

Oracle Financial Services Data Foundation Application Pack

Security Guide

Release 8.12.11.0

Jul 20266



Oracle Financial Services Data Foundation Application Pack Security Guide

Copyright © 2026 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 29, 2026	Added the Configure CONTENT-SECURITY-POLICY and Enabling the Content Security Policy (CSP) sections.

Table of Contents

- 1 Installing the Oracle Financial Services Data Foundation Application Pack 5
- 2 Secure Configuration 5
- 3 Secure Header Configuration..... 6
 - 3.1.1 Configure CONTENT-SECURITY-POLICY.....6
 - 3.1.2 Enabling the Content Security Policy (CSP)6
- 4 Web Application Server Security Configuration 7
- 5 Additional Security Configuration..... 7

1 Installing the Oracle Financial Services Data Foundation Application Pack

For detailed installation steps, see the [Oracle Financial Services Data Foundation Application Pack Installation and Configuration Guide Release 8.1.2.11.0](#).

2 Secure Configuration

A set of configurations must be performed to have a secure environment for OFSAA installation. The configuration is discussed in the following sections. For more information, see the [Oracle Financial Services Advanced Analytical Applications Infrastructure Administration and Configuration Guide Release 8.1.x](#).

- **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 [Oracle Financial Services Advanced Analytical Applications Infrastructure Installation Guide Release 8.1.2.0.0](#). To enable post-installation, see the *Data Redaction* section in the [Oracle Financial Services Advanced Analytical Applications Infrastructure Administration and Configuration Guide Release 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 [Oracle Financial Services Advanced Analytical Applications Infrastructure User Guide Release 8.1.2.0.0](#).
- **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 [Oracle Financial Services Advanced Analytical Applications Infrastructure Administration and Configuration Guide Release 8.1.x](#) 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 Analytical Applications Infrastructure Administration Guide](#).

For detailed information about data security implemented in OFSDF, see the [Oracle Financial Services Data Foundation Application Pack Data Protection Implementation Guide Release 8.1.x](#).

3 Secure Header Configuration

Secure header configuration protects you from website attacks such as XSS and Clickjacking. For more information, see the *Secure Header Configurations* section in the [Oracle Financial Services Advanced Analytical Applications Infrastructure Application Pack Security Guide Release 8.1.x](#).

3.1.1 Configure CONTENT-SECURITY-POLICY

The valid V_PROP_VALUE values are set as per the CSP Rules. The default is NONE. If you set this to NONE, the configuration is not enabled.

```
MERGE INTO aai_setup_props ut
USING (

    SELECT 'CONTENT-SECURITY-POLICY' AS V_PROP_NAME FROM dual
) md ON (ut.V_PROP_NAME = md.V_PROP_NAME)
WHEN NOT MATCHED THEN

    INSERT (V_PROP_NAME,V_PROP_VALUE,V_PROP_TIER,V_SEEDED_BY)
    VALUES ('CONTENT-SECURITY-POLICY','NONE','WEB','AAI')

/
```

3.1.2 Enabling the Content Security Policy (CSP)

```
MERGE INTO aai_setup_props ut
USING (

    SELECT 'CONTENT-SECURITY-POLICY' AS V_PROP_NAME FROM dual
) md
ON (ut.V_PROP_NAME = md.V_PROP_NAME)
WHEN MATCHED THEN
UPDATE SET

    ut.V_PROP_VALUE = 'default-src static.oracle.com ''self'' ; script-src
static.oracle.com ''self'' ''nonce-<__nonce__>''; style-src static.oracle.com
''self'' ''nonce-<__nonce__>''; img-src static.oracle.com ''self'' data;; font-
src static.oracle.com ''self'' data:',

    ut.V_PROP_TIER = 'WEB',

    ut.V_SEEDED_BY = 'AAI'
WHEN NOT MATCHED THEN
INSERT (V_PROP_NAME, V_PROP_VALUE, V_PROP_TIER, V_SEEDED_BY)
VALUES (

    'CONTENT-SECURITY-POLICY',

    'default-src static.oracle.com ''self'' ; script-src static.oracle.com
''self'' ''nonce-<__nonce__>''; style-src static.oracle.com ''self'' ''nonce-
```

```
<__nonce__>''; img-src static.oracle.com ''self'' data;; font-src  
static.oracle.com ''self'' data:',  
    'WEB',  
    'AAI'  
);
```

4 Web Application Server Security Configuration

Depending on your configured web application server, see the *Web Application Server Security Configurations* section in the [Oracle Financial Services Advanced Analytical Applications Infrastructure Application Pack Security Guide Release 8.1.x](#).

5 Additional Security Configuration

See the [Oracle Financial Services Advanced Analytical Applications Infrastructure Application Pack Security Guide Release 8.1.x](#) for more information.

OFSAA Support

Raise a Service Request (SR) in [My Oracle Support](#) 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 My 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 or recently released documents.

