Oracle® Communications
Policy Management Release 12.0

Release Notes

E61812 Revision 03

April 2015

ORACLE®

Oracle® Communications Policy Management Release 12.0 Release Notes

Table of Contents

List of Tables

Chapter

1

Introduction

This Release Notice identifies the functions and features of Oracle Communications Policy Management (OCPM) Release 12.0

This Release Notice includes Feature Descriptions, supported Hardware Baseline, Media and Documentation pack contents and identifies the Supported Upgrade Paths. This document also includes listings of both the Resolved and Known Bugs for this Release. Directions for accessing key Oracle sites and Services are also identified in the *Oracle References and Services* chapter.

Release Notices are included in the Documentation Pack made available with every Software Release.

Chapter

2

Feature Descriptions

- *Adding DB Behindness Information (BugID# 19109549)*
- *Allow for Configuration of Bulk Server WAN Replication (BugID# 19096708)*
- *Configuration Templates (BugID# 19102948)*
- *Diameter Timer Enhancements (BugID# 19104121)*
- *Flow-Description AVP Update (BugID# 19112181)*
- *Full IPv6 Support (BugID# 19114843)*
- *Global Time Limit on Diameter Request Processing (BugID# 19108365)*
- *Gx Synch After Message Loss (BugID# 19104124)*
- *Gx Synch After Session Loss (BugID# 19108450)*
- *Increase Replication Performance (BugID# 19110444)*
- *IPv6 Lawful Intercept Support (SS8, Cisco) (BugID# 19117228)*
- *MRA Binding Management Enhancement (BugID# 19105376)*
- *MRA Response to "Down" MPE May Cause Loss of Binding During Network Fail (BugID# 19102225)*
- *Multi-Level OAM Support (BugID# 19094410)*
- *Policy Conditions for Supporting Codec-Data (BugID# 19107434)*
- *PCRF Initiated Session Release in CCA (BugID# 19110367)*
- *Provide CMP Warning Message During MRA Manual Failover (BugID# 19108213)*
- *Second Level Authentication (BugID# 19104113)*
- *Session Correlation Variables for Gx Sessions (BugID# 20077660)*
- *Show LI Connection Status in CMP (BugID# 19108154)*
- *Support for 3GPP Gx Pending Transaction Error Code (BugID# 19108290)*

- *Support of Local Subscriber and Session State Variables (BugID# 19102894)*
- *Support for Multiple TCP Connections or SCTP Streams (BugID# 19106096)*
- *Sy Updates for Policy R12 (BugID# 19104126)*
- *Unique Rule Names Per Site (BugID# 19108468)*
- *User Profile Lookup on Session Updates (BugID# 19108448)*
- *Upgrade Framework Improvement - LVM Support (BugID# 19109449)*
- *Upgrade Framework Improvement - Patch Support (BugID# 19109446)*

Adding DB Behindness Information (BugID# 19109549)

This enhancement allows the PCRF management system to display information about the whether the databases on backup servers are up to date.

Allow for Configuration of Bulk Server WAN Replication (BugID# 19096708)

This enhancement allows multiple bulk transfers to occur concurrently over the WAN. When connectivity to a remote site is regained, the current system requires that bulk transfers occur serially. This enhancement allows these transfers to occur in parallel.

Configuration Templates (BugID# 19102948)

This feature allows the administrator to configure and save specific configuration templates in the CMP by unique names so that they can be associated to individual or multiple policy servers that require the same configuration of specific parameters. Each configuration template on each policy server may have a different order that determines the priority level and to determine the order in which the configuration parameters defined in the configuration templates are applied.

Diameter Timer Enhancements (BugID# 19104121)

This feature supports new AF 2AS server over Rx interface.

Flow-Description AVP Update (BugID# 19112181)

Modified support for this AVP per 3GPP Release 9

Full IPv6 Support (BugID# 19114843)

This feature allows IPv6 addressing to be used on all logical interfaces including management (OAM) and replication (REP).

Global Time Limit on Diameter Request Processing (BugID# 19108365)

In a LTE network, UE starts a timer (8 seconds, max 5 attempts - defined in 3GPP) after sending PDN connectivity request to eNB. This timer value determines the timer budget for all the subsequent message exchanges between various network elements (such as the PCRF) participating in setting up the PDN connection.

