Oracle Financial Services Credit Risk Analytics

Security Guide

Release 8.1.x

Oct 2020

ORACLE
Financial Services

ORACLE

OFS Credit Risk Analytics 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	Oct-2020	This document captures the necessary security-related configurations for OFS Credit Risk Analytics.

Table of Contents

1 Preface 5

1.1 Intended Audience 5

1.1.1 Prerequisites 5

1.2 Related Information Sources 5

2 Install the OFS Credit Risk Analytics Application Pack 7

3 Set Secure Configurations 8

4 Secure Header Configuration 9

5 Web Application Server Security Configurations 10

6 Additional Security Configurations 11

7 Appendix A: Servlet Filter Configurations 12

1 Preface

Oracle Financial Services Credit Risk Analytics 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 or 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 Credit Risk Analytics.

Topics:

- Intended Audience
- Prerequisites
- Related Information Sources

1.1 Intended Audience

This guide is intended for System Administrators (SA) who are instrumental in installing and performing secure configurations for Credit Risk Analytics Pack. 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

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

- Oracle Financial Services Credit Risk Analytics Pack components
- Oracle Financial Services Analytical Applications Infrastructure components
- OFSAA Architecture
- UNIX Commands
- Database Concepts
- Web server or web application server

1.2 Related Information Sources

The related documents are as follows:

- OFS Credit Risk Analytics Application Pack Installation and Configuration Guide 8.1.0.0.0 Release
- OFSAAI Security Guide

- Oracle Financial Services Analytical Applications Infrastructure Application Pack Installation and Configuration Guide

2 Install the OFS Credit Risk Analytics Application Pack

For detailed installation steps, see the OFS Credit Risk Analytics Application Pack Installation and Configuration Guide Release 8.1.0.0.0.

3 Set Secure Configurations

You must configure a set of security parameters to have a secure environment for the OFSAA installation. The OFS CRA application pack components are developed on the OFS Analytical Applications Infrastructure (OFSAAI) and use the OFSAAI secure configurations. The required configurations supported by OFS CRA, is as follows.

- **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 OFS AAI Installation and Configuration Guide. To enable post-installation, see the *Data Redaction* section in the OFSAAI Administration and Configuration 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 and Configuration 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 and Configuration 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 and Configuration Guide.

For detailed information about data security implemented in Oracle Financial Services Data Foundation (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.

OFS AAI 8.1.0.0.0 (platform) is packaged with the OFS CRA 8.1.0.0.0 installer. OFS CRA inherits the following security configurations for the web servers from the platform, 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

OFS AAI 8.1.0.0.0 (platform) is packaged with the OFS CRA 8.1.0.0.0 installer. OFS CRA inherits the following security configurations for the web servers, from the platform.

The OFSAAI framework defines the following:

- 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 OFSAAI Security Guide 8.1.x for more information.

6 Additional Security Configurations

OFS AAI 8.1.0.0.0 (platform) is packaged with the OFS CRA 8.1.0.0.0 installer. OFS CRA inherits the following additional configurations defined in the platform, 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 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 *Appendix A - Servlet Filter Configurations* 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.