Oracle® Retail Merchandising

Security Guide

Release 16.0

E76966-03

September 2017

ORACLE®

Oracle Retail Merchandising Security Guide, Release 16.0

E76966-03

Value-Added Reseller (VAR) Language

Oracle Retail VAR Applications

The following restrictions and provisions only apply to the programs referred to in this section and licensed to you. You acknowledge that the programs may contain third party software (VAR applications) licensed to Oracle. Depending upon your product and its version number, the VAR applications may include:

(i) the **MicroStrategy** Components developed and licensed by MicroStrategy Services Corporation (MicroStrategy) of McLean, Virginia to Oracle and imbedded in the MicroStrategy for Oracle Retail Data Warehouse and MicroStrategy for Oracle Retail Planning & Optimization applications.

(ii) the **Wavelink** component developed and licensed by Wavelink Corporation (Wavelink) of Kirkland, Washington, to Oracle and imbedded in Oracle Retail Mobile Store Inventory Management.

(iii) the software component known as **Access Via**™ licensed by Access Via of Seattle, Washington, and imbedded in Oracle Retail Signs and Oracle Retail Labels and Tags.

(iv) the software component known as **Adobe Flex**™ licensed by Adobe Systems Incorporated of San Jose, California, and imbedded in Oracle Retail Promotion Planning & Optimization application.

You acknowledge and confirm that Oracle grants you use of only the object code of the VAR Applications. Oracle will not deliver source code to the VAR Applications to you. Notwithstanding any other term or condition of the agreement and this ordering document, you shall not cause or permit alteration of any VAR Applications. For purposes of this section, "alteration" refers to all alterations, translations, upgrades, enhancements, customizations or modifications of all or any portion of the VAR Applications including all

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

2 Post Installation of Retail Infrastructure in Database

3 Post Installation of Retail Infrastructure in WebLogic

4 Installing the Merchandise Operations Management Security Applications

5 Troubleshooting

11 Post Installation - Application Administration

12 Extending/Customization

Part III Oracle Retail Sales Audit (ReSA)

13 ReSA Security Considerations

Part IV Oracle Retail Invoice Matching (ReIM)

14 General Security Considerations

15 Understanding Security

16 Post Installation - ReIM Application Administration

17 Extending/Customization

18 Securing the Database

19 Data Security

Part V Oracle Retail Price Management (RPM)

20 General Security Considerations

21 Understanding Security

22 Post Installation - Application Administration

23 Extending/Customization

24 Securing the Database

Part VI   Oracle Retail Allocation

25   Allocation Security Considerations

List of Examples

List of Figures

List of Tables

Send Us Your Comments

Oracle Retail Merchandising 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 guide serves as a guide for administrators, developers, and system integrators who securely administer, customize, and integrate Oracle Retail Merchandising Operations Management (MOM) Suite applications. Installation and configuration for each product are covered in more detail in the each product's 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 the Oracle Retail MOM Suite products, 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. Functional and technical description of the problem (include business impact)

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:

- *Oracle Retail Merchandising Data Conversion Operations Guide*

- *Oracle Retail Merchandising Batch Schedule*

- *Oracle Retail Merchandising Implementation Guide*

- *Oracle Retail POS Suite 14.1/Merchandising Operations Management 15.0 Implementation Guide*

- *Oracle Retail Xstore Suite Merchandising Implementation Guide*

- Oracle Retail Allocation documentation

- Oracle Retail Invoice Matching documentation

- Oracle Retail Merchandising System documentation

- Oracle Retail Trade Management documentation

- Oracle Retail Sales Audit documentation

- Oracle Retail Price Management documentation

- Oracle Retail Active Retail Intelligence documentation

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

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/technology/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.

xx

Part I

Oracle Retail Applications

The following chapters provide guidance for administrators, developers, and system integrators who securely administer, customize, and integrate the Oracle Retail Applications.

Part I contains the following chapters:

- Pre-installation of Retail Infrastructure in WebLogic
- Post Installation of Retail Infrastructure in Database
- Post Installation of Retail Infrastructure in WebLogic
- Installing the Merchandise Operations Management Security Applications
- Troubleshooting
- Importing Topology Certificate
- Using Self Signed Certificates
- Functional Security for Applications Using Fusion Middleware
- ReST Services Security Consideration

1

Pre-installation of Retail Infrastructure in WebLogic

Oracle Retail applications are primarily deployed in Oracle WebLogic server as Middleware tier. Java and forms based applications rely upon Middleware infrastructure for complete security apart from application specific security features.

This chapter describes the pre-installation steps for secured setup of Oracle Retail infrastructure in WebLogic.

The following topics are covered in this chapter:

- JDK Hardening for Use with Retail Applications
- Pre-installation - Steps for Secured Setup of Oracle Retail Infrastructure in WebLogic
- Certificate Authority
- Obtaining an SSL Certificate and Setting up a Keystore
- Creating a WebLogic Domain
- Configuring the Application Server for SSL
- Enforcing Stronger Encryption in WebLogic
- Securing Nodemanager with SSL Certificates
- Using Secured Lightweight Directory Access Protocol (LDAP)
- Enabling Access to Secured Database from Forms Oracle Home - Optional

JDK Hardening for Use with Retail Applications

See the following sections on JDK hardening for use with Retail applications:

- Upgrading JDK to use Java Cryptography extension
- Disabling weak SSL protocols and obsolete ciphers in JDK

Upgrading JDK to Use Java Cryptography Extension

You need to install the unlimited encryption Java Cryptography Extension (JCE) policy, if you want to use the strongest Cipher suites (256 bit_encryption). It is dependent on the Java Development Kit (JDK) version.

Using the following URL, download and install the JCE Unlimited Strength Jurisdiction Policy Files that correspond to the version of your JDK:

http://www.oracle.com/technetwork/java/javase/downloads/index.html

For JDK 7, download from the following URL:

http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432
124.html and replace the files in JDK/jre/lib/security directory

For JDK8, download the files from URL:

http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133
166.html

Disabling Weak SSL Protocols and Obsolete Ciphers in JDK7

> **Note:** This section is applicable only for applications using Java 7.

Edit the following lines in JDK:/jre/lib/security/java.security file

jdk.certpath.disabledAlgorithms=MD2, RC4, RSA keySize < 1024

and

jdk.tls.disabledAlgorithms=SSLv3, SSLV2Hello, MD5withRSA, DH keySize < 768

> **Note:** Restart the entire WebLogic instance using the JDK to enable changes to take effect once the JCE has been installed.

Pre-installation - Steps for Secured Setup of Oracle Retail Infrastructure in WebLogic

Secured Sockets Layer (SSL) protocol allows client-server applications to communicate across a network in a secured channel. Client and server should both decide to use SSL to communicate secured information like user credentials or any other secured information.

WebLogic Server supports SSL on a dedicated listen port. Oracle Forms are configured to use SSL as well. To establish an SSL connection, a Web browser connects to WebLogic Server by supplying the SSL port and the Hypertext Transfer Protocol (HTTPs) protocol in the connection URL.

For example: https://myserver:7002

Retail Merchandising System (RMS) setup is supported in WebLogic in secured mode. For enterprise deployment, it is recommended to use SSL certificates signed by certificate authorities.

> **Note:** You need to obtain a separate signed SSL certificates for each host where application is being deployed.

The Security Guide focuses on securing Oracle Retail Applications in single node setup and not on applications deployed on clusters.

Certificate Authority

Certificate Authority or Certification Authority (CA) is an organization which provides digital certificates to entities and acts as trusted third party. Certificates

issued by the commercial CAs are automatically trusted by most of the web browsers, devices, and applications. It is recommended to have certificates obtained from a trusted CA or commercial CAs to ensure better security.

Obtaining an SSL Certificate and Setting up a Keystore

> **Note:** SSL certificates are used to contain public keys. With each public key there is an associated private key. It is critically important to protect access to the private key. Otherwise, the SSL messages may be decrypted by anyone intercepting the communications.

Perform the following steps to obtain an SSL certificate and setting up a keystore:

1. Obtain an identity (private key and digital certificates) and trust (certificates of trusted certificate authorities) for WebLogic Server.

2. Use the digital certificates, private keys, and trusted CA certificates provided by the WebLogic Server kit, the CertGen utility, Sun Microsystem's keytool utility, or a reputed vendor such as Entrust or Verisign to perform the following steps:

   1. Set appropriate JAVA_HOME and PATH to java, as shown in the following example:

      ```
      export JAVA_HOME=/u00/webadmin/product/jdk
      export PATH=$JAVA_HOME/bin:$PATH
      ```

   2. Create a new keystore.

      keytool -genkey -keyalg RSA -keysize 2048 -keystore <keystore> -alias <alias>

      For example:

      ```
      keytool -genkey -keyalg RSA -keysize 2048 -keystore hostname.keystore
      -alias hostname
      ```

   3. Generate the signing request.

      keytool -certreq -keyalg RSA -file <certificate request file> -keystore <keystore> -alias <alias>

      For example:

      ```
      keytool -certreq -keyalg RSA -file hostname.csr -keystore hostname.keystore
      -alias hostname
      ```

   4. Submit the certificate request to CA.

3. Store the identity and trust.

   Private keys and trusted CA certificates which specify identity and trust are stored in a keystore.

   In the following examples the same keystore to store all certificates are used:

   1. Import the root certificate into the keystore as shown in the following example:

      ```
      keytool -import -trustcacerts -alias  verisignclass3g3ca -file Primary.pem
      -keystore  hostname.keystore
      ```
      A root certificate is either an unsigned public key certificate or a self-signed certificate that identifies the Root CA.

   2. Import the intermediary certificate (if required) into the keystore as shown in the following example:

```
keytool -import -trustcacerts -alias oracleclass3g3ca -file Secondary.pem
-keystore  hostname.keystore
```

3. Import the received signed certificate for this request into the keystore as shown in the following example:

```
keytool -import -trustcacerts -alias hostname -file cert.cer -keystore
hostname.keystore
```

Creating a WebLogic Domain

WebLogic domain is created for Oracle Retail Applications as part of the installation. Different domains are created in different hosts for different applications in situations where applications are being managed by different users or deployed on different hosts. Once the domains are created, you need to enable the SSL ports if not done already.

Perform the following steps to enable the SSL:

1. Log in to WebLogic console using Administrator user. For example, weblogic.

2. Navigate to <Domain> > Environment > Servers > < Servername> > Configuration > General tab.

3. Click **Lock & Edit**.

4. Select **SSL Listen Port Enabled** and assign the port number.

5. Click **Save** and **Activate Changes**.

6. Restart SSL to enable the changes.

Figure 1–1   Restarting the Admin Server
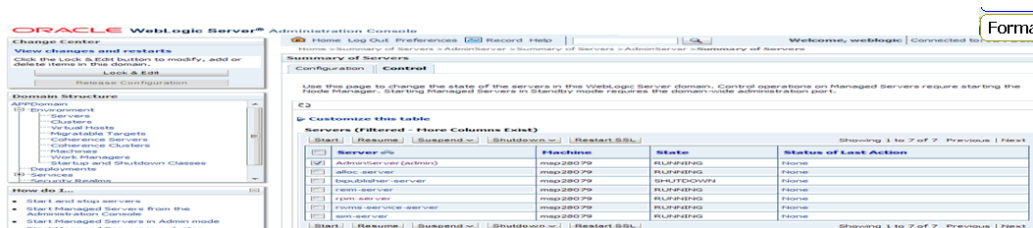
Configuring the Application Server for SSL

Perform the following steps to configure the Application Server for SSL:

1. Configure the identity and trust keystores for WebLogic Server in the WebLogic Server Administration Console.

    1. In the Change Center of the Administration Console, click **Lock & Edit**.

    2. In the left pane of the Console, expand **Environment** and select **Servers**.

    3. Click the name of the server for which you want to configure the identity and trust keystores as shown in the following example:

       ```
       WLS_FORMS is for Forms server
       ```

    4. Select **Configuration**, then select **Keystores**.

    5. In the **Keystores** field, select the method for storing and managing private keys/digital certificate pairs and trusted CA certificates.

       The following options are available:

- **Demo Identity and Demo Trust** - The demonstration identity and trust keystores, located in the BEA_HOME\server\lib directory and the Java Development Kit (JDK) cacerts keystore, are configured by default. You need to use for development purpose only.

- **Custom Identity and Java Standard Trust** - A keystore you create and the trusted CAs defined in the cacerts file in the JAVA_HOME\jre\lib\security directory.

- **Custom Identity and Custom Trust [Recommended]** - An Identity and trust keystores you create.

- **Custom Identity and Command Line Trust**: An identity keystore you create and command-line arguments that specify the location of the trust keystore.

6. Select **Custom Identity** and **Custom Trust**.

7. In the **Identity** section, define the following attributes for the identity keystore:

   - **Custom Identity Keystore** - This is the fully qualified path to the identity keystore.

   - **Custom Identity Keystore Type** - This is the type of the keystore. Generally, this attribute is Java KeyStore (JKS); if it is left blank, it defaults to JKS.

   - **Custom Identity Keystore Passphrase** - This is the password you must enter when reading or writing to the keystore. This attribute is optional or required depending on the type of keystore. All keystores require the passphrase in order to write to the keystore. However, some keystores do not require the passphrase to read from the keystore. WebLogic Server only reads from the keystore so whether or not you define this property depends on the requirements of the keystore.

8. In the **Trust** section, define properties for the trust keystore.

   If you choose **Java Standard Trust** as your keystore, specify the password defined when creating the keystore.

9. Confirm the password.

   If you choose **Custom Trust [Recommended]** define the following attributes:

   - **Custom Trust Keystore** - This is the fully qualified path to the trust keystore.

   - **Custom Trust Keystore Type** - This is the type of the keystore. Generally, this attribute is JKS; if it is left blank, it defaults to JKS.

   - **Custom Trust Keystore Passphrase** - This is the password that you need to enter when reading or writing to the keystore. This attribute is optional or required depending on the type of keystore. All keystores require the passphrase in order to write to the keystore. However, some keystores do not require the passphrase to read from the keystore. WebLogic Server only reads from the keystore, so whether or not you define this property depends on the requirements of the keystore.

10. Click **Save**.

11. To activate these changes, in the Change Center of the Administration Console, click **Activate Changes**.

Note: Not all changes take effect immediately, some require a restart.

Figure 1–2 shows how to configure the Application Server for SSL.

Figure 1–2   Configuring the Identity and Trust Keystores for WebLogic Server

For more information on configuring Keystores, see the *Administration Console Online Help*.

2. Set SSL configuration options for the private key alias and password in the WebLogic Server Administration Console.

1. In the Change Center of the Administration Console, click **Lock & Edit**.

2. In the left pane of the Console, expand **Environment** and select **Servers**.

3. Click the name of the server for which you want to configure the identity and trust keystores.

4. Select **Configuration**, then select **SSL**.

5. In the **Identity and Trust Locations**, the **Keystore** is displayed by default.

6. In the **Private Key Alias**, type the string alias that is used to store and retrieve the server's private key.

7. In the **Private Key Passphrase**, provide the keystore attribute that defines the passphrase used to retrieve the server's private key.

8. Save the changes.

9. Click **Advanced** section of SSL tab.

10. In the **Hostname Verification**, select **None**.

This specifies to ignore the installed implementation of the WebLogic.security.SSL.HostnameVerifier interface (this interface is generally used when this server is acting as a client to another application server).

For Weblogic Server 10.3.6 and former versions, enable Java Secure Socket Extension by enabling **Use JSSE SSL** to provide high security.

11. Save the changes.

Figure 1–3   Configuring SSL

For more information on configuring SSL, see the section *Configure SSL* in the *Administration Console Online Help*.

All the server SSL attributes are dynamic; when modified through the Console. They cause the corresponding SSL server or channel SSL server to restart and use the new settings for new connections. Old connections will continue to run with the old configuration. You must reboot WebLogic Server to ensure that all the SSL connections exist according to the specified configuration.

Use the **Restart SSL** button on the **Control**: Start/Stop page to restart the SSL server when changes are made to the keystore files. You have to apply the same for subsequent connections without rebooting WebLogic Server.

Upon restart you can see the following similar entries in the log:

```
<Mar 11, 2013 5:18:27 AM CDT> <Notice> <WebLogicServer> <BEA-000365> <Server
state changed to RESUMING>
<Mar 11, 2013 5:18:27 AM CDT> <Notice> <Server> <BEA-002613> <Channel
"DefaultSecure" is now ing on 10.141.15.214:57002 for protocols iiops, t3s,
ldaps, https.>
<Mar 11, 2013 5:18:27 AM CDT> <Notice> <Server> <BEA-002613> <Channel
"DefaultSecure[1]" is now ing on 127.0.0.1:57002 for protocols iiops, t3s,
ldaps, https.>
<Mar 11, 2013 5:18:27 AM CDT> <Notice> <WebLogicServer> <BEA-000329> <Started
WebLogic Admin Server "AdminServer" for domain "APPDomain" running in
Production Mode>
<Mar 11, 2013 5:18:27 AM CDT> <Notice> <WebLogicServer> <BEA-000365> <Server
state changed to RUNNING>
<Mar 11, 2013 5:18:27 AM CDT> <Notice> <WebLogicServer> <BEA-000360> <Server
started in RUNNING mode>
```

Note: For complete security of the WebLogic Server, it is recommended to secure both Administration as well the Managed Server where application is being deployed. You can choose to disable the non-SSL ports (HTTP). It is recommended to secure the Node Manager.

The steps to secure Node Manager is provided in the following section.

Configuring WebLogic Scripts if Admin Server is Secured

Perform the following steps to configure the WebLogic scripts if Admin Server is secured:

1. Update the WebLogic startup/shutdown scripts with secured port and protocol to start/stop services.

2. Backup and update the following files in <DOMAIN_HOME>/bin with correct Admin server urls:

   startManagedWebLogic.sh: echo "$1 managedserver1 http://apphost1:7001"

   stopManagedWebLogic.sh: echo "ADMIN_URL defaults to t3://apphost1:7001 if not set as an environment variable or the second command-line parameter."

   stopManagedWebLogic.sh: echo "$1 managedserver1 t3://apphost1:7001 WebLogic

   stopManagedWebLogic.sh: ADMIN_URL="t3://apphost1:7001"

   stopWebLogic.sh: ADMIN_URL="t3://apphost1:7001"

3. Change the URLs as follows:

   t3s://apphost1:7002

   https://apphost1:7002

Adding Certificate to the JDK Keystore for Installer

You will need the Oracle Retail Application installer to run Java. In situations where Administration Server is secured using signed certificate, the Java keystore through which the installer is launched must have the certificate installed.

In case the installer is being run using JDK deployed at location /u00/webadmin/product/jdk, follow the steps as shown in Example 1–1.

Example 1–1   Adding certificate to the JDK keystore for Installer

```
apphost1:[10.3.6_apps] /u00/webadmin/ssl> keytool -import -trustcacerts -alias
apphost1 -file /u00/webadmin/ssl/apphost1.cer -keystore
/u00/webadmin/product/jdk/jre/lib/security/cacerts
Enter keystore password:
Certificate was added to keystore
apphost1:[10.3.6_apps] /u00/webadmin/ssl>
```

Enforcing Stronger Encryption in WebLogic

It is recommended to use a stronger encryption protocol in your production environment.

See the following sections to enable the latest SSL and cipher suites.

SSL protocol version configuration

In a production environment, Oracle recommends Transport Layer Security (TLS) Version 1.1, or higher for sending and receiving messages in an SSL connection.

To control the minimum versions of SSL Version 3.0 and TLS Version 1 that are enabled for SSL connections, do the following:

- Set the **WebLogic.security.SSL.minimumProtocolVersion=protocol** system property as an option in the command line that starts WebLogic Server.

  This system property accepts one of the following values for protocol:

Figure 1–4   Values for Protocol of System Property

Value	Description
SSLv3	Specifies SSL V3.0 as the minimum protocol version enabled in SSL connections.
TLSv1	Specifies TLS V1.0 as the minimum protocol version enabled in SSL connections.
TLSv$x.y$	Specifies TLS V$x.y$ as the minimum protocol version enabled in SSL connections, where: • x is an integer between 1 and 9, inclusive • y is an integer between 0 and 9, inclusive For example, TLSv1.2.

- Set the following property in startup parameters in WebLogic Managed server for enabling the higher protocol:

  DWebLogic.security.SSL.minimumProtocolVersion=TLSv1.2
  -Dhttps.protocols=TLSv1.2

  > **Note:** In case protocol is set for Managed servers, the same should be set for Administration server. Ensure that all the managed servers are down when making changes to the Administration server for setting up the protocol. It is recommended to set the properties in Administration server and then the Managed server.

Enabling Cipher in WebLogic SSL Configuration (For Weblogic 10.3.6 Domains)

Configure the <ciphersuite> element in the <ssl> element in the <DOMAIN_HOME>\server\config\config.xml file in order to enable the specific Cipher Suite to use as follows:

> **Note:** You need to ensure that the tag <ciphersuite> is added immediately after tab <enabled>.

```
<ssl>
<name>examplesServer</name>
<enabled>true</enabled>
<ciphersuite>TLS_RSA_WITH_AES_256_CBC_SHA</ciphersuite>
<-port>17002</-port>
...
</ssl>
```

> **Note:** The above can be done using wlst script.
>
> For more information, go to http://docs.oracle.com/cd/E24329_01/web.1211/e24422/ssl.htm#BABDAJJG. It is advisable to bring down the managed server prior to making the changes.

Securing Nodemanager with SSL Certificates

Perform the following steps for securing the Nodemanager with SSL certificates:

1. Navigate to **<BEA_HOME>/wlserver_10.3/common/nodemanager** (In case of weblogic 12c domain, the location is **<DOMAIN_HOME>/nodemanager**) and take a backup of nodemanager.properties.

2. Add the following similar entries to nodemanager.properties:

   KeyStores=CustomIdentityAndCustomTrust

   CustomIdentityKeyStoreFileName=/u00/webadmin/ssl/hostname.keystore

   CustomIdentityKeyStorePassPhrase=[password to keystore, this will get encrypted]

   CustomIdentityAlias=hostname

   CustomIdentityPrivateKeyPassPhrase=[password to keystore, this will get encrypted]

   CustomTrustKeyStoreFileName=/u00/webadmin/ssl/hostname.keystore

   SecureListener=true

3. In case of weblogic 10.3.6 and former version servers enabled with JSSE, then Nodemanager start up script (startNodeManager.sh) should be added as the following parameter:

   -Dweblogic.security.SSL.enableJSSE=true

4. Log in to **WebLogic console**, navigate to **Environment**, and then **Machines**.

5. Select the nodemanager created already and navigate to **Node Manager** tab.

6. In the Change Center, click **Lock & Edit**.

7. In the **Type** field, select **SSL** from the list.

8. Click **Save** and **Activate**.

Figure 1–5   Securing the Nodemanager

9. You need to bounce the entire WebLogic Domain for changes to take effect, after activating the changes.

10. You need to verify if the nodemanager is reachable in **Monitoring** tab after restart.

Using Secured Lightweight Directory Access Protocol (LDAP)

The Application can communicate with LDAP server on a secured port. It is recommended to use the secured LDAP server to protect user names and passwords from being sent in clear text on the network.

For information on Configuring Secure Sockets Layer (SSL), see the *Oracle Fusion Middleware Administration Guide*.

It is important to import the certificates used in LDAP server into the Java Runtime Environment (JRE) of the WebLogic server for SSL handshake, in case the secure LDAP is used for authentication.

For example:

1. Set JAVA_HOME and PATH to the JDK being used by WebLogic Domain.

2. Backup the JAVA_HOME/jre/lib/security/cacerts

   /u00/webadmin/product/jdk/jre/lib/security> cp -rp cacerts cacerts_ORIG

3. Import the Root and Intermediary (if required) certificates into the java keystore.

   /u00/webadmin/product/jdk/jre/lib/security> keytool -import -trustcacerts -alias verisignclass3g3ca -file ~/ssl/Primary.pem -keystore cacerts

   /u00/webadmin/product/jdk/jre/lib/security> keytool -import -trustcacerts -alias oracleclass3g3ca -file ~/ssl/Secondary.pem -keystore cacerts

4. Import the User certificate from LDAP server into the java keystore.

   /u00/webadmin/product/jdk/jre/lib/security> keytool -import -trustcacerts -alias hostname -file ~/ssl/cert.cer -keystore cacerts

   > **Note:** The default password of JDK keystore is **changeit**.

   The deployed application should be able to communicate with LDAP on SSL port after successful SSL Handshake.

Enabling Access to Secured Database from Forms Oracle Home - Optional

You need to perform the following additional setup to connect to Oracle database on secured port (TCPs) from Forms Oracle Home:

1. Create wallet using orapki.

   > **Note:** A wallet is created using either orapki or mkstore utility. Forms installation provides orapki utility to create the wallet and is used for creation of wallet.

```
$ mkdir /u00/webadmin/product/10.3.X_FORMS/WLS/Oracle_FRHome1/network/wallet
$ cd /u00/webadmin/product/10.3.X_FORMS/WLS/Oracle_FRHome1/network/wallet

$  export JAVA_HOME=/u00/webadmin/product/jdk
$  export PATH=$JAVA_HOME/bin:$PATH

$  export ORACLE_HOME=/u00/webadmin/product/10.3.X_FORMS/WLS/Oracle_FRHome1
$  export PATH=$ORACLE_HOME/bin:$PATH
```

```
$ export PATH=/u00/webadmin/product/10.3.X_FORMS/WLS/oracle_common/bin:$PATH
$ orapki wallet create -wallet
/u00/webadmin/product/10.3.X_FORMS/WLS/Oracle_FRHome1/network/wallet/secured
-auto_login -pwd <wallet-pwd>
Oracle PKI Tool: Version 11.1.1.5.0
Copyright (c) 2004, 2011, Oracle and/or its affiliates. All rights reserved.
$ ls
cwallet.sso  ewallet.p12
```

2. Import the Signed certificates into the wallet.

Example 1–2   Importing all certificates into the wallet

```
$ orapki wallet jks_to_pkcs12 -wallet
/u00/webadmin/product/10.3.X_FORMS/WLS/Oracle_FRHome1/network/wallet/secured -pwd
<wallet-pwd> -keystore
/u00/webadmin/product/10.3.X_APPS/WLS/wlserver_10.3/server/lib/apphost1.keystore
-jkspwd <keystore-pwd>
Oracle PKI Tool: Version 11.1.1.5.0
Copyright (c) 2004, 2011, Oracle and/or its affiliates. All rights reserved.
```
For information on Oracle Wallet Manager and orapki, see *Fusion Middleware Administrator's Guide*.

3. Provide the wallet details in sqlnet.ora file.

> **Note:**   You need to create a sqlnet.ora file with details of the wallet in $ORACLE_HOME/network/admin directory, if the file is not available.

Example 1–3   sqlnet.ora file

```
SQLNET.AUTHENTICATION_SERVICES=(TCPS,NTS)
SSL_CLIENT_AUTHENTICATION = TRUE
WALLET_LOCATION =
   (SOURCE =
     (METHOD = FILE)
     (METHOD_DATA = (DIRECTORY = /u00/webadmin/product/10.3.X_FORMS/WLS/Oracle_
FRHome1/network/wallet/secured))
)
```

4. Connect using sqlplus.

```
$ export ORACLE_HOME=/u00/webadmin/product/10.3.X_FORMS/WLS/Oracle_FRHome1
$ export PATH=$ORACLE_HOME/bin:$PATH

$ sqlplus rms01app@<DB_NAME>_secure
SQL*Plus: Release 12.1.0.1.0 Production on Tue Aug 5 02:15:22 2014
Copyright (c) 1982, 2013, Oracle.  All rights reserved.
Connected to:
Oracle Database 12c Enterprise Edition Release 12.1.0.1.0 - 64bit Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options

SQL>
```

Webservice Security Policies

You need to configure the user credentials and other security related information at the service consumer and the app service provider layers, in order to provide end to end security between Web service consumer and provider.

The security policies certified by Oracle Retail are as follows:

1. Username Token over HTTPS - This security configuration is referred as Policy A in this document. This policy provides confidentiality due to the use of SSL, however it does not provide non-repudiation as nothing is signed.

   Wssp1.2-2007-Https-UsernameToken-Plain.xml

2. Message Protection - This security configuration is referred as Policy B in this document. This policy encrypts the messages itself, so SSL is not used. The sender also signs the messages, which provides non-repudiation of the messages. However, this policy is more complex to implement.

   - Wssp1.2-2007-Wss1.1-UsernameToken-Plain-EncryptedKey-Basic128
   - Wssp1.2-2007-EncryptBody
   - Wssp1.2-2007-SignBody

   Note:

   1. The web services are secured using WebLogic policies (as opposed to OWSM policies).

   2. If the application services are secured with any policy other than what is mentioned in this document or custom policies, the instructions in the document will not work.

   3. The security setup in the document does not address authorization. Authorization must be taken care by the individual application hosting the services.

   4. Policy B is not supported over HTTPS. So ensure that non SSL ports are enabled prior to applying Policy B.

Additional Pre-requisite for Oracle Retail Service Backbone (RSB) Security Policies

Perform the additional pre-requisites for Oracle Retail Service Backbone (RSB) security policies:

1. Create DB schema for OSB [PolicyA][PolicyB].

2. Ensure that <RSB_MDS> schema is created while running Repository Creation Utility (RCU) at <rcuHome>/bin/rcu.

3. Extend RSB Domain with OWSM Extention [PolicyA][PolicyB].

4. Ensure that OSB OWSM Extension-11.1.1.6 is selected, when RSBDomain is being created.

Advanced Infrastructure Security

Depending upon your security need for your production environment, infrastructure where Oracle Retail applications are deployed can be secured.

Ensure the following to secure complete protection of environment:

- Securing the WebLogic Server Host
- Securing Network Connections
- Securing your Database
- Securing the WebLogic Security Service
- Securing Applications

For more information on Ensuring the Security of Your Production Environment, see *Securing a Production Environment for Oracle WebLogic Server 12 C Release 1 (10.3.6) Guide*.

2

Post Installation of Retail Infrastructure in Database

Oracle Retail applications use the Oracle database as the backend data store for applications. In order to ensure complete environment security the database should be secured.

This chapter describes the post installation steps for secured setup of Retail infrastructure in the Database.

The following topics are covered in this chapter:

- Configuring SSL Connections for Database Communications
- Configuring the Password Stores for Database User Accounts
- Configuring the Database Password Policies
- Configuring SSL Connection for Oracle Data Integrator (ODI)
- Creating an Encrypted Tablespace in Oracle 12c Container Database
- Additional Information

Configuring SSL Connections for Database Communications

Secure Sockets Layer (SSL) is the standard protocol for secure communications, providing mechanisms for data integrity and encryption. This can protect the messages sent and received by the database to applications or other clients, supporting secure authentication and messaging. Configuring SSL for databases requires configuration on both the server and clients, which include application servers.

This section covers the steps for securing Oracle Retail Application Clusters (RAC) database. Similar steps can be followed for single node installations also.

Configuring SSL on the Database Server

The following steps are one way to configure SSL communications on the database server:

1. Obtain an identity (private key and digital certificate) and trust (certificates of trusted certificate authorities) for the database server from a Certificate Authority.

2. Create a folder containing the wallet for storing the certificate information. For Real Application Cluster (RAC) systems, this directory can be shared by all nodes in the cluster for easier maintenance.

   ```
   mkdir-p/oracle/secure_wallet
   ```
3. Create a wallet in the path. For example,

```
orapki wallet create -wallet /oracle/secure_wallet -auto_login
```

4. Import each trust chain certificate into the wallet as shown in the following example:

```
orapki wallet add -wallet /oracle/secure_wallet -trusted_cert -cert <trust
chain certificate>
```

5. Import the user certificate into the wallet, as shown in the following example:

```
orapki wallet add -wallet /oracle/secure_wallet -user_cert -cert <certificate
file location>
```

6. Update the listener.ora by adding a TCPS protocol end-point first in the list of end points

```
LISTENER1=
  (DESCRIPTION=
     (ADDRESS=(PROTOCOL=tcps)(HOST=<dbserver>)(PORT=2484))
     (ADDRESS=(PROTOCOL=tcp)(HOST=<dbserver>)(PORT=1521)))
```

7. Update the listener.ora by adding the wallet location and disabling SSL authentication.

```
WALLET_LOCATION =
 (SOURCE=
  (METHOD=File)
  (METHOD_DATA=
   (DIRECTORY=wallet_location)))
SSL_CLIENT_AUTHENTICATION=FALSE
```

8. Update the sqlnet.ora with the same wallet location information and disabling SSL authentication.

```
WALLET_LOCATION =
 (SOURCE=
  (METHOD=File)
  (METHOD_DATA=
   (DIRECTORY=wallet_location)))
SSL_CLIENT_AUTHENTICATION=FALSE
```

9. Update the tnsnames.ora to configure a database alias using TCPS protocol for connections.

```
<dbname>_secure=
  (DESCRIPTION=
   (ADDRESS_LIST=
    (ADDRESS=(PROTOCOL=TCPS)(HOST=<dbserver>)(PORT=2484)))
   (CONNECT_DATA=(SERVICE_NAME=<dbname>)))
```

10. Restart the database listener to pick up listener.ora changes.

11. Verify the connections are successful to the new <dbname>_secure alias

12. At this point either the new secure alias can be used to connect to the database, or the regular alias can be modified to use TCPS protocol.

13. Export the identity certificate so that it can be imported on the client systems

```
orapki wallet export -wallet /oracle/secure_wallet -dn <full dn of identity
certificate> -cert <filename_to_create>
```

Configuring SSL on an Oracle Database Client

The following steps are one way to configure SSL communications on the database client:

1. Create a folder containing the wallet for storing the certificate information.

```
mkdir-p /oracle/secure_wallet
```

2. Create a wallet in the path. For example,

```
orapki wallet create -wallet /oracle/secure_wallet -auto_login
```

3. Import each trust chain certificate into the wallet as shown in the following example:

```
orapki wallet add -wallet /oracle/secure_wallet -trusted_cert -cert <trust
chain certificate
```

4. Import the identity certificate into the wallet, as shown in the following example:

```
orapki wallet add -wallet /oracle/secure_wallet -trusted_cert -cert
<certificate file location>
```

> **Note:** On the client the identity certificate is imported as a trusted certificate, whereas on the server it is imported as a user certificate.

5. Update the sqlnet.ora with the wallet location information and disabling SSL authentication.

```
WALLET_LOCATION =
  (SOURCE=
   (METHOD=File)
   (METHOD_DATA=
    (DIRECTORY=wallet_location)))
SSL_CLIENT_AUTHENTICATION=FALSE
```

6. Update the tnsnames.ora to configure a database alias using TCPS protocol for connections.

```
<dbname>_secure=
(DESCRIPTION=
    (ADDRESS_LIST=
     (ADDRESS=(PROTOCOL=TCPS)(HOST=<dbserver>)(PORT=2484)))
    (CONNECT_DATA=(SERVICE_NAME=<dbname>)))
```

7. Verify the connections are successful to the new <dbname>_secure alias.

8. At this point either the new secure alias can be used to connect to the database, or the regular alias can be modified to use TCPS protocol.

Configuring SSL on a Java Database Connectivity (JDBC) Thin Client

The following steps are one way to configure SSL communications for a Java Database Connectivity (JDBC) thin client:

1. Create a folder containing the keystore with the certificate information.

```
mkdir-p /oracle/secure_jdbc
```

2. Create a keystore in the path. For example,

```
keytool -genkey -alias jdbcwallet -keyalg RSA -keystore /oracle/secure_
jdbc/truststore.jks -keysize 2048
```

3. Import the database certificate into the trust store as shown in the following example:

```
keytool -import -alias db_cert -keystore /oracle/secure_jdbc/truststore.jks
-file <db certificate file>
```

4. JDBC clients can use the following URL format for JDBC connections:

```
jdbc:oracle:thin:@(DESCRIPTION= (ADDRESS= (PROTOCOL=tcps) (HOST=<dbserver>)
(PORT=2484)) (CONNECT_DATA= (SERVICE_NAME=<dbname>)))
```

> **Note:** The <dbname> would be replaced with service name in case of multitenant database (12c).

5. You need to set the properties as shown in Table 2–1, either as system properties or as JDBC connection properties.

Table 2–1 Setting the Properties

Property	Value
javax.net.ssl.trustStore	Path and file name of trust store. For example, /oracle/secure_jdbc/truststore.jks
javax.net.ssl.trustStoreType	JKS
javax.net.ssl.trustStorePassword	Password for trust store

Configuring the Password Stores for Database User Accounts

Wallets can be used to protect sensitive information, including usernames and passwords for database connections. The Oracle Database client libraries have built-in support for retrieving credential information when connecting to databases. Oracle Retail applications utilize this functionality for non-interactive jobs such as batch programs so that they are able to connect to the database without exposing user and password information to other users on the same system.

For information on configuring wallets for database access, see the Appendix Setting Up Password Stores with Oracle Wallet in the product installation guide.

Configuring the Database Password Policies

Oracle Database includes robust functionality to enforce policies related to passwords such as minimum length, complexity, when it expires, number of invalid attempts, and so on. Oracle Retail recommends these policies are used to strengthen passwords and lock out accounts after failed attempts.

For example, to modify the default user profile to lock accounts after five failed login attempts, run the following commands as a database administrator:

1. Query the current settings of the default profile

   select resource_name,limit,resource_type from dba_profiles where profile='DEFAULT';

2. Alter the profile, if failed_login_attempts is set to unlimited:

   alter profile default limit FAILED_LOGIN_ATTEMPTS 5;

   > **Note:** Many other profile settings are available for increased security. For more information, see the *Oracle Database Security Guide.*

Configuring SSL Connection for Oracle Data Integrator (ODI)

This section covers the steps for securing Oracle data Integrator (ODI) and communication over HTTPS Protocol.

