Oracle® Communications

Policy Management

Security Guide

Release 12.6.1

F45229-02

April 2022

ORACLE

Oracle Communications Policy Management Security Guide, Release 12.6.1

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

List of Tables

List of Figures

1. Introduction

This document provides guidelines and recommendations for configuring the Oracle Communications Policy Management 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 Policy Management documentation set. See Oracle Help Center (OHC).

[1] SNMP User's Guide

[2] Platform Configuration User's Guide

[3] Configuration Management Platform Wireless User's Guide

[4] Policy End Wireless User's Guide

1.3 Acronyms

An alphabetized list of acronyms used in the document.

Table 1. Acronyms

Acronym	Definition
CLI	Command Line Interface
CMP	Configuration Management Platform
CSR	Customer Service Request
GUI	Graphical User Interface
HIDS	Host Intrusion Detection System
IKE	Internet Key Exchange
IPsec	Internet Protocol security
IV	Initialization Vector
LDAP	Lightweight Directory Access Protocol
OHC	Oracle Help Center
OS	Operating System
SOAP	Simple Object Access Protocol
SNMP	Simple Network Management Protocol
SSO	Single Sign On
TLS	Transport Layer Security

2. Oracle Communications Policy Management Security Overview

This chapter provides an overview of Oracle Communications Policy Management 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 Policy Management 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 Policy Management OS Standard Features, for more information.
- **Change default passwords**. The initial installation of the Policy Management software uses default passwords. These should be changed at installation time. (See Change Passwords for all Policy Management 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 Policy Management 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 Policy Management security features**. See Section 3 Implement Oracle Communications Policy Management 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 Policy Management System

There are three ways a user can access the Oracle Communications Policy Management system.

1. **Web browser GUI** – The client access to the Oracle Communications Policy Management graphical user interface (GUI) supporting industry-standard Web technologies (for example, SSL, HTTP, HTTPS, IPv4, IPv6, and XML). This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. When a user accesses the Policy Management system via the GUI interface, the Log In screen displays. Enter the **Username** and **Password** credentials, and click **Log In** to access the GUI. Access is controlled by a standard username/password login scheme.

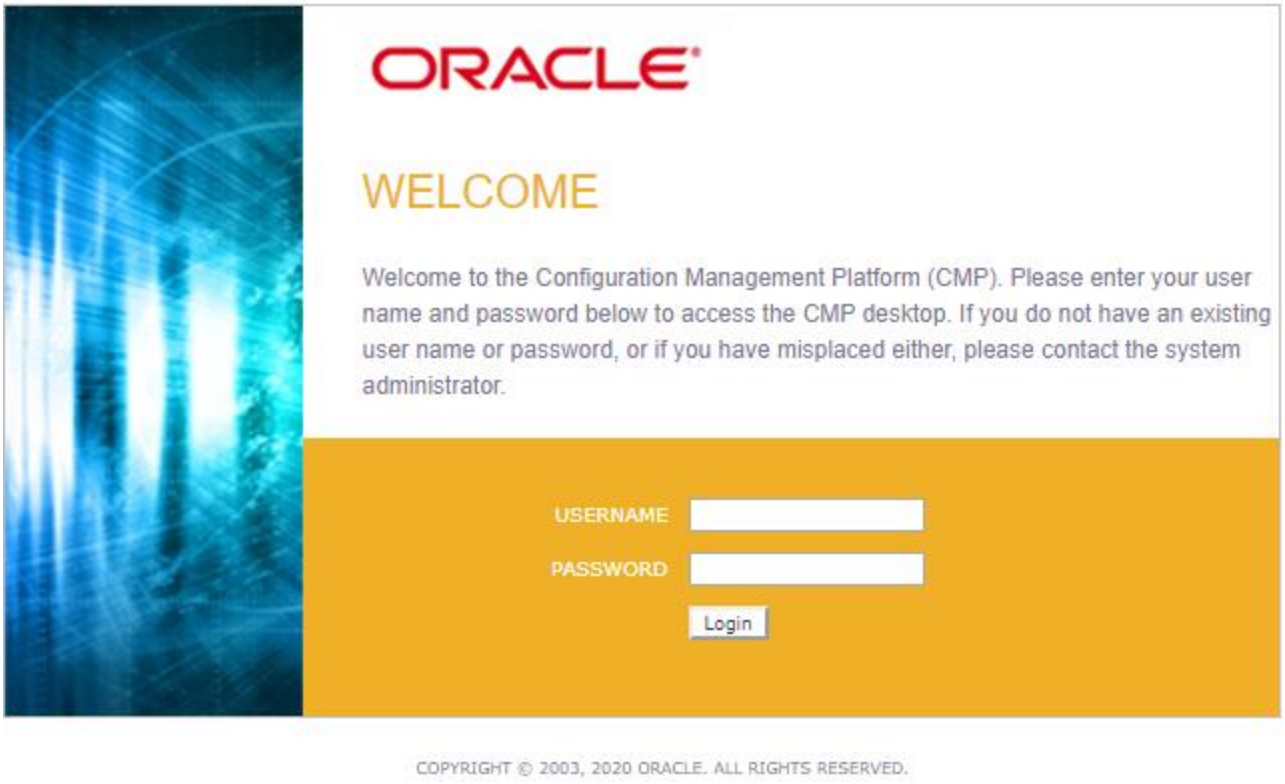


Figure 1. Oracle Communications Policy Management Login Page

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

Figure 2. Oracle Communications Policy Management Home Page

2. **CLI via SSH client** – Normal login access is remote through network connections. The client access to the command line interface (CLI) is with an SSH capable client such as PUTTY, SecureCRT, or similar client using the default administrative login account. SSH login is supported on the distinct management interface. To logout, enter the command, **exit**, 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 Web GUI access – Proliant Server iLO provides web GUI access from a web browser 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 Policy Management Security

Oracle Communications Policy Management 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 Policy Management Security

Oracle Communications Policy Management 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 Policy Management 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, Policy Management 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.

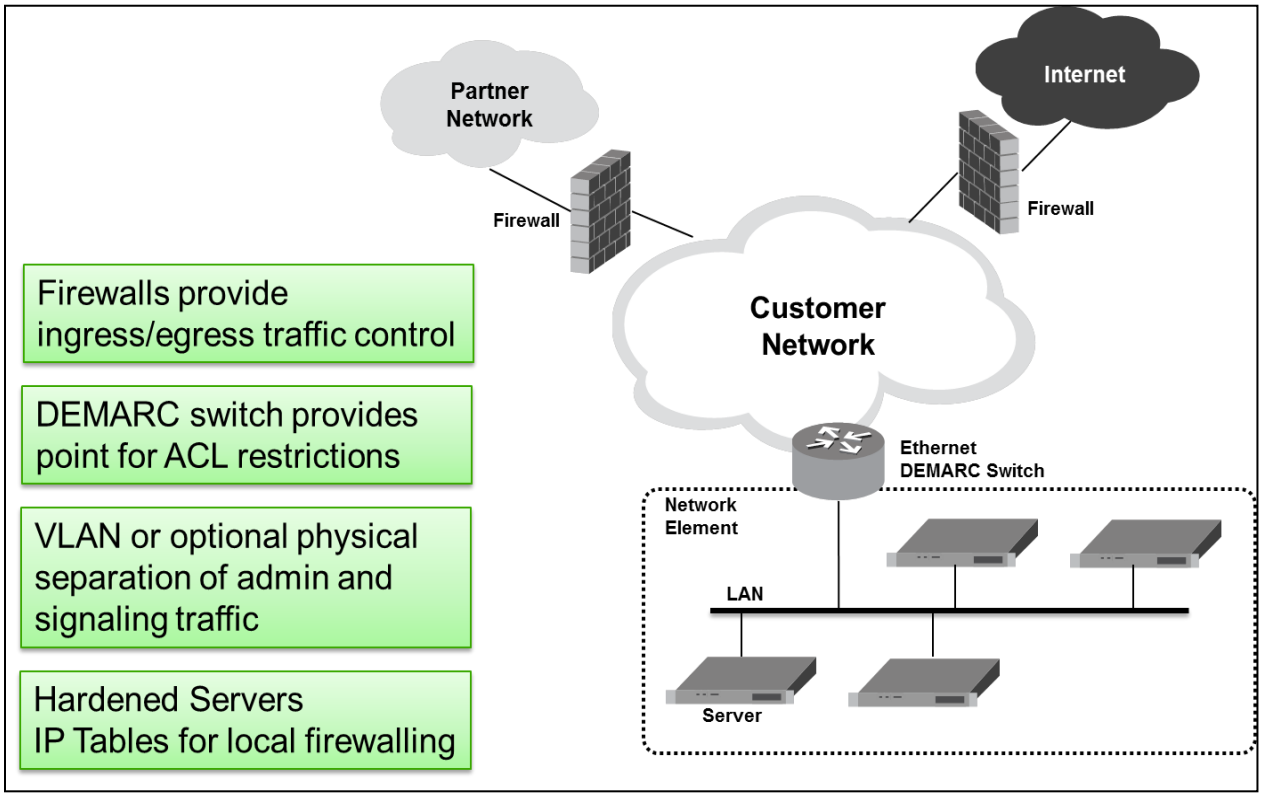


Figure 3. Oracle Communications Policy Management Generic DSR Deployment Model for a Generic Model of the Deployment Strategy

3. Implement Oracle Communications Policy Management Security

This chapter explains security-related configuration settings that may be applied to Oracle Communications Policy Management.

3.1 Oracle Communications Policy Management Web GUI Standard Features

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

3.1.1 User Administration

The CMP system lets you configure the following user attributes:

- Role
- Scope
- Users

There is a pre-defined admin and group delivered with the system for setting up the roles, scope and users by the customer. The following are details for this pre-defined admin.

Table 2. Predefined User and Group

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

The **admin** user is the only profile that cannot be deleted or have its username modified. Also, the **admin** user is the only user who can create, modify, or delete other users. The password assigned to the **admin** user can be changed. For security reasons, Oracle recommends changing this value from its default value as soon as the system is installed.

Note: When logging in, the username is not case sensitive; however, the password is case sensitive.

Each user needs to be associated with a role (what user can do) and scope (Context of the role). For more details on user administration, see the **About Managing Users** section in *Configuration Management Platform Wireless User's Guide*.

3.1.1.1 Configuring Roles

Assigning roles to the various users that access the CMP system lets you control who can configure and access what within the CMP system. The default roles are:

- Viewer: Permits read-only access to functions associated with Policy Management device management and configuration. Access is also permitted to limited system administration functions, such as Change Password.
- Operator — Permits full read/write access to all Policy Management device management and configuration functions. Access is also permitted to all system administration functions except user administration.
- Administrator — Permits full read/write access to all functions. You cannot delete the Administrator role.

