Oracle® Retail Advanced Inventory Planning

Security Guide

Release 16.0

December 2016

ORACLE®

Oracle Retail Advanced Inventory Planning Security Guide, Release 16.0

Primary Author: Melissa Artley

reconfigurations, reassembly or reverse assembly, re-engineering or reverse engineering and recompilations or reverse compilations of the VAR Applications or any derivatives of the VAR Applications. You acknowledge that it shall be a breach of the agreement to utilize the relationship, and/or confidential information of the VAR Applications for purposes of competitive discovery.

The VAR Applications contain trade secrets of Oracle and Oracle's licensors and Customer shall not attempt, cause, or permit the alteration, decompilation, reverse engineering, disassembly or other reduction of the VAR Applications to a human perceivable form. Oracle reserves the right to replace, with functional equivalent software, any of the VAR Applications in future releases of the applicable program.

Contents

3 Securing the WebLogic Server

List of Figures

List of Tables

Send Us Your Comments

Oracle Retail Advanced Inventory Planning Security Guide, Release 16.0.

Oracle welcomes customers' comments and suggestions on the quality and usefulness of this document.

Your feedback is important, and helps us to best meet your needs as a user of our products. For example:

- Are the implementation steps correct and complete?
- Did you understand the context of the procedures?
- Did you find any errors in the information?
- Does the structure of the information help you with your tasks?
- Do you need different information or graphics? If so, where, and in what format?
- Are the examples correct? Do you need more examples?

If you find any errors or have any other suggestions for improvement, then please tell us your name, the name of the company who has licensed our products, the title and part number of the documentation and the chapter, section, and page number (if available).

> **Note:** Before sending us your comments, you might like to check that you have the latest version of the document and if any concerns are already addressed. To do this, access the Online Documentation available on the Oracle Technology Network Web site. It contains the most current Documentation Library plus all documents revised or released recently.

Send your comments to us using the electronic mail address: retail-doc_us@oracle.com

Please give your name, address, electronic mail address, and telephone number (optional).

If you need assistance with Oracle software, then please contact your support representative or Oracle Support Services.

If you require training or instruction in using Oracle software, then please contact your Oracle local office and inquire about our Oracle University offerings. A list of Oracle offices is available on our Web site at http://www.oracle.com.

Preface

This document serves as a guide for administrators, developers, and system integrators who securely administer, customize, and integrate the Oracle Retail Advanced Inventory Planning (AIP) application. For more information on installing AIP, refer to the *Oracle Retail Advanced Inventory Planning Installation Guide*.

Audience

This document is intended for administrators, developers, and system integrators who perform the following functions:

- Document specific security features and configuration details for AIP in order to facilitate and support the secure operation of the Oracle Retail product and any external compliance standards.
- Guide administrators, developers, and system integrators on secure product implementation, integration, and administration.

It is assumed that the readers have general knowledge of administering the underlying technologies and the application.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

For more information, see the following documents in the Oracle Retail Advanced Inventory Planning Release 16.0 documentation set:

- *Oracle Retail Advanced Inventory Planning Administration Guide*
- *Oracle Retail Advanced Inventory Planning Data Management Online Help*
- *Oracle Retail Advanced Inventory Planning Data Management User Guide*

- *Oracle Retail Advanced Inventory Planning Data Model Volume 1—Oracle Database Data Model*
- *Oracle Retail Advanced Inventory Planning Data Model Volume 2—Measure Reference Guide*
- *Oracle Retail Advanced Inventory Planning Implementation Guide*
- *Oracle Retail Advanced Inventory Planning Installation Guide*
- *Oracle Retail Advanced Inventory Planning Operations Guide*
- *Oracle Retail Advanced Inventory Planning Order Management Online Help*
- *Oracle Retail Advanced Inventory Planning Order Management User Guide*
- *Oracle Retail Advanced Inventory Planning Release Notes*
- *Oracle Retail Advanced Inventory Planning Security Guide*
- *Oracle Retail Advanced Inventory Planning Store and Warehouse Replenishment Planning Online Help*
- *Oracle Retail Advanced Inventory Planning Store and Warehouse Replenishment Planning User Guide for the RPAS Fusion Client*

