Oracle® Hospitality OPERA Property Management

Sensitive Information Encryption Key Utility
Release 5.x
F18431-01

November 2021

ORACLE®

ORACLE

Contents

1   Change Encryption Key Utility Overview

This document is only applicable to OPERA V5.5.0.3 and later.

This utility allows users belonging to the Supervisor user group with access to **Utilities** to select **Utilities** then **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**:
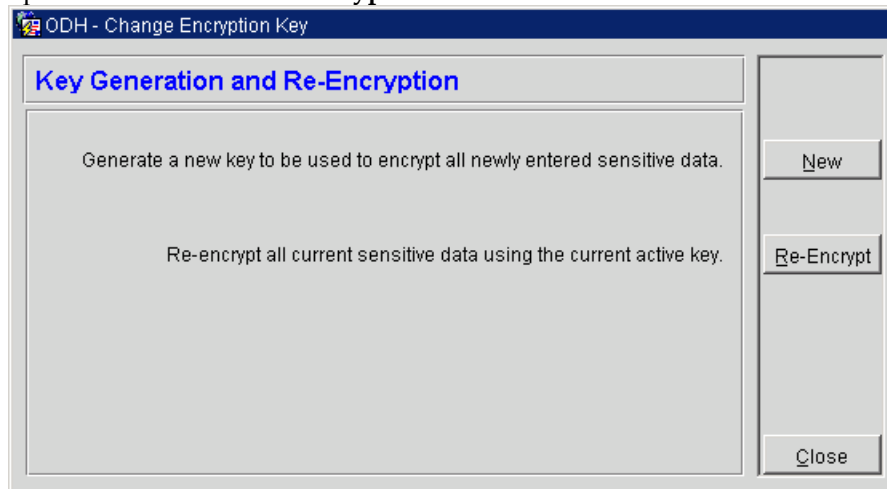
The **New** button generates a new key across the schema for all newly entered sensitive data from this time onward. This button is not available (greyed out) once the **Re-encrypt** button is clicked and running. Clicking the **New** button without clicking with **Re-encrypt** button afterwards allows 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 by clicking the **New** button. A Re-encrypt status bar appears when the re-encryption process is running.

Users can be in the system during either process.

Purge Unnecessary Sensitive 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.