Gx Synch After Message Loss (BugID# 19104124)

This feature provides enhancements in the Gx interface to allow the PCRF and PGW to sync-up after a session is lost (e.g. Gx:RAA is dropped due to overload control). This is not currently part of 3GPP 29.212. This functionality works with a specific PGW.

Gx Synch After Session Loss (BugID# 19108450)

This enhancement in the Gx interface between PCRF and PGW allows for message sync-up in the event of RAR or RAA message session loss in PCRF.

Increase Replication Performance (BugID# 19110444)

This enhancement improves COMCOL replication performance.

IPv6 Lawful Intercept Support (SS8, Cisco) (BugID# 19117228)

This enhancement allows using IPv6 for Lawful Intercept, in conjunction with specific third party equipment.

MRA Binding Management Enhancement (BugID# 19105376)

This enhancement ensures that the MRA will not delete binding information associated with an unreachable MPE on a Gx/Gxx session establishment. Initial dependent requests (which reference the original Gx session) can still be routed to the handling MPE, while new Gx sessions for the subscriber can be assigned to another MPE to prevent denial of service due to MPE server failure.

MRA Response to "Down" MPE May Cause Loss of Binding During Network Fail (BugID# 19102225)

If a new subscriber session is bound to an MPE that has been down for more than 30 seconds, the MRA will delete the binding and assign the new subscriber session to a new MPE. This prevents a subscriber bound to a failed MPE from being denied service. In a geo-diverse system where the MRA and MPE are co-located and connected via LAN, there is no problem. However, in a geo-redundant system where the MRA and the spare MPE are remote and connected via WAN the MRA could delete the binding for an active session if the WAN is down for more than 30 seconds.

Multi-Level OAM Support (BugID# 19094410)

This feature is used to create policies and download them to the various MPE's and also is used for configuration of the MPE and MRA. The CMP provides a consolidated view of system alarms and logs and has and OSSI/ XML API to interface to external systems.

Policy Conditions for Supporting Codec-Data (BugID# 19107434)

This feature allows the customer to create policies based on information provided in the Codec-Data AVP provided over Rx AAR.

PCRF Initiated Session Release in CCA (BugID# 19110367)

Supporting 'Session-Release-Cause' AVP in CCA-U message will save one RAR transaction for PCRF initiated session termination.

Provide CMP Warning Message During MRA Manual Failover (BugID# 19108213)

This enhancement provides a pop-up warning window asking the operator whether to proceed with the request to reverse site preferences.

Second Level Authentication (BugID# 19104113)

Allows creating policies which redirect devices attached to an Enterprise PDN to be redirected to an external system for authentication.

Session Correlation Variables for Gx Sessions (BugID# 20077660)

This enhancement implements limited cross-APN session correlation using variables. Session correlation is when the PCRF unifies the information for a single subscriber across multiple distinct sessions.

Show LI Connection Status in CMP (BugID# 19108154)

This feature allows any CMP user with the operator role to view information about the status of the X1 and X2 interfaces, which are used to communicate with the external Lawful Intercept Mediation Function (MF). The X1 interface sends target information (e.g., IMSI) to the PCRF, while X2 provides call data information to the Mediation Function (MF).

Support for 3GPP Gx Pending Transaction Error Code (BugID# 19108290)

Implementing 3GPP defined procedures for 'pending transaction' will enable the customer to comply with 3GPP specification.

Support of Local Subscriber and Session State Variables (BugID# 19102894)

The Support of Local Subscriber and Session State Policy Variables feature will allow policy subscriber and session state variables to be stored locally on the PCRF. This feature can be used to support subscriber and session state variable uses cases including the use case in the previous section. This could be done busing a subscriber session state variable "TrafficProfileName" and the specific traffic profile name/value could be stored locally on the PCRF and then referenced by polices in the PCRF when creating Charging Rule Updates.

Support for Multiple TCP Connections or SCTP Streams (BugID# 19106096)

This feature will allow the MRA and MPE to initiate multiple Diameter TCP connections to a peer. The MPE and MRA already support initiating an SCTP association with multiple streams. However, the number of streams that may be used is not configurable.

This feature will allow the operator to configure the number of TCP connections or SCTP streams between peers.

Sy Updates for Policy R12 (BugID# 19104126)

Implementing 3GPP defined AVPs for 'pending policy counters' will enable the customer to comply with 3GPP specification.

Unique Rule Names Per Site (BugID# 19108468)

Avoids having both active MPEs send rules with the same name to a PCEF during dual active (split brain) operation.