The following documentation may also be needed when implementing AIP:

- Oracle Retail Predictive Application Server Batch Script Architecture (RPASBSA) Implementation Guide
- Oracle Retail Integration Bus (RIB) documentation, based on type of deployment
- Oracle Retail Extract Transform and Load (RETL) documentation
- Oracle Retail Predictive Application Server (RPAS) documentation

My Oracle Support Documents

These Oracle Retail Advanced Inventory Planning Release 16.0 documents are available on My Oracle Support:

- *Oracle Retail Advanced Inventory Planning Calculations for Store and Warehouse Replenishment Planning* (Doc ID 2075628.1)
- *Oracle Retail Supply Chain Creation AIP White Paper 16.x (Doc ID 2184447.1)*
- *Oracle Retail AIP Order Review and Approval Workbook Configurations (Doc ID 2076972.1)*
- *Oracle Retail Advanced Inventory Planning Online Bypass 16.x (Doc ID 2206617.1)*

Customer Support

To contact Oracle Customer Support, access My Oracle Support at the following URL:

`https://support.oracle.com`

When contacting Customer Support, please provide the following:

- Product version and program/module name
- Functional and technical description of the problem (include business impact)
- Detailed step-by-step instructions to re-create
- Exact error message received
- Screen shots of each step you take

Review Patch Documentation

When you install the application for the first time, you install either a base release (for example, 16.0) or a later patch release (for example, 16.0.1). If you are installing the base release, additional patch, and bundled hot fix releases, read the documentation for all releases that have occurred since the base release before you begin installation. Documentation for patch and bundled hot fix releases can contain critical information related to the base release, as well as information about code changes since the base release.

Improved Process for Oracle Retail Documentation Corrections

To more quickly address critical corrections to Oracle Retail documentation content, Oracle Retail documentation may be republished whenever a critical correction is needed. For critical corrections, the republication of an Oracle Retail document may at times not be attached to a numbered software release; instead, the Oracle Retail document will simply be replaced on the Oracle Technology Network Web site, or, in the case of Data Models, to the applicable My Oracle Support Documentation container where they reside.

This process will prevent delays in making critical corrections available to customers. For the customer, it means that before you begin installation, you must verify that you have the most recent version of the Oracle Retail documentation set. Oracle Retail documentation is available on the Oracle Technology Network at the following URL:

http://www.oracle.com/technetwork/documentation/oracle-retail-100266.html

An updated version of the applicable Oracle Retail document is indicated by Oracle part number, as well as print date (month and year). An updated version uses the same part number, with a higher-numbered suffix. For example, part number E123456-02 is an updated version of a document with part number E123456-01.

If a more recent version of a document is available, that version supersedes all previous versions.

Oracle Retail Documentation on the Oracle Technology Network

Oracle Retail product documentation is available on the following web site:

http://www.oracle.com/technetwork/documentation/oracle-retail-100266.html

(Data Model documents are not available through Oracle Technology Network. You can obtain them through My Oracle Support.)

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

AIP Security Features

This chapter provides information on these topics:

- AIP Physical Deployment
- Dependent Applications
- Product Security Features

AIP Physical Deployment

Figure 1–1 illustrates the physical deployment model of the AIP application:

Figure 1–1 AIP Physical Deployment Model

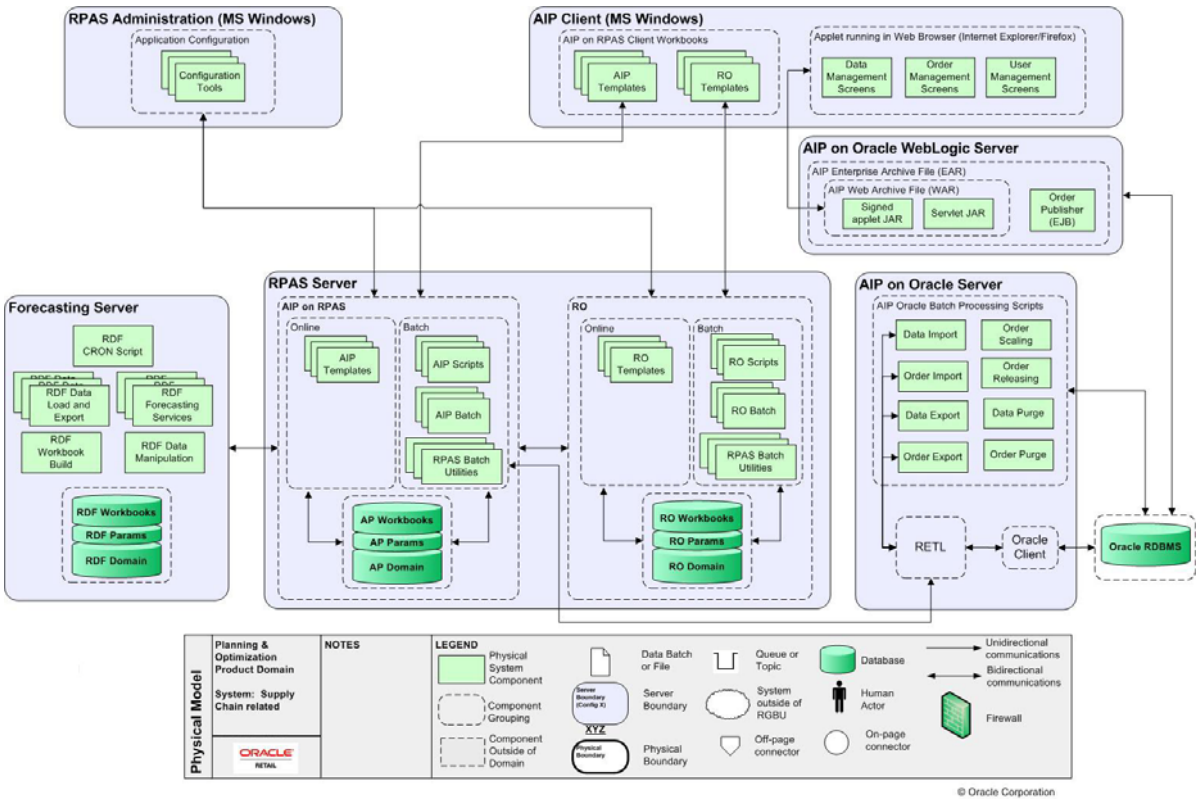
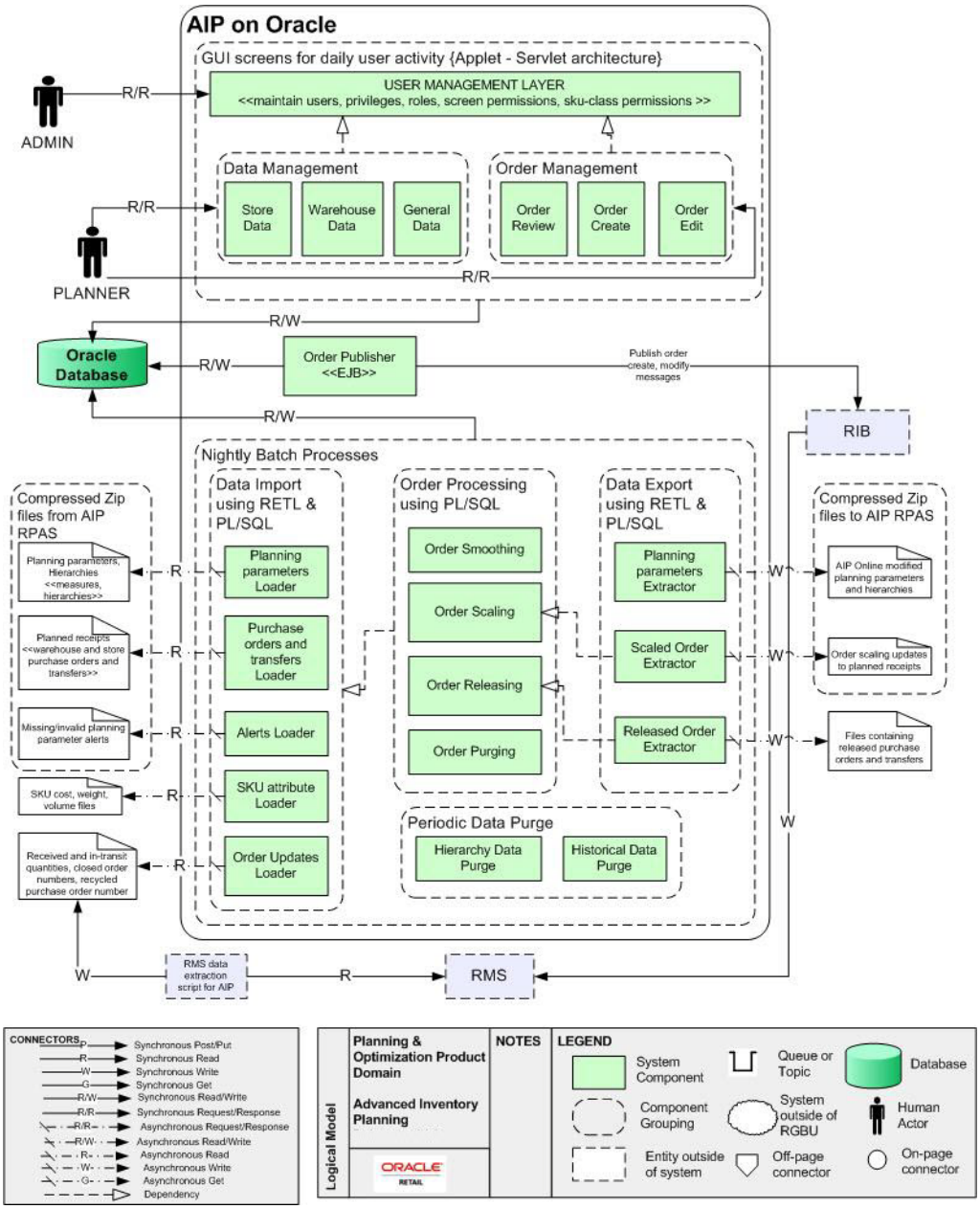