See the following steps to configure SSL communications for ODI:

1. Set the environment variable for JAVA_HOME as follows:

   $ export JAVA_HOME=/oracle/oracle_linux/jdk1.7 64bit

   $ export PATH=$JAVA_HOME/bin:$PATH

2. Create a Self Signed Keystore. Run the command to generate the keystore as shown in the following example:

```
$ keytool -genkey -keyalg RSA -alias selfsigned -keystore keystore.jks
-storepass password -validity 360 -keysize 2048
What is your first and last name?
  [Unknown]:  <Hostname>
What is the name of your organizational unit?
  [Unknown]:  <Organization Unit>
What is the name of your organization?
  [Unknown]:  <SomeORG>
What is the name of your City or Locality?
  [Unknown]:  <IN>
What is the name of your State or Province?
  [Unknown]:  <MSP>
What is the two-letter country code for this unit?
  [Unknown]:  <US>
Is CN= <Hostname>, OU=<Organization Unit>, O=<SomeORG>, L=<IN>, ST=<MSP>,
C=<US> correct?
  [no]:  yes
Enter key password for <selfsigned>
        (RETURN if same as keystore password):
Re-enter new password:
```

3. Export the certificate from the keystore created above into the file, server.cer:

```
keytool -export -alias selfsigned -storepass password -file server.cer
-keystore keystore.jks
```

For example:

```
$ keytool -export -alias selfsigned -storepass password -file server.cer
-keystore keystore.jks
Certificate stored in file <server.cer>
```

4. Create the trust-store file, cacerts.jks, and add the server certificate to the trust-store. For example,

```
$ keytool -import -v -trustcacerts -alias selfsigned -file server.cer -keystore
cacerts.jks -keypass password -storepass password
For Example -
$ keytool -import -v -trustcacerts -alias selfsigned -file server.cer -keystore
cacerts.jks -keypass password -storepass password
Owner: CN=<Hostname>, OU=<Organization Unit>, O=<SomeORG>, L=<IN>, ST=<MSP>,
C=<US>
Issuer: CN=<Hostname>, OU=<Organization Unit>, O=<SomeORG>, L=<IN>, ST=<MSP>,
C=<US>
Serial number: 1f5717fd
Valid from: Fri Aug 01 02:12:50 CDT 2014 until: Mon Jul 27 02:12:50 CDT 2015
Certificate fingerprints:
        MD5:  6E:67:FE:FA:4F:6C:E7:E8:C5:5F:17:97:18:E6:62:7E
        SHA1: 48:B7:66:58:24:C9:BD:A9:F9:E1:FB:08:70:94:35:9A:B0:44:DF:D6
        SHA256:
6A:88:40:E1:A7:2F:67:13:6A:F7:12:D0:F1:47:6C:D7:E8:68:45:73:C3:04:36:24:8A:41:1
8:3D:22:8A:DD:5F
        Signature algorithm name: SHA256withRSA
        Version: 3
Extensions:
#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 2E A6 E1 80 12 33 70 4C   72 FA DF ED 98 BB 33 DF  .....3pLr.....3.
0010: 81 6B 40 A4                                        .k@.
]
]
```

```
Trust this certificate? [no]:  yes
Certificate was added to keystore
[Storing cacerts.jks]
```

5. Encode the password used by Keystore and Truststore as follows:

```
$ cd $ODI_HOME/oracledi/agent/bin
$ ./encode.sh <password>
For Example -
$ ./encode.sh password
        fDyp8qdXcuuYUbBcg0Jr
```

6. After configuring repository connection information of the odiparams.sh file, configure and modify the following sections of the file and save it:

```
$ vi odiparams.sh
```

7. Modify the following entries:

```
ODI_KEYSTORE_ENCODED_PASS=fDyp8qdXcuuYUbBcg0Jr
ODI_KEY_ENCODED_PASS=fDyp8qdXcuuYUbBcg0Jr
ODI_TRUST_STORE_ENCODED_PASS=fDyp8qdXcuuYUbBcg0Jr
ODI_JAVA_OPTIONS="-Djava.security.policy=server.policy
-Doracle.security.jps.config=./jps-config.xml
-Djavax.net.ssl.keyStore=<KEYSTORE_LOCATION>/keystore.jks
-Djavax.net.ssl.trustStore=<KEYSTORE_LOCATION>/SSL/cacerts.jks $ODI_PARAMS_
JAVA_OPTION"
```

> **Note:** The encoded password is the one that you generated by running./encode.sh script.

8. Add the following lines to odi.conf before SetJavaHome Environment Variable in the file and save. This will set up ODI Studio for HTTPS.

```
$cd $ODI_HOME/oracledi/agent/bin
Append the odi.conf file with below entries:-
AddVMOption -Djavax.net.ssl.trustStore=<KEYSTORE_LOCATION>/cacerts.jks
AddVMOption -Djavax.net.ssl.trustStorePassword=password
For example
$ vi odi.conf
#Keystore Details
AddVMOption
-Djavax.net.ssl.trustStore=/u03/odi/product/11.1.1.7/SSL/cacerts.jks
AddVMOption -Djavax.net.ssl.trustStorePassword=password
```

> **Note:** The password is the actual password used while encoding. This is not the encoded password.

9. Configure ODI STUDIO with New Agent.

10. Go to the following location:

```
$ cd $ODI_HOME/oracledi/client
```

11. Run the following:

```
$ ./odi.sh
Oracle Data Integrator 11g
Copyright (c) 1997, 2012, Oracle and/or its affiliates. All rights reserved
```

Figure 2–1   Oracle Data Integrator
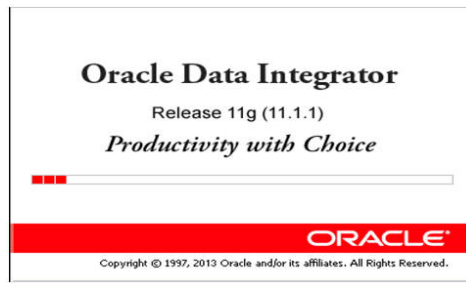
12. The Connect to Repository Window appears:

Figure 2–2   Connect to Repository
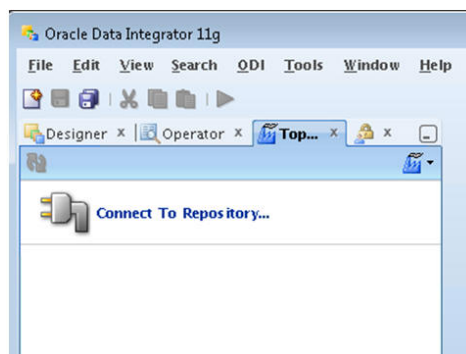
13. Once Connect to Repository Window appears, click **Connect to Repository**. The Oracle Data Integrator Login screen appears.

Figure 2–3   Oracle Data Integrator Login Window
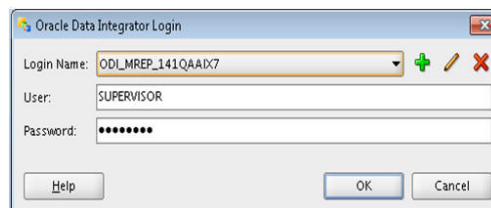
14. Click ➕ symbol and provide the Repository Connection Information.

Figure 2–4   Repository Connection Information Window
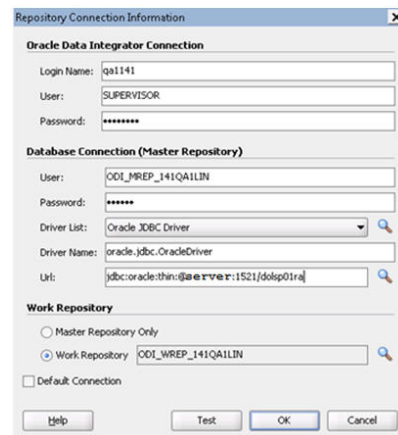
> **Note:**   The URL in Figure 2–4 is an example for Pluggable Database. If it is a non-container database, specify the following URL:
>
> jdbc:oracle:thin:@server:1521/<dbname>

15. Configure the New Agent by right clicking Agents and select New Agent.

Figure 2–5   Creation of ODI Agent
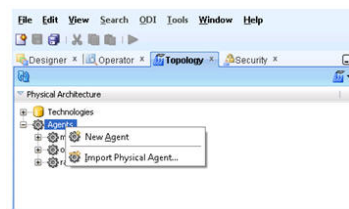
16. Specify all the details and make sure you are using an HTTPS protocol.

Figure 2–6   ODI Agent Connection Information
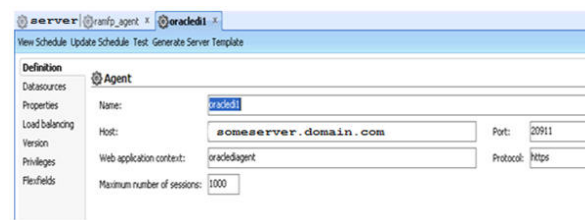
17. Finally start the ODI Agent to listen on HTTPS port:

```
$ $ODI_HOME/oracledi/agent/bin> ./agent.sh "-PROTOCOL=HTTPS" "-PORT=20911"
"-NAME=oracledi1"
Enter password for TrustStore:
2014-08-01 03:18:45.854 NOTIFICATION ODI-1128 Agent oracledi1 is starting.
Container: STANDALONE. Agent Version: 11.1.1.7.0 - 02/03/2013. Port: 20911. JMX
Port: 21911.
2014-08-01 03:18:51.209 NOTIFICATION ODI-1111 Agent oracledi1 started. Agent
```

```
version: 11.1.1.7.0 - 02/03/2013. Port: 20911. JMX Port: 21911.
2014-08-01 03:18:51.210 NOTIFICATION ODI-1136 Starting Schedulers on Agent
oracledi1.
2014-08-01 03:18:52.040 NOTIFICATION ODI-1137 Scheduler started for work
repository ODI_WREP_141QA1LIN on Agent oracledi1
```

Creating an Encrypted Tablespace in Oracle 12c Container Database

The retail tablespaces can be encrypted in container databases using the following method:

1. Update the SQLNET.ORA file with the following encryption details:

   a. Configure the sqlnet.ora File for a Software Keystore Location.

   ENCRYPTION_WALLET_LOCATION=

   (SOURCE=

   (METHOD=FILE)

   (METHOD_DATA=

   (DIRECTORY=path_to_keystore)))

   b. Restart the listener.

2. Set up the Tablespace Encryption in the Container Database.

   a. Create Software Keystores as follows:

   SQL> ADMINISTER KEY MANAGEMENT CREATE KEYSTORE '/u03/wallet_cdb' IDENTIFIED BY "val1ue#";

   Keystore altered.

   b. Create an Auto-Login Software Keystore as follows:

   SQL> ADMINISTER KEY MANAGEMENT CREATE AUTO_LOGIN KEYSTORE FROM KEYSTORE

        '/u03/wallet_cdb' identified by "val1ue#"; Keystore altered.

   Note: The auto-login software keystore can be opened from different computers from the computer where this keystore resides. However, the [local] auto-login software keystore can only be opened from the computer on which it was created.

   ---

   c. Open the Software Keystore as follows:

   SQL> ADMINISTER KEY MANAGEMENT SET KEYSTORE OPEN IDENTIFIED BY "val1ue#" Container=ALL;

   Keystore altered.

   d. Set the Software TDE Master Encryption Key as follows:

   SQL> ADMINISTER KEY MANAGEMENT SET KEY IDENTIFIED BY "val1ue#" WITH BACKUP USING 'TDE_ENCRYPTION' Container=all;

   Keystore altered.

> **Note:** One can set the Encryption KEY only for particular PDB if required, by specifying the CONTAINER=<PDB>.

   e. Create the ENCRYPTED TABLESPACE in PDB as follows:

   SQL> conn sys/D0ccafe1@QOLRP01APP as sysdba

   Connected.

   SQL> create tablespace test datafile '+DATA1' size 100m ENCRYPTION DEFAULT STORAGE (ENCRYPT);

   Tablespace created.

   f. Verify the Encryption:

   SQL> select * from v$encryption_wallet

WRL_ TYPE	WRL_ PARAMET ER	STATUS	WALLET_ TYPE	WALLET OR	FULLY BAC	CON ID
FILE	/u03/walle t_cdb	OPEN	PASSWOR D	SINGLE	NO	0

3. For more information on Configuring Transparent Data Encryption (TDE), see

   http://docs.oracle.com/database/121/ASOAG/asotrans_config.htm#ASOAG9529

4. Other useful information may be useful during maintenance activity.

   a. Close the Encryption Wallet as follows:

   SQL> ADMINISTER KEY MANAGEMENT SET KEYSTORE Close IDENTIFIED BY "val1ue#" Container=ALL;

Additional Information

For more information on the subjects covered in this section as well as information on other options that are available to strengthen database security, see the *Oracle Database Security Guide 12c Release 1*.

The Oracle Advanced Security Option provides industry standards-based solutions to solve enterprise computing security problems, including data encryption and strong authentication. Some of the capabilities discussed in this guide require licensing the Advanced Security Option.

For more information, see the *Oracle Database Advanced Security Administrator's Guide 12c Release 1*.

3

Post Installation of Retail Infrastructure in WebLogic

This chapter describes the post installation steps for secured setup of Oracle Retail infrastructure in WebLogic.

The following topics are covered in this chapter:

- Retail Application Specific Post installation Steps for Security
- Batch Set Up for SSL Communication
- Oracle Business Intelligence (BI) Publisher - Disable Guest User - Optional
- Asynchronous Task JMS Queue Security
- Hardening Use of Headers and Transport Layer Security
- Update weblogic.jdbc.remoteEnabled in setStartupEnv.sh

Retail Application Specific Post installation Steps for Security

See the following sections for steps to improve security after an Oracle Retail Application has been installed.

Batch Set Up for SSL Communication

Java batch programs communicate with Java applications deployed in WebLogic. For example, Oracle Retail Price Management (RPM) and Oracle Store Inventory Management (SIM). The communication needs to have SSL handshake with the deployed application. You need to import the SSL Certificates into the JAVA_HOME/jdk/jre/lib/security/cacerts keystore for successful running of the application batches.

Example 3–1   Importing certificates into JDK keystore

```
/u00/webadmin/product/jdk/jre/lib/security> cp -rp cacerts cacerts_ORIG

/u00/webadmin/product/jdk/jre/lib/security> keytool -import -trustcacerts -alias
verisignclass3g3ca -file ~/ssl/Primary.pem -keystore cacerts

/u00/webadmin/product/jdk/jre/lib/security> keytool -import -trustcacerts -alias
oracleclass3g3ca -file ~/ssl/Secondary.pem -keystore cacerts

/u00/webadmin/product/jdk/jre/lib/security> keytool -import -trustcacerts -alias
hostname -file ~/ssl/cert.cer -keystore cacerts
```

> **Note:** The default password of JDK keystore is **changeit**.

Oracle Business Intelligence (BI) Publisher - Disable Guest User - Optional

The guest account in Oracle Business Intelligence (BI) publisher is used for public facing reports that anyone can see. Disabling this account forces all users to supply their credentials before accessing any information. Disabling guest user enhances security of BI Publisher. However, application which requires guest user will have reporting feature which may cease to function after making this change. For example, RMS reports.

Perform the following steps to disable the guest user:

1. Log in to BI Publisher with user having Administrator privileges.

2. Navigate to Administration > Security Configuration.

3. Deselect **Allow Guest Access**.

Figure 3–1 Administration Window
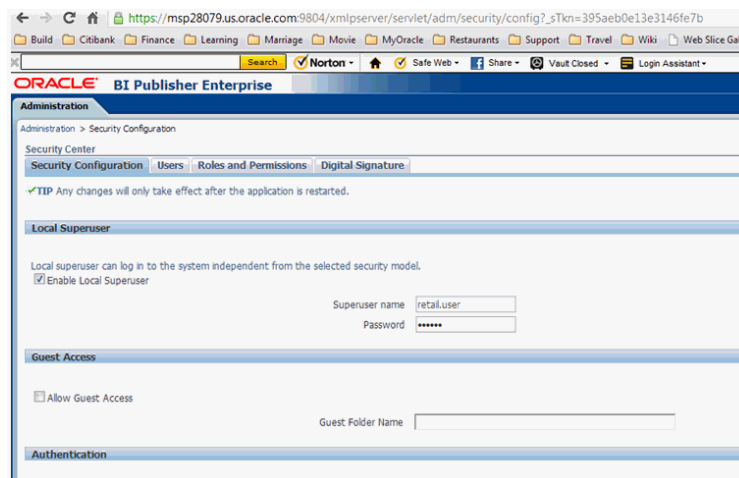
4. Save and restart the BI Publisher instance.

Asynchronous Task JMS Queue Security

This section describes the steps for adding security to the asynchronous task JMS queue. Securing the queue will allow only recognized users of the Retail Application to publish tasks to the JMS queue.

Verifying and Creating Required Async Task Job Role and User

Securing the JMS async task queue requires a special enterprise role and a special user to exist in the retailer's Oracle Internet Directory (OID) instance.

The RETAIL_ASYNC_TASK_JOB is an enterprise role that will be used to group users who will have access to the asynchronous task queue.

The RETAIL _ASYNC_TASK_USER is a special user Retail Applications can use as a principal for executing their message-driven-bean-based consumer processes.   This user is a member of the RETAIL_ASYNC_TASK_JOB.

The RETAIL_ASYNC_TASK_JOB and RETAIL_ASYNC_TASK_USER are included as part of the Retail Default Security Reference Implementation installed as part of the Retail Application.

Verify the existence of the job and user in the OID instance. You need to create them if they do not exist.

Securing the Asynchronous Task JMS Queue

Securing the queue can be done through the Weblogic Administration Console by adding a JMS Queue Scoped role.

1. Log into the WebLogic Administration Console.

2. Navigate to the JMS Module where the asynchronous task queue belongs to and go to the module's Security tab.

3. Under the Roles section, add a new JMS Queue Scoped Roles.

Figure 3–2   Adding a new JMS Queue Scoped Roles
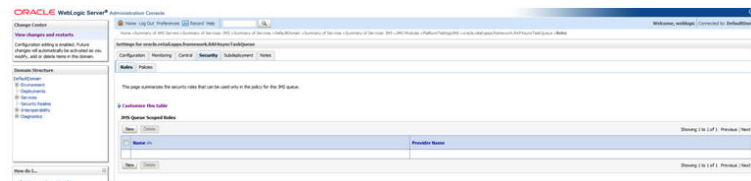
4. Specify a name for the JMS Queue Scoped Role. The suggested naming convention is [AppCode]AsyncJMSQueueAccessRole]. For example, AllocAsyncJMSQueueAccessRole. The JMS Queue Scoped Role will be created.

Figure 3–3   JMS Queue Scoped Role
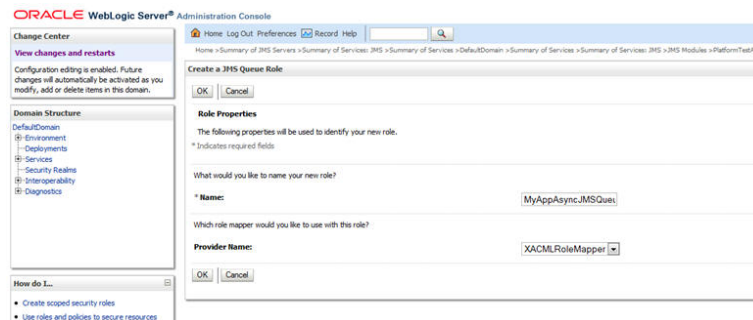
5. Navigate back to the JMS Module's Security tab.

6. Click the JMS Queue Scoped role that was created and add a Group condition for RETAIL_ASYNC_TASK_JOB.

Figure 3–4   Adding a Group condition for RETAIL_ASYNC_TASK_JOB
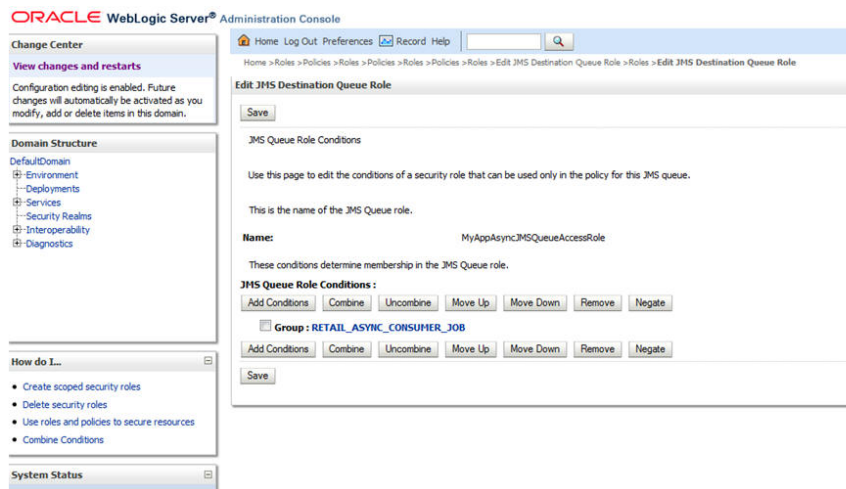
7. Navigate back to the JMS Module's Security tab.

8. Go to the Policies section.

Figure 3–5   Policies Tab
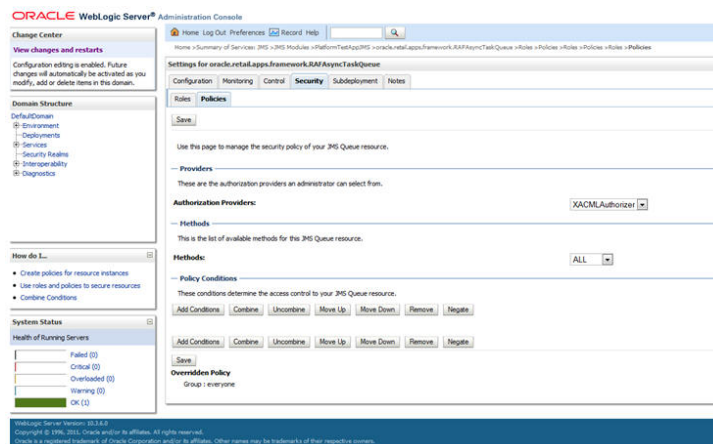
9. Add a new Role based condition specifying the JMS Queue Role created in the previous step.

Figure 3–6 Adding a New Role
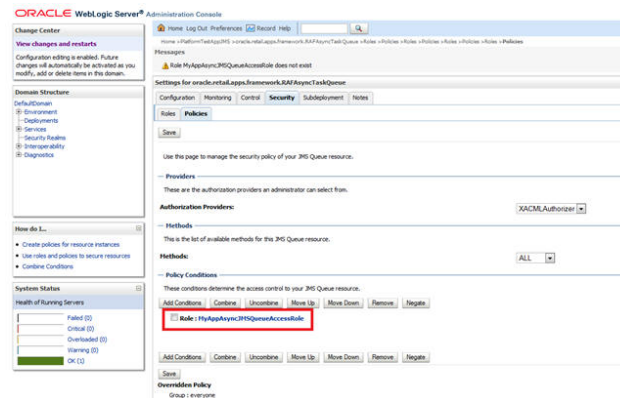
10. Save the changes. The queue is now secured.

11. Proceed to the next section to allow the Retail Web Application to publish tasks to the queue.

Allowing Publishing to a Secured Asynchronous Task JMS Queue

Once the Asynchronous Task Queue has been secured with a JMS Queue Scoped Role as described in the previous section, further configuration is required to allow users of the Retail web application to publish tasks to the queue.

The JMS Queue Scoped Role was created to include an enterprise role, RETAIL_ASYNC_TASK_JOB. Any users belonging to this enterprise role will be given access to publish tasks to the queue.

Instead of assigning users directly to the RETAIL_ASYNC_TASK_JOB,   it is recommended that applications should identify specific enterprise job roles in their system whose users will be allowed to perform asynchronous processing. Those job roles should be configured to extend from the RETAIL_ASYNC_TASK_JOB group.

See the Oracle Internet Directory documentation for details on how to extend one group to another.

Hardening Use of Headers and Transport Layer Security

This section describes the steps for adding security headers in Web server layer and transport security settings in the Retail Applications web.xml file.

Virtual Host Configuration

Navigate to Web server configuration file and add the following header configurations by restarting Web server:

```
# Header Settings to make sure no-store is active

<IfModule mod_headers.c>
    Header set Cache-Control "private, no-cache, no-store, proxy-revalidate,
no-transform"
    Header set Pragma "no-cache"
</IfModule>

# Guarantee HTTPS for 1 Year including Sub Domains
Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"
```

The X-Frame-Options header is appended automatically by the ADF framework. This header setting specifies whether content can be viewed via a third-party X-Frame. To protect against cross-site scripting, the ADF framework sets this value to SAMEORIGIN, which indicates that only websites within the same domain may frame content.

Retail Applications web.xml Configurations

1. Extract the respective Retail applications.

2. Navigate to web.xml file in WEB-INF directory of the application war file.

3. Add the following contents:

```
<security-constraint>
<web-resource-collection>
<web-resource-name>All</web-resource-name>
<url-pattern>/*</url-pattern>
</web-resource-collection>
<user-data-constraint>
<description>USE SSL</description>
<transport-guarantee>CONFIDENTIAL</transport-guarantee>
</user-data-constraint>
</security-constraint>
```

Update weblogic.jdbc.remoteEnabled in setStartupEnv.sh

Ensure to update weblogic.jdbc.remoteEnabled in setStartupEnv.sh to false and rebounce the domain and node manager.

4

Installing the Merchandise Operations Management Security Applications

This chapter indicates the additional steps to be followed in conjunction with Oracle Retail Applications standard installation document. For more information on installing the Oracle Retail Applications, see the *Installation Guides* listed in the subsequent sections for complete steps to be followed.

This chapter covers the following topics of each Merchandise Operations Management (MOM) Applications:

- Installing the ReIM Application
- Installing the RPM Application
- Installing the RMS Application
- Installing the ReSA Application
- Installing the Allocation Application

> **Note:** If MOM applications are installed in secure environment, then set the following parameter before installing the applications:
>
> export _JAVA_ OPTIONS="-Dweblogic.security.SSL.minimumProtocolVersion=TLSv 1.2

Installing the ReIM Application

For information on steps related to the installation of ReIM in secured environment, see Chapter 14 and *Oracle Retail Invoice Matching Installation Guide*.

Installing the RPM Application

For information on steps related to the installation of RPM in secured environment, see Chapter 20 and *Oracle Retail Price Management Installation Guide*.

Installing the RMS Application

For information on steps related to the installation of RMS in secured environment, see Chapter 11 and *Oracle Retail Merchandising System Installation Guide*.

Installing the ReSA Application

For information on steps related to the installation of ReSA in secured environment, see Chapter 13 and *Oracle Retail Sales Audit Installation Guide*.

Installing the Allocation Application

For information on steps related to the installation of Allocation in secured environment, see Chapter 25 and *Oracle Retail Allocation Installation Guide*.

5

Troubleshooting

This chapter covers the common errors, issues, and troubleshooting them.

The following topics are covered in this chapter:

- Enabling TLS1.1 and 1.2 Protocols in Internet Explorer 11
- Hardening Local JRE for Use with Retail Applications
- Java Version 7/8 SSL Handshake Issue while Using Self Signed Certificates
- Setup Secure Cookie
- Changes to Web Application Descriptor
- Launching Issues with RPM
- Disabling Hostname Verification
- Verifying the Certificate Content
- Integration Issues
- HTTPS Service Encountering Redirect Loop After Applying Policy A

Enabling TLS1.1 and 1.2 Protocols in Internet Explorer 11

To enable TLS 1.1 and 1.2 Internet explorer, do the following:

1. Click **Tools** (Alt+X) and the Internet Options.

Figure 5–1
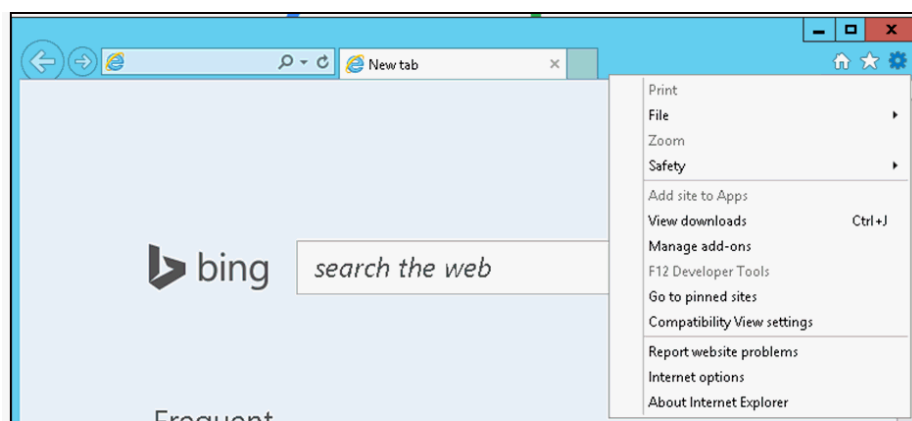
2. Under **Advanced**>**Settings**, scroll down and select TLS 1.0, 1.1 and 1.2. Disable SSL 2.0 and SSL 3.0 as follows:

Figure 5–2
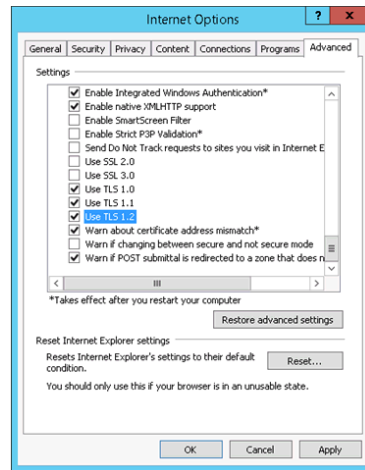
3. Click **Apply**.

Hardening Local JRE for Use with Retail Applications

This section is required to launch RMS, RPM and SIM applications. The configuration is required for both 32bit JRE(Default Location: C:\Program Files (x86)\Java\jre) and 64 bit JRE(Default Location: C:\Program Files\Java\jre8), referred as JRE in reminder of this section.

1. Download and install the JCE Unlimited Strength Jurisdiction Policy Files that correspond to the version of your JDK:

http://www.oracle.com/technetwork/java/javase/downloads/index.html

For JDK 8, download from the following URL:

http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2
133166.html and replace the files in JDK/jre/lib/security directory

Java Version 7/8 SSL Handshake Issue while Using Self Signed Certificates

Java Version 7/8 may have issues using self signed certificates. The self-signed root certificate may not be recognized by Java Version 1.7/1.8 and a certificate validation exception might be thrown during the SSL handshake. You need to create the private key with Subject Key Identifier to fix this problem. You need to include an option -addext_ski when the orapki utility is used to create the private key in the root wallet.

Importing the Root Certificate in Local Client JRE

If customers are using certificates other than provided by standard certificate authorities like custom CA implementation, then the JRE used for launching the applications from local machines like laptops or desktops might display a different error messages.

The most probable cause of this issue could be unavailability of root certificates of the CA within the local JRE being used.

Perform the following steps to import the root certificates:

1. Backup cacert at <JRE_HOME>/lib/security/cacert.

Figure 5–3   Cacert Backup
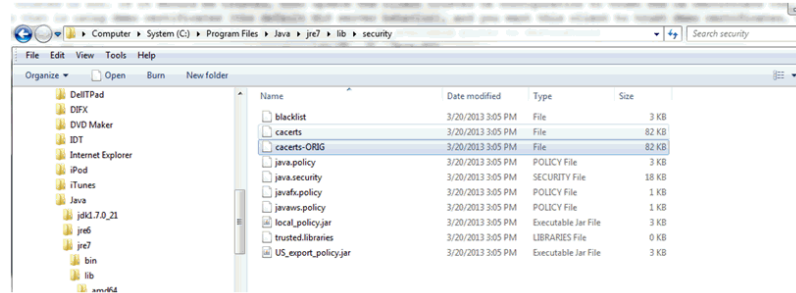
2. Import the certificate using keytool utility as shown in the following example:

```
C:\Program Files\Java\jre8\lib\security>..\..\bin\keytool.exe -import
-trustcacerts -file D:\ADMINISTRATION\SSL\apphost2\Selfsigned\apphost2.root.cer
-alias apphost2 -keystore "C:\Program Files\Java\jre7\lib\security\cacerts"

Enter keystore password: [default is changeit]
Owner: CN=apphost2, OU=<department>, O=<company>,L=<city>,ST=<state or
province>, C=<country>",
Issuer: CN=apphost2, OU=<department>, O=<company>,L=<city>,ST=<state or
province>, C=<country>"
Serial number: 515d4bfb
Valid from: Thu Apr 04 15:16:35 IST 2013 until: Fri Apr 04 15:16:35 IST 2014
Certificate fingerprints:
MD5:  AB:FA:18:2B:BC:FF:1B:67:E7:69:07:2B:DB:E4:C6:D9
SHA1: 2E:98:D4:4B:E0:E7:B6:73:55:4E:5A:BE:C1:9F:EA:9B:71:18:60:BB
SHA256: F3:54:FB:67:80:10:BA:9C:3F:AB:48:0B:27:83:58:BB:3D:22:C5:27:7D:
F4:D1:85:C4:4E:87:57:72:2B:6F:27
Signature algorithm name: SHA1withRSA
Version: 3
Trust this certificate? [no]:  (yes)
Certificate was added to keystore
C:\Program Files\Java\jre8\lib\security>
```

Importing the Root Certificate to the Browser

You need to add the signed Weblogic server certificate in the browser to avoid certificate verification error, if the Root Certificate is not in that list of trusted CAs.

Importing the Root Certificate through Internet Explorer

Perform the following steps to import the Root Certificate through Internet Explorer:

1. Copy the Root Certificate file to the workstation.

2. Rename the file to fa_root_cert.cer (this is a quick and easy way to associate the file with the Windows certificate import utility).

Figure 5–4   Importing the Root Certificate File to the Workstation
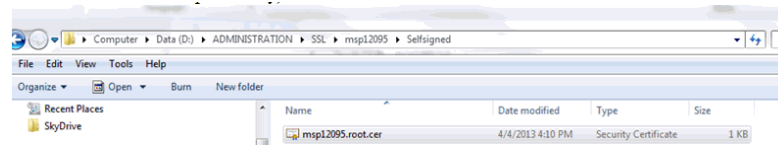
3. Select the file.

4. Click **Install Certificate** and click **Next**.

5. Select **Place all certificates in the following store** and click **Browse**.

6. Select **trusted Root Certification Authorities** and click **OK**.

7. Click **Next**.

8. Click **Finish** and then **Yes** at the Security Warning prompt.

9. Click **OK** to close the remaining open dialog boxes.

Importing the Root Certificate through Mozilla Firefox

Perform the following steps to import the Root Certificate through Mozilla Firefox:

1. Start Mozilla Firefox.

2. Select **Tools** > **Options** from the main menu.

3. Click **Advanced** >**Encryption** tab >**View Certificates**.

4. In Certificate Manager, click the **Authorities** tab and then the **Import** button.

5. In the Downloading Certificate dialog, choose **Trust this CA to identify websites** and click **OK**.

6. Click **OK** in Certificate Manager.

7. Open a browser and test the URL using the SSL port.

Figure 5–5   Importing the Root Certificate File through Mozilla Firefox
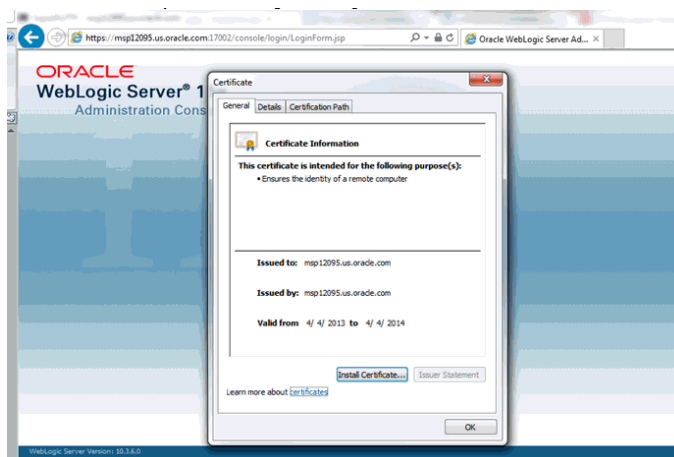
Setup Secure Cookie

To obtain secure cookies, do the following:

1. Enable SSL in the environment.

2. Update the weblogic.xml.

```
<session-descriptor>
<cookie-http-only>false</cookie-http-only>
<cookie-secure>true</cookie-secure>
<url-rewriting-enabled>false</url-rewriting-enabled>
<cookie-path>/<context_root></cookie-path>
</session-descriptor>
```

3. Redeploy the <app>.ear file.

4. Restart the services.

Changes to Web Application Descriptor

Following are the changes to be made to Web Application Descriptor:

1. Open the deployment descriptor of the Service Workspace, which has the jersey servlet configured.

2. Change transport-guarantee to CONFIDENTIAL.

3. Deploy the Application to secure the ReST Services as a one way SSL as follows:

```
<security-constraint>
    <web-resource-collection>
      <web-resource-name>Workflow Actions</web-resource-name>
   <url-pattern>/services/private/*</url-pattern>
       <http-method>GET</http-method>
       <http-method>POST</http-method>
    </web-resource-collection>
 <auth-constraint>
      ..
 </auth-constraint>
 <user-data-constraint>
      <transport-guarantee>CONFIDENTIAL</transport-guarantee>
 </user-data-constraint>
 </security-constraint>
```

> **Note:** An SSL connection needs to be used to ensure information being sent is not compromised, especially authentication credentials. If SSL is not used, the user credentials gets passed with BASE-64 encoding which does not encrypt the credentials and would be a hole in security.

Launching Issues with RPM

For launching errors of RPM in the Java console, see the following example:

```
Caused by: java.net.ConnectException: t3s://apphost2:17012: Destination
unreachable; nested exception is:
javax.net.ssl.SSLKeyException: [Security:090542]Certificate chain received from
apphost2 - 10.141.13.195 was not trusted causing SSL handshake failure. Check the
certificate chain to determine if it should be trusted or not. If it should be
trusted, then update the client trusted CA configuration to trust the CA
certificate that signed the peer certificate chain. If you are connecting to a WLS
server that is using demo certificates (the default WLS server behavior), and you
want this client to trust demo certificates, then specify
-Dweblogic.security.TrustKeyStore=DemoTrust on the command line for this client.;
```

```
No available router to destination
at weblogic.rjvm.RJVMFinder.findOrCreateInternal(RJVMFinder.java:216)
at weblogic.rjvm.RJVMFinder.findOrCreate(RJVMFinder.java:170)
at weblogic.rjvm.ServerURL.findOrCreateRJVM(ServerURL.java:153)
at
weblogic.jndi.WLInitialContextFactoryDelegate.getInitialContext(WLInitialContextFa
ctoryDelegate.java:352)
... 27 more
```

The reason could be SSL Handshake failing between Desktop client and the RPM server. Try importing the root certificates in local client JRE (see the steps as provided in Importing the Root Certificate in Local Client JRE section). In case this fails, try disabling hostname verification to NONE for SSL Configuration of the managed server where RPM is deployed. See Disabling Hostname Verification section. This will require restart of the RPM managed server.

