Oracle® Hospitality Cruise Fleet Management

Security Guide

Release 9.2
F81086-01
August 2023

ORACLE

Oracle Hospitality Cruise Fleet Management Security Guide, Release 9.2

F81086-01

Contents

Preface

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

Audience

This document is intended for the end users and System Administrator installing the Fleet Management software

Customer Support

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

https://iccp.custhelp.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
- Screen shots of each step you take

Documentation

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

Revision History

Date	Description of Change
August 2023	Initial publication.

1

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 applies.
- **Limit privileges as much as possible.** Users should only be given the necessary access 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

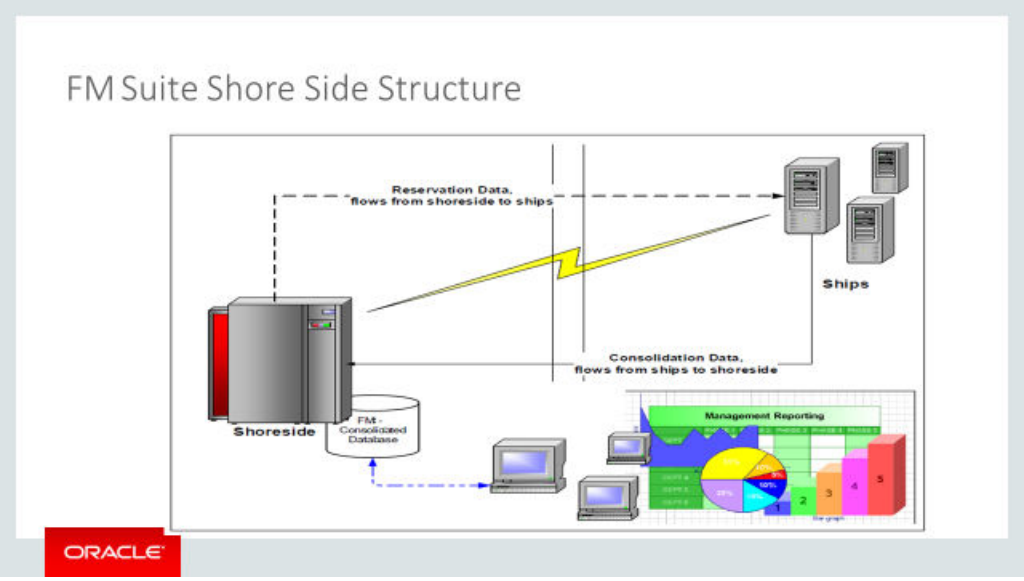
Fleet Management uses a Client-Server Architecture (partially 3-tier architecture) and is a collection of desktop applications, Interfaces, web apps/web services. Most of the application pieces are thick clients that can be deployed anywhere and few are thin clients with business layers in the form of web services, few are stand-alone applications/interfaces used for internal processing/integration. It is scalable and does not have to be deployed on a single machine.

Technology

Fleet Management Client-Server Architecture (partially 3-tier architecture) uses industry standards Simple Object Access Protocol (SOAP) web services to work with internal and

external applications. SOAP-based web services are deployed and exposed on Microsoft Internet Information Services (IIS) web server, and IIS provides options to secure the communication using Secure Sockets Layer (SSL). It also uses Microsoft Message Queuing (MSMQ) in Work Group mode and also with Active Directory Integration (secure mode), Transmission Control Protocol/Internet Protocol (TCP/IP), File System for data transfer/third-party integration. Most of the communication can be configured to use Secure Sockets Layer (SSL) and, Oracle Wallets is used to secure communication between the client and the Oracle Database. It also uses recommended encryption/hashing algorithms such as Microsoft managed Rijndael, Microsoft Windows Data Protection Application Programming Interface (DPAPI), SHA256, Password-Based Key Derivation Function 2 (PBKDF2) to encrypt and store sensitive customer information, application user passwords, application configuration information, secrets, and passwords. At the database level, it also uses Transparent Data Encryption (TDE) to protect the data at rest

Figure 1-1 Fleet Management Architecture



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 username and complex password to each user. Password must follow Payment Card Industry-Data Security Standard (PCI-DSS) guidelines, and must be at least 8 characters long and includes letters and numbers.

