Oracle® Communications
User Data Repository

Security Guide

Release 10.2

E64061 Revision 1

August 2015
User Data Repository Release 10.2

Table of Contents

1 INTRODUCTION .................................................................................................................. 5
  1.1 Audience ...................................................................................................................... 5
  1.2 References .................................................................................................................. 5
  1.3 My Oracle Support ..................................................................................................... 5
  1.4 Glossary ....................................................................................................................... 6

2 USER DATA REPOSITORY SECURITY OVERVIEW ............................................................. 7
  2.1 Basic Security Considerations .................................................................................... 7
  2.2 Accessing the Oracle Communications User Data Repository system ...................... 7
  2.3 Overview of Oracle Communications User Data Repository Security ....................... 8

3 IMPLEMENTING OCUDR SECURITY ................................................................................... 9
  3.1 OCUDR Web GUI Standard Features ......................................................................... 9
    3.1.1 User Administration ............................................................................................... 9
      3.1.1.1 Establishing GUI Groups and Group Privileges ................................................. 9
      3.1.1.2 Creating GUI Users and Assigning to Groups ................................................ 11
    3.1.2 GUI User Authentication ...................................................................................... 11
      3.1.2.1 GUI Passwords ............................................................................................... 11
      3.1.2.2 Changing Passwords for All OCUDR Administrative Accounts ................. 12
      3.1.2.3 Setting up Password Complexity .................................................................... 12
      3.1.2.4 Setting up Password Aging Parameters ......................................................... 12
      3.1.2.5 Restrict Concurrent GUI Logins ..................................................................... 12
      3.1.2.6 External Authentication .................................................................................. 13
      3.1.2.7 LDAP Authentication for GUI Users ............................................................... 13
      3.1.2.8 System Single Sign-On for GUI Users ............................................................. 13
    3.1.3 GUI Login and Welcome Banner Customization ..................................................... 13
    3.1.4 SNMP Configuration .............................................................................................. 13
      3.1.4.1 Selecting Versions ......................................................................................... 14
      3.1.4.2 Community Names / Strings ......................................................................... 14
    3.1.5 Authorized IPs ........................................................................................................ 14
    3.1.6 Enabling IPsec ........................................................................................................ 15
    3.1.7 Certificate Management ........................................................................................ 15
    3.1.8 SFTP Administration ............................................................................................. 15
    3.1.9 Remote Import/Export ........................................................................................... 15
    3.1.10 Provisioning Security ........................................................................................... 15
  3.2 OCUDR OS Standard Features ...................................................................................... 16
    3.2.1 Configure Password Expiry for OS Users .............................................................. 16
    3.2.2 Configuring minimum time before OS password can be changed ......................... 16
    3.2.3 Configuring Password Length for OS Users ........................................................ 17
    3.2.4 Configuring Session Inactivity for OS users .......................................................... 17
    3.2.5 Locking OS user accounts after a specified number of failed login attempts ........ 17
  3.3 Other Optional Configurations ...................................................................................... 18
    3.3.1 Changing OS User Account Passwords ................................................................... 18
    3.3.2 Changing Login Display Message ......................................................................... 18
    3.3.3 Setting up rsyslog for External Logging ................................................................. 19
    3.3.4 Adding Sudo Users ............................................................................................... 19
    3.3.5 Reporting and Disabling Expired OS User Accounts ............................................ 19
  3.4 Ethernet Switch Considerations ...................................................................................... 20
3.4.1 Configuring SNMP in Switches .......................................................... 20
3.4.2 Configuring Community Strings ......................................................... 20
3.4.3 Configuring Traps ............................................................................... 20
3.5 Security Logs and Alarms ....................................................................... 21
3.6 Optional IPsec Configuration .................................................................. 21
  3.6.1 IPsec Overview .................................................................................. 21
    3.6.1.1 Encapsulating Security Payload ................................................. 22
    3.6.1.2 Internet Key Exchange .............................................................. 22
  3.6.2 IPsec Process ..................................................................................... 22
  3.6.3 Pre-requisite Steps for Setting Up IPsec ............................................ 23
  3.6.4 Setting Up IPsec ............................................................................... 23
  3.6.5 IPsec IKE and ESP Elements ............................................................... 24
  3.6.6 Adding an IPsec Connection .............................................................. 25
  3.6.7 Editing an IPsec Connection ............................................................... 25
  3.6.8 Enabling and Disabling an IPsec Connection ...................................... 26
  3.6.9 Deleting an IPsec connection ............................................................ 27

