Oracle® Hospitality OPERA Property Management
Credit Card Encryption Key Utility
Release 5.x
E88549-01

October 2017
Contents

1 Tool Overview ........................................................................................................................................ 4
   Purge Unnecessary Credit Card Information ................................................................................. 5

2 Pre-Phase 1 Checks .................................................................................................................................. 6

3 Phase 1 – Using the Tool’s Web Application ....................................................................................... 7
   Prerequisites ........................................................................................................................................ 7
   Launching the Web Application ........................................................................................................... 7
   Results Following Completion of Phase 1 ............................................................................................ 7
   Troubleshooting .................................................................................................................................. 8
   Re-starting the Web Application ......................................................................................................... 8

4 Pre-Phase 2 Checks .................................................................................................................................. 9

5 Phase 2 – Using the Tool’s Windows Application ............................................................................... 10
   Prerequisites ......................................................................................................................................... 10
   Launching the Windows Application .................................................................................................... 10
   Results Following Completion of Phase 2 .......................................................................................... 10

6 Reference ................................................................................................................................................ 11
   Phase 1 – Key Generation and Re-encryption ...................................................................................... 11
   Phase 2 – Run the Wizard to Recompile the OPERA Database .......................................................... 16
      Option A. Starting WizCCUpd.exe from the Command Prompt ................................................. 16
      Option B. Starting WizCCUpd.exe by Double-clicking on the Executable ......................... 17

7 Appendix – The Change Encryption Key Utility .................................................................................. 20
1 Tool Overview

This information is not applicable to OPERA V5.5.0.3 and later. For OPERA V5.5.0.3 and later, see Appendix – The Change Encryption Key Utility.

The Oracle OPERA Key Gen Tool provides OPERA sites with the capability to generate a new AES256 encryption key that can be used to re-encrypt all stored system credit card data.

The Tool is comprised of 2-parts:
- Web Application – used to generate the new key and to encrypt existing credit card data into a temporary storage repository
- Windows Application – used to replace the existing credit card data (encrypted with a previous key) with the newly encrypted data stored in the temporary storage repository

It is recommended that these two steps be run as close together as possible to ensure that there is no mismatch of re-encrypted keys.

As a data security measure, Oracle recommends that this utility be run on an annual basis (at minimum).
Purge Unnecessary Credit Card Information

To improve the performance of the Credit Card Encryption Key utility, it is recommended that you set General > PURGE UNNECESSARY CREDIT CARDS (Days to Purge Credit Cards) to a value between 5 and 365. As part of the OPERA Purge Routine, OPERA will automatically remove encrypted credit card numbers and expiry dates no longer required for business needs.
2 Pre-Phase 1 Checks

Prior to OPERA V5.2.3.0 it was necessary to run a check for duplicate records before starting Phase 1 of the utility. This is no longer necessary.
3 Phase 1 – Using the Tool’s Web Application

Prerequisites

An OPERA User that is to run Phase 1 of the OPERA Key Gen Tool must have the following OPERA Permissions:

- CHANGE_ENCRYPT_KEY
- CC_EDIT_INFO

Launching the Web Application

To start the OPERA Key Gen Web Application, users need to launch OPERA Utilities. The option is under the Utilities menu drop-down and the name of the option is:

Change CC Encryption Key

Upon selecting this option, the OPERA key Gen Web Application will be launched. Users are required to re-enter their password in this application prior to proceeding.

Results Following Completion of Phase 1

A new encryption key has been dynamically generated and has been stored into an obfuscated (wrapped) Oracle package.

Each OPERA table containing credit card data has been updated with newly encrypted data (this new data exists in non-system temporary columns – no existing system credit card data has been modified at this juncture.)
Troubleshooting

In the unlikely event that a failure occurs during Phase 1, it is essential to note that NO existing OPERA credit card data could have become corrupted and/or lost.

It is possible, however, that a system disruption (i.e. Network Failure) or previously corrupt credit card data would prevent Phase 1 from completing successfully. If a failure did occur, users are alerted on screen of a potential problem. In addition, all exceptions are logged in the system at several levels.

In order to troubleshoot a problem, we recommend that users start by reviewing the OperaKeyGen.log file. This file is located under the following directory for most installations:

[App Server Drive]:\oracle\10gappsvr\j2ee\home

Error reports in this file can be located by searching for lines that include the keyword ‘Exception’.

If an exception is logged in OperaKeyGen.log, it is likely that additional troubleshooting information can be located in the following 2 tables in the OPERA database:

- CC_REENCRIPT_STATUS
- BATCH_PROC_LOG

Re-starting the Web Application

Once any previously encountered issue has been resolved, users of the OPERA Key Gen Tool can re-start Phase 1. This is an especially important feature, as it may have been the case that the prior attempt had accomplished 90% of the re-encryption prior to being pre-empted.

To re-start the Web Application, simply launch OPERA Utilities and chose the [Change CC Encryption Key] menu option. Once you have verified your credentials, you will be presented with a notification that a previous attempt to re-encrypt failed. You will then be offered the option to re-start the process.
1. Prior to running phase 2, be sure all external components such as interfaces, OXI, OWS are stopped.

