

Oracle® Communications
Diameter Signaling Router

Security Guide

Release 8.2

E88984-01

January 2018

ORACLE®

Oracle Communications Diameter Signaling Router Security Guide, Release 8.2

Copyright © 2016, 2018 Oracle and/or its affiliates. All rights reserved.

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

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

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

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

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

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

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



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	6
1.1 Audience	6
1.2 References.....	6
1.3 Acronyms/Terms	6
2. Oracle Communications Diameter Singling Router Security Overview	7
2.1 Basic Security Considerations.....	7
2.2 Access the Oracle Communications Diameter Signaling Router System.....	7
2.3 Overview of Oracle Communications Diameter Signaling Router Security	9
2.4 Overview of Oracle Communications Diameter Signaling Router Security	9
3. Implement Oracle Communications Diameter Signaling Router Security	10
3.1 Oracle Communications Diameter Signaling Router Web GUI Standard Features	10
3.1.1 User Administration	10
3.1.1.1 Establish GUI Groups and Group Privileges	11
3.1.1.2 Create GUI Users and Assign to Groups.....	12
3.1.2 GUI User Authentication	13
3.1.2.1 GUI Passwords	13
3.1.2.2 Change Passwords for all DSR Administrative Accounts	13
3.1.2.3 Set Up Password Complexity	13
3.1.2.4 Set Up Password Aging Parameters	13
3.1.2.5 Restrict Concurrent GUI Logins	14
3.1.2.6 External Authentication	14
3.1.2.7 LDAP Authentication for GUI Users	14
3.1.2.8 System Single Sign-On for GUI Users	14
3.1.3 GUI Login and Welcome Banner Customization	15
3.1.4 SNMP Configuration.....	15
3.1.4.1 Select Versions	15
3.1.4.2 Community Names/Strings.....	16
3.1.5 Authorized IPs	16
3.1.6 Enable IPsec	16
3.1.7 Certificate Management	16
3.1.8 SFTP Administration.....	17
3.2 Host Intrusion Detection System (HIDS)	17

3.2.1	Host Intrusion Detection System (HIDS) overview	17
3.2.2	Determine Host Intrusion Detection System (HIDS) Status.....	18
3.2.3	Initialize Host Intrusion Detection System (HIDS)	19
3.2.4	Enable or Disable Host Intrusion Detection System (HIDS)	21
3.2.5	Suspend or Resume Host Intrusion Detection System (HIDS).....	22
3.2.6	Run On-Demand Host Intrusion Detection System (HIDS) Security Check	24
3.2.7	Update Host Intrusion Detection System (HIDS) Baseline	28
3.2.8	Delete Host Intrusion Detection System (HIDS) Baseline	29
3.2.9	View Host Intrusion Detection System (HIDS) Alarms	31
3.3	Oracle Communications Diameter Signaling Router OS Standard Features	33
3.3.1	Configure NTP Servers	34
3.3.1.1	Configure NTP for the Host OS of the Application guest VM (TVOE).....	34
3.3.2	Set the Time on the TVOE Host	36
3.3.3	Configure Password Expiry for OS Users	36
3.3.4	Configure Minimum Time before OS Password Can Be Changed	36
3.3.5	Configure Password Length for OS Users	36
3.3.6	Configure Session Inactivity for OS Users	37
3.3.7	Lock OS User Accounts After a Specified Number of Failed Login Attempts	37
3.4	Other Optional Configurations	38
3.4.1	Change OS User Account Passwords	38
3.4.2	Change Login Display Message	38
3.4.3	Force iLO to Use Strong Encryption	39
3.4.4	Set Up rsyslog for External Logging	39
3.4.5	Add sudo Users.....	40
3.4.6	Report and Disable Expired OS User Accounts	40
3.5	Ethernet Switch Considerations	41
3.5.1	Configure SNMP in Switches.....	41
3.5.2	Configure Community Strings.....	41
3.5.3	Configure Traps.....	41
3.6	Security Logs and Alarms	42
3.7	Optional IPsec Configuration.....	42
3.7.1	IPsec Overview	42
3.7.1.1	Encapsulate Security Payload.....	43
3.7.1.2	Internet Key Exchange.....	43

3.7.2 IPsec Process	43
3.7.3 Pre-requisite Steps for Setting Up IPsec.....	44
3.7.4 Set up IPsec.....	44
3.7.5 IPsec IKE and ESP Elements.....	45
3.7.6 Add an IPsec Connection	46
3.7.7 Edit an IPsec Connection	46
3.7.8 Enable and Disable an IPsec Connection.....	47
3.7.9 Delete an IPsec connection	48
Appendix A. Secure Deployment Checklist.....	48
Appendix B. My Oracle Support (MOS).....	49
Appendix C. Locate Product Documentation on the Oracle Help Center Site	49
Appendix D. Available Ciphers for SSH and HTTPS/SSL	49

List of Tables

Table 1. Acronyms/Terms	6
Table 2. Predefined User and Group.....	10
Table 3. IPsec IKE and ESP Elements.....	45

List of Figures

Figure 1. Oracle Communications Diameter Signaling Router Login Page.....	8
Figure 2. Oracle Communications Diameter Signaling Router Home Page	8
Figure 3. Oracle Communications Diameter Signaling Router Generic DSR Deployment Model for a Generic Model of the Deployment Strategy	10
Figure 4. Global Action and Administration Permissions	12
Figure 5. DSR View Active Alarm Screen.....	27
Figure 6. DSR View Active Alarm Report Screen	27
Figure 7. Platcfg Alarm Screen	33
Figure 8. NTP Configuration (GUI)	34

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 herein are not recommended and may hinder the product's operation or Oracle's capability to provide appropriate support.

1.1 Audience

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

1.2 References

The following references capture the source material used to create this document. These documents are included in the Oracle Communications Diameter Signaling Router documentation set. See Appendix C Locate Product Documentation on the Oracle Help Center Site.

- [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 8.2.x Upgrade Procedure

1.3 Acronyms/Terms

An alphabetized list of acronyms/terms used in the document.

Table 1. Acronyms/Terms

Acronym/Term	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
MP	Message Processor
NOAMP	Network Operation, Administration, Maintenance, and Provisioning

Acronym/Term	Definition
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.
- **Monitor system activity.** Establish who should access which system components, and how often, and monitor those components.
- **Configure software securely.** For example, use secure protocols such as TLS and strong passwords.
- **Change default passwords.** The initial installation of the DSR system software uses default passwords. These should be changed at installation time.
- **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.
- **Learn and use the Oracle Communications Diameter Signaling Router security features.** See Section 3 Implement Oracle Communications Diameter Signaling Router Security for more information.
- **Keep up to date on security information.** Oracle regularly issues security alerts for vulnerability fixes deemed too critical. It is advisable to install the applicable security patches as soon as possible. See the security alerts page at <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 Appendix D 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.

ORACLE®

Oracle System Login Tue Aug 1 01:12:41 2017 EDT

Log In

Enter your username and password to log in

Username:

Password:

☐ Change password

Welcome to the Oracle System Login.

This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the [Oracle Software Web Browser Support Policy](#) for details.

Unauthorized access is prohibited.

Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Copyright © 2010, 2017, [Oracle](#) and/or its affiliates. All rights reserved.

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.