Figure 1–2 illustrates the deployment of the AIP application on the Oracle platform:

Figure 1–2 AIP on Oracle (AIPO)



The AIP Servers and database are expected to be deployed in a corporate data center environment, with computer and physical access restricted to the machines. Data is imported into the application databases through batch processes from data files. The application secures the batch import process, but assumes the import data files are from a trusted source. It is the retailer's responsibility to ensure the integrity of the import data files and to secure access to the import files on the servers.

The AIP application is not designed to run over the public internet, but is expected to run within a private network. Ensure that the server systems running the database and

application server and the client systems are located within a secured corporate network.

Corporate users accessing the system will use a Web browser on Microsoft Windows. Refer to the *Oracle Retail Advanced Inventory Planning Installation Guide* for supported versions. The retailer is responsible for applying the necessary security patches to the Web browser, operating system, and Java Runtime Environment.

The typical configuration of the AIP application runs on multiple servers: one for the Oracle WebLogic Server 12c (12.1.3), one for the Oracle Retail Predictive Application Server, and one for the Oracle database. The WebLogic Server is used to host the Data Management and Order Management applications as well as the RPAS Fusion Client. The retailer is responsible for applying any critical patch updates released for the server hardware, application servers, and database.

Dependent Applications

For information on Oracle Retail Security Guides, including those related to RPAS and Oracle Retail integration technologies, see the following:

http://www.oracle.com/technetwork/documentation/oracle-retail-100266.html

Product Security Features

This section provides information on these topics:

- AIP Dashboard Security
- Application Administration (Data Management and Order Management)
- Passwords
- Audit
- Integration Data Files
- Tools

AIP Dashboard Security

The AIP Dashboard is accessed by AIP RPAS users from the Fusion Client after authentication. Data displayed to the user is filtered by position level security set for each RPAS user. This includes all data in the product and location watchlists.

The AIP Dashboard uses the RPAS JDBC driver to access data from the RPAS domain. A connection is obtained from the pool maintained by the data source in the application server. The identity of the logged-in user is passed to the JDBC driver using the setClientInfo API call (supported in JDBC 4.0 and higher spec). The RPAS ODBC Server receives the RPAS user name sent from the client, and sets the current user for the domain.