2. Possible erroneous constraint on stage$_profile_cards table. Check by running the following script:
   
   ```
   select owner,count(*) from dba_constraints where constraint_name='STAGE_PROF_CARDS_PK' group by owner;
   ```

   If records are returned, drop the constraints as follows:
   ```
   alter table <owner>.stage$_profile_cards drop constraint STAGE_PROF_CARDS_PK;
   ```

   Replace <owner> with the owner of the schema returned from the previous statement.
# 5 Phase 2 – Using the Tool’s Windows Application

## Prerequisites

- Phase 2 of the OPERA Key Gen Tool requires system downtime.
- We highly recommend that system administrators perform a full Oracle backup of OPERA data prior to commencement of Phase 2.
- The Windows Application must be run from the Application Server that is serving the OPERA application for the schema being updated.

## Launching the Windows Application

To run Phase 2, users must log onto the console of the application server and perform the following:

1. Open a command prompt (cmd.exe).

2. Change directories to opera tools folder:
   `\[your opera application server name]\micros\opera\tools\`

3. Execute `WizCCUpd.exe WizCCUpd.ini connect=[your connection string]`
   Sample connection string: `V36_HOTEL1/V36_HOTEL1@OPERA`

These instructions are also provided to the user on the utility screen following successful completion of Phase 1.

## Results Following Completion of Phase 2

- All OPERA credit card data will have been re-encrypted using the new encryption key.
- The new encryption package created in Phase 1 will be registered such that future requests to encrypt and/or decrypt will be serviced by this package.
Phase 1 – Key Generation and Re-encryption

Upon selecting the Change CC Encryption Key utility, you are prompted to re-enter your password. Doing so is acknowledgement that you have read and acknowledge the prerequisites stated on the screen.

Enter your password and click the Next button (click Close to exit the utility without changing the credit card encryption key).
If you make a mistake in entering your password, this screen appears.

Enter your password and click the Next button (click Close to exit the utility without changing the credit card encryption key).

Key assembly uses four separate keys. PCI best practice is for each key to be entered by a separate individual so that no one person has access to the entire key.
Enter and re-enter each of the four keys.

After entering and re-entering each key, click the **Next** button (click **Close** to exit the utility without changing the credit card encryption key).
After entering and re-entering key part 4, click the Finish button (click Close to exit the utility without changing the credit card encryption key).
This screen appears following successful completion of re-encryption – Phase 1.

A list of the re-encrypted database tables appears.

A list of the steps involved in Phase 2 shows the Phase 2 activities which must be carried out in order to complete the re-encryption of credit card data using the new keys.
If for any reason Phase 1 fails, the following screen appears. This screen allows you to re-start the Credit Card Encryption Key utility.

![Screen showing re-encryption tool](image)

Phase 2 – Run the Wizard to Recompile the OPERA Database

Phase 2 should be started as soon as practical after completion of Phase 1. Note that Phase 2 will involve a re-compile of the database schema using the re-encrypted credit card information. This requires that all users be logged out of the OPERA schema.

*Back up your database schema before beginning Phase 2.*

To run Phase 2 log onto the console of the application server. You can run the WizCCUpd.exe executable in either of the following ways:

**Option A. Starting WizCCUpd.exe from the Command Prompt**

1. Open a command prompt (`cmd.exe`).

2. Change directories to the `micros\opera\tools` folder:

   `\[your opera application server name]micros\opera\tools\`

3. Execute the command: `WizCCUpd.exe WizCCUpd.ini connect=[your connection string]`

   Sample connection string: `V36_HOTEL1/V36_HOTEL1@OPERA`
If you want to have WizCCUpd.exe run in the background (“unattended mode”) execute the command with the auto parameter:

```
WizCCUpd.exe WizCCUpd.ini connect=[your connection string] auto
```

If you run in unattended mode, you will receive no further prompts after entering the execute command. The program closes once the encryption update is complete.

**Option B. Starting WizCCUpd.exe by Double-clicking on the Executable**

Alternatively, you may start the WizCCUpd.exe by navigating to:

```
\[your opera application server name]\micros\opera\tools\ WizCCUpd.exe
```

and double-clicking on the WizCCUpd.exe executable.

The following login screen appears.

![Login Screen](image)

Provide the connect string information by entering your **Username**, **Password**, and the database **Instance**.

Click **OK** to continue.
Once **WizCCUpd.exe** starts, the following window appears.

![Windows Image]

Click the **Start Upgrade** button. (The credit card encryption key change utility uses the same database management programs as those used for a system upgrade; thus, the reference to an “upgrade.”)

This phase may take some time because it requires that OPERA recompile the database schema.

When the schema has been recompiled, the following screen appears.

![Windows Image]
Click the **OK** button to complete the credit card encryption key change. The following prompt appears.

![Confirm dialog box](image)

Click **OK**.

Users may now re-login and resume using OPERA.
7 Appendix – The Change Encryption Key Utility

This information is applicable to OPERA V5.5.0.3 and later. With the enhanced security implemented in the Oracle encryption routine, it is no longer necessary to change the encryption key or re-encrypt data, but can be done seamlessly if preferred.

This utility allows users belonging to the Supervisor user group with access to Utilities to select Utilities > Change Encryption Key to re-encrypt existing sensitive data with the active key or generate a new key. This opens the Change Encryption Key screen with options for New and Re-encrypt:

The New button generates a new key across the schema for all newly entered sensitive data from this time onward. This button is not available (greyed out) once the Re-encrypt button is clicked and is running. The New button can be used without following with Re-encrypt, which allows all newly entered sensitive data to be stored with the new key and the existing sensitive data is encrypted with the previous key (multiple key support).

The Re-encrypt button re-encrypts all the existing sensitive data with the current active key at the schema level (all Chains and all the properties belonging to them). This button can be used without first initializing New. A Re-encrypt status bar appears when the re-encryption process is running.

Users can be in the system during either process.