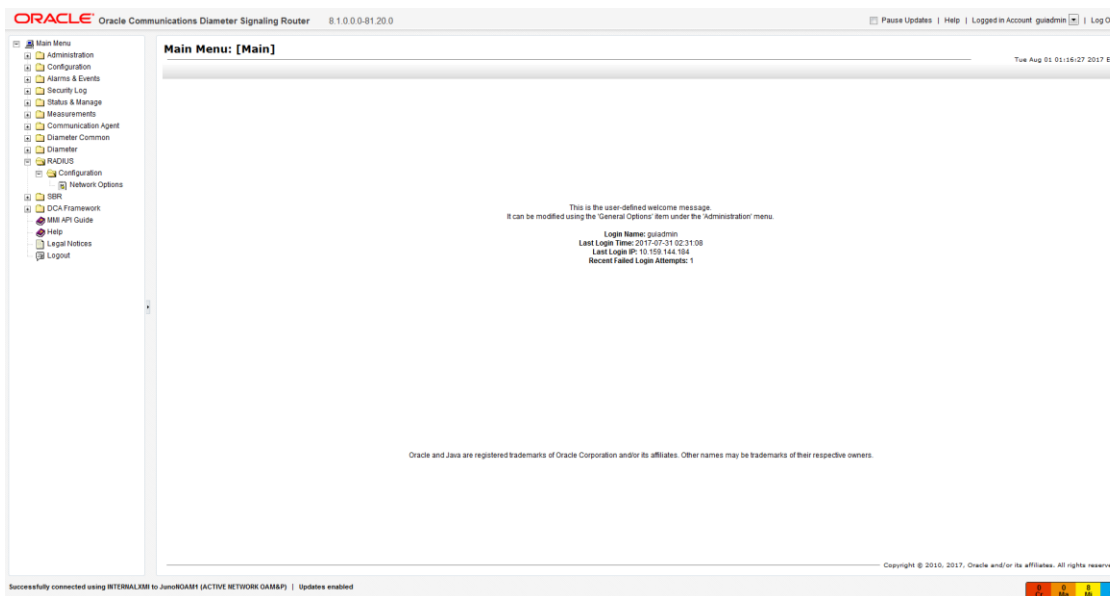


Figure 2. Oracle Communications Diameter Signaling Router Home Page

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 Appendix D 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 is 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.
4. iLO Web GUI access – Proliant Server iLO provides web GUI access from an Internet Explorer session using the URL, <https://<iLO IP Address>/>. Using a supported web browser, log into iLO 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.

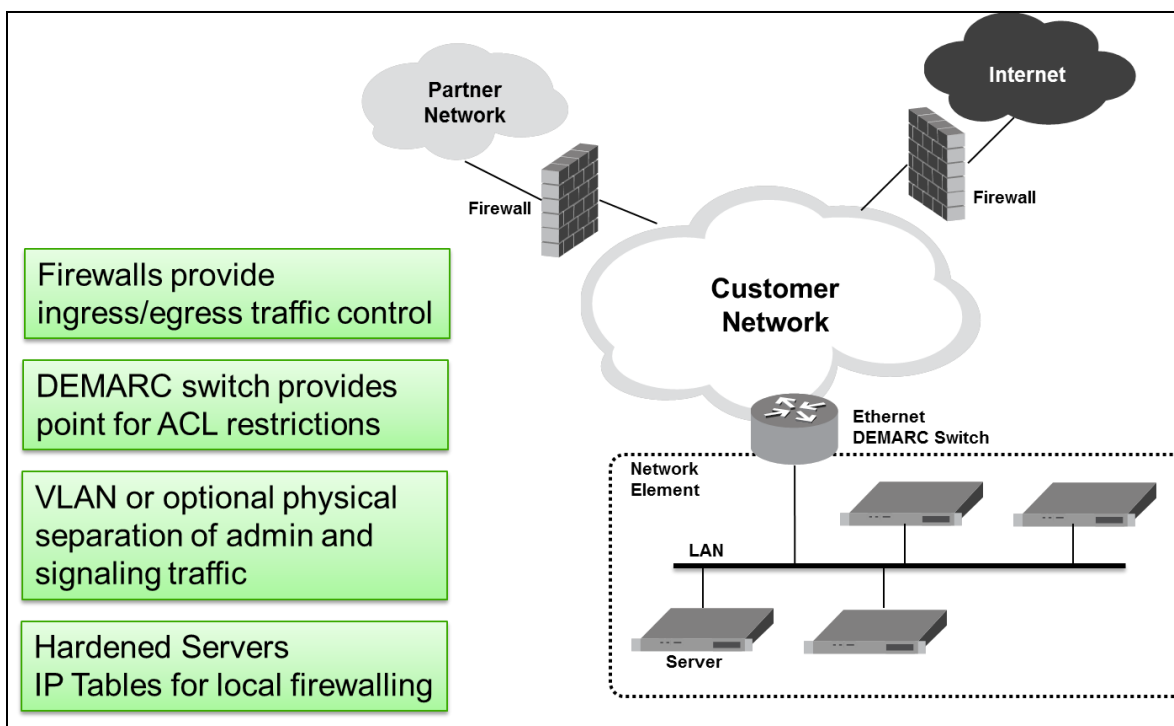


Figure 3. Oracle Communications Diameter Signaling Router Generic DSR Deployment Model for a Generic Model of the Deployment Strategy

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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Administration Permissions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
General Options	<input type="checkbox"/>		<input type="checkbox"/>		
Users	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Groups	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Sessions	<input type="checkbox"/>			<input type="checkbox"/>	
Certificate Management	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Authorized IPs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SFTP Users	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Software Versions	<input type="checkbox"/>				
Software Upgrade	<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>
Remote SNMP Trapping	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Remote LDAP Authentication	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Remote Export Server	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
DNS Configuration	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

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 3.4.1 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.

3.1.3 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 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 check box in 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, please refer to the [1] Operation, Administration, and Maintenance (OAM) Guide.

3.1.4.1 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.

3.1.4.2 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.”

3.1.5 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.

3.1.6 Enable IPsec

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

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

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

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

3.1.7 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.

3.1.8 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 (i.e., 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 as shown in Figure 7. Platcfg Alarm Screen. The Customers can view active alarms on the Oracle Communications Diameter Signaling Router GUI on the **Main Menu -> Alarms & Events -> View Active** GUI screen as shown in Figure 5. DSR View Active Alarm Screen and Figure 6. DSR View Active Alarm Report Screen.

3.2.2 Determine Host Intrusion Detection System (HIDS) Status

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

1. Login as **admusr** on the server.

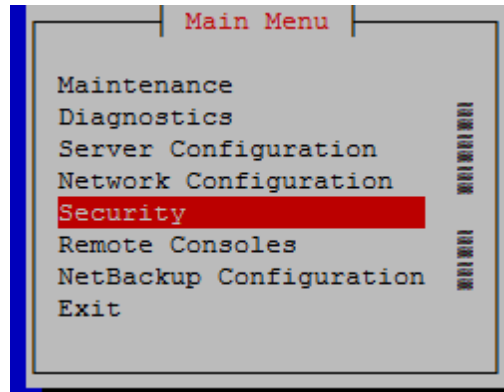
Login: admusr

Password: <current admin user password>

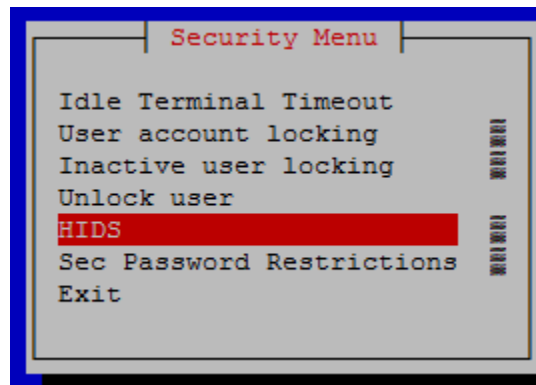
2. Open the platcfg menu by entering this command:

```
$sudo su - platcfg
```

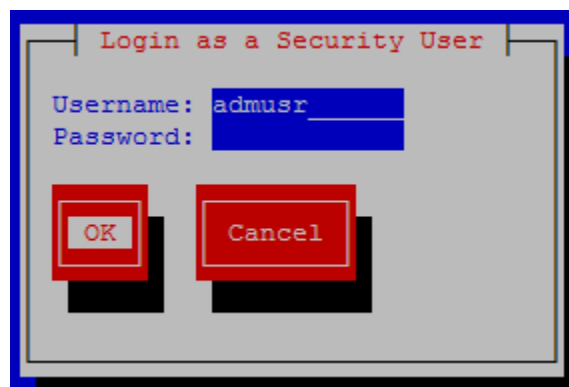
3. Select **Security** from the menu and press **Enter**.