Application Administration (Data Management and Order Management)

For both Data Management and Order Management there are user name and password controlled access to the applications. Security rights for each user is defined at a user level and administrated in a central screen. There are data access restrictions in both applications based on assigned rights to merchandise classes. There are screen level access restrictions based on assigned privileges.

Login Functionality

The parameters of login functionality include:

- System access is restricted by a User ID/Password login.
- The password can be updated by the user through the "Change Password" page.
- There are standard and administrator users. Standard users are business users, while administration users assign rights and administrate user accounts.
- General user administration, other than password changes, is restricted to the enterprise administrator user level only.
- The administrator may perform creation of user accounts, password administration, and access rights administration, as well as locking, unlocking and removal of user accounts.
- Password expiration and failed login lockout are available to be set and administrated by the admin user.
- Only application areas the user has rights are made available upon login
- User account information must at minimum include the following:
  - User ID
  - Password
  - E-mail
  - User type
  - Phone
  - Country
  - Location
  - Language
- User login is audited, including time and day of logging in. Refer to the section, Audit, for more details.
- User details are stored in the ENT_USERS table.
  - It is recommended to use database level auditing of DML statements on the ENT_USERS table. See the chapter "Configuring and Administering Auditing" in the *Oracle Database Security Guide*.

Merchandize Data Filtering Functionality

The parameters of merchandize data filtering functionality include:

- Merchandise classes are automatically be added and deleted from the assignment list upon changes in the class definitions in the database.
- The administrator can assign class access rights to users.
- Data in the following categories will be restricted by the classes assigned to the user:
  - SKU
  - SKU Pack-size
  - Demand Group
  - Class

- Data for classes not assigned to the user will not display in the listed drop-downs and List of Values (LOV).
- Users should be set up to receiving the minimum data privileges necessary.

Screen Level Access Functionality

The parameters of screen level access functionality include:

- Application access may be controlled at the tab level by the system administrator for each user account.
- All fields in the screens of inaccessible tabs are disabled, and an alert message displays indicating that this area is not accessible for the user.

> **Note:** This alert message will not display if the tab is the default selection in a selected area.

- User/class relationships are stored in the DEPARTMENT_SCOPE table.
- Users should be set up to receive access only to the screens required for their role.

User Roles

The assignment of screen and class-level permissions are done on a per user, per security permission basis. This means that adding a new user requires a detailed list of what screens they'll need to access and what Classes are necessary.

User role functionality is available in order to provide a method of mass assignment and mass maintenance. A user role may be associated with a particular screen, or set of screen privileges. This role can then be assigned to a user, thus granting the user permission to all screens assigned to the role.

The role is assigned to a user in the standard user permissions screen. All roles are prefaced with a type of role *security* indicator. The role is selected from the list of all available security types and saved to the user.

After the assignment of a role to users the administrator can grant additional screen access, or remove access from a particular role. The change will automatically be reflected in all user permissions assigned to the modified role.

It is important to note that the user roles only contain screen access permissions. They do not include Class permissions.

While the user roles are a tool to aid in assignment and maintenance of user permissions, individual screens may be assigned to a user on a screen-by-screen, user-by-user basis, as desired.

For more information, refer to the *Oracle Retail Advanced Inventory Planning Administration Guide*.

Default Accounts and Passwords

AIP does not contain any default accounts, user IDs, or passwords. An administration user account is created during the database installation process. The username and password of this administrator are chosen during installation. For more information, refer to the *Oracle Retail Advanced Inventory Planning Installation Guide*.

Passwords

AIP protects authentication passwords. There are no clear-text passwords available in the application.

Application Passwords

User passwords for Data Management and Order Management are stored in the Oracle database in the ENT_USERS table. Passwords are iteratively hashed using the SHA-1 secure hash algorithm with a salt before being inserted into the database.

Password policy settings are configured through a properties file (security.properties). Password policies are secure by default and it is not recommended to ease these restrictions. To prevent unauthorized changes to the password properties it is recommended to maintain strict file permissions (0600) on the properties file.

