Oracle Communications EAGLE Element Management System

Security Guide

Release 47.0
F99749-01
June 2024

Oracle Communications EAGLE Element Management System Security Guide, Release 47.0

F99749-01

Contents

What's New in This Guide

Release 47.0 - F99749-01 - June 2024

- Updated the information about the operating system compliant with OCEEMS 47.0 in the Overview of OCEEMS Security section.
- Added the details of TLSv1.3.
- Updated the Oracle Linux version from 7.0 to 8.0 in the Pre-Installation Configuration and Operating System Security Patch Update sections.
- Updated the information about the OCEEMS support for SNMP configurations for EPAP, EAGLE, and LSMS in the SNMP Configuration section.

1 Introduction

This chapter contains general information such as an overview of the guide, how to get technical assistance, and where to find additional information.

1.1 Overview

This guide describes how to ensure a secure installation of Oracle Communications EAGLE Element Management System (OCEEMS), and explains OCEEMS security features.

1.2 Scope and Audience

This guide is intended for administrators that are responsible for product and network security.

1.3 Documentation Admonishments

Admonishments are icons and text throughout this manual that alert the reader to assure personal safety, to minimize possible service interruptions, and to warn of the potential for equipment damage.

Table 1-1 Admonishments

Icon	Description
	Danger: (This icon and text indicate the possibility of *personal injury*.)
	Warning: (This icon and text indicate the possibility of *equipment damage*.)
	Caution: (This icon and text indicate the possibility of *service interruption*.)
	Topple: (This icon and text indicate the possibility of *personal injury* and *equipment damage*.)

1.4 Manual Organization

This manual contains the following chapters:

- Introduction contains general information such as an overview of the manual, how to get technical assistance, and where to find more information.

- OCEEMS Security Overview describes basic security considerations and provides an overview of OCEEMS security.
- Performing a Secure OCEEMS Installation describes the process to ensure a secure installation of OCEEMS.
- Implementing OCEEMS Security explains OCEEMS security features.

1.5 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.

1.6 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.

1.7 Related Publications

For information about additional publications related to this document, refer to the Oracle Help Center site. See Locate Product Documentation on the Oracle Help Center Site for more information on related product publications.

1.8 Customer Training

Oracle University offers training for service providers and enterprises. Visit our web site to view, and register for, Oracle Communications training:

http://education.oracle.com/communication

To obtain contact phone numbers for countries or regions, visit the Oracle University Education web site:

www.oracle.com/education/contacts

1.9 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.

2
OCEEMS Security Overview

This chapter describes basic security considerations and provides an overview of OCEEMS security.

2.1 Basic Security Considerations

The following principles are fundamental to using any application securely:

- **Limit privileges as much as possible.** Users should be given only the access necessary to perform their work. User privileges should be reviewed periodically to determine relevance to current work requirements.
- **Monitor system activity.** Establish who should access which system components, and how often, and then monitor the user activity logs.
- **Install software securely.** For example, use firewalls, secure protocols using **TLS** (**SSL**), and strong passwords. See Performing a Secure OCEEMS Installation for more information.
- **Learn about and use the OCEEMS security features.** See Implementing OCEEMS Security for more information.
- **Keep up to date on security information.** Oracle regularly issues security-related patch updates and security alerts. You must install all security patches as soon as possible. See the "Critical Patch Updates and Security Alerts" Web site: http://www.oracle.com/technetwork/topics/security/alerts-086861.html

2.2 Overview of OCEEMS Security

The OCEEMS is a secure and reliable Element Management System (**EMS**) that enables administration of EAGLE fault, admin, and measurement data in a central place. The OCEEMS also enables fault management for Oracle Communications EAGLE Application Processor (**EPAP**) and Oracle Communications **LSMS**.

Operating System Security

The OCEEMS requires a CentOS 64-bit operating system, such as Oracle Enterprise Linux 7. OCEEMS was tested on Oracle Enterprise Linux 7.

> **Note:**
>
> FTP and Telnet are disabled in the default Oracle Linux installation, so connections from OCEEMS to other systems in non-secure mode or to the OCEEMS Northbound Interface (NBI) application are not possible (NBI connection is via Secure FTP only). If the OCEEMS must support and manage systems that do not conform to the recommended secure installation, then FTP and Telnet must also be installed or another operating system that includes these packages should be used.