Disabling Hostname Verification

The hostname verification ensures that the hostname in the URL to which the client connects matches the hostname in the digital certificate that the server sends back as part of the SSL connection. However, in case SSL handshake is failing due to inability to verify hostname this workaround can be used.

> **Note:** Disabling hostname verification is not recommended on production environments. This is only recommended for testing purposes. Hostname verification helps to prevent man-in-the-middle attacks.

Perform the following steps to disable the hostname verification for testing purposes:

1. Go to **Environment** > **Domain** > **Servers** > **AdminServer**.

2. Click the **SSL** tab.

3. Click **Advanced**.

4. On Hostname Verification, select **NONE**.

5. Save and activate changes.

6. On the Node Manager startup script, look for JAVA. Add the following line:

   Dweblogic.nodemanager.sslHostNameVerificationEnabled=false

   After this change, the script should look as follows:

   ```
   JAVA_OPTIONS="-Dweblogic.nodemanager.sslHostNameVerificationEnabled=false
   ${JAVA_OPTIONS}"
   cd "${NODEMGR_HOME}"
   set -x
   if [ "$LISTEN_PORT" != "" ]
    then
       if [ "$LISTEN_ADDRESS" != "" ]
   ```

7. Restart Node manager.

Verifying the Certificate Content

In situations where the certificate expires or belongs to a different hosts, the certificates become unusable. You can use the keytool utility to determine the details of the

certificate. The certificates should be renewed or new certificates should be obtained from the appropriate certificate authorities, if the certificates expire.

Example:

```
apphost1:[10.3.6_apps] /u00/webadmin/ssl> keytool -printcert -file cert.cer
Certificate[1]:
Owner: CN=apphost1, OU=<department>, O=<company>,L=<city>,ST=<state or province>,
C=<country>"
Issuer: CN=Oracle SSL CA, OU=Class 3 MPKI Secure Server CA, OU=VeriSign Trust
Network, O=Oracle Corporation, C=US
Serial number: 0078dab9f1a5b56e2cd6g92a3987296
Valid from: Thu Oct 11 20:00:00 EDT 2012 until: Sat Oct 12 19:59:59 EDT 2013
Certificate fingerprints:
        MD5:  2B:71:89:11:01:40:43:FC:6F:D7:FB:24:EB:11:A5:1C
        SHA1:
DA:EF:EC:1F:85:A9:DA:0E:E1:1B:50:A6:8B:A8:8A:BA:62:69:35:C1
        SHA256:
C6:6F:6B:A7:C5:2C:9C:3C:40:E3:40:9A:67:18:B9:DC:8A:97:52:DB:FD:AB:4B:E5:B2:56:47:E
C:A7:16:DF:B6
        Signature algorithm name: SHA1withRSA
        Version: 3

Extensions:
```

Verifying the Keystore Content

Keystores are repository of the certificates. If you face issues related to SSL Certificates, you need to check the certificates which are available in the keystore. You need to import the certificates if they are not missing. The keytool command provides the list of the certificates available.

Example:

```
$ keytool -v -list -keystore /u00/webadmin/product/jdk/jre/lib/security/cacerts
$ keytool -v -list -keystore /u00/webadmin/product/10.3.X_APPS/WLS/wlserver_
10.3/server/lib/apphost1.keystore
```

Integration Issues

Oracle Retail applications can be deployed across different hosts and behind network firewalls. Ensure firewalls are configured to allow TCPS connections to enable secure communications among integrated application.

Secured applications using signed certificates need to use same secured protocols for communication. Ensure that all the communicating applications use the same protocol.

For more information on steps to specify secured protocol, see Enforcing Stronger Encryption in WebLogic section.

Communicating applications using signed certificates may need to verify the incoming connections. Root certificates should be available in the keystores of the applications to verify the requests from different host. It is important to import all the root certificates in the keystores of all communicating applications. For information on steps to import the root certificate in local client JRE, see Importing the Root Certificate in Local Client JRE section.

HTTPS Service Encountering Redirect Loop After Applying Policy A

The proxy server access enters into a redirect loop, if the services are secured with policy A (username token over SSL), and the deployment is in a cluster. The access to such services does not work.

Perform the following workaround through SB Console, for services that are secured with HTTPS:

1. Click **Resource Browser**.

2. Click **Proxy Services under Resource Browser**.

3. Click **Create under Change Center** to start a session.

4. For each of the SSL secured proxy services, perform the following steps:

    1. Click the proxy service you want to change.

    2. Click **Edit** next to **HTTP Transport Configuration**.

    3. Uncheck **HTTPS Required** check box.

    4. Click **Last**.

    5. Click **Save**.

5. Click **Activate** and then **Submit**.

6

Importing Topology Certificate

Implementation of SSL into the Oracle Retail deployment is driven by mapping the SSL certificates and wallets to various participating components in the topology.

Importing Certificates into Middleware and Repository of Oracle Retail Applications

Table 6–1 describes the trust stores to be updated while confirming the certificates imported into middleware and repository of Oracle Retail applications. Ensure you have updated the given trust stores with the signed (either self signed or issued by certifying authority) certificates

> **Note:** In Table 6–1, the *root.cer are the public key certificates and the *server.cer are the private key certificates.

Table 6–1   Importing Topology Certificate

| Component | Certificates | Java app-host | | Forms app-host | | RIB app-host | | BIPublisher-host | | OID-host | Client-host | |
		Java app-Managed server	Java app-JAVA cacerts	Forms app-Managed server	Forms app-JAVA cacerts	RIB app-Managed server	RIB app-JAVA cacerts	BIPublisher-Managed server	BIPublisher-JAVA cacerts	Wallet	Browser	Client-JAVA cacerts
Java.app	appserver.cer	Yes	No	No	No	No	No	No	No	No	No	No
Java.app	approot.cer	Yes	Yes	No	No	No	Yes	No	Yes	Yes	Yes	Yes
Forms.app	fmserver.cer.	No	No	Yes	No	No	No	No	No	No	No	No
Forms.app	fmroot.cer	No	No	No	Yes	No	No	No	Yes	Yes	Yes	Yes
RIB.app	ribserver.cer	No	No	No	No	Yes	No	No	No	No	No	No
RIB.app	ribroot.cer	No	Yes	No	No	Yes	Yes	No	No	No	Yes	Yes
BI Publisher	biserver.cer	No	No	No	No	No	No	Yes	No	No	No	No
BI Publisher	biroot.cer	No	Yes	No	Yes	No	No	Yes	Yes	No	Yes	Yes
OID	oidcer.cer	No	No	No	No	No	No	No	No	Yes	No	No
OID	oidroot.cer	No	Yes	No	No	No	No	No	Yes	Yes	Yes	Yes

7

Using Self Signed Certificates

Self signed certificates can be used for development environment for securing applications. The generic steps to be followed for creating self signed certificates and configuring for use for Oracle Retail application deployment are covered in the subsequent sections.

The following topics are covered in this chapter:

- Creating a Keystore through the Keytool in Fusion Middleware (FMW) 11g
- Exporting the Certificate from the Identity Keystore into a File
- Importing the Certificate Exported into trust.keystore
- Configuring WebLogic
- Configuring Nodemanager
- Importing Self Signed Root Certificate into Java Virtual Machine (JVM) Trust Store
- Disabling Hostname Verification
- Converting PKCS7 Certificate to x.509 Certificate

Creating a Keystore through the Keytool in Fusion Middleware (FMW) 11g

Perform the following steps to create a keystore through the keytool in Fusion Middleware (FMW) 11g:

1. Create a directory for storing the keystores.

   $ mkdir ssl

2. Run the following to set the environment:

   $ cd $MIDDLEWARE_HOME/user_projects/domains/<domain>/bin

   $ . ./setDomainEnv.sh

   Example:

   ```
   apphost2:[10.3.6_apps] /u00/webadmin/product/10.3.6/WLS/user_
   projects/domains/APPDomain/bin> . ./setDomainEnv.sh
   apphost2:[10.3.6_apps] /u00/webadmin/product/10.3.6/WLS/user_
   projects/domains/APPDomain>
   ```

3. Create a keystore and private key, by executing the following command:

   ```
   keytool -genkey -alias <alias> -keyalg RSA -keysize 2048 -dname <dn> -keypass
   <password> -keystore <keystore> -storepass <password> -validity 365
   ```
   Example:

   ```
   apphost2:[10.3.6_apps] /u00/webadmin/ssl> keytool -genkey -alias apphost2
   ```

```
-keyalg RSA -keysize 2048 -dname "CN=<Server Name>,OU=<Organization Unit>,
O=<Organization>,L=<City>,ST=<State>,C=<Country>" -keypass <kpass> -keystore
/u00/webadmin/ssl/apphost2.keystore -storepass <spass> -validity 365

apphost2:[10.3.6_apps] /u00/webadmin/ssl> ls -ltra
total 12
drwxr-xr-x 18 webadmin dba 4096 Apr  4 05:31 ..
-rw-r--r--  1 webadmin dba 2261 Apr  4 05:46 apphost2.keystore
drwxr-xr-x  2 webadmin dba 4096 Apr  4 05:46 .
apphost2:[10.3.6_apps] /u00/webadmin/ssl>
```

Exporting the Certificate from the Identity Keystore into a File

Perform the following steps to export the certificate from the identity keystore into a file (for example, pubkey.cer):

1. Run the following command:

   $ keytool -export -alias selfsignedcert -file pubkey.cer -keystore identity.jks -storepass <password>

   Example:

```
apphost2:[10.3.6_apps] /u00/webadmin/ssl> keytool -export -alias apphost2 -file
/u00/webadmin/ssl/pubkey.cer -keystore /u00/webadmin/ssl/apphost2.keystore
-storepass <spass>
Certificate stored in file </u00/webadmin/ssl/ropubkey.cerot.cer>
apphost2:[10.3.6_apps] /u00/webadmin/ssl> ls -l
total 8
-rw-r--r-- 1 webadmin dba 2261 Apr  4 05:46 apphost2.keystore
-rw-r--r-- 1 webadmin dba  906 Apr  4 06:40 pubkey.cer
apphost2:[10.3.6_apps] /u00/webadmin/ssl>
```

Importing the Certificate Exported into trust.keystore

Perform the following steps to import the certificate you exported into trust.keystore:

1. Run the following command:

   $ keytool -import -alias selfsignedcert -trustcacerts -file pubkey.cer -keystore trust.keystore -storepass <password>

   Example:

```
apphost2:[10.3.6_apps] /u00/webadmin/ssl> keytool -import -alias apphost2
-trustcacerts -file pubkey.cer -keystore trust.keystore -storepass <spass>
Owner: CN=apphost2, OU=<Organization Unit>, O=<company>,L=<city>,ST=<state or
province>, C=<country>
Issuer: CN=apphost2, OU=<Organization Unit>, O=<company>,L=<city>,ST=<state or
province>, C=<country>
Serial number: 515d4bfb
Valid from: Thu Apr 04 05:46:35 EDT 2013 until: Fri Apr 04 05:46:35 EDT 2014
Certificate fingerprints:
        MD5:  AB:FA:18:2B:BC:FF:1B:67:E7:69:07:2B:DB:E4:C6:D9
        SHA1: 2E:98:D4:4B:E0:E7:B6:73:55:4E:5A:BE:C1:9F:EA:9B:71:18:60:BB
        Signature algorithm name: SHA1withRSA
        Version: 3
Trust this certificate? [no]:  yes
Certificate was added to keystore
apphost2:[10.3.6_apps] /u00/webadmin/ssl>
```

Configuring WebLogic

You need to enable SSL for WebLogic server's Admin and managed servers by following the steps as provided in Configuring the Application Server for SSL section.

Configuring Nodemanager

You need to secure the Node manager by following the steps in Securing Nodemanager with SSL Certificates section.

Importing Self Signed Root Certificate into Java Virtual Machine (JVM) Trust Store

In order for the Java Virtual Machine (JVM) to trust in your newly created certificate, import your custom certificates into your JVM trust store.

Perform the following steps to import the root certificate into JVM Trust Store:

1. Ensure that JAVA_HOME has been already set up.

2. Run the following command:

   $keytool -import -trustcacerts -file rootCer.cer -alias selfsignedcert -keystore cacerts

   Example:

   ```
   apphost2:[10.3.6_apps] /u00/webadmin/product/jdk1.1.7_
   30.64bit/jre/lib/security> keytool -import -trustcacerts -file
   /u00/webadmin/ssl/root.cer -alias apphost2 -keystore
   /u00/webadmin/product/jdk1.6.0_30.64bit/jre/lib/security/cacerts -storepass
   [spass default is changeit]
   Owner: CN=apphost2, OU=<Organization Unit>, O=<company>,L=<city>,ST=<state or
   province>, C=<country>"
   Issuer: CN=apphost2, OU=<Organization Unit>, O=<company>,L=<city>,ST=<state or
   province>, C=<country>"
   Serial number: 515d4bfb
   Valid from: Thu Apr 04 05:46:35 EDT 2013 until: Fri Apr 04 05:46:35 EDT 2014
   Certificate fingerprints:
           MD5:  AB:FA:18:2B:BC:FF:1B:67:E7:69:07:2B:DB:E4:C6:D9
           SHA1: 2E:98:D4:4B:E0:E7:B6:73:55:4E:5A:BE:C1:9F:EA:9B:71:18:60:BB
           Signature algorithm name: SHA1withRSA
           Version: 3
   Trust this certificate? [no]:  yes
   Certificate was added to keystore
   apphost2:[10.3.6_apps] /u00/webadmin/product/jdk1.6.0_
   30.64bit/jre/lib/security>
   ```

Disabling Hostname Verification

This section has been covered under Disabling Hostname Verification section.

Converting PKCS7 Certificate to x.509 Certificate

Certificate authorities provide signed certificates of different formats. However, not all formats of certificates can be imported to Java based keystores. Hence the certificates need to be converted to usable form. Java based Keystores supports x.509 format of certificate.

The following example demonstrates converting certificate PKCS 7 to x.509 format:

1. Copy the PKCS 7 certificate file to a Windows desktop.

2. Rename the file and provide .p7b extension.

3. Open the .p7b file.

4. Click the plus (+) symbol.

5. Click the Certificates directory.

   An Intermediary certificate if provided by CA for trust.

   > **Note:** If an Extended Validation certificate is being converted you should see three files. The End Entity certificate and the two EV intermediate CA's.

6. Right click on your certificate file.

7. Select All Tasks > Export.

8. Click **Next**.

9. Select Base-64 encoded X.509 (.cer) > click Next.

10. Browse to a location to store the file.

11. Enter a File name.

    For example, MyCert. The .cer extension is added automatically.

12. Click **Save**.

13. Click **Next**.

14. Click **Save**.

The certificate can be now imported into java based keystores.

Example:

```
apphost1:[10.3.6_apps] /u00/webadmin/ssl> keytool -import -trustcacerts -alias
apphost1 -file /u00/webadmin/ssl/cert-x509.cer -keystore
/u00/webadmin/product/jdk/jre/lib/security/cacerts
Enter keystore password: [default is changeit]
Certificate was added to keystore
apphost1:[10.3.6_apps] /u00/webadmin/ssl>
```

8

Functional Security for Applications Using Fusion Middleware

The chapter provides guidance for administrators to understand, configure, and customize functional security for Application Development Framework (ADF) applications or applications using Fusion Middleware platform security infrastructure like OBIEE.

The following topics are covered in this chapter:

- Understanding the Security Model
- Key Security Elements
- Permission Grants and Inheritance
- Managing Authorization
- Customizing the Default Security Configuration
- Customizing the Policy Store

Understanding the Security Model

The Oracle Retail Fusion security model is built upon the Oracle Fusion Middleware platform, which incorporates the Java security model. The Java model is a role-based, declarative model that employs container-managed security where resources are protected by roles that are assigned to users. However, extensive knowledge of the Java-based architecture is unnecessary when using the Oracle Fusion Middleware Security model.

Key Security Elements

The Oracle Fusion Middleware security model depends upon the following key elements in order to provide uniform security and identity management across the enterprise:

- **Application policy**

  Application permissions are granted to members of its application roles. In the default security configuration, each application role conveys a predefined set of permissions. Permission grants are defined and managed in an application policy. After an application role is associated with an application policy, that role becomes a Grantee of the policy. An application policy is specific to a particular application.

- **Application role**

After permission grants are defined in an application policy, an application role can be mapped to that policy, and the application role then becomes the mechanism to convey the permissions. In this manner, an application role becomes the container that grants permissions to its members. The permissions become associated with the application role through the relationship between policy and role. After groups are mapped to an application role, the corresponding permissions are granted to all members equally. Membership is defined in the application role definition. Application roles are assigned in accordance with specific conditions and are granted dynamically based on the conditions present at the time authentication occurs. More than one group can be members of the same application role.

- **Authentication provider**

  An authentication provider is used to access user and group information and is responsible for authenticating users. An Oracle WebLogic Server authentication provider enables you to manage users and groups in one place.

  An identity store contains user name, password, and group membership information. An authentication provider accesses the data in the identity store and authenticates against it. For example, when a user name and password combination is entered at login, the authentication provider searches the identity store to verify the credentials provided. The Oracle Retail Fusion application's default authentication provider authenticates against Oracle Internet Directory (OID).

- **Users and groups**

  A user is an entity that can be authenticated. A user can be a person, such as an application user, or a software entity, such as a client application. Every user is given a unique identifier.

  Groups are organized collections of users that have something in common. Users should be organized into groups with similar access needs in order to facilitate efficient security management.

- **Security realm**

  An Oracle Retail Fusion application is installed on an Oracle WebLogic Server domain, which is created during installation. The Oracle Retail Fusion application security is managed within the security realm for this Oracle WebLogic Server domain. A security realm acts as a scoping mechanism. Each security realm consists of a set of configured security providers, users, groups, security roles, and security policies. Only one security realm can be active for the domain. The Oracle Retail Fusion application's authentication is performed by the authentication provider configured for the default security realm for the WebLogic Server domain in which it is installed. Oracle WebLogic Server Administration Console is the administration tool used for managing an Oracle WebLogic Server domain.

Permission Grants and Inheritance

Each Oracle Retail Fusion application provides application-specific permissions for accessing different features. Application permissions are typically granted by becoming a member in an application role. Permissions can be granted in two ways - through membership in an application role (direct) and through group and role hierarchies (inheritance). Application role membership can be inherited by nature of the application role hierarchy. In the default security configuration, each application role is pre configured to grant a predefined set of permissions. Groups are mapped to an application role. The mapping of a group to a role conveys the role's permissions to

all members of the group. In short, permissions are granted in Oracle Retail Fusion applications by establishing the following relationships:

- A group defines a set of users having similar system access requirements. Users are added as members to one or more groups according to the level of access required.

- Application roles are defined to represent the role a user typically performs when using the Oracle Retail Fusion application.

- The groups of users are mapped to one or more application roles that match the type of access required by the population.

- An application role is mapped to the application policy that grants the set of permissions required by the role type (an administrator, an author, a consumer).

- Group membership can be inherited by nature of the group hierarchy. Application roles mapped to inherited groups are also inherited, and those permissions are likewise conveyed to the members.

User permissions are determined by the system as follows:

1. A user enters credentials into a Web browser at login. The user credentials are authenticated by the authentication provider against data contained in the identity store.

2. After successful authentication, a Java subject and principal combination is issued, which is populated with the user name and a user's groups.

3. A list of the user's groups is generated and checked against the application roles. A list is created of the application roles that are mapped to each of the user's groups.

4. A user's permission grants are determined from knowing which application roles the user is a member of.

A user can also be granted permissions if they inherit other application roles. Members of application roles can include other groups and application roles. The result is a hierarchical role structure where permissions can be inherited in addition to being explicitly granted. This hierarchy provides that a group is granted the permissions of the application role for which it is a member, and the permissions granted by all roles descended from that role.

For example, the default security configuration includes several predefined groups and application roles. The default BIAdministrator application role includes the BIAdministrators group, the BIAuthor application role includes the BIAuthors group, and the BIConsumer application role includes the BIConsumers group. The default BIAdministrator application role is a member the BIAuthor application role, and the BIAuthor application role is a member of the BIConsumer application role. The members of these application roles inherit permissions as follows. Members of the BIAdministrators group are granted all the permissions of the BIAdministrator role, the BIAuthor role, and the BIConsumer role. By nature of this role hierarchy, the user who is a member of a particular group is granted permissions both explicitly and through inheritance.

> **Note:** By themselves, groups and group hierarchies do not enable any privilege to access resources controlled by an application. Privileges are conveyed by the permission grants defined in an application policy. A group or application role becomes a Grantee of the application policy. The application policy Grantee conveys the permissions and this is done by becoming a member of the Grantee (application role).

Figure 8–1 shows these relationships between the default groups and application roles.

Figure 8–1 Relationships between the Default Groups and Application Roles
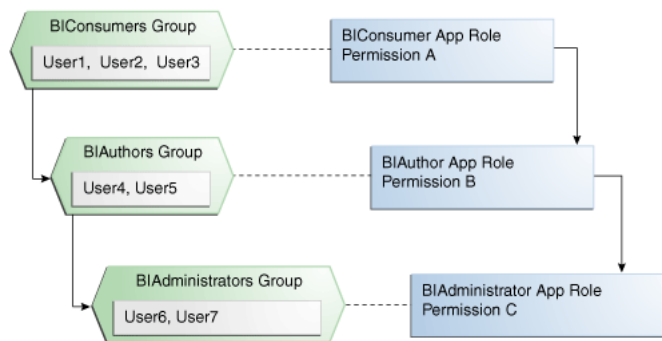
Table 8–1 summarizes how permissions are granted explicitly or are inherited in the previous example and in Figure 8–1.

Table 8–1 Permissions Granted by the Role Hierarchy Example

User Name	Group Membership: Explicit/Inherited	Application Role Membership: Explicit/Inherited	Permission Grants: Explicit/Inherited
User1, User2, User3	BIConsumers: Explicit	BIConsumer: Explicit	Permission A: Explicit
User4, User5	BIAuthors: Explicit BIConsumers: Inherited	BIAuthor: Explicit BIConsumer: Inherited	Permission B: Explicit Permission A: Inherited
User6, User7	BIAdministrators: Explicit BIAuthors: Inherited BIConsumers: Inherited	BIAdministrator: Explicit BIAuthor: Inherited BIConsumer: Inherited	Permission C: Explicit Permission B: Inherited Permission A: Inherited

Managing Authorization

After a user is authenticated, further access to application resources is controlled by the granting of permissions, also known as authorization. The policy store contains the system and application-specific policies and roles required for an application. A policy store can be file-based, LDAP-based or Oracle database and holds the mapping definitions between the default Oracle Retail Fusion Application's application roles, permissions and groups. Oracle Retail Fusion Application's permissions are granted by mapping groups from the identity store to application roles and permission grants located in the policy store. These mapping definitions between groups (identity store) and the application roles (policy store) are also kept in the policy store.

> **Note:** The best practice is to map groups instead of individual users to application roles. Controlling membership in a group reduces the complexity of tracking access rights for multiple individual users. Group membership is controlled in the identity store.

The system-jazn-data.xml file is installed and configured as the default policy store. You can continue to use the default store and modify it as needed for your environment, or you can migrate its data to an Oracle database.

The policy store and credential store must be of the same type in your environment. That is, both must be either filed-based, LDAP-based, or Oracle database.

Permissions must be defined in a manner that the Oracle Retail Fusion Application understands. All valid Oracle Retail Fusion Application permissions are premapped to application policies, which are in turn premapped to the default application roles. You cannot create new permissions in the policy store. However, you can customize the default application policy permission grants and application role mappings as well as create your own.

Accessing Oracle Enterprise Manager Fusion Middleware Control

Launch Fusion Middleware Control by entering its URL into a Web browser. The URL includes the name of the host and the administration port number assigned during the installation. This URL takes the following form: http://hostname:port_number/em. The default port is 7001. For more information about using Fusion Middleware Control, see *Oracle Fusion Middleware Administrator's Guide*.

To display the Security menu in Fusion Middleware Control

1. Log on to Oracle Enterprise Manager Fusion Middleware Control by entering the URL in a Web browser. For example, http://hostname:7001/em

   The Fusion Middleware Control login page is displayed.

Figure 8–2   Fusion Middlware Control Login Page
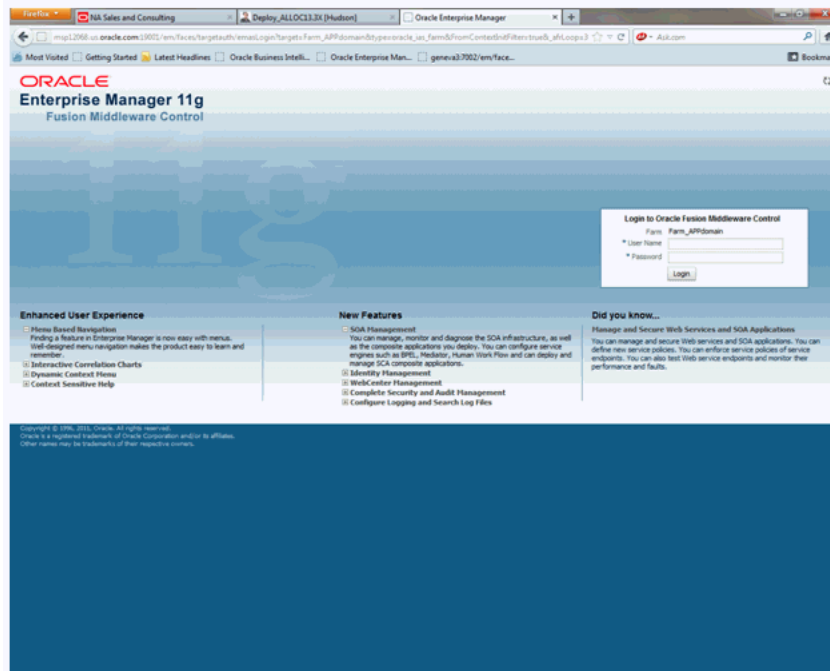
2. Enter the Oracle Retail Fusion Application's administrative user name and password and click **Login**.

    The password is the one you supplied during the installation of Oracle Retail Fusion Application. If these values have been changed, then use the current administrative user name and password combination.

3. From the target navigation pane, click **WebLogic Domain** to display **APPdomain**. Display the **Security** menu by selecting one of the following methods:

    ■   Right click **APPdomain** to display the Security menu.

    ■   Select **Security** to display a submenu.

Figure 8–3   Enterprise Manager AppDomain Security Submenu
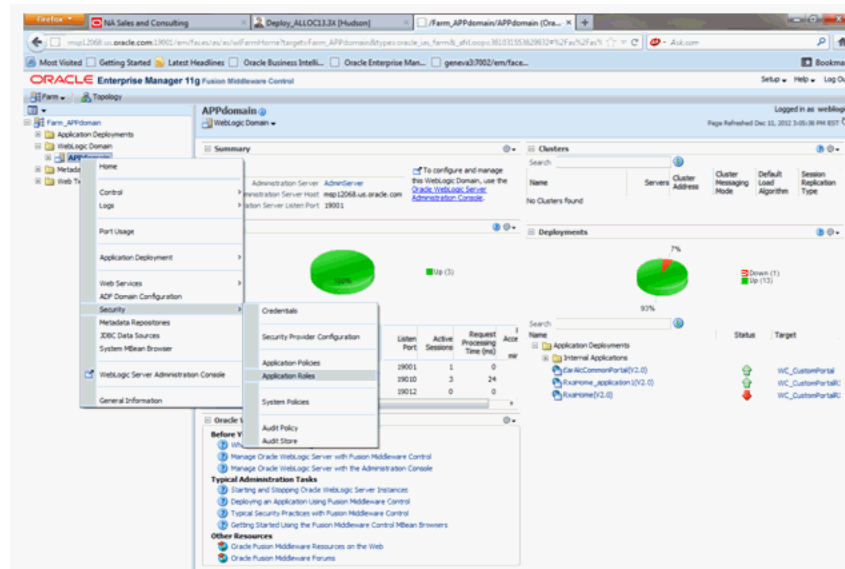
- From the content pane, go to **WebLogic Domain** menu and select **Security**
- Select **Security** to display a submenu.

Figure 8–4   Enterprise Manager WebLogic Domain Security Submenu
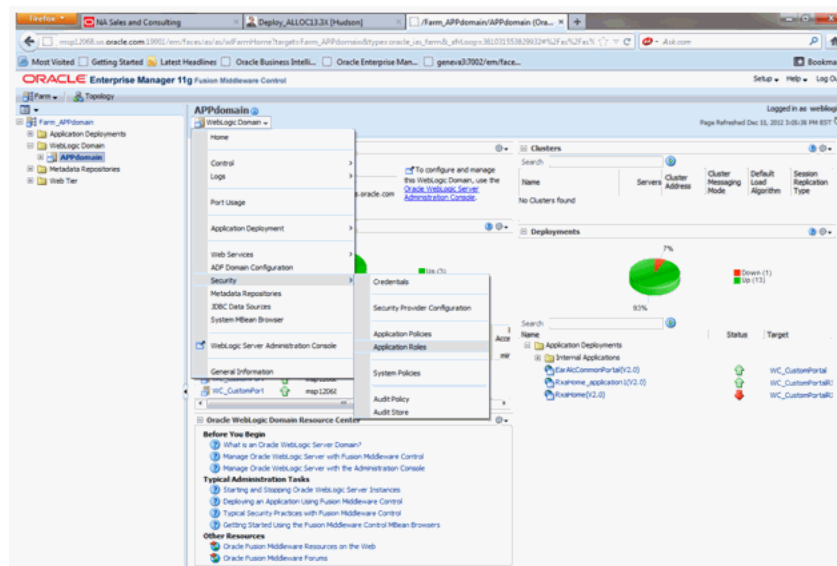
Managing the Policy Store Using Fusion Middleware Control

Use Fusion Middleware Control to manage the Oracle Retail Fusion Application's application policies and application roles maintained in the policy store whether it is filed-based, LDAP-based, or Oracle database.

> **Caution:** Oracle recommends you to make a copy of the original system-jazn-data.xml policy file and place it in a safe location. Use the copy of the original file to restore the default policy store configuration, if needed. Changes to the default security configuration may lead to an unwanted state. The default installation location is MW_HOME/user_projects/domain/your_domain/config/fmwconfig.

The following are common policy store management tasks:

- Modifying the membership of an application role. For more information, see Modifying Application Roles Using Fusion Middleware Control section.

- Creating a new application role from the beginning. For more information, see To create a new application role section.

- Creating a new application role based on an existing application role. For more information, see To create an application role based on an existing one section.

Modifying Application Roles Using Fusion Middleware Control

Members can be added or deleted from an application role using Fusion Middleware Control. You must perform these tasks while in the WebLogic Domain that Oracle Retail Fusion Application is installed in.

> **Caution:** You need to be careful when changing the permission grants and membership for the default application roles. Changes could result in an unusable system.

Valid members of an application role are groups, or other application roles. The process of becoming a member of an application role is called mapping. That is, being mapped to an application role is to become a member of an application role. The best practice is to map groups instead of individual users to application roles for easier maintenance.

To add or remove members from an application role

1. Log in to Fusion Middleware Control, navigate to **Security**, then select **Application Roles** to display the **Application Roles** page.

   For information on navigating to the Security menu, see Accessing Oracle Enterprise Manager Fusion Middleware Control section.

2. Choose **Select Application Stripe to Search**, then select the policy stripe name (example, ALC_CORE) from the list.

3. Click the search icon next to **Role Name**.

Figure 8–5   Retail Fusion Application's Application Roles Window
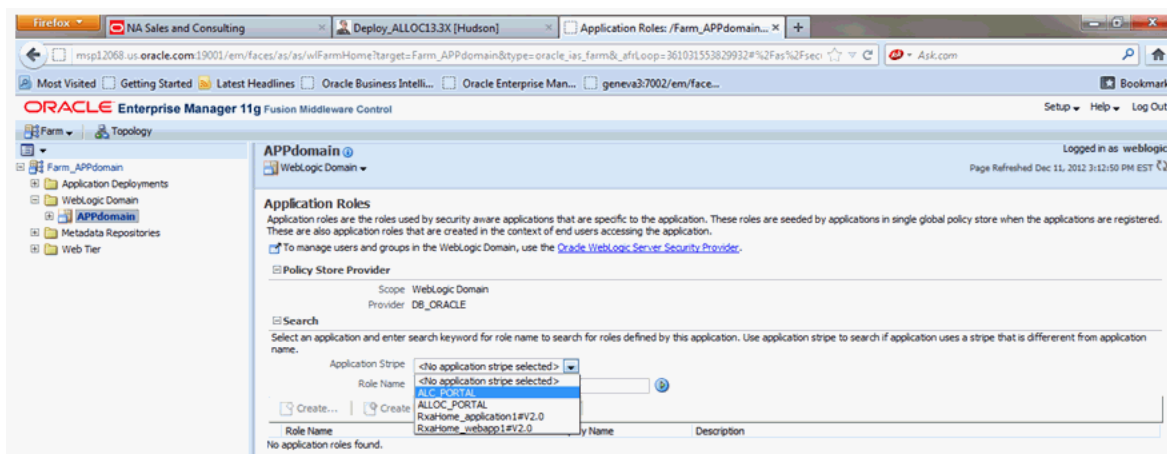
The Oracle Retail Fusion Application's application roles are displayed.

Figure 8–6 displays the default application roles.

Figure 8–6   Default Application Roles Window
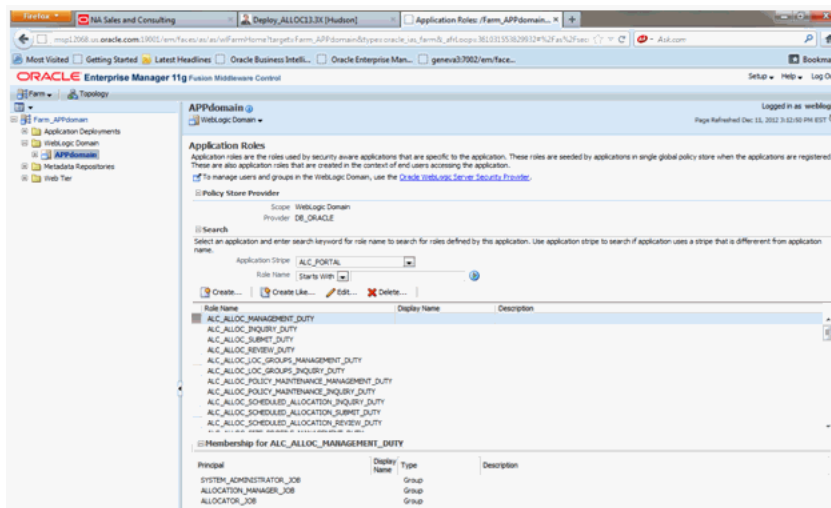
4. Select the cell next to the application role name and click **Edit** to display the **Edit Application Role** page.

Figure 8–7 shows ALC_ALLOC_MANAGEMENT_DUTY role is selected.

Figure 8–7   Edit Application Role Window
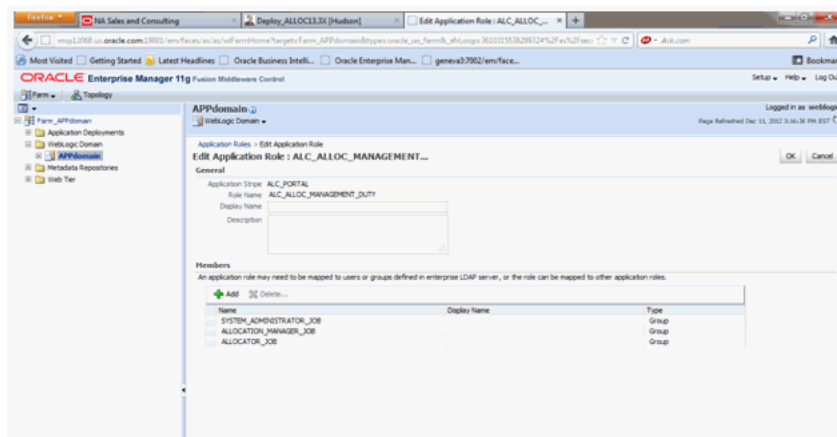
> **Note:**   You can add or delete members from the **Edit Application Role** page. The valid members are application roles, and groups

5. Select from the following options:

   - **To delete a member:** From **Members**, select from **Name** the member to activate the **Delete** button and click **Delete**.

   - **To add a member:** Click the **Add** button that corresponds to the member type being added. Select from **Add Application Role**, **Add Group**, and **Add User**.

6. For adding a member, complete **Search** and select from the available list and click **OK**.

   Figure 8–8 shows the **Add Group** dialog and after the **BUYER_JOB** group has been selected.

Figure 8–8   Add Group Dialog Window
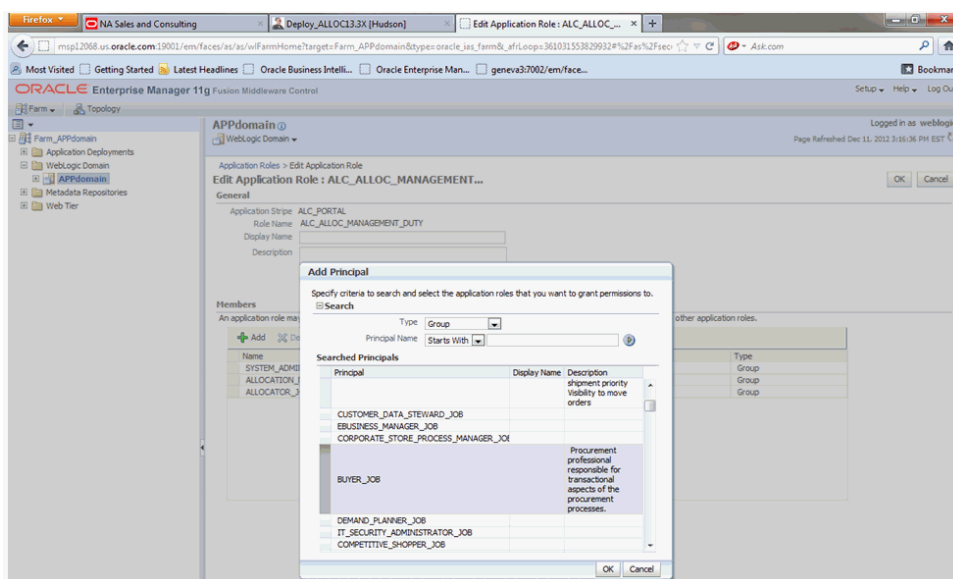
The added member displays in the **Members** column corresponding to the application role modified in the **Application Roles** page.