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

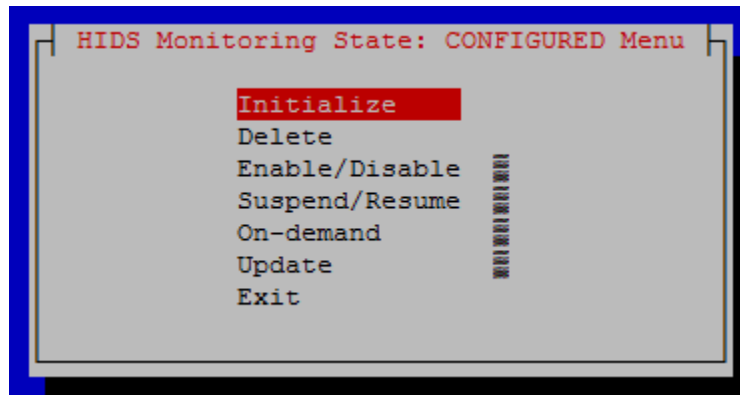


5. Type the **Username** and **Password** for a user that is part of the **secgrp** group.



Note: By default, **admusr** is part of the **secgrp** group.

The HIDS menu displays and the HIDS Monitoring State is listed on the top of the window.



6. 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.

1. Login as **admusr** on the server

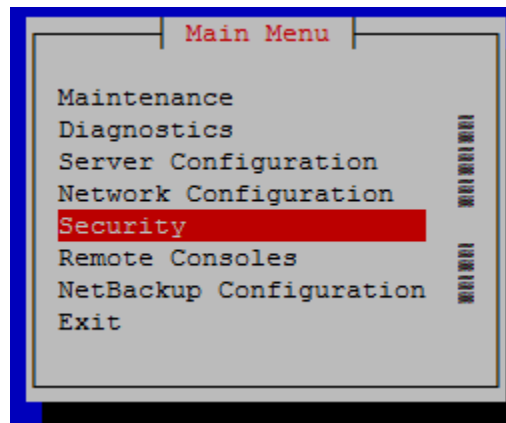
```
Login: admusr
```

```
Password: <current admin user password>
```

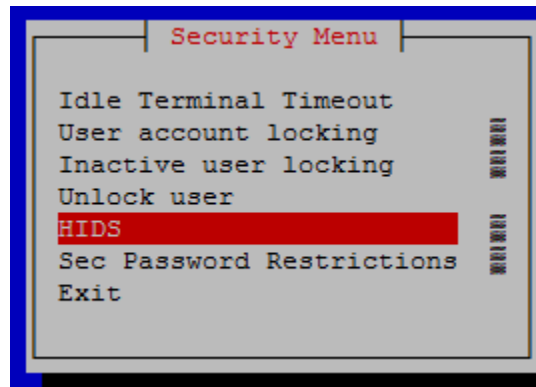
2. Open the platcfg menu by entering this command:

```
$ sudo su - platcfg
```

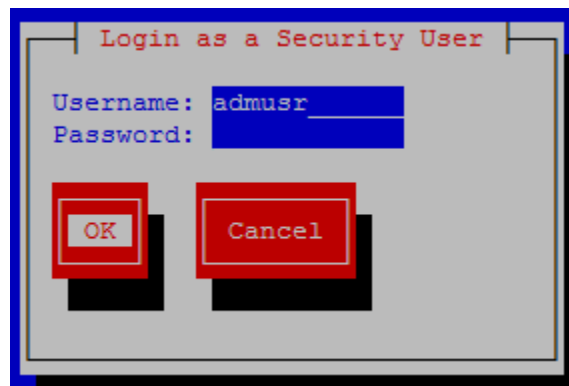
3. Select **Security** from the menu and press **Enter**.



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

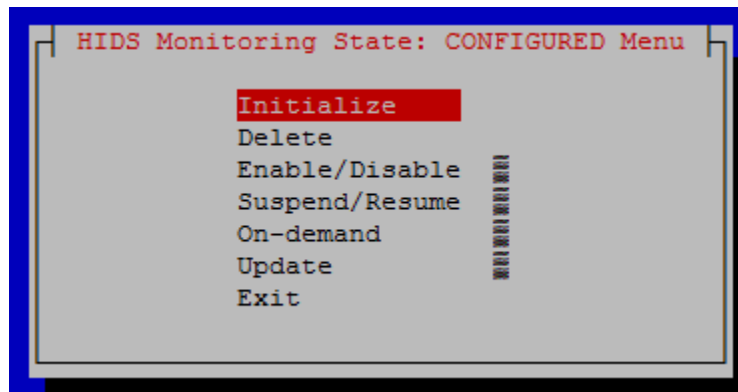


5. Type the **Username** and **Password** for a user that is part of the **secgrp** group.



Note: By default, **admusr** is part of the **secgrp** group.

6. Select **Initialize** and press **Enter**.



7. Select **Yes** and press **Enter**.
8. After the **HIDS baseline successfully initialized** message displays, press any key to continue.
9. 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.

1. Login as **admusr** on the server.

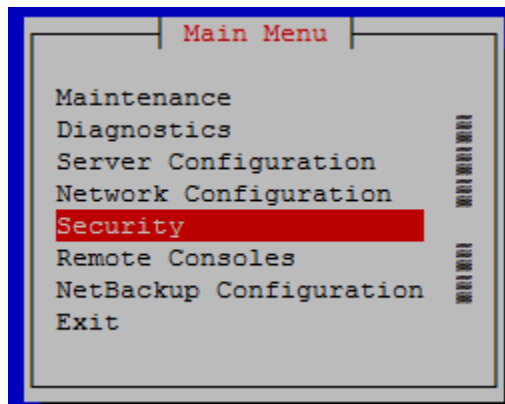
Login: admusr

Password: <current admin user password>

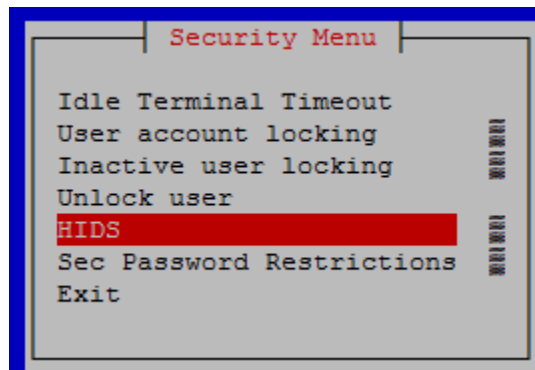
2. Open the platcfg menu by entering this command:

```
$ sudo su - platcfg
```

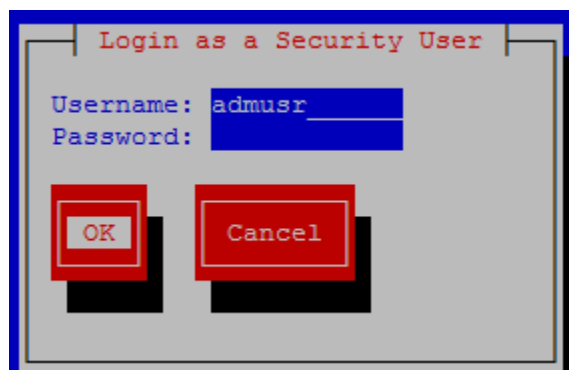
3. Select **Security** from the menu and press **Enter**.



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

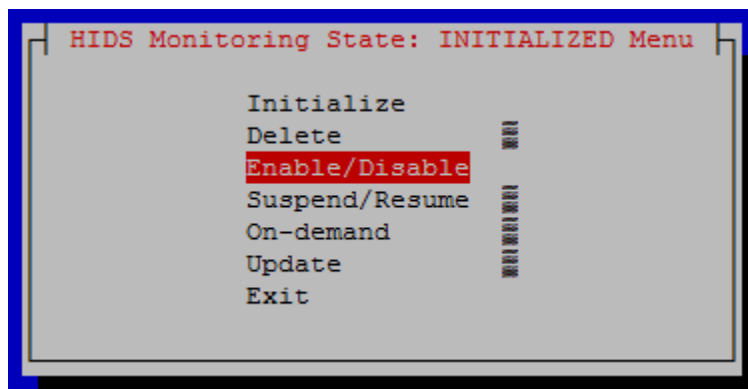


5. Type the **Username** and **Password** for a user that is part of the **secgrp** group.

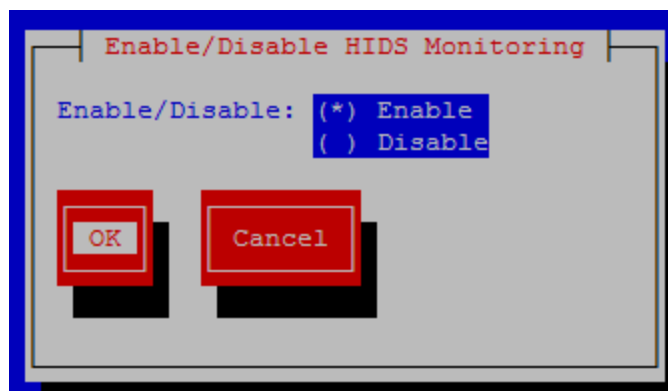


Note: By default, **admusr** is part of the **secgrp** group.