Ports Usage and Firewall Configuration

The ports used by OCEEMS need to be open in firewall configurations. For a complete list of OCEEMS ports, see the "OCEEMS Ports Usage and Firewall Configuration" section in *Interface User's Guide*.

MySQL Database Security

The following OCEEMS security considerations apply to the MySQL database:

- Secure Database Access Credentials
  No *direct* database access is provided for in the OCEEMS; all access is programmed.

  The internal OCEEMS database is pre-configured with a password that you need to change to prevent unauthorized access to the database from the command line. For information about changing the MySQL root user's password, see *OCEEMS Database Password Change* in *Interface User's Guide*.
- Use SSH/SSL Connections
  SSH/SSL is a robust, commercial-grade, and full-featured toolkit that implements the security and network encryption. SSH/SSL provides secure data transmission through encryption keys. Encryption is required for the connection between the OCEEMS and the EAGLE, EPAP, and LSMS systems.

> **Note:**
>
> It is recommended to use SSH in Eagle. Perform the following procedure to enable SSH on Eagle:
>
> 1. `rept-stat-card:appl=ips`
> 2. Inhibit all IPSM cards: `inh-card:loc=<IPSM loc>`
> 3. `rtrv-secu-dflt` (check SSH is ON or OFF)
>
>   > **Note:**
>   >
>   > If SSH FAK is not enabled, first enable FAK. Refer to Eagle documents on how to enable the control feature. However, if FAK is already enabled, go to step 4 to enable SSH.
>
> 4. `chg-secu-dflt:ssh=on`
> 5. `alw-card:loc=<IPSM loc>`

3
Performing a Secure OCEEMS Installation

This chapter presents planning information to ensure a secure installation of OCEEMS.

For information about installing OCEEMS, see *Upgrade/Install Guide*.

3.1 Pre-Installation Configuration

All pre-installation configuration is set by the default Oracle Linux installation. No additional user configuration regarding security is required.

For information about installing Oracle Linux, see *Oracle Linux 7 Installation Guide*.

3.2 Installing OCEEMS Securely

All non-essential and non-secure services are removed or excluded from the default installation.

Oracle recommends using the default installation, unless there are specific customer needs for additional services.

3.3 Post-Installation Configuration

There are no required post-installation configuration changes pertaining to security.

Establishing various network connections between the OCEEMS and other systems is performed by using the EAGLE Discovery, EPAP Discovery, and LSMS Discovery applications as documented in *Interface User's Guide*.

3.4 Operating System Security Patch Update

Since OCEEMS is not an engineered system and EMS does not provide an operating system, customers need to take care of the security patch updates for their operating system. They need to update their operating system periodically with new security updates with the help of their operating system vendor.

Also, customers should make sure to use the latest updates of Oracle Linux 7. The operating system updates need to be applied frequently.

Note: For any support on the Oracle Linux installation/upgrade/security patch updates, customers should contact Oracle Linux Support.

4

Implementing OCEEMS Security

This chapter explains the OCEEMS security features.

4.1 LDAP-based Authentication on OCEEMS

The LDAP Client on OCEEMS feature implements the Lightweight Directory Access Protocol (LDAP) client interface on the OCEEMS system to allow centralized user management and authentication. The LDAP protocol allows the authenticated clients to access the LDAP database and use the information to in turn authenticate users based on the information retrieved from the LDAP servers.

Figure 4-1 Sample Call Flow for LDAP Authentication

OCEEMS supports the following modes of User Authentication:

1. OCEEMS Local Authentication: In this mode, the LDAP interface is not used and all information about the user is locally stored, including encrypted passwords.
2. LDAP authentication: In this mode, the LDAP interface is used for authentication. In case the LDAP server is unreachable, authentication will not be allowed.

To enable LDAP authentication, a script file `configureLDAP.sh` will be provided in the `/Tekelec/WebNMS/bin` directory. This script will be used for enabling or disabling LDAP based authentication. The OCEEMS admin must provide four inputs to this script:

1. whether the user wants to enable or disable LDAP based authentication
2. the URL of the LDAP server which will be used for authentication
3. the Organization Unit(OU) which will be used for OCEEMS users on LDAP
4. the BASE DN which is configured while configuring LDAP Client and can be viewed using the `authconfig-tui` command

> **Note:**
>
> The second, third, and fourth inputs will be asked only if the user chooses to enable the LDAP based authentication.

