Oracle® Communications

Data Encryption User Guide

Release 14.2.0.0.0

G42419-01

2025

Oracle Communications Data Encryption User Guide, Release 14.2.0.0.0

G42419-01

Contents

1 Introduction

1.1 Description 1

2 Managing the Feature

2.1 Enable the Data Encryption Feature 1

2.2 Disable the Data Encryption Feature 3

2.3 Monitoring the Data Encryption Feature 3

2.4 Performance Impact 3

3 Upgrade Procedure

4 Measurement

5 Alarms

6 Error Codes

My Oracle Support

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:

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 My Oracle Support, select **2**.

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 lists the acronyms used in the document.

Table Acronyms

Field	Description
AES	Advanced Encryption Standard
DSA	Diameter Security Application
EIR	Equipment Identity Register
FABR	Full Address Based Resolution
GCM	Galois/Counter Mode
GUI	Graphical User Interface
MNP	Mobile Number Portability
NOAMP	Network OAM and Provisioning
REST	Representational State Transfer
SFAPP	SS7 Firewall - Stateful Applications
SOAP	Simple Object Access Protocol
TPD	Tekelec Platform Distribution
VIP	Virtual IP
VSTP	Virtual Signaling Transfer Point

What's New In This Guide

This section introduces the documentation updates for Release 14.2.0.0.0.

This is the initial release of the document.

1 Introduction

OCUDR stores subscriber data in its database in an unencrypted format. You can access this data through standard interfaces, such as SOAP, REST, and ComAgent. The subscriber database does not provide additional encryption when accessed from the MySQL prompt. The Data Encryption feature provides data-at-rest encryption for the subscriber database, giving added security for critical subscriber information, especially for Diameter Security Application (DSA) and SS7 Firewall - Stateful Applications (SFAPP) use cases. This feature encrypts data stored in the database and prevents unauthorized users from accessing the data.