Creating Application Roles Using Fusion Middleware Control

Following are the two methods for creating a new application role:

- **Create New**: A new application role is created. Members can be added at the same time or you can save the new role after naming it and add members later.

- **Copy Existing**: A new application role is created by copying an existing application role. The copy contains the same members as the original, and is made a Grantee of the same application policy. You can modify the copy as needed to finish creating the new role.

To create a new application role

1. Log in to Fusion Middleware Control, navigate to **Security**, then select **Application Roles** to display the **Application Roles** page.

    For information, see Accessing Oracle Enterprise Manager Fusion Middleware Control section.

2. Choose **Select Application Stripe to Search**, and then click the search icon next to **Role Name**.

    The Oracle Retail Fusion Application's application roles displays.

3. Click **Create** to display the **Create Application Role** page. You can enter all information at once or you can enter a **Role Name**, save it, and complete the remaining fields later.

4. In the **General** section, specify the following:

    - **Role Name** - Enter the name of the application role.

    - **Display Name** - Enter the display name for the application role. This is an optional field.

    - **Description** - Enter a description for the application role.This is an optional field.

5. In the **Members** section, select the groups, or application roles to be mapped to the application role.

6. Select **Add Application Role** or **Add Group** accordingly.

7. To search in the dialog box that displays, specify the following:

    - Enter a name in **Name** field and click the blue button to search.

    - Select from the results returned in the **Available** box.

    - Click **OK** to return to the **Create Application Role** page.

    - Repeat the steps until all members are added to the application role.

8. Click **OK** to return to the **Application Roles** page.

    The application role just created displays in the table at the bottom of the page.

To create an application role based on an existing one

1. Log in to Fusion Middleware Control, navigate to **Security**, then select **Application Roles** to display the **Application Roles** page.

For more information, see Accessing Oracle Enterprise Manager Fusion Middleware Control section.

2. Choose **Select Application Stripe to Search**, and then click the search icon next to **Role Name**.

The Oracle Retail Fusion Application's application roles is displayed.

3. Select an application role from the list to enable the action buttons.

4. Click **Create Like** to display the **Create Application Role Like** page.

The **Members** section is completed with the same application roles, groups that are mapped to the original role.

5. Complete the **Role Name**, **Display Name**, and **Description** fields.

Example 8–9 shows an application role based upon ALC_ALLOC_MANAGEMENT_DUTY after being named **MyNewRole**, as an example.

Figure 8–9   Create Application Role Window
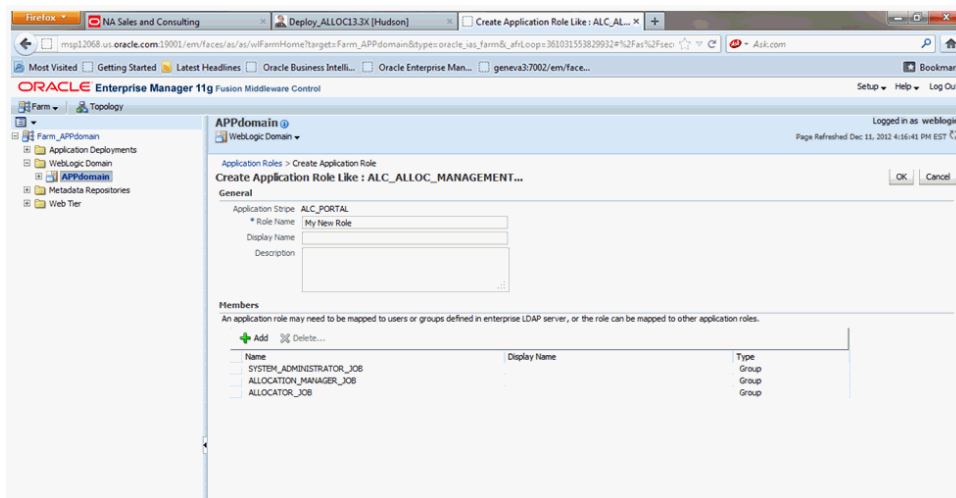
6. Use **Add** and **Delete** to modify the members as appropriate and click **OK**.

The just created application role displays in the table at the bottom of the page. The following figure shows the example **MyNewRole** that is based upon the default ALC_ALLOC_MANAGEMENT_DUTY application role.

Customizing the Default Security Configuration

You can customize the default security configuration in the following ways:

- Create new application roles. For more information, see To create a new application role section.

- Modifying membership in an Application Role. For more information, see Modifying Application Roles Using Fusion Middleware Control section.

Customizing the Policy Store

The Fusion Middleware Security model can be customized for your environment by creating your own application roles and modifying membership of application roles. Existing application roles can be modified by adding or removing members as needed.

For more information about managing application policies and application roles, see *Oracle Fusion Middleware Application Security Guide*.

> **Note:** Before creating a new application role and adding it to the default Oracle Retail Fusion Application's security configuration, familiarize yourself with how permission and group inheritance works. It is important when constructing a role hierarchy that circular dependencies are not introduced. The best practice is to leave the default security configuration in place and first incorporate your customized application roles in a test environment. For more information, see Permission Grants and Inheritance section.

Session Timeout

Session timeout is defined at the application server level. It is 60 minutes by default, but can be changed through WebLogic configuration.

9

ReST Services Security Consideration

The chapter provides the details on how to setup security for Representational State Transfer (ReST) Services.

The following topics are covered in this chapter:

- One Way SSL
- One Way SSL - ReST Services

One Way SSL

With one-way SSL, the server is required to present a certificate to the client but the client is not required to present a certificate to the server. To successfully negotiate an SSL connection, the client must authenticate the server, but the server will accept a connection from any client. One-way SSL is common on the Internet where customers want to create secure connections before they share personal data. Often, clients will also use SSL to log on in order for the server can authenticate them.

ReST Committee recommends the use of one way SSL over ReST Services for 16.0.

One Way SSL - ReST Services

Figure 9–1   One way SSL: ReST Services
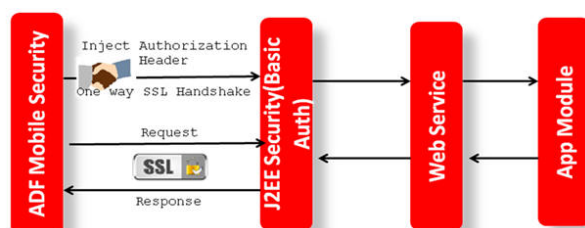
See the following sequence:

1. ADF Mobile Security Set at the Mobile Client Level to Allow Authentication.

2. ADF Mobile Client Injects Authorization Header for Every Service Call (configuration changes).

3. J2EE based Basic Authentication (SSL) is configured in the ReST Service Web Application Descriptor to allow secure connectivity to ReST Service.

Part II

Oracle Retail Merchandising System (RMS)

The following chapters provide guidance for administrators, developers, and system integrators who securely administer, customize, and integrate the Oracle Retail Merchandising System (RMS) application.

Part II contains the following chapters:

- Understanding Security
- Post Installation - Application Administration
- Extending/Customization

10

Understanding Security

This chapter covers the technical overview of the authentication process used for RMS, Oracle Retail Trade Management (RTM) using Oracle Access manager and Single Sign-On.

Further, it details the security considerations and implementations that are part of the Database, Data level security, as well as the Application layer.

The following topics are covered in this chapter:

- Security Features of the Application
- Encryption and Hashing
- Purchase Order Approval Amount

> **Note:** RTM share the same database as that of RMS. The Security features that are applicable to RMS are applicable to RTM as well.

Security Features of the Application

The security features of the Application are as follows:

- **Access Control** - It is the process of restricting access to a particular entity based upon a broad range of criteria that may or may not include the attributes related to a particular user.

- **Authentication** - It is the process of verifying the identity of a user. The authentication process usually requires a user to provide a user name and password or a combination thereof, upon signing into an application.

- **Authorization** - It is the process of checking to see if an authenticated user has the privilege to access particular system functionality.

- **Data Authorization** - It is the process of determining an authenticated user's rights to act upon a particular set of data. This process typically checks if the authenticated user is linked to a certain level in the organization hierarchy and/or a certain level in the merchandise hierarchy.

- **Role-Based Access** - Within the Oracle Retail's systems, users are assigned to different roles. The role logical grouping has different access rights to specific functions within the various Oracle Retail Systems.

- **User Store** - It is a repository that holds user data required for authentication and authorization processes.

In order to ensure users are limited to parts of the application and information that is relevant to their business role, RMS has a three-tier security structure.

The three levels of security offered by RMS are as follows:

- **Database-level security** - This is a built in feature of Oracle Database, based on database roles.

- **Application-level security** - This is the screen-level security based on Application User roles.

- **Data-level security** - This is built into RMS to give a client the ability to further limit user access to information.

Database-level security

For information on this section, see Chapter 2.

Application-level security

The Application-level security requires the users to authenticate at login and restricts them to resources only for which they are authorized.

The user's access to either entire areas of the system (for example, Purchase Orders) the modes in which users can access areas (for example, viewing Purchase Orders only) will be restricted through this.

The users are associated to groups that are mapped to application roles.The application specific permissions are granted to these security roles. For more information on the security roles, see Table 11–1.

Data-level security

Data-level security restricts user access to specific data within the merchandising system. The client has the ability to limit user data access both from a merchandise hierarchy perspective and organizational hierarchy perspective. For example, a buyer for the Small Appliances department could have data level security put in place so that they only have the ability to access items within the Small Appliances department. This prevents users from accessing information that does not pertain to their job.

Unlike the other layers of security, this level of security can be configured by the client in the RMS through the Data Upload utility available in the Application.

1. Data level security is defined at the group level in RMS.

2. For a user to have access to any data, the LDAP user ID used to login to the RMS application must be defined in the SEC_USER table as an 'APPLICATION_USER_ID'.

3. The user must be assigned to a security group in SEC_USER_GROUP. This is done through associating the USER_SEQ on SEC_USER assigned to the APPLICATION_USER_ID with a GROUP_ID on SEC_GROUP.

4. The security group can only access the merch hierarchies and the org hierarchies assigned to the user in FILTER_GROUP_MERCH and FILTER_GROUP_ORG respectively.

5. If a security group is NOT assigned to any data in FILTER_GROUP_MERCH or FILTER_GROUP_ORG, users in this group are considered 'super users' and will have access to all merch hierarchies or all org hierarchies respectively

Security groups are powerful tools for data authorization in RMS; however, they require significant administration. Security groups are defined on RMS tables, so it is

possible that the information can be interfaced onto these tables from an external system aware of the merchandise and organizational hierarchies.

The item/location security in RMS is based on relationships defined between groups of users and merchandise and organizational data.

The Security groups are defined on the SEC_GROUP table. These security groups are meant to define users with many job tasks who need to access the same information.

SEC_GROUP

The SEC_GROUP table stores group attributes. The Security groups allow users who need similar data to be grouped together.

- **GROUP_ID** - This contains the unique identifier associated with the security group.

- **GROUP_NAME** - This contains the name of the security group.

- **ROLE** - This contains the role that a client wants to assign to this group. This field is referenced in the code type ROLE. There are no pre-defined values for this field and it is completely user-defined. This field does not have any functionality linking it to Oracle Roles or any other type of roles used within the RMS. This field is used within the regionality dialog for searching and reporting.

The Security groups are defined in the RMS user interface. Users are added as members of a group by associations on the SEC_USER_GROUP table.

SEC_USER_GROUP

The SEC_USER_GROUP table link users.

The security groups are as follows:

- **GROUP ID** - This contains the unique identifier associated with the security group as defined in the SEC_GROUP table.

- **USER SEQ** - This contains the security user assigned to the security group. It references the user sequence defined on SEC_USER table.

SEC_USER

This table holds the database user ID and the application user ID associated with a security user.

The application user ID is copied to database session context RETAIL_CTX. APP_ USER_ID. The RMS security table SEC_USER now also holds application user ID in addition to database user ID. The data security function uses the application user ID for applying the security policy if database session context RETAIL_CTX. APP_USER_ ID is available else, it uses the logged in database ID for applying security policy.

The security groups are as follows:

- **DATABASE USER ID** - This column holds the database user login ID assigned to the security user.

- **USER SEQ** - This is a sequence generated number that uniquely identifies a security user.

- **APPLICATION USER ID** - This column holds the application user ID set up in enterprise LDAP for the security user.

The security groups can be associated with specific locations using the SEC_GROUP_ LOC_MATRIX tables.

The security group information is also used to determine the information that users have access to in RMS Search screens and LOVs/field validation. If a user is associated with a security group that has access to a limited range of items and the user searches in the item Search screen , the search will only return results that are in the items the user has access to. If the same user enters an item number in an item field, validation will ensure that the user has access to this item. Any item LOV will also display only the user 's list of items.

The intersection between security user groups and merchandise hierarchy levels are stored on the FILTER_GROUP_MERCH table.

- **SEC_GROUP_ID** - This is the ID of the User Security group as defined on the SEC_GROUP table.

- **FILTER_MERCH_LEVEL** - This is the merchandise hierarchy level assigned to the User Security Group. This can be a code representing group, department, class, or subclass.

- **FILTER_MERCH_ID** - This is a group or department included in the filtering.

- **FILTER_MERCH_ID_CLASS** - This is the class under the department which is included in the filtering.

- **FILTER_MERCH_ID_SUBCLASS** - This is the subclass under the class which is included in the filtering.

The intersection between security user groups and organizational hierarchy level is stored in FILTER_GROUP_ORG table.

- **SEC_GROUP_ID** - This is the ID of the User Security group as defined on the SEC_GROUP table.

- **FILTER_ORG_LEVEL** - This is the Organization hierarchy level assigned to the User Security Group. The valid values are contained in the CODE_DETAIL table with a CODE_TYPE of FLOW.

- **FILTER_ORG_ID** - This is the ID of the Organization hierarchy level assigned to the User Security Group.

RMS includes two install scripts that sets up some of this security information. The install script superGroup.sql creates a security group that must not to be associated with any level of the merchandise or organizational hierarchy. Members of this group will have access to all data in the Application. The install script superUser.sql associates the user running the script with the superUser group, and therefore ensures that the user running the script will have access to all data in the system.

RMS Users and Data Security

You need to create user roles within RMS and provide users with a mechanism for accessing the system. When security is leveraged, it controls a user's access to individual application functions and data sets.

Users in RMS are set up by the database administrator using a user creation script.

The Database Roles are created in RMS. Object level privileges are assigned to the roles that are created. Then business users are created and assigned these roles, hence allowing users to have access to objects for all the roles that are assigned to them.

A sample script is packaged with the product which contains privileges for the following:

1. DELETE tables

2. EXECUTE type, procedure, package, and function

3. INSERT into tables and views

4. SELECT sequence, table, view, and materialized view (except four ReSA tables SA_TRAN_TENDER_REV, SA_BANK_ACH, SA_TRAN_TENDER, SA_BANK_STORE)

5. UPDATE table (except four ReSA tables SA_TRAN_TENDER_REV, SA_BANK_ACH, SA_TRAN_TENDER, SA_BANK_STORE)

> **Note:**
>
> - System level privileges like *Execute Any*, *Select Any*, *Insert Any*, should not be granted to the users or to the roles. Granting such privileges would override the object level privileges described above as the user would have access to perform any action beyond his duty
>
> - Packages, procedures, and functions in RMS are defined as AUTHID CURRENT_USER to execute using only the privileges of the user that invokes it. Certain packages that require schema owner privileges are exempted from this change.

Each RMS database user has synonyms to the master RMS schema and is able to update and modify data within that schema, and cannot change the structure of the tables and objects. This user structure is specific to RMS and RTM. Applications such as RPM, Allocation, and ReIM use other means to manage users. User management for each application is discussed within its respective section.

When all of the security tools for RMS are effectively leveraged by a client a user can become a powerful tool to not only grant access to a system, but to ensure that every employee is systematically focused on the aspect of the client's business that they are responsible for.

Encryption and Hashing

Encryption and hashing techniques are a part of Oracle Advanced Security, hence System and Database Administrators are recommended to refer *Oracle Database Advanced Security Administrator's Guide 12 C Release 1* for more details.

The details of encryption and hashing are as follows:

- ORDCUST and SVC_FULFILORDCUST tables are in encrypted tablespace as it stores sensitive information about the customers.

- RETAIL_SERVICE_REPORT_URL table is used to hold the retail service code, retail service name, and URL for the Web services for Oracle Retail Financial Integration (RFI). The column sys_account is an encrypted column which stores the system account name.

- The function that perform encryption/decryption are further maintained as wrapped PLSQL functions.

For more information on Merch Mobile Security Consideration, see ReST Services Security Consideration chapter.

For more information on ReST Services Security Consideration, see the *Applications Operations Guide*.

Purchase Order Approval Amount

The Order Approval amount which determines the upper limit a user can approve on an order can be restricted through the application user roles.

- If a user has the privilege to approve a purchase order in RMS, the user can only approve an order up to a certain monetary amount. This limit is defined at the role level in RMS

- For a user to approve any order amount, the LDAP user id used to login to the RMS application (e.g. RMS_ADMIN) must be defined in the SEC_USER table as an 'APPLICATION_USER_ID'.

- The USER_SEQ on SEC_USER associated with the APPLICATION_USER_ID must be assigned to a security ROLE in the SEC_USER_ROLE table.

- The security ROLE must be defined on the RTK_ROLE_PRIVS table. ORD_APPR_ AMT on RTK_ROLE_PRIVS indicates the upper limit that the role is allowed to approve on an order. ORD_APPR_AMT is an optional field. If not defined, then the role can approve any order amount.

> **Note:** To avoid errors, make sure you have set up the Purchase Order Approver permissions to access the Buyer Dashboard.

11

Post Installation - Application Administration

This chapter covers the administration tasks performed during post installation of RMS application. The section covers the roles and permissions granted for Oracle Advanced Queuing, setting up table level auditing through the application UI, Security Policies around views, formweb.cfg, and the steps to secure the Webservice calls.

This chapter covers the following topics:

- Application Security Configuration
- Data Security Views
- Other Common Application Administration
- Post Installation Steps for Webservice Security

Application Security Configuration

Access control of system resources is achieved by requiring users to authenticate at login and by restricting users to only those resources for which they are authorized. A default security configuration is available for immediate use after the Oracle Retail Fusion application is installed and is configured to use the Oracle Fusion Middleware security model. The default configuration includes 11 predefined security roles for application specific permission grants. Users can be added to predefined groups that are mapped to pre-configured application roles. RMS is pre-configured to grant specific application permissions.

Table 11–1   Privileges

Name	Description
View Application Administration Priv	This privilege provides view access to the System Options screen, the Download Blank Template and the Foundation Data Download screens. Within the Foundation Data Download screen, this privilege provides access to download the following to a spreadsheet: Codes and Descriptions, Custom Flex Attribute Foundation, Languages, Error Messages, Security Users, Security Groups, Associate Users to Groups, Associate Locations to Groups, Filter Groups, and/or Role and Privileges.

Table 11–1 (Cont.) Privileges

Name	Description
Maintain Application Administration Priv	This privilege provides create/edit access to the System Options, the Foundation Data Download, the Foundation Data Upload, and the Foundation Data Issues screens. Foundation Data that can be created and maintained via spreadsheets with this privilege includes Codes and Descriptions, Custom Flex Attribute Foundation, Languages, Error Messages, Security Users, Security Groups, Associate Users to Groups, Associate Locations to Groups, Filter Groups, and Role and Privileges.
View Report Options Priv	A privilege for viewing Report Options and department level Report Option Exceptions.
Maintain Report Options Priv	A privilege for creating and maintaining Report Options and department level Report Option Exceptions.
View Translations Priv	This privilege provides view access to the centralized data 'Translations' screen.
Maintain Translations Priv	This privilege provides edit access to the centralized data 'Translations' screen.
View Asynchronous Jobs Priv	This privilege provides view access to the Asynchronous Job Log and the Data Loading Status screens.
Maintain Asynchronous Jobs Priv	This privilege provides edit access to the Data Loading Status, the Cost Event Search, and the Cost Event screens.
Maintain Custom Flex Attributes Priv	A privilege for creating and maintaining Custom Flex Attribute definitions.
View Custom Flex Attributes Priv	A privilege for viewing Custom Flex Attribute definitions.
View Foundation Data through Spreadsheet Priv	Gives users ability to download supporting data for Inventory, Price and Cost, and Items.
Maintain Foundation Data through Spreadsheet Priv	Gives users ability to upload supporting data for Inventory, Price and Cost, and Items.
View Competitive Shop Priv	A privilege for viewing Competitive Shop information including assignment of competitors to stores, viewing competitive price history.
Maintain Competitive Shop Priv	A privilege for creating and editing Competitive Shop information including Assigning Competitors to Stores, creating shop requests.
Approve Contracts Priv	A privilege for approving contracts.
Search Contracts Priv	A privilege for searching for contracts
View Contracts Priv	A privilege for viewing contracts and contract cost history.
Maintain Contracts Priv	A privilege for creating and maintaining contracts. Including creating orders from contracts.
Submit Contracts Priv	A privilege for submitting contracts.
Approve Cost Changes Priv	A privilege for approving cost changes.

Table 11–1 (Cont.) Privileges

Name	Description
Search Cost Changes Priv	A privilege for searching for cost changes.
View Cost Changes Priv	A privilege for viewing cost changes.
Maintain Cost Changes Priv	A privilege for creating and maintaining cost changes.
Submit Cost Changes Priv	A privilege for submitting cost changes.
View Cost Zones Priv	A privilege for viewing Cost Zone Groups and Cost Zones.
Maintain Cost Zones Priv	A privilege for creating and maintaining Cost Zone Groups and Cost Zones.
View Buyer Dashboard Priv	This privilege gives the user access to the Buyer Dashboard.
View Finance Analyst Dashboard Priv	This privilege gives the user access to the Finance Analyst Dashboard.
View Inventory Analyst Dashboard Priv	This privilege gives the user access to the Inventory Analyst Dashboard.
View Data Steward Dashboard Priv	This privilege gives the user access to the Data Steward Dashboard.
Approve Deals Priv	A privilege for approving deals.
Search Deals Priv	A privilege for searching for deals.
View Deals Priv	A privilege for viewing deals.
Maintain Deals Priv	A privilege for creating and maintaining deals.
Submit Deals Priv	A privilege for submitting deals.
View Expense Profiles Priv	A privilege for viewing Expense Profiles for Suppliers, Partners, and Countries.
Maintain Expense Profiles Priv	A privilege for creating and expenses Expense Profiles for Suppliers, Partners, and Countries.
View Up Charges Priv	A privilege for viewing the association of Up Charges with Departments.
Maintain Up Charges Priv	A privilege for creating and editing the association of Up Charges with Departments.
Maintain Average Cost Priv	A privilege for creating average cost adjustments and viewing transaction data.
View Budgets Priv	A privilege for the ability to download Monthly Budget and Open to Buy information as well as viewing the Open to Buy dashboard report.
Maintain Budgets Priv	Gives users ability to upload and download Monthly Budget and Open to Buy information.
View Finance Admin Priv	Gives users ability to download supporting data for GL Cross Reference, VAT, Terms, Currency Exchange Type Mapping, Currency, and Non-Merchandise Codes.
Maintain Finance Admin Priv	Gives users ability to upload and download supporting data for GL Cross Reference, VAT, Terms, Currency Exchange Type Mapping, Currency, and Non-Merchandise Codes.

Table 11–1 (Cont.) Privileges

Name	Description
View Financial Control Priv	Gives users ability to download Half Data Budget.
Maintain Financial Control Priv	Gives users ability to upload and download Half Data Budget.
View GL Drill Back Priv	A privilege for viewing Fixed Deal Transaction Data and GL drill back information.
View Transaction Data Priv	A privilege for viewing Transaction Data and Late Posted Transactions dashboard report.
View Franchise Cost Priv	A privilege for viewing franchise cost templates and cost relationships.
Maintain Franchise Cost Priv	A privilege for creating and maintaining franchise cost templates and cost relationships.
View Franchise Foundation Priv	Gives users ability to download supporting data for Deal Pass Through and Franchise Customers.
Maintain Franchise Foundation Priv	Gives users ability to upload and download supporting data for Deal Pass Through and Franchise Customers.
Approve Franchise Orders and Returns Priv	A privilege for approving franchise orders and returns.
View Franchise Orders and Returns Priv	A privilege for viewing franchise orders and returns.
Maintain Franchise Orders and Returns Priv	A privilege for creating and maintaining franchise orders and returns.
Search Actual Landed Cost Priv	A privilege for searching for actual landed cost.
View Actual Landed Cost Priv	A privilege for viewing actual landed cost.
Finalize Actual Landed Cost Priv	A privilege for finalizing actual landed cost.
Confirm Customs Entries Priv	A privilege for confirming customs entries.
Search Customs Entries Priv	A privilege for searching for customs entries.
View Customs Entries Priv	A privilege for viewing customs entries.
Maintain Customs Entries Priv	A privilege for creating and maintaining customs entries.
Submit Customs Entries Priv	A privilege for submitting/sending customs entries.
View Import Foundation Priv	Gives users ability to download supporting data for the import process, including Freight Sizes, Freight Types, HTS Headings, HTS Heading Restraints, Quota Categories, HTS Import Country Setup, Tariff Treatments, Origin Country Tariff Treatments, OGAs, SCACs and timelines. Also included is the ability to download HTS definitions which include HTS, HTS Tariff Treatments, HTS Tariff Treatment Zones, HTS Fees, HTS Fee Zones, HTS Taxes, HTS Tax Zones, HTS Anti-Dumping, HTS Countervailing Duty, HTS Reference and HTS Other Government Agencies.

Table 11–1   (Cont.) Privileges

Name	Description
Maintain Import Foundation Priv	Gives users ability to download and upload supporting data for the import process, including Freight Sizes, Freight Types, HTS Headings, HTS Heading Restraints, Quota Categories, HTS Import Country Setup, Tariff Treatments, Origin Country Tariff Treatments, OGAs, SCACs and timelines. Also included is the ability to download HTS definitions which include HTS, HTS Tariff Treatments, HTS Tariff Treatment Zones, HTS Fees, HTS Fee Zones, HTS Taxes, HTS Tax Zones, HTS Anti-Dumping, HTS Countervailing Duty, HTS Reference and HTS Other Government Agencies.
View Import Items Priv	A privilege for viewing import items, including, Item Suppliers, Item Supplier Countries, Item HTS, Item Import Attributes and Item Eligible Tariff Treatments.
Maintain Import Items Priv	A privilege for maintaining import items, including, Item Suppliers, Item Supplier Countries, Item HTS, Item Import Attributes, Item Eligible Tariff Treatments.
Approve Letters of Credit Priv	A privilege for approving letters of credit.
Confirm Letters of Credit Priv	A privilege for confirming letters of credit.
Search Letters of Credit Priv	A privilege for searching for letters of credit.
View Letters of Credit Priv	A privilege for viewing letters of credit.
Maintain Letters of Credit Priv	A privilege for creating and maintaining letters of credit.
Submit Letters of Credit Priv	A privilege for submitting letters of credit.
Approve Obligations Priv	A privilege for approving obligations.
Search Obligations Priv	A privilege for searching for obligations.
View Obligations Priv	A privilege for viewing obligations.
Maintain Obligations Priv	A privilege for creating and maintaining obligations.
Search Transportation Priv	A privilege for searching for transportation records.
View Transportation Priv	A privilege for viewing transportation records.
Finalize Transportation Priv	A privilege for finalizing transportation records, generating customs entries.
Maintain Transportation Priv	A privilege for creating and maintaining transportation records.
Maintain Inventory Adjustments Priv	A privilege for creating inventory adjustments by item or by location, breaking sellable packs, and creating and maintaining product transformations.

Table 11–1   (Cont.) Privileges

Name	Description
View Item Inventory and Sales Priv	A privilege for view item inventory and sales information via the Item Location Inventory, Store Sales/Issues by Location, and Sellable Pack Inquiry screens, as well as the Daily Sales, Inventory Variance to Forecast, Inventory by Store, and Inventory by Warehouse, Unexpected Inventory, and Negative Inventory dashboard reports.
Approve Intercompany Transfers Priv	A privilege for approving intercompany transfers. It is expected that a user with this privilege will also have the ability to view and maintain both intercompany and non-intercompany transfers.
View Intercompany Transfers Priv	A privilege for viewing intercompany transfers. It is expected that a user with this privilege will also have the View Transfers Priv.
Maintain Intercompany Transfers Priv	A privilege for creating and maintaining intercompany transfers. It is expected that a user with this privilege will also have the ability to view, create and maintain non-intercompany transfers.
Submit Intercompany Transfers Priv	A privilege for submitting intercompany transfers. It is expected that a user with this privilege will also have the ability to view, create and maintain non-intercompany transfers.
Approve MRTs Priv	A privilege for approving mass return transfers (MRTs).
Search MRTs Priv	A privilege for searching for mass return transfers (MRTs).
View MRTs Priv	A privilege for viewing mass return transfers (MRTs).
Maintain MRTs Priv	A privilege for creating and maintaining mass return transfers (MRTs).
Submit MRTs Priv	A privilege for submitting mass return transfers (MRTs).
Approve RTVs Priv	A privilege for approving mass return transfers (MRTs).
Search RTVs Priv	A privilege for searching for returns to vendors (RTVs).
View RTVs Priv	A privilege for viewing returns to vendors (RTVs) and Overdue RTVs dashboard report.
Maintain RTVs Priv	A privilege for creating and maintaining returns to vendors (RTVs).
View Shipments and Receipts Priv	A privilege for viewing shipment and receipt information via the Transportation Shipments, BOL Search, BOL, Shipment Search, Shipment, and Appointments screens, as well as the Early/Late Shipments and Stock Orders Pending Close dashboard reports.

Table 11–1   (Cont.) Privileges

Name	Description
Maintain Shipments and Receipts Priv	A privilege for creating and maintaining shipment and receipt information via the BOL Search, BOL, Receive by Carton, Receive by Item, Adjust Receipts, Shipment Search, Shipment, Order Shipment, MRT, Transfer, RTV, Stock Order Reconciliation, screens, as well as the Stock Orders Pending Close dashboard report.
	A user with this privilege will be able to close mass return transfers (MRTs), assuming they have the Maintain MRTs Priv as well. A user with this privilege will be able to ship returns to vendors (RTVs), assuming they have the Maintain RTVs Priv as well. A user with this privilege will be able to ship and close transfers, assuming they have the Maintain Transfers Priv.
Approve Transfers Priv	A privilege for approving transfers via the Transfer screen or the Transfers Pending Approval dashboard report.
View Transfers Priv	A privilege for viewing transfers and appointments via the Transfer Search and Appointments screens, as well as the Overdue Transfers and Transfers Pending Approval dashboard reports.
Search Transfers Priv	A privilege for searching for transfers via the Transfer Search screen.
Maintain Transfers Priv	A privilege for creating and maintaining transfers via the Transfer Search and Transfer screens, as well as the Unexpected Inventory, Overdue Transfers and Transfers Pending Approval dashboard reports.
Submit Transfers Priv	A privilege for submitting transfers via the Transfer screen.
Maintain Transfers with Finishing Priv	This priv allows users to create multi-leg transfers with finishers. Without this priv users can only create single leg transfers.
View Diffs Priv	A privilege for viewing Diffs including Diff Groups, Diff Ranges, and Pack Templates.
Maintain Diffs Priv	A privilege for creating and maintaining Diffs including Diff Groups, Diff Ranges, and Pack Templates.
Use Diffs Priv	The privilege provides access to the Diff Matrix, Diff Distribution, Re-distribution by Diff, and the Order, Transfer and Contract Parent/Diff Summary contextual reports. This privilege also provides access to the Differentiators container in the Item screen.
Search Diff Ratios Priv	A privilege for searching for Diff Ratios.
View Diff Ratios Priv	A privilege for viewing Diff Ratios.
Maintain Diff Ratios Priv	A privilege for creating and maintaining Diff Ratios.

Table 11–1   (Cont.) Privileges

Name	Description
Maintain/View Grocery Attributes Priv	A privilege for access to grocery attributes for grocery items.
Approve Items Priv	A privilege for approving items.
Search Items Priv	A privilege for searching for Items.
View Item Lists Priv	A privilege for viewing item lists.
Maintain Item Lists Priv	A privilege for creating and maintaining item lists.
View Item Locations Priv	A privilege for viewing item location information including Item Up Charges and Scheduled Item Maintenance, also to view WAC Variance dashboard report.
Maintain Item Locations Priv	A privilege for maintaining item location information including Item Up Charges, Scheduled Item Maintenance, using Item Lists, and Mass Change Item/Location Attributes.
Maintain Items Priv	A privilege for creating and editing Items, including Item Zone Retail, Item Seasons, Item Attributes, Item Timelines, Item UDAs, Item VAT, Images, Item Differentiators, Item Children, Mass Change Item Attributes, Simple Pack Setup, Pack Details, Item Approval Errors, Ticketing, Orders by Item, Item Transformation, Item Countries, Item Expenses and putting items back to Worksheet status.
Submit Items Priv	A privilege for submitting items.
View Item Suppliers Priv	A privilege for viewing item supplier relationships and sourcing information including Item Supplier Country of Manufacture, Item Supplier Country List, Item Supplier UOM, Item Supplier Country of Sourcing, Item Supplier Country Dimensions, Item Bracket Costing, Item Expenses, Item Supplier Country Locations and the Lead Time Days dashboard report.
View Price Change History Priv	A privilege for viewing price change history information through the Price Change History screen.
Maintain Ticket Requests Priv	A privilege for creating ticket printing requests through the Ticket Request screen.
View Stores Priv	A privilege for viewing Stores, including Addresses, CFAS, Store Location Traits and Walk Through Stores.
View Warehouses Priv	A privilege for viewing Physical and Virtual Warehouses, including Warehouse Department Parameters, Addresses and CFAS.
Search Location Lists Priv	A privilege for searching for Location Lists.
View Location Lists Priv	A privilege for viewing Location Lists, including Location List Criteria and Location List Details.
Maintain Location Lists Priv	A privilege for creating and editing Location Lists, including Location List Criteria and Location List Details.

Table 11–1   (Cont.) Privileges

Name	Description
Maintain Stores Priv	A privilege for creating and editing Stores, including Addresses, CFAS, Store Location Traits and Walk Through Stores.
Maintain Warehouses Priv	A privilege for creating and editing Physical and Virtual Warehouses, including Warehouse Department Parameters, Addresses and CFAS.
View Supply Chain Network Priv	A privilege for viewing Supply Chain Network information including Priority Groups, Location Activity Schedules, Warehouse Department Parameters, Transit Times, and Supplier and Location Delivery Schedules.
Maintain Supply Chain Network Priv	A privilege for creating and editing Supply Chain Network information including Priority Groups, Location Activity Schedules, Warehouse Department Parameters, Transit Times, and Supplier and Location Delivery Schedules.
Search Merchandise Hierarchy Priv	A privilege for searching for Pending Merchandise Hierarchy changes.
View Classes Priv	A privilege for viewing Classes, including CFAS.
View Departments Priv	A privilege for viewing Departments, including CFAS.
View Divisions Priv	A privilege for viewing Divisions.
View Groups Priv	A privilege for viewing Groups.
View Merchandise Hierarchy Defaults Priv	A privilege for viewing Merchandise Hierarchy Defaults and UDA Defaults for departments, classes, and subclasses.
View Merchandise Hierarchy Priv	The View Merchandise Hierarchy Priv provides ability to access the Pending Merchandise Hierarchy changes and to the Merchandise Hierarchy screen to view all levels of the merchandise hierarchy. In order to access further details of entities at each level of the hierarchy, the view privileges specific to each entity are used.
View Subclasses Priv	A privilege for viewing Subclasses, including CFAS.
Maintain Classes Priv	A privilege for creating and editing Classes, including CFAS.
Maintain Departments Priv	A privilege for creating and editing Departments, including CFAS. Also provides access to update budget information from the Cumulative Markon Variance dashboard report.
Maintain Divisions Priv	A privilege for creating and editing Divisions.
Maintain Groups Priv	A privilege for creating and editing Groups.
Maintain Merchandise Hierarchy Defaults Priv	A privilege for creating and editing Merchandise Hierarchy Defaults and UDA Defaults for departments, classes, and subclasses.
Maintain Merchandise Hierarchy Priv	A privilege for editing Pending Merchandise Hierarchy changes.

Table 11–1   (Cont.) Privileges

Name	Description
Maintain Reclassifications Priv	A privilege for maintaining merchandise hierarchy relationships.
Maintain Subclasses Priv	A privilege for creating and editing Subclasses, including CFAS.
View Areas Priv	A privilege for viewing Areas.
View Chains Priv	A privilege for viewing Chains.
View Districts Priv	A privilege for viewing Districts.
View Organizational Hierarchy Priv	A privilege for viewing the Organization Hierarchy.
View Regions Priv	A privilege for viewing Regions.
Maintain Areas Priv	A privilege for creating and editing Areas.
Maintain Chains Priv	A privilege for creating and editing Chains..
Maintain Districts Priv	A privilege for creating and editing Districts.
Maintain Regions Priv	A privilege for creating and editing Regions.
Maintain DSD Orders Priv	A privilege for creating Direct to Store Delivery (DSD) orders.
Maintain Pre-Issued Order Numbers Priv	A privilege for creating pre-issued order numbers and creating order using pre-issued numbers.
Approve Purchase Orders Priv	A privilege for approving purchase orders and viewing the Orders Pending Approval dashboard report..
Search Purchase Orders Priv	A privilege for searching for purchase orders.
View Purchase Orders Priv	A privilege for viewing purchase orders and viewing the Past Not After Date, Orders to Close, Never Approved, Once Approved, Missing Orders Data, Items Missing Data and Open Orders dashboard reports.
Close Purchase Orders Priv	A privilege for closing purchase orders.
Maintain Purchase Orders Priv	A privilege for creating and maintaining purchase orders.
Submit Purchase Orders Priv	A privilege for submitting purchase orders.
Maintain Receipt Adjustments by Cost Priv	A privilege for adjusting receipts by cost and viewing transaction data.
View Coupons Priv	A privilege for viewing coupons.
View Product Restrictions Priv	A privilege for viewing product restrictions.
Maintain Coupons Priv	A privilege for creating and maintaining coupons.
Maintain Product Restrictions Priv	A privilege for creating and maintaining production restrictions.
View Replenishment Attributes Priv	A privilege for viewing replenishment attributes.
Maintain Replenishment Attributes Priv	. privilege for creating and maintaining replenishment attributes.

