Oracle® Communications

EAGLE Security Guide

Release 47.1
F88468-01
October 2023

ORACLE

Oracle Communications EAGLE Security Guide, Release 47.1

F88468-01

Contents

My Oracle Support (MOS)

My Oracle Support (MOS) is your initial point of contact for any of the following requirements:

- **Product Support**:
  The generic product related information and resolution of product related queries.
- **Critical Situations**
  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.
- **Training Need**
  Oracle University offers training for service providers and enterprises.

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

Call the Customer Access Support 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:

- For Technical issues such as creating a new Service Request (SR), select **1**.
- For Non-technical issues such as registration or assistance with My Oracle Support, select **2**.
- For Hardware, Networking and Solaris Operating System Support, select **3**.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

Acronyms

The following table provides information about the acronyms and the terminology used in the document:

Table Acronyms

Acronym	Description
FTA	File Transfer Area
NMS	Network Management System
NP	Number Portability
SFTP	SSH File Transfer Protocol
SG	Signaling Gateway
SSH	Secure Shell
STP	Signal Transfer Point

What's New in This Guide

This section introduces the documentation updates for Release 47.1 in Oracle Communications EAGLE Security Guide.

Release 47.1 -F88468-01, October 2023

- There are no updates in this document for this release.

1
Introduction

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

1.1 Overview

This document provides guidelines and recommendations for configuring the Oracle Communications EAGLE to enhance the security of the system. The recommendations herein are optional and should be considered along with the approved security strategies of your organization. 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.

1.2 Scope and Audience

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

1.3 References

For more information, refer to the following documents:

1. *DatabaseAdministration - GTT User's Guide*
2. *Database Administration - System Management User's Guide*

2
EAGLE Security Overview

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

2.1 Basic Security Considerations

The following principles are fundamental to using any application securely:

- **Keep software up to date.** This includes the latest product release and any patches that apply to it.
- **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 monitor the **security log**.
- **Install software securely.** For example, use firewalls, secure protocols using **TLS** (**SSL**), and strong passwords. See Performing a Secure EAGLE Installation for more information.
- **Learn about and use the EAGLE security features.** See Implementing EAGLE 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

When planning your EAGLE implementation, consider the following questions:

- Which resources need to be protected?
  - You need to protect customer data, such as routing data and network traffic.
  - You need to protect internal data, such as proprietary source code.
  - You need to protect system components from being disabled by external attacks or intentional system overloads.
- Who are you protecting data from?
  For example, you need to protect your subscribers' data from other subscribers, but someone in your organization might need to access that data to manage it. You can analyze your work flows to determine who needs access to the data; for example, it is possible that a system administrator can manage your system components without needing to access the system data.
- What happens if protections on strategic resources fail?
  In some cases, a fault in your security scheme is nothing more than an inconvenience. In other cases, a fault might cause great damage to you or your customers. Understanding the security ramifications of each resource will help you protect it properly.

2.2 Overview of EAGLE Security

EAGLE is a secure and reliable signaling platform that provides **SS7**-focused signal transfer point (**STP**) and signaling gateway (**SG**) services that help manage intelligent routing, screening services, number portability (**NP**), equipment identity register, and integrated performance/service management.

Secure Database Access Credentials

Only authorized personnel are allowed to access the database/admin commands, and a user ID and password are required. Provide minimum database access privileges to the operators so that unauthorized modifications can be avoided. For more information, see Implementing EAGLE Security.

SSH and SFTP

The Secure Shell (**SSH**) protocol and SSH File Transfer Protocol (**SFTP**) are used by default for all IP connections, providing secure data transmission through encryption. These secure protocols can be disabled, but this is not recommended. The feature ON or OFF will not disable or enable the SSH or the SFTP.