APPENDIX A.  SECURE DEPLOYMENT CHECKLIST ............................................. 28

APPENDIX B.  IMAGES OF OCUDR PHYSICAL ACCESS POINTS ........................ 29

List of Figures
Figure 1. OCUDR Login Page .................................................................. 7
Figure 2. OCUDR Home Page ................................................................. 8
Figure 3. Global Action and Administration Permissions ............................... 10
Figure 4. Front View of Blades with local Terminal Connection in C-Class Enclosure ................................................................. 29
Figure 5. Custom Terminal Key Board Connector Cable ............................... 29
Figure 6. Custom Terminal Key Board Connector Cable Inserted in Local Terminal Connection ............................... 30
Figure 7. USB Connection for keyboard connection to Rack Mount Server ................................................................. 30
Figure 8. Terminal Video Connection on Rack Mount Server .......................... 31

List of Tables
Table 1. Glossary ......................................................................................... 6
Table 2. Predefined User and Group ............................................................. 9
Table 3. IPsec IKE and ESP Elements ......................................................... 24
1 Introduction

This document provides guidelines and recommendations for configuring the Oracle Communications User Data Repository (OCUDR) to enhance the security of the system. The recommendations herein are optional and should be considered along with your organization’s approved security strategies. Additional configuration changes that are not included herein are not recommended and may hinder the product’s operation or Oracle’s capability to provide appropriate support.

1.1 Audience

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

1.2 References

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

[2] Alarms, KPIs and Measurements Reference
[5] REST Provisioning Interface Reference
[6] Import / Export File Interface Reference

1.3 My Oracle Support

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

Web portal (preferred option): My Oracle Support (MOS) at https://support.oracle.com/

Phone: +1.800.223.1711 (toll-free in the US),

Or retrieve your local hotline from Oracle Global Customer Support Center at http://www.oracle.com/support/contact.html

Make the following selections on the Support telephone menu:

Select 2 for New Service Request

Then select 3 for Hardware, Networking, and Solaris Operating System Support

Then: either

- select 1 for Technical Issues,
  When talking to the agent, please indicate that you are an existing Tekelec customer.

  Note: Oracle support personnel performing installations or upgrades on a customer site must obtain the customer Support Identification (SI) number prior to seeking assistance.

  OR

- select 2 for Non-Technical Issues, for example, for My Oracle Support (MOS) registration.
  When talking to the agent, mention that you are a Tekelec Customer new to MOS.
1.4 Glossary
This section lists terms and acronyms specific to this document.