Table 11–1 (Cont.) Privileges

Name	Description
View Required Documents Priv	.A privilege for viewing the association of Required Documents with Suppliers, Partners, HTS Headings/Chapters, Countries, Letters of Credit, Letter of Credit Amendments, Items, Orders, and Order Items.
Maintain Required Documents Priv	A privilege for creating and editing the association of Required Documents with Suppliers, Partners, HTS Headings/Chapters, Countries, Letters of Credit, Letter of Credit Amendments, Items, Orders, and Order Items.
View Stock Count Units Priv	A privilege for viewing stock count results and viewing the Stock Count Unit Variance dashboard report.
View Stock Counts Priv	A privielge for viewing stock count requests and viewing the Stock Counts Missing dashboard report.
Maintain Stock Count Units Priv	A privilege for maintaining stock count results, unit variance and adjustments, and virtual warehouse distribution.
Maintain Stock Counts Priv	A privilege for creating and maintaining stock count requests.
Maintain Stock Count Values Priv	A privilege for maintaining stock count value variance and adjustments.
View Stock Ledger Priv	A privilege for viewing the stock ledger and viewing the Cumulative Markon Variance and Shrinkage Variance dashboard reports.
Maintain Stock Ledger Priv	A privilege for maintaining the stock ledger.
Activate Partners Priv	A privilege for activating a Partner.
Deactivate Partners Priv	A privilege for deactivating a Partner.
Search Partners Priv	A privilege for searching for Partners.
View Partners Priv	A privilege for viewing Partners including Partner Address and Invoice Matching Attributes.
Maintain Partners Priv	A privilege for creating and editing Partners including Partner Address, Invoice Matching Attributes and CFAS via the Address screen.
Activate Suppliers Priv	A privilege for activating a supplier.
Deactivate Suppliers Priv	A privilege for deactivating a supplier.
Search Suppliers Priv	A privilege for searching for Suppliers.
View Suppliers Priv	A privilege for viewing Suppliers, including Supplier Address, EDI, Returns, Traits, Import Attributes, Invoice Matching Attributes, Importer/Exporter, Routing Location, CFAS, and Org Unit information.
View Supplier Inventory Management Priv	A privilege for creating and editing Supplier Inventory Management information including Supplier Brackets.

Table 11–1   (Cont.) Privileges

Name	Description
Maintain Supplier Inventory Management Priv	A privilege for creating and editing Supplier Inventory Management information including Supplier Brackets.
Maintain Suppliers Priv	A privilege for creating and editing Suppliers, including Supplier Address, EDI, Returns, Traits, Import Attributes, Invoice Matching Attributes, Importer/Exporter, Routing Location, CFAS, and Org Unit information.
View VAT Priv	A privilege for viewing the association of VAT information with Departments and Items.
Maintain VAT Priv	A privilege for creating and editing the association of VAT information with Departments and Items.

Table 11–2   Duties

Duty	Description	List of Privileges
Application Admin Inquiry Duty	A duty for viewing application administrative information including system options.	View Application Administration Priv
Application Admin Management Duty	A duty for maintaining application administration information, including system options. This duty is an extension of the Application Admin Inquiry Duty.	All privileges in the Application Admin Inquiry Duty Maintain Application Administration Priv
Asynchronous Job Inquiry Duty	A duty for viewing the asynchronous job log.	View Asynchronous Jobs Priv
Asynchronous Job Management Duty	A duty for managing asynchronous jobs. This duty is an extension of the Application Admin Inquiry Duty.	All privileges included in the Asynchronous Job Inquiry Duty. Maintain Asynchronous Jobs Priv
Data Security Inquiry Duty	A duty for viewing data security definitions.	View Data Security Priv
Data Security Management Duty	A duty for maintaining data security definitions. This duty is an extension of the Data Security Inquiry Duty.	All privileges included in the Data Security Inquiry Duty. Maintain Data Security Priv
Foundation Data through Spreadsheet Inquiry Duty	A duty for viewing supporting data for Inventory, Price and Cost, and Items via downloaded spreadsheets.	View Foundation Data via Spreadsheet Priv
Foundation Data through Spreadsheet Management Duty	A duty tfor maintaining supporting data for Inventory, Price and Cost, and Items via spreadsheet downloads and uploads. This duty is an extension of the Foundation Data via Spreadsheet Inquiry Duty..	All privileges included in the Foundation Data Admin Inquiry Duty. Maintain Foundation Data via Spreadsheet Priv
Custom Flex Attributes Inquiry Duty	A duty for viewing custom flex attribute (CFAS) definitions	View Custom Flex Attributes Priv

Table 11–2   (Cont.) Duties

Duty	Description	List of Privileges
Custom Flex Attributes Management Duty	A duty for maintaining custom flex attribute (CFAS) definitions. This duty is an extension of the Custom Flex Attributes Inquiry Duty.	All privileges included in the Custom Flex Attributes Inquiry Duty. Maintain Custom Flex Attributes Priv
Report Options Inquiry Duty	A duty for viewing dashboard and contextual BI report configuration options.	View Report Options Priv
Report Options Management Duty	A duty for maintaining dashboard and contextual BI report configuration options. This duty is an extension of the Report Options Inquiry Duty.	All privileges included in the Report Options Inquiry Duty Maintain Report Options Priv
Centralized Data Translation Inquiry Duty	A duty for viewing data translations via a centralized online screen.	View Translations Priv
Centralized Data Translation Management Duty	A duty for maintaining data translations via a centralized online screen. This duty is an extension of the Centralized Data Translation Inquiry Duty.	All privileges included in the Centralized Data Translation Inquiry Duty Maintain Translations Priv
Competitor Inquiry Duty	A duty for viewing competitive shop requests and competitive price history.	View Competitive Shop Priv
Competitor Management Duty	A duty for maintaining competitive shop requests. This duty is an extension of the Competitive Shop Inquiry Duty.	All privileges included in the Competitor Inquiry Duty. Maintain Competitive Shop Priv
Contract Inquiry Duty	A duty for searching for and viewing Contracts.	Search Contracts Priv View Contracts Priv
Contract Management Duty	A duty for maintaining and submitting contracts. This duty is an extension of the Contract Inquiry Duty.	All privileges included in the Contract Inquiry Duty. Maintain Contracts Priv Submit Contracts Priv
Contract Approval Duty	A duty for approving contracts. This duty is an extension of the Contract Management Duty.	All privileges included in the Contract Management Duty. Approve Contracts Priv
Cost Change Inquiry Duty	A duty for viewing item cost changes.	View Cost Changes Priv
Cost Change Management Duty	A duty for maintaining and submitting item cost changes. This duty is an extension of the Cost Change Inquiry Duty.	All privileges included in the Cost Change Inquiry Duty. Maintain Cost Changes Priv Submit Cost Changes Priv
Cost Change Approval Duty	A duty for approving item cost changes. This duty is an extension of the Cost Change Management Duty.	All privileges included in the Cost Change Management Duty. Approve Cost Changes Priv
Cost Zone Inquiry Duty	A duty for viewing cost zones.	View Cost Zones Priv

Table 11–2   (Cont.) Duties

Duty	Description	List of Privileges
Cost Zone Management Duty	A duty for maintaining cost zones. This duty is an extension of the Cost Zone Inquiry Duty.	All privileges included in the Cost Zone Inquiry Duty. Maintain Cost Zones Priv
Deal Inquiry Duty	A duty for searching for and viewing deals.	Search Deals Priv View Deals Priv
Deal Management Duty	A duty for maintaining and submitting deals. This duty is an extension of the Deal Inquiry Duty.	All privileges included in the Deal Inquiry Duty. Maintain Deals Priv Submit Deals Priv
Deal Approval Duty	A duty for approving deals. This duty is an extension of the Deal Management Duty.	All privileges included in the Deal Management Duty. Approve Deals Priv
Expense Inquiry Duty	A duty for viewing expense profiles used to build up an item's ELC.	View Expense Profiles Priv
Expense Management Duty	A duty for maintaining expense profiles used to build up an item's ELC. This duty is an extension of the Expense Inquiry Duty.	All privileges included in the Expense Inquiry Duty. Maintain Expense Profiles Priv
Up Charge Inquiry Duty	A duty for viewing department up charges.	View Up Charges Priv
Up Charge Management Duty	A duty for maintaining department up charges. This duty is an extension of the Up Charge Inquiry Duty.	All privileges included in the Up Charge Inquiry Duty. Maintain Up Charges Priv
Average Cost Management Duty	A duty for maintaining average cost values.	Maintain Average Cost Priv
GL Drill Back Inquiry Duty	A duty for viewing general ledger drill back.	View GL Drill Back Priv
Tran Data Inquiry Duty	A duty for viewing transaction data.	View Transaction Data Priv
Franchise Cost Inquiry Duty	A duty for viewing franchise cost information.	View Franchise Cost Priv
Franchise Cost Management Duty	A duty for maintaining franchise cost. This duty is an extension of the Franchise Cost Inquiry Duty.	All privileges included in the Franchise Cost Inquiry Duty. Maintain Franchise Cost Priv
Franchise Orders and Returns Inquiry Duty	A duty for viewing franchise orders and returns.	View Franchise Orders and Returns Priv
Franchise Orders and Returns Management Duty	A duty for maintaining franchise orders and returns. This duty is an extension of the Franchise Orders and Returns Inquiry Duty.	All privileges included in the Franchise Orders and Returns Inquiry Duty. Maintain Franchise Orders and Returns Priv

Table 11–2   (Cont.) Duties

Duty	Description	List of Privileges
Franchise Orders and Returns Approval Duty	A duty for approving franchise orders and returns. This is an extension of the Franchise Orders and Returns Management Duty.	All privileges included in the Franchise Orders and Returns Management Duty. Approve Franchise Orders and Returns Priv
ALC Inquiry Duty	A duty for searching for and viewing actual landed cost (ALC).	Search Actual Landed Cost Priv View Actual Landed Cost Priv
ALC Management Duty	A duty for finalizing actual landed cost (ALC).This duty is an extension of the ALC Inquiry Duty.	Search Customs Entries Priv View Customs Entries Priv
Customs Entry Inquiry Duty	A duty for searching for and viewing customs entries.	Search Customs Entries Priv View Customs Entries Priv
Customs Entry Management Duty	A duty for maintaining and submitting customs entries. This is an extension of the Customs Entry Inquiry Duty.	All privileges included in the Customs Entry Inquiry Duty. Maintain Customs Entries Priv Submit Customs Entries Priv
Customs Entry Confirmation Duty	A duty for confirming customs entries. This is an extension of the Customs Entry Management Duty.	All privileges included in the Customs Entry Management Duty. Confirm Customs Entries Priv
Import Item Inquiry Duty	A duty for viewing item data related to imports.	View Import Items Priv
Import Item Management Duty	A duty for maintaining item data related to imports. This is an extension of the Import Item Inquiry Duty.	All privileges included in the Import Item Management Duty. Maintain Import Items Priv
Letter of Credit Inquiry Duty	A duty for searching for and viewing letters of credit.	Search Letters of Credit Priv View Letters of Credit Priv
Letter of Credit Management Duty	A duty for maintaining and submitting letters of credit. This is an extension of the Letter of Credit Inquiry Duty.	All privileges included in the Letter of Credit Inquiry Duty. Maintain Letters of Credit Priv Submit Letters of Credit Priv
Letter of Credit Approval Duty	A duty for approving and confirming letters of credit. This is an extension of the Letter of Credit Management Duty.	All privileges included in the Letter of Credit Management Duty. Approve Letters of Credit Priv Confirm Letters of Credit Priv
Obligation Inquiry Duty	A duty for searching for and viewing obligations.	Search Obligations Priv View Obligations Priv
Obligation Management Duty	A duty for maintaining obligations. This is an extension of the Obligation Inquiry Duty.	All privileges included in the Obligation Inquiry Duty. Maintain Obligations Priv

Table 11–2   (Cont.) Duties

Duty	Description	List of Privileges
Obligation Approval Duty	A duty for approving obligations. This is an extension of the Obligation Management Duty.	All privileges included in the Obligation Management Duty. Approve Obligations Priv
Transportation Inquiry Duty	A duty for searching for and viewing transportation information.	Search Transportation Priv View Transportation Priv
Transportation Management Duty	A duty for maintaining transportation information.This duty is an extension of the Transportation Inquiry Duty.	All privileges included in the Transportation Inquiry Duty. Maintain Transportation Priv Finalize Transportation Priv
Transfer Approval Duty	A duty for approving transfers. This duty is an extension of the Transfer Management Duty.	All privileges included in the Transfer Management Duty. Approve Transfers Priv
Transfer with Finishing Management Duty	A duty for maintaining transfers with finishing. This duty is an extension of the Transfer Management Duty.	All privileges included in the Transfer Management Duty. Maintain Transfers with Finishing Priv
Intercompany Transfer Inquiry Duty	A duty for viewing intercompany transfers. This is an extension of the Transfer Inquiry Duty.	All privileges included in the Transfer Inquiry Duty. View Intercompany Transfers Priv
Intercompany Transfer Management Duty	A duty for maintaining and submitting intercompany transfers. This is an extension of the Transfer Management Duty and the Intercompany Transfer Inquiry Duty.	All privileges included in the Transfer Management Duty. All privileges included in the Intercompany Transfer Inquiry Duty. Maintain Intercompany Transfers Priv Submit Intercompany Transfers Priv
Intercompany Transfer Approval Duty	A duty for approving intercompany transfers. This is an extension of the Transfer Management Duty and the Intercompany Transfer Management Duty.	All privileges included in the Transfer Approval Duty. All privileges included in the Intercompany Transfer Management Duty. Approve Intercompany Transfers Priv
MRT Inquiry Duty	A duty for searching for and viewing mass return transfers (MRTs).	Search MRTs Priv View MRTs Priv
MRT Management Duty	A duty for maintaining and submitting mass return transfers (MRTs). This duty is an extension of the MRT Inquiry Duty.	All privileges included in the MRT Inquiry Duty. Maintain MRTs Priv Submit MRTs Priv
MRT Approval Duty	A duty for the approval of mass return transfers (MRTs). This duty is an extension of the MRT Management Duty.	All privileges included in the MRT Management Duty. Approve MRTs Priv

Table 11–2   (Cont.) Duties

Duty	Description	List of Privileges
RTV Inquiry Duty	A duty for searching for and viewing returns to vendors (RTVs).	Search RTVs Priv View RTVs Priv
RTV Management Duty	A duty for maintaining returns to vendors (RTVs). This duty is an extension of the RTV Inquiry Duty.	All privileges included in the RTV Inquiry Duty. Maintain RTVs Priv
RTV Approval Duty	A duty for approving returns to vendors (RTVs). This duty is an extension of the RTV Management Duty.	All privileges included in the RTV Management Duty. Approve RTVs Priv
Shipment and Receipts Inquiry Duty	A duty for viewing shipments and receipts.	View Shipments and Receipts Priv
Shipment and Receipts Management Duty	A duty for maintaining shipments and receipts. This is an extension of the Shipment and Receipts Inquiry Duty.	All privileges included in the Shipment and Receipts Inquiry Duty. Maintain Shipments and Receipts Priv
Diff Inquiry Duty	A duty for viewing differentiators.	View Diffs Priv
Diff Management Duty	A duty for maintaining differentiators. This duty is an extension of the Diff Inquiry Duty.	All privileges included in Diff Inquiry Duty. Maintain Diffs Priv
Diff Ratio Inquiry Duty	A duty for searching for and viewing differentiator ratios.	Search Diff Ratios Priv View Diff Ratios Priv
Diff Ratio Management Duty	A duty for maintaining differentiator ratios. This duty is an extension of the Diff Ratio Inquiry Duty.	All privileges included in the Diff Ratio Inquiry Duty. Maintain Diff Ratios Priv
Grocery Attribute Management Duty	A duty for viewing and maintaining grocery item related attributes.	Maintain/View Grocery Attributes Priv
Item Inquiry Duty	A duty for searching for and viewing items.	Search Items Priv View Items Priv
Item Management Duty	A duty for maintaining and submitting items. This duty is an extension of the Item Inquiry Duty.	All privileges included in the Item Inquiry Duty. Maintain Items Priv Submit Items Priv
Item Approval Duty	A duty for approving items. This duty is an extension of the Item Management Duty.	All privileges included in the Item Management Duty. Approve Items Priv
Item List Inquiry Duty	A duty for searching for and viewing item lists.	Search Item Lists Priv View Item Lists Priv
Item List Management Duty	A duty for maintaining item lists. This duty is an extension of the Item List Inquiry Duty.	All privileges included in the Item List Inquiry Duty. Maintain Item Lists Priv

Table 11–2   (Cont.) Duties

Duty	Description	List of Privileges
Item Supplier Inquiry Duty	A duty for viewing item supplier sourcing information. This is an extension of the Item Inquiry Duty.	All privileges included in the Item Inquiry Duty. View Item Suppliers Priv
Item Supplier Management Duty	A duty for maintaining item supplier sourcing information. This duty is an extension of the Item Supplier Inquiry Duty and the Item Inquiry Duty.	All privileges included in the Item Supplier Inquiry Duty. Maintain Item Suppliers Priv
Item Location Inquiry Duty	A duty for viewing item location information. This is an extension of the Item Inquiry Duty.	All privileges included in the Item Inquiry Duty. View Item Locations Priv
Item Location Management Duty	A duty for maintaining item location information. This duty is an extension of the Item Location Inquiry Duty and the Item Inquiry Duty.	All privileges included in the Item Location Inquiry Duty. Maintain Item Locations Priv
Price Change Inquiry Duty	A duty for viewing price change history.	View Price Change History Priv
Ticket Management Duty	A duty for maintaining ticket requests.	Maintain Ticket Requests Priv
Location Inquiry Duty	A duty for searching for and viewing stores and warehouses.	View Organizational Hierarchy Priv View Stores Priv View Warehouses Priv
Location Management Duty	A duty for maintaining stores and warehouses. This duty is an extension of the Location Inquiry and Organizational Hierarchy Inquiry Duties.	All privileges included in the Location Inquiry Duty. Maintain Stores Priv Maintain Warehouses Priv
Location List Inquiry Duty	A duty for searching for and viewing location lists.	Search Location Lists Priv View Location Lists Priv
Location List Management Duty	A duty for maintaining location lists. This duty is an extension of the Location List Inquiry Duty.	All privileges included in the Location List Inquiry Duty. Maintain Location Lists Priv
Supply Chain Network Inquiry Duty	A duty for viewing supplier chain network information.	View Supply Chain Network Priv
Supply Chain Network Management Duty	A duty for maintaining supply chain network information. This duty is an extension of the Supply Chain Network Inquiry Duty.	All privileges included in the Supply Chain Network Inquiry Duty. Maintain Supply Chain Network Priv

Table 11–2   (Cont.) Duties

Duty	Description	List of Privileges
Merchandise Hierarchy Inquiry Duty	A duty for searching for and viewing the merchandise hierarchy, viewing defaults defined at various levels of the merchandise hierarchy, viewing pending merchandise hierarchy changes. This also includes viewing all grouping levels of the hierarchy, Division, Group, Department, Class, and Subclass, and viewing department level up charges and VAT information.	Search Merchandise Hierarchy Priv View Merchandise Hierarchy Priv View Divisions Priv View Groups Priv View Departments Priv View Classes Priv View Subclasses Priv View Merchandise Hierarchy Defaults Priv View Up Charges Priv View VAT Priv
Merchandise Hierarchy Management Duty	A duty for creating and maintaining the grouping levels of the merchandise hierarchy, creating and maintaining defaults at various levels of the hierarchy, creating and maintaining item reclassifications and maintaining pending merchandise hierarchy changes. This also includes maintaining the details of all grouping levels of the hierarchy, Division, Group, Department, Class and Subclass, and maintaining department level up charges and VAT information. This duty is an extension of the Merchandise Hierarchy Inquiry Duty.	All privileges included in the Merchandise Hierarchy Inquiry Duty. Maintain Merchandise Hierarchy Priv Maintain Divisions Priv Maintain Groups Priv Maintain Departments Priv Maintain Classes Priv Maintain Subclasses Priv Maintain Merchandise Hierarchy Defaults Priv Maintain Reclassifications Priv Maintain Up Charges Priv Maintain VAT Priv
Organizational Hierarchy Inquiry Duty	A duty for searching for and viewing the Organization Hierarchy. This also includes viewing all grouping levels of the hierarchy, Chain, Area, Region, and District.	View Organizational Hierarchy Priv View Chains Priv View Areas Priv View Regions Priv View Districts Priv
Organizational Hierarchy Management Duty	A duty for creating and maintaining the grouping levels of the Organization Hierarchy. This includes all grouping levels of the hierarchy, Chain, Area, Region, and District. This duty is an extension of the Organizational Hierarchy Inquiry Duty.	All privileges included in the Organizational Hierarchy Inquiry Duty. Maintain Chains Priv Maintain Areas Priv Maintain Regions Priv Maintain Districts Priv
DSD Management Duty	A duty for maintaining DSD purchase orders.	Maintain DSD Orders Priv
Pre-issued Order Numbers Management Duty	A duty for generating pre-issue order numbers and creating orders using pre-issued numbers.	Maintain Pre-Issued Order Numbers Priv

Table 11–2   (Cont.) Duties

Duty	Description	List of Privileges
Purchase Order Inquiry Duty	A duty for searching for and viewing purchase orders.	Search Purchase Orders Priv View Purchase Orders Priv
Purchase Order Management Duty	A duty for maintaining and submitting purchase orders. This duty is an extension of the Purchase Order Inquiry Duty.	All privileges included in the Purchase Order Inquiry Duty. Maintain Purchase Orders Priv Submit Purchase Orders Priv
Purchase Order Approval Duty	A duty for approving purchase orders. This duty is an extension of the Purchase Order Management Duty.	All privileges included in the Purchase Order Management Duty. Approve Purchase Orders Priv
Receipt Adjustments by Cost Management Duty	A duty for creating receipt adjustments by cost.	Maintain Receipt Adjustments by Cost Priv
POS Configuration Inquiry Duty	A duty for searching for and viewing coupons and product restrictions.	View Coupons Priv View Product Restrictions Priv
POS Configuration Management Duty	A duty for maintaining coupons and product restrictions. This duty is an extension of the POS Configuration Inquiry Duty.	All privileges included in the POS Configuration Inquiry Duty. Maintain Coupons Priv Maintain Product Restrictions Priv
Replenishment Inquiry Duty	A duty for searching for and viewing replenishment attributes.	View Replenishment Attributes Priv
Replenishment Management Duty	A duty for maintaining replenishment attributes. This duty is an extension of the Replenishment Inquiry Duty.	All privileges included in the Replenishment Inquiry Duty. Maintain Replenishment Attributes Priv
Required Document Inquiry Duty	A duty for viewing required documents.	View Required Documents Priv
Required Document Management Duty	A duty for maintaining required documents. This duty is an extension of the Required Documents Inquiry Duty.	All privileges included in the Required Documents Inquiry Duty. Maintain Required Documents Priv
Stock Count Inquiry Duty	A duty for searching for and viewing stock count requests and stock count unit results.	View Stock Counts Priv View Stock Count Units Priv
Stock Count Management Duty	A duty for maintaining stock count requests and stock count unit results. This duty is an extension of the Stock Count Inquiry Duty.	All privileges included in the Stock Count Inquiry Duty. Maintain Stock Counts Priv Maintain Stock Count Units Priv
Stock Count Value Management Duty	A duty for maintaining stock count value variances and adjustments. This duty is an extension of the Stock Count Inquiry Duty.	All privileges included in the Stock Count Inquiry Duty. Maintain Stock Count Values Priv

Table 11–2 (Cont.) Duties

Duty	Description	List of Privileges
Stock Ledger Inquiry Duty	A duty for viewing the stock ledger.	View Stock Ledger Priv
Stock Ledger Management Duty	A duty for maintaining the stock ledger. This duty is an extension of the Stock Ledger Inquiry Duty.	All privileges included in the Stock Ledger Inquiry Duty. Maintain Stock Ledger Priv
Buyer Dashboard Inquiry Duty	A duty for viewing the Buyer Dashboard.	View Buyer Dashboard Priv
Finance Analyst Inquiry Duty	A duty for viewing the Finance Analyst Dashboard.	View Finance Analyst Dashboard Priv
Inventory Analyst Inquiry Duty	A duty for viewing the Inventory Analyst Dashboard.	View Inventory Analyst Dashboard Priv
Inventory Control Inquiry Duty	A duty for viewing the Inventory Control Dashboard.	View Inventory Control Dashboard Priv
Data Steward Inquiry Duty	A duty for viewing the Data Steward Dashboard.	View Data Steward Dashboard Priv
Partner Inquiry Duty	A duty for searching for and viewing partners.	Search Partners Priv View Partners Priv
Partner Management Duty	A duty for maintaining partners. This duty is an extension of the Partner Inquiry Duty.	All privileges included in the Partner Inquiry Duty. Maintain Partners Priv
Partner Activation Duty	A duty for activating or deactivating a partner. This duty is an extension of the Partner Management Duty.	All privileges included in the Partner Management Duty. Activate Partners Priv Deactivate Partners Priv
Supplier Inquiry Duty	A duty for searching for and viewing suppliers and supplier sites.	Search Suppliers Priv View Suppliers Priv
Supplier Management Duty	A duty for maintaining suppliers and supplier sites. This duty is an extension of the Supplier Inquiry Duty.	All privileges included in the Supplier Inquiry Duty. Maintain Suppliers Priv
Supplier Activation Duty	A duty for activating or deactivating a supplier or supplier site. This duty is an extension of the Supplier Management Duty.	All privileges included in the Supplier Management Duty. Activate Suppliers Priv Deactivate Suppliers Priv
Supplier Inventory Inquiry Duty	A duty for viewing supplier inventory information.	View Supplier Inventory Management Priv
Supplier Inventory Management Duty	A duty for maintaining supplier inventory information. This duty is an extension of the Supplier Inventory Inquiry Duty.	All privileges included in the Supplier Inventory Inquiry Duty. Maintain Supplier Inventory Management Priv
VAT Inquiry Duty	A duty for viewing department VAT information.	View VAT Priv
VAT Management Duty	A duty for maintaining department VAT information. This duty is an extension of the VAT Inquiry Duty.	All privileges included in the VAT Inquiry Duty. Maintain VAT Priv

Table 11–2 (Cont.) Duties

Duty	Description	List of Privileges
Import Foundation Inquiry Duty	A duty for viewing supporting data for the import process via downloaded spreadsheets.	View Import Foundation Priv
Import Foundation Management Duty	A duty for maintaining supporting data for the import process via spreadsheet downloads and uploads. This duty is an extension of the Import Foundation Inquiry Duty.	All privileges included in the Import Foundation Inquiry Duty. Maintain Import Foundation Priv

Table 11–3   Function Security Mapping

Role	Duty	List of Privileges
RMS/RTM Application Administrator	Application Admin Inquiry Duty	View Application Administration Priv
	Application Admin Management Duty	Maintain Application Administration Priv
	Report Options Inquiry Duty	Maintain Report Options Priv
	Report Options Management Duty	View Translations Priv
		Maintain Translations Priv
	Centralized Data Translation Inquiry Duty	View Asynchronous Jobs Priv
	Centralized Data Translation Management Duty	Maintain Asynchronous Jobs Priv
		Maintain Custom Flex Attributes Priv
	Asynchronous Job Inquiry Duty	
	Asynchronous Job Management Duty	View Custom Flex Attributes Priv
		View Foundation Data via Spreadsheet Priv
	Custom Flex Attributes Management Duty	Maintain Foundation Data via Spreadsheet Priv
	Custom Flex Attributes Inquiry Duty	View Competitive Shop Priv
	Foundation Data through Spreadsheet Inquiry Duty	Maintain Competitive Shop Priv
		Approve Contracts Priv
	Foundation Data through Spreadsheet Management Duty	Search Contracts Priv
	Competitor Inquiry Duty	View Contracts Priv
	Competitor Management Duty	Maintain Contracts Priv
	Contract Approval Duty	Submit Contracts Priv
	Contract Inquiry Duty	Approve Cost Changes Priv
	Contract Management Duty	View Cost Changes Priv
	Cost Change Approval Duty	Maintain Cost Changes Priv
	Cost Change Inquiry Duty	Submit Cost Changes Priv
	Cost Change Management Duty	View Cost Zones Priv
	Cost Zone Inquiry Duty	Maintain Cost Zones Priv
	Cost Zone Management Duty	View Buyer Dashboard Priv
	Buyer Dashboard Inquiry Duty	View Finance Analyst Dashboard Priv
	Finance Analyst Inquiry Duty	View Inventory Analyst Dashboard Priv
	Inventory Analyst Inquiry Duty	
	Inventory Control Inquiry Duty	View Inventory Control Dashboard Priv
	Data Steward Inquiry Duty	View Data Steward Dashboard Priv
	Deal Approval Duty	
	Deal Inquiry Duty	Approve Deals Priv
	Deal Management Duty	Search Deals Priv
	Expense Inquiry Duty	View Deals Priv
	Expense Management Duty	Maintain Deals Priv
	Up Charge Inquiry Duty	Submit Deals Priv
	Up Charge Management Duty	View Expense Profiles Priv

Table 11–3   (Cont.) Function Security Mapping

Role	Duty	List of Privileges
	Average Cost Management Duty	Maintain Expense Profiles Priv
	Budgets Inquiry Duty	View Up Charges Priv
	Budgets Management Duty	Maintain Up Charges Priv
	Finance Admin Inquiry Duty	Maintain Average Cost Priv
	Finance Admin Management Duty	View Budgets Priv
		Maintain Budgets Priv
	Financial Control Inquiry Duty	View Finance Admin Priv
	Financial Control Management Duty	Maintain Finance Admin Priv
		View Financial Control Priv
	GL Drill Back Inquiry Duty	Maintain Financial Control Priv
	Tran Data Inquiry Duty	View GL Drill Back Priv
	Franchise Cost Inquiry Duty	View Transaction Data Priv
	Franchise Cost Management Duty	View Franchise Cost Priv
		Maintain Franchise Cost Priv
	Franchise Foundation Inquiry Duty	View Franchise Foundation Priv
	Franchise Foundation Management Duty	Maintain Franchise Foundation Priv
	Franchise Orders and Returns Approval Duty	Approve Franchise Orders and Returns Priv
	Franchise Orders and Returns Inquiry Duty	View Franchise Orders and Returns Priv
	Franchise Orders and Returns Management Duty	Maintain Franchise Orders and Returns Priv
	ALC Inquiry Duty	Search Actual Landed Cost Priv
	ALC Management Duty	View Actual Landed Cost Priv
	Customs Entry Confirmation Duty	Finalize Actual Landed Cost Priv
		Confirm Customs Entries Priv
	Customs Entry Inquiry Duty	Search Customs Entries Priv
	Customs Entry Management Duty	View Customs Entries Priv
	Import Foundation Inquiry Duty	Maintain Customs Entries Priv
	Import Foundation Management Duty	Submit Customs Entries Priv
		View Import Foundation Priv
	Import Item Inquiry Duty	Maintain Import Foundation Priv
	Import Item Management Duty	View Import Items Priv
	Letter of Credit Approval Duty	Maintain Import Items Priv
	Letter of Credit Inquiry Duty	Approve Letters of Credit Priv
	Letter of Credit Management Duty	Confirm Letters of Credit Priv
	Obligation Approval Duty	Search Letters of Credit Priv
	Obligation Inquiry Duty	View Letters of Credit Priv
	Obligation Management Duty	Maintain Letters of Credit Priv
	Transportation Inquiry Duty	Submit Letters of Credit Priv
	Transportation Management Duty	Approve Obligations Priv
		Search Obligations Priv

Table 11–3   (Cont.) Function Security Mapping

Role	Duty	List of Privileges
	Inventory Adjustment Management Duty	View Obligations Priv
	Inventory and Sales Inquiry Duty	Maintain Obligations Priv
		Search Transportation Priv
	Intercompany Transfer Approval Duty	View Transportation Priv
		Finalize Transportation Priv
	Intercompany Transfer Inquiry Duty	Maintain Transportation Priv
	Intercompany Transfer Management Duty	Maintain Inventory Adjustments Priv
	MRT Approval Duty	View Item Inventory and Sales Priv
	MRT Inquiry Duty	Approve Intercompany Transfers Priv
	MRT Management Duty	
	RTV Approval Duty	View Intercompany Transfers Priv
	RTV Inquiry Duty	Maintain Intercompany Transfers Priv
	RTV Management Duty	Submit Intercompany Transfers Priv
	Shipment and Receipts Inquiry Duty	
		Approve MRTs Priv
	Shipment and Receipts Management Duty	Search MRTs Priv
		View MRTs Priv
	Transfer Approval Duty	Maintain MRTs Priv
	Transfer Inquiry Duty	Submit MRTs Priv
	Transfer Inquiry Duty AND	Approve RTVs Priv
	Intercompany Transfer Inquiry Duty	Search RTVs Priv
		View RTVs Priv
	Transfer Management Duty	Maintain RTVs Priv
	Transfer with Finishing Management Duty	View Shipments and Receipts Priv
	Diff Inquiry Duty	Maintain Shipments and Receipts Priv
	Diff Management Duty	
	Diff Ratio Inquiry Duty	Approve Transfers Priv
	Diff Ratio Management Duty	View Transfers Priv
	Grocery Attribute Management Duty	Search Transfers Priv
		Maintain Transfers Priv
	Item Approval Duty	Submit Transfers Priv
	Item Inquiry Duty	Maintain Transfers with Finishing Priv
	Item List Inquiry Duty	
	Item List Management Duty	View Diffs Priv
	Item Location Inquiry Duty	Maintain Diffs Priv
	Item Location Management Duty	Use Diffs Priv
		Search Diff Ratios Priv
	Item Management Duty	View Diff Ratios Priv
	Item Supplier Inquiry Duty	Maintain Diff Ratios Priv
	Item Supplier Management Duty	Maintain/View Grocery Attributes Priv
	Price Change Inquiry Duty	Approve Items Priv

Table 11–3 (Cont.) Function Security Mapping

Role	Duty	List of Privileges
	Ticket Management Duty	Search Items Priv
	Location Inquiry Duty	View Items Priv
	Location List Inquiry Duty	Search Item Lists Priv
	Location List Management Duty	View Item Lists Priv
	Location Management Duty	Maintain Item Lists Priv
	Supply Chain Network Inquiry Duty	View Item Locations Priv
		Maintain Item Locations Priv
	Supply Chain Network Management Duty	Maintain Items Priv
		Submit Items Priv
	Merchandise Hierarchy Management Duty	View Item Suppliers Priv
	Organizational Hierarchy Inquiry Duty	Maintain Item Suppliers Priv
		View Price Change History Priv
	Organizational Hierarchy Management Duty	Maintain Ticket Requests Priv
		View Stores Priv
	DSD Management Duty	View Warehouses Priv
	Pre-issued Order Numbers Management Duty	Search Location Lists Priv
	Purchase Order Approval Duty	View Location Lists Priv
	Purchase Order Inquiry Duty	Maintain Location Lists Priv
	Purchase Order Management Duty	Maintain Stores Priv
		Maintain Warehouses Priv
	Receipt Adjustments by Cost Management Duty	View Supply Chain Network Priv
	POS Configuration Inquiry Duty	Maintain Supply Chain Network Priv
	POS Configuration Management Duty	Search Merchandise Hierarchy Priv
	Replenishment Inquiry Duty	View Classes Priv
	Replenishment Management Duty	View Departments Priv
	Required Document Inquiry Duty	View Divisions Priv
		View Groups Priv
	Required Document Management Duty	View Merchandise Hierarchy Defaults Priv
	Stock Count Inquiry Duty	View Merchandise Hierarchy Priv
	Stock Count Management Duty	View Subclasses Priv
	Stock Count Value Management Duty	Maintain Classes Priv
		Maintain Departments Priv
	Stock Ledger Inquiry Duty	Maintain Divisions Priv
	Stock Ledger Management Duty	Maintain Groups Priv
	Partner Activation Duty	Maintain Merchandise Hierarchy Defaults Priv
	Partner Inquiry Duty	
	Partner Management Duty	Maintain Merchandise Hierarchy Priv
	Supplier Activation Duty	
	Supplier Inquiry Duty	Maintain Reclassifications Priv
	Supplier Inventory Inquiry Duty	Maintain Subclasses Priv

Table 11–3   (Cont.) Function Security Mapping

Role	Duty	List of Privileges
	Supplier Inventory Management Duty	View Areas Priv
		View Chains Priv
	Supplier Management Duty	View Districts Priv
	VAT Inquiry Duty	View Organizational Hierarchy Priv
	VAT Management Duty	View Regions Priv
		Maintain Areas Priv
		Maintain Chains Priv
		Maintain Districts Priv
		Maintain Regions Priv
		Maintain DSD Orders Priv
		Maintain Pre-Issued Order Numbers Priv
		Approve Purchase Orders Priv
		Search Purchase Orders Priv
		View Purchase Orders Priv
		Close Purchase Orders Priv
		Maintain Purchase Orders Priv
		Submit Purchase Orders Priv
		Maintain Receipt Adjustments by Cost Priv
		View Coupons Priv
		View Product Restrictions Priv
		Maintain Coupons Priv
		Maintain Product Restrictions Priv
		View Replenishment Attributes Priv
		Maintain Replenishment Attributes Priv
		View Required Documents Priv
		Maintain Required Documents Priv
		View Stock Count Units Priv
		View Stock Counts Priv
		Maintain Stock Count Units Priv
		Maintain Stock Counts Priv
		Maintain Stock Count Values Priv
		View Stock Ledger Priv
		Maintain Stock Ledger Priv
		Activate Partners Priv
		Deactivate Partners Priv
		Search Partners Priv
		View Partners Priv

Table 11–3   (Cont.) Function Security Mapping

Role	Duty	List of Privileges
		Maintain Partners Priv
		Activate Suppliers Priv
		Deactivate Suppliers Priv
		Search Suppliers Priv
		View Suppliers Priv
		View Supplier Inventory Management Priv
		Maintain Supplier Inventory Management Priv
		Maintain Suppliers Priv
		View VAT Priv
		Maintain VAT Priv