User Profile Lookup on Session Updates (BugID# 19108448)

The purpose of this feature is to allow the PCRF to query the SPR on Gx, Gxx, and S9 session updates if the subscriber information is not currently available in the PRCF for use for policy evaluation or execution.

Upgrade Framework Improvement - LVM Support (BugID# 19109449)

This feature supports migration from the ext3 file system to the ext4 file system in R12.0.

Upgrade Framework Improvement - Patch Support (BugID# 19109446)

This enhancements provides changes in the software upgrade process to support different procedures based on the amount of software that is changing.

Chapter

3

Policy Management Release 12.0 Media and Documentation

Topics:

Oracle Communications software is available for electronic download on the Oracle Software Delivery Cloud (OSDC). Documentation is delivered electronically on the Oracle Technology Network (OTN). Both the software Media Pack and the Documentation Pack are listed in this chapter.

Media Pack

All components available for download from the Oracle Software Delivery Cloud
(*https://edelivery.oracle.com/*) are in *Table 1: Media Pack Contents*.

Note: This list is accurate at the time of release, but is subject to change. Please view the Oracle Software
Delivery Cloud site for the latest information.

Table 1: Media Pack Contents

Name
Oracle Communications Policy Configuration Management Platform 12.0.0_45.1.0
Oracle Communications Policy Front End 12.0.0_45.1.0
Oracle Communications Policy Multimedia Policy Engine 12.0.0_45.1.0
Oracle Communications Tekelec Platform Distribution 7.0.0.0.0-86.14.0
Oracle Communications Tekelec Virtual Operating Environment 3.0.0.0_86.14.0
Oracle Communications Tekelec Platform Management and Configuration 6.0.0.0_60.14.0
Oracle Communications Tekelec Platform Distribution 7.0.0.0.0-86.14

Documentation Pack

All documents available for download from the Oracle Technology Network (OTN) site
(*http://docs.oracle.com*) are listed in *Table 2: Documentation Pack Contents*.

Note: This list is accurate at the time of release, but is subject to change. Please view the OTN site for
the latest information.

Table 2: Documentation Pack Contents

Name
Related Publications Reference
Hardware Documentation Roadmap Reference
Platform Configuration User's Guide
Configuration Management Platform Wireless User's Guide
Policy Wizard Reference
SNMP User's Guide
OSSI XML Interface Definitions Reference
Policy Front End User's Guide
Troubleshooting Reference

Name
Analytics Data Stream Reference

Chapter

4

Supported Hardware Baseline

Topics:

The Hardware identified in *Table 3: Supported Hardware Baseline* comprises the hardware and server versions that have been verified with this Release.

Supported Hardware Baseline

Table 3: Supported Hardware Baseline

Hardware	Description
Wireless HP Gen8 C-Class Blades	C-Class Blade Servers configured as defined in configuration workbook

Chapter

5

Policy Management Release 12.0 Supported Upgrade Paths

Topics:

* *Supported Upgrade Paths.....19*

This release has been tested for upgrades from specific prior releases; this chapter contains the exact paths for upgrade. Please verify that your current installed release is listed on a valid upgrade path.

Supported Upgrade Paths

The possible upgrade paths to Policy Management Release 12.0 are listed below.

Table 4: Policy Management Release 12.0 Upgrade Paths

From	To
11.1.X	12.0.0

Policy Management Release 12.0 Resolved and Known Bugs

Topics:

This chapter lists the Resolved and Known Bugs for Policy Management Release 12.0

These bug lists are distributed to customers with a new software release at the time of General Availability (GA), and are updated for each Maintenance release.

Severity Definitions

The problem report sections in this document refer to Bug severity levels. Definitions of these levels can be found in the publication, *TL 9000 Quality Management System Measurement Handbook*.

Problem Report: A report from a customer or on behalf of the customer concerning a product or process defect requesting an investigation of the issue and a resolution to remove the cause. The report may be issued via any medium. Problem reports are systemic deficiencies with hardware, software, documentation, delivery, billing, invoicing, servicing or any other process involved with the acquisition, operation, or performance of a product. An incident reported simply to request help to bring back the service or functionality to normal without the intent to investigate and provide a resolution to the cause of the incident is not a problem report.