Table 1. Glossary

<table>
<thead>
<tr>
<th>Acronym/Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLI</td>
<td>Command Line Interface</td>
</tr>
<tr>
<td>CSR</td>
<td>Customer Service Request</td>
</tr>
<tr>
<td>ESP</td>
<td>Encapsulating Security Payload</td>
</tr>
<tr>
<td>GUI</td>
<td>Graphical User Interface</td>
</tr>
<tr>
<td>IKE</td>
<td>Internet Key Exchange</td>
</tr>
<tr>
<td>IPsec</td>
<td>Internet Protocol security</td>
</tr>
<tr>
<td>IV</td>
<td>Initialization Vector</td>
</tr>
<tr>
<td>KPI</td>
<td>Key Performance Indicator</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>MP</td>
<td>Message Processor</td>
</tr>
<tr>
<td>NOAMP</td>
<td>Network Operation, Administration, Maintenance, and Provisioning</td>
</tr>
<tr>
<td>OAM</td>
<td>Operation, Administrations and Maintenance</td>
</tr>
<tr>
<td>OCUDR</td>
<td>Oracle Communications User Data Repository</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>REST</td>
<td>Representational State Transfer. A type of Northbound provisioning interface.</td>
</tr>
<tr>
<td>SFTP</td>
<td>Secure File Transfer Protocol</td>
</tr>
<tr>
<td>SOAM</td>
<td>System Operation, Administration, and Maintenance</td>
</tr>
<tr>
<td>SOAP</td>
<td>Simple Object Access Protocol</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>SSO</td>
<td>Single Sign On</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>UDR</td>
<td>User Data Repository</td>
</tr>
</tbody>
</table>
2 User Data Repository Security Overview

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

2.1 Basic Security Considerations

The following principles are fundamental to using any application securely:

- **Keep software up to date.** Consider upgrading to the latest maintenance release. Consult with your Oracle support team to plan for OCUDR software upgrades.
- **Limit privileges.** Users should be assigned to the proper user group and reviewed periodically to determine relevance to current work requirements.
- **Monitor system activity.** Establish who should access which system components, and how often, and monitor those components.
- **Configure software securely.** For example, use secure protocols such as TLS and strong passwords.
- **Learn about and use of the OCUDR security features.** See Chapter 3 “Implementing OCUDR Security” for more information.
- **Keep up to date on security information.** Oracle regularly issues Security Alerts for vulnerability fixes deemed too critical. It is advisable to install the applicable security patches as soon as possible. See the Security Alerts page at the following link.
  

2.2 Accessing the Oracle Communications User Data Repository system

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

1. **Web browser GUI** – The client access to the OCUDR GUI for remote administration requires a web browser supporting a TLS 1.1 enabled session to the OCUDR. This application supports the use of Microsoft® Internet Explorer 8.0, 9.0 or 10.0, and both cookies and java script must be enabled. When a user accesses the OCUDR system via the GUI interface, the following screen is presented. On the Log In screen, enter the Username and Password credentials, then click **Log In** to access the GUI.

   ![OCUDR Login Page](image-url)
When successfully logged in, the OCUDR home page appears as shown below. To log out, the user can click the upper-right corner link labelled Logout or select the bottom menu item.

Figure 2. OCUDR 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 cli ent using the default administrative login account. SSH login is supported on the distinct management interface. To log out, enter the command, “logout” and press the Enter key.

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

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

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

2.3 Overview of Oracle Communications User Data Repository Security

The OCUDR is developed with security in mind and is delivered with a standard configuration that includes Linux operating system security hardening best practices. These practices include the following security objectives:

- Attack Surface Reduction
- Attack Surface Hardening
- Vulnerability Mitigation
3 Implementing OCUDR Security

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

3.1 OCUDR Web GUI Standard Features

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

3.1.1 User Administration

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

Table 2. Predefined User and Group

<table>
<thead>
<tr>
<th>User</th>
<th>Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>guiadmin</td>
<td>admin</td>
<td>Full access (read/write privileges) to all functions including administration functions</td>
</tr>
</tbody>
</table>

The User Administration page enables the administrator to perform functions such as adding, modifying, enabling, or deleting user accounts. Each user that is allowed access to the user interface is assigned a unique Username. This username and associated password must be provided during login. After three consecutive, unsuccessful login attempts, a user account is disabled. The number of failed login attempts before an account is disabled is a value that is configured through Administrations> Options. The customer can set this value to 0-10, with a default of 3. If the customer sets the value to 0, the user account will never be disabled for unsuccessful login attempts.

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

For more details on user administration, see the Users Administration section in [1] Operation, Administration, and Maintenance User's Guide.

