Oracle® Hospitality Cruise Fleet Management

Security Guide

Release 9.0

E89561-02

April 2018

Contents

Figures

Tables

Preface

This document provides security reference and guidance for Oracle Hospitality Cruise Fleet Management.

Audience

This document is intended for:

- System administrators installing Fleet Management.
- End users of Fleet Management.

Customer Support

To contact Oracle Customer Support, access My Oracle Support at the following URL:

https://support.oracle.com

When contacting Customer Support, please provide the following:

- Product version and program/module name
- Functional and technical description of the problem (include business impact)
- Detailed step-by-step instructions to re-create
- Exact error message received and any associated log files
- Screen shots of each step you take

Documentation

Oracle Hospitality product documentation is available on the Oracle Help Center at http://docs.oracle.com/en/industries/hospitality/

Revision History

Date	Description of Change
March 2017	• Initial publication
April 2018	• Formatting updates

Fleet Management Security Overview

This chapter provides an overview of Oracle Hospitality Cruise Fleet Management security and explains the general principles of application security.

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 those components.
- **Install software securely.** For example, use firewalls, secure protocols using Transport Layer Security (TLS), Secure Sockets Layer (SSL) and secure passwords. See Performing a Secure Fleet Management Installation for more information.
- **Learn about and use the Fleet Management security features.** See Implementing Fleet Management Security for more information.
- **Use secure development practices.** For example, take advantage of existing database security functionality instead of creating your own application security. See Security Considerations for Developers 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” website: http://www.oracle.com/technetwork/topics/security/alerts-086861.html

Overview of Fleet Management Security

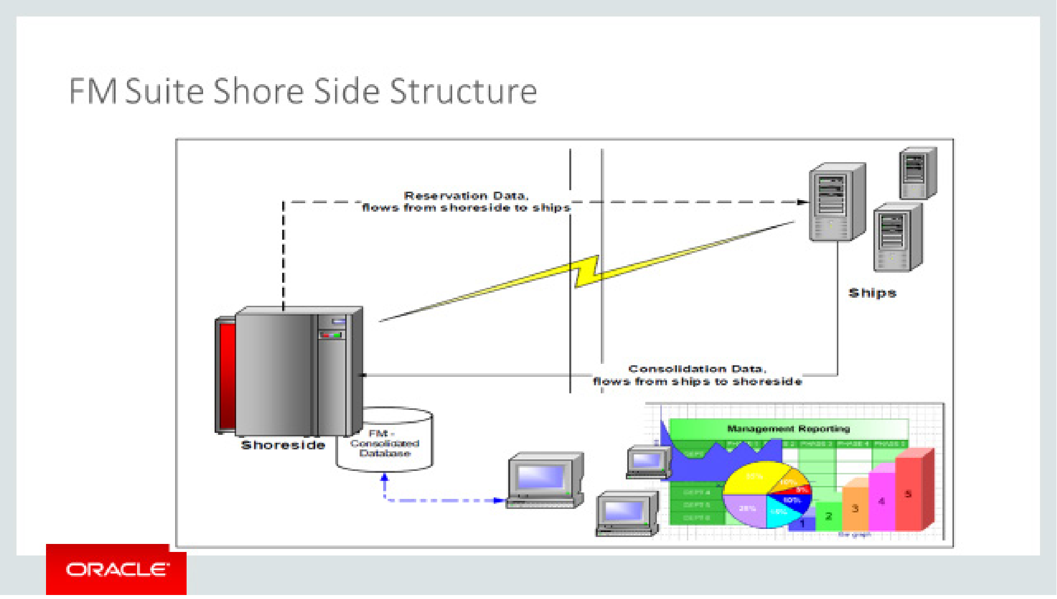
Fleet Management Architecture Overview

Fleet Management uses a Service-Oriented Architecture (SOA) and is a collection of loosely-coupled services. Most of the application pieces are services that can be deployed anywhere and only few are stand-alone applications/interfaces used for internal processing/integration. It is scalable since services can be distributed and do not have to be deployed on a single machine.

Technology

Fleet Management Service-Oriented Architecture (SOA) uses industry standards Simple Object Access Protocol (SOAP)/Representational State Transfer (REST) web services to work with internal and external applications. Typically, web services are deployed and exposed on Microsoft Internet Information Services (IIS) webserver, and IIS provides options to secure the communication using Secure Sockets Layer (SSL). It also uses Microsoft Message Queuing (MSMQ)/ Transmission Control Protocol/Internet Protocol (TCP/IP) / /File System for integration internally and externally. Every communication can be configured to use Secure Sockets Layer (SSL) if required. It also uses powerful encryption/hashing algorithms (Microsoft managed Rijndael, Microsoft Windows Data Protection Application Programming Interface (DPAPI), Password-Based Key Derivation

Function 2 (PBKDF2)) to encrypt and store sensitive customer information, application user passwords, application configuration information, secrets, and passwords.