The default password policy includes the following restrictions:

- Minimum of six (6) characters and a maximum of 128.
- Minimum of five (5) different characters.
- May not be simple.
  - For example, sequences (ABCDE or ABCXYZ) and may not contain more than four consecutive characters as this will result in "pairing" (ABCDEF results in (5) pairs AB, BC, CD, DE, EF)
- May not be easily derivable from user name or full name.
- May not be derivable from a dictionary entry (the dictionary is configurable).
- It is case sensitive.
- Passwords expire after 60 days.
- Accounts are locked after three (3) incorrect password entries.

For more information on setting up and maintaining password policies, see the Password Restrictions section in the *Oracle Retail Advanced Inventory Planning Administration Guide*.

Oracle Database Credentials

Batch programs access the database using credentials stored in an Oracle Wallet. For more information, see the Setting Up Application Password Stores chapter in the *Oracle Retail Advanced Inventory Planning Installation Guide*.

Oracle Retail Integration Bus (RIB) Credentials

Credentials for the RIB are collected during the AIP Online application installation and stored in a secured wallet file. Refer to the "Installing AIPOnlineApp on WebLogic" chapter in the *Oracle Retail Advanced Inventory Planning Installation Guide*.

Audit

Security changes and session activity are recorded in an audit table in the Oracle database. Table 1–1 shows the events included in the audit table

Table 1–1 Audit Events

Event Type	Event	Event ID
Login	login	1

Table 1–1 (Cont.) Audit Events

Event Type	Event	Event ID
Login	logout	2
Login	badLogin	3
Login	passwordExpired	4
Login	loginTemporaryLock	5
Login	loginPermanentLock	6
Updates	userCreated	50
Updates	passwordChangedByUser	51
Updates	passwordChangedByAdmin	52
Updates	accountTemporaryLock	53
Updates	accountPermanentLock	54
Updates	accountLockCleared	55
Admin Events	adminLogin	100
Admin Events	adminLogout	101
Admin Events	adminBadLogin	102
Admin Events	adminCreated	150
Admin Events	adminPasswordChanged	151

Audit events are stored in the ENT_AUDIT table. Details stored in the table include the user id and timestamp of the event, as well as an event-specific details field. It is recommended to limit access to this table to system administrators. The audit table should also be reviewed on an ongoing basis for irregularities.

For more information on auditing, refer to the *Oracle Retail Advanced Inventory Planning Administration Guide*.

Integration Data Files

AIP receives data from external systems in flat file format. Flat files are also used for integration internally in AIP between the Oracle and RPAS platforms.

Access to data flat files should be restricted to the user accounts that run AIP batch processes. It is recommended to use FTP over SLL to move data files securely over the network.

External systems for AIP can include:

- Oracle Retail Demand Forecasting (RDF) supplies a demand forecast.
- Oracle Retail Merchandising System (RMS) provides hierarchy data such as SKUs, stores, and warehouses, as well as measure data such as current inventory, in-transits, on-orders, product supplier links.
- Oracle Retail Replenishment Optimization (RO) which provides optimized replenishment methods and parameters.

For more information on AIP interfaces, refer to the chapter AIP Integration in the *Oracle Retail Advanced Inventory Planning Operations Guide.*

Tools

The AIP application uses a number of security tools to scan for security issues. This includes tools such as WebInspect and an internal fuzzing tool to test SQL security.

Retailers and system integrators who are customizing or extending any of the applications should consider running the following or similar tools on their customizations and extensions. As with any tool, the output of these tools should be analyzed in detail since the output may contain false positive warnings.

Fortify

Fortify 360 is a tool that analyzes software for vulnerabilities. The static analysis component examines an application's source code for potentially exploitable vulnerabilities. The dynamic analysis component identifies vulnerabilities that can be found only when an application is running. All vulnerabilities can be ranked according to their PCI relevance.

Fortify is found at the following Web site:

http://www.fortify.com/

WebInspect

HP WebInspect performs Web application security testing and assessment for complex Web applications, built on emerging technologies.

HP WebInspect is found at the following Web site:

https://www.fortify.com/products/web_inspect.html

2

Securing the Database

AIP supports the use of the Oracle Database 12c (12.1.0.2). The database must be secured using the recommendations provided in the *Oracle Database 12c Security Guide*. This chapter provides additional specific guidance for securing the database for use with AIP.

