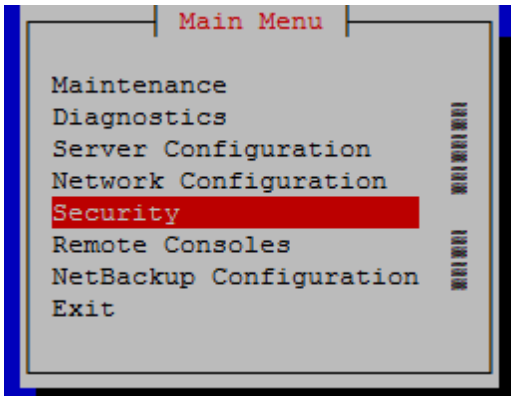
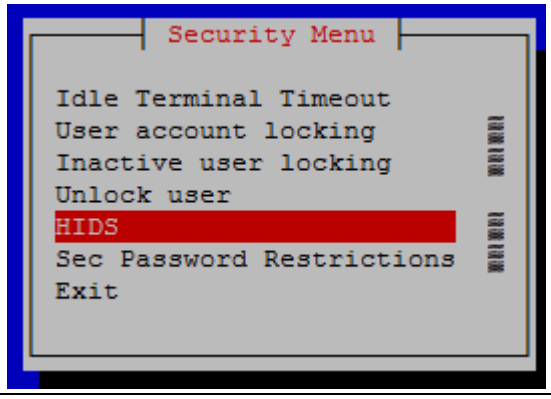
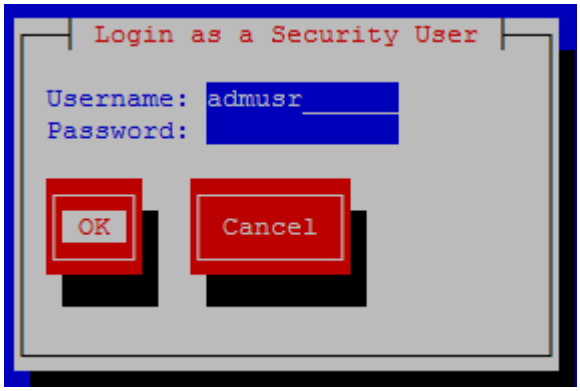
3.2.7 Update Host Intrusion Detection System (HIDS) Baseline

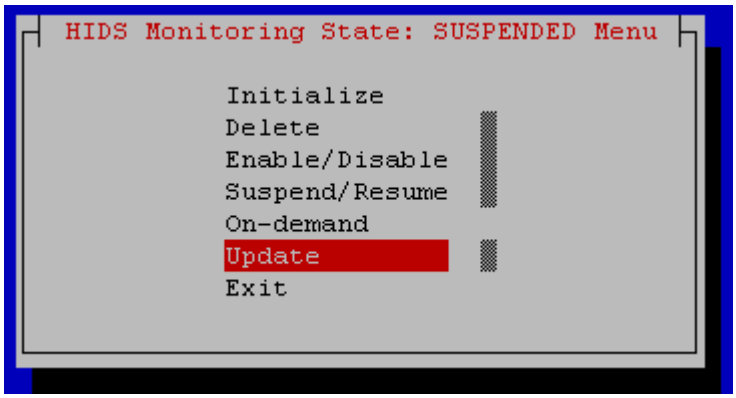
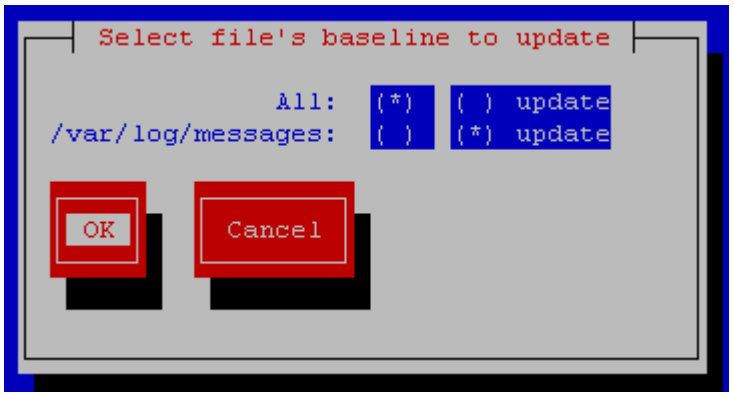
The HIDS Update menu is used to update the checksums on all files or specific files in the HIDS baseline, which can clear HIDS alarms associated with the updated files.

Procedure 19. Update HIDS		

1. ☐	Log in to server	Log in as **admusr** on the server.
		`Login: admusr`
		`Password: <current admin user password>`

2. ☐	Open platcfg menu	Open the **platcfg** menu by entering this command: `$ sudo su - platcfg`

Procedure 19. Update HIDS		
3. ☐	Select Security	Select **Security** from the menu and press **Enter**. 
4. ☐	Select HIDS	Select **HIDS** from the menu and press **Enter**. 
5. ☐	Check HIDS status	1. Type the **Username** and **Password** for a user that is part of the **secgrp** group.  ***Note:*** By default, **admusr** is part of the **secgrp** group. 2. Click **OK** and press **Enter**.

Procedure 19. Update HIDS		
6. ☐	Update HIDS	1. Select **Update** and press **Enter**.  2. Select file's baseline to update.  3. Click **OK** and press **Enter**. 4. After the message box that indicates the success/fail result displays, press any key to continue.
7. ☐	Exit	Select **Exit** in each of the menus until a command prompt is reached.