6. Click **OK** and press **Enter**.
7. Select **Enable/Disable** and press **Enter**.



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



9. Click **OK** and press **Enter**.
10. After the message box that indicates that DB monitoring has been enabled/disabled or a failure message displays, press any key to continue.
11. Select **Exit** in each of the menus until a command prompt is reached.

3.2.5 Suspend or Resume Host Intrusion Detection System (HIDS)

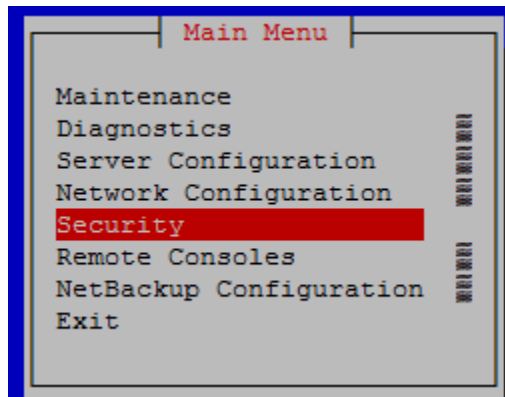
The HIDS monitoring can temporarily be suspended or resumed on a system that has HIDS enabled.

1. Login as **admusr** on the server.

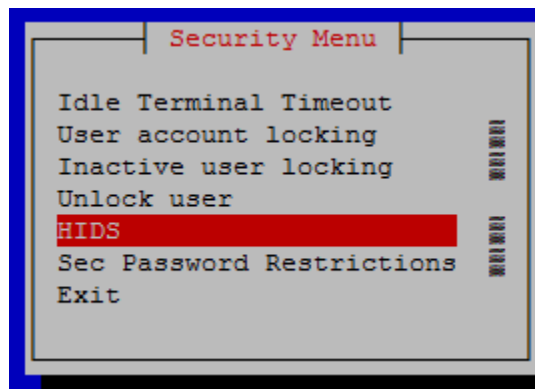
```
Login: admusr
Password: <current admin user password>
```
2. Open the platcfg menu by entering this command:

```
$ sudo su - platcfg
```

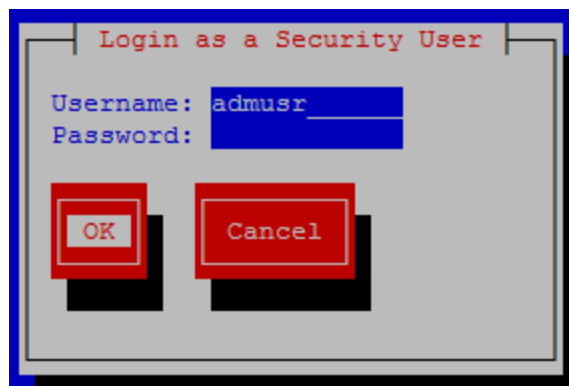
3. Select **Security** from the menu and press **Enter**.



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



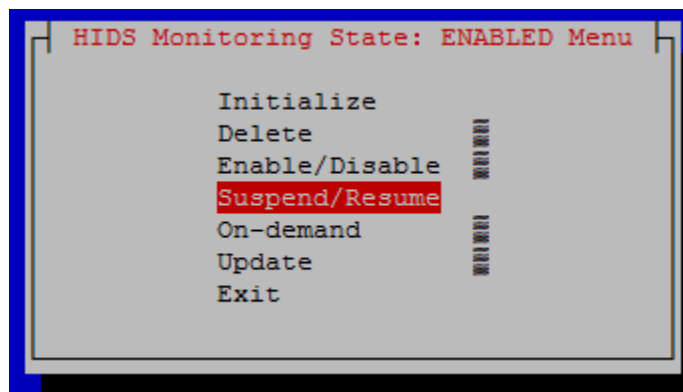
5. Type the **Username** and **Password** for a user that is part of the **secgrp** group.



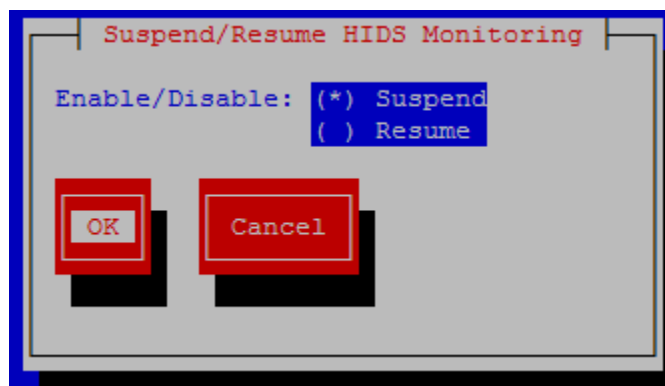
Note: By default, **admusr** is part of the **secgrp** group.

6. Click **OK** and press **Enter**.

7. Select **Suspend/Resume** and press **Enter**.



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



9. Click **OK** and press **Enter**.
10. After the message box that indicates that DB monitoring has been suspended/resumed or a failure message displays, press any key to continue.
11. 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.

1. Login as **admusr** on the server.

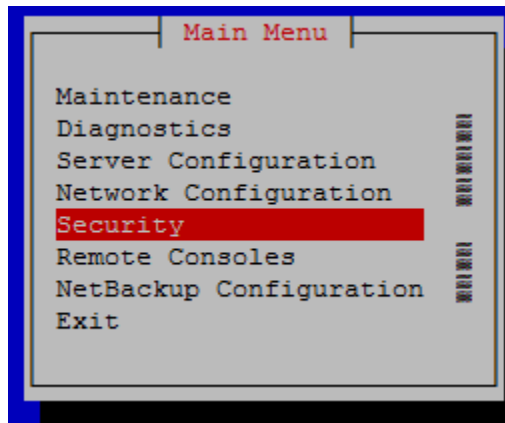
```
Login: admusr
```

```
Password: <current admin user password>
```

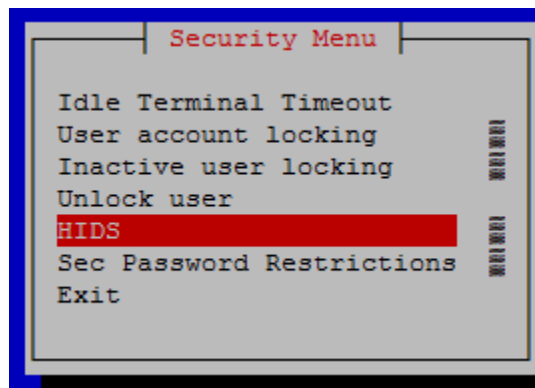
2. Open the platcfg menu by entering this command:

```
$ sudo su - platcfg
```

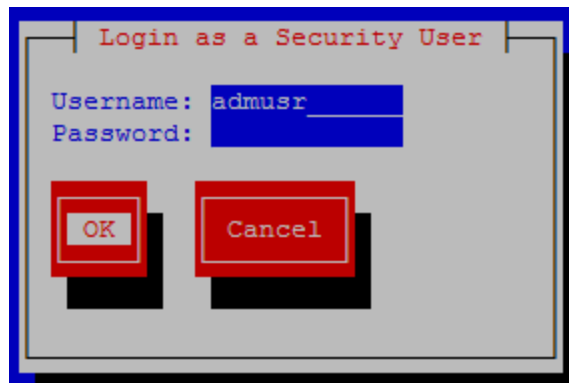

3. Select **Security** from the menu and press **Enter**.



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

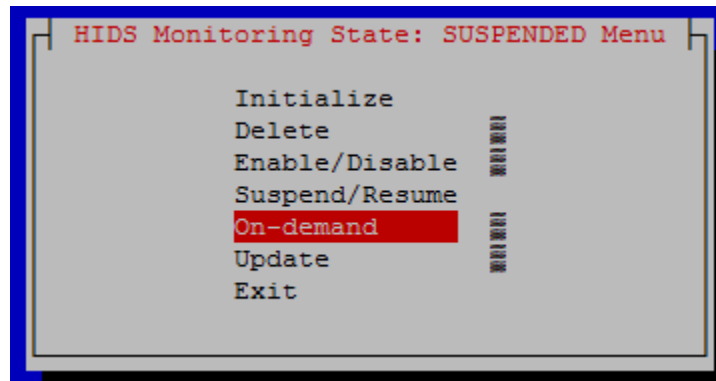


5. Type the **Username** and **Password** for a user that is part of the **secgrp** group.



Note: By default, **admusr** is part of the **secgrp** group.