FM Suite Shore Side Structure

Reservation Data,
flows from shoreside to ships
Ships
Consolidation Data,
flows from ships to shoreside
Shoreside
FM - Consolidated Database
Management Reporting
1
2
3
4
5
ORACLE

Figure 1 - Fleet Management Architecture Diagram

User Authentication

Overview

Authentication is the process of ensuring that people are who they say they are.

Thin and Thick Client Authentication

All user's credentials of Fleet Management are stored in the database. Anyone who wishes to access the thin or thick clients must provide a valid user name and password. To ensure strict access control of the Fleet Management, always assign unique usernames and complex passwords to each user. Password must follow Payment Card Industry-Data Security Standard (PCI-DSS) guide lines and must be at least 8 characters long and include letters and numbers.

An alternative authentication method for the thin and thick clients is Active Directory Lightweight Directory Access Protocol (LDAP). In this case, the Microsoft Windows username is used to login into the thin and thick clients.

Web Service Authentication

Web service uses two level approach for the authentication.

Security Token Approach: This method is used in the Web Services/Web Apps Only. For the first time/first request, predefined credentials are passed to gain a security token, and a security token is used with subsequent requests throughout the session.

Basic Authentication In Combination With Secure Sockets Layer (SSL): This method is used for the web services/web apps in combination with the above method. Authentication is linked to a specific Microsoft Windows user account. Microsoft Windows user account/password needs to be passed with each request for validation, and the Secure Sockets Layer (SSL) certificate is configured to make the requests secure.

Database Users

Fleet Management creates and uses predefined database users as required. FIDELIOBK, FCFMSADMIN, FCONSOL, FCRESVINT, FCRESVEXT, FCITIN, FCEVENT, FCSPSMCONFIG, FCWKF, FCCAM, FCUCI are the important predefined users used for different applications/solutions. FIDELIOBK is the key database user that stores the passwords/encryption keys for other database users in the encrypted form. Clients connect to the FIDELIOBK user and grab the passwords/encryption keys for database other users. FCFMSADMIN is the admin database user with all of the required configuration, application user security and parameters. The remaining database users are used for different applications/solutions.

Security Note

FIDELIOBK user password and Key Encryption Key (KEK) are hosted/stored on a Fleet Management Security Server. Clients need to connect to the Fleet Management Security Server one time to fetch the FIDELIOBK user password and KEK and store them locally in its configuration file in the encrypted form using Microsoft Windows Data Protection Application Programming Interface (DPAPI) method. Clients connect to the Fleet Management Security Server if the FIDELIOBK user password is changed and then connects to the FIDELIOBK user using the fetched password and grabs the passwords and encryption keys for the other database users.

Understanding the Fleet Management Environment

When planning your Fleet Management implementation, consider the following:

- **Which resources need to be protected?**
  - You need to protect customer data, such as credit-card numbers.
  - 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 subscriber's data from other subscribers, but someone in your organization might need to access that data to manage it. You can analyze your workflows 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 will happen 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.

Recommended Deployment Configurations

This section describes recommended deployment configurations for Fleet Management. Fleet Management can be deployed on a single server or in a cluster of servers. The simplest deployment architecture is the one shown Figure 2.
This single-computer deployment may be cost effective for small organizations, however, it cannot provide high availability because all components are stored on the same computer. In a single server environment such as the typical installation, the server should be protected behind a firewall.