- Critical: Conditions that severely affect the primary functionality of the product and because of the business impact to the customer requires non-stop immediate corrective action, regardless of time of day or day of the week as viewed by a customer on discussion with the organization such as

    1. product inoperability (total or partial outage),
    2. a reduction in the capacity capability, that is, traffic/data handling capability, such that expected loads cannot be handled,
    3. any loss of emergency capability (for example, emergency 911 calls), or
    4. safety hazard or risk of security breach.

- Major: Product is usable, but a condition exists that seriously degrades the product operation, maintenance or administration, etc., and requires attention during pre-defined standard hours to resolve the situation. The urgency is less than in critical situations because of a lesser immediate or impending effect on product performance, customers and the customer's operation and revenue such as

    1. reduction in product's capacity (but still able to handle the expected load),
    2. any loss of administrative or maintenance visibility of the product and/or diagnostic capability,
    3. repeated degradation of an essential component or function, or
    4. degradation of the product's ability to provide any required notification of malfunction.

- Minor: Other problems of a lesser severity than 'critical' or 'major' such as conditions that have little or no impairment on the function of the system

The numbered severity levels in the tables below correspond to these definitions:

- 1 - Critical
- 2 - Major
- 3 - Minor

Resolved Bug Listing

Table 5: Policy Management Release 12.0 Resolved Bugs lists bugs that are resolved in the following builds:

Application Lineup

- Oracle Communications Policy Configuration Management Platform 12.0.0_45.1.0

Platform Lineup

- Oracle Communications Policy Front End 12.0.0_45.1.0
- Oracle Communications Policy Multimedia Policy Engine 12.0.0_45.1.0
- Oracle Communications Tekelec Platform Distribution 7.0.0.0.0-86.14.0
- Oracle Communications Tekelec Virtual Operating Environment 3.0.0.0_86.14.0
- Oracle Communications Tekelec Platform Management and Configuration 6.0.0.0_60.14.0
- Oracle Communications Tekelec Platform Distribution 7.0.0.0.0-86.14

Above listed load line-up provides a view of our GA milestone release.

Note: Resolved bugs are sorted in ascending order by Severity (Sev), and then by Bug number.

Table 5: Policy Management Release 12.0 Resolved Bugs

Bug number	SR	Severity	Title
19116142	-	3-Minor	[232575]Flow-Description AVP doesn't comply with 3GPP Release 9
19118365	-	3-Minor	[240712]Isolate policy/policy group warning exists even though the policy is imp
19531512	-	3-Minor	Termination-cause AVP is missing in the S9:CCR-T
19548582	-	3-Minor	[Timer Enhancement]timer profile for Rx-over-S9 messages isn't implemented yet
19563917	-	3-Minor	[S9] H-MPE responds to S9 CCR-T with CCA-T "DIAMETER_UNABLE_TO_COMPLY"
19571633	-	3-Minor	RP Acceptable Default EPS Bearer QosClassIdentifier=9 is not pushed down to MPE
19589974	-	3-Minor	V-MPE doesn't create S9 subsession for 2nd CCR-i for subscriber
19605867	-	3-Minor	LI Status message not sent to Trace Log
19619726	-	2-Major	[PLAT]Bond configuration missing primary device and primary_reselect settings
19623182	-	3-Minor	S9: Local Rx session is created when Rx:AAR fails with IP-CAN_SESSION_NOT_AVAIL
19631744	-	3-Minor	S9 over Rx session is not removed when VPLMN receives UNKNOWN_SESSION from PGW
19646195	-	3-Minor	Connectivity Degraded/Lost Alarms Should AutoClear
19667837	-	3-Minor	Response delay should support SDR message in Diamcli Tool
19683764	-	3-Minor	[MRA Associate] There is an exception while clicking MRA association.
19683887	-	3-Minor	[S9]Content of Description for roaming profile can't be imported successfully
19690042	-	3-Minor	[S9] S9:CCR-U to H-MPE contains V-MPE Rules
19699369	-	3-Minor	[S9] Removal of rule installed over S9 by VPLMN - CCA