3.1.1.1 Establishing GUI Groups and Group Privileges

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

The permissions in this page are grouped into the below sections

- Global Action Permissions
- Administration Permissions
- Configuration Permissions
- Alarms & Events Permissions
- Security Log Permissions
- Status & Manage Permissions
- Measurements Permissions
- Communication Agent Configuration Permissions
- Communication Agent Maintenance Permissions
- Diameter Configuration Permissions
- Diameter Maintenance Permissions
- Diameter Diagnostics Permissions
- Diameter Mediation Permissions
- Diameter Troubleshooting with IDIH Permissions
- Diameter AVP Dictionary Permissions
- UDR Configuration Permissions
- UDR SEC Permissions
- UDR Maintenance Permissions


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

**Figure 3. Global Action and Administration Permissions**

<table>
<thead>
<tr>
<th>Resource</th>
<th>View</th>
<th>Insert</th>
<th>Edit</th>
<th>Delete</th>
<th>Manage</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Global Action Permissions</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Administration Permissions</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>General Options</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Users</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Groups</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sessions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certificate Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authorized IPs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SFTP Users</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software Versions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software Upgrade</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote LDAP Authentication</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote SNMP Trapping</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote Export Server</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
3.1.1.2 Creating GUI Users and Assigning to Groups

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

The Insert User page displays the following elements:

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

For more details on these elements, please refer the Administration chapter in the Operation, Administration, and Maintenance User’s Guide.

The user administration page lets users perform the below actions:

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

For details on how to perform these actions, please refer the Administration chapter in the Operation, Administration, and Maintenance User’s Guide.

3.1.2 GUI User Authentication

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

3.1.2.1 GUI Passwords

Password configuration, such as setting passwords, password history rules, and password expiration, occurs in Administration. The application provides two ways to set passwords: through the user interface from the Users Administration page, and at the OCUDR Login page. For more detailed steps on performing these two methods, please refer to the Administration chapter in the Operation, Administration, and Maintenance User’s Guide.
3.1.2.2 Changing Passwords for All OCUDR Administrative Accounts

The System Installation procedure will create the following default accounts:

- guiadmin – for OCUDR Application GUI
- root – for CLI
- admusr – for CLI

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

To change the default password of an account created for web GUI access, see the [1] Operation, Administration, and Maintenance User's Guide for “Passwords” in the “Administration” chapter.

For changing the OS account passwords of a CLI account, please see the section 3.3.1, Changing OS User Account Passwords.

3.1.2.3 Setting up Password Complexity

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

3.1.2.4 Setting up Password Aging Parameters

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

The user interface provides two forms of password expiration:

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

By default, password expiration occurs after 90 days.


3.1.2.5 Restrict Concurrent GUI Logins

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

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

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

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

3.1.2.7 LDAP Authentication for GUI Users

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

Below are the elements required to configure an LDAP server:

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


3.1.2.8 System Single Sign-On for GUI Users

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

3.1.3 GUI Login and Welcome Banner Customization

When logged in to the OCUDR GUI as an administrator user, the Options page under Administration enables the administrative user to view a list of global options.

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

3.1.4 SNMP Configuration

The application has an interface to retrieve KPIs and alarms from a remote location using the industry-standard Simple Network Management Protocol (SNMP) interface. Only the active Network OAM&P server allows SNMP administration. For more details, see the section SNMP Trapping in the [1]Operation, Administration, and Maintenance User's Guide under the Administration chapter.
The Active Network OAM&P server provides a single interface to SNMP data for the entire network and individual servers interface directly with SNMP managers. The application sends SNMP traps to SNMP Managers that are registered to receive traps. IP addresses and authorization information can be viewed and changed using the SNMP Trapping page.

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

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

The SNMP Trapping page provides the below functionalities:

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

For more details on these actions, please refer to the [1] Operation, Administration, and Maintenance User's Guide.

### 3.1.4.1 Selecting Versions

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

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

The recommended option is SNMPv3 for secure operation.