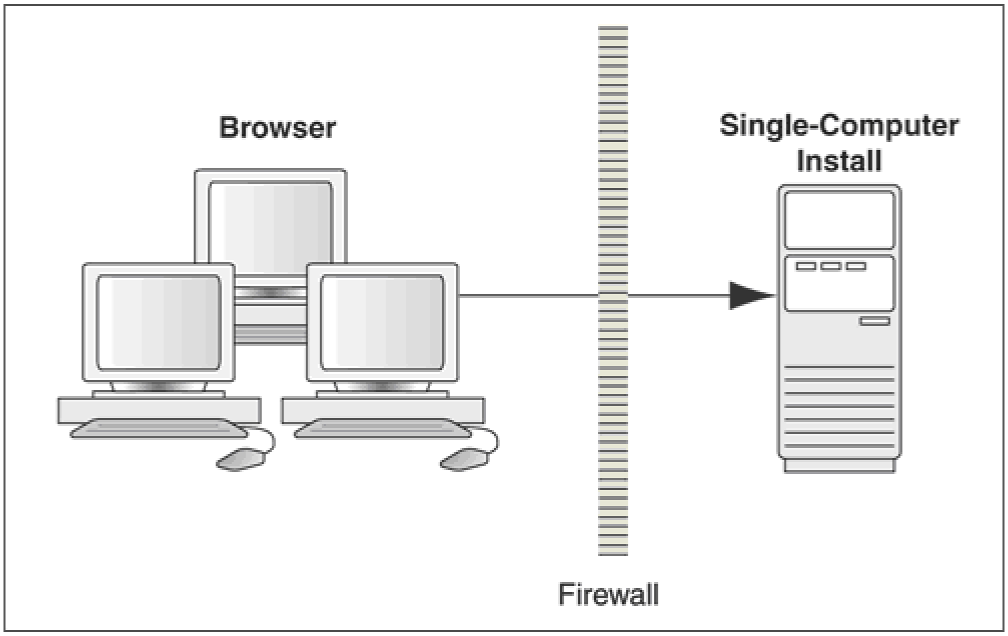


Figure 2 - Single Computer Deployment Architecture

The general architectural recommendation is to use the well-known and generally accepted Internet-Firewall-DMZ-Firewall-Intranet architecture shown in Figure 3 - Traditional DMZ View.

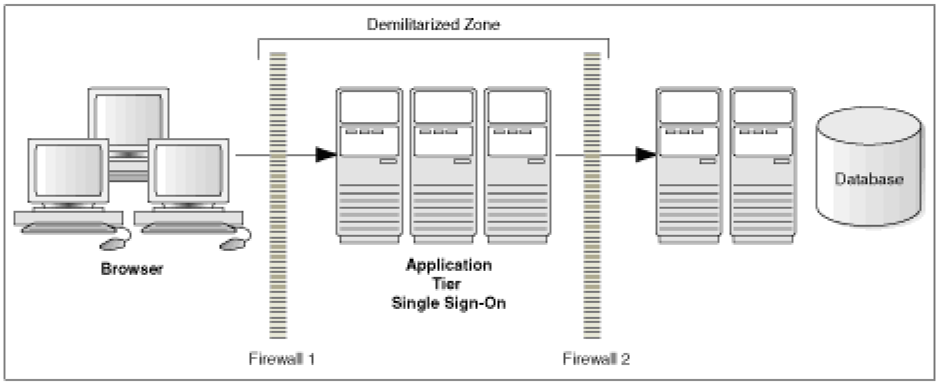


Figure 3 - Traditional DMZ View

The term demilitarized zone (DMZ) refers to a server that is isolated by firewalls from both the Internet and the Intranet, thus forming a buffer between the two. Firewalls separating DMZ zones provide two essential functions:

- Blocking any traffic types that are known to be illegal
- Providing intrusion containment, should successful intrusions take over processes or processors

See Appendix A Fleet Management Ports Numbers for more information about Fleet Management network port usage.

Component Security

Operating System Security

Prior to installing Fleet Management, it is essential that the operating system be updated with the latest security updates.

Refer to the following Microsoft TechNet articles for more information about operating system security:

- Windows Server 2012 Security
- Windows Server 2008 R2 Security

Oracle Database Security

Oracle Database

Refer to the Oracle Database Security Guide for more information about Oracle Database security.

Performing a Secure Fleet Management Installation

This chapter presents planning information for your Fleet Management installation.

For information about installing Fleet Management, see the *Oracle Hospitality Cruise Fleet Management Installation Guide*.

Pre-Installation Configuration

Prior to installation of Fleet Management, perform the following tasks:

- Apply critical security patches to the operating system.
- Apply critical security patches to the database server application.
- Create the required Oracle Database objects per the instructions in the *Oracle Hospitality Cruise Fleet Management Installation Guide* located on the Oracle Help Center (http://docs.oracle.com).
- Acquire Secure Sockets Layer (SSL) compliant security certificate from Certification Authority.
- Install Fleet Management Security Server and Configure, please check *Oracle Hospitality Cruise Fleet Management Security Server Installation Guide* for more information on how to install and configure.

Fleet Management Installation

You can perform a custom installation or a typical installation. Perform a custom installation to avoid installing options and products you do not need. If you perform a typical installation, remove or disable features that you do not need after the installation. The installation requires the user running the installation to have administrator privileges. No other users have the required access to successfully complete the installation.

When creating a database, enter a complex password that adheres to the database hardening guides for all users.

The following Desktop applications are required for proper operation of the system:

- Fleet Management Data Viewer
- Fleet Management Itinerary Tracker
- Shipboard Property Management System (SPMS) Configurator
- Report Sequencer
- Workflow

The following Web applications/Web services are required for proper operation of the system:

- Emergency Response System (Mobile App)
- Gangway (Web App)
- Event (Web App)
- Universal Check-In (Web App)
- Content Manager (Web App)
- OHCFMSDWS (Web Service)
- OHCITINDWS (Web Service)
- OHCUCIDWS (Web Service)

- OHCCAMDWS (Web Service)
- OHCSHAREDDWS (Web Service)
- OHCEVENTDWS (Web Service)

The following Interfaces are required for proper operation of the system:

- Fleet Management Sender
- Fleet Management Receiver
- Corporate Data Transfer Interface (CDTI)
- Fleet Management Encryption Manager

The following add-ons are installed if required:

- ResOnline
- Corporate Access Module
- Event
- Universal Check-In

Post-Installation Configuration

This section explains additional security configuration steps to complete after Fleet Management is installed.