For Release 46.5 and later. the EAGLE OA&M IP Security feature is enabled by default and the feature entry is used to control only the alarming if the SSH for terminals or Security of FTP Server entries is OFF. SSH for terminals and Security of FTP Server entries are controlled via the SECU-DFLT: SSH parameter and SECUIRTY parameter against the FTP servers entries, respectively. The following is expected after upgrade to release 46.5 or later from release 46.4 or earlier:

1. If the OA&M IP Security feature is currently (R46.4 or earlier) OFF, then it will remain OFF after the upgrade to R46.5.
2. If the OA&M IP Security feature is currently (R46.4 or earlier) ON, and all the FTP Servers have Security ON and the Telnet terminals are using SSH, then it will remain ON after the upgrade to R46.5.
3. If the OA&M IP Security feature is currently (R46.4 or earlier) ON, and there was 1 or more FTP Servers or Telnet terminals not using SSH, then it will be turned OFF after upgrade to R46.5, so that no new alarms will be generated after the upgrade.
4. If the OA&M IP Security feature is currently (R46.4 or earlier) OFF and SECU-DFLT-SSH parameter is ON, then the SECU-DFLT-SSH parameter will be turned OFF after the upgrade to R46.5, so that the access protocol used will not be changed after the upgrade.
5. If the OA&M IP Security feature is currently (R46.4 or earlier) OFF and the SECURITY parameter is ON for the FTP server entry in the FTP server table, then the SECURITY parameter for the FTP server entry (except for the SFLOG FTP server entry) will be turned OFF after the upgrade to R46.5, so that the file transfer protocol used will not be changed after the upgrade.

Use the SS7 Firewall Feature

The SS7 Firewall feature provides an additional set of capabilities to monitor, throttle, and validate messages:

- Logging capability on the SCCP card

The logging engine logs events from an SCCP card, primarily containing the MTP, SCCP, TCAP, and MAP portions of a message. The SCCP card transfers all log events for the MSUs that trigger the SFLOG GTT action. Two IPS cards act as the primary and secondary logging cards.

- Egress throttling
  For each SFTHROT GTT action, a threshold can be provisioned to limit the number of MSUs triggering the GTT action in a 30 second period, throttling such messages if the number of messages crosses the provisioned threshold.
- Map-Based Routing
  Map-based routing provides enhancements to the existing FLOBR/TOBR/GTT Actions framework to allow additional MAP components to be used in the selection process.
- MAP SCCP validation
  In certain MAP operations, some MAP parameters are expected to be the same as either the SCCP CdPA or CgPA. With SS7 Firewall, GTT Action SCPVAL will be used for this validation. This validation will be done only on MO-FSM and MT-FSM messages coming to the EAGLE.
- SS7 Firewall Stateless Enhancement
  This enhancement is comprised of a combination of SS7 Firewall Enhancement features, including Support for MAPv1 in MAP Based Routing, Support for Additional MAP Opcodes, Support for IMSI in MO-FSM, Support for Segmented XUDT, TCAP Decoding, GTTSET Measurements, and others.
- Support for CAT2 SS7 Security
  The CAT2 SS7 Security functionality allows Eagle to detect anomalies on inbound packets through bulk upload of customer IR.21 documents using CAT2 Utility. The CAT2 Utility runs outside EAGLE and can be downloaded from Oracle Softeware Delivery Cloud along with the other components. This is supported through EAGLE Category 2 security feature.

  > **Note:**
  >
  > The IR.21 document contains operator wise network information such as, MCC-MNC, Node GT (HLR/VLR/MSC), and CC-NDC. RAEX IR.21 provides the means of exchanging the IR.21 using a pre-defined data format and according to a standardized business process.

  The CAT2 functionality is divided into three parts:

  – **Conversion of IR.21 XML file**: The IR.21 XML file data is parsed on a linux machine and extracted in specific database tables.
  – **Bulk upload after conversion**: The data from the tables is uploaded to Eagle along with the Network card, supporting SCCP functionality.
  – **Data Validation**: Based on the data available in tables, the SCPVAL GTT action validates that CgPA and IMSI of MSU belongs to same operator. For more details, refer *Database Administration - GTT User's Guide*.

  For more details related to CAT2 SS7 Security functianality, refer *Database Administration - GTT User's Guide*.

For more information on the SS7 Firewall feature, see *Database Administration - GTT User's Guide*.

It is possible to use EAGLE Visualization with the SS7 security features for data visualization purposes. Visualized data allows understanding the current state of the network, which provides important insights for taking the security measures required to secure the network. For more information on the EAGLE Visualization feature, see *Logging and Visualization Feature User's Guide*.

Do Not Use Default Community Strings for SNMP Agent Implementation

SNMP is an industry-wide standard protocol used for network management. SNMP agents interact with Network Management Systems (NMSs) that are used to monitor and control the network. Community Names are used to validate commands sent from an NMS and traps sent to an NMS. You should not use the well-known default community strings, and instead use unique community strings (for example, for requests and traps). Unique community strings lessen the impact if a community string is compromised.

