Oracle Financial Services Analytical Applications Reconciliation Framework Pack

Security Guide

Release 8.1.x

July 2020

OFS Analytical Applications Reconciliation Framework Pack Security Guide

Document Control

Version Number	Revision Date	Change Log
1.0	July-2020	This document captures the necessary security-related configurations for OFS Analytical Applications Reconciliation Framework.

Table of Contents

1 Preface

Oracle Financial Services Analytical Applications Reconciliation Framework 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 Analytical Applications Reconciliation Framework Pack.

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 Reconciliation Framework 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 for the Audience

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

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

1.2 Related Documents

The list of related documents are as follows:

- OFS Analytical Applications Reconciliation Framework Pack Installation and Configuration Guide 8.1.0.0.0 Release
- OFSAAI Security Guide 8.1.x
- OFS Analytical Applications Reconciliation Framework Pack Security Guide 8.1.0.0.0 Release

2 Install the OFS Analytical Applications Reconciliation Framework Pack

For detailed installation steps, see the OFS Analytical Applications Reconciliation Framework Pack Installation and Configuration Guide Release 8.1.0.0.0.

3 Set Secure Configurations

The OFS Analytical Applications Reconciliation Framework 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 OFSAA installation. The required configurations are presented in the following list. For more details on the configurations, see the OFSAAI Administration and Configuration Guide and the OFSAAI Security Guide 8.1.x.

- **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.
- **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 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 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 Analytical Applications Reconciliation Framework 8.1.0.0.0, and is packaged with the OFS Analytical Applications Reconciliation Framework Pack 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 Analytical Applications Reconciliation Framework 8.1.0.0.0, and is packaged with the OFS Analytical Applications Reconciliation Framework Pack installer. The OFSAAI framework defines the following security configurations for the web servers.

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

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

6 Additional Security Configurations

OFSAAI 8.1.0.0.0 is the platform used to build OFS Analytical Applications Reconciliation Framework 8.1.0.0.0, and is packaged with the OFS Analytical Applications Reconciliation Framework Pack 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 as follows:

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

See the *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.