### 3.1.4.2 Community Names / Strings

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

### 3.1.5 Authorized IPs

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

Enabling Authorized IPs functionality prevents unauthorized IP addresses from accessing the GUI. See the [1] Operation, Administration, and Maintenance User’s Guide, Authorized IPs section for more details on how to enable this feature.
3.1.6 Enabling IPsec

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

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

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

Internet Key Exchange (IKE) is used to exchange secure keys to set up IPsec security associations. See Section 3.6 Optional IPsec Configuration for more details on how to enable IPsec.

3.1.7 Certificate Management

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

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


3.1.8 SFTP Administration

The OCUDR supports SFTP sessions with external servers for transfer of various files from the OCUDR. The authentication process requires a digital certificate for authenticating the sessions.

The transfer of files is driven from the external server. Please see section SFTP Users Administration in [1] Operation, Administration, and Maintenance User’s Guide.

3.1.9 Remote Import/Export

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

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

3.1.10 Provisioning Security

The OCUDR provisioning interface supports both SOAP and REST interfaces. Only IP addresses that are configured by the user in the Provisioning Connections Whitelist are allowed to connect to the primary provisioning site’s NOAMP server and execute commands. Please see Provisioning Connections in [4] Enhanced Subscriber Profile Repository User’s Guide for more information.
The customer also configures what type of provisioning interfaces are enabled – SOAP and/or REST. The customer can also configure whether the REST interface runs in secure mode (using TLS) or unsecure mode (plain text). The SOAP interface only runs in unsecure (plain text) mode. For more information regarding the configuration options, please see Provisioning Options in [4] Enhanced Subscriber Profile Repository User’s Guide.

The secure REST interface uses SSL certificates and public/private key pairs as described in [5] REST Provisioning Interface Reference.

For both REST and SOAP provisioning interfaces, the customer can configure their IP address to use Internet Protocol Security (IPsec) to provide secure connections. For more information regarding IPsec, please see section 3.6: Optional IPsec Configuration.

### 3.2 OCUDR OS Standard Features

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

#### 3.2.1 Configure Password Expiry for OS Users

Use the below procedure to configure password expiry:

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

2. Open the platcfg menu by entering the following command.
   
   `$ sudo su - - platcfg`

3. Select Security from the menu and hit Enter.

4. Fill out the following settings:
   
   **Maximum number of days a password may be used:** 99999

5. Select OK and hit Enter.

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

#### 3.2.2 Configuring minimum time before OS password can be changed

Procedure to configure minimum time before password can be changed:

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

2. Open the platcfg menu by entering the following command.
   
   `$ sudo su - - platcfg`

3. Select Security from the menu and hit Enter.

4. Fill out the following settings:
   
   **Minimum number of days allowed between password changes:** 0

5. Select OK and hit Enter.

6. Select Exit in each of the menus until a command prompt is reached.
3.2.3 Configuring Password Length for OS Users

Procedure to configure password length:

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

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

   $ sudo su - platcfg

3. Select Security from the menu and hit Enter.

4. From the menu select Sec Password Restrictions option

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

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

3.2.4 Configuring Session Inactivity for OS users

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

1. Log in as <admin user> on the server

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

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

   $ sudo su - platcfg

3. Select Security from the menu and hit Enter.

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

5. Select OK and hit Enter.

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

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

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

1. Log in as admin user on the server

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

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

   $ sudo su - platcfg

3. Select Security from the menu and hit Enter.

4. Select User Account Locking from the menu and hit Enter

5. Fill out the following settings:

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

6. Select OK and hit Enter.
7. Select Exit in each of the menus until a command prompt is reached.

3.3 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.