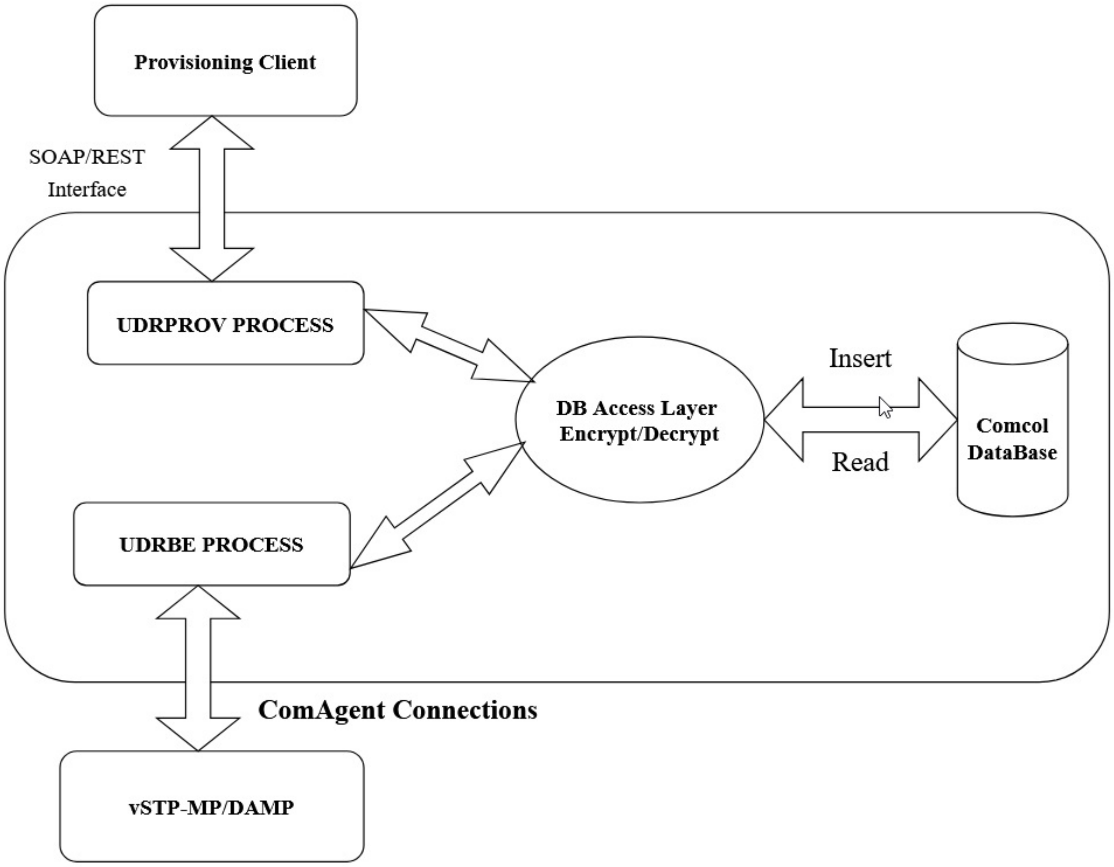
1.1 Description

The Data Encryption feature is implemented using the AES-256-GCM mode algorithm from the libcrypto library in OpenSSL 1.1.1k. This library is included as part of the TPD build. AES-256-GCM is a symmetric encryption algorithm that combines the Advanced Encryption Standard (AES) with the Galois/Counter Mode (GCM) of operation. The system encrypts or decrypts data in the database access layer for all incoming requests from all interfaces, such as provisioning and signaling. The system stores this encrypted data in the COMCOL database.

The data stored in UDR can be either encrypted or unencrypted. From 14.2.0 release onwards, UDR supports encrypting data stored in the comcol database. The system encrypts data using a preconfigured key. The same key is used to decrypt the data when a read request is received.

> **Note**
>
> For UDR 14.2.0 release, the Data Encryption feature supports only DSA and SFAPP use cases.

Figure 1-1   Data Encryption



2 Managing the Feature

This section provides information about configuring this feature.

2.1 Enable the Data Encryption Feature

Perform the following steps to enable the Data Encryption feature:

1. Before you enable data encryption, export the existing subscriber data using the xmlexport tool. For more information, see Upgrade Procedure.
2. To activate the feature, you must generate a passphrase to use as the key for data encryption and decryption.
3. Perform the following steps to generate passphrase and to enable the Data Encryption feature.

Table 2-1 Enabling the Data Encryption feature

Step	Procedure	Result
1	**Active Network OAM and Provisioning (NOAMP) Virtual IP (VIP)**: a. Access the command prompt. b. Log in to the server as the `admusr` user. **Note:** The system does not display the password on the screen as you enter the characters.	Login as: `admusr`. Use keyboard interactive authentication. Password: `<password>`
2	**Active NOAMP VIP** The server returns the output to the command prompt.	`*** TRUNCATED OUTPUT *** VPATH=/opt/TKLCcomcol/runcm8.1.0:/opt/TKLCcomcol/cm8.1.0 PRODPATH= RELEASE=8.1.0 RUNID=00 VPATH=/var/TKLC/rundb:/usr/TKLC/appworks:/usr/TKLC/udr:/usr/TKLC/awpcommon:/usr/TKLC/comagent-gui:/usr/TKLC/comagent-gui:/usr/TKLC/comagent:/usr/TKLC/ccl PRODPATH=/opt/comcol/prod RUNID=00 VPATH=/opt/TKLCcomcol/runcm8.1.0:/opt/TKLCcomcol/cm8.1.0 PRODPATH= RELEASE=8.1.0 RUNID=00 VPATH=/var/TKLC/rundb:/usr/TKLC/appworks:/usr/TKLC/udr:/usr/TKLC/awpcommon:/usr/TKLC/comagent-gui:/usr/TKLC/comagent-gui:/usr/TKLC/comagent:/usr/TKLC/ccl:/usr/TKLC/dpi:/usr/TKLC/capm/prod/plugins PRODPATH=/opt/comcol/prod RUNID=00 [admusr@NOAMP-A ~]$`

Table 2-1 (Cont.) Enabling the Data Encryption feature

Step	Procedure	Result

3	Go to the upgrade path: `"/usr/TKLC/udr/prod/maint/loaders/upgrade/"`	`[admusr@NO-A ~]$ cd /usr/TKLC/udr/prod/maint/loaders/`
		`helper/         install/`
		`load.udr.install  patches/`
		`upgrade/`
		`[admusr@NO-A ~]$ cd /usr/TKLC/udr/prod/maint/loaders/upgrade/`
		`[admusr@NO-A upgrade]$`

4	Run the following command to generate the passphrase:
	`"./configurePassPhraseKey.sh"`
	Note: The minimum password length must be 8 characters.
		`[admusr@NO-A upgrade]$ ./configurePassPhraseKey.sh`
		`Please enter passphrase key:`
		`Dukw1@m?1`
		`Entered passphrase key is:  Dukw1@m?1`
		`  === changed 1 records ===`
		`[admusr@NO-A upgrade]$`