Operating System

Turn On Data Execution Prevention (DEP)

Turn on DEP if required. Refer to the Microsoft product documentation library at https://technet.microsoft.com/en-us/ for instructions.

Turning Off Auto Play

Turn off Auto play if required. Refer to the Microsoft product documentation library at https://technet.microsoft.com/en-us/ for instructions.

Turning Off Remote Assistance

Turn off Remote Assistance if required. Refer to the Microsoft product documentation library at https://technet.microsoft.com/en-us/ for instructions.

Application

Software Patches

If available, apply the latest Fleet Management patches available on My Oracle Support. Follow the deployment instructions included with the patch.

Security Certificates

Secure Sockets Layer (SSL) certificate must be configured if required either on load balancer or in Internet Information Server (IIS) web server for communication to web services.

Secure Sockets Layer (SSL) usage on Fleet Management Security Server is mandatory. Self-signed certificate should be used only if customer fails to provide one. Refer to the *Oracle Hospitality Cruise Fleet Management Installation Guide* for information about the installation of secure certificates.

Passwords Overview

The configuration of Fleet Management product passwords is performed in the Fleet Management Administration module. Administrators should configure a strong password policy after initial installation of the application and review the policy periodically.

Maintaining Strong Passwords

Ensure that passwords adhere to the following strength requirements:
1. The password must be at least 8 characters long.
2. The password must contain letters and numbers.
3. Must not choose a password equal to the last 3 passwords used.

Change Default Passwords

Fleet Management is installed with a default administrative user and password. Change the default administrative user password in the Fleet Management, following the above guidelines, after logging in for the first time.

Configure User Accounts and Privileges

When setting up users of the Fleet Management application, ensure that they are assigned the minimum privilege level required to perform their job function.

Encryption Keys

Fleet Management maintains separate encryption key for each database user in a table of FidelioBK database user and stores them encrypted using Key Encryption Key (KEK). Each Fleet Management client need to connect FidelioBK DB user to fetch passwords and encryption keys for other database users.

Implementing Fleet Management Security

This chapter reviews Fleet Management security features.

Authorization Privileges

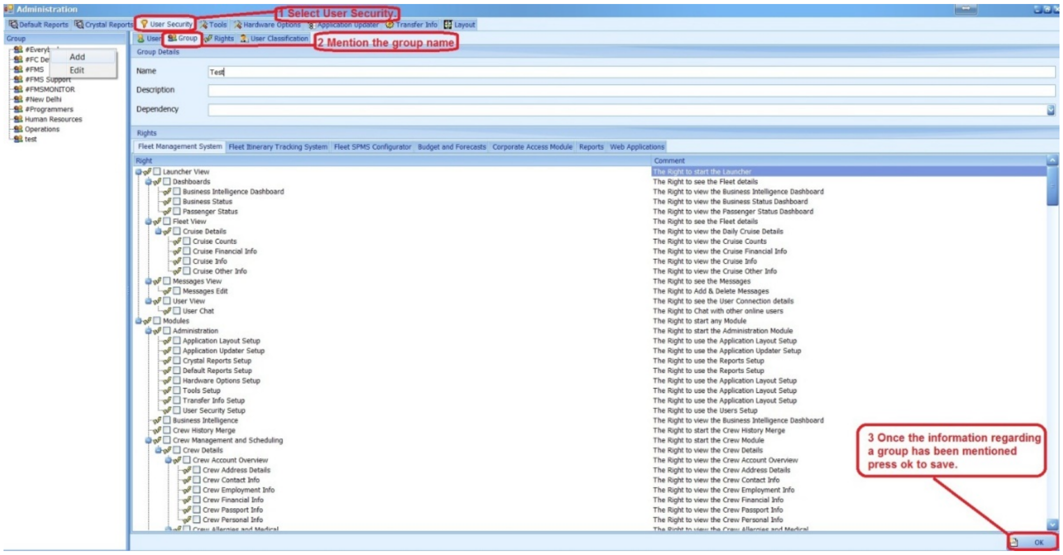
Overview

Setting Authorization privileges establishes strict access control, explicitly enabling or restricting the ability to do something with a computer resource.

User authorization privileges are configured in Fleet Management within the Fleet Management Administration module. Fleet Management uses simple authorization model, where each user belongs to one more user groups, and the user gets all the privileges assigned to the user group(s). Alternatively, Fleet Management can use Active Directory as an alternative for authentication/authorization. In the Active Directory mode, the Microsoft Windows user is used to login into the Fleet Management.