3.3.1 Changing OS User Account Passwords

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

Procedure to Change Default Passwords

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

2. Change the passwords for each of the accounts being changed:
   
   ```
   $ sudo passwd <user account>
   Changing password for user <user account>.
   New UNIX password: <new password - will not display>
   Retype new UNIX password: <new password - will not display>
   ```

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

3.3.2 Changing Login Display Message

1. Use this procedure to change the Login Display Message. Log in as <admin user> on the source server.
   
   ```
   login: <admin user>
   Password: <current admin user password>
   ```

2. Create a backup copy of sshd_config
   
   ```
   $ sudo cd /etc/ssh
   $ sudo cp sshd_config sshd_config.bak
   ```

3. Edit the sshd configuration file.
   
   ```
   $ sudo rcstool co sshd_config
   $ sudo vi sshd_config
   ```

   Uncomment and edit the following line:
   
   ```
   $ Banner /some/path
   ```

   To this:
   
   ```
   Banner /etc/ssh/sshd-banner
   ```

   Save and exit the vi session.

4. Edit the banner file.
   
   ```
   $ sudo vi sshd-banner
   ```

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

5. Restart the sshd service.
   
   ```
   $ sudo service sshd restart
   ```
User Data Repository Release 10.2

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

   $ sudo ssh <current server name>

   Verify message line feeds are formatted correctly.

   $ exit

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

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

3.3.3 Setting Up rsyslog for External Logging

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

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

2. Enable remote logging:

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

3. Repeat on all necessary NOAMs and SOAMs

Note: The following restrictions exist:

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

3.3.4 Adding Sudo Users

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

3.3.5 Reporting and Disabling Expired OS User Accounts

Procedure to Report and Disable Expired User Accounts

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

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

2. Run the report of expired users.

   $ sudo lastlog -b <N>

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

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

3. Disable the user accounts identified by the lastlog report

   $ sudo passwd -l <user acct>
Repeat this step for each user account you want to disable.

4. To re-enable an account:
   
   ```
   $ sudo passwd -u <user acct>
   ```

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

### 3.4 Ethernet Switch Considerations

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

#### 3.4.1 Configuring SNMP in Switches

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

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

1. Log in to the server as root user and list all the configured switches using the below command.
   
   ```
   # netConfig --repo listDevices
   ```

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

3. For any given switch by switch name, display SNMP community information using the below command:
   
   ```
   # netConfig getSNMP --device=<switch_name>
   ```

4. For any given switch by switch name, display its SNMP trap information using the below command
   
   ```
   # netConfig listSNMPNotify --device=<switch_name>
   ```

   **Note:** If the reply indicates “Could not lock device”, enter the following command to clear the lock in order to proceed:
   
   ```
   # netConfig --wipe --device=<switch_name>
   ```

   (reply “y” if prompted)

#### 3.4.2 Configuring Community Strings

1. To ADD a community string to ANY switch by switch name, use below command with appropriate switch name
   
   ```
   #netConfig addsSNMP --device=<switch_name> community=<community string> uauth=RO
   ```

2. To DELETE a community string to ANY switch by switch name, use appropriate switch name in the below command
   
   ```
   #netConfig deleteSNMP --device=<switch_name> community=<community_string>
   ```

#### 3.4.3 Configuring Traps

1. To ADD a trap server, use below command with appropriate switch name:
   
   ```
   #netConfig addSNMPNotify --device=<switch_name> host=<snmp_server_ip> version=2c auth=<community_string> [traplvl=not-info]
   ```

2. To DELETE a trap server, use the below command with appropriate switch name:
#netConfig deleteSNMPNotify --device=<switch_name> host=<snmp_server_ip> version=2c auth=<community_string> [traplvl=not-info ]

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

### 3.5 Security Logs and Alarms

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

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

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

- Critical
- Major
- Minor
- Cleared


OS-level logging is captured in

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

### 3.6 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.

#### 3.6.1 IPsec Overview

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

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

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

Note:  OCUDR supports IPsec with an SCTP/IPv6 configuration.
3.6.1.1 Encapsulating Security Payload

OCUDR 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.

3.6.1.2 Internet Key Exchange

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

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

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

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

3.6.2 IPsec Process

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

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

IKE operates in two phases.

