Oracle® Communications
EAGLE Element Management System

Release Notes

Release 46.3

E78336 Revision 2

January 2017

ORACLE®

Oracle Communications EAGLE Element Management System Release Notes, Release 46.3

Table of Contents

List of Tables

Chapter 1

Introduction

This Release Notes includes Feature Descriptions, 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 Notes are included in the Documentation Pack made available with every Software Release.

Chapter 2

Feature Descriptions

Topics:

This release delivers the following features:

- *Add Command History in EMS CMI for each user*
- *Configurable CMI behavior against errors during script execution*
- *Counter for command rejection at CMI*
- *EAGLE EMS Support and Compatibility with EAGLE 46.3*
- *EAGLE EMS to support IPv6 for SBI for EPAP*
- *Remove the need of root privileges to run/maintain/operate EEMS*
- *Search engine in EMS CMI script execution results page*

Add Command History in EMS CMI for each user

This feature provides Command Manager Interface (CMI) users the ability to access the last N commands executed in the CMI Send Command screen. The command history for the last N commands is provided for the **Type Command** pane on the **Send Command** screen.

The default value of command history size is 30. This value is configurable through the commandHistorySize parameter in the `/Tekelec/WebNMS/conf/tekelec/CmiParameters.conf` file.

See *Interface User's Guide* for more information.

Configurable CMI behavior against errors during script execution

This feature provides more options when using CMI Scripts, specifically in case of errors during script execution. While creating/modifying a script via the Create Script/Modify Script interfaces, a CMI user will be able to select one of the following behaviors:

- Continue - continue script execution on errors
- Stop - stop script execution on errors
- Configurable Stop On Error - define the required script execution behavior on command failures on a per-command basis

See *Interface User's Guide* for more information.

Counter for command rejection at CMI

This feature provides a summary of script execution. In order to show a summary of script execution, OCEEMS supports a number of counters related to script execution. These counters are available to users at the end of the script execution. They provide information regarding the CMI script execution, including the user who executed the script, start and stop time for the script, commands that failed or executed successfully, etc. Examples are as follows:

- Script executed by <username>
- Start time: <Date and time when script execution started>
- End time: <Date and time when script execution ended>
- Estimated No. Of Commands: <An estimated no. of commands in the script>
- Executed Commands: <number of commands that were executed>
- Successful Commands: <number of commands that were successful>
- Failed Commands: <number of commands that failed>
- Global Error: <any error of global nature that failed the script e.g., login failure on EAGLE>

This feature is supported for both Ad hoc and scheduled script execution. The execution summary is to be done on a per EAGLE node basis. For scheduled CMI scripts, these counters can be viewed by launching script execution results in the **Last Execution Result** column.

See *Interface User's Guide* for more information.

EAGLE EMS Support and Compatibility with EAGLE 46.3

This feature provides OCEEMS Release 46.3 with support and compatibility with EAGLE Release 46.3 and its features. The following features are introduced in EAGLE 46.3:

- AINP LNP Feature
- EAGLE MNP Data Base support for 240M DN
- EAGLE - Obsolete OAM Measurements
- Increase LNP DB Capacity (504M)
- Remove EAGLE FAK control
- Sigtran IPSG application on SLIC Card
- SMS-MO Blocking SCCP Spoofing
- SS7 Firewall on EAGLE

See *Release Notes* for EAGLE Release 46.3 for detailed information on the features.

Hardware

The IPSG on Service and Link Interface Card (SLIC) Feature introduces support for the SLIC.

Commands

The following commands are modified to support the AINP LNP feature:

- `chg-ainpopts`
- `rtrv-ainpopts`

The following command is modified to support the EPAP DB Expansion to 480M feature:

- `chg-stpopts`

The following commands are added to support the SS7 Firewall feature:

- `rept-stat-sflog` – This command displays the overall status of the logging framework on the EAGLE.
- `rept-stat-sfthrot` – This command displays the overall status of the throttling framework on the EAGLE.