The script will have the option of enabling/disabling the LDAP authentication. Three new parameters will be introduced in the property file `server_conf.properties`, which is present in the `/Tekelec/WebNMS/bin/tekelec` directory. The three parameters are:

- LDAP_AUTHENTICATION
- LDAP_URL
- OU
- BASE_DN

The `LDAP_AUTHENTICATION` parameter will be set to false by default. The `LDAP_URL, OU` and `BASE_DN` parameters have a sample value by default. Only when a user configures LDAP based authentication will these parameters be initialized.

Enabling LDAP Authentication

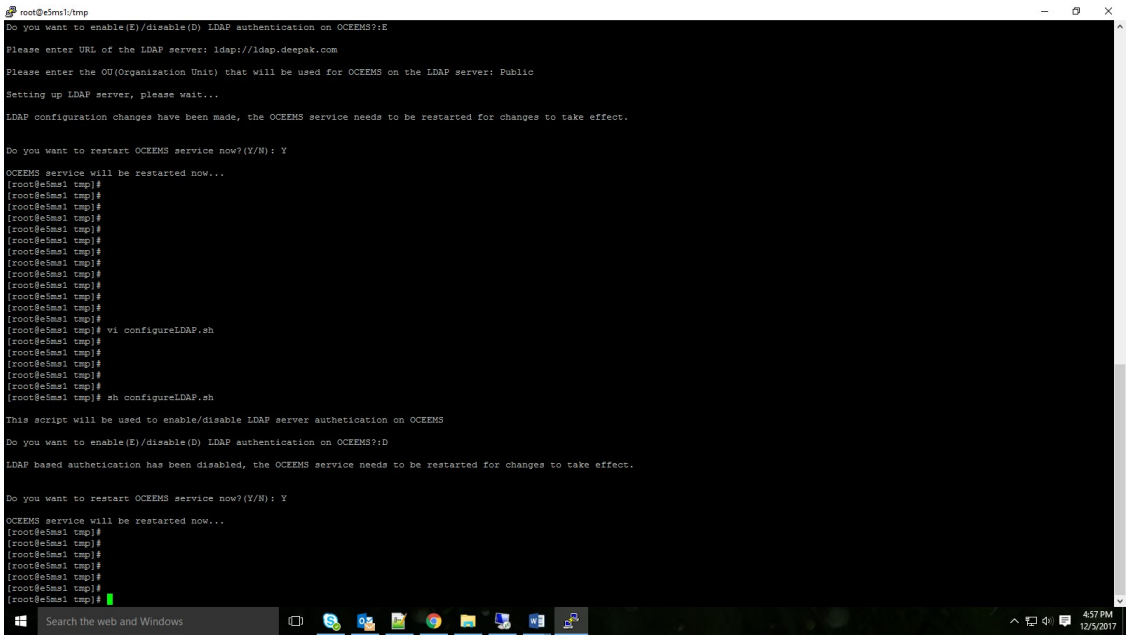
The `configureLDAP.sh` script is used by the OCEEMS admin to enable the LDAP server. An option to enable/disable LDAP authentication will be available, as seen in the following figure:

Figure 4-2 Enable LDAP Authentication

Disabling LDAP Authentication

The `configureLDAP.sh` script is used by the OCEEMS admin to disable the LDAP server, as seen in the following figure:

Figure 4-3 Disable LDAP Authentication



4.2 Managing Database Password Security

The internal OCEEMS database is pre-configured with a password that you need to change to prevent unauthorized access to the database from the command line. For information, see *OCEEMS Database Password Change* in *Interface User's Guide*.

4.3 Managing User Password Security

The OCEEMS provides default security settings and the System Administrator can change various rules and constraints. For example, by default, the OCEEMS does not provide any user password expiration limit, which can be set by the administrator after installation by using the OCEEMS GUI. Other examples of configurable settings include rules for password composition (minimum length and number of alphabetic/numeric/special characters) and login restrictions such as the maximum permissible number of incorrect login attempts. For more information, see *Password Management* and *Login Restrictions Management* in *Interface User's Guide*.