Table 11–3   (Cont.) Function Security Mapping

Role	Duty	List of Privileges
Data Steward	Application Admin Inquiry Duty	View Application Administration Priv
	Report Options Inquiry Duty	Maintain Report Options Priv
	Report Options Management Duty	View Asynchronous Jobs Priv
	Asynchronous Job Inquiry Duty	Maintain Asynchronous Jobs Priv
	Asynchronous Job Management Duty	View Foundation Data via Spreadsheet Priv
	Foundation Data through Spreadsheet Inquiry Duty	Maintain Foundation Data via Spreadsheet Priv
	Foundation Data through Spreadsheet Management Duty	View Competitive Shop Priv
	Competitor Inquiry Duty	Maintain Competitive Shop Priv
	Competitor Management Duty	View Cost Changes Priv
	Cost Change Inquiry Duty	Maintain Cost Changes Priv
	Cost Change Management Duty	Submit Cost Changes Priv
	Cost Zone Inquiry Duty	View Cost Zones Priv
	Cost Zone Management Duty	Maintain Cost Zones Priv
	Data Steward Inquiry Duty	View Data Steward Dashboard Priv
	Finance Admin Inquiry Duty	View Finance Admin Priv
	Finance Admin Management Duty	Maintain Finance Admin Priv
	GL Drill Back Inquiry Duty	View GL Drill Back Priv
	Tran Data Inquiry Duty	View Transaction Data Priv
	Franchise Foundation Inquiry Duty	View Franchise Foundation Priv
	Franchise Foundation Management Duty	Maintain Franchise Foundation Priv
	Import Foundation Inquiry Duty	View Import Foundation Priv
	Import Foundation Management Duty	Maintain Import Foundation Priv
	Import Item Inquiry Duty	View Import Items Priv
	Import Item Management Duty	Maintain Import Items Priv
	Diff Inquiry Duty	View Diffs Priv
	Diff Management Duty	Maintain Diffs Priv
	Diff Ratio Inquiry Duty	Use Diffs Priv
	Diff Ratio Management Duty	Search Diff Ratios Priv
	Grocery Attribute Management Duty	View Diff Ratios Priv
	Item Approval Duty	Maintain Diff Ratios Priv
	Item Inquiry Duty	Maintain/View Grocery Attributes Priv
	Item List Inquiry Duty	Approve Items Priv
	Item List Management Duty	Search Items Priv
	Item Location Inquiry Duty	View Items Priv
	Item Location Management Duty	Search Item Lists Priv
		View Item Lists Priv
		Maintain Item Lists Priv
		View Item Locations Priv

Table 11–3   (Cont.) Function Security Mapping

Role	Duty	List of Privileges
	Item Management Duty	Maintain Item Locations Priv
	Item Supplier Inquiry Duty	Maintain Items Priv
	Item Supplier Management Duty	Submit Items Priv
	Price Change Inquiry Duty	View Item Suppliers Priv
	Ticket Management Duty	Maintain Item Suppliers Priv
	Location Inquiry Duty	View Price Change History Priv
	Location List Inquiry Duty	Maintain Ticket Requests Priv
	Location List Management Duty	View Stores Priv
	Location Management Duty	View Warehouses Priv
	Supply Chain Network Inquiry Duty	Search Location Lists Priv
	Supply Chain Network Management Duty	View Location Lists Priv
	Merchandise Hierarchy Inquiry Duty	Maintain Location Lists Priv
	Merchandise Hierarchy Management Duty	Maintain Stores Priv
	Organizational Hierarchy Management Duty	Maintain Warehouses Priv
	POS Configuration Inquiry Duty	View Supply Chain Network Priv
	POS Configuration Management Duty	Maintain Supply Chain Network Priv
	Partner Activation Duty	Search Merchandise Hierarchy Priv
	Partner Inquiry Duty	View Classes Priv
	Partner Management Duty	View Departments Priv
	Supplier Activation Duty	View Divisions Priv
	Supplier Inquiry Duty	View Groups Priv
	Supplier Inventory Inquiry Duty	View Merchandise Hierarchy Defaults Priv
	Supplier Inventory Management Duty	View Merchandise Hierarchy Priv
	Supplier Management Duty	View Subclasses Priv
	VAT Inquiry Duty	Maintain Classes Priv
	VAT Management Duty	Maintain Departments Priv
		Maintain Divisions Priv
		Maintain Groups Priv
		Maintain Merchandise Hierarchy Defaults Priv
		Maintain Merchandise Hierarchy Priv
		Maintain Reclassifications Priv
		Maintain Subclasses Priv
		View Areas Priv
		View Chains Priv
		View Districts Priv
		View Organizational Hierarchy Priv
		View Regions Priv
		Maintain Areas Priv

Table 11–3   (Cont.) Function Security Mapping

Role	Duty	List of Privileges
		Maintain Chains Priv
		Maintain Districts Priv
		Maintain Regions Priv
		View Coupons Priv
		View Product Restrictions Priv
		Maintain Coupons Priv
		Maintain Product Restrictions Priv
		Activate Partners Priv
		Deactivate Partners Priv
		Search Partners Priv
		View Partners Priv
		Maintain Partners Priv
		Activate Suppliers Priv
		Deactivate Suppliers Priv
		Search Suppliers Priv
		View Suppliers Priv
		View Supplier Inventory Management Priv
		Maintain Supplier Inventory Management Priv
		Maintain Suppliers Priv
		View VAT Priv
		Maintain VAT Priv
Buyer	Asynchronous Job Inquiry Duty	View Asynchronous Jobs Priv
	Asynchronous Job Management Duty	Maintain Asynchronous Jobs Priv
	View Foundation Data via Spreadsheet Priv	Maintain Custom Flex Attributes Priv
	Competitor Inquiry Duty	View Custom Flex Attributes Priv
	Contract Approval Duty	View Foundation Data via Spreadsheet Priv
	Contract Inquiry Duty	Maintain Foundation Data via Spreadsheet Priv
	Contract Management Duty	View Competitive Shop Priv
	Cost Change Approval Duty	Maintain Competitive Shop Priv
	Cost Change Inquiry Duty	Approve Contracts Priv
	Cost Change Management Duty	Search Contracts Priv
	Buyer Dashboard Inquiry Duty	View Contracts Priv
	Deal Approval Duty	Maintain Contracts Priv
	Deal Inquiry Duty	Submit Contracts Priv
	Deal Management Duty	Approve Cost Changes Priv
	Budgets Inquiry Duty	Search Cost Changes Priv
	Budgets Management Duty	View Cost Changes Priv
	GL Drill Back Inquiry Duty	Maintain Cost Changes Priv

Table 11–3   (Cont.) Function Security Mapping

Role	Duty	List of Privileges
	Tran Data Inquiry Duty	Submit Cost Changes Priv
	Franchise Cost Inquiry Duty	View Buyer Dashboard Priv
	Franchise Cost Management Duty	View Finance Analyst Dashboard Priv
	Franchise Foundation Inquiry Duty	View Inventory Analyst Dashboard Priv
	Franchise Foundation Management Duty	View Inventory Control Dashboard Priv
	Franchise Orders and Returns Approval Duty	View Data Steward Dashboard Priv
	Franchise Orders and Returns Inquiry Duty	Approve Deals Priv
		Search Deals Priv
	Franchise Orders and Returns Management Duty	View Deals Priv
	Import Foundation Inquiry Duty	Maintain Deals Priv
	Import Foundation Management Duty	Submit Deals Priv
		View Budgets Priv
	RTV Inquiry Duty	Maintain Budgets Priv
	Diff Management Duty	View Finance Admin Priv
	Diff Ratio Inquiry Duty	Maintain Finance Admin Priv
	Diff Ratio Management Duty	View Financial Control Priv
	Grocery Attribute Management Duty	Maintain Financial Control Priv
		View GL Drill Back Priv
	Item Approval Duty	View Transaction Data Priv
	Item Inquiry Duty	View Franchise Cost Priv
	Item List Inquiry Duty	Maintain Franchise Cost Priv
	Item List Management Duty	View Franchise Foundation Priv
	Item Location Inquiry Duty	Maintain Franchise Foundation Priv
	Item Location Management Duty	
	Item Management Duty	Approve Franchise Orders and Returns Priv
	Item Supplier Inquiry Duty	View Franchise Orders and Returns Priv
	Item Supplier Management Duty	Maintain Franchise Orders and Returns Priv
	Price Change Inquiry Duty	View Import Foundation Priv
	Location List Inquiry Duty	Maintain Import Foundation Priv
	Location List Management Duty	View Item Inventory and Sales Priv
	Pre-issued Order Numbers Management Duty	
	Purchase Order Approval Duty	Search RTVs Priv
	Purchase Order Inquiry Duty	View RTVs Priv
	Purchase Order Management Duty	Use Diffs Priv
		Search Diff Ratios Priv
		View Diff Ratios Priv
		Maintain Diff Ratios Priv
		Approve Items Priv

Table 11–3   (Cont.) Function Security Mapping

Role	Duty	List of Privileges
		Maintain/View Grocery Attributes Priv
		Search Items Priv
		View Items Priv
		Search Item Lists Priv
		View Item Lists Priv
		Maintain Item Lists Priv
		View Item Locations Priv
		Maintain Item Locations Priv
		Maintain Items Priv
		Submit Items Priv
		View Item Suppliers Priv
		View Price Change History Priv
		Maintain Ticket Requests Priv
		View Stores Priv
		View Warehouses Priv
		Search Location Lists Priv
		View Location Lists Priv
		Maintain Location Lists Priv
		Maintain Pre-Issued Order Numbers Priv
		Approve Purchase Orders Priv
		Search Purchase Orders Priv
		View Purchase Orders Priv
		Close Purchase Orders Priv
		Maintain Purchase Orders Priv
		Submit Purchase Orders Priv

Table 11–3 (Cont.) Function Security Mapping

Role	Duty	List of Privileges
Inventory Analyst	Asynchronous Job Inquiry Duty	View Asynchronous Jobs Priv
	Asynchronous Job Management Duty	Maintain Asynchronous Jobs Priv
	Foundation Data via Spreadsheet Inquiry Duty	View Foundation Data via Spreadsheet Priv
		Search Contracts Priv
	Contract Inquiry Duty	View Contracts Priv
	Contract Management Duty	Maintain Contracts Priv
	Inventory Analyst Inquiry Duty	Submit Contracts PrivView Inventory Analyst Dashboard Priv
	Budgets Inquiry Duty	
	Franchise Orders and Returns Approval Duty	View Budgets Priv
	Franchise Orders and Returns Inquiry Duty	Approve Franchise Orders and Returns Priv
	Franchise Orders and Returns Management Duty	View Franchise Orders and Returns Priv
	Customs Entry Inquiry Duty	Maintain Franchise Orders and Returns Priv
	Transportation Inquiry Duty	Search Customs Entries Priv
	Inventory and Sales Inquiry Duty	View Customs Entries Priv
	Intercompany Transfer Approval Duty	Search Transportation Priv
		View Transportation Priv
	Intercompany Transfer Inquiry Duty	View Item Inventory and Sales Priv
	Intercompany Transfer Management Duty	Approve Intercompany Transfers Priv
	MRT Approval Duty	View Intercompany Transfers Priv
	MRT Inquiry Duty	Maintain Intercompany Transfers Priv
	MRT Management Duty	
	RTV Approval Duty	Submit Intercompany Transfers Priv
	RTV Inquiry Duty	Approve MRTs Priv
	RTV Management Duty	Search MRTs Priv
	Transfer Approval Duty	View MRTs Priv
	Transfer Inquiry Duty	Maintain MRTs Priv
	Transfer Inquiry Duty AND Intercompany Transfer Inquiry Duty	Submit MRTs Priv
		Approve RTVs Priv
	Transfer Management Duty	Search RTVs Priv
	Transfer with Finishing Management Duty	View RTVs Priv
	Diff Management Duty	Maintain RTVs Priv
	Diff Ratio Inquiry Duty	Approve Transfers Priv
	Diff Ratio Management Duty	View Transfers Priv
	Grocery Attribute Management Duty	Search Transfers Priv
		Maintain Transfers Priv
	Item Approval Duty	Submit Transfers Priv

Table 11–3   (Cont.) Function Security Mapping

Role	Duty	List of Privileges
	Item Inquiry Duty	Maintain Transfers with Finishing Priv
	Item List Inquiry Duty	
	Item List Management Duty	Use Diffs Priv
	Item Location Inquiry Duty	Search Diff Ratios Priv
	Item Location Management Duty	View Diff Ratios Priv
		Maintain Diff Ratios Priv
	Item Management Duty	Maintain/View Grocery Attributes Priv
	Item Supplier Inquiry Duty	
	Item Supplier Management Duty	Approve Items Priv
		Search Items Priv
	Ticket Management Duty	View Items Priv
	Location List Inquiry Duty	Search Item Lists Priv
	Location List Management Duty	View Item Lists Priv
	Pre-issued Order Numbers Management Duty	Maintain Item Lists Priv
		View Item Locations Priv
	Purchase Order Approval Duty	Maintain Item Locations Priv
	Purchase Order Inquiry Duty	Maintain Items Priv
	Purchase Order Management Duty	Submit Items Priv
		View Item Suppliers Priv
	Replenishment Inquiry Duty	Maintain Item Suppliers Priv
	Replenishment Management Duty	View Price Change History Priv
		Maintain Ticket Requests Priv
		Search Location Lists Priv
		View Location Lists Priv
		Maintain Location Lists Priv
		Maintain Pre-Issued Order Numbers Priv
		Approve Purchase Orders Priv
		Search Purchase Orders Priv
		View Purchase Orders Priv
		Close Purchase Orders Priv
		Maintain Purchase Orders Priv
		Submit Purchase Orders Priv
		View Replenishment Attributes Priv
		Maintain Replenishment Attributes Priv
Inventory Manager	Asynchronous Job Inquiry Duty	View Asynchronous Jobs Priv
	Asynchronous Job Management Duty	Maintain Asynchronous Jobs Priv
	Foundation Data via Spreadsheet Inquiry Duty	View Foundation Data via Spreadsheet Priv
		Maintain Foundation Data via Spreadsheet Priv
	Contract Approval Duty	
	Contract Inquiry Duty	Approve Contracts Priv

Table 11–3   (Cont.) Function Security Mapping

Role	Duty	List of Privileges
	Contract Management Duty	Search Contracts Priv
	Inventory Analyst Inquiry Duty	View Contracts Priv
	Budgets Inquiry Duty	Maintain Contracts Priv
	Franchise Orders and Returns Approval Duty	Submit Contracts Priv
	Franchise Orders and Returns Inquiry Duty	View Inventory Analyst Dashboard Priv
		View Budgets Priv
	Franchise Orders and Returns Management Duty	Approve Franchise Orders and Returns Priv
	ALC Inquiry Duty	View Franchise Orders and Returns Priv
	ALC Inquiry Duty	
	ALC Management Duty	Maintain Franchise Orders and Returns Priv
	Customs Entry Confirmation Duty	Search Customs Entries Priv
	Customs Entry Inquiry Duty	View Customs Entries Priv
	Transportation Inquiry Duty	Search Transportation Priv
	Inventory and Sales Inquiry Duty	View Transportation Priv
		View Item Inventory and Sales Priv
	Intercompany Transfer Approval Duty	Approve Intercompany Transfers Priv
	Intercompany Transfer Inquiry Duty	View Intercompany Transfers Priv
	Intercompany Transfer Management Duty	Maintain Intercompany Transfers Priv
	MRT Approval Duty	Submit Intercompany Transfers Priv
	MRT Inquiry Duty	
	MRT Management Duty	Approve MRTs Priv
	RTV Approval Duty	Search MRTs Priv
	RTV Inquiry Duty	View MRTs Priv
	RTV Management Duty	Maintain MRTs Priv
	Transfer Approval Duty	Submit MRTs Priv
	Transfer Inquiry Duty	Approve RTVs Priv
	Transfer Inquiry Duty AND	Search RTVs Priv
	Intercompany Transfer Inquiry Duty	View RTVs Priv
		Maintain RTVs Priv
	Transfer Management Duty	Approve Transfers Priv
	Transfer with Finishing Management Duty	View Transfers PrivSearch Transfers Priv
	Diff Management Duty	Maintain Transfers Priv
	Diff Ratio Inquiry Duty	Submit Transfers Priv
	Diff Ratio Management Duty	Maintain Transfers with Finishing Priv
	Grocery Attribute Management Duty	Use Diffs Priv
	Item Approval Duty	Search Diff Ratios Priv
	Item Inquiry Duty	View Diff Ratios Priv

Table 11–3   (Cont.) Function Security Mapping

Role	Duty	List of Privileges
	Item List Inquiry Duty	Maintain Diff Ratios Priv
	Item List Management Duty	Maintain/View Grocery Attributes Priv
	Item Location Inquiry Duty	
	Item Location Management Duty	Approve Items Priv
		Search Items Priv
	Item Management Duty	View Items Priv
	Item Supplier Inquiry Duty	Search Item Lists Priv
	Item Supplier Management Duty	View Item Lists Priv
		Maintain Item Lists Priv
	Price Change Inquiry Duty	View Item Locations Priv
	Ticket Management Duty	Maintain Item Locations Priv
	Location List Inquiry Duty	Maintain Items Priv
	Location List Management Duty	Submit Items Priv
	Pre-issued Order Numbers Management Duty	View Item Suppliers Priv
	Purchase Order Inquiry Duty	Maintain Item Suppliers Priv
		View Price Change History Priv
	Purchase Order Management Duty	Maintain Ticket Requests Priv
	Replenishment Inquiry Duty	Search Location Lists Priv
	Replenishment Management Duty	View Location Lists Priv
		Maintain Location Lists Priv
		Maintain Pre-Issued Order Numbers Priv
		Approve Purchase Orders Priv
		Search Purchase Orders Priv
		View Purchase Orders Priv
		Close Purchase Orders Priv
		Maintain Purchase Orders Priv
		Submit Purchase Orders Priv
		View Replenishment Attributes Priv
		Maintain Replenishment Attributes Priv
Corporate Inventory Control Analyst	Asynchronous Job Inquiry Duty	View Asynchronous Jobs Priv
	Asynchronous Job Management Duty	Maintain Asynchronous Jobs Priv
	Foundation Data via Spreadsheet Inquiry Duty	View Foundation Data via Spreadsheet Priv
	Inventory Control Inquiry Duty	View Inventory Control Dashboard Priv
	Customs Entry Inquiry Duty	Search Customs Entries PrivView Customs Entries Priv
	Transportation Inquiry Duty	Search Transportation Priv
	Inventory Adjustment Management Duty	View Transportation Priv
	Inventory and Sales Inquiry Duty	Maintain Inventory Adjustments Priv

Table 11–3   (Cont.) Function Security Mapping

Role	Duty	List of Privileges
	Intercompany Transfer Approval Duty	View Item Inventory and Sales Priv
	Intercompany Transfer Inquiry Duty	Approve Intercompany Transfers Priv
	Intercompany Transfer Management Duty	View Intercompany Transfers Priv
		Maintain Intercompany Transfers Priv
	MRT Approval Duty	
	MRT Inquiry Duty	Submit Intercompany Transfers Priv
	MRT Management Duty	
	RTV Approval Duty	Approve MRTs Priv
	RTV Inquiry Duty	Search MRTs Priv
	Shipment and Receipts Inquiry Duty	View MRTs Priv
		Maintain MRTs Priv
	Shipment and Receipts Management Duty	Submit MRTs Priv
		Approve RTVs Priv
	Transfer Approval Duty	Search RTVs Priv
	Transfer Inquiry Duty	View RTVs Priv
	Transfer Inquiry Duty AND	View Shipments and Receipts Priv
	Intercompany Transfer Inquiry Duty	Maintain Shipments and Receipts Priv
	Transfer Management Duty	Approve Transfers Priv
	Transfer with Finishing Management Duty	View Transfers Priv
		Search Transfers Priv
	Diff Management Duty	Maintain Transfers Priv
	Item Inquiry Duty	Submit Transfers Priv
	Stock Count Inquiry Duty	Maintain Transfers with Finishing Priv
	Stock Count Management Duty	
		Use Diffs Priv
		Search Items Priv
		View Items Priv
		View Item Locations Priv
		View Item Suppliers Priv
		Search Purchase Orders Priv
		View Purchase Orders Priv
		Close Purchase Orders Priv
		Maintain Purchase Orders Priv
		Submit Purchase Orders Priv
		View Stock Count Units Priv
		View Stock Counts Priv
		Maintain Stock Count Units Priv
		Maintain Stock Counts Priv
Inventory Control Manager	Asynchronous Job Inquiry Duty	View Asynchronous Jobs Priv
	Asynchronous Job Management Duty	Maintain Asynchronous Jobs Priv

Table 11–3   (Cont.) Function Security Mapping

Role	Duty	List of Privileges
	Foundation Data via Spreadsheet Inquiry Duty	View Foundation Data through Spreadsheet Priv
	Inventory Control Inquiry Duty	Maintain Foundation Data through Spreadsheet Priv
	Customs Entry Inquiry Duty	
	Transportation Inquiry Duty	View Competitive Shop Priv
	Inventory Adjustment Management Duty	Maintain Competitive Shop Priv
		Approve Contracts Priv
	Inventory and Sales Inquiry Duty	Search Contracts Priv
		View Contracts Priv
	Intercompany Transfer Approval Duty	Maintain Contracts Priv
	Intercompany Transfer Inquiry Duty	Submit Contracts Priv
		Approve Cost Changes Priv
	Intercompany Transfer Management Duty	Search Cost Changes Priv
		View Cost Changes Priv
	MRT Approval Duty	Maintain Cost Changes Priv
	MRT Inquiry Duty	Submit Cost Changes Priv
	MRT Management Duty	View Cost Zones Priv
	RTV Approval Duty	Maintain Cost Zones Priv
	RTV Inquiry Duty	View Buyer Dashboard Priv
	Shipment and Receipts Inquiry Duty	View Finance Analyst Dashboard Priv
	Shipment and Receipts Management Duty	View Inventory Analyst Dashboard Priv
	Transfer Approval Duty	View Inventory Control Dashboard Priv
	Transfer Inquiry Duty	
	Transfer Inquiry Duty AND Intercompany Transfer Inquiry Duty	View Data Steward Dashboard Priv
		Approve Deals Priv
	Transfer Management Duty	Search Deals Priv
	Transfer Management Duty	View Deals Priv
	Transfer with Finishing Management Duty	Maintain Deals Priv
	Diff Management Duty	Submit Deals Priv
	Item Inquiry Duty	View Expense Profiles Priv
	Item Location Inquiry Duty	Maintain Expense Profiles Priv
	Item Supplier Inquiry Duty	View Up Charges Priv
	Purchase Order Inquiry Duty	Maintain Up Charges Priv
	Purchase Order Management Duty	Maintain Average Cost Priv
		View Budgets Priv
	Stock Count Inquiry Duty	Maintain Budgets Priv
	Stock Count Management Duty	View Finance Admin Priv
		Maintain Finance Admin Priv
		View Financial Control Priv
		Maintain Financial Control Priv
		View GL Drill Back Priv

Table 11–3   (Cont.) Function Security Mapping

Role	Duty	List of Privileges
		View Transaction Data Priv
		View Franchise Cost Priv
		Maintain Franchise Cost Priv
		View Franchise Foundation Priv
		Maintain Franchise Foundation Priv
		Approve Franchise Orders and Returns Priv
		View Franchise Orders and Returns Priv
		Maintain Franchise Orders and Returns Priv
		Search Actual Landed Cost Priv
		View Actual Landed Cost Priv
		Finalize Actual Landed Cost Priv
		Confirm Customs Entries Priv
		Search Customs Entries Priv
		View Customs Entries Priv
		Maintain Customs Entries Priv
		Submit Customs Entries Priv
		View Import Foundation Priv
		Maintain Import Foundation Priv
		View Import Items Priv
		Maintain Import Items Priv
		Approve Letters of Credit Priv
		Confirm Letters of Credit Priv
		Search Letters of Credit Priv
		View Letters of Credit Priv
		Maintain Letters of Credit Priv
		Submit Letters of Credit Priv
		Approve Obligations Priv
		Search Obligations Priv
		View Obligations Priv
		Maintain Obligations Priv
		Search Transportation Priv
		View Transportation Priv
		Finalize Transportation Priv
		Maintain Transportation Priv
		Maintain Inventory Adjustments Priv
		View Item Inventory and Sales Priv
		Approve Intercompany Transfers Priv

Table 11–3   (Cont.) Function Security Mapping

Role	Duty	List of Privileges
		View Intercompany Transfers Priv
		Maintain Intercompany Transfers Priv
		Submit Intercompany Transfers Priv
		Approve MRTs Priv
		Search MRTs Priv
		View MRTs Priv
		Maintain MRTs Priv
		Submit MRTs Priv
		Approve RTVs Priv
		Search RTVs Priv
		View RTVs Priv
Sourcing Analyst	Asynchronous Job Inquiry Duty	View Asynchronous Jobs Priv
	Asynchronous Job Management Duty	Maintain Asynchronous Jobs Priv
	Foundation Data through Spreadsheet Inquiry Duty	View Foundation Data via Spreadsheet Priv
	Cost Change Inquiry Duty	View Cost Changes Priv
	Cost Zone Inquiry Duty	View Cost Zones Priv
	Cost Zone Management Duty	Maintain Cost Zones Priv
	Expense Inquiry Duty	View Expense Profiles Priv
	Expense Management Duty	Maintain Expense Profiles Priv
	ALC Inquiry Duty	Search Actual Landed Cost Priv
	ALC Management Duty	View Actual Landed Cost Priv
	Customs Entry Confirmation Duty	Finalize Actual Landed Cost Priv
		Confirm Customs Entries Priv
	Customs Entry Inquiry Duty	Search Customs Entries Priv
	Customs Entry Management Duty	View Customs Entries Priv
		Maintain Customs Entries Priv
	Import Item Inquiry Duty	Submit Customs Entries Priv
	Import Item Management Duty	View Import Items Priv
	Letter of Credit Approval Duty	Maintain Import Items Priv
	Letter of Credit Inquiry Duty	Approve Letters of Credit Priv
	Letter of Credit Management Duty	Confirm Letters of Credit Priv
		Search Letters of Credit Priv
	Obligation Approval Duty	View Letters of Credit Priv
	Obligation Inquiry Duty	Maintain Letters of Credit Priv
	Obligation Management Duty	Submit Letters of Credit Priv
	Transportation Inquiry Duty	Approve Obligations Priv
	Transportation Management Duty	Search Obligations Priv
		View Obligations Priv
	Diff Management Duty	Maintain Obligations Priv
	Item Inquiry Duty	

Table 11–3   (Cont.) Function Security Mapping

Role	Duty	List of Privileges
	Item Location Inquiry Duty	Search Transportation Priv
	Item Supplier Inquiry Duty	View Transportation Priv
	Item Supplier Management Duty	Finalize Transportation Priv
		Maintain Transportation Priv
	Purchase Order Inquiry Duty	Use Diffs Priv
	Purchase Order Management Duty	Search Items Priv
		View Items Priv
	Required Document Inquiry Duty	View Item Locations Priv
	Required Document Management Duty	View Item Suppliers Priv
		Maintain Item Suppliers Priv
	Partner Inquiry Duty	Search Purchase Orders Priv
	Partner Management Duty	View Purchase Orders Priv
	Supplier Inquiry Duty	Close Purchase Orders Priv
		Maintain Purchase Orders Priv
		Submit Purchase Orders Priv
		View Required Documents Priv
		Maintain Required Documents Priv
		Search Partners Priv
		View Partners Priv
		Maintain Partners Priv
		Search Suppliers Priv
		View Suppliers Priv
		Maintain Suppliers Priv
Finance Analyst	Asynchronous Job Inquiry Duty	View Asynchronous Jobs Priv
	Asynchronous Job Management Duty	Maintain Asynchronous Jobs Priv
	Foundation Data through Spreadsheet Inquiry Duty	View Foundation Data via Spreadsheet Priv
	Competitor Inquiry Duty	View Competitive Shop Priv
	Finance Analyst Inquiry Duty	View Finance Analyst Dashboard Priv
	Deal Approval Duty	Approve Deals Priv
	Deal Inquiry Duty	Search Deals Priv
	Deal Management Duty	View Deals Priv
	Deal Management Duty	Maintain Deals Priv
	Budgets Inquiry Duty	Submit Deals Priv
	Finance Admin Inquiry Duty	View Budgets Priv
	Finance Admin Management Duty	View Finance Admin Priv
		Maintain Finance Admin Priv
	Financial Control Inquiry Duty	View Financial Control Priv
	Financial Control Management Duty	Maintain Financial Control Priv
	Customs Entry Inquiry Duty	Search Customs Entries Priv

Table 11–3   (Cont.) Function Security Mapping

Role	Duty	List of Privileges
	Obligation Inquiry Duty	View Customs Entries Priv
	Transportation Inquiry Duty	Search Obligations Priv
	Inventory and Sales Inquiry Duty	View Obligations Priv
	Intercompany Transfer Inquiry Duty	Search Transportation Priv
		View Transportation Priv
	Intercompany Transfer Management Duty	View Item Inventory and Sales Priv
	MRT Inquiry Duty	View Intercompany Transfers Priv
	RTV Inquiry Duty	Maintain Intercompany Transfers Priv
	Shipment and Receipts Inquiry Duty	Submit Intercompany Transfers Priv
	Transfer Inquiry Duty	Search MRTs Priv
	Transfer Inquiry Duty AND	View MRTs Priv
	Intercompany Transfer Inquiry Duty	Search RTVs Priv
	Transfer Management Duty	View RTVs Priv
	Diff Management Duty	View Shipments and Receipts Priv
	Item Inquiry Duty	View Transfers Priv
	Item List Inquiry Duty	Search Transfers Priv
	Item List Management Duty	Maintain Transfers Priv
	Item Location Inquiry Duty	Use Diffs Priv
	Item Supplier Inquiry Duty	Search Items Priv
	Price Change Inquiry Duty	View Items Priv
	Location List Inquiry Duty	Search Item Lists Priv
	Location List Management Duty	View Item Lists Priv
	Purchase Order Inquiry Duty	Maintain Item Lists Priv
	Stock Count Inquiry Duty	View Item Locations Priv
	Stock Count Value Management Duty	View Item Suppliers Priv
	Stock Ledger Inquiry Duty	View Price Change History Priv
	Partner Activation Duty	Search Location Lists Priv
	Partner Inquiry Duty	View Location Lists Priv
	Partner Management Duty	Maintain Location Lists Priv
	Supplier Activation Duty	Search Purchase Orders Priv
	Supplier Inquiry Duty	View Purchase Orders Priv
	Supplier Inventory Inquiry Duty	View Stock Count Units Priv
	Supplier Inventory Management Duty	View Stock Counts Priv
		Maintain Stock Count Values Priv
	Supplier Management Duty	View Stock Ledger Priv
	VAT Inquiry Duty	Activate Partners Priv
		Deactivate Partners Priv
		Search Partners Priv
		View Partners Priv
		View Suppliers Priv

Table 11–3   (Cont.) Function Security Mapping

Role	Duty	List of Privileges
		Activate Suppliers Priv
		Deactivate Suppliers Priv
		Search Suppliers Priv
		View Supplier Inventory Management Priv
		Maintain Supplier Inventory Management Priv
		Maintain Suppliers Priv
		View VAT Priv
Supply Chain Analyst	Asynchronous Job Inquiry Duty	View Asynchronous Jobs Priv
	Asynchronous Job Management Duty	Maintain Asynchronous Jobs Priv
	Foundation Data through Spreadsheet Inquiry Duty	View Foundation Data via Spreadsheet Priv
	Cost Zone Inquiry Duty	View Cost Zones Priv
	Cost Zone Management Duty	Maintain Cost Zones Priv
	Expense Inquiry Duty	View Expense Profiles Priv
	Expense Management Duty	Maintain Expense Profiles Priv
	Up Charge Inquiry Duty	View Up Charges Priv
	Up Charge Management Duty	Maintain Up Charges Priv
	Transportation Inquiry Duty	Search Transportation Priv
	Transportation Management Duty	View Transportation Priv
		Finalize Transportation Priv
	Diff Management Duty	Maintain Transportation Priv
	Item Inquiry Duty	Use Diffs Priv
	Item List Inquiry Duty	Search Items Priv
		View Items Priv
	Item List Management Duty	Search Item Lists Priv
	Item Location Inquiry Duty	View Item Lists Priv
	Item Location Management Duty	Maintain Item Lists Priv
		View Item Locations Priv
	Item Supplier Inquiry Duty	Maintain Item Locations Priv
	Item Supplier Management Duty	View Item Suppliers Priv
		Maintain Item Suppliers Priv
	Location Inquiry Duty	View Stores Priv
	Location List Inquiry Duty	View Warehouses Priv
	Location List Management Duty	Search Location Lists Priv
	Supply Chain Network Inquiry Duty	View Location Lists Priv
	Supply Chain Network Management Duty	Maintain Location Lists Priv
		View Supply Chain Network Priv
	Purchase Order Inquiry Duty	Maintain Supply Chain Network Priv
	Replenishment Inquiry Duty	
	Supplier Inventory Management Duty	Search Purchase Orders Priv
	Supplier Inventory Inquiry Duty	View Suppliers Priv

Table 11–3   (Cont.) Function Security Mapping

Role	Duty	List of Privileges
	Supplier Inquiry Duty	View Purchase Orders Priv
	Supplier Management Duty	View Replenishment Attributes Priv
		Search Suppliers Priv
		View Supplier Inventory Management Priv
		Maintain Supplier Inventory Management Priv
		Maintain Suppliers Priv
Finance Manager	Foundation Data through Spreadsheet Inquiry Duty	View Foundation Data through Spreadsheet Priv
	Finance Analyst Inquiry Duty	View Finance Analyst Dashboard Priv
	Expense Inquiry Duty	
	Expense Management Duty	View Expense Profiles Priv
	Up Charge Inquiry Duty	Maintain Expense Profiles Priv
	Up Charge Management Duty	View Up Charges Priv
	Average Cost Management Duty	Maintain Up Charges Priv
	Budgets Inquiry Duty	Maintain Average Cost Priv
	Budgets Management Duty	View Budgets Priv
	Finance Admin Inquiry Duty	Maintain Budgets Priv
	Finance Admin Management Duty	View Finance Admin Priv
		Maintain Finance Admin Priv
	Financial Control Inquiry Duty	View Financial Control Priv
	Financial Control Management Duty	Maintain Financial Control Priv
	ALC Inquiry Duty	Search Actual Landed Cost Priv
	ALC Management Duty	View Actual Landed Cost Priv
		Finalize Actual Landed Cost Priv
	Customs Entry Inquiry Duty	Search Customs Entries Priv
	Letter of Credit Approval Duty	View Customs Entries Priv
	Letter of Credit Inquiry Duty	Approve Letters of Credit Priv
	Letter of Credit Management Duty	Confirm Letters of Credit Priv
	Obligation Approval Duty	Search Letters of Credit Priv
	Obligation Inquiry Duty	View Letters of Credit Priv
	Obligation Management Duty	Maintain Letters of Credit Priv
		Submit Letters of Credit Priv
	Transportation Inquiry Duty	Approve Obligations Priv
	Intercompany Transfer Inquiry Duty	Search Obligations Priv
	Intercompany Transfer Management Duty	View Obligations Priv
		Maintain Obligations Priv
	MRT Inquiry Duty	Search Transportation Priv
	RTV Inquiry Duty	View Transportation Priv
	Shipment and Receipts Inquiry Duty	View Intercompany Transfers Priv
	Item Inquiry Duty	View RTVs Priv

Table 11–3   (Cont.) Function Security Mapping

Role	Duty	List of Privileges
	Transfer Inquiry Duty	Maintain Intercompany Transfers Priv
	Transfer Inquiry Duty AND Intercompany Transfer Inquiry Duty	Submit Intercompany Transfers Priv
	Transfer Management Duty	Approve MRTs Priv
	Diff Management Duty	Search MRTs Priv
	Item Location Inquiry Duty	View MRTs Priv
	Item Supplier Inquiry Duty	Search RTVs Priv
	Price Change Inquiry Duty	View Shipments and Receipts Priv
	DSD Management Duty	View Transfers Priv
	Purchase Order Inquiry Duty	Search Transfers Priv
	Receipt Adjustments by Cost Management Duty	Maintain Transfers Priv
		Use Diffs Priv
	Stock Count Inquiry Duty	Search Items Priv
	Stock Count Management Duty	View Items Priv
	Stock Count Value Management Duty	View Item Locations Priv
	Stock Ledger Inquiry Duty	View Item Suppliers Priv
	Stock Ledger Management Duty	View Price Change History Priv
	Partner Activation Duty	Maintain DSD Orders Priv
	Partner Inquiry Duty	Search Purchase Orders Priv
	Partner Management Duty	View Purchase Orders Priv
	Supplier Activation Duty	Maintain Receipt Adjustments by Cost Priv
	Supplier Inquiry Duty	View Stock Count Units Priv
	Supplier Inventory Inquiry Duty	View Stock Counts Priv
	Supplier Inventory Management Duty	Maintain Stock Count Values Priv
		View Stock Ledger Priv
	Supplier Management Duty	Maintain Stock Ledger Priv
	VAT Inquiry Duty	Activate Partners Priv
	VAT Management Duty	Deactivate Partners Priv
		Search Partners Priv
		View Partners Priv
		Maintain Partners Priv
		Activate Suppliers Priv
		Deactivate Suppliers Priv
		Search Suppliers Priv
		View Suppliers Priv
		View Supplier Inventory Management Priv
		Maintain Suppliers Priv
		View VAT Priv
		Maintain VAT Priv

Data Security Views

In RMS application as part of security, all search screens and LOVs (List of Values) access the views. Those users who have privileges will only be able to see the data from these views.

These views are implemented by the following scripts:

1. add_filter_policy.sql

   - This script adds filter policy to four main categories of data in RMS

     – Organizational Hierarchy Filtering Policies: Views under this category are V_CHAIN, V_AREA, V_REGION, V_DISTRICT, V_STORE, V_WH, V_EXTERNAL_FINISHER, V_INTERNAL_FINISHER and V_TSF_ENTITY

     – Merchandise Hierarchy Filtering Policies: V_DIVISION, V_GROUPS, V_DEPS, V_CLASS, V_SUBCLASS and V_ITEM_MASTER

     – Data Element Filtering Policies: V_DIFF_GROUP_HEAD, V_LOC_LIST_HEAD, V_LOC_TRAITS, V_SEASONS, V_SKULIST_HEAD, V_TICKET_TYPE_HEAD, V_UDA and V_SUPS

     – Product Location Security Policies: V_TRANSFER_FROM_STORE, V_TRANSFER_FROM_WH, V_TRANSFER_TO_STORE and V_TRANSFER_TO_WH

Other Common Application Administration

This section covers the common Application Administration.

File Permissions

For file permission, the following permissions should be given to users to access files once the installation is complete:

- All configuration files should at most have 660 permission
- All static data (flat files) should at most have 640 permission

Based on the permissions above, besides the owner (the installer user), the group member can also view, read, modify the configuration files, and read the static file. A user out of the group cannot perform any action on the ReSA files. Explicit permissions need to be given by the Administrator to users outside of the group.