An alternative authentication method for 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 a two-level approach for 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 validation request, 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, 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 an encrypted form. Clients connect to the FIDELIOBK user to obtain 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 once to fetch the FIDELIOBK user password and KEK, and store them locally in its configuration file in an encrypted form using Microsoft Windows Data Protection Application Programming Interface (DPAPI) method. In the event where the FIDELIOBK user password has changed, the application then fetches the updated password from the Security Server before updating the Clients password 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?**

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, 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.

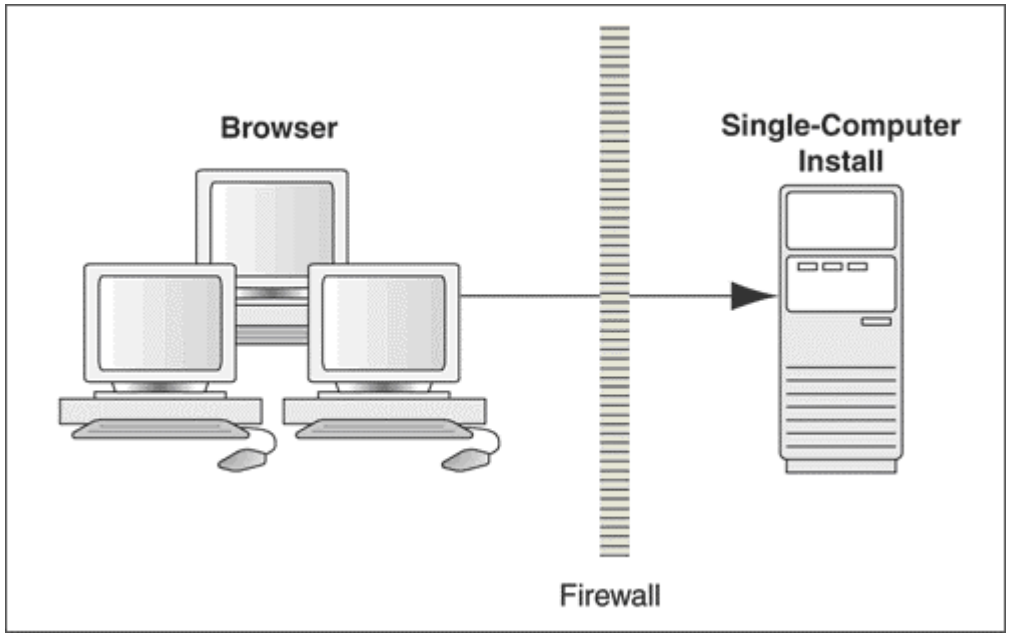
Recommended Deployment Configurations

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 1-2

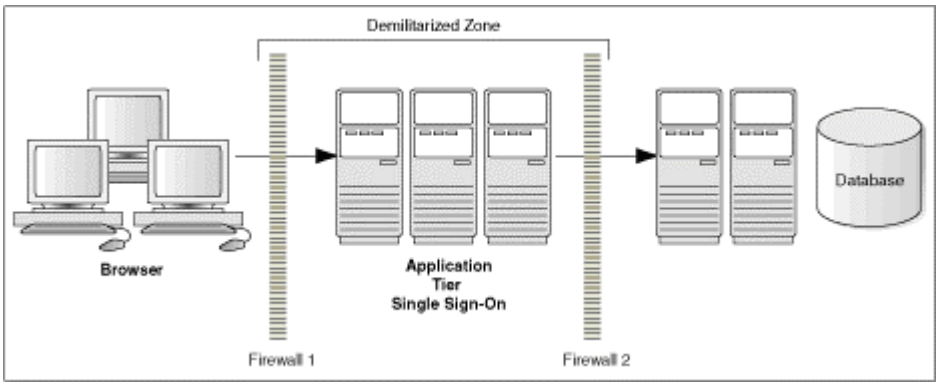
This single-computer deployment may be cost effective for small organizations, however, it cannot provide high availability because all components are stored on the same computer. In a single server environment such as the typical installation, the server should be protected behind a firewall.