The permissions in the **Role Administration** page are grouped into these sections:

- Policy Server Privileges
- Subscriber Privileges
- SPR Privileges
- Network Privileges
- MRA Privileges
- Policy Management Privileges
- System Wide Report Privileges
- Platform Setting Privileges
- Upgrade Manager Privileges
- System Administration Privileges

For more details on user roles and the permissions, see the **About Managing Users** section in *Configuration Management Platform Wireless User's Guide*.

3.1.1.2 Creating a New Scope

You can configure scopes that contain selections of network element groups and Policy Management device groups that provide a context for a role. This lets you control what areas or devices in a network a user can manage. The default scope, Global, contains all items defined within the CMP database. Once you define a scope you can apply it to a user.

For more details on user scopes, see the **About Managing Users** section in *Configuration Management Platform Wireless User's Guide*.

3.1.1.3 User Profiles

The User Management functions include the tools necessary to create, modify, or delete system user profiles. The CMP system is configured initially with the following default user profiles and passwords:

- admin / policies (you cannot delete this profile)
- operator / policies
- viewer / policies

Each default user profile has an associated role assigned to it. The **admin** user is the only profile that cannot be deleted or have its username modified. Also, the **admin** user is the only user who can create, modify, or delete other users. The password assigned to the **admin** user can be changed. For security reasons, Oracle recommends changing this value from its default value as soon as the system is installed.

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 **New User Configuration** page displays these elements:

- User Name
- Description/Location

- Password and Confirm Password
- Password Expiration Period
- Force to Change Password
- Role
- Scopes

For more details on these elements, see the **About User Profiles** section in *Configuration Management Platform Wireless User's Guide*.

3.1.2 GUI User Authentication

Users are authenticated using either login credentials or Single Sign-On. See the Passwords section under the **System Settings** section in *Configuration Management Platform Wireless User's 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.

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. See the Passwords section under the **System Settings** section in *Configuration Management Platform Wireless User's Guide* for more details on password setup.

3.1.2.2 Change Passwords for all Policy Management Administrative Accounts

The System Installation procedure creates these default accounts:

- **admin** – for Oracle Communications Policy Management Application GUI
- **root** – for CLI
- **admusr** – for CLI
- **configUser** – 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 Passwords section under the **System Settings** section in *Configuration Management Platform Wireless User's Guide*.

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.

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 **Configuring System Settings** section in *Configuration Management Platform Wireless User's Guide.*

3.1.2.5 Restrict Concurrent GUI Logins

The **System Settings** page has **Maximum Concurrent Sessions Per User Account (0=unlimited)** 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.

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 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, see the **About External Authentication** section in *Configuration Management Platform Wireless User's Guide*.

3.1.2.8 Set Password Strength Minimum Digit Characters

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

1. Login as **admusr** on the server using below command:

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

2. Checkout the file system-auth and grep for variable 'dcredit' in the file using below command:

   ```
   $ sudo rcstool co /etc/pam.d/system-auth
   $ grep "dcredit=" /etc/pam.d/system-auth
   ```

3. If no result is returned then execute below command:

   ```
   $ sudo sed -i --follow-symlinks "/pam_cracklib.so/ s/$/ dcredit=-2/"
   /etc/pam.d/system-auth
   ```

If some result is returned by executing Step 2, then execute the below command:

```
sudo sed -i --follow-symlinks "s/\(dcredit *= *\).*/\1-2/"
/etc/pam.d/system-auth
```

4. Checkin the file `system-auth` using below command:

```
$ sudo rcstool ci /etc/pam.d/system-auth
```

3.1.2.9 Set Password Strength Use Dictionary

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

1. Login as **admusr** on the server using below command:

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

2. Checkout the file system-auth using below command:

```
$ sudo rcstool co /etc/pam.d/system-auth
$ grep "dictpath" /etc/pam.d/system-auth
```

3. If no result is returned then run the below command:

```
$ sudo sed -i --follow-symlinks '/password.*pam_cracklib.so/ s/$/
    dictpath=\/usr\/share\/cracklib\/pw_dict/' /etc/pam.d/system-auth
```

4. Checkin the file `system-auth` using below command:

```
$ sudo rcstool ci /etc/pam.d/system-auth
```

3.1.2.10 Set Password Strength Minimum Length

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

1. Login as **admusr** on the server using below command:

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

2. Checkout the file system-auth and grep for variable 'minlen' in the file using below command:

```
$ sudo rcstool co /etc/pam.d/system-auth
$ grep minlen /etc/pam.d/system-auth
```

3. If no result is returned from step 2, then run below command:

```
$ sudo sed -i --follow-symlinks "/pam_cracklib.so/ s/$/ minlen=14/"
/etc/pam.d/system-auth
```

If some result is returned from step 2, then run below command:

```
sudo sed -i --follow-symlinks '/password.*pam_cracklib.so/
s/minlen=./minlen=14/' /etc/pam.d/system-auth
```

4. Checkin the file `system-auth` using below command:

```
$ sudo rcstool ci /etc/pam.d/system-auth
```

3.1.2.11 Set Password Strength Minimum Uppercase Characters

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

1. Login as **admusr** on the server using below command:

```
login: admusr
```

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

2. Checkout the file system-auth and grep for variable ‘ucredit’ in the file using below command:

```
$ sudo rcstool co /etc/pam.d/system-auth
$ grep “ucredit=” /etc/pam.d/system-auth
```

3. If no result is returned then execute below command:

```
$ sudo sed -i --follow-symlinks "/pam_cracklib.so/ s/$/ ucredit=-2/"
/etc/pam.d/system-auth
```

If some result is returned by executing Step 2, then execute the below command:

```
sudo sed -i --follow-symlinks "s/\(ucredit *= *\).*/\1-2/"
/etc/pam.d/system-auth
```

4. Checkin the file `system-auth` using below command:

```
$ sudo rcstool ci /etc/pam.d/system-auth
```

3.1.2.12 Set Password Strength Minimum Special Characters

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

1. Login as **admusr** on the server using below command:

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

2. Checkout the file system-auth and grep for variable ‘ocredit’ in the file using below command:

```
$ sudo rcstool co /etc/pam.d/system-auth
$ grep “ocredit=” /etc/pam.d/system-auth
```

3. If no result is returned then execute below command:

```
$ sudo sed -i --follow-symlinks "/pam_cracklib.so/ s/$/ ocredit=-2/"
/etc/pam.d/system-auth
```

If some result is returned by executing Step 2, then execute the below command:

```
sudo sed -i --follow-symlinks "s/\(ocredit *= *\).*/\1-2/"
/etc/pam.d/system-auth
```

4. Checkin the file `system-auth` using below command:

```
$ sudo rcstool ci /etc/pam.d/system-auth
```

3.1.2.13 Set Password Strength Minimum Lowercase Characters

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

1. Login as **admusr** on the server using below command:

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

2. Checkout the file system-auth and grep for variable ‘lcredit’ in the file using below command:

```
$ sudo rcstool co /etc/pam.d/system-auth
$ grep “lcredit=” /etc/pam.d/system-auth
```

3. If no result is returned then execute below command:

```
$ sudo sed -i --follow-symlinks "/pam_cracklib.so/ s/$/ lcredit=-2/"
/etc/pam.d/system-auth
```

If some result is returned by executing Step 2, then execute the below command:

```
sudo sed -i --follow-symlinks "s/\(lcredit *= *\).*/\1-2/"
/etc/pam.d/system-auth
```

4. Checkin the file `system-auth` using below command:

```
$ sudo rcstool ci /etc/pam.d/system-auth
```

3.1.2.14 Set Deny for Failed Password Attempts

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

1. Login as **admusr** on the server using below command:

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

2. Checkout the file `system-auth` and `password-auth` using below command:

```
 $ sudo rcstool co /etc/pam.d/system-auth
 $ grep "lcredit=" /etc/pam.d/system-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
```

4. Checkin the file `system-auth` and `password-auth` using below command:

```
$ sudo rcstool ci /etc/pam.d/system-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 Policy Management GUI as an administrator user, the **System Settings** page under **System Administration** enables the administrative user to view a list of global options.

The **Login Banner Title** 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 **Login Banner Text** 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:

1. Login as **admusr** on the server using below command:
   ```
   login: admusr
   Password: <current admin user password>
   ```
2. Checkout the file `sshd_config` and grep for variable 'ClientAliveCountMax' in the file using below command:
   ```
   $ sudo rcstool co /etc/ssh/sshd_config
   $ sudo grep ^ClientAliveCountMax /etc/ssh/sshd_config
   ```
3. If no result is returned then execute below command:
   ```
   $ sudo echo "ClientAliveCountMax 0" >> /etc/ssh/sshd_config
   ```
   If some result is returned by executing Step 2, then execute the below command:
   ```
   $ sudo sed -i "s/ClientAliveCountMax.*/ClientAliveCountMax 0/g"
   /etc/ssh/sshd_config
   ```
4. Checkin the file `sshd_config` using below command:
   ```
   $ sudo rcstool ci /etc/ssh/sshd_config
   ```
5. Restart sshd service using below command:
   ```
   $ sudo service sshd restart
   ```

3.1.4.2 Disable SSH Access via Empty Passwords

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

1. Login as **admusr** on the server using below command:
   ```
   login: admusr
   Password: <current admin user password>
   ```
2. Checkout 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, then execute the below command:
   ```
   $ sudo sed -i "s/PermitEmptyPasswords.*/ PermitEmptyPasswords no/g"
   /etc/ssh/sshd_config
   ```
4. Checkin the file `sshd_config` using below command:
   ```
   $ sudo rcstool ci /etc/ssh/sshd_config
   ```

5. Restart sshd service using below command:

```
$ sudo service sshd restart
```

3.1.4.3 Enable SSH Warning Banner

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

1. Login as **admusr** on the server using below command:

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

2. Checkout the file `sshd_config` and grep for variable 'Banner' in the file using below command:

```
$ sudo rcstool co /etc/ssh/sshd_config
$ sudo grep ^Banner /etc/ssh/sshd_config
```

3. If no result is returned then execute below command:

```
$ sudo echo "Banner /etc/issue" >> /etc/ssh/sshd_config
```

   If some result is returned by executing Step 2, then execute the below command:

```
$ sudo sed -i "s/Banner.*/Banner \/etc\/issue/g" /etc/ssh/sshd_config
```

4. Checkin the file `sshd_config` using below command:

```
$ sudo rcstool ci /etc/ssh/sshd_config
```

5. Restart sshd service using below command:

```
$ sudo service sshd restart
```

3.1.4.4 Do not allow SSH Environment Options

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

1. Login as **admusr** on the server using below command:

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

2. Checkout 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, then execute the below command:

```
$ sudo sed -i "s/PermitUserEnvironment.*/PermitUserEnvironment no/g"
/etc/ssh/sshd_config
```

4. Checkin the file `sshd_config` using below command:

```
$ sudo rcstool ci /etc/ssh/sshd_config
```

5. Restart sshd service using below command:

```
$ sudo service sshd restart
```

3.1.4.5 Disable Root User Login

Note: Before disabling root user at any node, make sure the system is not in mixed state and all the clusters are upgraded to OCPM 12.6.1. Disabling Root User Login is a security feature that needs to be reverted, from every node in the topology, before attempting a rollback of an upgraded application.

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

1. Login as **admusr** on the server using below command:

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

2. Checkout the file `sshd_config` and grep for variable 'PermitRootLogin' in the file using below command:

   ```
   $ sudo rcstool co /etc/ssh/sshd_config
   $ sudo grep ^PermitRootLogin /etc/ssh/sshd_config
   ```

3. If no result is returned then run below command:

   ```
   $ sudo echo "PermitRootLogin no" >> /etc/ssh/sshd_config
   ```

   If some result is returned by executing Step 2, then execute the below command:

   ```
   $ sudo sed -i "s/PermitRootLogin.*/PermitRootLogin no/g"
   /etc/ssh/sshd_config
   ```

4. Checkin the file `sshd_config` using below command:

   ```
   $ sudo rcstool ci /etc/ssh/sshd_config
   ```

5. Restart sshd service using below command:

   ```
   $ sudo service sshd restart
   ```

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:

1. Login as **admusr** on the server using below command:

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

2. Remove the tftp-server package using below 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:

1. Login as **admusr** on the server using below command:

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

2. Disable xinetd for all run levels and Stop xinetd, if currently running, using below command:

   ```
   $ 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:

1. Login as **admusr** on the server using below command:
   ```
   login: admusr
   Password: <current admin user password>
   ```
2. Disable xinetd for all run levels and Stop xinetd, if currently running, using below command:
   ```
   $ sudo yum erase xinetd
   ```

3.1.5.4 Disable ntpdate Service

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

1. Login as **admusr** on the server using below command:
   ```
   login: admusr
   Password: <current admin user password>
   ```
2. Disable `ntpdate` service using below command:
   ```
   $ sudo chkconfig ntpdate off
   ```

3.1.6 Upgrade Manager

The Upgrade Manager allows you to manage upgrade ISOs and perform software upgrades on servers in the topology. The upgrade process allows a geo redundant site to be upgraded in serial order, so no data is lost and there is no down time. During the upgrade process, the System Maintenance page displays the upgrade status. Note that access to these GUI options can be affected by settings on the role setting page. For specific steps on performing an upgrade, contact the Oracle Customer Care Center.

For more details on ISO files and performing upgrades see the section **Upgrade Manager** in *Configuration Management Platform Wireless User's Guide*.

3.1.7 SNMP Configuration

The application has an interface to retrieve alarms from a remote location using the industry-standard Simple Network Management Protocol (SNMP) interface. Only the active Network CMP server allows SNMP administration. For more details, see the *Policy Management SNMP User's Guide*.

The Active CMP 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 Settings** 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, see the **Configuring SNMP Settings** section in *Configuration Management Platform Wireless User's Guide*.

3.1.7.1 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.

3.1.7.2 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."

3.1.8 Performing System and Server Backups and Restores

The platcfg utility provides GUI menu for performing Backups and Restores for Servers and Systems. The details are provided in section **Performing System and Server Backups and Restores** in *Plaform Configuration User's Guide*.

3.1.9 Exporting and Purging Audit Log Data

The CMP system provides functionality to export the audit log files securely. The System provides the downloadable audit log file based on the selection criteria of the user. For more details please see the section **Exporting or Purging Audit Log Data** under the chapter **System Administration** in *Configuration Management Platform Wireless User's Guide*.

3.1.10 Certificate Management

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

Normal web traffic is sent unencrypted over the Internet, which allows anyone with access to the right tools to snoop and view all of that traffic and data. This can lead to problems, especially where security and privacy is necessary. To combat this, the Secure Socket Layer (SSL) is used to encrypt the data

stream between the web server and the web client (the browser). Each SSL Certificate consists of a public key and a private key. The public key is shared with other SSL clients and is used to set up secure sessions, while the private key never leaves the server. When a Web browser points to a secured domain, an SSL handshake authenticates the server and the client. The Policy Management uses the Platform Configuration (platcfg) utility to manage SSL security certificates, which allow two systems to interact with a high level of security.

The following are common terms used:

• Local certificate - the certificate created on the local system and then exported to the peer system.

• Peer certificate - the certificate created on the peer system that is imported by the local system.

• Private/Public Key - As previously stated, the public key is used to encrypt information and the private key is used to decipher it.

See the *Platform Configuration User's Guide* for information on creating and exchanging security certificates within and between Policy Management clusters to support secure communication. .

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 CMP 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.

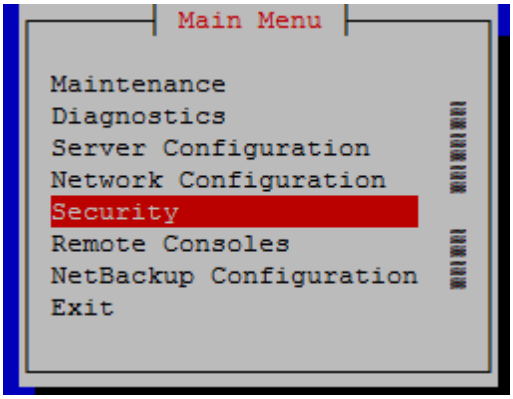
No other system resources (files, processes, actions, etc.) are monitored by HIDS.

Customers can view active alarms in the platcfg GUI. The Customers can view active alarms on the Oracle Communications Policy Management GUI by navigating to **Alarms** under **System Wide Reports** section of the navigation pane.

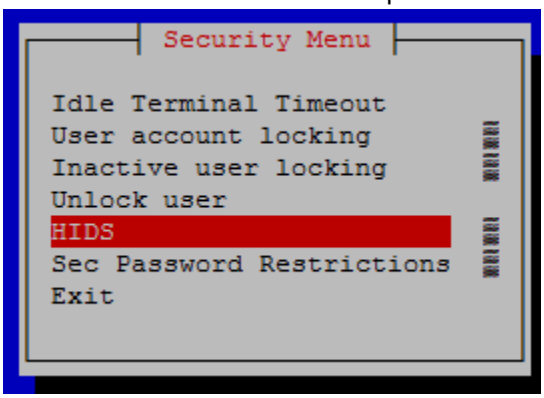
3.2.2 Determine Host Intrusion Detection System (HIDS) Status

The HIDS status for the server is displayed along the top of the HIDS menu window. Execute the below procedure to check the HIDS status:

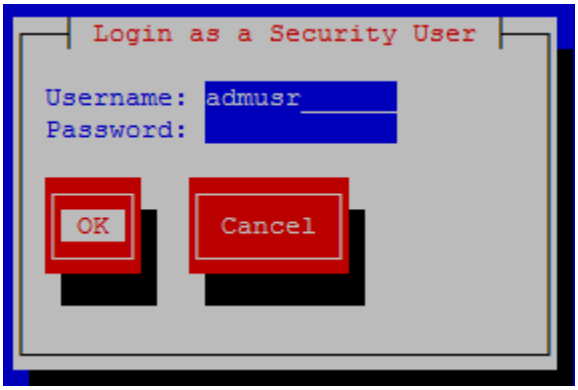
1. Login as **admusr** on the server using below command:
   ```
   login: admusr
   Password: <current admin user password>
   ```
2. Open the **platcfg** menu by entering this command:
   ```
   $ sudo su - platcfg
   ```
3. Select **Security** from the menu and press **Enter**.



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



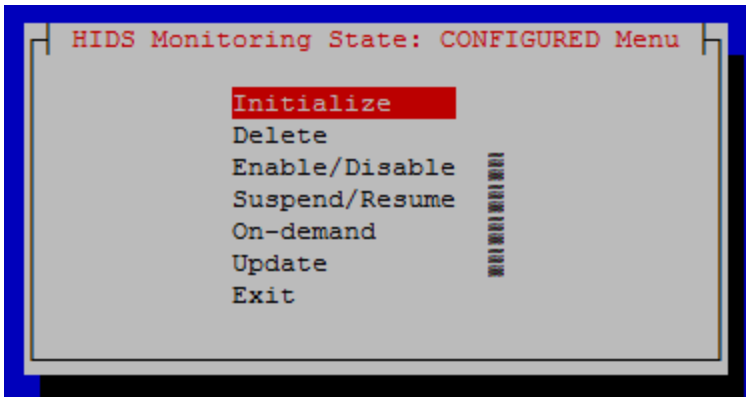
5. To check **HIDS** status, enter the **Username** and **Password** for a user that is part of the **secgrp** group.



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

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

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

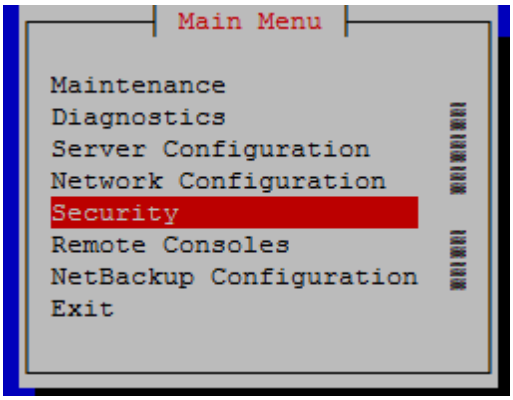


6. Select **Exit** in each of the menus until a command prompt is reached.

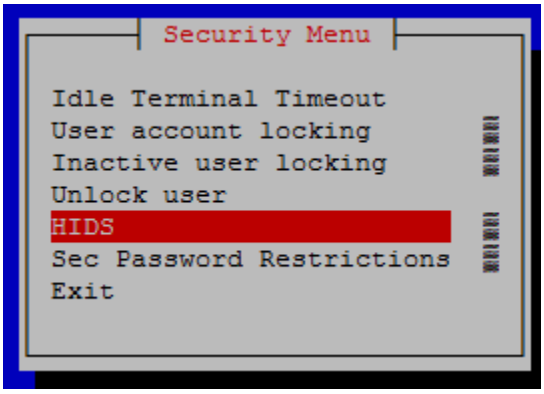
3.2.3 Initialize Host Intrusion Detection System (HIDS)

The Host Intrusion Detection System (HIDS) feature must be initialized before enabling HIDS for the first time on a system. Execute the below procedure to initialize the HIDS:

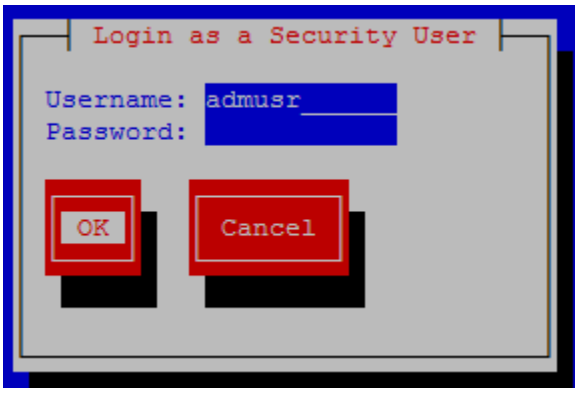
1. Login as **admusr** on the server using below command:
   ```
   login: admusr
   Password: <current admin user password>
   ```
2. Open the **platcfg** menu by entering this command:
   ```
   $ sudo su - platcfg
   ```
3. Select **Security** from the menu and press **Enter**.