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



7. Click **Yes** and press **Enter**.

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:



Note: This alarm can also be seen when viewing alarms in the platcfg system, as described in section 3.2.9: View Host Intrusion Detection System (HIDS) Alarms, and shown in Figure 7. Platcfg Alarm Screen.

Note 2: This alarm is also propagated through normal COMCOL channels ultimately resulting in the alarm being accessible on the Oracle Communications Diameter Signaling Router GUI on the **Main Menu -> Alarm & Events -> View Active** GUI screen, as shown in step 9.

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

9. (Optional) Log into the DSR GUI and navigate to **Main Menu -> Alarms & Events -> View Active** GUI screen 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
97	32349	2016-06-02 14:52:04.063 EDT	MAJOR	TPD	cmplat alarm	SO_UDR	pc9112032-so-a	PLAT	
	File Tampering		GN_WARNING/WRN Platform detected an error condition [cmplatalarm.cxx:194] ... More...						
17	10300	2016-05-30 15:55:58.567 EDT	MINOR	OAM	audit	SO_UDR	pc9112032-so-a	DB	
	SNMP Trapping Not Configured		No SNMP trap configuration found for this site!						

Figure 5. DSR View Active Alarm Screen

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	
<pre> 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/arise/alarm.log (timestamp: 1464893524) [cmplatalarm.cxx:198] ^^ [6114:cmplatalarm.cxx:200] NSECS: 1572917444489037368 ID: 0 </pre>	

Figure 6. DSR View Active Alarm Report Screen

3.2.7 Update Host Intrusion Detection System (HIDS) Baseline

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

1. Login as **admusr** on the server.

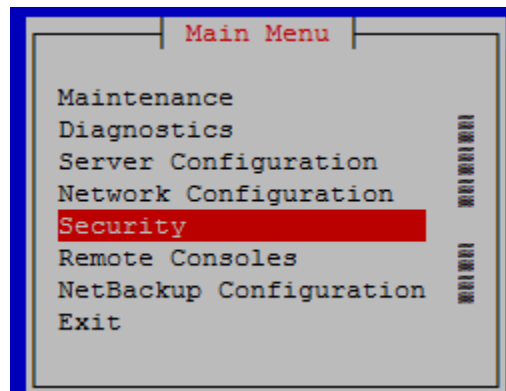
Login: admusr

Password: <current admin user password>

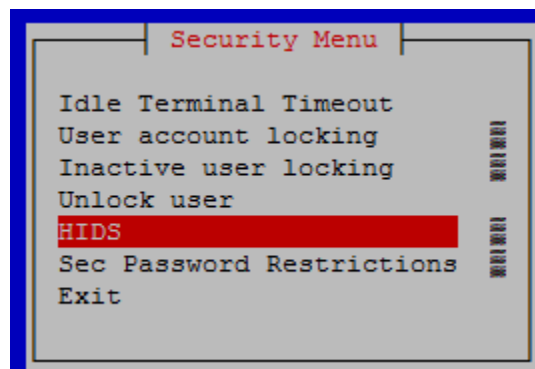
2. Open the platcfg menu by entering this command:

```
$ sudo su - platcfg
```

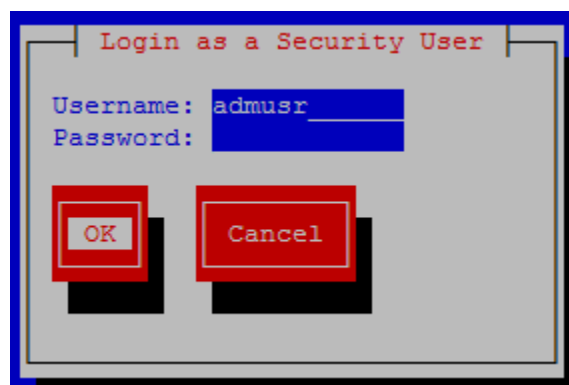
3. Select **Security** from the menu and press **Enter**.



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

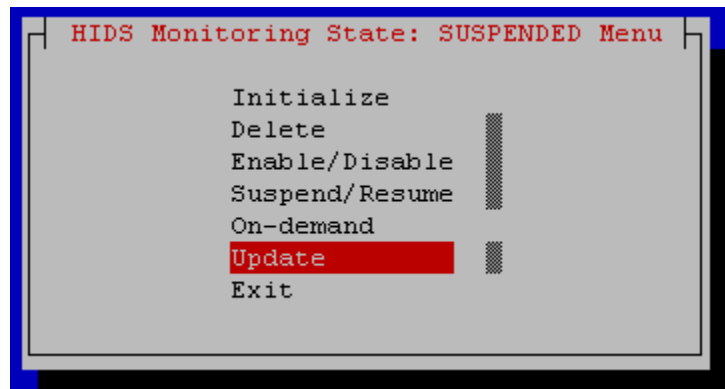


5. Type the **Username** and **Password** for a user that is part of the **secgrp** group.



Note: By default, **admusr** is part of the **secgrp** group.

6. Click **OK** and press **Enter**.
7. Select **Update** and press **Enter**.



8. Select file's baseline to update.



9. Click **OK** and press **Enter**.
10. After the message box that indicates the success/fail result displays, press any key to continue.
11. Select **Exit** in each of the menus until a command prompt is reached.

3.2.8 Delete Host Intrusion Detection System (HIDS) Baseline

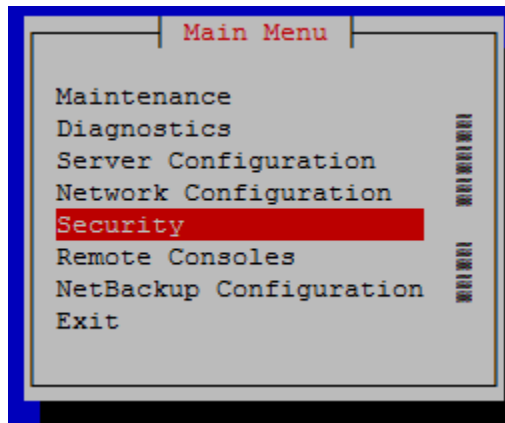
The HIDS **Delete** menu can be used for permanently disabling HIDS or for backing out of a product upgrade.

1. Login as **admusr** on the server.

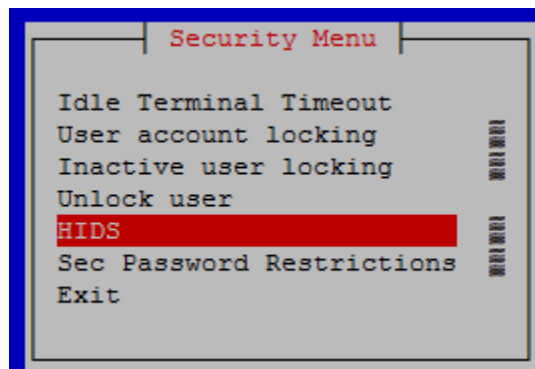

```
Login: admusr
Password: <current admin user password>
```
2. Open the platcfg menu by entering this command:


```
$ sudo su - platcfg
```

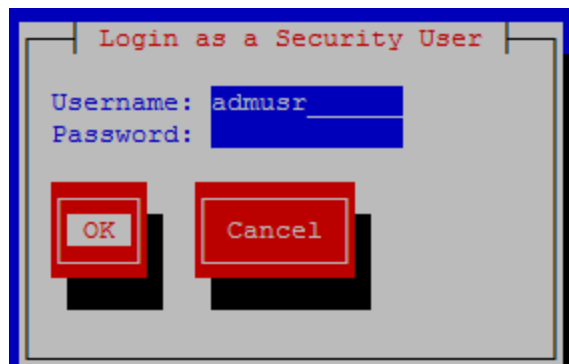
3. Select **Security** from the menu and press **Enter**.