This chapter provides information on these topics:

Install Patch Set Updates

Before you start setting up the database, ensure that you have installed all the critical patch updates (CPU) and patches for the database. Critical patch updates and patch sets for Oracle products are made available on the My Oracle Support Web site (`https://support.oracle.com`) along with documentation or instructions on how you can install them.

Application Schema Owners

The following recommendations should be considered for the schema owners:

- Database Administrators should create an account to act as the schema owner for the database schema.
- The schema owner should only have enough access privileges to install the application.
- For more information on creating database user accounts and the specific access privileges for the schema owners, see the section "Creating the AIP Schema Owner" in the chapter "Installing the AIP Oracle Databases Server Components" of the *Oracle Retail Advanced Inventory Planning Installation Guide*.
- It is recommended that the User ID and password comply with the following policies:
  - Do not use group, shared, or generic accounts and passwords.
  - Require a minimum password length of at least seven characters.
  - Use passwords containing both numeric and alphabetic characters.

- Do not allow an individual to submit a new password that is the same as any of the last four passwords used.
- Limit repeated access attempts by locking out the User ID after not more than six attempts.
- Set the lockout duration to 35 minutes or until an administrator enables the User ID.

Note: You can also choose to change user passwords at least every 90 days. In case you do choose to set this policy, ensure that the passwords set up in the connection pools for the AIP data sources in the WebLogic Server Administration Console are also updated to reflect the latest password. Once updated, the WebLogic server will need to be restarted for the changes to take effect.

Database Security Considerations

The following recommendations should be considered for the database:

- The database should be on its own dedicated server.
- The database server should be in a private network.
- The database server should be in a locked secure facility and inaccessible to non-administrator personnel.
- The database should only be accessed using trusted network hosts.
- The database server should have minimal use of ports and any communications should be under secure protocols.
- The database server should be behind a firewall.
- Any database user beyond the schema application owner should be audited.
- Only minimal rights should be granted to the owner of database processes and files such that only this owner has the right to read and write from the database related files and no one else has the capability to read and write from such files.

Special Security Options for Oracle Databases

Password policies can be enforced using database profiles. The options in the following table are based on version 12.1.0.2 of Oracle Database.

The options can be changed using a SQL statement, for example:

```
alter profile appsample limit
```

Password policies can be enforced using a password complexity verification script, for example:

```
UTLPWDMG.SQL
```

Table 2–1 Oracle Database Security Options

Option	Setting	Description
PASSWORD_LOCK_TIME	30	Time account will be locked in minutes.
FAILED_LOGIN_ATTEMPTS	4	Maximum number of login attempts before the account is locked.

Table 2–1 (Cont.) Oracle Database Security Options

Option	Setting	Description
PASSWORD_GRACE_TIME	3	Number of days a user has to change an expired password before the account is locked.
PASSWORD_REUSE_MAX	10	Number of unique passwords the user must supply before the first password can be reused.
PASSWORD_VERIFY_ FUNCTION	<routine _name>	Name of the procedure that can be created to ensure the password is acceptable.

3

Securing the WebLogic Server

AIP supports the use of Oracle WebLogic Server 12c (12.1.3). The WebLogic server must be secured using the security recommendations provided in the Oracle Fusion Middleware Information Roadmap for Oracle WebLogic Server 12c. This chapter provides additional specific guidance for securing the WebLogic server for use with AIP.

This chapter provides information on these topics:

Install Patch Set Updates

Before you start setting up the database, ensure that you have installed all the critical patch updates (CPU) and patches for the WebLogic server. Critical patch updates and patch sets for Oracle products are made available on the My Oracle Support Web site along with documentation or instructions on how you can install them.

Setting Up a Secure WebLogic Domain

When setting up the WebLogic domain, set up the following configuration parameters to ensure a secured configuration:

Administrative User Account

In a secured configuration, the WebLogic server administrative user names and passwords must not use any default or predictable values, such as weblogic1, welcome1, weblogic, and so on. When setting up the WebLogic domain, ensure that you use non-standard user names and passwords.

Operating System User Account

When the WebLogic server and domains are installed and set up, ensure that they are not running under the root operating system user account. You can check for this by reviewing the permissions on the WebLogic server files and folders. None of these objects should be owned by the root operating system user.