Bug number	SR	Severity	Title
19725133	-	3-Minor	Upgrade 11.1.0_8.1.0 to 12.0.0_15.2.0 - Server status toggles from Active to OOS
19768521	-	2-Major	Unable to configure VIP on MPE/MRA correctly
19788740	-	3-Minor	CMP doesn't display/create any members under MRA associations
19789916	-	3-Minor	MRA replaces binding for separate PGWs due to shared APN
19846970	-	3-Minor	[S9] java.lang.IndexOutOfBoundsException after V-MPE receives RAA w DIAMETER_UN
19889595	-	3-Minor	S9 HPLMN sends RAR with wrong GBR for application rules
19954003	-	2-Major	[Connection] The connection to MRA cannot be established successfully.
19989312	-	3-Minor	[CMP]After chose IP preference to IPv6 and save then the page shows "IPv-1"
20003265	-	3-Minor	Unable set unset forced standby server at topology modification page
20025869	-	3-Minor	Configuration Templates: Policies Tab Show Details Application Error
20027517	-	3-Minor	[LI IPv6] MF does not respond to the MPE's IPv6 TCP SYN messages on Port 51000
20061258	-	3-Minor	arping hangs when called by qp_networktool.pl
20062907	-	3-Minor	Upgrade fails due to insufficient free space in vgroot
20096472	-	3-Minor	After upgrading CMP, schema version did not get upgraded
20124756	-	3-Minor	[LIConnectionStatus] MF name is not correct on page "LI Statistics".
20137081	-	2-Major	Policy 12.0: Clean install of 24.1 load and CMP GUI won't start
20161912	-	3-Minor	Failed to bring up GUI after clicking S-CMP name in NW-CMP
20164714	-	3-Minor	"Changing value in System setting didn't take affect in CMP
20174622	-	3-Minor	Initial config is not validating the OAM Default Route against the OAM Real IP
20192165	-	3-Minor	Add support for the custom AVP capabilities to all Diameter protocols supported
20213185	-	3-Minor	AAR-U reject by MRA after incremental upgrade
20219726	-	3-Minor	MPE doesn't remove rule in Charging-Rule-Report with status INACTIVE from RAA
20225758	-	3-Minor	[MPE]12. 0 PCRF need to modify config files for upgrading COMCOL

Bug number	SR	Severity	Title
20247550	-	3-Minor	[Upgrade Director] Upgrade Log displaying the wrong month
20263055	-	3-Minor	[System] Sync UID error is observed when adding S-CMP to NW-CMP
20264545	-	3-Minor	[System] PDN and Active session counts are incorrect in the NW-CMP KPI Dashboard
20282106	-	3-Minor	[System] Policies/policy group created at NW-CMP are not pushed to S-CMP
20290722	-	3-Minor	Platcfg Display Routes should include OAM IPv6 default route
20320226	-	3-Minor	[System] Unable to establish multiple TCP connections between MRA and its backup
20345253	-	3-Minor	Can't add S-CMP to NW-CMP
20360093	-	3-Minor	[System] Issue with Gx-Lite CCR-T route from backup MRA
20363539	-	3-Minor	[SessRec]MPE will failover automatically when testing SessionRecovery
20411642	-	3-Minor	"Rec'd Java Null Pointer Exception after Reapplying Config - MPE
20417363	-	3-Minor	[Upgrade Director] Upgrade manager page remains blank after a major upgrade
20424226	-	3-Minor	Call Model I - MPE reports DIAMETER_TOO_BUSY at 95% TPS load
20430834	-	3-Minor	[System] SDR is sent by MRA when AAR doesn't contain MIP6 information
20456850	-	2-Major	Upgrade from 11.1.0 to 12.0.0 failed -issue with network element model objects
20465753	-	3-Minor	G8 blade MPE server null point exception hit at MRA connection
20486109	-	3-Minor	Non-OAM routes cannot be auto re-applied during reboot process
20488912	-	3-Minor	[Upgrade Director] Spare blades fail to upgrade
20507283	-	3-Minor	[Upgrade Director] Failed to rebuild /var/camiant/log because cpustat logs
20524768	-	3-Minor	In Retryprofile RAR is not being resent if 1st RAA received with Error
20542850	-	3-Minor	MRA Associations: CMP Fails to Apply Settings to MRA

Bug number	SR	Severity	Title
20557011	-	3-Minor	Advanced Config: Default DIAMETER.EnableSessionCleanUp value can't be changed
20569052	-	3-Minor	[Backout] Unable to open rcmgr in MPEs after backout operation.
20569447	-	3-Minor	At 95% TPS rate (Call Model 3), the MPEs report DIAMETER_TOO_BUSY
20576928	-	3-Minor	[System] X1 IP address is set to <None> after upgrade from 11.1.2 to 12.0