Figure 1-2 Single Computer Deployment



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

Figure 1-3 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 Port Numbers for more information about Fleet Management network port usage.

Component Security

Operating System Security

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

See below Microsoft TechNet articles for more information about operating system security:

- Windows Server 2016 Security
- Windows Server 2019 Security

Oracle Database Security

See Oracle Database Security Guide for more information about Oracle Database security requirements.

2

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

Before installing the 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*, available at Oracle Help Center
- Acquire Secure Sockets Layer (SSL) compliant security certificate from Certification Authority and you can apply it while running the FMS Web Applications Enablement scripts.
- Install Fleet Management Security Server and Configure. See the *Oracle Hospitality Cruise Fleet Management Security Server section in the 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 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:

- OHCFMS (Data Viewer)
- Fleet Management Security Server (on Web Server)

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

- Emergency Response System (Mobile App)
- Gangway Activity
- OHCFMSDWS (Web Service)
- Security Server Gateway (Web Service)

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

- Fleet Management Sender
- Fleet Management Receiver
- Corporate Data Transfer Interface (CDTI)
- Watchdog
- Report Auto Sequencer

The following add-ons are installed if required:

- Reservation Online
- Corporate Access Module
- Fleet Management Encryption Manager
- Database Password Schema Manager

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. A Self-signed certificate should only be used if the customer fails to

provide one. See the *Oracle Hospitality Cruise Fleet Management Installation Guide* for information about secure certificates installation.

Password Overview

The configuration of Fleet Management product passwords is performed in the Fleet Management Administration module. Administrators should configure a strong password policy after the initial installation of the application and review the policy periodically. Password verification functions are used to ensure that user password meets the minimum requirements for complexity. Check and ensure the PASSWORD_VERIFY_FUNCTION parameter for the user profile created in the Database is not NULL.

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 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.

Password Lifetime

Password expiration is used to ensure that users change their passwords on a regular basis. It also provides a mechanism to automatically disable temporary accounts. Set the PASSWORD_LIFE_TIME parameter for the user profile in the Database.

Configure User Accounts and Privileges

When setting up users for the Fleet Management application, ensure that they are assigned the minimum privilege level required to perform their job function. Set INACTIVE_ACCOUNT_TIME in the profiles assigned to users to automatically lock accounts that have not logged in to the database instance for a specified number of days. It is also recommended to audit infrequently used accounts for unauthorized activities.

Concurrent Sessions and Constraints

The database user by default has unlimited concurrent connections and this may result in memory resource exhaustion or Denial-of-Service attacks. It is advisable to set the SESSIONS_PER_USER for this. We recommend that you check for disabled constraints, and determine where applicable if they need to be disabled, deleted, or enabled as these are a potential cause for concern.

Encryption Keys

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

Microsoft Message Queuing (MSMQ)

For better security, use MSMQ with Active Directory integration. The enabled MSMQ not only encrypt messages transferred between FMS Sender and FMS Receiver, but also to check the authentication if they are coming from a trusted source. MSMQ uses internal certificates stored in Active Directory Domain Controller for encryption and authentication purposes. Internal Certificates can be rotated as required through MSMQ console. Please note MSMQ integration with Active Directory is possible on the client machines where FMS Sender and FMS Receiver are installed, and only if they are logged in using a domain user with the required privileges and public queues are used for the transport of the messages.

3
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 the Fleet Management Administration module. Fleet Management uses a simple authorization model, where each user belongs to one more user group, and the user gets all the privileges assigned to the user group(s). Alternatively, you can use the Active Directory for authentication/authorization. In the Active Directory mode, the Microsoft Windows user is used to login into Fleet Management

Adding a User Group

1. Select the **Group** tab under **User Security**.
2. At the Group tree view pane, select **Add** and enter the group name, description and dependency.
3. Select the check boxes for the desired user rights, and then click **OK**. The Administrator can select various modules a user should have access in the new group as shown in below example.