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



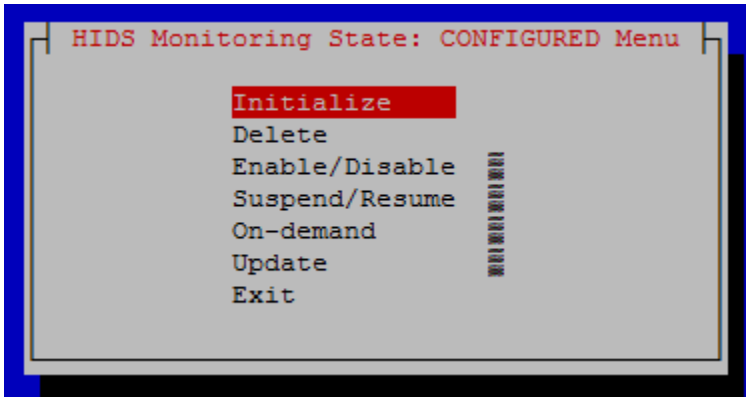
5. To check **HIDS** status, enter the **Username** and **Password** for a user that is part of the **secgrp** group.



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

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

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



6. Select **Initialize** and press **Enter**.
7. Select **Yes** and press **Enter**. After the HIDS baseline successfully initialized message displays, **press any key to continue**.
8. 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. Execute the below procedure to enable/disable the HIDS:

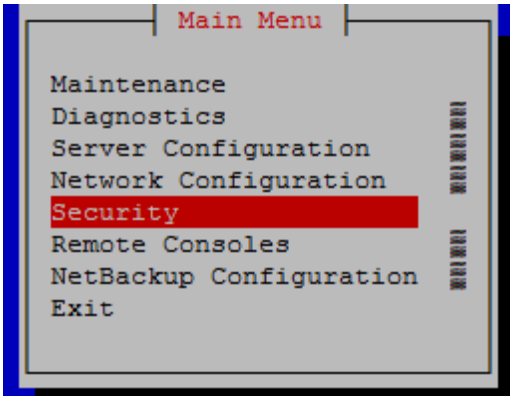
1. Login as **admusr** on the server using below command:

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

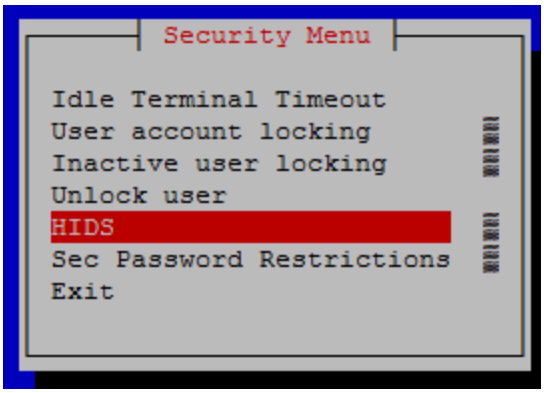
2. Open the **platcfg** menu by entering this command:

```
$ sudo su - platcfg
```

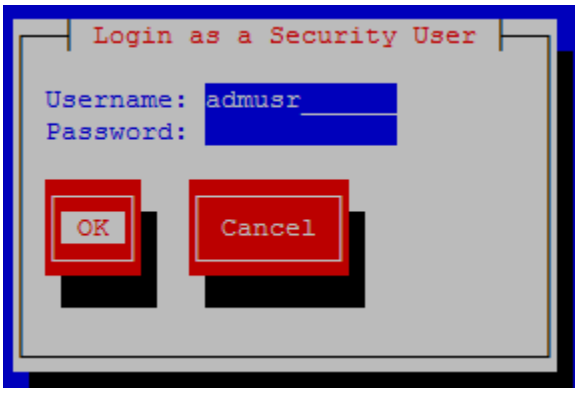
3. Select **Security** from the menu and press **Enter**.



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



5. To check **HIDS** status, enter the **Username** and **Password** for a user that is part of the **secgrp** group.

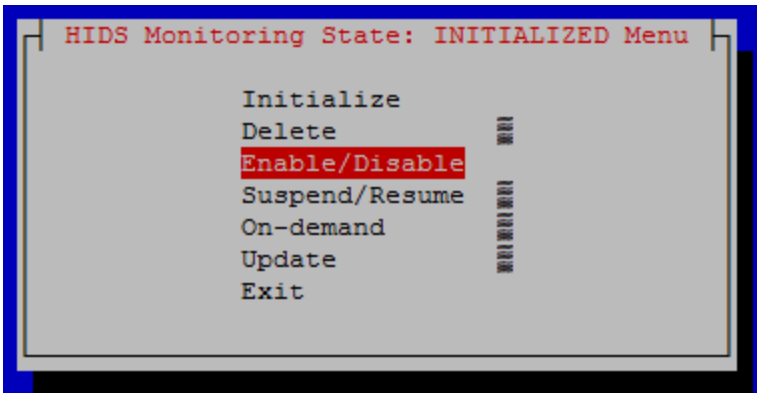


Note: By default, **admusr** is part of the **secgrp** group.

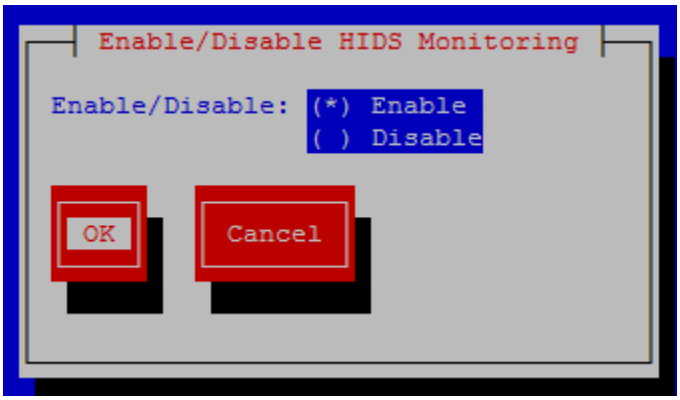
Click **OK** and press **Enter**.

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

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



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

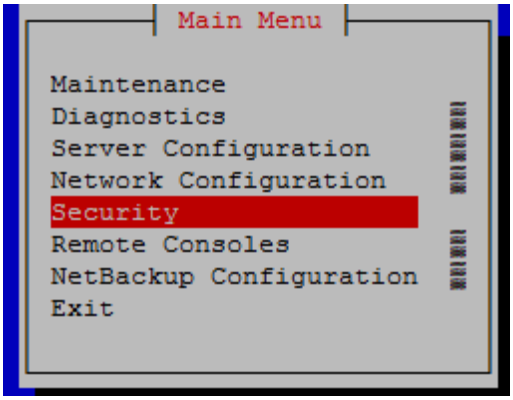


8. Click **OK** and press **Enter**. After the message box that indicates that DB monitoring has been enabled/disabled or a failure message displays, **press any key to continue**.
9. Select **Exit** in each of the menus until a command prompt is reached.

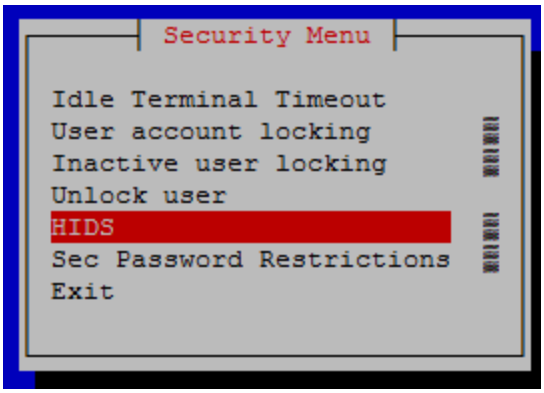
3.2.5 Suspend or Resume Host Intrusion Detection System (HIDS)

The HIDS monitoring can temporarily by suspended or resumed on a system that has HIDS enabled. Execute the below procedure to suspend/resume the HIDS:

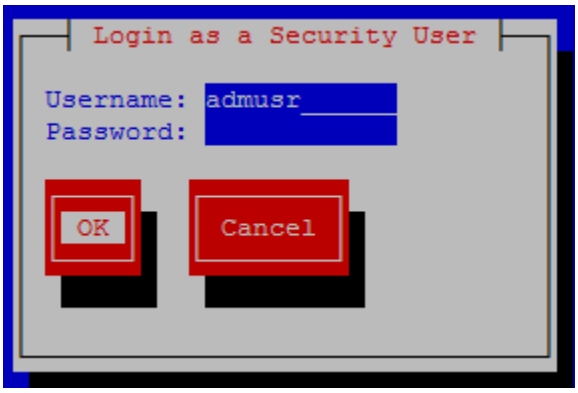
1. Login as **admusr** on the server using below command:
   ```
   login: admusr
   Password: <current admin user password>
   ```
2. Open the **platcfg** menu by entering this command:
   ```
   $ sudo su - platcfg
   ```
3. Select **Security** from the menu and press **Enter**.



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



5. To check **HIDS** status, enter the **Username** and **Password** for a user that is part of the **secgrp** group.

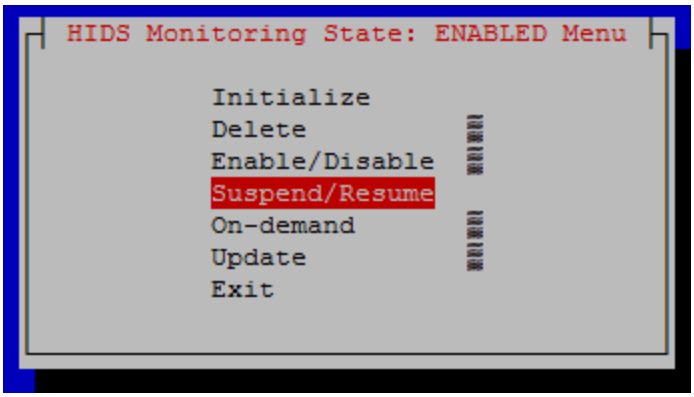


Note: By default, **admusr** is part of the **secgrp** group.

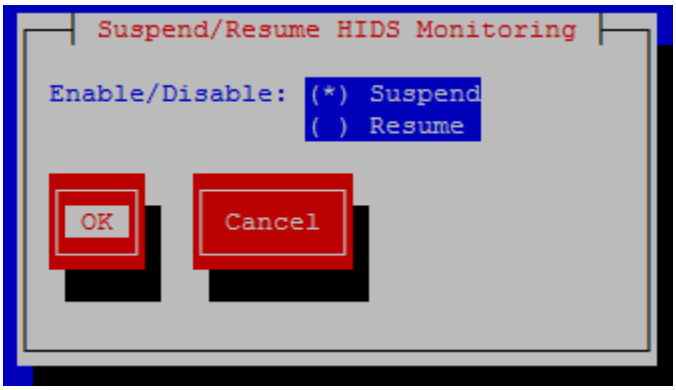
Click **OK** and press **Enter**.

