Oracle Financial Services Data Integration

Security Guide

Release 8.1.x

June 2020

ORACLE
Financial Services

ORACLE

Oracle Financial Services Data Integration Security Guide

Copyright © 2020 Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

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.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

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
1.0	June-2020	This document captures the necessary security-related configurations for OFS Data Integration.

Table of Contents

1 Installing OFS DIH Integration 5

2 Set Secure Configurations 6

2.1 Security Configurations 6

3 Secure Header Configuration 7

4 Web Application Server Security Configurations 8

5 Additional Security Configurations 9

6 Secure Database Connection Configurations 10

7 Appendix A - Servlet Filter Configurations 11

1 Installing OFS Data Integration

See the OFS Data Integration Hub Application Pack Installation and Configuration Guide for detailed installation steps.

2 Set Secure Configurations

The OFS DI 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.

2.1 Security Configurations

To have a secure environment for OFSAA installation, there are a set of configurations that must be accomplished. The configurations are discussed in the following sections in this document. For more information, see 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 *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.
- **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 *Update General Details* section 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 or generate a new encryption key if required.

  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.

3 Secure Header Configuration

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

4 Web Application Server Security Configurations

Depending on your configured web application server, see the sections in the *Web Application Server Security Configurations* chapter in the OFSAAI Security Guide.

5 Additional Security Configurations

See the OFSAA Security Guide on how to perform additional security configurations.

6 Secure Database Connection Configurations

See the OFSAA Security Guide on how to secure database connection configurations.

7 Appendix A - Servlet Filter Configurations

See the OFSAA Security Guide on how to configure the servlet filters.

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 My Oracle Support site that has all the revised/recently released documents.