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



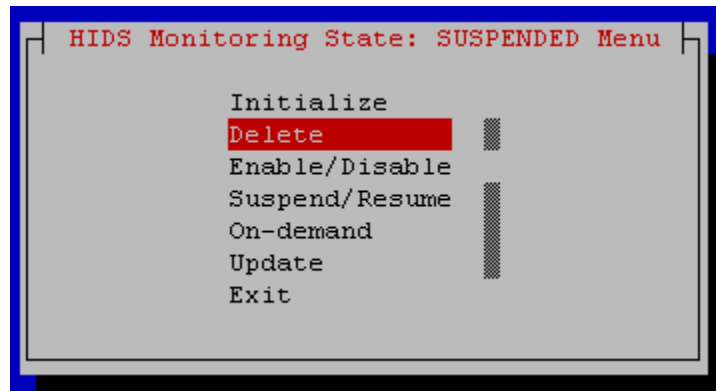
5. Type the **Username** and **Password** for a user that is part of the **secgrp** group.



Note: By default, **admusr** is part of the **secgrp** group.

6. Click **OK** and press **Enter**.

7. Select **Delete** and press **Enter**.



8. Click **Yes** and press **Enter**.
9. After the message box that indicates the success/fail result displays, press any key to continue.
10. Select **Exit** in each of the menus until a command prompt is reached.

3.2.9 View Host Intrusion Detection System (HIDS) Alarms

HIDS alarms can be viewed using multiple methods. HIDS alarms are standard TPD alarms with the alarmEventType set to **securityServiceOrMechanismViolation**. The HIDS alarms are propagated through normal COMCOL channels ultimately resulting in SNMP traps being sent to the customer's SNMP management system, if configured. The multiple ways to view the alarms include:

- Customers can view current, previously cleared, and how alarms were cleared in the `/var/TKLC/logs/hids/alarms.log` file.
- Customers can view active alarms on the DSR GUI on the **Main Menu -> Alarms & Events -> View Active** GUI screen as shown in Figure 5. DSR View Active Alarm Screen and Figure 6. DSR View Active Alarm Report Screen.
- Customers can view active alarms on the platcfg GUI, including HIDS alarms, by using the following steps:

1. Login as **admusr** on the server.

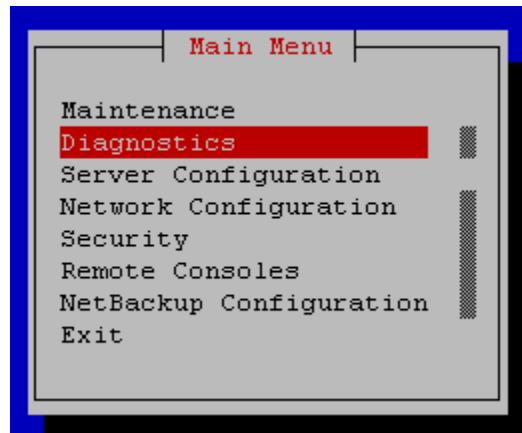
```
Login: admusr
```

```
Password: <current admin user password>
```

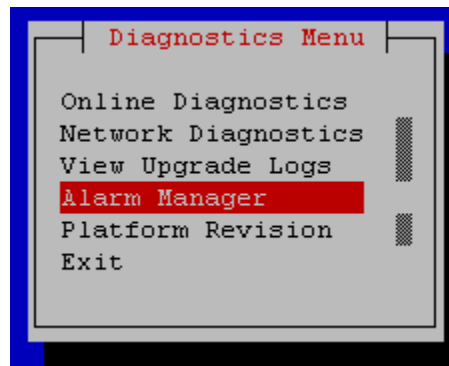
2. Open the platcfg menu by entering this command:

```
$ sudo su - platcfg
```

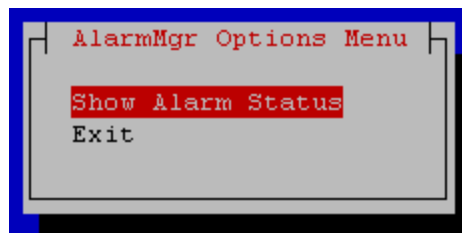
3. Select **Diagnostics** from the menu and press **Enter**.



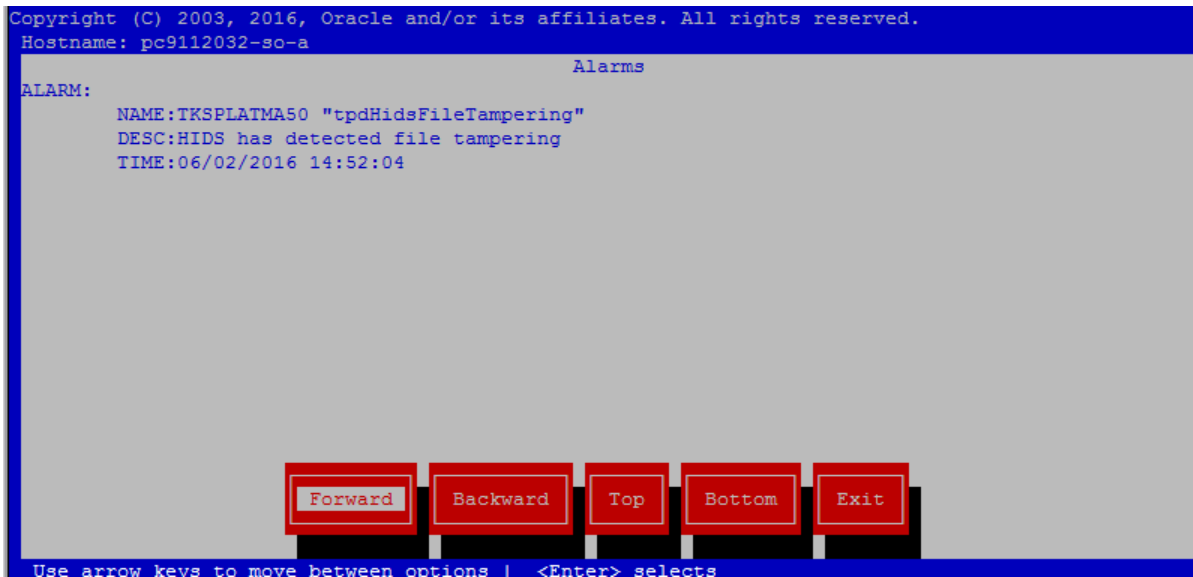
4. Select **Alarm Manager** from the menu and press **Enter**.



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



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:



```
Copyright (C) 2003, 2016, Oracle and/or its affiliates. All rights reserved.  
Hostname: pc9112032-so-a  
Alarms  
ALARM:  
  NAME:TKSPLATMA50 "tpdHidsFileTampering"  
  DESC:HIDS has detected file tampering  
  TIME:06/02/2016 14:52:04  
  
[Forward] [Backward] [Top] [Bottom] [Exit]  
Use arrow keys to move between options | <Enter> selects
```

Figure 7. Platcfg Alarm Screen

6. 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.

Main Menu: Configuration -> Servers [Edit] Tue Aug 01 04:05:23 2017 EDT

Edit Server MauiNOAM1

Attribute	Value	Description
Hostname *	MauiNOAM1	Unique name for the server. [Default = n/a. Range = A 20-character string. Valid characters are alphanumeric and minus sign. Must start with an alphanumeric and end with an alphanumeric.] [A value is required]
Role *	NETWORK_OAM&P	Select the function of the server [A value is required]
System ID	Maui	System ID for the NOAMP or SOAM server. [Default = n/a. Range = A 64-character string. Valid value is any text string.]
Hardware Profile	DSR TVOE Guest	Hardware profile of the server
Network Element Name *	MAUI_50207	Select the network element [A value is required]
Location		Location description [Default = "". Range = A 15-character string. Valid value is any text string.]

OAM Interfaces [At least one interface is required]:

Network	IP Address	Interface
XMI (10.240.192.128/25)	10.240.192.135	xmi <input checked="" type="checkbox"/> VLAN (3)
IMI (169.254.2.0/24)	169.254.2.5	imi <input checked="" type="checkbox"/> VLAN (4)

NTP Servers:

NTP Server IP Address	Prefer	
10.250.32.10	<input type="checkbox"/>	<div>Add</div> <div>Remove</div>

Copyright © 2010, 2017, Oracle and/or its affiliates. All rights reserved.