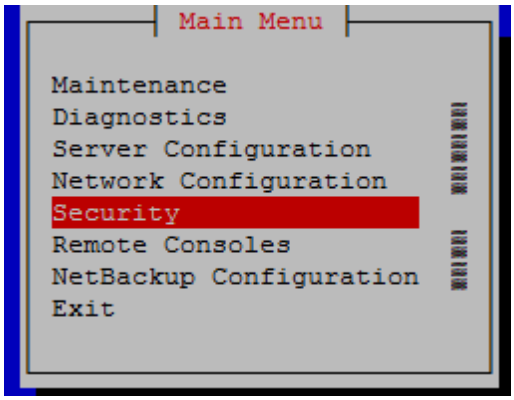
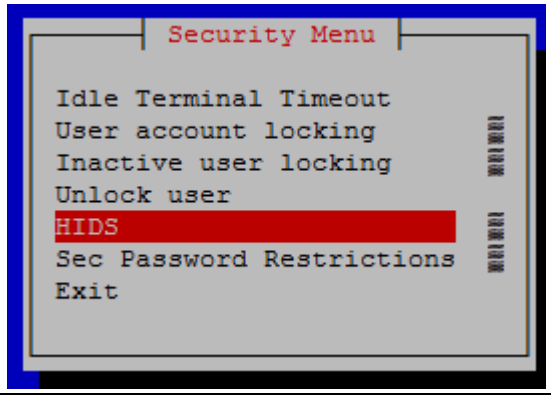
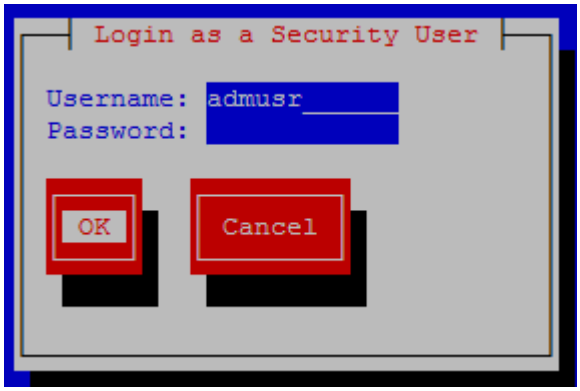
3.2.8 Delete Host Intrusion Detection System (HIDS) Baseline

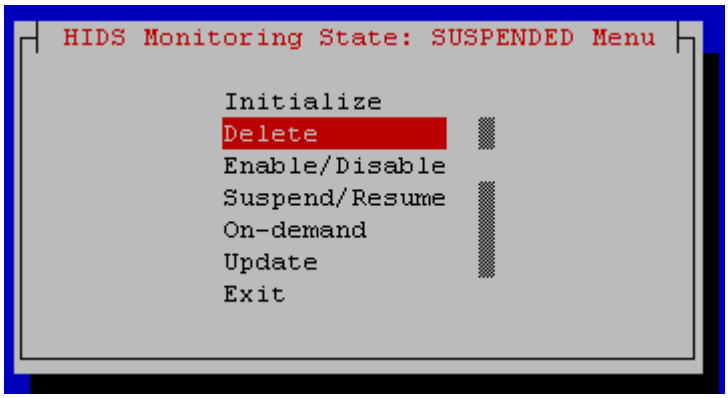
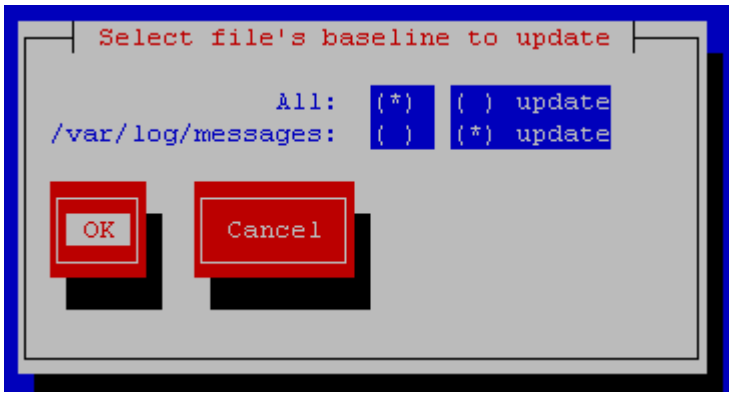
The HIDS **Delete** menu can be used for permanently disabling HIDS or for backing out of a product upgrade.

Procedure 20. Delete HIDS		

1. ☐	Log in to server	Log in as **admusr** on the server.
		`Login: admusr`
		`Password: <current admin user password>`

2. ☐	Open platcfg menu	Open the **platcfg** menu by entering this command: `$ sudo su - platcfg`

Procedure 20. Delete HIDS		
3. ☐	Select Security	Select **Security** from the menu and press **Enter**. 
4. ☐	Select HIDS	Select **HIDS** from the menu and press **Enter**. 
5. ☐	Check HIDS status	1. Type the **Username** and **Password** for a user that is part of the **secgrp** group.  ***Note:*** By default, **admusr** is part of the **secgrp** group. 2. Click **OK** and press **Enter**.

Procedure 20. Delete HIDS		
6. ☐	Delete HIDS	1. Select **Delete** and press **Enter**.  2. Select file's baseline to update.  3. Click **OK** and press **Enter**. 4. After the message box that indicates the success/fail result displays, press any key to continue.
7. ☐	Exit	Select **Exit** in each of the menus until a command prompt is reached.

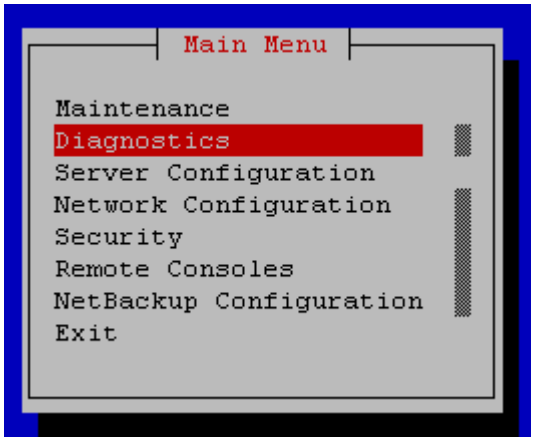
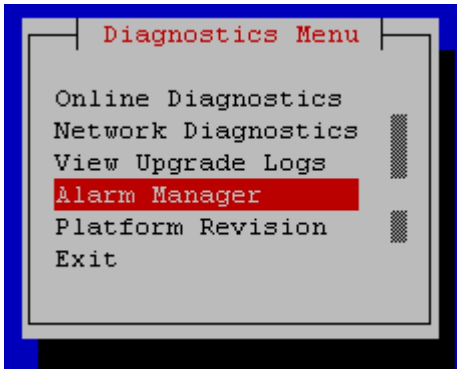
3.2.9 Host Intrusion Detection System (HIDS) Alarms

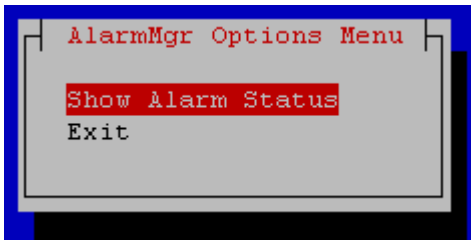
HIDS alarms can be viewed using multiple methods. HIDS alarms are standard TPD alarms with the alarmEventType set to **securityServiceOrMechanismViolation**. The HIDS alarms are propagated through normal COMCOL channels ultimately resulting in SNMP traps being sent to the customer's SNMP management system, 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 DSR GUI on the **Main Menu -> Alarms & Events -> View Active** GUI screen.
- Customers can view active alarms on the platcfg GUI, including HIDS alarms, by using the following steps:

Procedure 21. View HIDS Alarms		

1. ☐	Log in to server	Log in as **admusr** on the server.
		`Login: admusr`
		`Password: <current admin user password>`

2. ☐	Open platcfg menu	Open the **platcfg** menu by entering this command: `$ sudo su - platcfg`
3. ☐	Select Diagnostics	Select **Diagnostics** from the menu and press **Enter**. 
4. ☐	Select Alarm Manager	Select **Alarm Manager** from the menu and press **Enter**. 