3
Performing a Secure EAGLE Installation

This chapter describes the process to ensure a secure installation of EAGLE.

For information about installing EAGLE, see the EAGLE *Installation Guide*.

3.1 Pre-Installation Configuration

No pre-installation configuration regarding security is required.

3.2 Installing EAGLE Securely

System servers are securely installed by Oracle personnel with passwords set at the start of the installation process that are known only by the Oracle installer. For each EAGLE, the Oracle installer sets the password to a unique and secure password.

3.3 Post-Installation Configuration

Following installation, the customer sets their own authorized password. For details about the secure password change process, see Secure Turnover to Customer.

For information about controlling user access to the database/admin commands, see Managing User IDs and Passwords.

4
Implementing EAGLE Security

This chapter explains the EAGLE security features.

4.1 Managing User IDs and Passwords

User IDs and passwords protect the system from unauthorized entry. To enter the system through a terminal, a user must enter a valid user ID/password combination at the system prompt. Up to 100 user ID/password combinations can be in use on the EAGLE. To maintain the security of the system, assign user IDs, passwords, and privileges to each user only as needed.

User IDs and passwords are not case sensitive.

User IDs must begin with an alphabetic character (a-z) and can contain up to 16 printable characters.

A password must not contain the associated user ID, and can contain up to 20 characters. A password must contain at least as many:

- Characters as specified by the `minlen` parameter of the `chg-secu-dflt` command
- Alphabetic characters as specified by the `alpha` parameter of the `chg-secu-dflt` command
- Numeric characters as specified by the `num` parameter of the `chg-secu-dflt` command
- Punctuation characters as specified by the `punc` parameter of the `chg-secu-dflt` command

These and other `chg-secu-dflt` command parameters can be used to change the global security settings for user IDs and passwords.

Managing Global Security Settings for User IDs and Passwords

Use the following commands to manage the global security settings for user IDs and passwords:

- `chg-secu-dflt`
  Table 4-1 shows the default value of each security parameter after EAGLE is installed, and the possible range for each parameter. Review and modify these settings as appropriate for your installation.

Table 4-1 Global Security Settings for User IDs and Passwords

Parameter	Default Value at Installation	Range	Description
:alpha	1	0-12	The minimum number of alphabetic characters (a-z) required in a password.

Table 4-1 (Cont.) Global Security Settings for User IDs and Passwords

Parameter	Default Value at Installation	Range	Description
:minintrvl	1	0-30	The minimum number of days before a password can be changed again.
:minlen	8	1-20	The minimum number of characters required in a password.
:multlog	no	no, yes	Specifies whether a user ID can be logged into only one terminal at the same time (no) or into multiple terminals at the same time (yes).
:num	1	0-12	The minimum number of numeric characters (0-9) required in a password.
:page	90	0-999	The number of days that the password for a user ID can be used before the user must change their password. The value of this parameter applies to all **EAGLE** user **IDs** unless a different value is specified for a specific user **ID** with the `chg/ent-user` command.
:pchreuse	4	0-10	The number of characters from an existing password that cannot be reused when setting a new password.
:pgrace	3	0-7	The number of days after a password expires that a user can continue to log in without changing their password.
:pnotify	7	0-30	The number of days before a password expires that a user is notified about the expiration.
:preuse	5	0-12	The number of most recent previous passwords that cannot be reused when setting a new password.
:punc	1	0-12	The minimum number of punctuation characters (any printable non-alphanumeric character, such as $, %, @, #).
:ssh	on	off, on	Makes all of the IPS telnet terminals use SSH instead of plain telnet.
:uout	90	0-999	The number of consecutive days that a user ID can remain active in the EAGLE and not be used. When the user ID has not been used for the number of days specified, the user ID is no longer valid and the EAGLE rejects any attempt to log into the EAGLE with that user ID. The value of this parameter applies to all EAGLE user IDs unless a different value is specified for a specific user ID with the `chg/ent-user` command.

- `rtrv-secu-dflt`

The `rtrv-secu-dflt` command displays the current values of the various security-related parameters that have been configured with the `chg-secu-dflt` command.

For more information about *Changing the Security Defaults*, refer to *System Administration Procedures* in *Database Administration - System Management User's Guide*.

Managing Users

Use the following commands to add users, modify users/access, and remove users:

- `ent-user`
  Use this command to add a user to the database.