4.4 Managing Usergroups and Users

The OCEEMS provides a Security Administration interface to manage usergroups and users. Usergroups are created and OCEEMS operations (such as Security Administration and EAGLE Discovery) are assigned to the group. The operations assigned to a group indicate the operations to which users in the group are permitted access. A user can perform only the operations associated with the usergroup to which they belong.

The OCEEMS also offers usergroup management to limit and separate users' access authority to both commands and the managed equipment (for example, which EAGLE systems) they can access.

The EAGLE selection option will be available only when a user selects either of the CMI and Link Utilization modules.

For more information, see *Management of Usergroups and Users* in *Interface User's Guide*.

4.5 SNMP Configuration

The OCEEMS can use the industry-standard Simple Network Management Protocol (SNMP) interface to send alarms as trap messages to an **OCEEMS**. Release 46.5 introduces a feature that provides support for EPAP over SNMPv3, and a feature that provides support for LSMS over SNMPv3, both on southbound interface. With both features, the OCEEMS supports both SNMP v2c and SNMP v3 for EPAP/LSMS.

> **Note:**
>
> SNMP v3 is recommended and enabled by default.

In order to continue trap forwarding to the existing NMS(s) after the upgrade, it is recommended to update the NMS(s) to support SNMP v3 and then update the SNMP mode from v2c to v3 through the NMS configuration screen.

The three supported SNMP modes on the northbound interface include:

1. SNMP v2c Only Mode - the OCEEMS only supports SNMP v2c on the northbound interface.
2. SNMP v3 Only Mode - the OCEEMS only supports SNMP v3 on the northbound interface.
3. Both SNMP v2c and v3 Mode - the OCEEMS supports both SNMP v2c and SNMP v3 on the northbound interface.

> **Note:**
>
> In SNMPv2c, the default community string is `public`. Customers are advised to change the community string to something else of their choice for security reasons. Otherwise, there will be a risk that somebody might guess the default community string, thereby creating problems.

For more information about SNMP Configuration, see *Interface User's Guide*.

4.6 Create an OCEEMS SSL Certificate

To create an SSL certificate needed for HTTPS-based access for OCEEMS, the user must execute the `E5MSCertificateCreationScript.sh` script present in the `/Tekelec/WebNMS/bin directory`. During execution of the script, the user will be prompted for various inputs. The user must provide appropriate inputs (fitting the constraints) as highlighted in the following sample script execution:

```
[root@e5ms8 bin]# cd /Tekelec/WebNMS/bin

[root@e5ms8 bin]# sh E5MSCertificateCreationScript.sh

Welcome to OCEEMS SSL Certificate creation wizard!!!
```

```
Please provide OCEEMS home path (Absolute path till 'WebNMS' directory e.g. /
Tekelec/WebNMS): /Tekelec/WebNMS

Please provide the country name (e.g. US)-
(Must not be empty, permitted characters - alphabets and space): US

Please provide the state name (e.g. North Carolina)-
(Must not be empty, permitted characters - alphabets and space): North
Carolina

Please provide the organization name (e.g. Oracle)-
(Must not be empty, permitted characters - alphanumeric, underscore, dot and
space): Oracle

Please provide the organization unit name (e.g. E5MS)-
(Must not be empty, permitted characters - alphanumeric, underscore, dot and
space): OCEEMS

Please provide the keystore password -
(Must not be empty, length at least six, space not allowed, permitted
characters- alphanumeric, !, @ and #):<provide a password fitting the
constraints>

Please provide E5MS root user's password (used for E5MS client login):<>

Trying to generate encrypted password for keystore and trust store...

Creating certificates for BE in localhost server.
Certificate stored in file </Tekelec/WebNMS/Certs/server.cer>
Certificate was added to keystore
The Certificates and key files were created in /Tekelec/WebNMS/Certs and
copied into the respective conf directories
Done.

Updating keystore and trust store password in transportProvider.conf file...

Passwords successfully updated.
```

4.7 TLSv1.3

OCEEMS 47.0 introduces TLSv1.3, which is more secure and facilitates enhanced ciphers.