Procedure 21. View HIDS Alarms		
5. ☐	View Alarm status	1. Select **Show Alarm Status** from the menu and press **Enter**.  2. After the message box that indicates the success/fail result displays, press any key to continue. If an error exists, a screen similar to the following screen displays: 
6. ☐	Exit	Select **Exit** in each of the menus until a command prompt is reached.

3.3 Oracle Communications Diameter Signaling Router OS Standard Features

This section explains the security features of Oracle Communications Diameter Signaling Router 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 NTP Servers

Each server that is being added at the NOAM server under **Administration > Configuration > Servers** has the option to specify the NTP server details. The NTP servers field is visible after selecting a network element. The following screen displays a configured server with NTP server details.

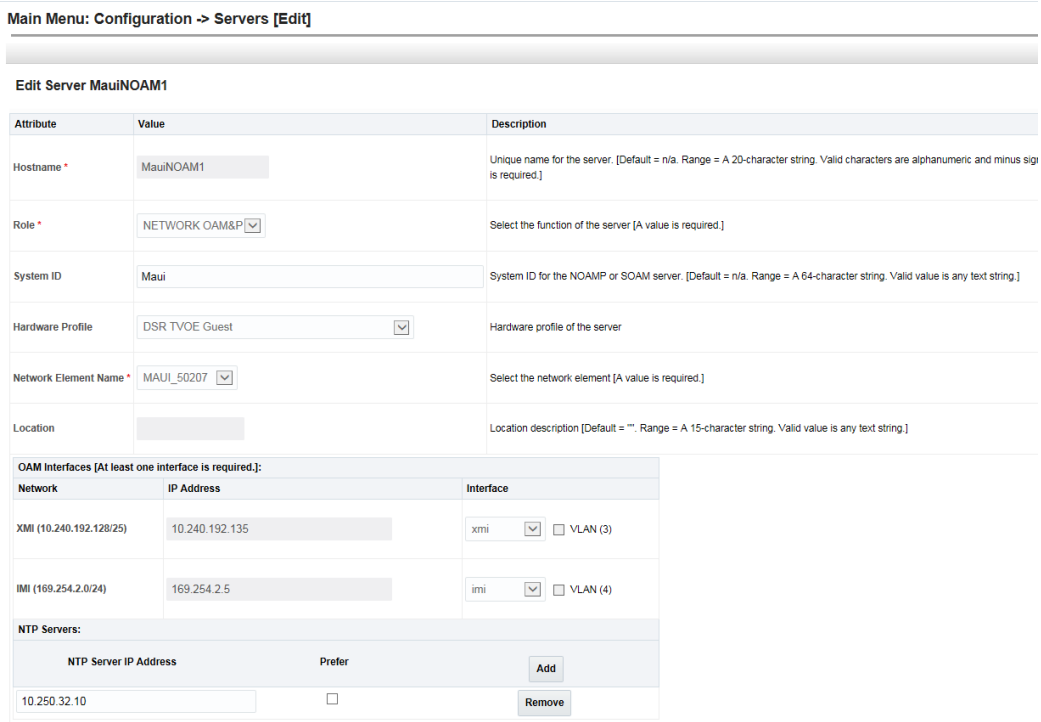
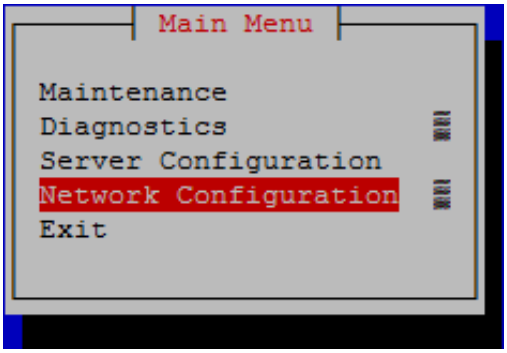


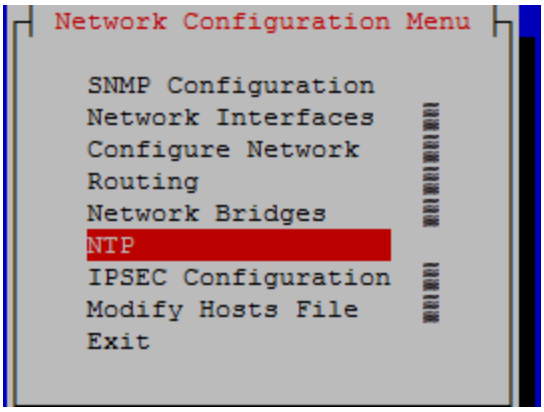
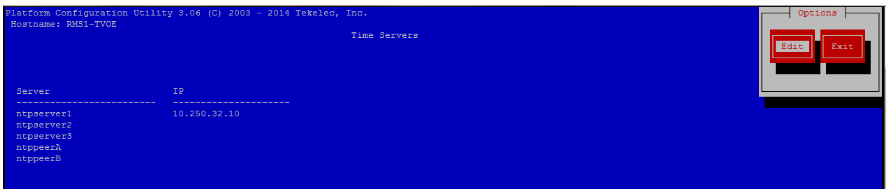
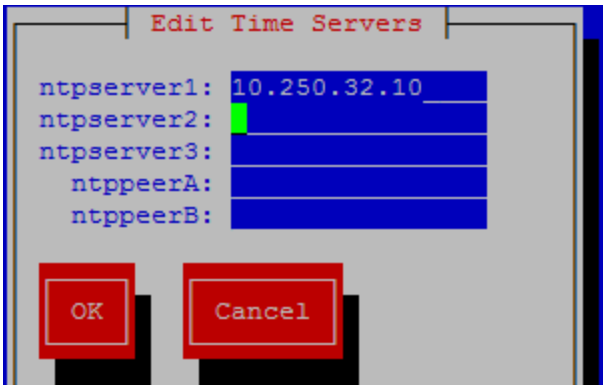
Figure 5. NTP Configuration (GUI)

For details on adding a server, see the Inserting a Server section under the Servers chapter in [1] Operation, Administration, and Maintenance (OAM) Guide.