Adding a User Group

1. Select the **Group** tab under **User Security**, and then right-click on the left vertical pane
2. Select **Add** and enter the group name, description, and dependency.
3. Select the checkboxes for the desired user rights, and then click **OK**. The administrator can select various modules (for example, Fleet Management is shown in the figure below) that should have access to the new group.



1 Select User Security.

2 Mention the group name

Name: Test

Description:

Dependency:

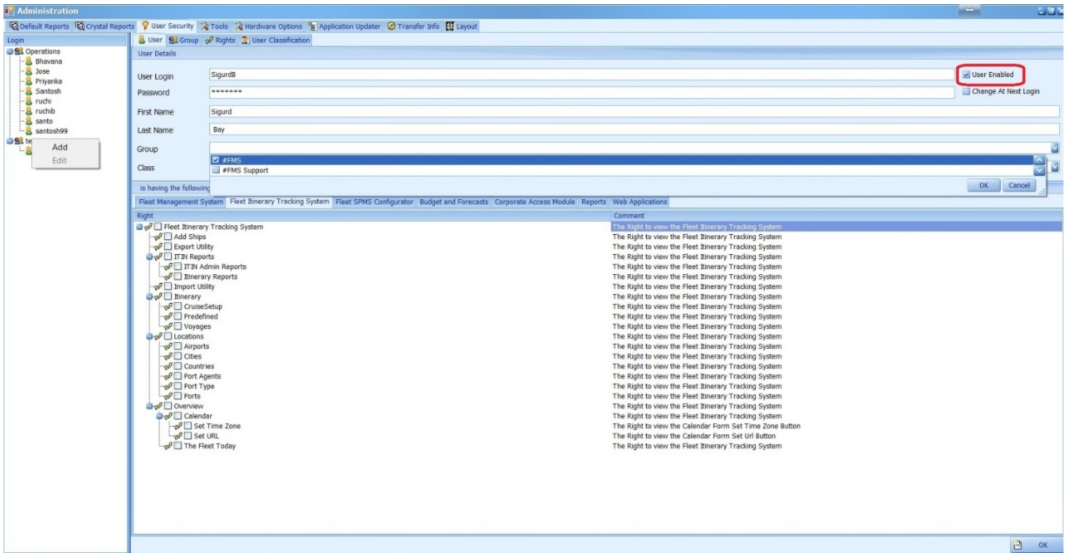
Right	Comment
□ Launcher View	The Right to start the Launcher
□ Dashboards	The Right to see the Fleet details
□ Business Intelligence Dashboard	The Right to view the Business Intelligence Dashboard
□ Business Status	The Right to view the Business Status Dashboard
□ Passenger Status	The Right to view the Passenger Status Dashboard
□ Fleet View	The Right to see the Fleet details
□ Cruise Details	The Right to view the Daily Cruise Details
□ Cruise Counts	The Right to view the Cruise Counts
□ Cruise Financial Info	The Right to view the Cruise Financial Info
□ Cruise Info	The Right to view the Cruise Info
□ Cruise Other Info	The Right to view the Cruise Other Info
□ Messages View	The Right to see the Messages
□ Messages Edit	The Right to Add & Delete Messages
□ User View	The Right to see the User Connection details
□ User Chat	The Right to Chat with other online users
□ Modules	The Right to start any Module
□ Administration	The Right to start the Administration Module
□ Application Layout Setup	The Right to use the Application Layout Setup
□ Application Updater Setup	The Right to use the Application Updater Setup
□ Crystal Reports Setup	The Right to use the Reports Setup
□ Default Reports Setup	The Right to use the Reports Setup
□ Hardware Options Setup	The Right to use the Application Layout Setup
□ Tools Setup	The Right to use the Application Layout Setup
□ Transfer Info Setup	The Right to use the Application Layout Setup
□ User Security Setup	The Right to use the Users Setup
□ Business Intelligence	The Right to view the Business Intelligence Dashboard
□ Crew History Merge	The Right to start the Crew History Merge
□ Crew Management and Scheduling	The Right to start the Crew Module
□ Crew Details	The Right to view the Crew Details
□ Crew Account Overview	The Right to view the Crew Account Overview
□ Crew Address Details	The Right to view the Crew Address Details
□ Crew Contact Info	The Right to view the Crew Contact Info
□ Crew Employment Info	The Right to view the Crew Employment Info
□ Crew Financial Info	The Right to view the Crew Financial Info
□ Crew Passport Info	The Right to view the Crew Passport Info
□ Crew Personal Info	The Right to view the Crew Personal Info
□ Crew Allergies and Medical	The Right to view the Crew Allergies and Medical

3 Once the information regarding a group has been mentioned press ok to save.

Figure **4 - Saving Group Information**

Adding a User

1. Select the **User** tab under **User Security**, and then right-click on the group name in the left pane.
2. Select **Add** and enter the user login, password, first name and last name.
3. Select the drop-down menu of the group section and click **OK**.