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

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

IPsec uses Security Associations to determine which type of encryption algorithm and authentication transportation should be used when creating an IPsec packet, and to apply the correct decryption algorithm when a packet is received. Because security associations change with time, a lifetime parameter is used to force the security associations to expire so that IPsec must renegotiate them.
An IPsec connection can be set up on a virtual IP, which can be used for HA. However, when a switchover occurs and the VIP is added on the new box a SIGHUP is sent to the iked daemon on the newly active box, so that the VIP is under iked management. Also, the switchover will not occur until the security associations have expired and the renegotiation can begin.

### 3.6.3 Pre-requisite Steps for Setting Up IPsec

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

1. Log in as root on the active NOAMP server
2. On the active NOAMP server using the below commands
   ```
   iadd -xu -fallowPgmChg -fname -fvalue LongParam \
   <<'!!!'
   Yes|cm.ha.enableIpsecWhack|1
   !!!
   ```

### 3.6.4 Setting Up IPsec

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

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

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

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

1. Open platcfg
2. Add and configure an IPsec connection. See section 3.6.6: Adding an IPsec Connection
3. Select an IKE version.
   a. Complete the IKE configuration for the IPsec connection.
   b. Complete the ESP configuration for the IPsec connection.
   c. Complete the IPsec connection configuration entries.
   d. Wait for the connection to be added.
4. Enable the IPsec connection. See section 3.6.8: Enabling and Disabling an IPsec Connection.
5. Log out of platcfg
6. Restart IPsec service by using the below command.
   ```
   # service ipsec restart
   ```
### 3.6.5 IPsec IKE and ESP Elements

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

<table>
<thead>
<tr>
<th>Description</th>
<th>Valid Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Key Exchange Version</td>
<td>ikev1, ikev2</td>
<td>ikev2</td>
</tr>
<tr>
<td>IKE Configuration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IKE Encryption</td>
<td>aes128_cbc, aes192_cbc, aes256_cbc, 3des_cbc, hmac_md5</td>
<td>aes128_cbc, hmac_md5</td>
</tr>
<tr>
<td>IKE Authentication</td>
<td>hmac_sha1, aes_xcbc, hmac_md5</td>
<td>hmac_md5</td>
</tr>
<tr>
<td>Pseudo Random Function.</td>
<td>hmac_sha1, aes_xcbc (ikev2)</td>
<td>-</td>
</tr>
<tr>
<td>Diffie-Hellman Group</td>
<td>2, 14 (ikev2)</td>
<td>2 (IKEv1), 14 (IKEv2)</td>
</tr>
<tr>
<td>IKE SA Lifetime</td>
<td>Number of time units</td>
<td>60</td>
</tr>
<tr>
<td>Lifetime Units</td>
<td>hours, mins, secs</td>
<td>mins</td>
</tr>
<tr>
<td>Perfect Forward Secrecy</td>
<td>yes, no</td>
<td>yes</td>
</tr>
<tr>
<td>ESP Configuration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ESP Authentication</td>
<td>hmac_sha1, hmac_md5</td>
<td>hmac_sha1</td>
</tr>
<tr>
<td>ESP Configuration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encryption Algorithm</td>
<td>aes128_cbc, aes192_cbc, aes256_cbc, 3des_cbc</td>
<td>aes128_cbc</td>
</tr>
</tbody>
</table>
3.6.6 Adding an IPsec Connection

Procedure to add an IPsec connection:

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

2. Open the platcfg menu by entering the following command.
   
   $ sudo su - platcfg

3. Select Network Configuration.
4. Select IPsec Configuration.
5. Select IPsec Connections.
7. Select Add Connection.
8. Select the Internet Key Exchange Version: either IKEv1 or IKEv2.
9. Complete the IKE Configuration fields for the desired connection, then click OK.
   
   The fields are described in Table 3. IPsec IKE and ESP Elements.

10. Select the desired ESP Encryption algorithm, then click OK.
    
    The fields are described Table 3. IPsec IKE and ESP Elements.