5	Run the following command to enable the Data Encryption feature:
	`"./enableDataEncryption"`
		The data encryption feature will be enabled as follows after successful execution of `"./enableDataEncryption"` command:
		`root@NO-A upgrade]# ./enableDataEncryption`
		`  === changed 1 records ===`
		`Enabling the data encryption feature is successful`
		`[root@NO-A upgrade]#`
		If any non-encrypted subscribers are present when you enable the Data Encryption feature, the system does not enable the feature and displays the following error message:
		`[root@NO-A upgrade]# ./enableDataEncryption`
		`Warning: There are non encrypted subscribers in the setup.Please clean the db first and then enable the data encryption feature.`
		`[root@NO-A upgrade]#`
		As indicated in the the error message, you must export the subscribers, clean up the database, and then try enabling the Data Encryption feature again.

2.2 Disable the Data Encryption Feature

Disable the Data Encryption feature as follows:

1. Run the following command to disable the Data Encryption feature:

   ```
   "./disableDataEncryption"
   ```

2. The feature will be disabled as follows:

   ```
   [root@NO-A upgrade]# ./disableDataEncryption
     === changed 1 records ===
   Disabled the data encryption feature
   [root@NO-A upgrade]#
   ```

3. If encrypted subscribers are present, the system does not disable the feature and displays the following error message:

   ```
   [root@NO-A upgrade]# ./disableDataEncryption
   Warning: There are encrypted subscribers in the setup.Please clean the db
   first and then disable the data encryption feature.
   [root@NO-A upgrade]#
   ```

4. According to the error code, you can clean up the database by exporting the subscribers, converting the data to ixml format, and then disabling the feature. After you disable the feature, import the subscribers that you exported earlier.

2.3 Monitoring the Data Encryption Feature

For successful use cases, all interfaces works the same as they do without data encryption. With data encryption enabled, the system encrypts and decrypts the data before storing it in the database. For failure cases, monitor the feature using the Error Codes, Measurement, and Alarms. Follow the corrective actions listed in the Alarms details for each failure.

2.4 Performance Impact

Enabling the Data Encryption feature has minimal impact on performance. The effect on capacity is also minimal.

3 Upgrade Procedure

If any non-encrypted subscribers are present when you enable the Data Encryption feature, the system does not enable the feature and displays an error message. As indicated in the error message, you must export the subscribers, clean up the database, and then try enabling the Data Encryption feature again. By default, the Data Encryption feature is disabled. To enable this feature post upgrade to UDR 14.2.0 release, you must export the subscriber data using XmlExport tool, and then enable the feature. For more information about enabling the feature, see Enable the Data Encryption Feature.

After you enable the feature, you must convert the exported subscriber data from `*.exml` to `*.ixml` format. Export all the subscriber data using Graphical User Interface (GUI). For more information, see "Scheduling Exports" section in *User Data Repository Bulk Import/Export File Specification*.

Table 3-1 Scheduling Export

Step	Procedure	Result
1	To schedule the export option from GUI, go to **Main Menu**, click **UDR**, then **Maintenance**, and **Export Schedule**. **Note**: You can export up to 30 million subscribers at one time. If you have more than 30 million subscribers, schedule multiple exports with appropriate key ranges.	The Export Schedule page is displayed. For more information, see *User Data Repository Bulk Import/Export File Specification*.
2	To monitor the status after scheduling the export, go to **Main Menu**, click **UDR**, then **Maintenance**, and **Export Status**.	The Export Status page is displayed. For more information, see *User Data Repository Bulk Import/Export File Specification*.
3	After you successfully export all subscribers, enable the Data Encryption feature. For more information, see Enable the Data Encryption Feature	For more information, see *User Data Repository Bulk Import/Export File Specification*.

Table 3-1 (Cont.) Scheduling Export

Step	Procedure	Result

4	After you enable the Data Encryption feature, generate the passphrase then convert the exported file to `*.ixml` format.	XmlConversion example as follows:
		`[root@NO-A provexport]# /usr/TKLC/udr/bin/xmlconverter  /var/TKLC/db/filemgmt/provexport/export_Test.MSISDN.202508130950.exml  /var//TKLC/db/filemgmt/provimport/import_Test.MSISDN.202508130950.ixml  create`
		`Completed (5 of 5)`
		`[root@NO-A provexport]# cd ../provimport/`
		`[root@NO-A provimport]# ls`
		`import_Test.MSISDN.202508130950.ixml`
		`[root@NO-A provimport]#`

5	Copy the `*.ixml` files to the configured import path. Go to **Main Menu**, click **UDR**, then **Configuration**, and **Provisioning Options**	The Provisioning Options page is displayed. For more information, see *User Data Repository Bulk Import/Export File Specification*.
6	Monitor the import status. Go to **Main Menu**, click **UDR**, then **Maintenance**, and **Import Status**	After you complete the import task, the Import Status screen displays the status as "Completed". For more information, see *User Data Repository Bulk Import/Export File Specification*.