User Login: SigurdB

Password: *******

☑ User Enabled

□ Change At Next Login

First Name: Sigurd

Last Name: Bay

Group:

☑ #FMS

□ #FMS Support

Class:

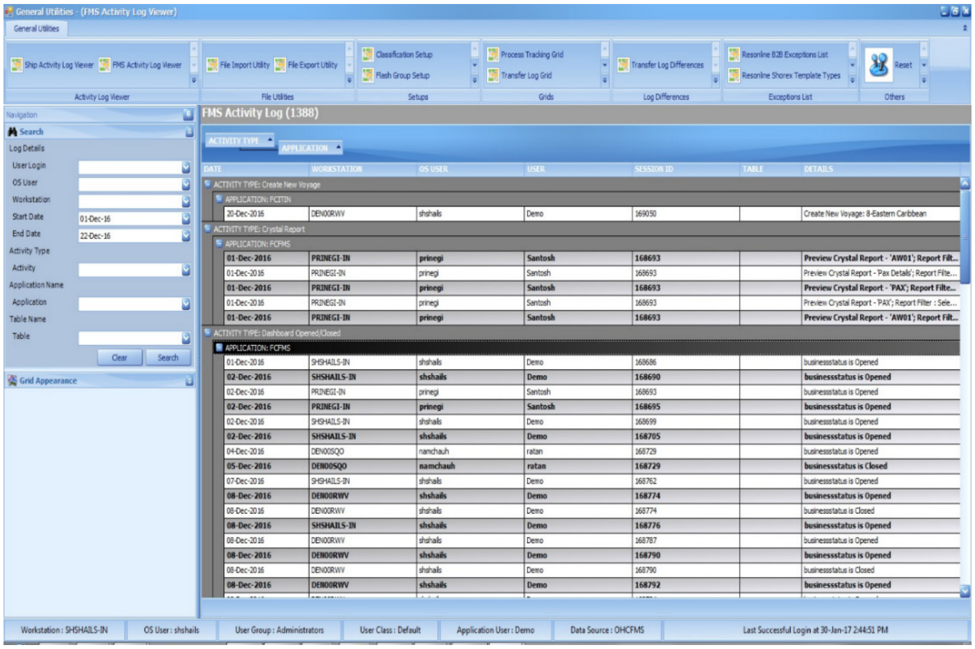
Right	Comment
□ Fleet Itinerary Tracking System	The Right to view the Fleet Itinerary Tracking System
□ Add Ships	The Right to view the Fleet Itinerary Tracking System
□ Export Utility	The Right to view the Fleet Itinerary Tracking System
□ ITIN Reports	The Right to view the Fleet Itinerary Tracking System
□ ITIN Admin Reports	The Right to view the Fleet Itinerary Tracking System
□ Itinerary Reports	The Right to view the Fleet Itinerary Tracking System
□ Import Utility	The Right to view the Fleet Itinerary Tracking System
□ Itinerary	The Right to view the Fleet Itinerary Tracking System
□ CruiseSetup	The Right to view the Fleet Itinerary Tracking System
□ Predefined	The Right to view the Fleet Itinerary Tracking System
□ Voyages	The Right to view the Fleet Itinerary Tracking System
□ Locations	The Right to view the Fleet Itinerary Tracking System
□ Airports	The Right to view the Fleet Itinerary Tracking System
□ Cities	The Right to view the Fleet Itinerary Tracking System
□ Countries	The Right to view the Fleet Itinerary Tracking System
□ Port Agents	The Right to view the Fleet Itinerary Tracking System
□ Port Type	The Right to view the Fleet Itinerary Tracking System
□ Ports	The Right to view the Fleet Itinerary Tracking System
□ Overview	The Right to view the Fleet Itinerary Tracking System
□ Calendar	The Right to view the Fleet Itinerary Tracking System
□ Set Time Zone	The Right to view the Calendar Form Set Time Zone Button
□ Set URL	The Right to view the Calendar Form Set Url Button
□ The Fleet Today	The Right to view the Fleet Itinerary Tracking System

Figure 5 - Adding a User

NOTE: The user can be enabled/disabled by using the User Enabled check box shown in the figure.

Audit Trail/Application Activity Log

Fleet Management logs the important activities performed in the applications. The search panel lets you select different criteria like user, operating system user, workstation, date range, and activity type, application, and table. The main grid shows the activity with required details.