  By default, all users are assigned to the **Basic** command class only. Each user ID (`uid`) can also be assigned to one or more of the non-configurable command classes shown in Table 4-2.

  The command class to which a user ID is assigned controls the set of system commands that the user can enter. Use the `rtrv-cmd` command to see the command classes to which commands are assigned.

Table 4-2 Adding Users to Non-Configurable Command Classes

ent/chg-user Parameter	Default Value	Range	Description
:uid		axxxxxxxxxxxxxxx	The user ID to be added to the database, beginning with an alphabetic character, up to a total of 16 characters.
:all	no	no, yes	The user has access to all commands in all non-configurable command classes (db, dbg, link, pu, sa, sys).
:db	no	no, yes	The user has access to all commands in the **Database Administration** command class.
:dbg	no	no, yes	The user has access to all commands in the **Debug** command class.
:link	no	no, yes	The user has access to all commands in the **Link Maintenance** command class.
:pu	no	no, yes	The user has access to all commands in the **Program Update** command class.
:sa	no	no, yes	The user has access to all commands in the **Security Administration** command class.
:sys	no	no, yes	The user has access to all commands in the **System Maintenance** command class.

- `chg-user`
  Use this command to change user access to commands, change user IDs, and change passwords.
- `dlt-user`
  Use this command to remove a user from the system database.

For more information about *Adding a User to the System*, *Changing User Information*, and *Removing a User from the System*, refer to *System Administration Procedures* in *Database Administration - System Management User's Guide*.

Configuring Command Classes

If the non-configurable command classes are too broad, the Command Class Management feature can be used. The Command Class Management feature is used to define up to 32 configurable command classes that contain selected commands, and these configurable command classes can then be assigned to users.

For more information about *Configuring Command Classes*, refer to *System Administration Procedures* in *Database Administration - System Management User's Guide*.

4.2 Managing Terminal Command Class Assignments

You can configure access rights for a terminal using the `chg-secu-trm` command, and display access rights for a terminal with the `rtrv-secu-trm` command. Access rights determine whether a terminal or port can be used to issue commands in the various command classes. This can be useful to restrict the types of commands that can be entered on an EAGLE terminal.

For additional information about *Changing Terminal Command Class Assignments*, refer to *System Administration Procedures* in *Database Administration - System Management User's Guide*.

4.3 Managing Security-Related Terminal Characteristics

Terminal characteristics related to security are set using the `chg-trm` command parameters shown in Table 4-3, and should be reviewed and modified as needed for your installation.

Table 4-3 Security-Related Terminal Characteristics

chg-trm Parameter	Default Value at Installation	Range	Description
:dural	0100 (1 minute, 0 seconds)	0-59 (ss) 0-5959 (mmss) 0-995959 (hhmmss)	Terminal lockout time. The length of time that a terminal is disabled after the login/unlock failure threshold (see mxinv) has been exceeded.
:mxinv	5 attempts	0-9	Login/unlock failure threshold. The number of login attempt failures or attempts to unlock a terminal that can occur on the terminal before the terminal is disabled.
:tmout	30 minutes	0-99	Maximum channel idle time. The maximum amount of time, in minutes, that a login session on the specified port can remain idle (that is, no user input) on the port before being automatically logged off.

For additional information about *Changing Terminal Characteristics*, refer to *System Administration Procedures* in *Database Administration - System Management User's Guide*.

4.4 Managing Security Logs

EAGLE security logs collect information about commands that are issued on the EAGLE, such as user ID that issued the command, terminal on which the command was received, date/time that a command was received, and the result of the command execution. Use the following commands to manage EAGLE security logs:

- `rtrv-seculog`
  Use the `rtrv-seculog` command to display the contents of a security log.
- `copy-seculog`
  Use the `copy-seculog` command to periodically copy the contents of a security log to the file transfer area (FTA).
- `chg-attr-seculog`
  Use the `chg-attr-seculog` command to modify attributes that affect the operation of the security logging feature. As shown in Table 4-4, the `upldalm` and `upslg` parameters of the `chg-attr-seculog` command control whether security log alarms are used to assist in determining when to copy the contents of the security log to the FTA.

