

Oracle Financial Services Retail Customer Analytics

Security Guide

Release 8.1.1.0.0

Mar 2021

ORACLE
Financial Services

Oracle Financial Services Retail Customer Analytics Security Guide

Copyright © 2021 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	25-Jan-2021	Created the Security Guide for Oracle Financial Services Retail Customer Analytics application Release 8.1.1.0.0.

Table of Contents

- 1 Preface..... 5**
 - 1.1 Audience 5
 - 1.2 Prerequisites for the Audience 5
 - 1.3 Reference Documents..... 5
- 2 Installing the Oracle Financial Services Retail Performance Analytics Application 6**
- 3 Secure Configurations..... 6**
- 4 Secure Header Configuration 6**
- 5 Web Application Server Security Configuration 7**
- 6 Additional Security Configuration 7**
- 7 Secure Database Connection 8**
 - 7.1 Configurations for Connecting OFSAA to Oracle Database using Secure Database Connection (TCPS)8

1 Preface

Oracle Financial Services Analytical Applications Infrastructure (OFSAAI) provides for configuration of security parameters and this guide provides information about the configurations required and how to set it.

The information contained in this document is intended to give you quick exposure and understanding of the security configurations required after the installation of the OFSAAI.

1.1 Audience

This guide is intended for System Administrators (SA) who are instrumental in installing and performing secure configurations for the OFSAAI. 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.

1.2 Prerequisites for the Audience

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

- OFSAAI pack components
- OFSAA Architecture
- UNIX Commands
- Database Concepts
- Web server and web application server

1.3 Reference Documents

This section identifies the following additional documents related to the OFSAA Infrastructure:

- [OFS Advanced Analytical Applications Infrastructure Installation Guide Release 8.1.10.0](#)
- [OFS Advanced Analytical Applications Infrastructure Environment Check Utility Guide Release 8.1.x](#)
- [OFS Advanced Analytical Applications Infrastructure Application Pack Administration and Configuration Guide Release 8.1.x](#)
- [OFS AAI Application Security Guide Release 8.1.x](#)
- [Oracle Financial Services Analytical Applications Infrastructure Cloning Guide Release 8.1.x](#)
- [Oracle Financial Services Analytical Applications Infrastructure User Guide](#)

2 Installing the Oracle Financial Services Retail Performance Analytics Application

For detailed installation steps, see the [Oracle Financial Services Customer Analytics Pack Installation and Configuration Guide Release 8.1.1.0.0](#).

Oracle Financial Services Retail Performance Analytics Application is built on the Oracle Financial Services Analytical Applications Infrastructure (OFS AAI).

3 Secure Configurations

A set of configurations must be performed to have a secure environment for OFSAA installation. The configurations are discussed in the following sections. For more information, see the [OFS AAI Application Pack Administration and Configuration 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 [OFS AAI Installation and Configuration Guide](#). To enable post-installation, see the *Data Redaction* section in the [OFS AAI Application Pack Administration and Configuration Guide](#).
- **CSRF Enabled:** This option results in setting the Cross-Site Request Forgery (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 [OFS AAI 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 [OFS AAI Application Pack 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 [OFS AAI Application Pack Administration and Configuration Guide](#).

4 Secure Header Configuration

Secure Header configurations protect you from website attacks such as XSS and Clickjacking. For more information, see the *Secure Header Configurations* chapter in the [OFS AAI Security Guide](#),

5 **Web Application Server Security Configuration**

Depending on your configured web application server, see the sections in the *Web Application Server Security Configurations* chapter in the [OFS AAI Security Guide](#).

6 **Additional Security Configuration**

See the *Additional Security Configurations* chapter in the [OFS AAI Security Guide](#) for more information.

7 Secure Database Connection

The Oracle database product supports SSL/TLS connections in its standard edition (since 12c). 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.

To establish an SSL connection the Oracle database sends its certificate, which is stored in a wallet. Therefore, on the server the configuration requires a wallet and on the client, the JDBC thin driver can use different formats to store the client's certificate and key: JKS, Wallet or PKCS12.

This document details about steps to establish an SSL connection over TLSv1.2 using the JDBC thin driver with Oracle wallet having storetype as SSO with OraclePKIProvider.

7.1 Configurations for Connecting OFSAA to Oracle Database using Secure Database Connection (TCPS)

For the documentation, see *Configurations for Connecting OFSAA to Oracle Database using Secure Database Connection (TCPS)* section in [OFS AAI Application Pack Administration and Configuration Guide](#).

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.