3.3.1.1 Configure NTP for the Host OS of the Application guest VM (TVOE)

To configure the NTP setting for the host Operating System hosting the application guest (for example, TVOE), follow these instructions:

Procedure 22. Configure NTP for the Host OS of the Application Guest VM		
1. ☐	Log in to TVOE server	Log in or switch user to platcfg user on the TVOE server. The platcfg main menu displays.
2. ☐	Select Network Configuration	Navigate to **Network Configuration**. 

Procedure 22. Configure NTP for the Host OS of the Application Guest VM		
3. ☐	Select NTP	1. Select **NTP**.  2. The Time Servers screen shows the configured NTP servers and peers. Click **Edit**. 
4. ☐	Enter NTP server information	On the Edit Time Servers menu, enter the NTP Server information and click **OK**. 
5. ☐	Exit TVOE	1. Exit the platcfg menu. 2. Ensure the time is set correctly by executing the steps in the 3.3.2 Set the Time on the TVOE Host.

3.3.2 Set the Time on the TVOE Host

At the time of DSR installation, the date and time is set on TVOE hosts as follows:

Log in as **admusr** and execute these commands:

```
$ sudo /sbin/service ntpd stop
$ sudo /usr/sbin/ntpdate ntpserver1
$ sudo /sbin/service ntpd start
```

These steps synchronize the time to the NTP server.

3.3.3 Configure Password Settings for OS Users

Use the following procedure to configure various password settings including:

- Minimum password length
- Minimum time between password changes
- Maximum number of days that a password can be used
- Warning time for password expiration
- Minumum number of character differences between passwords
- Password history size (prevents reusing passwords)

Here are the steps:

Procedure 23. Configure Password Settings 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 this command: `$ sudo su - platcfg`
3. ☐	Select **Security** from the menu and press **Enter**.
4. ☐	Select **Sec Password Restrictions** option and press **Enter**
5. ☐	Select **Global Password Restrictions for New Users** and press **Enter**

6. ☐	Fill out the appropriate settings:
	`Minimum acceptable size for the new password: 15`
	`Minimum number of days allowed between password changes: 0`
	`Maximum number of days a password may be used: 99999`
	`Number of days a user is warned before password expiration: 7`
	`Minimum number of characters different between passwords: 0`
	`Minimum number of passwords between reuse: 5`

7. ☐	Click **OK** and press **Enter**.
8. ☐	Select **Exit** in each of the menus until a command prompt is reached.

If you need to also ensure that the login name is not embedded in user passwords, the following procedure can be used to configure this:

Procedure 24. Don't Allow Usernames to be Embedded in Passwords	

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

Procedure 24. Don't Allow Usernames to be Embedded in Passwords	
2. ☐	Check out the system-auth-ac file: `$ sudo rcstool co /etc/pam.d/system-auth-ac`

3. ☐	Add the reject_username setting to the system-auth-ac file:
	`$ sudo sed -i -e '/^password.*reject_username/n' \`
	`-e '/^password.*pam_cracklib.so.*$/s/$/ reject_username/' \`
	`/etc/pam.d/system-auth-ac`

4. ☐	Check in the `system-auth-ac` file: `$ sudo rcstool ci /etc/pam.d/system-auth-ac "reject_username"`

3.3.4 Configure Other Session and Account Settings for OS Users

This procedure sets various session and account settings for OS users:

- Session inactivity
- Account locking for invalid login attempts
- Account locking for inactive accounts

Procedure 25. Configure Session Inactivity 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 this command: `$ sudo su - platcfg`
3. ☐	Select **Security** from the menu and press **Enter**.
4. ☐	Select **Idle Terminal Timeout** option from the security menu and enter the desired value in minutes for the **Idle Terminal Timeout** field.
5. ☐	Click **OK** and press **Enter**.
6. ☐	Select **Exit** in each of the menus until a command prompt is reached.

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

Procedure 26. Lock OS User Accounts After Too Many Failed Login Attempts	

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

2. ☐	Open the platcfg menu by entering this command: `$ sudo su - platcfg`

Procedure 26. Lock OS User Accounts After Too Many Failed Login Attempts	
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>`
	Click **OK** and press **Enter**.

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

This procedure sets the lockout time for inactive accounts.

Procedure 27. Lock Inactive OS User Accounts	

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

2. ☐	Open the platcfg menu by entering this command: `$ sudo su - platcfg`
3. ☐	Select **Security** from the menu and press **Enter**.
4. ☐	Select **Inactive user locking** from the menu and press **Enter**.

5. ☐	Fill out the following settings:
	`Feature: ( ) disable (*) enable`
	`Deny after # of days of inactivity: <max tries>`
	Click **OK** and press **Enter**.

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

3.3.5 Update the TPD-Provd Cipher List

The procedure for this update defines the methods required to update the TPD-Provd cipher list and how to verify the update was successful. For more detailed steps on performing these methods, refer to Appendix P in [6] PMAC Configuration Guide.

3.3.6 Operational Dependencies on Platform Account Passwords

This section describes the operational dependencies on platform account passwords to provide guidance in cases when the customer insists on modifying a default password. Note that changing passwords should be attempted only on systems that are fully configured and stable. Modifying passwords during

system installation is strongly discouraged. For more detailed steps on performing these methods, refer to Appendix H in [6] PMAC Configuration Guide.

3.3.7 Update the SELinux mode to 'permissive'

By default, DSR ships with the SELinux mode as 'disabled'. Execute the below procedure to update the SELinux mode to 'permissive'. 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.

For A - level and B - level servers the sequence of execution should be Spare -> Stand-by -> Active.