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

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



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

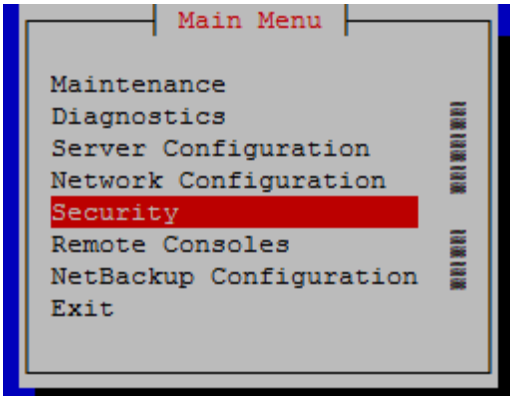


8. Click **OK** and press **Enter**. After the message box that indicates that DB monitoring has been suspended/resumed or a failure message displays, **press any key to continue**.
9. Select **Exit** in each of the menus until a command prompt is reached.

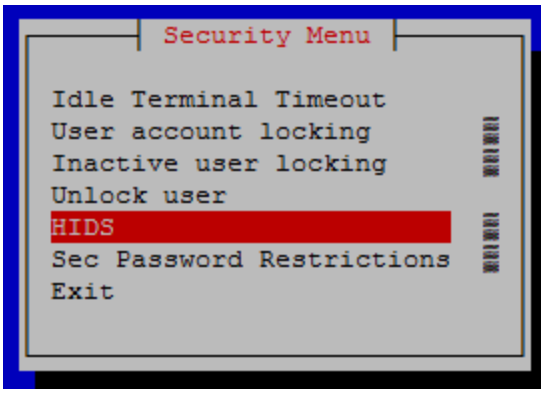
3.2.6 Run On-Demand Host Intrusion Detection System (HIDS) Security Check

The HIDS tests run periodically. A user can force an immediate run of the HIDS tests by using the **On-demand** HIDS menu. Execute the below procedure to run on-demand HIDS security check:

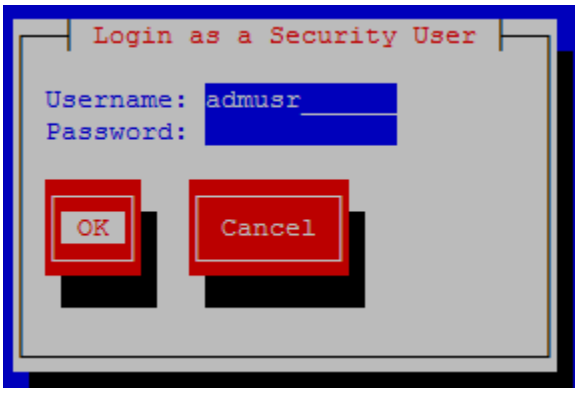
1. Login as **admusr** on the server using below command:
   ```
   login: admusr
   Password: <current admin user password>
   ```
2. Open the **platcfg** menu by entering this command:
   ```
   $ sudo su - platcfg
   ```
3. Select **Security** from the menu and press **Enter**.



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



5. To check **HIDS** status, enter the **Username** and **Password** for a user that is part of the **secgrp** group.

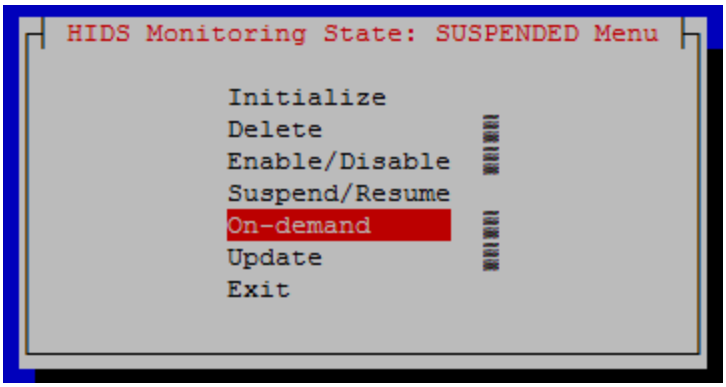


Note: By default, **admusr** is part of the **secgrp** group.

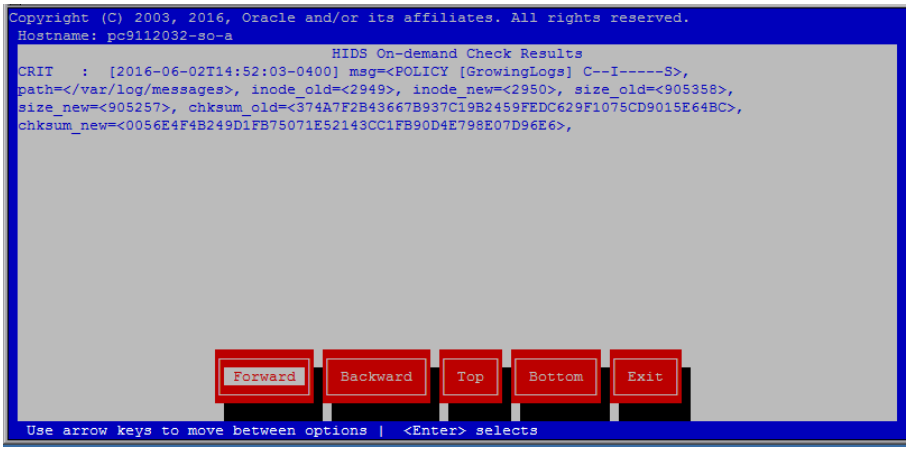
Click **OK** and press **Enter**.

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

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:

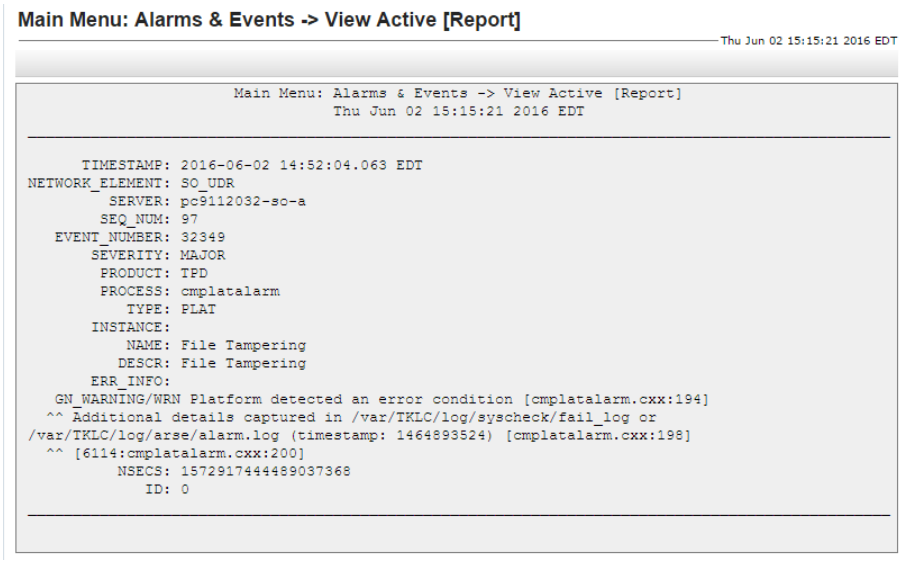


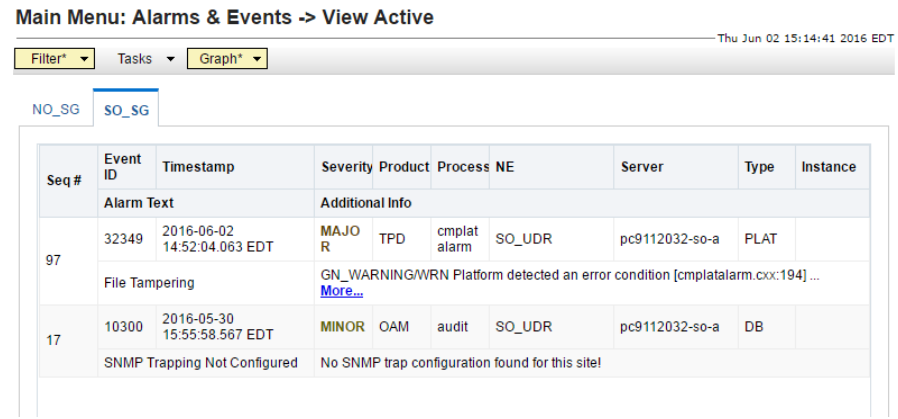
This alarm can also been seen when viewing alarms in the platcfg system, as described in section 3.2.9: Host Intrusion Detection System (HIDS) Alarms.

This alarm is also propagated through normal COMCOL channels ultimately resulting in the alarm being accessible on the Oracle Communications Policy Management GUI by navigating to **System Wide Reports->Alarms-> Active Alarms**, as shown in step 8 and press **Enter**. After the message box that indicates that DB monitoring has been suspended/resumed or a failure message displays, **press any key to continue**.

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

   (optional) Log into the OCPM GUI and navigate to **Alarms & Events > View Active** to view details for the HIDS error. Examples of screens from the current error follow:

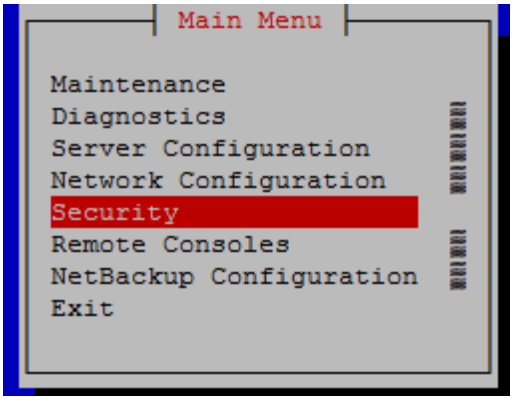




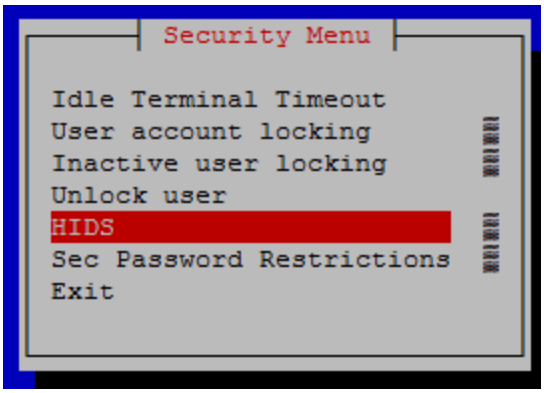
3.2.7 Update Host Intrusion Detection System (HIDS) Baseline

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. Execute the below procedure to update the HIDS baseline:

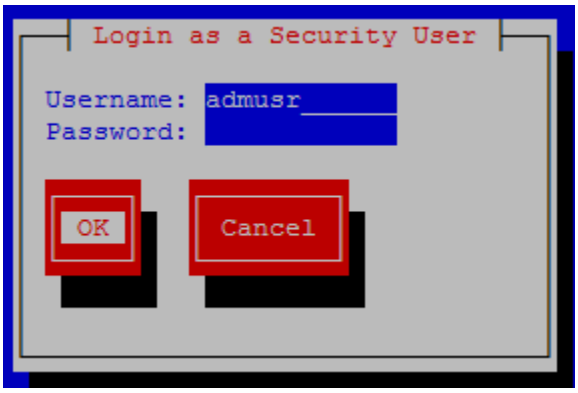
1. Login as **admusr** on the server using below command:
   ```
   login: admusr
   Password: <current admin user password>
   ```
2. Open the **platcfg** menu by entering this command:
   ```
   $ sudo su - platcfg
   ```
3. Select **Security** from the menu and press **Enter**.