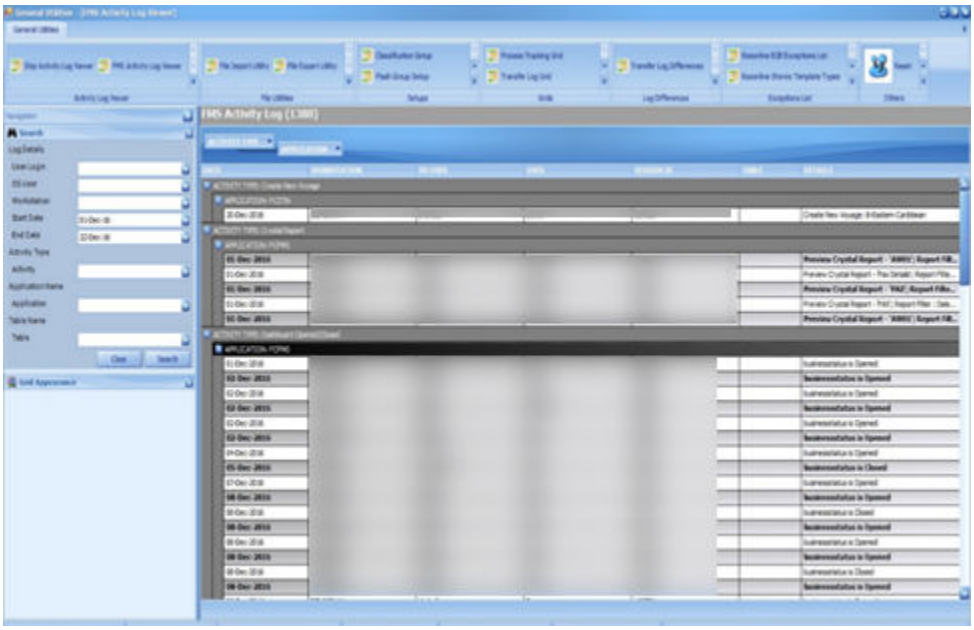
Adding a User

1. Select the **User** tab under **User Security**.
2. At the Group tree view pane, 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**

> **Note:**
>
> You have the option to an enable/disable a user using the **User Enabled** check box shown in the above figure.

Audit Trail / Application Activity Log

Figure 3-1 Activity Log window



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, activity type, application, and table. The main grid shows the activity and the required details.