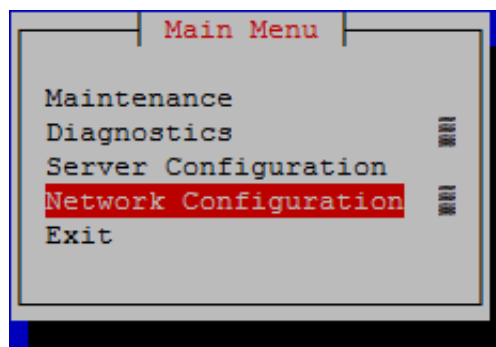
Figure 8. NTP Configuration (GUI)

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

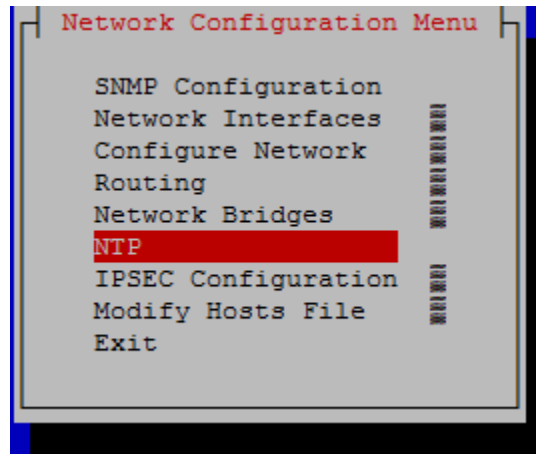
3.3.1.1 Configure NTP for the Host OS of the Application guest VM (TVOE)

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

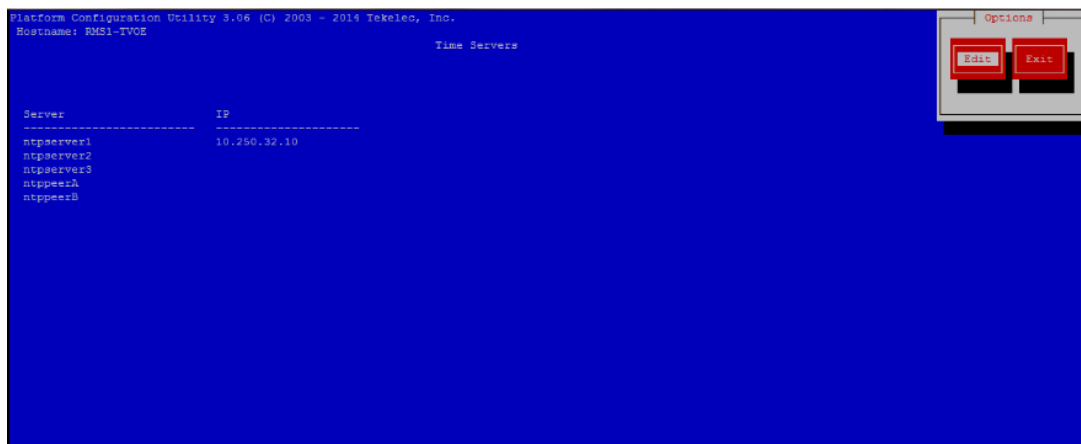
1. Login or switch user to platcfg user on the TVOE server. The platcfg main menu displays.
2. Navigate to **Network Configuration**.



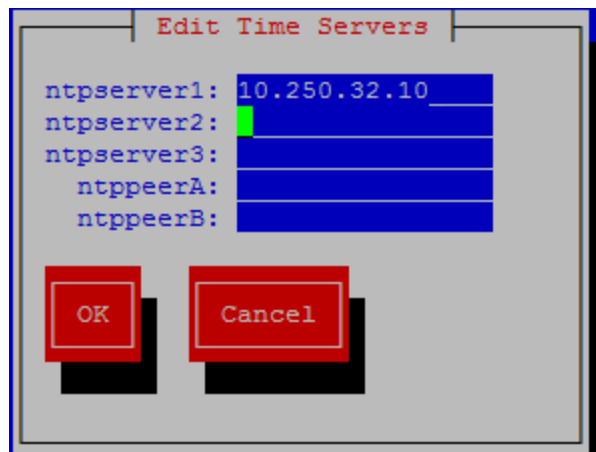
3. Select **NTP**.



4. The Time Servers screen displays, which shows the configured NTP servers and peers. Click **Edit**.



5. On the Edit Time Servers menu, enter the NTP Server information and click **OK**.



6. Exit the platcfg menu.
7. 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:

1. Login 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 Expiry for OS Users

Use the following procedure to configure password expiry:

1. Login 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. Fill out the following settings:

```
Maximum number of days a password may be used: 99999
```

5. Click **OK** and press **Enter**.

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

3.3.4 Configure Minimum Time before OS Password Can Be Changed

Procedure to configure minimum time before password can be changed.

1. Login 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. Fill out the following settings:

```
Minimum number of days allowed between password changes: 0
```

5. Click **OK** and press **Enter**.

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

3.3.5 Configure Password Length for OS Users

Procedure to configure password length.

1. Login 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. From the menu, select **Sec Password Restrictions** option.
5. Select **Global Password Restrictions for New Users**. And in the menu displayed, fill out the field Minimum acceptable size for the new password. Click **OK** and press **Enter**.
6. Select exit in each of the menus until a command prompt is reached.

3.3.6 Configure Session Inactivity for OS Users

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

1. Login 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 in 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.

3.3.7 Lock OS User Accounts After a Specified Number of Failed Login Attempts

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

1. Login as admin user on the server.
`Login: admusr`
`Password: <current admusr password>`
2. Open the platcfg menu by entering this command:
`$ sudo su - platcfg`
3. Select **Security** from the menu and press **Enter**.
4. Select **User Account Locking** from the menu and press **Enter**.
5. Fill out the following settings:
`Feature: () disable (*) enable`
`Deny after # of attempts: <max tries>`
`Fail interval in minutes: <interval minutes>`
`Unlock time in minutes: <unlock time>`
6. Click **OK** and press **Enter**.
7. Select **Exit** in each of the menus until a command prompt is reached.

3.4 Other Optional Configurations

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

3.4.1 Change OS User Account Passwords

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

1. Login as **admusr** on the source server.

```
login: admusr
Password: <current admin user password>
```

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

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

3. Repeat step 1 for all servers.

3.4.2 Change Login Display Message

Use this procedure to change the Login Display Message.

1. Login as **admusr** on the source server.

```
Login: admusr
Password: <current admin user password>
```

2. Create a backup copy of `sshd_config`

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

3. Edit the `sshd` configuration file.

```
$ sudo rcstool co sshd_config
$ sudo vi sshd_config
```

Uncomment and edit the following line:

```
$ Banner /some/path
```

To this:

```
Banner /etc/ssh/sshd-banner
```

Save and exit the `vi` session.

4. Edit the banner file.

```
$ sudo vi sshd-banner
```

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

5. Restart the `sshd` service.

```
$ sudo service sshd restart
```

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

```
$ sudo ssh <current server name>
```

Verify message line feeds are formatted correctly.

```
$ exit
```

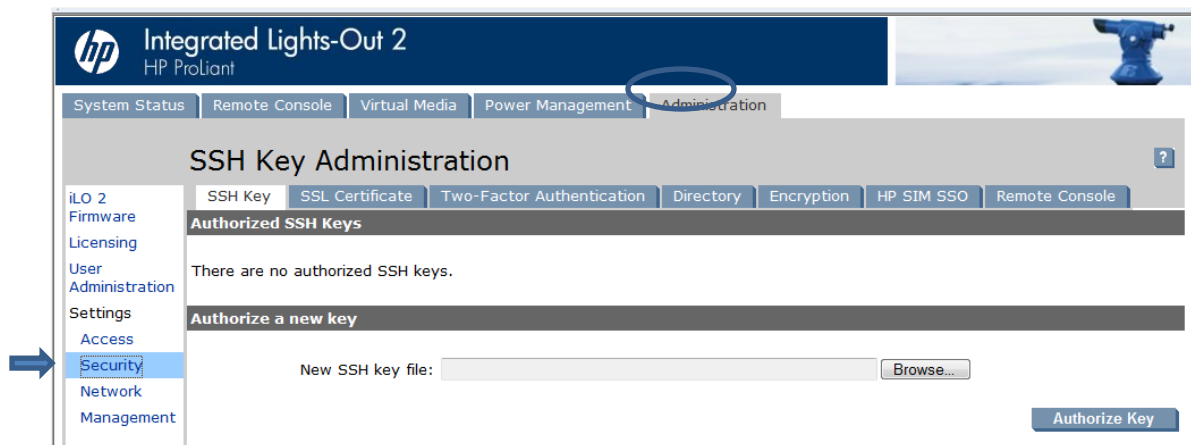
7. Check the files into rcs to preserve changes during upgrades.