The following existing commands are modified to support the SS7 Firewall feature:

- `alw-card`
- `chg-ftp-serv`
- `chg-gta`
- `chg-gttact`
- `chg-gttaset`

- chg-gttset
- chg-measopts
- chg-mtc-measopts
- chg-th-alm
- dlt-card
- dlt-ftp-serv
- dlt-gttaset
- ent-card
- ent-ftp-serv
- ent-gta
- ent-gttact
- ent-gttaset
- ent-gttset
- inh-card
- rept-ftp-meas
- rept-stat-alm
- rept-stat-card
- rept-stat-mfc
- rept-stat-sys
- rept-stat-trbl
- rmv-card
- rst-card
- rtrv-card
- rtrv-ftp-serv
- rtrv-gta
- rtrv-gttact
- rtrv-gttaset
- rtrv-gttset
- rtrv-measopts
- rtrv-mtc-measopts
- rtrv-th-alm

See *Commands User's Guide* for EAGLE for more information on the commands and parameters.

Measurements

As part of the SS7 Firewall feature, two new reports are added for the SFTHROT GTT Action. These two reports include a daily ("MTCD-SFTHROT") and a 30-minute ("SYSTOT-SFTHROT") report. There are also two new GTT Throttling Action measurement registers added to the MTCD-SFTHROT and SYSTOT-SFTHROT reports for the SS7 Firewall feature. The pegs for these measurement registers are collected on a per-system basis for 30-minute and daily intervals.

Subsystem Level:

- GTTATHTO - total number of messages that hit a particular Throttling GTT action
- GTTATHDI - total number of messages discarded because the Throttling GTT action was in "BLOCKED" state

One new GTT Logging Action measurement register is added for the SS7 Firewall feature. The pegs for this measurement register is collected on a per-system basis for 30-minute and daily intervals.

System Level:

- GTTASFLOG - total number of messages that hit SFLOG GTT action

Three new GTT Action MAP-SCCP Validation measurement registers are added for the SS7 Firewall feature. The pegs for these measurement registers are collected on a per-system basis for 30-minute and daily intervals.

- GTTAMSVTO - total number of messages that hit this GTT action
- GTTAMSVDI - total number of messages discarded by this GTT action
- GTTAMSVNA - total number of messages where validation was not applied by this GTT action

EAGLE EMS to support IPv6 for SBI for EPAP

This feature enhances OCEEMS to manage IPv6 enabled EPAP nodes. As part of this feature, OCEEMS provides the following functionality:

- Discovery - An interface to discover IPv6 enabled EPAPs in network and add them to OCEEMS.
- Map - An interface to display the added IPv6 enabled EPAP in OCEEMS map view and provide options for launching SSH terminal and web interface on the EPAP.
- Fault - An interface to display IPv6 enabled EPAP's alarms in both tabular and map interfaces.
- Security - An interface to restrict users' access to IPv6 enabled EPAPs discovery, map, and fault operations.

Note: In order to discover and manage IPv6 enabled EPAPs, the OCEEMS server must be dual stack (IPv4/IPv6) enabled.

See *Interface User's Guide* for more information.

Remove the need of root privileges to run/maintain/operate EEMS

This feature removes the need of super user 'root' for running the OCEEMS application. This feature allows non-root users to perform start/stop/restart server operations, as well as update configuration files.

With this feature, the use of 'root' user is limited to OCEEMS installation/upgrade/uninstallation procedures only.

Once the OCEEMS installation/upgrade is completed and a non-root user for OCEEMS operations has been created using the `updatePrivilegesForUser.sh` script, the installer is required to logout of the root user session. Now only the configured non-root user is used for further initial configuration for OCEEMS (creation of the SSL certificate, installation of schema, running other required scripts, etc.) and for OCEEMS operations.

See *Interface User's Guide* for more information.

Search engine in EMS CMI script execution results page

This feature provides a keyword-based search for CMI command/script execution results.