Data Access Schema (DAS) - Overview

Data Access Schema (DAS) is an extension of RMS database used by external applications requiring RMS data. The external applications extracting data from RMS increases the server load on the main RMS schema which impacts the performance of core RMS functionality. The data in the DAS schema is replicated real time from the main RMS schema allowing the server load of the extract job to be restricted to this separate database.

The core RMS tables are replicated to the DAS schema in near real time. On top of these replicated tables, there is a layer of data base views which structures the data and exposes them as business data. An external application that is not aware of the RMS data structure can read the business data exposed.

For a new external application required data extract from RMS, the client should check if the existing tables and views in the DAS schema is sufficient. If not, the RMS table

should be included in the list of replicated tables. The client should also build additional views on top of the table or views to structure the data in way it is useful to the requesting application while also considering the reuse for the view for any future use.

The DAS schema is exposed to the external application as a read only schema and external applications should not write into this schema:

- Database tables which are replicated from main RMS schema should not be accessed directly from external application. The external application should always access the data using the views only. This will avoid changes to the external application when there is a change in RMS table structure. Any change in RMS data structure should be transparent to the external application just by changing the view built on these tables.

- The external application should not be granted permission on the database views. The access to the views should be restricted based on the functional data requirement for a specific application.

Post Installation Steps for Webservice Security

You need to configure the user credentials and other security related information at the service consumer and the app service provider layers, in order to provide end to end security between web service consumer and the provider.

> **Note:**
>
> 1. The following steps are used for webservices deployed according to the Oracle Retail Installation guides.
>
> 2. The following steps are not applicable for RSB. For more information, see the *Oracle Retail Service Backbone Security Guide*.

Applying Policy A

Applying policy A involves the following:

- Enabling the HTTPS servers
- Creating the Webservice users
- Securing services
- Updating the Webservice deployment
- Webservice Clock Skew setting

Enabling the HTTPS servers

Perform the following steps to enable HTTPS servers:

1. In WebLogic Admin Console, click Environment > Servers.

2. Click the server where the web service has been deployed.

3. Click the **General** tab.

4. Check the SSL Listen Port Enabled check box.

5. Enter a port number for the SSL Listen Port. This is the port number for service end point.

6. Enter the hostname in Listen Address field.

7. Click **Save**.

Figure 11–1 Enabling the HTTPS Servers

Creating the Webservice User

Perform the following steps to create roles and users who can access the Web services:

1. In WebLogic Admin Console, click the Domain Structure window, and click the Security Realms link.

The default realm appears.

2. Click the link on the realm.

3. Click the **Users and Groups** tab.

4. Click **New**.

5. Enter the user name and password details on the next screen.

6. Leave the default value for Provider.

7. Click **OK** to save the changes.

The new user is shown in the list of users.

Securing services

Perform the following steps in WebLogic Admin Console for each of the services to be secured:

1. Attach the user created in previous step to the service.

2. Click Deployments.

3. Click the service you want to secure.

4. Click **Securities** and then **Policies**.

Figure 11–2   Securing Services

5. Click Add **Conditions** > Predict List: Pick User from dropdown > Next > User Argument Name: > Type username you created > Add > Finish > Save.

Figure 11–3   Add Conditions Window

6. Attach policy to the service.

7. Navigate to **Configuration** tab.

8. Click **WSB Policy** tab and select the service port.

Figure 11–4   Attaching WS Policy to the Service
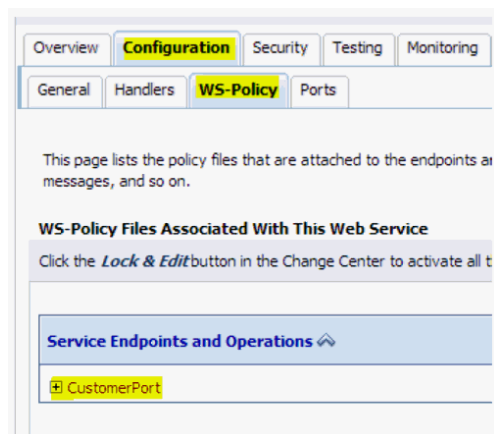
9. Pick WebLogic > Next > Service Endpoint Policies: select policy:Wssp1.22007HttpsUsernameTokenPlain.xml > Finish

Figure 11–5   Service Endpoint Policies
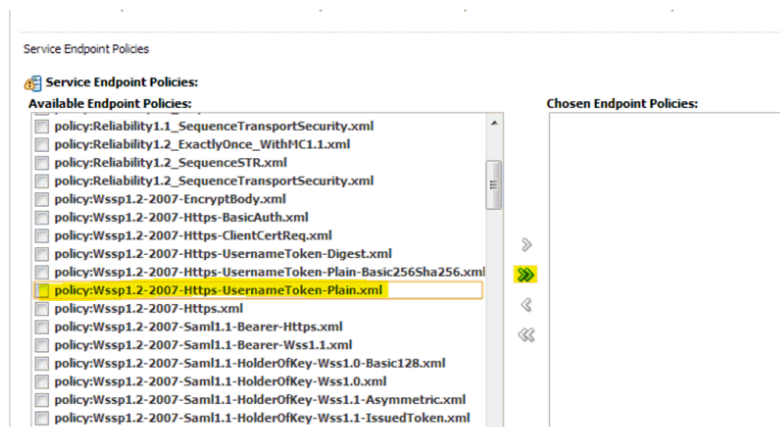
10. Click **OK** if WebLogic prompts you to save Plan.xml.

Updating the Webservice deployment

Perform the following steps to update the Webservice deployment:

1. In WebLogic Admin Console, click **Deployments**.

2. Click **Lock & Edit** and select the deployed application which has the Webservices to be secured.

3. Click **Update** and select the deployment ear along with the Plan.xml if saved in the previous steps.

4. Click **Finish**.

5. Click **Activate Changes** to reflect the changes.

6. Verify the configuration by checking the WSDL of the service.

   The WSDL must have the policy information in it.

Webservice Clock Skew setting

Webservices when secured need to be time synched with providers and consumers. However, due to various reasons the providers and consumers can have different time gap.

Weblogic can be configured to different tolerance level for webservices to work.

Perform the following steps to set the tolerance level of time different:

1. Navigate to WLS Console > Domain > Web Service Security > default_wss > Timestamp.

2. Click **Lock and Edit** and update the **Clock Skew** with tolerance limit (in milliseconds).

3. Click **Activate Changes**.

Figure 11–6   Setting the Tolerance Level of Time Different
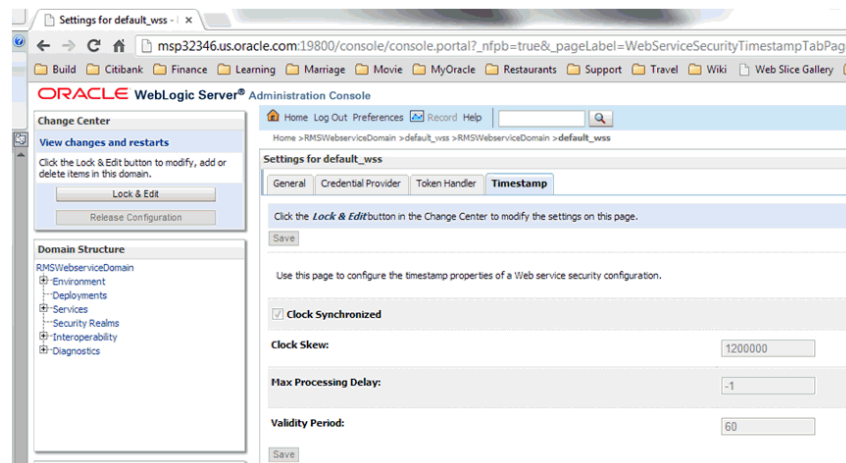
4. Bounce the managed server hosting Webservice once the changes are implemented.

Applying Policy B

Applying policy B involves the following:

- Creating the Webservice users

- Securing services

- Updating the Webservice deployment

Creating the Webservice user

Perform the following steps to create roles and users who can access the Web services:

1. In WebLogic Admin Console, click the Domain Structure window, and click the Security Realms link.

   The default realm appears.

2. Click the link on the realm.

3. Click the **Users and Groups** tab.

4. Click **New**.

5. Enter the user name and password details on the next screen.

6. Leave the default value for Provider.

7. Click **OK** to save the changes.

   The new user is shown in the list of users.

Securing services

Perform the following steps in WebLogic Admin Console for each of the services to be secured:

1. Attach the user created in previous step to the service.

2. Click Deployments.

3. Click the service you want to secure.

4. Click **Securities** and then **Policies**.

Figure 11–7   Securing Services

5. Click Add **Conditions** > Predict List: Pick User from dropdown > Next > User Argument Name: > Type username you created > Add > Finish > Save.

Figure 11–8   Add Conditions Window

6. Attach policy to the service.

7. Navigate to **Configuration** tab.

8. Click **WSB Policy** tab and select the service port.

Figure 11–9   Attaching WS Policy to the Service
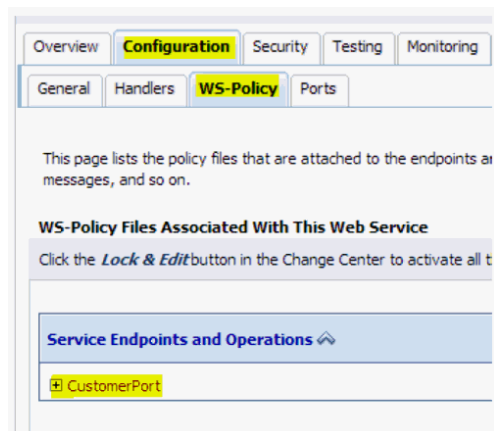
9. Pick WebLogic > Next > Service Endpoint Policies: select policy:Wssp1.22007HttpsUsernameTokenPlain.xml > Finish

Figure 11–10   Service Endpoint Policies
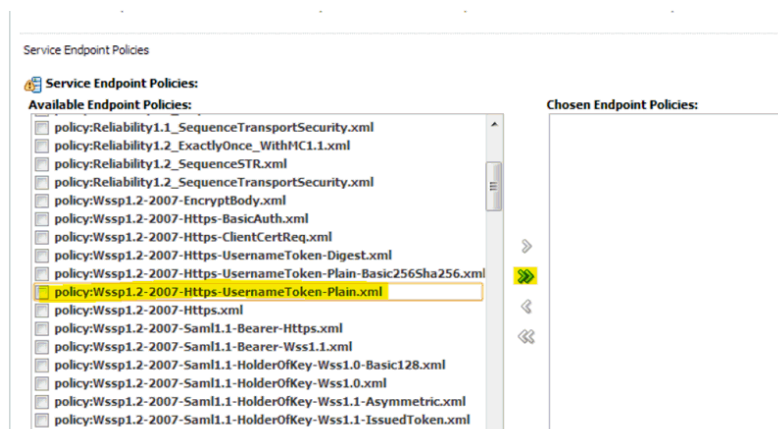
10. Click **OK** if WebLogic prompts you to save Plan.xml.

Updating the Webservice deployment

Perform the following steps to update the Webservice deployment:

1. In WebLogic Admin Console, click **Deployments**.

2. Click **Lock & Edit** and select the deployed application which has the Webservices to be secured.

3. Click **Update** and select the deployment ear along with the Plan.xml if saved in the previous steps.

4. Click **Finish**.

5. Click **Activate Changes** to reflect the changes.

6. Verify the configuration by checking the WSDL of the service.

   The WSDL must have the policy information in it.

ReSTful Services

Services are secured using J2EE-based security model.

- **Realm-based User Authentication**: This verifies users through an underlying Realm. The username and password is passed using HTTP basic authentication.

- **Role-based Authorization**: This assigns users to roles; you can either grant or restrict access to the resource/service. The authorization to the ReSTful Web services is static and cannot be reassigned to other roles during post installation.

Role Name: DATA_STEWARD_MANAGER

Principal Name: DATA_STEWARD_MANAGER_JOB

All enterprise roles defined in the table are mapped in web.xml and weblogic.xml of the ReST Service web application.

- The communication between the server and the client is encrypted using one way SSL. In a non-SSL environment, the encoding defaults to BASE-64 so it is highly recommended that these ReST services are configured to be used in production environments secured with SSL connections.

- RMS user data security is implemented in the APIs. The application user ID should be added to the RMS SEC_USER.APP_USER_ID table then associated to the appropriate group in SEC_USER _GROUP table.

For more information on the secure implementation of Webservices, see the *RMS Implementation Guide*.

12

Extending/Customization

Customization and extending capabilities is an important part of any application. This chapter discusses how to securely implement customizations and extensions such that they do not jeopardize application security.

If customization is required it should be done in such a way that no built-in explicit security features would be circumvented.

If additional integration credentials are required, the customization should store them in the Secure Credential Store along with all other RMS credentials.

Part III

Oracle Retail Sales Audit (ReSA)

Oracle Retail Sales Audit (ReSA) is a part of the Merchandise Operations Management (MOM) product group. The chapters mentioned below are for users and administrators of Oracle Retail Sales Audit. This includes auditors, auditor managers, finance manager, and administrative personnel.

Part III contains the following chapters:

- ReSA Security Considerations

For more information on ReSA Security Considerations, see Chapter 8, "Functional Security for Applications Using Fusion Middleware".

13

ReSA Security Considerations

The chapter provides guidance for administrators to understand, configure, and customize functional security for the Oracle Retail Sales Audit (ReSA) application.

The following topics are covered in this chapter:

- Default Security Configuration
- Data Security
- Securing ReSA Tables

> **Note:** ReSA should implement similar file permissions as the RMS. For more information, see File Permissions.

Default Security Configuration

Access control of system resources is achieved by requiring users to authenticate at login and by restricting users to only those resources for which they are authorized. A default security configuration is available for immediate use after the Oracle Retail Fusion application is installed and is configured to use the Oracle Fusion Middleware security model. The default configuration includes four predefined security roles for application specific permission grants. Users can be added to predefined groups that are mapped to pre-configured application roles. ReSA is pre-configured to grant specific application permissions.

Table 13–1   Privileges

Name	Description
Search Store Days Priv	A privilege for searching for store days and store day total transaction data summary information (transaction data summary).
Maintain Store Days Priv	A privilege for editing a store day including error list, over/short totals, miscellaneous totals, combined totals, total export log, revisions of totals (total audit trail), missing transactions and comments.
Delete Store Day Priv	A privilege for deleting a store day.

Table 13–1 (Cont.) Privileges

Name	Description
View Store Day Priv	A privilege for viewing a store day including error list, over/short totals, miscellaneous totals, combined totals, total export log, revisions of totals (total audit trail), missing transactions, store day import log, store day export log, store day total transaction data summary information (transaction data summary), and comments.
Manually Set Store Day Data Status Priv	A privilege for submitting an allocation for approval.
Reset Store Day Audit Status Priv	A privilege for resetting a store day's audit status.
Search Transactions Priv	A privilege for searching for transactions, transaction revisions (audit trail) and transaction summaries (item and tender).
Maintain Transactions Priv	A privilege for creating and editing transactions, mass updating items on transactions through Item Summary, and comments.
Delete Transactions Priv	A privilege for deleting transactions.
View Transactions Priv	A privilege for viewing transactions, transaction revisions (audit trail), transaction summaries (item and tender) and comments.
Post Void Transactions Priv	A privilege for post voiding transactions.
Maintain Application Administration Priv	A privilege for editing system options.
View Application Administration Priv	A privilege for viewing system options.
Search Total Definition Priv	A privilege for searching total definitions.
Maintain Total Definition Priv	A privilege for creating and editing total definitions.
Submit Total Definition Priv	A privilege for submitting a total definition for review.
Approve Total Definition Priv	A privilege for approving a total definition.
Disable Total Definition Priv	A privilege for disabling a total definition.
Delete Total Definition Priv	A privilege for deleting a total definition.
View Total Definition Priv	A privilege for viewing total definitions.
Search Audit Rule Priv	A privilege for searching audit rules.
Maintain Audit Rule Priv	A privilege for creating and editing audit rules.
Submit Audit Rule Priv	A privilege for submitting an audit rule for review.
Approve Audit Rule Priv	A privilege for approving an audit rule.
Disable Audit Rule Priv	A privilege for disabling an audit rule.
Delete Audit Rule Priv	A privilege for deleting an audit rule.
View Audit Rule Priv	A privilege for viewing audit rules.
Maintain ACH Information Priv	A privilege for maintaining Bank ACH and Store ACH information.
View ACH Information Priv	A privilege for viewing Bank ACH and Store ACH information.

Table 13–1   (Cont.) Privileges

Name	Description
Maintain ReSA Admin Data Priv	A privilege for maintaining error messages, GL (General Ledger) Cross Reference, Reference Fields, Currency Rounding Rules, and Store Data through Admin Data Loading.
View ReSA Admin Data Priv	A privilege for viewing error messages, GL (General Ledger) Cross Reference, Reference Fields, Currency Rounding Rules, and Store Data through Admin Data Loading.
View GL Drill Back Priv	A privilege for viewing General Ledger Drill Back.
View GL Cross Reference Priv	A privilege for viewing GL Cross Reference through Foundation Data Loading.
Maintain Bank Store Priv	A privilege for maintaining Bank Store relationships.
View Bank Store Priv	A privilege for viewing Bank Store relationships.
Maintain Employees Priv	A privilege for viewing assigned stores for ReSA users through location traits.
View Employees Priv	A privilege for viewing assigned stores for ReSA users through location traits.
Maintain Error Override Priv	A privilege for editing the Override check box on the Error List tab in either the Store Day Summary or Balance Level Summary screens.
View Error Override Priv	A privilege for viewing the Override check box on the Error List tab in either the Store Day Summary, Balance Level Summary screens, or on the Sales Audit Errors popup.
View Store Day Summary Over/Short Value Priv	A privilege for viewing the Over/Short value in the Status container in the Store Day Summary screen.
View Balance Level Summary Over/Short Value Priv	A privilege for viewing the Over/Short value in the Status container in the Balance Level Summary screen.
View Over/Short Totals Trial Over/Short Values Priv	A privilege for viewing the Trial Over/Short values in both the Accounted for and the Accountable containers on the Over/Short Totals tab in either the Store Day Summary or the Balance Level Summary screens.
Maintain Over/Short Totals HQ Reported Value Priv	A privilege for editing the HQ Reported values in both the Accounted For and the Accountable For containers on the Over/Short Totals tab in either the Store Day Summary or Balance Level Summary screens.
View Over/Short Totals HQ Reported Value Priv	A privilege for viewing the HQ Reported values in both the Accounted For and the Accountable For containers on the Over/Short Totals tab in either the Store Day Summary or Balance Level Summary screens.
Maintain Miscellaneous Totals HQ Reported Value Priv	A privilege for editing the HQ Reported value on the Miscellaneous Totals tab in either the Store Day Summary or Balance Level Summary screens.

Table 13–1 (Cont.) Privileges

Name	Description
View Miscellaneous Totals HQ Reported Value Priv	A privilege for viewing the HQ Reported value on the Miscellaneous Totals tab in either the Store Day Summary or Balance Level Summary screens.
View System Calculated Totals Value Priv	A privilege for viewing the System Reported Totals values in both the Accounted For and the Accountable For containers on the Over/Short Totals tab in either the Store Day Summary or Balance Level Summary screens, as well as on the Miscellaneous Totals tab in either the Store Day Summary or Balance Level Summary screens.
View Flash Reports Priv	A privilege for viewing the Flash Totals and Flash Sales reports accessed through the main Tasks list or through the Store Day Summary screen.
View Transaction Reports Priv	A privilege for viewing the Credit Card Summary and the Voucher Activity reports accessed through the main Tasks list.

Table 13–2 Duties

Duty	Description	List of Privileges
Store Day Inquiry Duty	A duty for viewing store days.	Search Store Days Priv View Store Days Priv View Flash Reports Priv
Store Day Management Duty	A duty for managing Store Days. This duty is an extension of the Store Day Inquiry Duty.	All privileges found in the Store Day Inquiry Duty. Maintain Store Day Priv Delete Store Day Priv
Store Day Manual Status Update Duty	A duty for setting a Store Day's Data Status and Audit Status.	Manually Set Store Day Data Status Priv Reset Store Day Audit Status Priv
Transaction Inquiry Duty	A duty for viewing transactions, transaction revisions and transaction summaries.	Search Transactions Priv View Transactions Priv View Transaction Reports Priv
Transaction Management Duty	A duty for managing transactions. This duty is an extension of the Transaction Inquiry Duty.	All privileges found in the Transaction Inquiry Duty. Maintain Transaction Priv Delete Transaction Priv
Transaction Post Void Duty	A duty for post voiding a transaction.	Post Void Transaction Priv
Application Administration Inquiry Duty	A duty for viewing ReSA System Options.	View Application Administration Priv

Table 13–2   (Cont.) Duties

Duty	Description	List of Privileges
Application Administration Management Duty	A duty for managing ReSA System Options. This duty is an extension of the Application Administration Inquiry Duty.	All privileges found in the Application Administration Inquiry Duty. Maintain Application Administration Priv
Total Definition Inquiry Duty	A duty for viewing total definitions.	Search Total Definition Priv View Total Definition Priv
Total Definition Management Duty	A duty for managing total definitions. This duty is an extension of the Total Definition Inquiry Duty.	All privileges found in the Total Definition Inquiry Duty. Maintain Total Definition Priv Delete Total Definition Priv
Total Definition Submit Duty	A duty for submitting an Total Definition for approval.	Submit Total Definition Priv
Total Definition Review Duty	A duty for approving or disabling a total definition.	Approve Total Definition Priv Disable Total Definition Priv
Audit Rule Inquiry Duty	A duty for viewing audit rules.	Search Audit Rule Priv View Audit Rule Priv
Audit Rule Management Duty	A duty for managing audit rules. This duty is an extension of the Audit Rule Inquiry Duty.	All privileges found in the Audit Rule Inquiry Duty. Maintain Audit Rule Priv Delete Audit Rule Priv
Audit Rule Submit Duty	A duty for submitting an audit rule for approval.	Submit Audit Rule Priv
Audit Rule Review Duty	A duty for approving or disabling an audit rule.	Approve Audit Rule Priv Disable Audit Rule Priv
ACH Information Inquiry Duty	A duty for viewing ACH information including Bank ACH and Store ACH.	View ACH Information Priv
ACH Information Management Duty	A duty for managing ACH information. This duty is an extension of the ACH Information Inquiry Duty.	All privileges found in the ACH Information Inquiry Duty. Maintain ACH Information Priv
ReSA Admin Data Management Duty	A duty for managing ReSA Error Messages, GL Cross Reference, Reference Fields, Currency Rounding Rules and Store Data through the Upload and Download Actions in Admin Data Loading. This duty is an extension of the Admin Data Inquiry Duty.	View ReSA Admin Data Priv Maintain ReSA Admin Data Priv
Bank Store Inquiry Duty	A duty for viewing Bank Store.	View Bank Store Priv
Bank Store Management Duty	A duty for managing Bank Store. This duty is an extension of the Bank Store Inquiry Duty.	All privileges found in the Bank Store Inquiry Duty. Maintain Bank Store Priv
Employee Inquiry Duty	A duty for viewing Employee.	View Employees Priv

Table 13–2 (Cont.) Duties

Duty	Description	List of Privileges
Employee Management Duty	A duty for managing Employee. This duty is an extension of the Employee Inquiry Duty.	All privileges found in the Employee Inquiry Duty. Maintain Employees Priv
Error Override Review Duty	A duty for viewing the Override check box on the Error List tab on either the Store Day Summary or Balance Level Summary screens, or on the Sales Audit Errors popup.	View Error Override Priv
Error Override Management Duty	A duty for the ability to override errors by checking the Override check box on the Error List tab on either the Store Day Summary or Balance Level Summary screens.	All privileges found in the Error Override Review Duty. Edit Error Override Priv
Totals HQ Reported Value Review Duty	A duty for viewing the HQ Reported values on both the Over/Short Totals and Miscellaneous Totals tabs on either the Store Day Summary or Balance Level Summary screens.	View Over/Short Totals HQ Reported Value Priv View Miscellaneous Totals HQ Reported Value Priv
Totals HQ Reported Value Management Duty	A duty for the ability to override errors by checking the Override check box on the Error List tab on either the Store Day Summary or Balance Level Summary screens.	All privileges found in the Totals HQ Reported Value Review Duty. Edit Over/Short Totals HQ Reported Value PrivEdit Miscellaneous Totals HQ Reported Value Priv
Over/Short Value Review Duty	A duty for viewing the Over/Short values in the Status container on either the Store Day Summary or Balance Level Summary screens as well as the Trial Over/Short values on the Over/Short Totals tabs in either the Store Day Summary or Balance Level Summary screens.	View Store Day Summary Over/Short Value Priv View Balance Level Summary Over/Short Value Priv View Over/Short Totals Trial Over/Short Values Priv
Totals System Reported Value Review Duty	A duty for viewing the System Reported values on both the Over/Short Totals and Miscellaneous Totals tabs on either the Store Day Summary or Balance Level Summary screens.	View System Calculated Totals Value Priv
GL Inquiry Duty	A duty for viewing GL Cross Reference and GL Drill Back.	View GL Cross Reference Priv View GL Drill Back Priv

Table 13–3   Function Security Mapping

Duty	Description	List of Privileges
Sales Audit Analyst	Store Day Management Duty	Search Store Days Priv
	Store Day Manual Status Update Duty	Maintain Store Days Priv
		Delete Store Day Priv
	Transaction Management Duty	View Store Day Priv
	Transaction Post Void Duty	Manually Set Store Day Data Status Priv
	Total Definition Management Duty	Reset Store Day Audit Status Priv
	Total Definition Submit Duty	View Flash Reports Priv
	Total Definition Review Duty	Search Transactions Priv
	Audit Rule Management Duty	Maintain Transactions Priv
	Audit Rule Submit Duty	Delete Transactions Priv
	Audit Rule Review Duty	View Transactions Priv
	ACH Information Management Duty	Post Void Transactions Priv
	Error Override Management Duty	View Transaction Reports Priv
		Search Total Definition Priv
	Error Override Review Duty	View Total Definition Priv
	Totals HQ Reported Value Management Duty	Maintain Total Definition Priv
		Delete Total Definition Priv
	Totals HQ Reported Value Review Duty	Submit Total Definition Priv
	Totals System Reported Value Review Duty	Approve Total Definition Priv
		Disable Total Definition Priv
	Over/Short Value Review Duty	Search Audit Rule Priv
		View Audit Rule Priv
		Maintain Audit Rule Priv
		Delete Audit Rule Priv
		Submit Audit Rule Priv
		Approve Audit Rule Priv
		Disable Audit Rule Priv
		Maintain ACH Information Priv
		View ACH Information Priv
		Edit Error Override Priv
		View Error Override Priv
		Edit Over/Short Totals HQ Reported Value Priv
		View Over/Short Totals HQ Reported Value Priv
		Edit Miscellaneous Totals HQ Reported Value Priv
		View Miscellaneous Totals HQ Reported Value Priv
		View System Calculated Totals Value Priv

Table 13–3   (Cont.) Function Security Mapping

Duty	Description	List of Privileges
		View Store Day Summary Over/Short Value Priv
		View Balance Level Summary Over/Short Value Priv
		View Over/Short Totals Trial Over/Short Values Priv

Table 13–3   (Cont.) Function Security Mapping

Duty	Description	List of Privileges
Sales Audit Manager	Store Day Management Duty	Search Store Days Priv
	Store Day Manual Status Update Duty	Maintain Store Days Priv
		Delete Store Day Priv
	Transaction Management Duty	View Store Day Priv
	Transaction Post Void Duty	Manually Set Store Day Data Status Priv
	Total Definition Management Duty	Reset Store Day Audit Status Priv
	Total Definition Submit Duty	View Flash Reports Priv
	Total Definition Review Duty	Search Transactions Priv
	Audit Rule Management Duty	Maintain Transactions Priv
	Audit Rule Submit Duty	Delete Transactions Priv
	Audit Rule Review Duty	View Transactions Priv
	ACH Information Management Duty	Post Void Transactions Priv
	ReSA Admin Data Management Duty	View Transaction Reports Priv
		Search Total Definition Priv
	Employee Management Duty	View Total Definition Priv
	Error Override Management Duty	Maintain Total Definition Priv
		Delete Total Definition Priv
	Error Override Review Duty	Submit Total Definition Priv
	Totals HQ Reported Value Management Duty	Approve Total Definition Priv
	Totals HQ Reported Value Review Duty	Disable Total Definition Priv
		Search Audit Rule Priv
	Totals System Reported Value Review Duty	View Audit Rule Priv
	Over/Short Value Review Duty	Maintain Audit Rule Priv
		Delete Audit Rule Priv
		Submit Audit Rule Priv
		Approve Audit Rule Priv
		Disable Audit Rule Priv
		Maintain ACH Information Priv
		View ACH Information Priv
		Maintain ReSA Admin Data Priv
		View ReSA Admin Data Priv
		Maintain Employees Priv
		View Employees Priv
		Edit Error Override Priv
		View Error Override Priv
		Edit Over/Short Totals HQ Reported Value Priv
		View Over/Short Totals HQ Reported Value Priv
		Edit Miscellaneous Totals HQ

Table 13–3   (Cont.) Function Security Mapping

Duty	Description	List of Privileges
		Reported Value Priv
		View Miscellaneous Totals HQ Reported Value Priv
		View System Calculated Totals Value Priv
		View Store Day Summary Over/Short Value Priv
		View Balance Level Summary Over/Short Value Priv
		View Over/Short Totals Trial Over/Short Values Priv
Finance Manager	Store Day Inquiry Duty	Search Store Days Priv
	Transaction Inquiry Duty	View Store Day Priv
	GL Management Duty	View Flash Reports Priv
	Bank Store Management Duty	Search Transactions Priv
	Total Definition Management Duty	View Transactions Priv
		View Transaction Reports Priv
	Total Definition Submit Duty	Maintain ReSA Admin Data Priv
	Total Definition Review Duty	View ReSA Admin Data Priv
	ACH Information Inquiry Duty	View GL Drill Back Priv
	Audit Rule Inquiry Duty	Maintain Bank Store Priv
	Error Override Review Duty	View Bank Store Priv
	Totals HQ Reported Value Review Duty	Search Total Definition Priv
		View Total Definition Priv
	Totals System Reported Value Review Duty	Maintain Total Definition Priv
	Over/Short Value Review Duty	Delete Total Definition Priv
		Submit Total Definition Priv
		Approve Total Definition Priv
		Disable Total Definition Priv
		View ACH Information Priv
		View Audit Rules Priv
		View Error Override Priv
		View Over/Short Totals HQ Reported Value Priv
		View Miscellaneous Totals HQ Reported Value Priv
		View System Calculated Totals Value Priv
		View Store Day Summary Over/Short Value Priv
		View Balance Level Summary Over/Short Value Priv
		View Over/Short Totals Trial Over/Short Values Priv

Table 13–3   (Cont.) Function Security Mapping

Duty	Description	List of Privileges
Sales Audit System Administrator	Store Day Inquiry Duty	Search Store Days Priv
	Store Day Management Duty	Maintain Store Days Priv
	Store Day Manual Status Update Duty	Delete Store Day Priv
		View Store Day Priv
	Transaction Inquiry Duty	Manually Set Store Day Data Status Priv
	Transaction Management Duty	
	Transaction Post Void Duty	Reset Store Day Audit Status Priv
	Application Administration Inquiry Duty	Search Transactions Priv
		Maintain Transactions Priv
	Application Administration Management Duty	Delete Transactions Priv
		View Transactions Priv
	Total Definition Inquiry Duty	View Employees Priv
	Total Definition Management Duty	Post Void Transactions Priv
	Total Definition Submit Duty	Maintain Application Administration Priv
	Total Definition Review Duty	Application Administration Priv
	Audit Rule Inquiry Duty	Total Definition Priv
	Audit Rule Management Duty	Maintain Total Definition Priv
	Audit Rule Submit Duty	Submit Total Definition Priv
	Audit Rule Review Duty	Approve Total Definition Priv
	ACH Information Inquiry Duty	Disable Total Definition Priv
	ACH Information Management Duty	Delete Total Definition Priv
	ReSA Admin Data Management Duty	Total Definition Priv
		Audit Rule Priv
	Bank Store Inquiry Duty	Maintain Audit Rule Priv
	Bank Store Management Duty	Submit Audit Rule Priv
	Employee Inquiry Duty	Approve Audit Rule Priv
	Employee Management Duty	Disable Audit Rule Priv
	Error Override Review Duty	Delete Audit Rule Priv
	Error Override Management Duty	Audit Rule Priv
	Totals HQ Reported Value Review Duty	Maintain ACH Information Priv
		View ACH Information Priv
	Over/Short Value Review Duty	Maintain ReSA Admin Data Priv
	Totals System Reported Value Review Duty	View ReSA Admin Data Priv
		View GL Drill Back Priv
		Maintain Bank Store Priv
		View Bank Store Priv
		Maintain Employees Priv
		View Employees Priv
		Maintain Error Override Priv
		View Error Override Priv
		View Store Day Summary Over/Short Value Priv

Table 13–4   Function Security Mapping (Cont.)

Duty	Description	List of Privileges
		View Balance Level Summary Over/Short Value Priv
		View Over/Short Totals Trial Over/Short Values Priv
		Maintain Over/Short Totals HQ Reported Value Priv
		View Over/Short Totals HQ Reported Value Priv
		Maintain Miscellaneous Totals HQ Reported Value Priv
		View Miscellaneous Totals HQ Reported Value Priv
		View System Calculated Totals Value Priv
		View Flash Reports Priv
		View Transaction Reports Priv
		View All Reports Priv
		GL Inquiry Duty

Table 13–5   Role to Task Mapping

Column Name	Role			
	Sales Auditor	**Sales Auditor Manager**	**Finance Manager**	**Administrator**
Main Navigation Tasks	Store Day Audit	Store Day Audit	Store Day Audit (View Only)	Foundation Data Loading ■ All
	Create Transaction	Create Transaction	Manage Transaction (View Only)	System Options
	Manage Transactions	Manage Transactions	Foundation Data Loading ■ All	RMS Company Closing
	Bank ACH	Bank ACH	Create Total Definition	Employees
	Store ACH	Store ACH	Manage Total Definition	Bank Store
	Total Audit Trail	Total Audit Trail	Bank Store	
	Transaction Audit Trail	Transaction Audit Trail	Bank ACH (View Only)	
	Item Summary	Item Summary	Store ACH (View Only)	
	Tender Summary	Tender Summary	General Ledger Drill Back	
	Create Audit Rule	Create Audit Rule	Manage Audit Rule (View Only)	

Table 13–5   (Cont.) Role to Task Mapping

Column Name	Sales Auditor	Sales Auditor Manager	Finance Manager	Administrator
			Role	
	Manage Audit Rule	Manage Audit Rule	View Reports ▪ Flash Totals ▪ Flash Sales ▪ Credit Card Summary ▪ Voucher Activity	
	Create Total Definitions	Create Total Definitions		
	Manage Total Definitions	Manage Total Definitions		
	View Reports ▪ Flash Totals ▪ Flash Sales ▪ Credit Card Summary ▪ Voucher Activity	RMS Company Closing		
		Employees		
		Foundation Data Loading ▪ All		
		View Reports ▪ Flash Totals ▪ Flash Sales ▪ Credit Card Summary ▪ Voucher Activity		

Data Security

Data security can be set up to limit visibility to data within the merchandise and organizational Hierarchies. In ReSA, only data security on the organizational hierarchy is used. ReSA users have access to all items in the merchandise hierarchy, but can only see data for stores to which they have data authorization based on this data security setup in RMS.

For more information on the Data security, see Security Features of the Application section under Chapter 10.

ReSA uses the application logged in LDAP ID. The logged in application user ID is copied to database session context RETAIL_CTX. APP_USER_ID. The RMS security table SEC_USER holds the application user ID and the database user ID. The data security function uses the application user ID for applying the security policy if database session context RETAIL_CTX. APP_USER_ID is available else, it uses the logged in database ID for applying security policy.

Securing ReSA Tables

When setting up RMS database roles and privileges, it is important to consider that roles with access to the RMS schema also have access to sensitive ReSA data. The ReSA tables listed in Table 13–6 contain sensitive information, including bank account information. ReSA resides in the same database as RMS and other MOM products, so it may be required to secure the ReSA tables so that unauthorized users do not access/modify the data in the ReSA tables. This access can be secured by using the database roles and privileges. Caution is advised when applying duplicate ReSA application login rules and/or privileges to non-ReSA users, as the sensitive data in the below tables will be accessible to these users.

Additionally, the following ReSA tables should be protected via an encrypted tablespace. For more information on setting up an encrypted tablespace, see Chapter 2 Creating an Encrypted Tablespace in Oracle 12c Container Database section.

Due to the sensitive nature of the data in these ReSA tables, any new custom applications used by the retailer must be fully tested for SQL injection vulnerabilities, especially if the applications have full access to the RMS schema.

It is recommended that access to these tables is audited by the retailer. Oracle RMS and ReSA are the only Oracle-supplied software that have access to these tables. Batch programs that access these tables can be found in the Oracle Retail Sales Audit Operations Guide. If sensitive data in these tables is not used by the retailer, it is recommended that this data is removed from the tables.

Table 13–6   ReSA Tables

User Name
SA_TRAN_TENDER_REV
SA_BANK_ACH
SA_TRAN_TENDER
SA_BANK_STORE
SA_CUSTOMER

One other additional recommended security measure is for retailers to ensure that credit card numbers are not sent in to ReSA through the RTLOG files. The credit card number field in the TTEND record should be sent in as NULL.

Credit Card Information and Check Account Number Information Processing

The Credit card information and check account number information processing has changed for ReSA version 16.0. In previous releases when ReSA receives an RTLOG with a non-masked credit card number, it simply logs an error in the system and continues with the processing.

With version 16.0, when ReSA encounters an RTLOG with a non-masked credit card number, the entire file will be rejected and will not be processed. To adhere to this security measure, it is recommended that retailers ensure that credit card numbers are masked when sent through RTLOGs.

Similarly, when the tender type is check, it is recommended that retailers ensure that check account numbers are masked when sent through RTLOGs. In version 16.0, when

non-masked check account numbers are encountered, the entire file will be rejected and will not be processed.

For more information on Merch Mobile Security Consideration, see the ReST Services Security Consideration chapter.

For more information on the ReST Services Security Consideration, see the *Oracle Retail Sales Audit Operations Guide*.