Log Details

User Login:

OS User:

Workstation:

Start Date: 01-Dec-16

End Date: 22-Dec-16

Activity Type

Activity:

Application Name

Application:

Table Name

Table:

FMS Activity Log (1388)

DATE	WORKSTATION	OS USER	USER	SESSION ID	TABLE	DETAILS
ACTIVITY TYPE: Create New Voyage						
APPLICATION: FCITIN						
20-Dec-2016	DEN00RWV	shshails	Demo	169050		Create New Voyage: 8-Eastern Caribbean
ACTIVITY TYPE: Crystal Report						
APPLICATION: FCFMS						
01-Dec-2016	PRINEGI-IN	prinegi	Santosh	168693		Preview Crystal Report - 'AW01'; Report Filt...
01-Dec-2016	PRINEGI-IN	prinegi	Santosh	168693		Preview Crystal Report - 'Pax Details'; Report Filte...
01-Dec-2016	PRINEGI-IN	prinegi	Santosh	168693		Preview Crystal Report - 'PAX'; Report Filte...
01-Dec-2016	PRINEGI-IN	prinegi	Santosh	168693		Preview Crystal Report - 'PAX'; Report Filter : Sele...
01-Dec-2016	PRINEGI-IN	prinegi	Santosh	168693		Preview Crystal Report - 'AW01'; Report Filt...
ACTIVITY TYPE: Dashboard Opened/Closed						
APPLICATION: FCFMS						
01-Dec-2016	SHSHAILS-IN	shshails	Demo	168686		businessstatus is Opened
02-Dec-2016	SHSHAILS-IN	shshails	Demo	168690		businessstatus is Opened
02-Dec-2016	PRINEGI-IN	prinegi	Santosh	168693		businessstatus is Opened
02-Dec-2016	PRINEGI-IN	prinegi	Santosh	168695		businessstatus is Opened
02-Dec-2016	SHSHAILS-IN	shshails	Demo	168699		businessstatus is Opened
02-Dec-2016	SHSHAILS-IN	shshails	Demo	168705		businessstatus is Opened
04-Dec-2016	DEN00SQO	namchauh	ratan	168729		businessstatus is Opened
05-Dec-2016	DEN00SQO	namchauh	ratan	168729		businessstatus is Closed
07-Dec-2016	SHSHAILS-IN	shshails	Demo	168762		businessstatus is Opened
08-Dec-2016	DEN00RWV	shshails	Demo	168774		businessstatus is Opened
08-Dec-2016	DEN00RWV	shshails	Demo	168774		businessstatus is Closed
08-Dec-2016	SHSHAILS-IN	shshails	Demo	168776		businessstatus is Opened
08-Dec-2016	DEN00RWV	shshails	Demo	168787		businessstatus is Opened
08-Dec-2016	DEN00RWV	shshails	Demo	168790		businessstatus is Opened
08-Dec-2016	DEN00RWV	shshails	Demo	168790		businessstatus is Closed
08-Dec-2016	DEN00RWV	shshails	Demo	168792		businessstatus is Opened

Workstation : SHSHAILS-IN | OS User : shshails | User Group : Administrators | User Class : Default | Application User : Demo | Data Source : OHCFMS | Last Successful Login at 30-Jan-17 2:44:51 PM