To support search engine functionality for command/script execution results, a **Search** button is provided on Send Command/Adhoc execution/Scheduled execution screens.

See *Interface User's Guide* for more information.

Enhancement Bugs

OCEEMS 46.3 supports the following enhancement Bugs:

Table 1: OCEEMS 46.3 Enhancement Bugs

Bug # and Title	Description
20889177 Identification and Management of EAGLE SLIC card	OCEEMS Release 46.3 supports and is compatible with the SLIC card.

Operational Changes

OCEEMS Release 46.3 contains new alarm messages.

OCEEMS 46.3 was tested with Java 8.

Alarm Messages

The Unsolicited Alarm Messages (UAMs) in this section are introduced or updated as part of the OCEEMS Support and Compatibility with EAGLE 46.3 feature.

SS7 Firewall feature

Table 2: New UAMs for SS7 Firewall

UAM ID	Severity	Message Text	Output Group	Notes
099	Major	Incompatible HW for provisioned slot	CARD	If E5-IPSM card is inserted in the slot that is provisioned as an IPSHC GPL with SS7 Firewall logging capability, the card shall be auto-inhibited.
423	Normal	Card reload attempted	CARD	
627	Critical	SFLOG SYSTEM is not available	SFLOG SYSTEM	The System has no SFLOG card that is Active/IS_NR.
628	Normal	SFLOG SYSTEM is available	SFLOG SYSTEM	The System has at least one SFLOG card that is Active/IS_NR.
629	Normal	SFLOG SYSTEM is removed	SFLOG SYSTEM	All SFLOG cards are deleted from the system.
630	Major	Throttle Threshold - exceeded	GTT	The Throttle threshold for a particular Throttling GTT Action has exceeded and any new messages hitting this Throttling Action are discarded for the remaining time of the current 30-second window. This alarm will be issued for each Throttling action for which the threshold has exceeded.
631	Normal	Throttle Threshold - cleared	GTT	The Throttle threshold for a particular Throttling GTT Action has cleared. This will be issued after the completion of the 30-second interval during which that action was in a BLOCKED state. This alarm will be issued for each Throttling action for which the threshold has cleared.
632	Minor	Alarm Threshold - exceeded	SCCP System	The system wide alarm threshold has exceeded.
633	Normal	Alarm Threshold condition cleared	SCCP System	The system wide alarm threshold has cleared.

Chapter 3

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 3: 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 3: Media Pack Contents

Name
Oracle Communications EAGLE Element Management System (46.3.0.0.1), Linux x86-64
Oracle Communications EAGLE Element Management System (46.3.0.0.0), Linux x86-64

Installed Patches

OCEEMS 46.3 uses Zoho (WebNMS) release v5.2 SP1 with patch 1.17.

Documentation Pack

All documents available for download from the Oracle Technology Network (OTN) site (*http://docs.oracle.com*) are listed in *Table 4: Documentation Pack Contents*.

Note: This list is accurate at the time of release but is subject to change. See Oracle Help Center for all available documents.

Table 4: Documentation Pack Contents

Core OCEEMS Documentation
Release Notes
Interface User's Guide
Security Guide
Upgrade/Installation Documentation
Upgrade/Install Guide
Reporting Studio Upgrade/Installation Guide
Reference Documentation
Licensing Information User Manual
Reporting Studio Licensing Information User Manual

Chapter 4

Upgrade Paths

Topics:

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.

Upgrade Paths

The possible full upgrade paths to OCEEMS 46.3 are listed in *Table 5: OCEEMS 46.3 Full Upgrade Paths*.

Table 5: OCEEMS 46.3 Full Upgrade Paths

From	To
OCEEMS Release 46.0	OCEEMS Release 46.3
OCEEMS Release 46.2	OCEEMS Release 46.3

Chapter 5

Product Compatibility

Topics:

This section shows release-specific compatibility with other related products.

Product Compatibility

Table 6: OCEEMS 46.3 Compatibility with Other Products shows OCEEMS 46.3 compatibility with other products.