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



5. To check **HIDS** status, enter the **Username** and **Password** for a user that is part of the **secgrp** group.

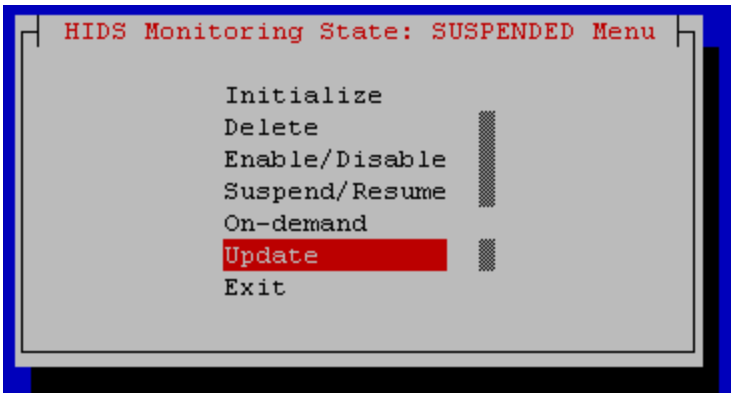


Note: By default, **admusr** is part of the **secgrp** group.

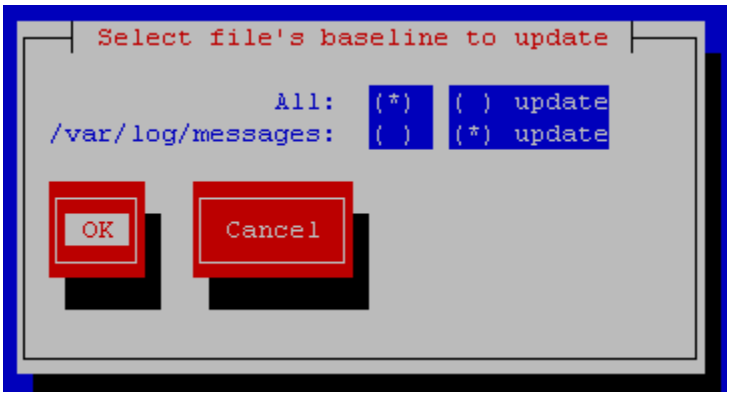
Click **OK** and press **Enter**.

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

6. Select **Update** and press **Enter**.



7. Select **file's baseline** to update.

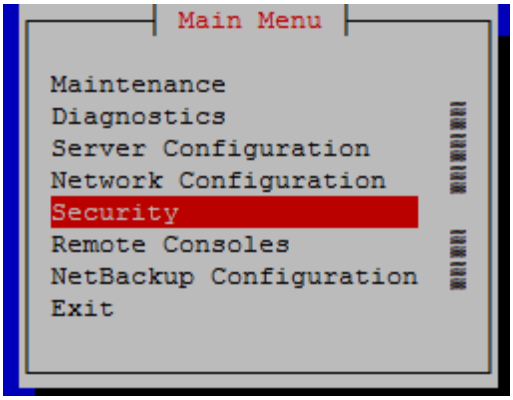


8. Click **OK** and press **Enter**. After the message box that indicates the success/fail result displays, **press any key to continue**.
9. Select **Exit** in each of the menus until a command prompt is reached.

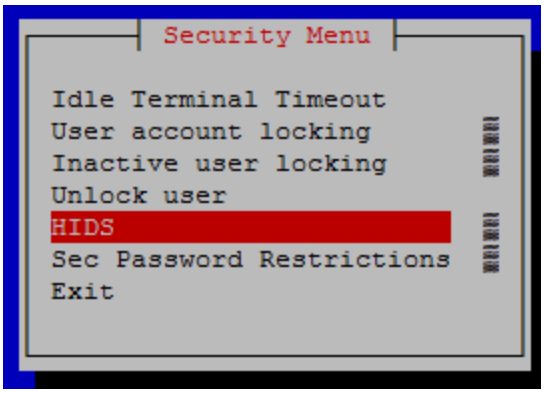
3.2.8 Delete Host Intrusion Detection System (HIDS) Baseline

The HIDS **Delete** menu can be used for permanently disabling HIDS or for backing out of a product upgrade. Execute the below procedure to delete the HIDS baseline:

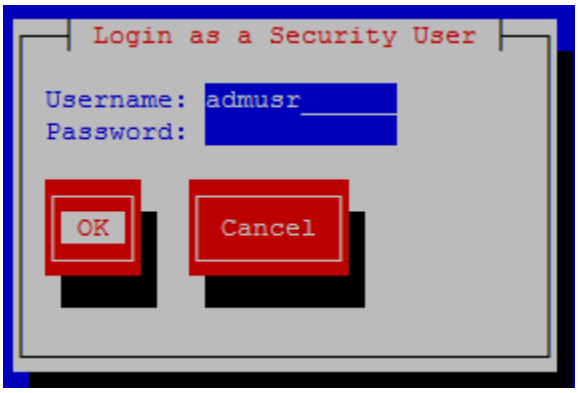
1. Login as **admusr** on the server using below command:
   ```
   login: admusr
   Password: <current admin user password>
   ```
2. Open the **platcfg** menu by entering this command:
   ```
   $ sudo su - platcfg
   ```
3. Select **Security** from the menu and press **Enter**.



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



5. To check **HIDS** status, enter the **Username** and **Password** for a user that is part of the **secgrp** group.

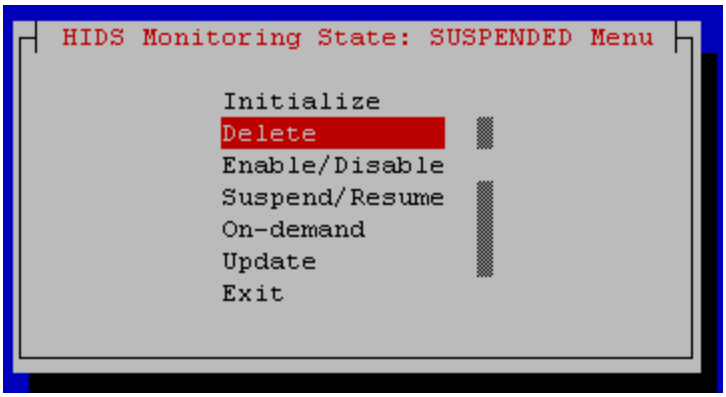


Note: By default, **admusr** is part of the **secgrp** group.

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

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

6. Select **Delete** and press **Enter**.



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

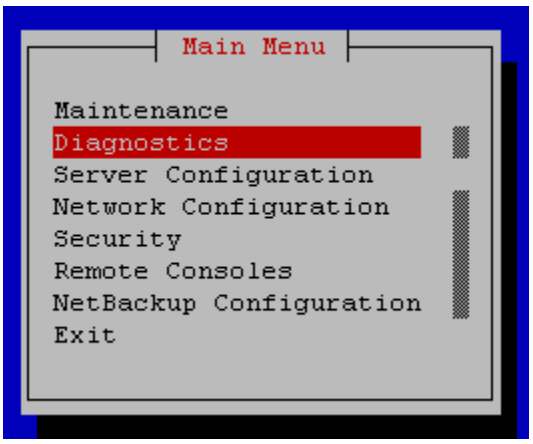
3.2.9 Host Intrusion Detection System (HIDS) Alarms

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:

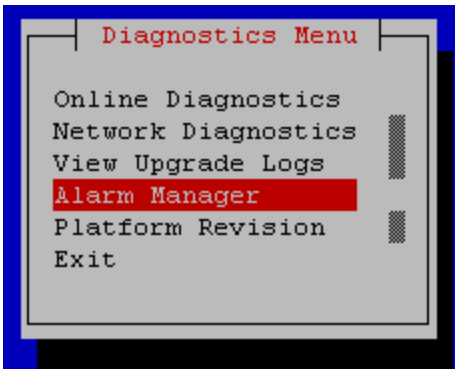
- Customers can view current, previously cleared, and how alarms were cleared in the /var/TKLC/logs/hids/alarms.log file.
- Customers can view active alarms on the GUI on the **System Wide Reports -> Trending Reports ->Alarms -> Active Alarms** GUI screen.

  Customers can view active alarms on the platcfg GUI, including HIDS alarms. Execute the below procedure to view HIDS alarms:

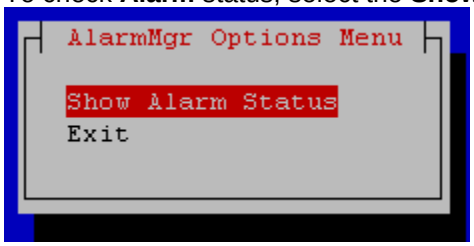
  1. Login as **admusr** on the server using below command:
     ```
     login: admusr
     Password: <current admin user password>
     ```
  2. Open the **platcfg** menu by entering this command:
     ```
     $ sudo su - platcfg
     ```
  3. Select **Diagnostics** from the menu and press **Enter**.



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



5. To check **Alarm** status, select the **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:

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

3.3 Oracle Communications Policy Management OS Standard Features

This section explains the security features of Oracle Communications Policy Management available to the Platform Administrator through the Platform Configuration (Platcfg) utility to configure Policy Management servers.

3.3.1 Configure NTP Servers

Policy Configuration Menu provides GUI menu options to configure policy servers. This menu can be accessed from Platcfg utility by logging in to the server via command line interface (CLI).

This Policy Configuration menu can be used to perform the following operations.

a. Set Policy Mode
b. Restart Application

c. Cluster Configuration Removal
d. Verify Initial Configuration
e. Verify Server Status
f. SSL Key Configuration
g. Ethernet Interface Parameter Settings
h. Save Platform Debug Logs
i. Cluster File Sync
j. Routing Config
k. DSCP Config
l. Firewall
m. Backup and Restore

For the detailed steps on these actions are available in *Platform Configuration User's Guide*.