Figure 6 - Activity Log

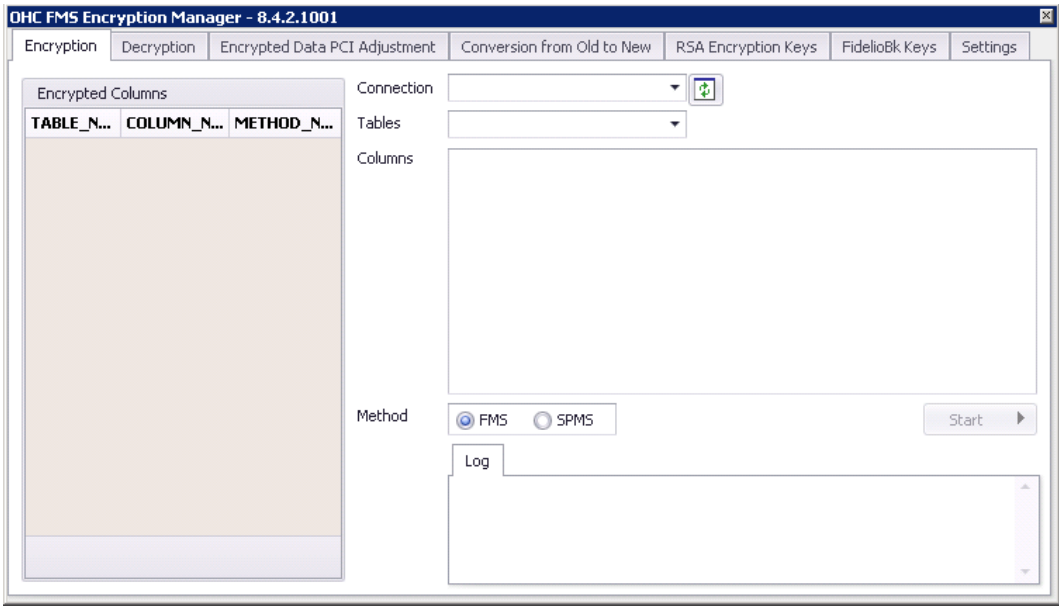
Fleet Management Encryption Manager

Fleet Management Encryption manager is a tool to encrypt and store sensitive information. The customer can choose sensitive data to encrypt and store. Encryption Manager Uses Microsoft managed Rijndael encryption algorithm to encrypt the data. It is Symmetric Encryption, single encryption key is used for both encryption and decryption. Encryption keys are stored securely in the FidelioBK DB user. Encryption manager need to connect to the FidelioBK user on startup to grab the encryption keys.

Fleet Management customers are instructed not to transfer and store credit card data. If they do so, they fall under Payment Application Data Security Standard (PA-DSS) scope and need to get certified on their own.

Encryption

To encrypt selected tables/columns, go to the Encryption tab. The Encryption tab shows a list of tables/columns encrypted on the left, options to select a database user, and tables and columns on the right.

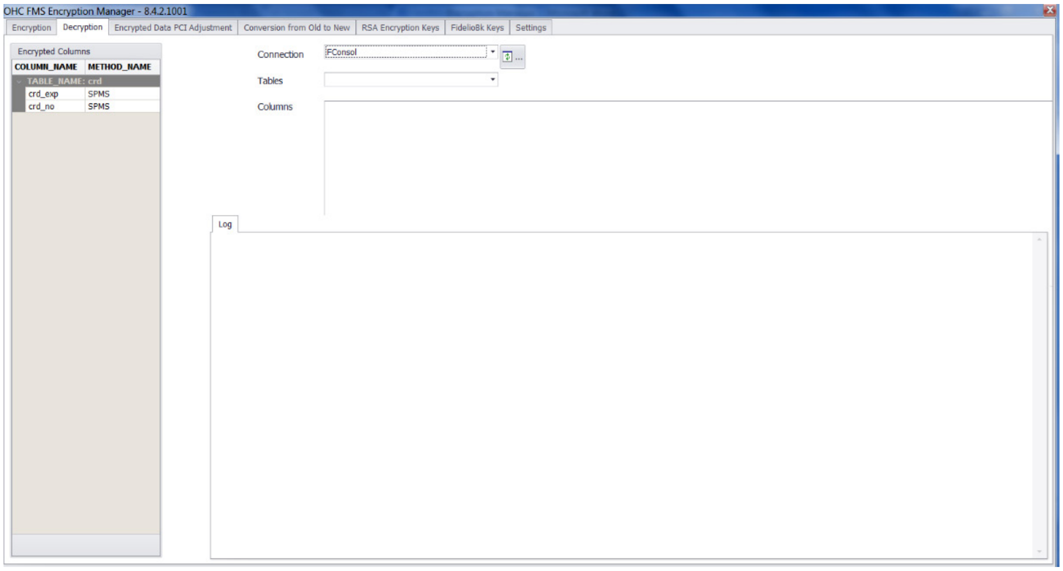


Method: ● FMS ○ SPMS

Figure 7 - Encryption Tab

Decryption

Fleet Management Encryption Manager also decrypts the data encrypted using the Encryption Manager. To decrypt any encrypted tables/columns, go to the Decryption tab as shown below. The Encryption Tab shows a list of tables/columns encrypted on the left, options to select database user, tables and columns to decrypt.


OHC FMS Encryption Manager - 8.4.2.1001
Encryption
Decryption
Encrypted Data PCI Adjustment
Conversion from Old to New
RSA Encryption Keys
FidelioBk Keys
Settings
Encrypted Columns
Tables
Columns
Log

COLUMN_NAME	METHOD_NAME
TABLE_NAME: crd	
crd_exp	SPMS
crd_no	SPMS

Connection: FConsol

Figure 8 - Decryption Tab

Encryption Manager is a batch tool, it reads a batch at a time and encrypts/decrypts.
A log is generated in both encryption/decryption to indicate the progress. We can also configure it to generate debug log. The debug log is more detailed log and is helpful in troubleshooting.

Appendix A Fleet Management Ports Number

This is a list of port numbers that are used in Fleet Management. Open a port only if required.

Table 1 - Service/Protocol/Port Number Table

Service	Protocol	Port Number
Web Services	HTTP(S)	80/8080(SSL)
MSMQ	TCP	1801
MSMQ	UDP	3257, 1801
E-Mail	SMTP	25
E-Mail	POP3	110/995(SSL)
E-Mail	IMAP	143/993(SSL)

Refer to the below links for more information on Microsoft Message Queuing (MSMQ):

- Ports used in MSMQ
- How to configure a Firewall for MSMQ access