Table 6: OCEEMS 46.3 Compatibility with Other Products

Product	Release	Compatibility
EAGLE	46.0	NC
	46.1	NC
	46.2	NC
	46.3	FC
LSMS	<13.0	NC
	13.0	PC
	13.1	PC
	13.2	FC
EPAP	<16.0	NC
	16.0	PC
	16.1	FC

Note: Customers should upgrade to the Fully Compatible release identified in the previous table.

Legend:

- FC - Fully Compatible
- PC - Partially Compatible (compatible but not fully functional; feature dependent)
- NC - Not compatible

Chapter 6

Resolved and Known Bugs

Topics:

This chapter lists the Resolved and Known Bugs for this release.

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
- Minor, No Loss of Service: Oracle severity beyond what is defined by TL 9000.

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

- 1 - Critical
- 2 - Major
- 3 - Minor
- 4 - Minor, No Loss of Service

Resolved Bug Listing

The tables in this section list bugs that are resolved in the following builds:

OCEEMS 46.3.0.0.1-463.13.0.

OCEEMS Reporting Studio 46.3.0.0.1-463.15.0.

OCEEMS 46.3.0.0.0-463.11.0.

OCEEMS Reporting Studio 46.3.0.0.0-463.11.0.

The Resolved Bugs table shows an impact statement for Severity 1 and 2 Bugs as well as for Severity 3 Bugs that are associated with a SR.

Note: Resolved bugs are sorted in ascending order by severity and then by bug number.

Table 7: OCEEMS Release 46.3.0.0.1-463.13.0 Resolved Bugs (December 2016)

Bug#	SR	Sev	Title	Customer Impact
24692667		2	CDS: Unable to start OCEEMS service from root with reboot	The OCEEMS service will not automatically start on system reboot when using a non-root administration user. A manual start for the service is required to restore operation of the system after reboot.
24848010		2	CDS :Alarm resynchronization for EPAP getting failed	The synchronization of alarms between the OCEEMS and EPAP system will fail when the host is being resolved by hostname instead of IP address.
24910429		2	OCEEMS_46.3: Port forwarding stops working after server reboot	The OCEEMS will stop receiving SNMP fault traps when configured for a non-root admin user.
24707925		3	LUI reports(Link, Linkset, Card) enhancements for large dataset	
24716267		3	CDS: Report Designer not opening from client	
24902988		4	CDS: Update Script /Tekelec/WebNMS/bin/E5MSConfigurationScript.sh	

Table 8: OCEEMS Reporting Studio Release 46.3.0.0.1-463.15.0 Resolved Bugs (January 2017)

Bug#	SR	Sev	Title	Customer Impact
24716105		3	CDS: Stop/Start of Reporting Studio is via root	
25168680		3	Update TMPDIR for i-net Clear Reports	

Table 9: OCEEMS Release 46.3.0.0.0-463.11.0 Resolved Bugs (September 2016)

Bug#	SR	Sev	Title	Customer Impact
21815475		3	Remove unused menu items from E5-MS GUI	
21942837	Y	3	SR: LinkSet report to be corrected	The report generation may produce duplicated row values in very uncommon situations.
22156512		3	OCEEMS_46.2_ST: Not able to launch LSMS web interface through OCEEMS	
23021762		3	Some LSMS alarms are not displayed on Network Events and Alarms GUI	
23146788		3	E5E1T1B card not displayed in Network Maps	
23598072		3	Update Java check from Java 7 to Java 8	
23630166	Y	3	SR: LUI report not opening: Error : 2003:A timeout is occur on waiting	The LUI Link Report is timing out for large ranges of data. This prevents the user from generating reports for multiple days or multiple Network Elements.
24300835		3	OCEEMS shows only 10 STPs on On Demand Polling page	
19941889		4	Status Update messages are displayed in the Alarm view	
21858473		4	The path for incoming CSV files needs to be changed for new installs.	
22302153		4	Move E5-MS 46.3 to use 5-digit marketing ID to be consistent with other products	
22757336		4	Update Maverick J2SSH to the latest release	
22902904		4	Update iNet packages	
22902925		4	Update MySQL to current version	
22924985		4	Configurable CMI behavior against errors during script execution	
22931343		4	Add Command History in EMS CMI for each user	
22931382		4	Search engine in EMS CMI script execution results page	

