Oracle Financial Services Regulatory Reporting for US Federal Reserve - Lombard Risk Integration Pack

Security Guide

Release 8.1.0.0.0

February 2021

Oracle Financial Services Regulatory Reporting for US Federal Reserve - Lombard Risk Integration Pack (OFS REG REP USFED) Security Guide.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are “commercial computer software” pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

For information on third party licenses, click here.

Document Control

Version Number	Revision Date	Change Log
01	February 18, 2021	This document captures the necessary security-related configuration.

Table of Contents

1 Preface

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 Regulatory Reporting for US Federal Reserve – Lombard Risk Integration Pack (OFS REG REP USFED).

Topics:

- Audience
- Prerequisites
- Related Documents

1.1 Audience

This guide is intended for System Administrators (SA) who are instrumental in installing and performing secure configurations for Oracle Financial Services Regulatory Reporting for US Federal Reserve – Lombard Risk Integration Pack. It is assumed that the SAs are technically sound and proficient in UNIX, Database Administration, and Web Application Administration to install and configure OFSDF in the released environment.

1.1.1 Prerequisites for the Audience

The document assumes you have experience in installing Enterprise components. Basic knowledge about the Oracle Financial Services Data Foundation Application Pack components, OFSAA Architecture, UNIX commands, Database concepts, and web server or web application server is recommended.

1.2 Related Documents

The list of related documents is provided here.

- Oracle Financial Services Regulatory Reporting for US Federal Reserve – Lombard Risk Integration Pack (OFS REG REP USFED) Installation Guide Release 8.1.0.0.0
- Oracle Financial Services Data Foundation Installation and Configuration Guide Release 8.1.0.1.0
- Oracle Financial Services Data Foundation Application Pack Security Guide

2 Installing OFS REG REP USFED Application Pack

See the OFS Regulatory Reporting for US Federal Reserve – Lombard Risk Integration Pack (OFS REG REP USFED) Installation Guide Release 8.1.0.0.0, for detailed installation steps.

3 Set Secure Configuration

The OFS REG REP USFED 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 Configuration

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 information about the configuration, see the OFS AAI Administration Guide. and the OFSAA Security Guide

- **Input and Output Encoding**: OFS REG REP USFED is enabled with input validation and output encoding to protect from various types of security attacks.
- **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.
- **Oracle Data Redaction –** This is an Oracle Database Advanced Security option to enable the protection of data. It is used to mask (redact) sensitive data shown to the user in real-time. To enable this option during installation, see the section Enabling Data Redaction in the OFSAAI Installation and Configuration Guide. To enable post-installation, see the section Data Redaction in the OFS AAI Administration Guide.
- **CSRF Enabled** - Enabling this option results in setting CSRF tokens in requests. OFSAAI System Configuration UI provides the option to enable or disable CSRF. For more information on enabling CSRF, see the section Update General Details in the OFSAAI User 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 128 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 OFS AAI 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 section File Encryption in the OFS AAI Administration Guide.

NOTE	For detailed information about the data protection implementation in OFSAA, see OFS Data Foundation Application Pack Data Protection Implementation 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 OFS AAI Administration Guide.
- **Password Reset**: Reset passwords for users, if required. For more information, see the *Database Password Reset/ Change* section in the OFS AAI Administration Guide.
- **Enable and Disable Users**: For more information, see the *Enable and Disable Users* section in the OFS AAI Administration Guide
- **SSO Authentication (SAML) Configuration**: For more information, see the *SSO Authentication (SAML) Configuration* section in the OFS AAI 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 OFS AAI 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 OFS AAI 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 OFS AAI 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 OFS 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 REG REP USFED 8.1.0.0.0 and is packaged with the OFS REG REP USFED installer. OFSAAI supports the following configurations to protect from website attacks such as XSS:

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

Secure header configurations protect you from website attacks such as XSS and Clickjacking. See the *Secure Header Configurations* chapter in the OFSAA Security Guide for more information.

5 Web Application Server Security Configuration

OFSAAI 8.1.0.0.0 is the platform used to build OFS REG REP USFED 8.1.0.0.0 and is packaged with the OFS REG REP USFED 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 sections in the *Web Application Server Security Configurations* chapter in the OFSAA Security Guide for more information.

6 Additional Security Configuration

OFSAAI 8.1.0.0.0 is the platform used to build OFS REG REP USFED 8.1.0.0.0 and is packaged with the OFS REG REP USFED 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 or POST
- Configure to Enable Unlimited Cryptographic Policy for Java

See the *Additional Security Configurations* section in the OFSAA Security Guide for more information.

7 Secure Database Connection Configuration

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* OFSAA Security Guide, for more information.

8 Appendix A: Servlet Filter Configuration

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 as follows:

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

See the *Appendix A - Servlet Filter Configurations* in the OFSAA Security Guide, for more information.

9 Using X-Frame-Options to Embed Drill-down in the Lombard Report

By default, the OFSAA configuration refrains to embed the OFSAA content in the Lombard portal, therefore, the `web.xml` file must be modified to enable the same.

> **NOTE** The preceding step is mandatory to access the OFSAA drill-down from the Lombard AgileREPORTER portal.

To embed the drill-down content in the Lombard portal, change the default OFSAA setting of X-Frame-Options from **SAMEORIGIN** to **ALLOW-FROM** in the `web.xml` file.

9.1 Modifying the web.xml File

This section describes the steps to modify the `web.xml` file to embed the drill-down content from the Lombard portal:

1. Open the `web.xml` file in an editor.
2. Search for the following tag:

```
<filter>
<filter-name>FilterServlet</filter-name>
<filter-class>com.iflex.fic.filters.FilterServlet</filter-class>
</filter>
```

3. Add the following tag before the tag shown in the preceding step:

```
<filter>
   <filter-name>FilterServletAllowFrom</filter-name>
   <filter-class>com.iflex.fic.filters.FilterServlet</filter-class>
   <init-param>
       <param-name>mode</param-name>
       <param-value>ALLOW-FROM https://example.com/</param-value>
   </init-param>
</filter>
<filter-mapping>
   <filter-name>FilterServletAllowFrom</filter-name>
   <url-pattern>/url1</url-pattern>
</filter-mapping>
```

4. Replace the `http://<HOST>:<PORT>/<CONEXT>/` with the URL of Lombard portal and replace the `/url1` with the OFSAA relative URL.

This embeds the OFSAA content in the Lombard portal.

OFSAA Support

Raise a Service Request (SR) in the 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 the My Oracle Support site that has all the revised or recently released documents.