Table 4-4 chg-attr-seculog Parameters for Security Log Characteristics

Parameter	Default Value at Installation	Range	Description
upldalm	yes	yes, no	Specifies whether the security log alarms are on (yes) or off (no). The security log alarms are: **upload required** Indicates that the log has reached the threshold (set by the `upslg` parameter), at which point the log entries should be copied to the FTA of the fixed disk. **log overflowed** Indicates that the log is 100% full and log entries are being lost. The security log entries must be copied to the FTA of the fixed disk. **standby log contains >0 un-uploaded entries** Indicates that the log on the standby fixed disk contains entries that have not been copied to the FTA of the fixed disk.

Table 4-4 (Cont.) chg-attr-seculog Parameters for Security Log Characteristics

Parameter	Default Value at Installation	Range	Description
upslg	90	1-99	The percentage of the maximum security log capacity at which the EAGLE generates the **upload required** security log alarm, if the `upldalm=yes` parameter has been specified.
purgeperiod	0	0-180	Specifies the number of days after which the logs must get deleted. The database can contain up to 50,000 log entries. When the `purgeperiod` value is **0**, no security logs will be deleted but alarms will be generated based on the values of `upslg` and `upldalm` parameters. – `upslg` generates alarm when table logs go beyond the threshold. – `upldalm` generates overflow alarm when table is full. The logs are periodically purged. Each stale entry is deleted within few minutes of exceeding the age (in days). **Example**: On 1st of January (considering there are no prior log entries), the `purgeperiod` value is **1**. Then the log entries of 1st of January will start getting deleted from 3rd of January (If some entries are configured).

- `rtrv-attr-seculog`
  The `rtrv-attr-seculog` command is used to display the security log attributes that were configured using the `chg-attr-seculog` command.
- `rept-stat-seculog`
  The `rept-stat-seculog` command displays security log statistics, such as the number of new (not uploaded) entries in the log and the percentage of space used by those new entries.

For additional information about *Changing the Security Log Characteristics* and *Copying the Security Log to the File Transfer Area*, refer to *System Administration Procedures* in *Database Administration - System Management User's Guide*.

A

Secure Turnover to Customer

To ensure security of systems delivered to our customers and to satisfy Oracle policies, all passwords must be owned by the customer once transfer of ownership of systems has occurred.

A.1 Secure Turnover Process

Three key requirements address the fundamental principles of the secure turnover process:

- Oracle passwords will not remain on fielded systems.
- Oracle passwords will not be revealed to customers.
- Customer passwords will not be known by Oracle.

Goals of the Secure Turnover Process

Following are the goals of the password handoff process:

1. The Oracle installer sets passwords at the start of the installation process to unique values (passwords exclusively known and used by the Oracle installer, meeting the password complexity rules required by the system).
2. Following installation, the customer sets all passwords to values known only by the customer.

Secure Turnover Procedure

Perform the following steps for secure system turnover:

1. System servers are installed by Oracle personnel using common USB or tar file deliverables and installation procedures. The passwords set by the Oracle installer are known only to Oracle.
2. Following installation, the Oracle installer and authorized customer agent log into each EAGLE and change the password to the authorized operational setting for the customer. The Oracle passwords must remain known only to Oracle, and the customer passwords must be known only by the customer.
3. Following the entry of the new passwords by the customer agent, the Oracle installer attempts to log in to each server using the previously known password. This should result in a failed login attempt verifiable in the server logs.
4. The customer agent again logs in to each account using the new customer passwords to verify success with the new customer passwords.

B
SEAS Forwarder Script

SEAS Forwarder is a python script that installs as an SSH daemon subsystem, similar to how sftp-server installs as an sftp subsystem. The forwarder allows the EAGLE SEAS client to connect via SSH to the SEAS server running this script.

The EAGLE SEAS client connects to the SSH SEAS subsystem. The SSH daemon, upon seeing the SEAS subsystem request, starts an instance of the SEAS Forwarder script. Then, the forwarder establishs a TCP/IP connection to the local SEAS server.

After the connections are established, SEAS Forwarder acts as a conduit for all IP traffic passed between the EAGLE SEAS client and the SEAS server. The traffic that is passed through SEAS Forwarder is unaltered.