Bug#	SR	Sev	Title	Customer Impact
23022893		4	EAGLE EMS Support and Compatibility with EAGLE 46.3	
23071514		4	Identification and Management of EAGLE SLIC card	
23071546		4	Counter for command rejection at CMI	
23071641		4	EAGLE EMS to support IPv6 for SBI for EPAP	
23071794		4	Remove the need of root privileges to run/maintain/operate EEMS	
23293673		4	EAGLE 46.3 Commands Updates for OCEEMS 46.3	
23558014		4	New RoHS complaint EAGLE cards to be added	
23717415		4	INFO alarm shown as CLEAR alarm in the Fault GUI	

Customer Known Bug Listing

Table 10: OCEEMS Release 46.3 Customer Known Bugs (January 2017) lists known bugs in this release:

Table 10: OCEEMS Release 46.3 Customer Known Bugs (January 2017)

Bug#	SR	Sev	Title	Customer Impact
19092737		3	[215626]EMS : Multiple login failures in CMI script execution	In case of a login failure on EAGLE, user should try to login again and should be able to login successfully in the next attempt.
19092911		3	[217240]CMI Login Status Indicator not updated on loss of connectivity with STP	The CMI does not always reflect the accurate login status and can cause more work for the customer by issuing commands only to have them fail and then need to retry the commands once the user reconnects to the STPs.
19095580		3	[222774]E5-MS security operation tree issues needs to be fixed	There is no system impact as dependencies need to be manually resolved and only administrator needs to perform these operations.
19095859		3	[223022]Support of fbp (Frame Power Budget) shelf in E5-MS needs to be provided	Frame Power Budget shelf will not be available in Frame View.

Bug#	SR	Sev	Title	Customer Impact
19098846		3	[225467]Transaction APIs are using infinite timeouts	No impact to customers. No issues have been noted.
19098880		3	[225495]E5MS_45:Unable to scroll complete result set	User must expand frame to see complete results on one screen.
19098953		3	[225549]Some filtering criteria not supported in Network Events/Alarms section	No impact to system other than filtering options may be limited in custom views.
19099361		3	[225861]E5MS_45:Command box does not work correctly	No impact to customer operation.
19099362		3	[225862]E5MS_45:Renaming of category name fails intermittently	If the rename operation fails once, a user can perform the same on retrying it.
19099815		3	[226249]E5MS_45:Audit trails visible to user on Security Administration GUI	No impact to customer operation.
19100656		3	[226924]Message during backup is not visible on status bar of E5-MS	No impact to customer operation.
19101825		3	[227820]Whitespace between * accepted as a parameter for Sub-Resource criteria	No effect other than the Resource and Sub-Resource parameter entries do not work exactly the same.
19101895		3	[227874]Expand/collapse does not work properly on Polling script result panel	Window size is larger than desired for some screen sizes. User must use the scroll bar to see the information.
19102497		3	[228359]EMS terminal makes prov. change at login w/out checking if change needed	No impact to customer operation.
19103096		3	[228821]Audit trail issues	Operator can't create custom audits.
19104237		3	[229727]E5MS_45:logs flooded with failed status update messages	No impact to customer operation.
19104410		3	[229877]Non-permitted users can update inventory; are correctly barred from CMI	Customers create a few users who can work on a particular EAGLE only. These users would be barred from all other activities for another EAGLE. This is not currently possible for Inventory.
19105092		3	[230396]E5MS_45:Reports in HTML format are not resizable	No impact to Customer operation as other report formats work for generating reports.
19105219		3	[230483]All UIMs not captured, only system alive messages captured in Fault Mgmt	Customer can start monitoring all UIMs on the basis of column name.
19105302		3	[230538]Card graphic for E5-APP-B card not visible in E5-MS	The E5-APP-B card will not be displayed on the STP shelf graphics.

