Oracle Financial Services Liquidity Risk Management

Security Guide

Release 8.1.x

Apr 2021

ORACLE
Financial Services

OFS Liquidity Risk Management Security Guide

For information on third party licenses, see the *OFSAA Licensing Information User Manual*.

Document Control

Version Number	Revision Date	Change Log
1.0	June-2020	This document captures the necessary security-related configurations for OFS Liquidity Risk Management.

Table of Contents

1 Preface

Oracle Financial Services Liquidity Risk Solution pack (developed on Oracle Financial Services Analytical Applications Infrastructure) provides for configuration of security parameters and this guide provides information about the configurations required and how to set it. You can find the latest copy of this document in the *OHC Documentation Library* which includes all the recent additions/revisions (if any) done to date.

The information contained in this document is intended to give you a quick exposure and an understanding of the security configurations required after the installation of Oracle Financial Services Liquidity Risk Solution - Liquidity Risk Management, which includes the following SKUs:

- *OFS Liquidity Risk Measurement and Management*
- *OFS Liquidity Risk Regulatory Calculations for Reserve Bank of India*
- *OFS Liquidity Risk Regulatory Calculations for US Federal Reserve*
- *OFS Liquidity Risk Regulatory Calculations for European Banking Authority*
- *OFS Liquidity Risk Regulatory Calculations for Bank of Thailand*
- *OFS Liquidity Risk Regulatory Calculations for Bank Negara Malaysia*
- *OFS Liquidity Risk Regulatory Calculations for Monetary Authority of Singapore*
- *OFS Liquidity Risk Regulatory Calculations for Hong Kong Monetary Authority*

Topics:

- *Intended Audience*
- *Prerequisites*
- *Related Information Sources*

1.1 Audience

This guide is intended for System Administrators (SA) who are instrumental in installing and performing secure configurations for Liquidity Risk Solution Pack-Liquidity Coverage Ratio SKUs. It is assumed that the SAs are technically sound and proficient in UNIX, Database Administration, and Web Application Administration to install and configure OFSAAI in the released environment.

1.1.1 Prerequisites for the Audience

This document assumes that you have experience installing Enterprise components and basic knowledge about the following:

- Oracle Financial Services Liquidity Risk Solution Pack components
- Oracle Financial Services Analytical Applications Infrastructure components
- OFSAA Architecture
- UNIX Commands
- Database Concepts

- Web server/web application server

1.2 Related Documents

The list of related documents is provided here.

- *OFS Liquidity Risk Solution Application Pack Installation and Configuration Guide 8.1.0.0.0 Release*
- *OFSAAI Security Guide*
- *Oracle Financial Services Advanced Analytical Applications Infrastructure Application Pack Installation and Configuration Guide*

2 Install the OFS Liquidity Risk Solution Application Pack

For detailed installation steps, see the *OFS Liquidity Risk Solution Application Pack Installation and Configuration Guide Release 8.1.0.0.0*.

3 Set Secure Configurations

The OFS LRS application pack components are developed on the OFSAA infrastructure and uses the OFSAAI secure configurations.

See the following sections to configure the security parameters in OFSAAI.

3.1 Security Configurations

Configure a set of security parameters to have a secure environment for the OFSAA installation. The required configurations are presented in the following list. For more details on the configurations, see the *OFSAAI Administration Guide* and the *OFSAAI Security Guide 8.1.x*.

- **Input and Output Encoding**: LRS is enabled with input validation and output encoding to protect from various types of security attacks.
- **CSRF Enabled**: This option results in setting the CSRF tokens in requests. OFSAAI System Configuration UI provides the option to enable or disable CSRF. For more information on enabling CSRF, see the Update General Details section in the *OFSAAI User Guide*.
- **Oracle Data Redaction**: This is an Oracle Database Advanced Security option to enable data protection. It is used to mask (redact) sensitive data shown to the user in real-time. To enable this option during installation, see the Enabling Data Redaction section in the *OFSAAI Installation and Configuration Guide*. To enable post-installation, see the Data Redaction section in the *OFSAAI Administration Guide*.
- **Transparent Data Encryption (TDE)**: Enable this option to secure the data at rest when stored in the Oracle database. To configure TDE during installation, see the *Transparent Data Encryption (TDE)* section in the *OFSAAI Installation and Configuration Guide*. If you want to configure after installation, see the *Transparent Data Encryption (TDE)* section in the *OFSAAI Administration Guide.*
- **Key Management**: The OFSAA configuration schema (CONFIG) is the repository to store passwords for users and application database schemas centrally. These values are AES-256 -bit encrypted using an encryption key uniquely generated for each OFSAA instance during the installation process. The OFSAA platform provides a utility (`EncryptC.sh`) to rotate/generate a new encryption key if needed.

  The Key Management section in the *OFSAAI Administration Guide* explains how to generate and store this key in a Java Key Store.

  NOTE Integration with any other Key management solution is out of the scope of this release.

- **File Encryption**: OFSAA supports file encryption using AES 256-bit format. For more information, see the *File Encryption* section in the *OFSAAI Administration Guide*.
- **Database Password Reset**: Change the database password for the Config schema and Atomic schema periodically. For more information, see the *Database Password Reset/ Change* section in the *OFSAAI Administration Guide*.
- **Password Reset**: Reset passwords for users, if required. For more information, see the *Database Password Reset/ Change* section in the *OFSAAI Administration Guide*.