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

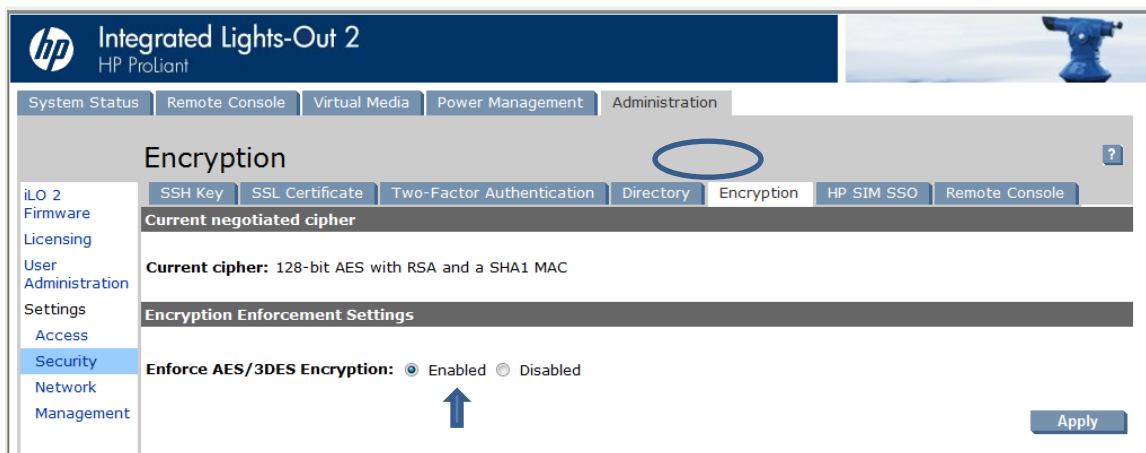
3.4.3 Force iLO to Use Strong Encryption

Login as an administrator to the iLO and execute these steps.

1. On the Administration tab, click **Security** from the side menu.



2. On the Encryption tab, under Encryption Enforcement Settings set the Enforce AES/3DES Encryption to **Enabled**.



3. Click **Apply**. Logout and wait 30 seconds before logging back in.

3.4.4 Set Up rsyslog for External Logging

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

1. Login as admin user on the server.

```
login: adminusr
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.

3.4.5 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.

The syntax of the configuration file can be somewhat tedious and editing mistakes could leave a system without needed access. For this reason, details of the configuration rules are available through Oracle Help Center (OHC) or by opening a ticket with Oracle technical support.

3.4.6 Report and Disable Expired OS User Accounts

Procedure to Report and Disable Expired User Accounts.

1. Login as admin user on the source server.

```
login: admusr
Password: <current admin user password>
```

2. Run the report of expired users.

```
$ sudo lastlog -b <N>
```

Note: This command 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. Disable the user accounts identified by the lastlog report.

```
$ sudo passwd -l <user acct>
```

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

4. To re-enable an account:

```
$ sudo passwd -u <user acct>
```

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

3.5 Ethernet Switch Considerations

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

3.5.1 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).
1. Log into the server as root user and list all the configured switches by typing this command:

```
# netConfig --repo listDevices
```
 2. 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>.
 3. For any given switch by switch name, display SNMP community information by typing this command:

```
# netConfig getSNMP --device=<switch_name>
```
 4. 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>
```

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 addsSNMP -device=<switch name> community=<community string>
uauth=RO
```
2. To delete a community string to ANY switch by switch name, use appropriate switch name in 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 6120 switch. The switches 4948 or 3020 do not need this field in the above commands.

3.6 Security Logs and Alarms

The Security Log page in the GUI allows you to view the application historical security logs from all configured Security logs that are displayed in a scrollable, optionally filterable table. The security logs can also be exported to file management area in .csv format. For more details, see the Security Log chapter in 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.

3.7.2 IPsec Process

When an IPsec connection is configured, Security Policies 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 Policies 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. Login 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)
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:

1. Login as **admusr** on the server.
`Login: admusr`
`Password: <current admin user password>`
2. Open the platcfg menu by typing this command.
`$ sudo su - platcfg`
3. Select **Network Configuration**.
4. Select **IPsec Configuration**.
5. Select **IPsec Connections**.
6. Click **Edit**.
7. Select **Add Connection**.
8. Select the Internet Key Exchange Version: either **IKEv1** or **IKEv2**.
9. Complete the **IKE Configuration** fields for the desired connection, then click **OK**.
 The fields are described in Table 3. IPsec IKE and ESP Elements.
10. Select the desired ESP Encryption algorithm, and click **OK**.
 The fields are described Table 3. IPsec IKE and ESP Elements.
11. Complete the **Add Connection** fields for the desired connection.
 - a. Enter the **Local Address**.
 - b. Enter the **Remote Address**.
 - c. Enter the **Pass Phrase**.
 - d. Select the **Mode**.
12. Click **OK**.
 Wait for the connection to be added.
 When the connection has been successfully added, the Internet Key Exchange Version menu displays.
13. 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:

1. Login as **admusr** on the server.
`Login: admusr`
`Password: <current admin user password>`
2. Open the platcfg menu by typing this command:
`$ sudo su - platcfg`
3. Select **Network Configuration**.
4. Select **IPsec Configuration**.
5. Select **IPsec Connections**.

6. Click **Edit**.
7. Select **Edit Connection**.
8. Select **IPsec connection** to edit.
9. View the IPsec connection's current configuration.
10. Click **Edit**.
11. Select either **IKEv1** or **IKEv2**.
12. Complete the **IKE Configuration** fields if needed, then click **OK**.
The fields are described in Table 3. IPsec IKE and ESP Elements.
13. Select the desired **ESP Configuration** fields, then click **OK**.
The fields are described in Table 3. IPsec IKE and ESP Elements.
14. Complete the Add Connection fields for the desired connection.
 - a. Type the **Local Address**.
 - b. Type the **Remote Address**.
 - c. Type the **Pass Phrase**.
 - d. Select the **Mode**.
15. Click **OK**.
16. Select **Yes** to restart the connection.
When the connection has been successfully updated, the Internet Key Exchange Version menu displays.
17. 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:

1. Login as **admusr** on the server.

```
Login: admusr
Password: <current admin user password>
```
2. Open the platcfg menu by typing this command:

```
$ sudo su - platcfg
```
3. Select **Network Configuration**.
4. Select **IPsec Configuration**.
5. Select **IPsec Connections**.
6. Click **Edit**.
7. Select **Connection Control**.
8. Select **IPsec connection** to enable or disable.
9. Select **Enable** or **Disable**.
10. Click **OK** to enable or disable the selected IPsec connection.
11. Select **Exit** in each of the menus until a command prompt is reached.

3.7.9 Delete an IPsec connection

Procedure to delete an IPsec connection.

1. Login as **admusr** on the server.

```
Login: admusr
```

```
Password: <current admin user password>
```

2. Open the platcfg menu by typing this command:

```
$ sudo su - platcfg
```

3. Select **Network Configuration**.
4. Select **IPsec Configuration**.
5. Select **IPsec Connections**.
6. Click **Edit**.
7. Select **Delete Connection**.
8. Select IPsec connection to delete.
9. Click **Yes** to confirm the delete.
10. Wait for the connection to be deleted.

When the IPsec connection has been successfully deleted, the Connection Action menu displays.

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

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

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.

Appendix C. Locate Product Documentation on the Oracle Help Center Site

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

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

The Communications Documentation page displays. Most products covered by these documentation sets display under the headings **Network Session Delivery and Control Infrastructure** or **Platforms**.

4. Click on your product and then the release number.

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

Appendix D. 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
```

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`.