Bug#	SR	Sev	Title	Customer Impact
19105365		3	[230598]E5MS_45:Support for SIP commands should be present on CMI	Customer will not be able to use SIP commands from the EMS.
19105966		3	[231056]Cannot specify which server will be started as primary by default	Customer would need to manually check the server which is currently acting as Primary server.
19105967		3	[231057]After failed primary server recovers, it does not resume primary control	After the failed primary server recovers, it keeps running as a secondary server instead of resuming its primary role.
19107305		3	[232111]R45.1:Unable to distinguish different domain same point code Alarms	If the customer is using both N24 and ANSI and have the same point code in each, it is not possible to tell which point code the alarm is from. The user must do a `rept-stat-` on both point codes to determine which has an issue.
19111943		3	[235744]Complete result not visible via Send Command but OK with cut-through	Customer is directly running commands via cut through on STP. They are using CMI for very less work considering that it may give lesser output.
19114654		3	[237835]"Enter Password :" shown in server console after unknown duration	No impact. The "Enter Password" message is displayed in the console. Entering the password manually has no impact. All modules keep working in the intended way.
19114663		3	[237842]Discovery info events persist even after EAGLE discovery fails	None. Info events remain in the Event viewer.
19117355		3	[239911]E5MS installation directory Tekelec should be renamed to Oracle	The E5-MS system is installed under /Tekelec. This location will be updated in a future release.
19120548		3	[242468]E5MS_46:Results for aud-data not received on E5MS	STP Commands that require additional command responses are not supported in the E5-MS CMI scripting. These commands should be run interactively from a connection to an IPSM or fixed terminal.
20016363		3	E5MS_46.0.1:Unable to login E5MS client .	Single occurrence of an issue that prevented login to the client. The issue cleared itself. It could also be cleared manually by restarting the OCEEMS services.
21258142	Y	3	SR: Missing requirements for connection between Active and Standby systems	Replication and failover between servers is only possible when the IP connection between the servers is reliable and of sufficient capacity to

Bug#	SR	Sev	Title	Customer Impact
				support the amount of data being replicated between the server databases. If the IP connection is insufficient to properly replicate the data, the systems will not operate properly.
21798119		3	OCEEMS_46.2_FT: Resync getting performed on SET request with wrong username	A user associated with the OCEEMS in SNMPv3 configuration could be used by the northbound system even if it was not assigned to that particular STP.
21801499		3	OCEEMS_46.2_FT: Incorrect names are displayed on NBI and Agent GUIs	No impact to Customer operations.
21801553		3	OCEEMS_46.2_FT:-User is able to delete associated SNMPv3 view	No impact to customer operations.
21816644		3	OCEEMS_46.2_FT: Wrong alertSourceIP displayed in traps from EAGLE	During IPSM card failover, the alertSourceIP is reported as the IP address of the IPSM card. This impacts customer operations only when the Northbound system uses this field to perform alarming.
21828371		3	OCCEMS_46.2_FT: GetNextRequest-PDU not supported in SNMPv3	SNMP GetNextRequest and GetBulkRequest are not supported on OCEEMS. No impact to customer operations.
22058494		3	OCEEMS_46.2_ST: Wrong licensed components' name on OCEEMS GUI.	No impact to customer operation.
22126601		3	OCEEMS_46.2_ST: Redundancy lost in failover setup	There is no impact to the system unless the failover is initiated rapidly from system to system multiple times. If the failover is switched multiple times in series, the failover replication may need to be reconfigured on the system.
22126630		3	OCEEMS_46.2_ST: Dynamic update is not working properly.	If a user updates the NBI configuration, this change is not updated in the open GUI screens for other users. The new configuration information will be reflected when the GUI screen is reopened.
22157264		3	OCEEMS_46.2_ST: OCEEMS sends traps twice after upgrade.	This issue has not been reproduced. There is no impact to customer operations.
23266331	Y	3	SR: revoke unused replication privileges during upgrade procedure	Additional configured replication users in the MySQL database may be present if the original configuration is not reused.