Procedure 28. Update SELinux mode on the server	

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

2.	Check out the file `config` and update the SELinux state to 'permissive' :
	`$ sudo rcstool co /etc/selinux/config`
	`$ sudo sed -i 's/^SELINUX=.*$/SELINUX=permissive/g' /etc/selinux/config`

3. ☐	Check in the file `config`: `$ sudo rcstool ci /etc/selinux/config`
4.	Reboot the server : `$ sudo init 6`

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 Require Authentication for Single User Mode

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

Procedure 29. Require Authentication for Single User Mode	

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

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

3. ☐	If no result is returned then execute below command:
	`$ sudo echo "SINGLE=/sbin/sulogin" >> /etc/sysconfig/init`
	
	If some result is returned by executing Step 2, the execute the below command:
	`$ sudo sed -i "s/SINGLE.*/SINGLE=\/sbin\/sulogin/g" /etc/sysconfig/init`

Procedure 29. Require Authentication for Single User Mode	
4. ☐	Check in the file `init`: `$ sudo rcstool ci /etc/sysconfig/init`

3.4.2 Change OS User Account Passwords

All OS accounts that need to change the respective default passwords, use this procedure to change default passwords.

Procedure 30. Change OS User Account 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 steps 1 and 2 for all servers.

3.4.3 Change Login Display Message

Use this procedure to change the Login Display Message.

Procedure 31. Change Login Display Message	

1. ☐	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. ☐	1. Edit the **sshd** configuration file.
	`$ sudo rcstool co sshd_config`
	`$ sudo vi sshd_config`
	2. Uncomment and edit this line:
	`$ Banner /some/path`
	3. To this:
	`Banner /etc/ssh/sshd-banner`
	4. Save and exit the **vi** session.

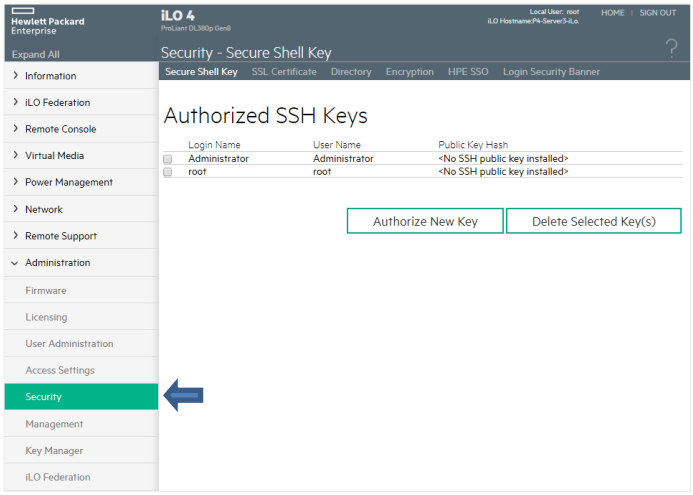
Procedure 31. Change Login Display Message	
4. ☐	1. Edit the banner file. `$ sudo vi sshd-banner` 2. Add and format the desired text. Save and exit the **vi** session.
5. ☐	Restart the **sshd** service. `$ sudo service sshd restart`

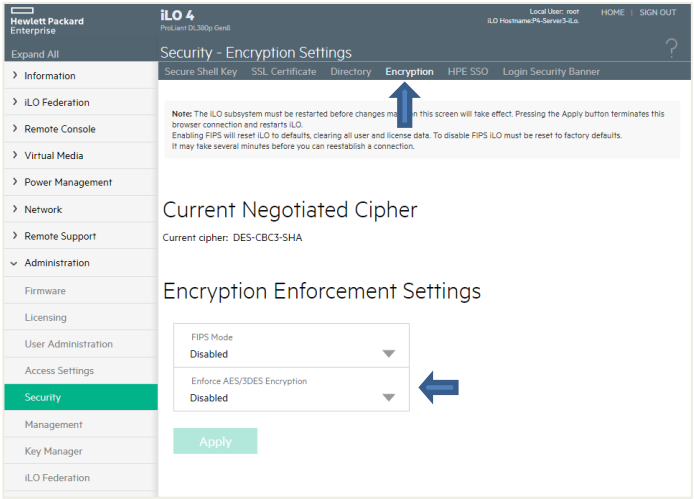
6. ☐	1. Test the change. Repeat steps 4 and 5 until the message is formatted correctly.
	`$ sudo ssh <current server name>`
	2. Verify message line feeds are formatted correctly.
	`$ exit`

7. ☐	Check the files into **rcs** to preserve changes during upgrades.
	`$ sudo rcstool init /etc/ssh/sshd-banner`
	`$ sudo rcstool ci sshd_config`

3.4.4 Force iLO to Use Strong Encryption

Log in as an administrator to the iLO and execute these steps.

Procedure 32. Force iLO to Use Strong Encryption	
1. ☐	On the Administration menu, click **Security**. 

Procedure 32. Force iLO to Use Strong Encryption	
2. ☐	Select the Encryption tab and, under Encryption Enforcement Settings, set the Enforce AES/3DES Encryption to **Enabled**. 
3. ☐	1. Click **Apply**. 2. Logout and wait 30 seconds before logging back in.

3.4.5 Set Up rsyslog for External Logging

Use this procedure to set up rsyslog for external logging to a central server from NOAMs and SOAMs.

Procedure 33. Set Up rsyslog for External Logging	

1. ☐	Log in as **admusr** on the source 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 are 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.

3.4.6 Add 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.

Here is one procedure for requiring that a password be used with all sudo access by the admusr account:

Procedure 34. Require admusr to Enter a Password to Run Commands Using sudo	

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

2. ☐	Check out the `plat.admusr.sudo` file: `$ sudo rcstool co /usr/TKLC/plat/etc/sudoers.d/plat.admusr.sudo`

3. ☐	Suppress the NOPASSWD line:
	`$ sudo sed -i '/^%admgrp ALL = NOPASSWD: ALL$/ s/^/#/' \`
	`/usr/TKLC/plat/etc/sudoers.d/plat.admusr.sudo`

4. ☐	Check in the plat.admusr.sudo file:
	`$ sudo rcstool ci /usr/TKLC/plat/etc/sudoers.d/plat.admusr.sudo`
	`"require password"`

After making this change, all uses of sudo by admusr require the admusr password be entered. Existing documentation does not and will not indicate this.

The sudo configuration file is constructed from piece parts; the syntax is also complex and editing mistakes could leave a system without needed access. For this reason, details of the configuration rules are available through Oracle Help Center (OHC) or by opening a ticket with Oracle technical support.

3.4.7 Report and Disable Expired OS User Accounts

Procedure to report and disable expired user accounts.