- **Enable and Disable Users**: For more information, see the *Enable and Disable Users* section in the *OFSAAI Administration Guide*
- **SSO Authentication (SAML) Configuration**: For more information, see the *SSO Authentication (SAML) Configuration* section in the *OFSAAI Administration Guide*.
- **Public Key Authentication**: Configure the Public Key Authentication on UNIX. For more information, see the *Setting Up Public Key Authentication on Client Server* section in the *OFSAAI Administration Guide*.
- **Data Security and Data Privacy**: Configure to protect data against unauthorized access and data theft. For more information, see the *Data Security and Data Privacy* section in the *OFSAAI Administration Guide*.
- **Input and Output Encoding**: OFSAAI is enabled with input validation and output encoding to protect from various types of security attacks.
- **Password rotation every 30 days**: For more information, see the *Changing Password* section in the relevant version of the *OFSAAI User Guides*.
- **Additional Cross-Origin Resource Sharing (CORS)**: Configure CORS. For more information, see the *Knowing Additional Cross-Origin Resource Sharing (CORS)* section in the *OFSAAI Administration Guide*.
- **System Configuration and Identity Management**: Configure the following parameters from the information in the *System Configuration and Identity Management* section in the relevant version of the *OFSAAI User Guides*:
  - Set session timeout
  - Enable CSRF
  - Set frequency of password change
  - Configure password restriction details
  - Configure password history
  - Configure security questions for a password reset
  - Configure the activation period by setting Dormant Days, Inactive Days, and Working Hours

For detailed information about data security implemented in OFSDF, see the *Oracle Financial Services Data Foundation Data Protection Implementation Guide Release 8.1.x*.

4 Secure Header Configuration

Secure header configurations protect you from website attacks such as XSS. OFSAAI 8.1.0.0.0. is the platform used to build OFS LRS 8.1.0.0.0, and is packaged with the OFS LRS installer. OFSAAI supports the following configurations to protect from website attacks such as XSS.

- Configure for X-Frame-Options
- Configure CORS Header
- Set Content Security Policy
- Configure Referer Header Validation
- Configure HSTS in Response Header

See the *Secure Header Configurations* chapter in the *OFSAAI Security Guide 8.1.x*, for more information.

5 Web Application Server Security Configurations

OFSAAI 8.1.0.0.0. is the platform used to build OFS LRS 8.1.0.0.0, and is packaged with the OFS LRS installer. The OFSAAI framework defines the following security configurations for the web servers.

- Enable HTTPS Configuration for OFSAA
- Configure Security for Tomcat
- Configure Security for WebSphere
- Configure Security for WebLogic

Depending on your configured web application server, see the following sections in the chapter *Web Application Server Security Configurations* in the *OFSAAI Security Guide 8.1.x*, for more information.

6 Additional Security Configurations

OFSAAI 8.1.0.0.0. is the platform used to build OFS LRS 8.1.0.0.0, and is packaged with the OFS LRS installer. OFSAAI framework defines the following additional configurations for providing security to the applications.

- Configure to Restrict Access to Default Web Server Pages
- Configure to Restrict Display of the Web Server Details
- Configure to Restrict File Uploads
- Configure to restrict HTTP methods other than GET/POST
- Configure to enable unlimited cryptographic policy for Java

See the *Additional Security Configurations* section in the *OFSAAI Security Guide 8.1.x*, for more information.

7 Secure Database Connection Configurations

The Oracle database product supports SSL/TLS connections in its standard edition. The Secure Sockets Layer (SSL) protocol provides network-level authentication, data encryption, and data integrity. When a network connection over SSL is initiated, the client and server perform a handshake that includes:

- Negotiating a cipher suite for encryption, data integrity, and authentication
- Authenticating the client by validating its certificate
- Authenticating the server by verifying that its Distinguished Name (DN) is expected
- Client and server exchange key information using public key cryptography

See the *Secure Database Connection Configurations* section in the *OFSAAI Security Guide 8.1.x*, for more information.

8 Appendix A: Servlet Filter Configurations

Servlet Filter is a controller in the web-container with the Servlet Filter required configurations. This section also lists out the Keywords and Key Characters. It Includes:

- Security and Access
- Vulnerability Checks
- Cross-Site Scripting
- SQL Injection
- Configure Servlet Filter

See the *Appendix A - Servlet Filter Configurations* chapter in the *OFSAAI Security Guide 8.1.x*, for more information

OFSAA Support

Raise a Service Request (SR) in *My Oracle Support (MOS)* for queries related to the OFSAA applications.

Send Us Your Comments

Oracle welcomes your comments and suggestions on the quality and usefulness of this publication. Your input is an important part of the information used for revision.

- Did you find any errors?
- Is the information clearly presented?
- Do you need more information? If so, where?
- Are the examples correct? Do you need more examples?
- What features did you like most about this manual?

If you find any errors or have any other suggestions for improvement, indicate the title and part number of the documentation along with the chapter/section/page number (if available) and contact the Oracle Support.

Before sending us your comments, you might like to ensure that you have the latest version of the document wherein any of your concerns have already been addressed. You can access My Oracle Support site that has all the revised/recently released documents.