Listen Port Configuration

Once the WebLogic domain for AIP is created, ensure that you manually disable the HTTP port and enable the HTTPS port. This ensures that only a secure channel is used for accessing AIP.

You must also ensure that the secure HTTPS port number is changed to a non-default value. This value must be environment-specific, non-standard, and not easily predictable.

For more information on configuring the listen ports, refer to the *Oracle Fusion Middleware Administrator's Guide*.

Setting Up Keystores

A Java keystore (JKS) is a secured database that stores keys and certificates for an organization. It is used to achieve authentication, integrity, and privacy within in a network. The WebLogic server uses JKS keystores for applications deployed in the WebLogic server.

By default, the WebLogic server is configured with a demo identity keystore and trust keystore. These keystores must not be used in a production environment. You must create your own keystores in the production environment and set up the WebLogic server to use them.

This section describes how you can create your own keystore and trust store. It also describes the necessary configuration steps to set up the WebLogic server with your JKS keystore.

This section provides information on these topics:

Setting Up Keystores and Trust Stores

Use the following steps to set up your own keystore and trust store:

Note: In the following code snippets, the alias name (**AIPselfsigned**), keystore name (**AIPkeystore**), and trust store **(AIPtrust**) are used as examples. You may set up names of your own choosing

---

1. Create a new directory named *keystores* in your AIP deployment and then navigate to this directory.
2. Run the following command to create your keystore and certificate:

   ```
   keytool -genkey -keyalg RSA -alias AIPselfsigned -keystore
   AIPkeystore.jks -storepass  password -validity 360 -keysize 2048
   ```

3. Run the following command to export your certificate from the keystore:

   ```
   keytool -export -alias AIPselfsigned -keystore AIPkeystore.jks -rfc
   -file AIPselfsigned.cer
   ```

4. Run the following command to create a trust store and add your certificate to the list of trusted certificates:

   ```
   keytool -import -alias AIPselfsigned -file AIPselfsigned.cer -keystore
   AIPtrust.ts -storepass password
   ```

Once completed, there are these three files in the keystores folder:

- Keystore
- Trust store
- Certificate

Associating the Keystore and Trust Store with WebLogic Server

To associate the keystore and trust store with the WebLogic server instance:

1. Log on to the WebLogic Server Administration Console.
2. From the Domain Configurations section, click **Servers**, under the Environment category. The Summary of Servers page opens.
3. On the Summary of Servers page, under the Configuration tab, click the relevant server used for AIP. The Settings page for the server opens.
4. On the Settings page, in the Configuration tab, click the Keystores tab.
5. In the Keystores tab, click **Change**.

> **Note:** You may need to lock the configuration for editing.

6. From the drop-down list, select Custom Identity and Custom Trust.
7. Click **Save**.
8. Enter relevant information in the following fields:

Field	Description
Custom Identity Keystore	Specify the location of the keystore file (.jks). For example, `/u00/oracle/AIP133/keystore/AIPkeystore.jks`.
Custom Identity Keystore Type	Specify the type of the keystore. Enter the text: **jks**.
Custom Identity Keystore Passphrase	Specify the password associated with the keystore (set up when you created the keystore).
Confirm Custom Identity Keystore Passphrase	Specify the same password again to confirm.
Custom Trust Keystore	Specify the location of the trust store file (.ts). For example, `/u00/oracle/AIP133/keystore/AIPtrust.ts`.
Custom Trust Keystore Type	Specify the type of the trust store. Enter the text: **jks**.
Custom Trust Keystore Passphrase	Specify the password associated with the trust store (set up when you created the trust store).
Confirm Custom Trust Keystore Passphrase	Specify the same password again to confirm.

9. Click **Save** to save the entries on the Keystores tab.
10. Click the SSL tab and enter the relevant values in the following fields:

Field	Description
Private Key Alias	Specify the name of the keystore self-signed certificate. For example, AIPselfsigned.

Field	Description
Private Key Passphrase	Specify the private key password associated with the certificate (set up when you created the certificate).
Confirm Private Key Passphrase	Specify the password again to confirm.

11. Click **Save** and activate your configuration changes.
12. Restart the WebLogic server for the changes to take effect.

To see the changes to the keystores, ensure that the SSL is already enabled.