Procedure 35. Report and Disable Expired OS User Accounts	

1. ☐	Log in as **admusr** 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 displays the users who have not logged in over N number of days. It also shows 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. ☐	1. Disable the user accounts identified by the lastlog report. `$ sudo passwd -l <user acct>` 2. Repeat this step for each user account you want to disable.
4. ☐	1. To re-enable an account: `$ sudo passwd -u <user acct>` 2. 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 Configure SNMP in Switches

It is essential that all switches have been configured successfully using the procedures in references [3] and [4].

- Configure Cisco 3020 switch (netConfig), and/or
- Configure HP 6120XG switch (netConfig), and/or
- Configure Cisco 4948/4948E/4948E-F (netConfig).

Procedure 36. Report and Disable Expired OS User Accounts	
1. ☐	Log into the server as root user and list all the configured switches by typing this command: `# netConfig --repo listDevices` Refer to application documentation to determine which switches to add/remove from the community string, making a note of the DEVICE NAME of each switch. This is used as <switch_name>.
2. ☐	For any given switch by switch name, display SNMP community information by typing this command: `# netConfig getSNMP --device=<switch_name>`

Procedure 36. Report and Disable Expired OS User Accounts	

3. ☐	1. For any given switch by switch name, display its SNMP trap information by typing this command:
	`#netConfig listSNMPNotify --device=<switch_name>`
	Note: If the Could not lock device displays, type this command to clear the lock to proceed:
	`# netConfig --wipe --device=<switch_name>`
	2. Reply **y** if prompted.

3.5.2 Configure Community Strings

1. To add a community string to ANY switch by switch name, type this command with appropriate switch name:

```
#netConfig addSNMP --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 this command:

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

3.5.3 Configure Traps

1. To add a trap server, type this 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, type this 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 6120XG, 6125G, and 6125XLG switches. 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 the [1] Operation, Administration, and Maintenance (OAM) 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 the Alarms and Events and Security Log chapters in [2] Alarms, KPIs, and Measurements Reference and [1] Operation, Administration, and Maintenance (OAM) 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 works for both IPv4 and IPv6 on the Diameter interface. The provisioning interface only supports IPsec on IPv4.

Note: Oracle Communications Diameter Signaling Router supports IPsec with an SCTP/IPv6 configuration.

3.7.1.1 Encapsulate Security Payload

Oracle Communications Diameter Signaling Router 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. These main differences exist between IKEv1 and IKEv2:

- IKEv1
  - Security associations are established in in 8 messages
  - Does not use a Pseudo Random Function

- IKEv2
  - Security associations are established in in 4 messages
  - Uses an increased number of encryption algorithms and authentication transformations
  - 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. IKEv2 is more secure and should be the preferred option.

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:

- **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.
- 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 does not occur until the security associations have expired and the renegotiation can begin.

3.7.3 Pre-requisite Steps for Setting Up IPsec

Run these steps once on the active NOAMP server before configuring IPsec.

1. Log in as root on the active NOAMP server.
2. On the active NOAMP server, type the following commands:

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

3.7.4 Set 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 Add 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 Enable and Disable an IPsec Connection.
5. Logout of **platcfg**.
6. Restart IPsec service by typing this command:

```
# service ipsec restart
```

3.7.5 IPsec IKE and ESP Elements

Table 3. IPsec IKE and ESP Elements 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)

Description	Valid Values	Default
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 does not re-establish 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 does not occur until the 60 minutes expire. The recommendation is to set the lifetime to the lowest possible time that does not impact network connectivity, such as 3-5 minutes.	Number of time units	60
Lifetime Units	hours, mins, secs	mins
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 Add an IPsec Connection

Procedure to add an IPsec connection:

Procedure 37. Add an IPsec Connection	

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

2. ☐	Open the **platcfg** menu by entering this command: `$ sudo su - platcfg`
3. ☐	1. Select **Network Configuration**. 2. Select **IPsec Configuration**. 3. Select **IPsec Connections**. 4. Click **Edit**.
4. ☐	1. Select **Add Connection**. 2. Select the Internet Key Exchange Version: either **IKEv1** or **IKEv2**. 3. Complete the **IKE Configuration** fields for the desired connection, then click **OK**. The fields are described in Table 3. IPsec IKE and ESP Elements.

Procedure 37. Add an IPsec Connection	
5. ☐	Select the desired ESP Encryption algorithm, and click **OK**. The fields are described Table 3. IPsec IKE and ESP Elements.
6. ☐	Complete the **Add Connection** fields for the desired connection. 1. Enter the **Local Address**. 2. Enter the **Remote Address**. 3. Enter the **Pass Phrase**. ***Note:*** Select a non-trivial passphrase. 4. Select the **Mode**.
7. ☐	Click **OK**. Wait for the connection to be added. When the connection has been successfully added, the Internet Key Exchange Version menu displays.
8. ☐	Select **Exit** in each of the menus until a command prompt is reached.

3.7.7 Edit an IPsec Connection

Procedure to edit an IPsec connection:

Procedure 38. Edit an IPsec Connection	

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

2. ☐	Open the platcfg menu by typing this command. `$ sudo su - platcfg`
3. ☐	1. Select **Network Configuration**. 2. Select **IPsec Configuration**. 3. Select **IPsec Connections**. 4. Click **Edit**.
4. ☐	1. Select **Edit Connection**. 2. Select **IPsec connection** to edit. 3. View the IPsec connection's current configuration. 4. Click **Edit**.
5. ☐	1. Select either **IKEv1** or **IKEv2**. 2. Complete the **IKE Configuration** fields if needed, then click **OK.** The fields are described in Table 3. IPsec IKE and ESP Elements.

Procedure 38. Edit an IPsec Connection	
6. ☐	1. Select the desired **ESP Configuration** fields, then click **OK**. 2. The fields are described in Table 3. IPsec IKE and ESP Elements. 3. Complete the Add Connection fields for the desired connection. a. Type the **Local Address**. b. Type the **Remote Address**. c. Type the **Pass Phrase**. d. Select the **Mode**.
7. ☐	1. Click **OK**. 2. Select **Yes** to restart the connection. When the connection has been successfully updated, the Internet Key Exchange Version menu displays.
8. ☐	Select **Exit** in each of the menus until a command prompt is reached.

3.7.8 Enable and Disable an IPsec Connection

Procedure to enable or disable an IPsec connection:

Procedure 39. Enable/Disable an IPsec Connection	

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

2. ☐	Open the platcfg menu by typing this command. `$ sudo su - platcfg`
3. ☐	1. Select **Network Configuration**. 2. Select **IPsec Configuration**. 3. Select **IPsec Connections**. 4. Click **Edit**.
4. ☐	1. Select **Edit Connection**. 2. Select **IPsec connection** to edit. 3. View the IPsec connection's current configuration. 4. Click **Edit**.
5. ☐	1. Select **Connection Control**. 2. Select **IPsec connection** to enable or disable. 3. Select **Enable** or **Disable.**
6. ☐	Click **OK** to enable or disable the selected IPsec connection.

Procedure 39. Enable/Disable an IPsec Connection	
7. ☐	Select **Exit** in each of the menus until a command prompt is reached.

3.7.9 Delete an IPsec Connection

Procedure to delete an IPsec connection.

Procedure 40. Delete an IPsec Connection	

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

2. ☐	Open the platcfg menu by typing this command. `$ sudo su - platcfg`
3. ☐	1. Select **Network Configuration**. 2. Select **IPsec Configuration**. 3. Select **IPsec Connections**. 4. Click **Edit**.
4. ☐	1. Select **Delete Connection**. 2. Select IPsec connection to delete. 3. Click **Yes** to confirm the delete.
5. ☐	Wait for the connection to be deleted. When the IPsec connection has been successfully deleted, the Connection Action menu displays.
6. ☐	Select **Exit** in each of the menus until a command prompt is reached.

3.8 Firewall Configuration Changes

3.8.1 Iptables

DSR 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 DSR product support.

3.8.2 TCP Wrappers

DSR 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 DSR product support.

3.9 Internal Web Services

DSR uses a number of internal web services in support of centralized configuration and management. These services use the SOAP protocols and implement WS-Security profiles to authenticate internal clients. These services ship with self-signed certificates and default passwords; you should plan to update the default passwords at install time, and you may wish to also replace the self-signed certificates with certificates signed by a trusted authority. The following sections provide procedures to perform these actions.

3.9.1 Changing the Internal Web Service Passwords

In general, shortly after initial configuration is complete and before deploying / turning up services – you should update the internal web service passwords.

3.9.1.1 Changing the TPD Web Service Password

Use the following procedures to change the OS-level provisioning web service password:

Procedure 41. Update TPD Web Service Password on Active NO	

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

2. ☐	1. Reset the TPD web service password by running:
	`$ /usr/TKLC/appworks/bin/resetTpdPassword`
	2. You are prompted to provide a password:
	`password: <enter the new password>`

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

4. ☐	Verify that the web service is still functional:
	`$ AppWorks Network interfaces`
	You should see a list of network interfaces reported by the Web Service backend:
	`{`
	`"element":[`
	`"eth0",`
	`"eth1"`
	`]`
	`}`

This update command synchronizes the TPD web service (`tpdprovd`) 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. If any servers were not reachable when this command is run, run the command again later when those servers are reachable.

Some DSR deployments include a PMAC system to support installation and growth; once you update the servers in the DSR topology, the PMAC loses the ability to inventory deployed DSR nodes. You can restore the inventory function by running this procedure on the PMAC:

Procedure 42. Update TPD Web Service Password on PMAC	

1. ☐	Log in as **admusr** on the **PMAC server**.
	`Login: admusr`
	`Password: <current admin user password>`

2. ☐	1. Reset the TPD web service password by running:
	`$ sudo /usr/TKLC/smac/bin/updateCredentials -type=tpdPlatCfg`
	2. You are prompted to provide a password:
	`password: <enter the same password used in the procedure above>`

3. ☐	The command adds the password to the credential cache on the PMAC server.

3.9.1.2 Changing the Configuration Web Services Password

Use the following procedure to change the configuration web services password:

Procedure 43. Update Configuration Web Service Password on Active NO	

1. ☐	Log in as **admusr** on the active NOA server.
	`Login: admusr`
	`Password: <current admin user password>`

2. ☐	Reset the TPD web service password by running: `$ /usr/TKLC/appworks/sbin/resetSoapPassword` You are **not** be prompted for a password; the `resetSoapPassword` command generates a large random string which is used as the new password.
3. ☐	The command copies and installs the new password to each reachable server in the topology, and flushes client password caches. You might see output related to these activities.
4.	Restart all the servers in the topology from active NOA GUI: Log in to active NOA GUI – Main Menu -> Status & Manage -> Server Restart all the servers in the topology in below mentioned order a. Restart the Non-Active OAM Servers i.e. Standby/Spare NO, Standby/Spare SO, DR-NO. b. Restart all the C-Level Servers. c. Restart the Active OAM Servers i.e. Active NO, Active SO.

5. ☐	Verify that the web service is functional:
	`$ AppWorks Alarms getData`
	You should see a list of active alarms as reported by the Web Service backend:
	`[`
	`<alarm list (if any)>`
	`]`

This update command synchronizes the configuration web services password on all reachable servers in the topology. After running this command, any servers added to the topology is configured to use the new password. If any servers were not reachable when this command is run, run the command again later when those servers are reachable.

Some DSR deployments include an IDIH system to support message trace and debugging; once you update the servers in the DSR topology, IDIH loses the ability to interact with the deployed DSR nodes. You can restore the IDIH function by running this procedure on the IDIH:

Procedure 44. Update Configuration Web Service Password on IDIH	

1. ☐	Log in as **admusr** on the active NOA server.
	`Login: admusr`
	`Password: <current admin user password>`

2. ☐	Retrieve the current configuration web services password in plaintext; this is needed below in step 4:
	`$ /usr/TKLC/appworks/bin/aw.wallet credential get cmsoapa password`
	The command prints the current plain text configuration web service password. For example:
	`7w57q9U0OvOtKtgtLVTMajDcXfhCj2F4nyXw45qK6EXNHA9jACyQ`

3. ☐	Log in as **admusr** on the IDIH application server.
	`Login: admusr`
	`Password: <current admin user password>`

4. ☐	Change the user to tekelec by executing sudo su – tekelec command.
	Reset the configuration web service password by running:
	`$ cd /usr/TKLC/xIH/apps/trace-refdata-adapter/`
	`$ ./resetSoapPassword.sh`
	You are prompted to provide a password:
	`password: <enter the password from step 2>`

5. ☐	The command stores the new SOAP password into IDIH Oracle database

6. ☐	After executing the command in Step4, the WebLogic application server has to be restarted on IDIH application server.
	Type **exit** to become **admusr**.
	`sudo service xih-apps stop`
	`sudo service xih-apps start`
	The Weblogic server may take a few minutes to resume its service after executing the command.
	Notes:
	• TraceRefDataAdapter(TRDA) sync must happen automatically after WebLogic server has been restarted. If TRDA sync does not happen automatically, then execute the following command to sync IDIH with DSR : As tekelec user, navigate to **/usr/TKLC/xIH/apps/trace-refdata-adapter** directory and execute the command "**./trda-config.sh** < SOAM VIP >", where <SOAM VIP> is a place-holder for SOAM VIP address.
	• To verify TRDA sync, please look into application.log in the path:
	`/var/TKLC/xIH/log/apps/weblogic/apps/application.log`
	Ensure that this log does not show any java exceptions.

3.9.2 Changing the Internal Web Service Certificates and Key Material

In general, the TPD and Configuration web services are configured to work with self-signed certificates; it is possible to replace these certificates using the procedures outlined in this section.

The following procedure assumes that you have already obtained a signed certificate / key file from the customer's certificate authority, and that these files are in PEM format. Each server in the topology needs

its own certificate/key pair; the certificate should have a DN field that matches the hostname of the server. The procedures below assume the customer provides files following this naming convention:

- <hostname>_crt.pem – a PEM encoded X.509 certificate for the host <hostname>
- <hostname>_priv.pem – a PEM encoded private key for the host <hostname>

The private key file should not be protected with a passphrase.

Procedure 45. Create and Distribute a Combined Certificate/Key PEM File	

1. ☐	Log in as **admusr** on the active NOA server.
	`Login: admusr`
	`Password: <current admin user password>`

2. ☐	Copy all of the `<hostname>_crt.pem` and `<hostname>_priv.pem` files to the home directory for admusr on the active NOA using a utility such as `scp` or `rsync`.

3. ☐	1. Confirm each of the cert/key pairs are compatible (assume `<hostname>` is **noa**):
	`$ openssl rsa -noout -in noa_priv.pem | openssl md5`
	`(stdin)= d41d8cd98f00b204e9800998ecf8427e`
	`$ openssl x509 -noout -in noa_crt.pem | openssl md5`
	`(stdin)= d41d8cd98f00b204e9800998ecf8427e`
	2. Verify the md5 output matches for each `<hostname>` certificate/private key pair. Additionally, the md5 should be different for different `<hostnames>`.

4. ☐	1. Combine the certificate/private key pair into a single PEM file (assume `<hostname>` is **noa**): `$ cat noa_priv.pem noa_crt.pem > noa.pem` 2. Repeat for each `<hostname>`.
5. ☐	1. Copy the key pair to the server (again, assume `<hostname>` is **noa**): `$ scp noa.pem admusr@noa:` 2. Repeat for each `<hostname>`.

After this procedure is completed, you should have one combined certificate/private key pair PEM file for each server in the topology. Next, log into each server in the topology and install the combined PEM file.

Procedure 46. Install a Combined PEM File on Each Distinct <hostname>	
1. ☐	Log in as **admusr** on the **<hostname>** (assume `<hostname>` is **noa**). `$ ssh admusr@noa`

2. ☐	Copy your new certificate/private key pair PEM file into place (assume `<hostname>` is **noa**):
	`$ sudo cp noa.pem /usr/TKLC/plat/etc/ssl/`
	`$ sudo chown root:ssl /usr/TKLC/plat/etc/ssl/noa.pem`
	`$ sudo chmod 640 /usr/TKLC/plat/etc/ssl/noa.pem`

3. ☐	Replace the existing combined certificate/private key file with the new file:
	`$ sudo mv /usr/TKLC/plat/etc/ssl/server.pemcert /usr/TKLC/plat/etc/ssl/old_server.pemcert`
	`$ sudo ln -s /usr/TKLC/plat/etc/ssl/server.pemcert /usr/TKLC/plat/etc/ssl/noa.pem`

Procedure 46. Install a Combined PEM File on Each Distinct <hostname>	

4. ☐	Restart the configuration web services and exit:
	`$ sudo pm.kill apwSoapServer`
	`$ sudo pm.kill cmsoapa`
	`$ exit`

Repeat the above procedure for each and every distinct `<hostname>`.

3.10 Update MySQL Password

3.10.1 Updating the MySQL Password

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

Procedure 47. 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 :
	3. Reset the MySQL default user password by running:
	`$ /usr/TKLC/appworks/bin/resetMysqlPassword`
	4. 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 :
	5. Reset the MySQL root password by running:
	`$ /usr/TKLC/appworks/bin/resetMysqlPassword root`
	6. 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 helps you secure Oracle Communications Diameter Signaling Router and its components.

- Change default passwords
- Utilize LDAP for authentication purposes
- Utilize authorized IP addresses feature
- 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
- Restrict network access by enabling the DSR firewall feature
- Enforce iLO to use strong encryption
- Available Ciphers for SSH and HTTPS/SSL

The DSR system has been preconfigured to require modern strong ciphers for both SSH and TLS. The supported ciphers/MACs for SSH connections are:

```
Ciphers aes128-ctr,aes192-ctr,aes256-ctr
MACs hmac-sha2-512,hmac-sha2-256
```

This is configured in `/etc/ssh/sshd_conf`. The supported cipher set (using openssl notation) for HTTPS/TLS is:

```
ECDH+AES128:ECDH+AESGCM:ECDH+AES256:DH+AES:DH+AESGCM:DH+AES256:RSA+AES
:RSA+AESGCM:!aNULL:!MD5:!DSS:!SSLv3:!3DES
```

For the default TLS (https) connection, this is configured in `/etc/httpd/conf.d/ssl.conf`; for certificates loaded via the GUI, this is configured in `/var/TKLK/appworks/etc/https.template`.

For detailed information on importing HTTPS/SSL Certificate into VNFM, refer [7] DSR VNFM Installation and User Guide.

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 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 are connected to a live agent who can assist you with MOS registration and opening a support ticket. MOS is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

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

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

- A total system failure that results in loss of all transaction processing capability

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

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

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.

4. Access the Oracle Help Center site at http://docs.oracle.com.
5. Click **Industries**.
6. Under the Oracle Communications subheading, click the **Oracle Communications documentation** link.

   The Communications Documentation page displays. Most products covered by these documentation sets display under the headings **Network Session Delivery and Control Infrastructure** or **Platforms**.
7. Click on your product and then the release number.

   A list of the entire documentation set for the selected product and release displays.

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.