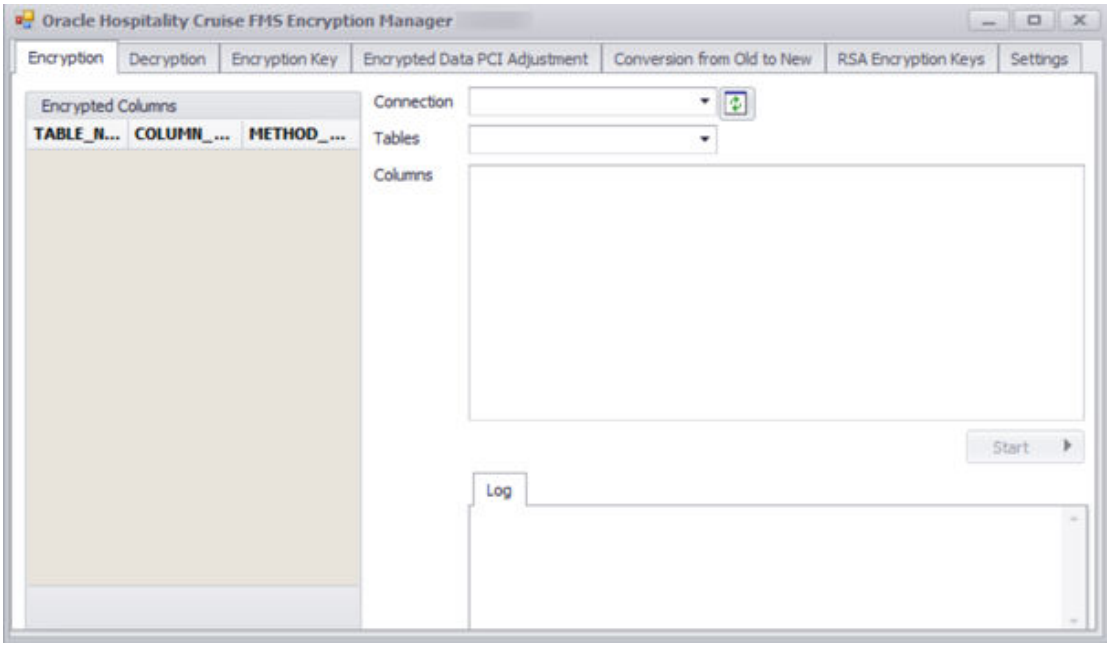
Fleet Management Encryption Manager

Fleet Management Encryption Manager is a tool that encrypts and stores sensitive information in which the customer can choose the type of sensitive data to encrypt and store. The Encryption Manager uses Microsoft-managed Rijndael encryption algorithm to encrypt the data. It is Symmetric Encryption using a single encryption key for both encryption and decryption. The encryption keys are stored securely in the FidelioBK DB user, and you need to connect to the FidelioBK user on startup to obtain the encryption keys.

Fleet Management customers are instructed not to transfer and store any credit card data. If customers choose to do so, this is then categorized under the Payment Application Data Security Standard (PA-DSS) scope and customers need to get themselves certified on their own.