Bug#	SR	Sev	Title	Customer Impact
23291061		3	OCEEMS_46.3_FT: Occurrence of E5-MS in custom views post upgrade	No impact to customer operations. The Timestamp column contains the name E5-MS instead of OCEEMS.
23561768		3	OCEEMS_46.3_FT: Alarm GUI's filter not removed	The alarm filter becomes fixed on a GUI client and is unable to be removed. A restart of the Client GUI application will resolve the issue.
23590522		3	OCEEMS_46.3_FT: No alertSourceIP in OCEEMS generated traps	For alerts generated from within the OCEEMS system, the alertSourceIP binding may not contain the IP address of the OCEEMS system.
24382757	Y	3	Exception raised while running restoration of backup file	A java exception related to conf files is sometimes displayed on the console during the restore backup operations. This message may be safely ignored.
24404425		3	Handle failover.xml and log4j.xml files for user changes	Manual changes to these two files are not preserved during an upgrade. No impact to normal operations.
24447454		3	OCEEMS_46.3_ST: OCEEMS stuck in stopping script execution	If the CMI script execution does not stop after executing a stop action, the OCEEMS client may need to be restarted.
24481007	Y	3	SR: Login to Eagle fails sometimes when daily schedule task runs	The daily scheduled CMI scripts can occasionally fail in the login function. The script can be manually run as a workaround.
24488045	Y	3	SR: Map save does not work properly sometimes	The Save Map function is not functional for some system configurations.
19185383		4	Export is not working correctly for Auth Audit GUI	The Auth Audit export is not functioning from the E5-MS GUI. This export does not impact the reliable operation of the E5-MS service.
19652751	Y	4	SR: Alarms_SpecificDuration_WithSeverity_ UAM_Number.rpt is not functional	The report Alarms_SpecificDuration_WithSeverity_ UAM_Number.rpt is not functional.
20310455		4	Help buttons redirect to webnms.com	No impact to customer operations.
20890630		4	SR: Framework updates to permit regional views	Map and alarm views cannot be assigned on a regional basis.
21621882		4	NMS_STATUS_MONITOR table missing	No impact to customer operations.
21832884		4	CDS: Upgrade output of "No mysql backup directory found"	No impact to customer operations.

Bug#	SR	Sev	Title	Customer Impact
21848874		4	CDS: OCEEMS 46.2.0 CDS] Procedure to change timeformat should be via GUI	No impact to customer operations.
21848909		4	CDS: Critical alarms displayed during resynchronization of alarms	Critical Status update messages will be displayed during the resynchronization process. These alarms do not impact customer operations.
24390214	Y	4	SR: Remove test DB from E5-MS	No impact to customer operations.

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 Help Center Site

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

1. Access the Oracle Help Center site at *http://docs.oracle.com*.
2. Click **`Industries`**.
3. Under the Oracle Communications subheading, click the **`Oracle Communications documentation`** link.
   The Communications Documentation page appears. Most products covered by these documentation sets will appear under the headings “Network Session Delivery and Control Infrastructure” or “Platforms.”
4. Click on your Product and then the Release Number.
   A list of the entire documentation set for the selected product and release appears.
5. To download a file to your location, right-click the **`PDF`** link, select **`Save target as`** (or similar command based on your browser), and save to a local folder.

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 site, *https://edelivery.oracle.com*. Only authorized customers with a valid password may download software from the site.

For directions on downloading the software and other information about using this site, click **FAQ** in the top right corner.

Appendix A

Firmware Components

This appendix is not applicable to EAGLE, ExAP or LSMS releases.