3.3.1.1 Initial Configuration

Initial Configuration Menu lets the user to define and verify the policy servers settings. See the chapter on **Performing Initial Server Configuration** in *Platform Configuration User's Guide*.

3.3.1.2 Configuring Firewall Settings

Configure firewall settings on the server to restrict access to ports from undesired network interfaces. The detailed steps are in *Platform Configuration User's Guide*, topic **Configuring Firewall Settings** under the chapter **Performing Initial Server Configuration**.

3.3.2 Configure NTP Servers

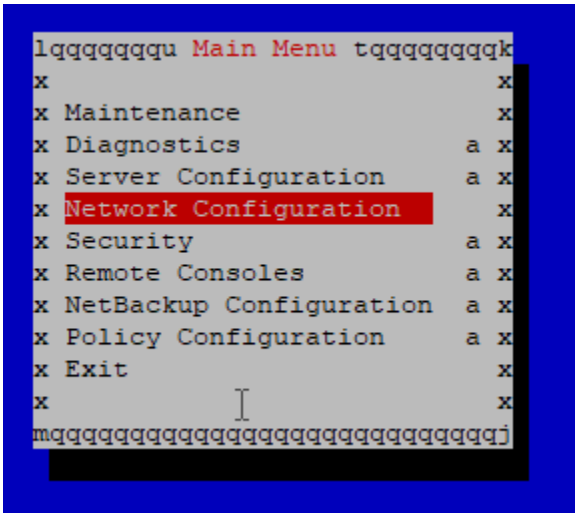
The *platcfg* utility provides GUI menu for configuring NTP server in Policy Management.

For details on configuring a server, see the **About Setting Up the Topology** chapter in *Configuration Management Platform Cable User's Guide*.

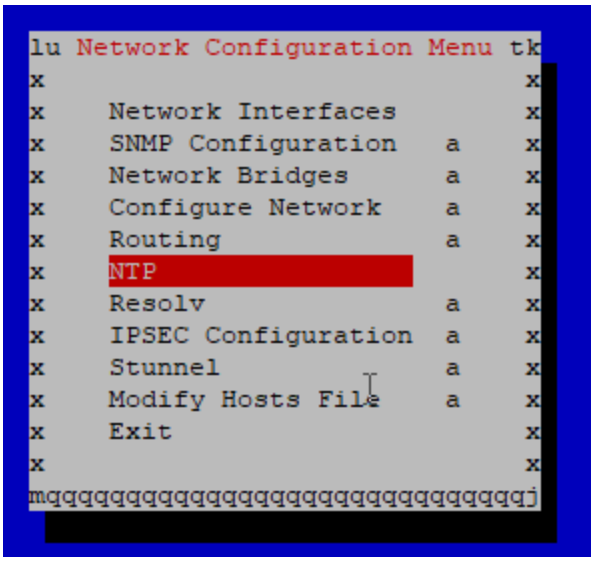
3.3.2.1 Configure NTP for the Host OS of the Application guest VM (CMP)

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

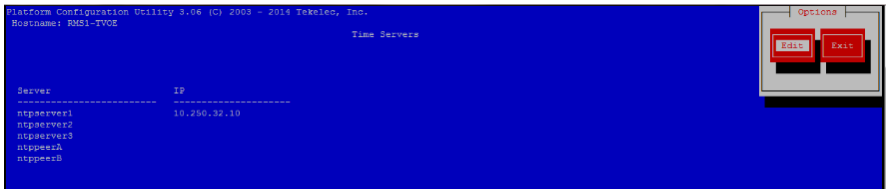
1. Login or switch user to platcfg user on the CMP server. The platcfg main menu displays.
2. Select **Network Configuration** from the menu and press **Enter**.



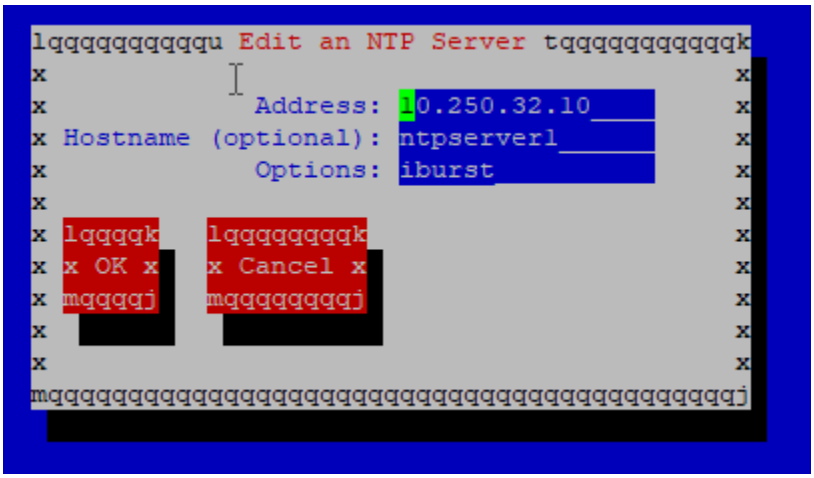
3. Select **NTP** from the menu and press **Enter**.



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



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



5. Exit the platcfg menu. Ensure the time is set correctly by executing the steps in the 3.3.3 Set the Time on the CMP Host.

3.3.3 Set the Time on the CMP Host

At the time of Policy Management installation, the date and time is set on CMP hosts as follows:

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.

3.3.4 Configure Password Settings for OS Users

Use the following procedure to configure various password settings including:

- Minimum acceptable size for the new password
- Minimum number of days allowed between password changes
- Maximum number of days a password may be used
- Number of days a user is warned before password expiration
- Minimum number of characters different between passwords
- Minimum number of passwords between reuse

Here are the steps:

1. Login as **admusr** on the server using below command:
   ```
   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 **Password Restrictions for the Particular User** or **Global Password Restrictions for New Users** as per the requirement option**.**
5. 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
   ```
6. Click **OK** and press **Enter**.
7. 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:

1. Login as **admusr** on the server using below command:
   ```
   login: admusr
   Password: <current admin user password>
   ```
2. Checkout the `system-auth-ac` file using below command:
   ```
   $ sudo rcstool co /etc/pam.d/system-auth-ac
   ```
3. Add the reject_username setting to the system-auth-ac file using below command:
   ```
   $ sudo sed -i -e '/^password.*reject_username/n' \
    -e '/^password.*pam_cracklib.so.*$/s/$/ reject_username/' \
     /etc/pam.d/system-auth-ac
   ```
4. Checkin the file `system-auth-ac` using below command:

```
$ sudo rcstool ci /etc/pam.d/system-auth-ac "reject_username"
```

3.3.5 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

Execute the below procedure to set various session and account settings for OS users:

1. Login as **admusr** on the server using below command:
   ```
   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.

1. Login as **admusr** on the server using below command:
   ```
   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 **User Account Locking** from the menu and press **Enter**.
5. Fill out the following settings:
   ```
   Feature:  ( ) disable (*) enable
   Disable after # of days of inactivity: <max tries>
   Fail interval in minutes: <interval minutes>
   Unlock time in minutes: <unlock time>
   ```
6. Click **OK** and press **Enter**.Click **OK** and press **Enter**.
7. Select **Exit** in each of the menus until a command prompt is reached.

This procedure sets the lockout time for inactive accounts.

1. Login as **admusr** on the server using below command:
   ```
   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
Disable after # of days of inactivity:  <max tries>
```

6. Click **OK** and press **Enter**.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 Require Authentication for Single User Mode

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

1. Login as **admusr** on the server using below command:
   ```
   login: admusr
   Password: <current admin user password>
   ```
2. Checkout the file `init` and grep for variable 'SINGLE' 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, then execute the below command:
   ```
   $ sudo sed -i "s/SINGLE.*/SINGLE=\/sbin\/sulogin/g" /etc/sysconfig/init
   ```
4. Checkin the file `sshd_config` using below command:
   ```
   $ 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.

1. Login as **admusr** on the source server using below command:
   ```
   login: admusr
   Password: <current admin user password>
   ```
2. Change the passwords for each of the accounts being changed using below command:
   ```
   $ 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.
   ```

   Note: Changing the password of '**configUser**' user will update its password expiry information. Password expiry details can be checked using the following command:
   ```
   chage -l <user account>
   ```

To prevent updating non-expired tokens, while changing the password, use the following command to change the password:

```
$ sudo passwd –k configUser
Changing password for user <user account>
Changing password for <user account>
(current) UNIX password: <Enter the current user password – will not display>
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

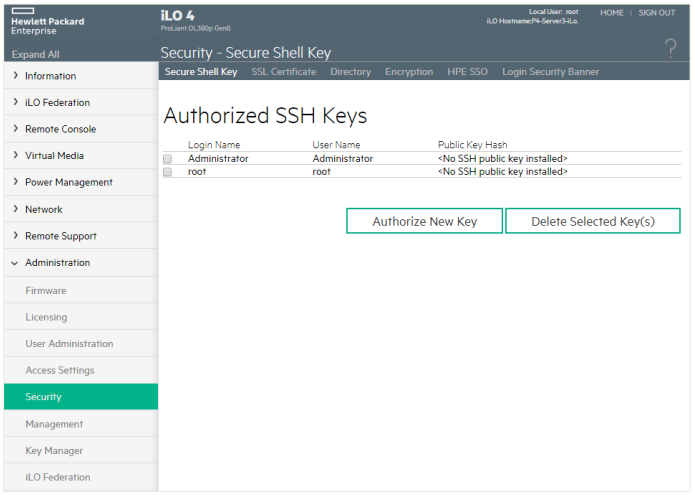
Use the below procedure to change the Login Display Message:

1. Login as **admusr** on the server using below command:
   ```
   login: admusr
   Password: <current admin user password>
   ```
2. Create a backup copy of **sshd_config** using below command:
   ```
   $ sudo cd /etc/ssh
   $ sudo cp sshd_config sshd_config.bak
   ```
3. Edit the **sshd** configuration file using below command:
   ```
   $ sudo rcstool co sshd_config
   $ sudo vi sshd_config
   ```
4. Uncomment the following line:
   ```
   $ Banner /some/path
   ```
5. Edit the line to:
   ```
   Banner /etc/ssh/sshd-banner
   ```
6. Save and exit the **vi** session.
7. Edit the banner file using below command:
   ```
   $ sudo vi sshd-banner
   ```
8. Add and format the desired text. Save and exit the **vi** session.
9. Restart the **sshd** service using below command:
   ```
   $ sudo service sshd restart
   ```
10. Test the change. Repeat steps 4 and 5 until the message is formatted correctly.
    ```
    $ sudo ssh <current server name>
    ```
11. Verify message line feeds are formatted correctly and exit.
    ```
    $ exit
    ```
12. Check the files into **rcs** to preserve changes during upgrades.
    ```
    $ sudo rcstool init /etc/ssh/sshd-banner
    $ sudo rcstool ci sshd_config
    ```

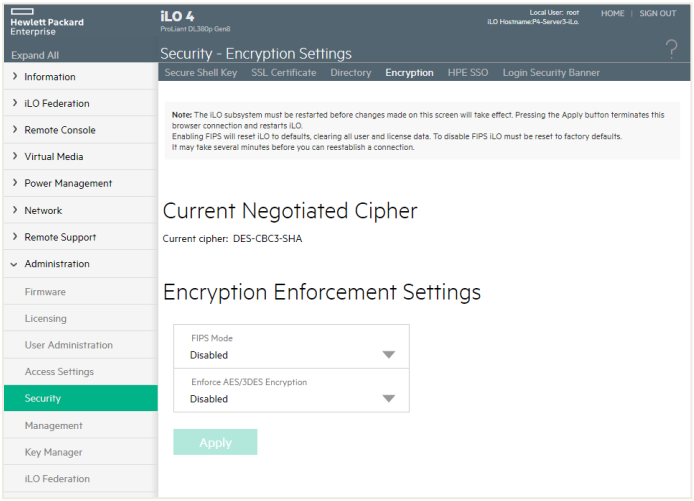
3.4.4 Force iLO to Use Strong Encryption

Login as an administrator to the iLO and execute the below procedure to use strong encryption:

1. On the Administration menu, click **Security**.



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



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

3.4.5 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.