Requirements

Following are the requirements for installing SEAS Forwarder:

- Python 2.5.6 and above (Python 3.x not supported)
- SSH Daemon

Configuration

The following table lists the field configuration:

Table B-1 SEAS Forwarder Configuration

Field	Description	Value
logEnable	Enables or disables all logging support (syslogd and trace logging). Trace logging must still be enabled separately. If trace logging is enabled and logEnable is set to 0, all logging including trace logging will be disabled.	Valid values: 0 or 1 0 disable all logging 1 (default) enable logging
logLevel	If enabled, set the verbosity of the log output	Valid values: INFO, DEBUG, or TRACE INFO (default) The minimum output level. Logs the start and end of the seas forwarder instance. DEBUG Provides additional details. Includes INFO output. TRACE Very verbose output. Logs all traffic sent between SEAS server and EAGLE SEAS client. Includes INFO and DEBUG output.
syslogdAddress	Specifies the location of the syslogd log socket	Default value: /dev/log

Table B-1 (Cont.) SEAS Forwarder Configuration

Field	Description	Value
traceLogFileDir	Destination directory for "logLevel = TRACE" output	Default value: /tmp/
traceLogFileName	Name for "logLevel = TRACE" output file	Default value: seas_forwarder.log
traceLogFileSize	Maximum size of "logLevel = TRACE" output file in MBs.	Valid values: 1 or higher Default value: 2
traceBackupCount	Maximum number of "logLevel = TRACE" backup files.	Valid values: 0 or higher Default value: 5
traceLogEnable	Enable or disable trace logging for all instances of the SEAS Forwarder process if logEnable is set to 1.	Valid values: 0 or 1 0 (default) disable trace logging 1 enable trace logging
hostName	The name of the SEAS server host	Default value: localhost
hostPort	Port number the SEAS server is listening on	Default value: 4000
serverTimeout	The amount of time the connection between the SEAS Forwarder and the SEAS server can remain idle before disconnecting.	Default value: 300 seconds

Installation

> **Note:**
>
> The SEAS Forwarder zip file contains the following files:
>
> - seas_forwarder.py
> - seas_forwarder.cfg
> - README.txt

Perform the following steps to install SEAS Forwarder:

1. Create the `seas_forwarder` directory.
   The directory may be placed anywhere you choose.
2. Install all the three files into the `<install path>/seas_forwarder/` path.
3. Open `seas_forwarder.cfg`.Verify or update the following settings for logging.
   Verify the following field descriptions:
   - logEnable
   - logLevel
   - syslogdAddress
   - traceLogFileDir

- traceLogFileName
- traceLogFileSize
- traceBackupCount
- traceLogEnable

4. Open `seas_forwarder.cfg`. Verify or update the following settings for SEAS Server. Verify the following field descriptions:
   - hostName
   - hostPort
   - serverTimeout
5. Save the changes to the `seas_forwarder.cfg` file.
6. Add the SEAS subsystem to the SSH daemon:
   a. Edit the SSH daemon configuration file: `/etc/ssh/sshd_config`.
   b. Add the following line: `Subsystem seas /<install path>/seas_forwarder/seas_forwarder.py`.
   c. Save and close the file.
7. Restart the SSH daemon to allow the `sshd_config` file changes to take effect using the following command
   ```
   > service sshd restart
   ```
   The service restart does not affect the existing SSH sessions.

Logging

There are three supported log levels: INFO, DEBUG, and TRACE. Log output for INFO and DEBUG are written to the syslog daemon (syslogd). This allows multiple instances of SEAS Forwarder to log simultaneously to one log file location. On most systems, the output file for syslogd is in `/var/log/messages`.

The TRACE log level is the most verbose. It logs all data sent between the SEAS server and the EAGLE SEAS client. This log output is not sent to syslogd to prevent the SEAS Forwarder from overrunning the syslogd log file. Instead, a new log file is created based on the setting of traceLogFileDir, traceLogFileName, traceLogFileSize, and traceBackupCount.

When TRACE is enabled, INFO and DEBUG log output is written to the trace log file and to syslogd.

Based on the default values, up to six log files will be created at 2MB in size. This takes the form of:

- seas_forwarder.log.<process id> (newest log)
- seas_forwarder.log.<process id>.1
- ....
- seas_forwarder.log.<process id>.5 (oldest log)

The default settings allow the trace log to consume no more than 12MB of disk space per instance of the SEAS Forwarder process.

When trace logging is enabled, each instance of the SEAS Forwarder process has its own log file. By default, as mentioned above, each instance is limited to using 12MB of disk space. It is up to the system administrator to delete these log files. It is only recommended to

enable trace logging when debugging issues with SEAS Forwarder since this could produce several log files.