Customer Known Bug Listing

Table 6: Policy Management Release 12.0 Customer Known Bugs lists known bugs in this release:

Table 6: Policy Management Release 12.0 Customer Known Bugs

Bug Number	SR#	Severity	Title	Customer Impact
19116834	-	3-Minor	[239507][SEC] Policy Web Application must follow ARB Cookie Design and Disclosure Req. and Guidelines	None - This is a security enhancement
19116835	-	3-Minor	[239508][SEC] Policy Web Application needs to comply with SCS and use CSRF recommended protections	None - This is a security enhancement
20386371	-	2-Major	Incompatibility between Multi-Level OAM and Checkpoint feature implementations	Due to the incompatibility, when a customer is using the Multi-Level OAM feature (in other words, all the CMP installations are configured to be S-CMPs or NW-CMPs), then the functions for managing checkpoints are disabled (not available in the GUI). This is to prevent the user from relying on the checkpoint function when it will not work as expected. If the customer relies on the Checkpoint functions as a key part of their processes for managing changes then they should not use the Multi-Level OAM feature

Chapter

7

Oracle References and Services

Topics:

My Oracle Support (MOS)

MOS (*https://support.oracle.com*) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with MOS registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at *http://www.oracle.com/us/support/contact/index.html*. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select 2 for New Service Request
2. Select 3 for Hardware, Networking and Solaris Operating System Support
3. Select one of the following options:

   - For Technical issues such as creating a new Service Request (SR), Select 1
   - For Non-technical issues such as registration or assistance with MOS, Select 2

You will be connected to a live agent who can assist you with MOS registration and opening a support ticket.

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

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (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 that 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.

Customer Training

Oracle University offers expert training on Oracle Communications solutions for service providers and enterprises. Make sure your staff has the skills to configure, customize, administer, and operate your communications solutions, so that your business can realize all of the benefits that these rich solutions offer. Visit the Oracle University web site to view and register for Oracle Communications training: *education.oracle.com/communication*. To reach Oracle University:

- In the US, please dial 800-529-0165.

- In Canada, please dial 866-825-9790.

- In Germany, please dial 0180 2000 526 (toll free) or +49 8914301200 (International).

- In Spain, please dial +34 91 6267 792.

- In the United Kingdom, please dial 0845 777 7 711 (toll free) or +44 11 89 726 500 (International).

For the appropriate country or region contact phone number for the rest of the world, please visit Oracle University's web site at *http://www.oracle.com/education/contacts*.

Locate Product Documentation on the Oracle Technology Network Site

Oracle customer documentation is available on the web at the Oracle Technology Network (OTN) 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 *www.adobe.com*.

1. Log into the Oracle Technology Network site at *http://docs.oracle.com*.
2. Select the `Applications` tile.
   The **Applications Documentation** page appears.
3. Select `Apps A-Z`.
4. After the page refreshes, select the `Communications` link to advance to the **Oracle Communications Documentation** page.
5. Navigate to your Product and then the Release Number, and click the `View` link (note that the Download link will retrieve the entire documentation set).
6. To download a file to your location, right-click the `PDF` link and select `Save Target As`.

Locate Product Release Software on the Oracle Software Delivery Cloud Site

Oracle Communications software is available for electronic download at the Oracle Software Delivery Cloud (OSDC) site, *https://edelivery.oracle.com*. Only authorized customers with a valid password may download software from the site.

1. Log into the Oracle Software Delivery Cloud site at *https://edelivery.oracle.com*.
   The **Terms & Restrictions** page appears.
2. Read and accept both the Oracle Trial License Agreement and the Export Restrictions Agreement.
   The **Media Pack Search** page appears.
3. Select `Oracle Communications` for Product Pack and `Tekelec` for Platform.
4. Click the **Go** button.
   All media packs that meet the search criteria are displayed on the page.
5. Select the media pack for your Product and Release Number and click the **Continue** button.
   The **Download** page appears.
6. Provide a valid password in the **Password** field and click the **Go** button.
7. To download a file to your location, click the **Download** button.

Chapter

8

Firmware Components

Topics:

The firmware components are software that is installed on the hardware. These components are listed in this chapter, and are also listed in the Firmware Release Notice. Please refer to the latest Firmware Release Notice for any updates to this list.

Firmware Components

The firmware document is available on the Oracle Technology Network (OTN) site at:

- *http://docs.oracle.com/cd/E57059_01/docs.67/E56670.pdf*