11. Complete the Add Connection fields for the desired connection.
    a. Enter the Local Address.
    b. Enter the Remote Address.
    c. Enter the Pass Phrase.
    d. Select the Mode.
12. Click OK.
   
   Wait for the connection to be added.

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

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

3.6.7 Editing an IPsec Connection

Procedure to edit an IPsec connection:

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

2. Open the platcfg menu by entering the following command.
   
   $ sudo su - platcfg
3. Select Network Configuration.
4. Select IPsec Configuration.
5. Select **IPsec Connections**.
6. Select **Edit**.
7. Select **Edit Connection**.
8. Select **IPsec connection** to edit.
9. View the IPsec connection’s current configuration.
10. Select **Edit**.
11. Select either **IKEv1** or **IKEv2**.
12. Complete the **IKE Configuration** fields if needed, then click **OK**.
   
   The fields are described in Table 3. IPsec IKE and ESP Elements.
13. Select the desired **ESP Configuration** fields, then click **OK**.
   
   The fields are described in Table 3. IPsec IKE and ESP Elements.
14. Complete the Add Connection fields for the desired connection.
   a. Enter the **Local Address**.
   b. Enter the **Remote Address**.
   c. Enter the **Pass Phrase**.
   d. Select the **Mode**.
15. Click **OK**.
16. Select **Yes** to restart the connection.
   
   When the connection has been successfully updated, the **Internet Key Exchange Version** Menu appears.
17. Select **Exit** in each of the menus until a command prompt is reached.

### 3.6.8 Enabling and Disabling an IPsec Connection

Procedure to enable or disable an IPsec connection:

1. Log in as `<admin user>` on the server
   
   **Login:** `<admin user>`
   **Password:** `<current admin user password>`
2. Open the platcfg menu by entering the following command.
   
   `$ sudo su - platcfg`
3. Select **Network Configuration**.
4. Select **IPsec Configuration**.
5. Select **IPsec Connections**.
6. Select **Edit**.
7. Select **Connection Control**.
8. Select **IPsec connection** to enable or disable.
9. Select **Enable** or **Disable**.
10. Click **OK** to enable or disable the selected IPsec connection.
11. Select **Exit** in each of the menus until a command prompt is reached.
3.6.9 Deleting an IPsec connection

Procedure to delete an IPsec connection:

1. Log in as <admin user> on the server

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

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

   $ sudo su - platcfg

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

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

11. Select Exit in each of the menus until a command prompt is reached.
Appendix A. Secure Deployment Checklist

The following security checklist lists guidelines to help you secure Oracle OCUDR and its components.

- Change default passwords
- Utilize LDAP for authentication purposes
- Use TLS or IPSEC
- Enforce strong password management
- Restrict admin functions to the required few administrator groups
- Configure community strings and traps explained in section 3.3 Other Optional Configurations
- Change provisioning options to only enable secure REST provisioning in section 3.1.10 Provisioning Security
Appendix B. Images of OCUDR Physical Access Points

Figure 4 shows the local terminal connection in the upper left for each blade used by a unique combination connector shown in Figure 5.

**Figure 4. Front View of Blades with local Terminal Connection in C-Class Enclosure**

Figure 5 shows the custom terminal key board connector cable, which inserts into the local terminal of a blade and has a connector attachment each for a xx connection, a video terminal,, and a double USB port

**Figure 5. Custom Terminal Key Board Connector Cable**
Figure 6 shows the custom terminal keyboard connector cable inserted in the local terminal connection on the front of a blade.

**Figure 6. Custom Terminal Key Board Connector Cable Inserted in Local Terminal Connection**

Figure 7 shows the USB connections for the double USB connector on the custom terminal key board connector cable.

**Figure 7. USB Connection for keyboard connection to Rack Mount Server**
User Data Repository Release 10.2

Figure 8 shows the video connection of a rackmount server for the video connector of the custom terminal keyboard connector cable.

Figure 8. Terminal Video Connection on Rack Mount Server