ⓘ Note

For instructions on using XmlExport, XmlImport, and converting from `*.exml` to`*.ixml` format, see *User Data Repository Bulk Import/Export File Specification*.

4 Measurement

Two new measurements are introduced to capture encryption and decryption failures. You can use these measurements to monitor the failures.

1. **DataEncryptionFailed**: This measurement gets pegged whenever encryption fails. It applies to both provisioning and signaling operations.

Table 4-1 DataEncryptionFailed

Field	Details
Measurement ID	4020
Measurement Type	Simple
Measurement Dimension	Single
Description	The total number of data encryption failed.
Collection Interval	5 Mins
Peg Condition	When the data encryption fails.
Recovery	Verify that the configured passphrase is correct and then retry the operation.

2. **DataDecryptionFailed**: This measurement gets pegged whenever decryption fails. It applies to both provisioning and signaling operations.

Table 4-2 DataDecryptionFailed

Field	Details
Measurement ID	4021
Measurement Type	Simple
Measurement Dimension	Single
Description	The total number of data decryption failed.
Collection Interval	5 Mins
Peg Condition	When the data decryption fails.
Recovery	Verify that the configured passphrase is correct. You must use the same passphrase that was used when the subscriber was inserted. If the passphrase has changed, configure the passphrase that was used when creating the subscriber.

5 Alarms

Alarms and events are recorded in a database log table. You can view currently active alarms from the Launch Alarms Dashboard in the GUI. To view the alarms and events log, go to **Alarms & Events** and click **View History**.

The following alarms are introduced as part of the Data Encryption feature.

Table 5-1 23360 - DataEncryptionFailed

Field	Details
Alarm Type	UDR
Description	Data encryption failed. Check the passphrase and refer to the result log for details.
Severity	Major
Auto Clear Seconds	300
OID	DataEncryptionFailed
Recovery	Verify that the configured passphrase is correct and then retry the operation. If this event is unexpected, contact My Oracle Support for assistance.

Table 5-2 23361 - DataDecryptionFailed

Field	Details
Alarm Type	UDR
Description	Data decryption failed. Check the passphrase and refer to the result log for details.
Severity	Major
Auto Clear Seconds	300
OID	DataDecryptionFailed
Recovery	Verify that the configured passphrase is correct. You must use the same passphrase that was used when the subscriber was inserted. If the passphrase has changed, configure the passphrase that was used when creating the subscriber. If this event is unexpected, contact My Oracle Support for assistance.

Table 5-3 23362 -DataEncryptionPassPhraseConfigurationNotFound

Field	Details
Alarm Type	UDR
Description	Data Encryption feature is enabled but passphrase is not configured.
Severity	Major

Table 5-3 (Cont.) 23362 -DataEncryptionPassPhraseConfigurationNotFound

Field	Details
Auto Clear Seconds	300
OID	DataEncryptionPassPhraseConfigurationNotFound
Recovery	Data Encryption feature is enabled but passphrase is not configured. Configure the passphrase and retry the operation. If this event is unexpected, contact My Oracle Support for assistance.

6

Error Codes

Error codes are introduced for all the interfaces, such as like provisioning and signaling. The following table lists the set of response error codes and their associated value:

Table 6-1 Error Codes

Value	Error Code	Interface
70058	DataEncryptionFailed	SOAP
70059	DataDecryptionFailed	SOAP
70060	DataEncryptionPassPhraseConfigurationNotFound	SOAP
4106	DataEncryptionFailed	REST
4107	DataDecryptionFailed	REST
4108	DataEncryptionPassPhraseConfigurationNotFound	REST
230	DataEncryptionFailure	DSA/SFAPP -Signaling
231	DataDecryptionFailure	DSA/SFAPP -Signaling
232	DataEncryptionPassPhraseConfigurationNotFound	DSA/SFAPP -Signaling
171	DataEncryptionFailure	MNP/FABR/EIR/Enum – Signaling
172	DataDecryptionFailure	MNP/FABR/EIR/Enum – Signaling
173	DataEncryption PassPhraseConfigurationNotFound	MNP/FABR/EIR/Enum – Signaling