Encryption

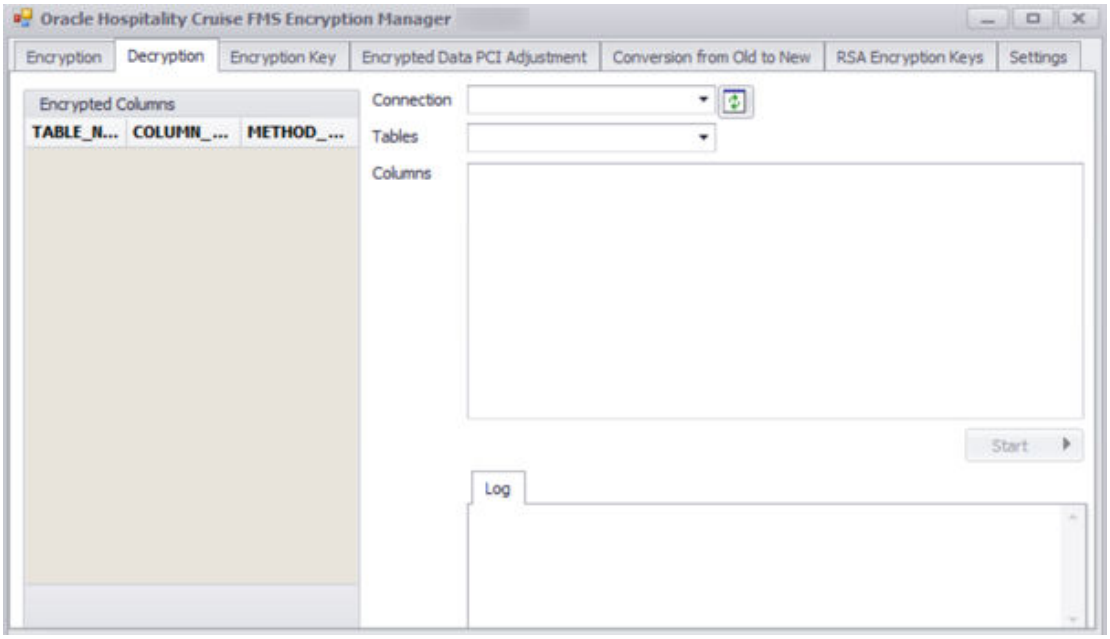
Figure 3-2 Encryption Tab



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

Decryption

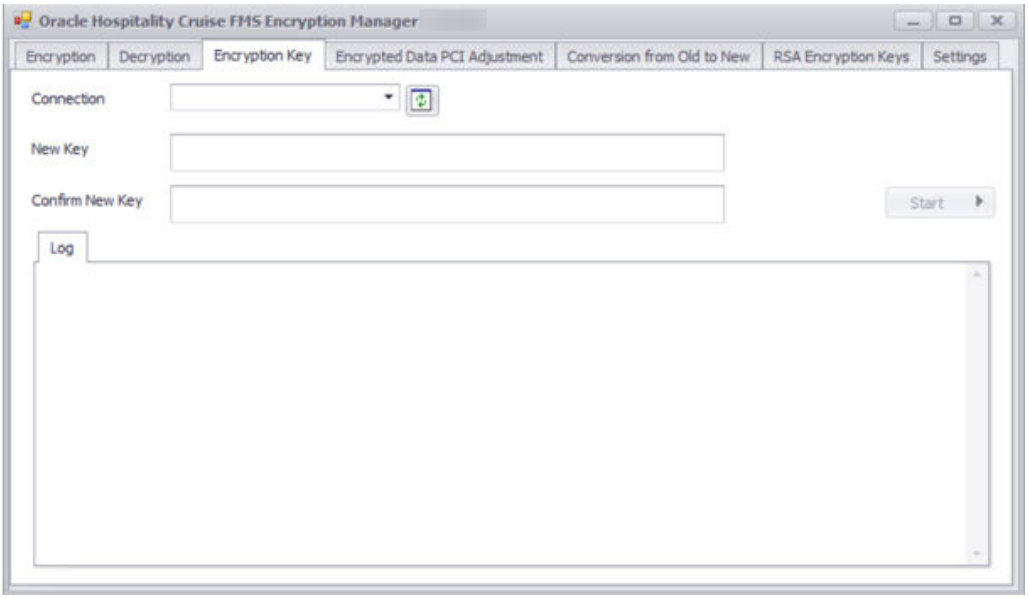
Figure 3-3 Decryption Tab



To decrypt any encrypted tables/columns, go to the Decryption tab. The Encryption tab shows a list of tables/columns encrypted on the left, options to select **Connection**, **Tables** and **Columns** to decrypt.

Encryption Key

Figure 3-4 Encryption Key Tab



Fleet Management Encryption Manager also rotates the data encryption key using the Encryption Manager. To rotate with a new key, go to the Encryption Key tab. In the Encryption Key Tab select a **Connection,** enter a **New Key** and click **Start**.

Encryption Manager is a batch tool that reads one batch a time and encrypts/decrypts the data. A log is generated in both encryption/decryptions to indicate the progress. It can also be configured to generate a debug log which contain more details for troubleshooting.

4

Appendix A – Fleet Management Port Numbers

Table 4-1 Services Protocol and Port Numbers

Services	Protocol	Port Number
Web Services	HTTP	80/8080
Web Services	HTTPS	443
MSMQ	TCP	1801
MSMQ	UDP	3257, 1801
E-Mail	SMTP	25
E-Mail	POP3	110/995(SSL)
E-Mail	IMAP	143/993(SSL)

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

- Ports used in MSMQ
- Security Considerations for Message Queuing

5

Appendix B – Secure Deployment Checklist

The following security checklist is included to guide you on how to secure your database:

- Install only what is required.
- Lock and expire default user accounts.
- Enforce password management.
- Enable data dictionary protection.
- Practice the principle of least privilege.
- Grant necessary privileges only.
- Revoke unnecessary privileges from the PUBLIC user group.
- Restrict permissions on run-time facilities.
- Enforce access controls effectively and authenticate clients stringently.
- Restrict network access.
- Apply all security patches and workarounds.
- Use a firewall.
- Never poke a hole through a firewall.
- Protect the Oracle listener.
- Monitor listener activity.
- Monitor who accesses your systems.
- Check network IP addresses.
- Encrypt network traffic.
- Harden the operating system.