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

1. Login as **admusr** on the server using below command:

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

2. Check out the `plat.admusr.sudo` file using below command:

```
$ sudo rcstool co /usr/TKLC/plat/etc/sudoers.d/plat.admusr.sudo
```

3. Suppress the NOPASSWD line using below command:

```
$ 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 using below command::

```
$ 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.

3.4.6 Report and Disable Expired OS User Accounts

Execute the below procedure to report and disable expired user accounts:

1. Login as **admusr** on the server using below command:
   ```
   login: admusr
   Password: <current admin user password>
   ```
2. Run the report of expired users using below command:
   ```
   $ 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 using below command:
   ```
   $ sudo passwd -l <user acct>
   ```
   Repeat this step for each user account you want to disable.
4. Re-enable an account using below command:
   ```
   $ sudo passwd -u <user acct>
   ```
   Repeat this step for each user account you want to re-enable.

3.4.7 Use JEP Filters

Note: This feature has not been completely tested in Release 12.6.1.

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

1. Login as **admusr** on the server using below command:

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

2. Run the following command:

```
appRev | grep "Product Name"
```

3. If the above command's output contains the string "cmp", run the following steps:

```
a. $ sudo rcstool co /usr/TKLC/camiant/tomcat/bin/run_tomcat.sh
b. $ sudo rcstool co /usr/TKLC/camiant/dc/bin/run_dc.sh
c. $ sudo sed -i -s 's/^UseJEPFilter=.*/UseJEPFilter=true;/'
/usr/TKLC/camiant/dc/bin/run_dc.sh
/usr/TKLC/camiant/tomcat/bin/run_tomcat.sh
d. $ sudo rcstool ci /usr/TKLC/camiant/dc/bin/run_dc.sh
e. $ sudo rcstool ci /usr/TKLC/camiant/tomcat/bin/run_tomcat.sh
```

4. If the above command's output contains the string "mra", run the following steps:

```
a. $ sudo rcstool co /usr/TKLC/camiant/tomcat/bin/run_tomcat.sh
b. $ sudo rcstool co /usr/TKLC/camiant/mra/bin/run_mra.sh
c. $ sudo sed -i -s 's/^UseJEPFilter=.*/UseJEPFilter=true;/'
/usr/TKLC/camiant/mra/bin/run_mra.sh
/usr/TKLC/camiant/tomcat/bin/run_tomcat.sh
d. $ sudo rcstool ci /usr/TKLC/camiant/mra/bin/run_mra.sh
e. $ sudo rcstool ci /usr/TKLC/camiant/tomcat/bin/run_tomcat.sh
```

5. If the above command's output contains the string "mpe" or "mpe-li", run the following steps:

```
a. $ sudo rcstool co /usr/TKLC/camiant/tomcat/bin/run_tomcat.sh
b. $ sudo rcstool co /usr/TKLC/camiant/rc/bin/run_policyserver.sh
c. $ sudo sed -i -s 's/^UseJEPFilter=.*/UseJEPFilter=true;/'
/usr/TKLC/camiant/rc/bin/run_policyserver.sh
/usr/TKLC/camiant/tomcat/bin/run_tomcat.sh
d. $ sudo rcstool ci /usr/TKLC/camiant/rc/bin/run_policyserver.sh
e. $ sudo rcstool ci /usr/TKLC/camiant/tomcat/bin/run_tomcat.sh
```

6. Run the following command:

```
$ sudo service qp_procmgr restart
```

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 below procedures.

- Configure Cisco 3020 switch (netConfig), and/or

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

1. Log into PMAC server as admusr and switch to root user 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>
```

Note: If the Could not lock device displays, type this command to clear the lock to proceed:

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

3. Reply **y** if prompted.

3.5.2 Configure Community Strings

4. 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
```

5. 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 Audit Logs let the user to track and view configuration changes in the CMP system. Using the audit log, you can track and monitor each configuration event, affording you better system control. The audit log is stored in the database, so it is backed up and can be restored. The log files trace the activity of a Policy Management device. You can view and configure the logs for an individual cluster.

For more details see the section **View the Audit Logs** in *Configuration Management Platform Cable User's Guide*.

The "Manager Report" provides cluster's information like cluster status, topology status, utilization etc. For more details see the section "Manager Report" under "System Administration" chapter in *Configuration Management Platform Cable User's Guide*.

The Trace Log is part of system administration records notifications for management activity on the CMP system. You can configure the severity level of messages written to the Trace Log. For more information see the section “Trace Log” under “System Administration” chapter in *Configuration Management Platform Cable User’s Guide*.

There are Trace Log, Policy Syslog, SMS log and SMTP log, specific to each MPE in the PCRF system, which can be helpful. For more details on these MPE specific logs and configuration settings, see the section “Policy Server Logs” under the chapter “Managing Multimedia Policy Engine Devices” in *Configuration Management Platform Cable User’s Guide*.

Application Alarms and Events are unsolicited messages used in the system for trouble notification and to communicate the status of the system to Operations Services (OS). Alarms enable a network manager to detect faults 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

More details are in the section “Viewing Active Alarms” under “System-wide Reports” chapter in *Configuration Management Platform Cable User’s Guide*.

OS-level logging is captured in

- **/var/camiant/log/tomcat.log** – CMP server
- **/var/camiant /log/rc.log** – MPE server
- **/var/camiant /log/mra.log** – MRA server

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 Policy Management supports IPsec with an SCTP/IPv6 configuration.

3.7.1.1 Encapsulate Security Payload

Oracle Communications Policy Management 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. 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

Description	Valid Values	Default
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

Execute the below procedure to add an IPsec connection:

1. Login as **admusr** on the server using below command:
   ```
   login: admusr
   Password: <current admin user password>
   ```
2. Open the **platcfg** menu by entering this command:
   ```
   $ sudo su - platcfg
   ```
3. Select **Network Configuration, IPsec Configuration,** and **IPsec Connections** and Click **Edit**.
4. Select **Add Connection**.
5. Select the Internet Key Exchange Version: either **IKEv1** or **IKEv2**.
6. Complete the **IKE Configuration** fields for the desired connection, then click **OK**.

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

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

3.7.7 Edit an IPsec Connection

Execute the below procedure to edit an IPsec connection:

1. Login as **admusr** on the server using below command:
   ```
   login: admusr
   Password: <current admin user password>
   ```
2. Open the **platcfg** menu by entering this command:
   ```
   $ sudo su - platcfg
   ```
3. Select **Network Configuration, IPsec Configuration,** and **IPsec Connections** and Click **Edit**.
4. Select **Edit Connection**.
5. Select **IPsec connection** to edit.
6. View the IPsec connection's current configuration.
7. Click **Edit**.
8. Select either **IKEv1** or **IKEv2**.
9. Complete the **IKE Configuration** fields fields if needed, then click **OK**.
   The fields are described in Table 3. IPsec IKE and ESP Elements.
10. Select the desired **ESP Configuration** fields, and click **OK**.
    The fields are described Table 3. IPsec IKE and ESP Elements.
11. Complete the **Add Connection** fields for the desired connection by entering the **Local Address**, **Remote Address**, and **Pass Phrase** fields.
12. Select the **Mode**.
13. Click **OK**.
14. Select **Yes** to restart the connection. When the connection has been successfully added, the Internet Key Exchange Version menu displays.
15. Select **Exit** in each of the menus until a command prompt is reached.

3.7.8 Enable and Disable an IPsec Connection

Execute the below procedure to enable or disable an IPsec connection:

1. Login as **admusr** on the server using below command:
   ```
   login: admusr
   Password: <current admin user password>
   ```
2. Open the **platcfg** menu by entering this command:
   ```
   $ sudo su - platcfg
   ```

3. Select **Network Configuration, IPsec Configuration,** and **IPsec Connections** and Click **Edit**.
4. Select **Edit Connection**.
5. Select **IPsec connection** to edit.
6. View the IPsec connection's current configuration.
7. Click **Edit**.
8. Select **Connection Control**.
9. Select **IPsec connection** to enable or disable.
10. Select **Enable** or **Disable**.
11. Click **OK** to enable or disable the selected IPsec connection.
12. Select **Exit** in each of the menus until a command prompt is reached.

3.7.9 Delete an IPsec Connection

Execute the below procedure to delete an IPsec connection:

1. Login as **admusr** on the server using below command:
   ```
   login: admusr
   Password: <current admin user password>
   ```
2. Open the **platcfg** menu by entering this command:
   ```
   $ sudo su - platcfg
   ```
3. Select **Network Configuration, IPsec Configuration,** and **IPsec Connections** and Click **Edit**.
4. Select **Delete Connection**.
5. Select IPsec connection to delete.
6. Click **Yes** to confirm the delete.
7. Wait for the connection to be deleted. When the IPsec connection has been successfully deleted, the Connection Action menu displays.
8. 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 Policy Management and its components.

- Change default passwords
- Verify RADIUS for authentication purposes if configured
- Verify Firewall Configuration for network
- Verify TLS Configuration
- Configure community strings and traps explained in section SNMP Configuration
- Utilize LDAP for authentication purposes
- Enforce strong password management
- Restrict admin functions to the required few administrator groups

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:

- 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**.
- For Hardware, Networking, and Solaris Operating System Support, select **3**.

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.

1. Access the Oracle Help Center site at http://docs.oracle.com.
2. Click **Industries** link. The **Industries Documentation** page displays.
3. Click the **Oracle Communications** link.

   The Communications Documentation page displays. Most products covered by these documentation sets display under the heading **Signaling & Policy**.
4. Click on your product and then the release number.

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