ReSTful Web Services

Services are secured using J2EE-based security model.

1. Realm-based User Authentication. This verifies users through an underlying realm. The username and password is passed using Http Basic authentication.

2. Role-based Authorization. This assigns users to roles, which in turn are granted or restricted access to resources/services. The authorization of ReSTful web services is static and cannot be reassigned to other rules post installation. The following role(s) is/are associated with ReSTful Web Services and should be added to the Enterprise LDAP:

   - ADMINISTRATOR_JOB

   - AUDITOR_JOB

   - AUDITOR_MANAGER_JOB

   - FINANCE_MANAGER_JOB

All enterprise roles defined above are mapped in web.xml and weblogic.xml of the ReST Service webapp.

The communication between the server and client is encrypted using one way SSL. In non-SSL environments the encoding defaults to BASE-64 so it is highly recommended that these ReST services are configured to be used in production environments secured with SSL connections.

For information on secure implementation of ReSTful services, see the *ReSA Implementation Guide*.

Part IV

Oracle Retail Invoice Matching (ReIM)

The following chapters provide guidance for administrators, developers, and system integrators who securely administer, customize, and integrate the Oracle Retail Invoice Matching (ReIM) application.

Part IV contains the following chapters:

- General Security Considerations
- Understanding Security
- Post Installation - ReIM Application Administration
- Extending/Customization
- Securing the Database

14

General Security Considerations

This chapter discusses how to securely install the Oracle Retail Invoice Matching (ReIM) application. To obtain a secure configuration, follow the instructions and advice provided below.

The ReIM application is installed on a managed server, but is used in the distributed environment. Both client and server security should be taken into consideration when hardening application deployment. You need to reference your desktop and server operation system security guides, if available for more information on reinforcing security for the execution environment.

In particular, only valid users should have access to the client workstations running clients for the application. The reasonable locking policy should be established to lock out computer screens after some time of inactivity. The Security policy should be established at the desktop level to monitor unsuccessful login attempts. The System administrator should guarantee that the operation system has the latest mandatory update patches.

You should use only the supported browsers to access the application. The browsers should be patched with all the mandatory security updates dictated by the browser's vendor. The browser's auto-complete feature should be disabled by the system administrator. It is advised to add the server ReIM is deployed at to the list of sites for Local Intranet in the Web browser. The browser should be allowed to open pop-ups initiated by the Invoice Matching application. In addition, the browser should allow submitting non-encrypted form data.

For more information on how to secure the internal network used to access Invoice Matching server(s), see the *Network Security Configuration Guide*. This should include both physical and logical security of the network. Only SSL enabled communication should be used. Please make sure that browsers have certificates verification turned on.

Only the desktops on the intranet should be allowed to access the application server. The best approach is to limit the set of client computers on the network that can access the application server. That can be done at the network level to prevent guest users on the local network from even seeing the application server. In addition, the server can be configured to serve requests from the specified set of network addresses.

Only system administrators should have access to the application server(s). Business users (even power users) should not an account on the application server. If such accounts do exist, the OS account privileges should prevent business user from accessing application server files/directories associated with the Invoice Matching application.

The users running batches should never be OS system administrators or WebLogic administrator. The best approach is to have a single dedicated user for running

batches, rather than having multiple users running batches ad hoc. The user running batches should have ReIM application administrator privileges. The user should be setup with access to all locations (see location Security section below).

Only authorized users should be able to upload/download files consumed/produced by the Invoice Matching application. The directory structure for incoming EDI files should be accessible to the OS user running batches as read-only. It is recommended to keep outbound files in a separate directory. The outbound files directory should allow write access. It is also recommended to have separate write accessible directories for rejected files and for audit files. Please note that the system maintains the reference to the locations of the intended loads rejection and will attempt o write to that location at the later load retries. As such, the locations should be accessible for writing even after initial load attempt.

Management of spreadsheet files on client's workstations for the document upload and rejection download processes should be done securely. As rejection data files can be downloaded by a user different than the once that supplied the files for upload, care should be taken to control file access. Users triggering the upload process should be responsible for the files getting uploaded.

It is recommended to keep audit copies of any processed files and it is up to the retailer to provide this process. Audit copies should be created prior to supplying the files for ReIM processing. The files can be kept in an audit directory or using any other appropriate document management system that would allow easy retrieval later on.

> **Note:** ReIM processes files that have been supplied by vendors or that have been supplied by RMS. Secure file transfer should be deployed in both cases.

It is also recommended to keep copies of the physical documents sent by vendors and manually entered into the system via the Document Entry screen, so that potential data integrity issues related to data entry can be resolved.

15

Understanding Security

This chapter provides an overview of all the security features available in the ReIM application. It is provided as a reference for how the application securely communicates with other applications; how the application authenticates, authorizes, and audits users; and the encryption and hashing mechanisms used by the application.

The following topics are covered in this chapter:

- Security Features Overview
- Dependent Applications
- Technical Overview of the Security Features
- ReIM Web Application Deployment
- Security Features of the Application
- Encryption and Hashing

Security Features Overview

Figure 15–1 shows the physical deployment of ReIM.

Figure 15–1   ReIM Physical Deployment
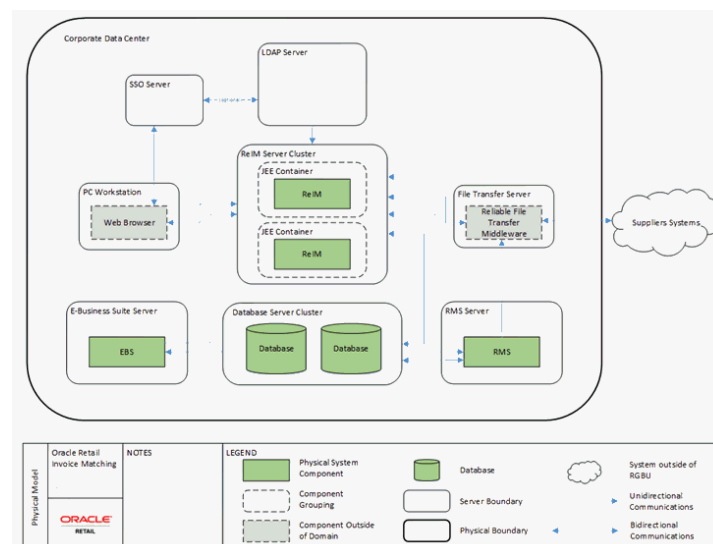
The Application Server is deployed on the corporate intranet on WebLogic cluster. The Application Server is connected to a cluster of Oracle databases and a corporate LDAP server or any other authentication provider. Optionally Single Sign-On infrastructure can be deployed. In addition, a secure FTP server is responsible for transferring files in/out of the application if EDI functionality is used. Optionally 3rd party batch running infrastructure can be deployed to run batch scripts (for example, Appworx, and so on). The client workstation can be either at the corporate data center or at the retailer locations (stores and warehouses). The client workstations need to run supported browsers with optionally printers attached. For file processing batches such as EDIInjector, the files should be on the network location accessible by the server.

The WebLogic Application Server executes the server side of the application logic. Oracle Database provides data handling functionality. A configured LDAP server can provide authentication or any other authentication provider can be used. Single Sign-On infrastructure provides capability to share authentication tokens across multiple retail applications. FTP server provides delivery for EDI files. Workstation browsers can be used to execute client side application logic. Printers can be used to create physical outbound documents when EDI functionality is not used.

ReIM exchanges data with other retail applications that are part of the Oracle Retail Suite, such as RMS, and with the applications that are not part of Oracle Retail Suite, such as Enterprise Business Suite (EBS) and PeopleSoft.

Each component of the deployment should be secured to provide minimum required access. This includes OS security, network security, browser security, LDAP security, WebLogic security, database Security, and FTP server security. For information on how to secure each component, see the reference documentation.

Dependent Applications

Security Guides for dependent applications are found at the following Web sites:

- Oracle Database 12 C Release 1:

  http://docs.oracle.com/database/121/DBSEG/toc.htm

- Oracle WebLogic 12.2.1:

  http://docs.oracle.com/middleware/1221/wls/INTRO/security.htm#INTRO232

  Contact your vendor for other components of security guides.

ReIM Web Application Deployment

SSL

The ReIM application should be deployed using a secure HTTP endpoint, but at the same ime regular HTTP can be used (although this is not advised). The secure application should only be available through an "https" protocol. This requires the associated Oracle HTTP Server to be configured appropriately and to register the secure endpoint with the Single Sign-On Server. Configuration of the WebLogic hosting ReIM application should be secured as per WebLogic documentation.

Single Sign-On

In the standard supported deployment, ReIM leverages Single Sign-On infrastructure for authentication (optional). To avoid clear-text transmission of user IDs and passwords, Single Sign-On infrastructure must be configured to user TLS/SSL within all offered URLs. For specific information on configuring Single Sign-On to use TLS/SSL, see the *WebLogic Single Sign-On Administrator's Guide*.

WebLogic Wallet

The ReIM application relies on WebLogic Application Server to provide secure storage and retrieval for username and passwords required to communicate with other security conscious components or to run batches. WebLogic stores data securely in Credential Store, where a Wallet is one of the possible implementations. Credential Store stores access credentials for Web services access on the server and Secure Wallet implementation of Credential Store is used on the client to store batch user credentials.

Technical Overview of the Security Features

The following section describes the authentication, authorization, audit, and user management.

Security Features of the Application

The relevant security features fall into one or more of the following categories. For information on these categories, see the following sections:

- Authentication
- Authorization
- Audit
- User Management

Authentication

Only authenticated users should have access to ReIM application. By the point of application authentication the user potentially successfully authenticates with the network and/or the workstation OS.

ReIM supports the following two types of authentication:

- Dedicated
- Single Sign-On

Dedicated authentication - User credentials (username and password) are submitted by the Application Server to the LDAP server or any other configured authentication provider If the authentication provider can successfully identify the user then that user is considered authenticated with the ReIM application. Dedicated authentication credentials are either provided by the online application user in real time (entering user name and password on the ReIM provided login page) or are retrieved by the client from the Secure Wallet in the case of batch process. The batch user still needs to provide credentials alias, so that the appropriate username and passwords is retrieved from the Secure Wallet.

Single Sign-On authentication - In case of Single Sign-On, authentication happens only once per application suite. Authentication is performed by Single Sign-On infrastructure (potentially backed by the same LDAP server as the case for dedicated authentication). In this case login page is provided by the Single Sign-On infrastructure.

In both cases of authentication, the authentication is performed when it is determined that the session is not authenticated or the session has been invalidated (in case of dedicated authentication).

Authorization

Only application users that belong to one of the ReIM user roles will be authorized to use functionality provided by the ReIM application. If the user is a valid enterprise user, login may be successful but authorization may prevent access to specific workflows based on the user's assigned role. Authorization is performed for each user driven operation. It is assumed that the batch user is assigned to the administrator role which is authorized to perform all operations.

Audit

Auditing can be performed at the application level and at the infrastructure level. The operating system (OS) can be configured to audit user access and processes invoked. The network layer can be configured to audit entire communication data set. The application server can be configured to audit access to the application, including all URLs requested. The database can be configured to audit each table separately or entire sessions. The ReIM application also has some limited auditing capabilities.

The application will maintain some level of audit trail by keeping track of the last user modifying data and the date and time it was done, as well as version id of the data. See LAST_UPDATED_BY.

- LAST_UPDATED_BY
- LAST_UPDATE_DATE
- CREATED_BY
- CREATION_DATE
- OBJECT_VERSION_ID

Additional audit can be performed by decreasing logging level of the application. In this case additional information is reported into logs. The drawback is that performance can suffer and that amount of log entries to be recorded will increase. You can selectively decrease logging (see Log4J and Java Logging documentation on logging configuration for more information). Also make sure that the log files generated by the application are secure and are accessible to authorized OS users only.

User Management

The ReIM application does not store or maintains users. Instead, ReIM relies on external systems such as LDAP to provide user management functionality on its behalf.

To create a new user to be used within the ReIM application, you need to create a new user in the LDAP or whatever data store the configured authentication provider relies on. To access ReIM workflows, the user should be assigned to a valid ReIM user role. If RMS data security is enabled, users must be added to the SEC_USER table and have REIM_USER_IND enabled. The user must also be mapped to a valid RMS security group in the SEC_USER_GROUP table.

> **Note:** When removing a user, you must also delete the user entries from the RMS security tables. Failure to do this could result in inherited privileges.

Encryption and Hashing

JPS encrypts data stored into the Secure Wallet. For more information on the default encryption algorithm used, see the *Credential Store Manager* section in WebLogic documentation.

16

Post Installation - ReIM Application Administration

This chapter provides information about application administrative tasks related to security. How to manage users and roles as well as some other common application administrative tasks such as secure credential management and logging are discussed.

The following topics are covered in this chapter:

- Roles and Permissions

- Other Common Application Administration

Roles and Permissions

ReIM has several predefined application roles:

- Accounts Payable Specialist

- Finance Manager

- Buyer

- Corporate Inventory Control Analyst

- ReIM Application Administrator

These application roles are predefined in the application's security descriptors and users are mapped from their respective enterprise roles through the configured WebLogic Security Providers. Typically, the deployment will use Oracle Internet Directory as the Security Provider and enterprise roles will exist as user groups in the LDAP. By default, WebLogic maps enterprise roles to application roles of the same name. Therefore, any LDAP users that should be considered for ReIM processing should be made a member of one of these groups.

As the name suggests, the Application Administrator role has the highest level of privileges whereas all other user roles will have a predefined subset of privileges. Avoid assigning all users to the Application Administrator role. This will grant users more privileges than is required.

The privileges and duties that comprise ReIM's application roles are as follows:

Table 16–1   Privileges

Name	Description
Search Documents Priv	A privilege for searching for documents.
Maintain Documents Priv	A privilege for creating and editing documents.
Delete Documents Priv	A privilege for deleting documents.
View Documents Priv	A privilege for viewing documents.
Pay Invoice Manually Priv	A privilege to allow user to pay an invoice before matching the invoice.
EDI Maintenance Priv	A privilege for allowing a user to fix EDI errors.
Reverse Debit Memo Priv	A privilege for allowing a user to reverse a Debit Memo.
Create Credit Note from CNR Priv	A privilege for allowing a user to create a credit note from a credit note request.
Void Credit Note Priv	A privilege for allowing a user to void a credit note.
Approve Document Priv	A privilege to approve documents.
Unmatch Priv	A privilege for allowing a user to unmatch a merchandise invoice.
Upload Documents Priv	A privilege for allowing a user to upload documents.
Search Financal Posting Error Priv	A privilege for searching for financial posting errors.
Maintain Financial Posting Error Priv	A privilege for editing financial posting errors.
View Financial Posting Error Priv	A privilege for viewing financial posting errors.
Search Tolerance Priv	A privilege for searching for tolerance settings.
Maintain Tolerance Priv	A privilege for creating and editing tolerance settings.
Delete Tolerance Priv	A privilege for deleting a tolerance setting.
View Tolerance Priv	A privilege for viewing for tolerance settings.
Search Tolerance Mapping Priv	A privilege for searching for tolerance mapping settings.
Maintain Tolerance Mapping Priv	A privilege for creating and editing tolerance mapping settings.
Delete Tolerance Mapping Priv	A privilege for deleting a tolerance mapping settings.
View Tolerance Mapping Priv	A privilege for viewing for tolerance mapping settings.
Search Match Strategy Priv	A privilege for searching for Match Strategy settings.
Maintain Match Strategy Priv	A privilege for creating and editing Match Strategy settings.
Delete Match Strategy Priv	A privilege for deleting a Match Strategy settings.

Table 16–1   (Cont.) Privileges

Name	Description
View Match Strategy Priv	A privilege for viewing for Match Strategy settings.
Search Match Strategy Mapping Priv	A privilege for searching for Match Strategy mapping settings.
Maintain Match Strategy Mapping Priv	A privilege for creating and editing Match Strategy mapping settings.
Delete Match Strategy Mapping Priv	A privilege for deleting a Match Strategy mapping setting.
View Match Strategy Mapping Priv	A privilege for viewing for Match Strategy mapping settings.
Search G/L Cross Reference Priv	A privilege for searching for G/L Cross Reference settings.
Maintain G/L Cross Reference Priv	A privilege for creating and editing t G/L Cross Reference settings.
Delete G/L Cross Reference Priv	A privilege for deleting a G/L Cross Reference setting.
View G/L Cross Reference Priv	A privilege for viewing for G/L Cross Reference settings.
Search Reason Code Priv	A privilege for searching for Reason Code settings.
Maintain Reason Code Priv	A privilege for creating and editing Reason Code settings.
Delete Reason Code Priv	A privilege for deleting a Reason Code setting.
View Reason Code Priv	A privilege for viewing for Reason Code settings.
Search G/L Options Priv	A privilege for searching for G/L Options settings.
Maintain G/L Options Priv	A privilege for creating and editing G/L Options settings.
Delete G/L Options Priv	A privilege for deleting a G/L Options settings.
View G/L Options Priv	A privilege for viewing for G/L Options settings.
Maintain System Options Priv	A privilege for creating and editing System Options settings.
Delete System Options Priv	A privilege for deleting a System Options setting.
View System Options Priv	A privilege for viewing for System Options settings.
Search Supplier Options Priv	A privilege for searching for Supplier Options settings.
Maintain Supplier Options Priv	A privilege for creating and editing Supplier Options settings.
Delete Supplier Options Priv	A privilege for deleting a Supplier Options setting.
View Supplier Options Priv	A privilege for viewing for Supplier Options settings.
Search Location Dynamic Mapping Priv	A privilege for searching for Location Dynamic Mapping settings.

Table 16–1 (Cont.) Privileges

Name	Description
Maintain Location Dynamic Mapping Priv	A privilege for creating and editing Location Dynamic Mapping settings.
Delete Location Dynamic Mapping Priv	A privilege for deleting a Location Dynamic Mapping setting.
View Location Dynamic Mapping Priv	A privilege for viewing for Location Dynamic Mapping settings.
Search Dept Class Dynamic Mapping Priv	A privilege for searching for Dept Class Dynamic Mapping settings.
Maintain Dept Class Dynamic Mapping Priv	A privilege for creating and editing Dept Class Dynamic Mapping settings.
Delete Dept Class Dynamic Mapping Priv	A privilege for deleting a Dept Class Dynamic Mapping settings.
View Dept Class Dynamic Mapping Priv	A privilege for viewing for Dept Class Dynamic Mapping settings.
Search Manual Match Priv	A privilege to allow a user search for invoices and receipts to be manually matched.
Manual Match Priv	A privilege to allow a user to match an invoice manually through the UI.
Search Credit Note Match Priv	A privilege to allow a user to search for Credit Notes to Credit Note Requests to be matched.
Credit Note Match Priv	A privilege to match Credit Notes to Credit Note Requests.
Search Discrepancy List Priv	A privilege to search for Discrepancies.
Cost Resolution Priv	A privilege to allow a cost discrepancy to be resolved.
Quantity Resolution Priv	A privilege to allow a quantity discrepancy to be resolved.
Search Tax Discrepancy List Priv	A privilege to search for Tax Discrepancies.
Tax Discrepancy Resolution Priv	A privilege to allow a tax discrepancy to be resolved.
Dashboard Priv	A privilege for viewing the dashboard.

Table 16–2 Duties

Duty	Description	List of Privileges
Document Management Duty	A Duty for managing documents. This duty is an extension of the Document Inquiry Duty.	- All privileges found in the Document Inquiry Duty. - Maintain Documents Priv. - Delete Documents Priv.
Document Inquiry Duty	A duty for viewing documents.	- View Documents Priv. - Search Documents Priv.
Pay Invoice Duty	A duty for paying an invoice manually.	Pay Invoice Manually Priv.
EDI Maintenance Duty	A duty for fixing EDI Errors.	EDI Maintenance Priv.

Table 16–2   (Cont.) Duties

Duty	Description	List of Privileges
Reverse Debit Memo Duty	A duty to allow user to reverse a Credit Note.	Reverse Debit Memo Priv.
Create Credit Note from CNR Duty	A duty to allow user to create a Credit Note from a Credit Note Request.	Create Credit Note from CNR Priv.
Void Credit Note Duty	A duty for voiding a Credit Note.	Void Credit Note Priv.
Approve Document Duty	A duty for approving documents.	Approve Document Priv.
Unmatch Duty	A duty for unmatching a merchandise invoice.	Unmatch Priv.
Upload Duty	A duty for uploading documents.	Unload Documents Priv.
Financial Posting Error Duty	A Duty for managing Financial Posting Errors. This duty is an extension of the Financial Posting Errors Inquiry Duty.	All privileges found in the Financial Posting Error Inquiry Duty. Maintain Financial Posting Error Priv.
Financial Posting Error Inquiry Duty	A duty for viewing Financial Posting Errors.	View Financial Posting Error Priv. Search Financial Posting Error Priv.
Tolerance Maintenance Duty	A Duty for managing Tolerance settings. This duty is an extension of the Tolerance Inquiry Duty.	- All privileges found in the Tolerance Inquiry Duty. -Maintain Tolerance Priv. -Delete Tolerance Priv. -Maintain Tolerance Mapping Priv. -Delete Tolerance Mapping Priv.
Tolerance Inquiry Duty	A duty for viewing Tolerance settings.	-View Tolerance Priv. -View Tolerance Mapping Priv. -Search Tolerance Priv. -Search Tolerance Mapping Priv.
Match Strategy Maintenance Duty	A Duty for managing Match Strategy settings. This duty is an extension of the Match Strategy Inquiry Duty	-All privileges found in the Match Strategy Inquiry Duty. -Maintain Match Strategy Priv. -Delete Match Strategy Priv. -Maintain Match Strategy Mapping Priv. -Delete Match Strategy Mapping Priv.
G/L Cross Reference Maintenance Duty	A Duty for managing G/L Cross Reference settings. This duty is an extension of the G/L Cross Reference Inquiry Duty	-All privileges found in the G/L Cross Reference Inquiry Duty. --Maintain G/L Cross Reference Priv. -Delete G/L Cross Reference Priv.

Table 16–2 (Cont.) Duties

Duty	Description	List of Privileges
G/L Cross Reference Inquiry Duty	A duty for viewing G/L Cross Reference settings	-View G/L Cross Reference Priv. --Search G/L Cross Reference Priv
Reason Code Maintenance Duty	A Duty for managing Reason Code settings. This duty is an extension of the Reason Code Inquiry Duty	-All privileges found in the Reason Code Inquiry Duty. -Maintain Reason Code Priv. -Delete Reason Code Priv.
Reason Code Inquiry Duty	A duty for viewing Reason Code settings	-View Reason Code Priv. -Search Reason Code Priv.
G/L Options Maintenance Duty	A Duty for managing G/L Options settings. This duty is an extension of the G/L Options Inquiry Duty	-All privileges found in the G/L Options Inquiry Duty. -Maintain G/L Options Priv. -Delete G/L Options Priv.
G/L Options Inquiry Duty	A duty for viewing G/L Options settings	-View G/L Options Priv. -Search G/L Options Priv.
System Options Maintenance Duty	A Duty for managing System Options settings. This duty is an extension of the System Options Inquiry Duty	-All privileges found in the System Options Inquiry Duty. -Maintain System Options Priv. -Delete System Options Priv.
System Options Inquiry Duty	A duty for viewing System Options settings	View System Options Priv.
Supplier Options Maintenance Duty	A Duty for managing Supplier Options settings. This duty is an extension of the Supplier Options Inquiry Duty	-All privileges found in the Supplier Options Inquiry Duty. -Maintain Supplier Options Priv. -Delete Supplier Options Priv.
Supplier Options Inquiry Duty	A duty for viewing Supplier Options settings	-View Supplier Options Priv. -Search Supplier Options Priv.
Location Dynamic Mapping Maintenance Duty	A Duty for managing Location Dynamic Mapping settings. This duty is an extension of the Location Dynamic Mapping Inquiry Duty	-All privileges found in the Location Dynamic Mapping Inquiry Duty. -Maintain Location Dynamic Mapping Priv. -Delete Location Dynamic Mapping Priv.
Location Dynamic Mapping Inquiry Duty	A duty for viewing Location Dynamic Mapping settings	-View Location Dynamic Mapping Priv. -Search Location Dynamic Mapping Priv.
Dept Class Dynamic Mapping Maintenance Duty	A Duty for managing Dept Class Dynamic Mapping settings. This duty is an extension of the Dept Class Dynamic Mapping Inquiry Duty	-All privileges found in the Dept Class Dynamic Mapping Inquiry Duty. -Maintain Dept Class Dynamic Mapping Priv. -Delete Dept Class Dynamic Mapping Priv.

Table 16–2   (Cont.) Duties

Duty	Description	List of Privileges
Dept Class Dynamic Mapping Inquiry Duty	A duty for viewing Dept Class Dynamic Mapping settings	-View Dept Class Dynamic Mapping Priv. -Search Dept Class Dynamic Mapping Priv.
Invoice Matching Duty	A duty for manually matching invoices	-Manually Match Priv. -Search Manual Match Priv
Resolve Cost Discrepancies Duty	A duty for resolving cost discrepancies	-Cost Discrepancy Priv -Search Discrepancy List Priv.
Resolve Quantity Discrepancies Duty	A duty for resolving quantity discrepancies	-Quantity Discrepancy Priv. -Search Discrepancy List Priv.
Resolve Discrepancies Duty	A duty for resolving either cost or quantity discrepancies	-Cost Discrepancy Priv. -Quantity Discrepancy Priv. -Search Discrepancy List Priv.
Credit Note Matching Duty	A duty for matching Credit Notes	-Credit Note Match Priv. -Search Credit Note Match Priv.
Resolve Tax Discrepancy Duty	A duty for resolving tax discrepancies	-Tax Discrepancy Resolution Priv. -Search Tax Discrepancy List Priv.
Dashboard Duty	A duty for viewing the dashboard	-Dashboard Priv.

Table 16–3 Function Security Mapping

Role	Duty	Privileges
Accounts Payable Specialist	Document Management Duty	-All privileges found in the Document Inquiry Duty.
	Pay Invoice Duty	-Maintain Documents Priv.
	EDI Maintenance Duty	-Delete Documents Priv.
	Reverse Debit Memo Duty	-Pay Invoice Manually Priv.
	Create Credit Note from CNR Duty	-EDI Maintenance Priv.
	Void Credit Note Duty	-Reverse Debit Memo Priv.
	Approve Document Duty	-Create Credit Note from CNR Priv.
	Tolerance Inquiry Duty	-Approve Document Priv.
	Match Strategy Inquiry Duty	-Void Credit Note Priv.
	G/L Cross Reference Inquiry Duty	-View Tolerance Priv.
	Reason Code Inquiry Duty	-View Tolerance Mapping Priv.
	G/L Options Inquiry Duty	-Search Tolerance Priv.
	System Options Inquiry Duty	-Search Tolerance Mapping Priv.
	Supplier Options Inquiry Duty	-View Match Strategy Priv.
	Location Dynamic Mapping Inquiry Duty	-View Match Strategy Mapping Priv.
	Dept Class Dynamic Mapping Inquiry Duty	-Search Match Strategy Priv.
	Invoice Matching Duty	-Search Match Strategy Mapping Priv.
	Credit Note Matching Duty	-View G/L Cross Reference Priv.
	Discrepancy Resolution Duty	-Search G/L Cross Reference Priv.
	Resolve Tax Discrepancy Duty	-View Reason Code Priv.
	Unmatch Duty	-Search Reason Code Priv.
	Upload Documents Duty	-View G/L Options Priv.
	Financial Posting Error Duty	-Search G/L Options Priv.
	Dashboard Duty	-View System Options Priv.
		-Search System Options Priv.
		-View Supplier Options Priv.
		-Search Supplier Options Priv.
		-View Location Dynamic Mapping Priv.
		-Search Location Dynamic Mapping Priv.
		-View Dept Class Dynamic Mapping Priv.
		-Search Dept Class Dynamic Mapping Priv.
		-Manually Matching Priv.
		-Cost Discrepancy Priv.
		-Quantity Discrepancy Priv.

Table 16–3   (Cont.) Function Security Mapping

Role	Duty	Privileges
		-Credit Note Matching Priv.
		-Unmatch Priv.
		-Upload documents Priv.
		-Financial Posting Error Priv.
		Dashboard Priv.

Table 16–3   (Cont.) Function Security Mapping

Role	Duty	Privileges
Finance Manager	Document Management Duty	-All privileges found in the Document Inquiry Duty.
	Pay Invoice Duty	-Maintain Documents Priv.
	EDI Maintenance Duty	-Delete Documents Priv.
	Reverse Debit Memo Duty	-Pay Invoice Manually Priv.
	Create Credit Note from CNR Duty	-EDI Maintenance Priv.
	Void Credit Note Duty	-Reverse Debit Memo Priv.
	Approve Document Duty	-Create Credit Note from CNR Priv.
	Tolerance Maintenance Duty	-Approve Document Priv.
	Match Strategy Maintenance Duty	-Void Credit Note Priv.
	G/L Cross Reference Maintenance Duty	-All privileges found in the Tolerance Inquiry Duty.
	Reason Code Maintenance Duty	-Maintain Tolerance Priv.
	G/L Options Maintenance Duty	-Delete Tolerance Priv.
	System Options Inquiry Duty	-Maintain Tolerance Mapping Priv.
	Supplier Options Maintenance Duty	-Delete Tolerance Mapping Priv.
	Location Dynamic Mapping Maintenance Duty	-All privileges found in the Match Strategy Inquiry Duty.
	Dept Class Dynamic Mapping Maintenance Duty	-Maintain Match Strategy Priv.
	Invoice Matching Duty	-Delete Match Strategy Priv.
	Credit Note Matching Duty	-All privileges found in the G/L Cross Reference Inquiry Duty.
	Discrepancy Resolution Duty	-Maintain G/L Cross Reference Priv.
	Resolve Tax Discrepancy Duty	-Delete G/L Cross Reference Priv.
	Unmatch Duty	-All privileges found in the Reason Code Inquiry Duty.
	Upload Documents Duty	-Maintain Reason Code Priv.
	Financial Posting Error Duty	-Delete Reason Code Priv.
	Dashboard Duty	-All privileges found in the G/L Options Inquiry Duty.
		-Maintain G/L Options Priv.
		-Delete G/L Options Priv.
		--All privileges found in the System Options Inquiry Duty.
		-All privileges found in the Supplier Options Inquiry Duty.
		-Maintain Supplier Options Priv.
		-Delete Supplier Options Priv.

Table 16–3   (Cont.) Function Security Mapping

Role	Duty	Privileges
		-All privileges found in the Location Dynamic Mapping Inquiry Duty.
		-Maintain Location Dynamic Mapping Priv.
		-Delete Location Dynamic Mapping Priv.
		-All privileges found in the Dept Class Dynamic Mapping Inquiry Duty.
		-Maintain Dept Class Dynamic Mapping Priv.
		-Delete Dept Class Dynamic Mapping Priv.
		-Manually Match Priv.
		-Search Manual Match Priv.
		-Credit Note Match Priv.
		-Search Credit Note Match Priv.
		-Cost Discrepancy Priv.
		-Quantity Discrepancy Priv.
		-Search Discrepancy List Priv.
		-Tax Discrepancy Resolution Priv.
		-Search Tax Discrepancy List Priv.
		-Unmatch Priv.
		-Upload documents Priv.
		-All privileges found In the Financial Posting Error Inquiry Duty.
		-Financial Posting Error Priv.
		-Dashboard Priv.
Buyer	Resolve Cost Discrepancies Duty	-Cost Discrepancy Priv.
		-Search Discrepancy List Priv.
Corporate Inventory Control Analyst	Resolve Quantity Discrepancies Duty	-Quantity Discrepancy Priv.
		-Search Discrepancy List Priv.
ReIM Application Administrator	All duties	-All privileges.

Table 16–3   (Cont.) Function Security Mapping

Role	Duty	Privileges
Financial Analyst	Document Inquiry Duty	-All privileges in
	Pay Invoice Duty	-Document Inquiry Duty.
	Tolerance Inquiry Duty	-All privileges in
	Match Strategy Inquiry Duty	-Tolerance Inquiry Duty.
	G/L Cross Reference Inquiry Duty	-All privileges found in the Match Strategy Inquiry Duty.
	Reason Code Inquiry Duty	
	G/L Options Inquiry Duty	-All privileges found in the G/L Cross Reference Inquiry Duty.
	System Options Inquiry Duty	
	Supplier Options Inquiry Duty	-All privileges found in the Reason Code Inquiry Duty.
	Location Dynamic Mapping Inquiry Duty	-All privileges found in the G/L Options Inquiry Duty.
	Dept Class Dynamic Mapping Inquiry Duty	-All privileges found in the System Options Inquiry Duty.
	Financial Posting Error Inquiry Duty	-All privileges found in the Supplier Options Inquiry Duty.
		-All privileges found in the Location Dynamic Mapping Inquiry Duty.
		-All privileges found in the Dept Class Dynamic Mapping Inquiry Duty.
		-All privileges found In the Financial Posting Error Inquiry Duty.

Table 16–3   (Cont.) Function Security Mapping

Role	Duty	Privileges
Accounts Payable Manager	Document Management Duty	-All privileges found in the Document Inquiry Duty.
	Pay Invoice Duty	-Maintain Documents Priv.
	EDI Maintenance Duty	-Delete Documents Priv.
	Reverse Debit Memo Duty	-Pay Invoice Manually Priv.
	Create Credit Note from CNR Duty	-EDI Maintenance Priv.
	Approve Document Duty	-Reverse Debit Memo Priv.
	Void Credit Note Duty	-Create Credit Note from CNR Priv.
	Tolerance Maintenance Duty	-Approve Document Priv.
	Match Strategy Maintenance Duty	-Void Credit Note Priv.
	G/L Cross Reference Maintenance Duty	-All privileges found in the Tolerance Inquiry Duty.
	Reason Code Maintenance Duty	-Maintain Tolerance Priv.
	G/L Options Maintenance Duty	-Delete Tolerance Priv.
	System Options Inquiry Duty	-Maintain Tolerance Mapping Priv.
	Supplier Options Maintenance Duty	-Delete Tolerance Mapping Priv.
	Location Dynamic Mapping Maintenance Duty	-All privileges found in the Match Strategy Inquiry Duty.
	Dept Class Dynamic Mapping Maintenance Duty	-Maintain Match Strategy Priv.
	Invoice Matching Duty	-Delete Match Strategy Priv.
	Credit Note Matching Duty	-Maintain Match Strategy Mapping Priv.
	Discrepancy Resolution Duty	-Delete Match Strategy Mapping Priv.
	Resolve Tax Discrepancy Duty	-All privileges found in the G/L Cross Reference Inquiry Duty.
	Unmatch Duty	-Maintain G/L Cross Reference Priv.
	Upload Documents Duty	-Delete G/L Cross Reference Priv.
	Financial Posting Error Duty	-All privileges found in the Reason Code Inquiry Duty.
		-Maintain Reason Code Priv
		-Delete Reason Code Priv
		-All privileges found in the G/L Options Inquiry Duty.
		-Maintain G/L Options Priv
		-Delete G/L Options Priv
		-All privileges found in the System Options Inquiry Duty.
		-All privileges found in the Supplier Options Inquiry Duty.

Table 16–3   (Cont.) Function Security Mapping

Role	Duty	Privileges
		-Maintain Supplier Options Priv.
		-Delete Supplier Options Priv.
		-All privileges found in the Location Dynamic Mapping Inquiry Duty.
		-Maintain Location Dynamic Mapping Priv.
		-Delete Location Dynamic Mapping Priv.
		-All privileges found in the Dept Class Dynamic Mapping Inquiry Duty.
		-Maintain Dept Class Dynamic Mapping Priv.
		-Delete Dept Class Dynamic Mapping Priv.
		-Manually Match Priv.
		-Search Manual Match Priv.
		-Credit Note Match Priv.
		-Search Credit Note Match Priv.
		-Cost Discrepancy Priv.
		-Quantity Discrepancy Priv.
		-Search Discrepancy List Priv.
		-Tax Discrepancy Resolution Priv.
		-Search Tax Discrepancy List Priv.
		-Unmatch Priv.
		-Upload documents Priv.
		-All privileges found In the Financial Posting Error Inquiry Duty.
		-Financial Posting Error Priv.

Table 16–3   (Cont.) Function Security Mapping

Role	Duty	Privileges
Data Steward	Document Management Inquiry Duty	-All privileges found in the Document Inquiry Duty.
	EDI Maintenance Duty	-EDI Maintenance Priv.
	Tolerance Maintenance Duty	-All privileges found in the Tolerance Inquiry Duty.
	Match Strategy Maintenance Duty	-Maintain Tolerance Priv.
	G/L Cross Reference Maintenance Duty	-Delete Tolerance Priv.
	Reason Code Maintenance Duty	-Maintain Tolerance Mapping Priv.
	G/L Options Maintenance Duty	-Delete Tolerance Mapping Priv.
	System Options Maintenance Duty	
	Supplier Options Maintenance Duty	-All privileges found in the Match Strategy Inquiry Duty.
	Location Dynamic Mapping Maintenance Duty	-Maintain Match Strategy Priv.
	Dept Class Dynamic Mapping Maintenance Duty	-Delete Match Strategy Priv.
	Upload Documents Duty	-Maintain Match Strategy Mapping Priv.
	Financial Posting Error Duty	-Delete Match Strategy Mapping Priv.
		-All privileges found in the G/L Cross Reference Inquiry Duty.
		-Maintain G/L Cross Reference Priv.
		-Delete G/L Cross Reference Priv.
		-All privileges found in the Reason Code Inquiry Duty.
		-Maintain Reason Code Priv.
		-Delete Reason Code Priv.
		-All privileges found in the G/L Options Inquiry Duty.
		-Maintain G/L Options Priv
		-Delete G/L Options Priv
		-All privileges found in the System Options Inquiry Duty.
		-Maintain System Options Priv
		-All privileges found in the Supplier Options Inquiry Duty.
		-Maintain Supplier Options Priv.
		-Delete Supplier Options Priv.
		-All privileges found in the Location Dynamic Mapping Inquiry Duty.
		-Maintain Location Dynamic Mapping Priv.

Table 16–3   (Cont.) Function Security Mapping

Role	Duty	Privileges
		-Delete Location Dynamic Mapping Priv.
		-All privileges found in the Dept Class Dynamic Mapping Inquiry Duty.
		-Maintain Dept Class Dynamic Mapping Priv.
		-Delete Dept Class Dynamic Mapping Priv.
		-Upload documents Priv.
		-All privileges found In the Financial Posting Error Inquiry Duty.
		-Financial Posting Error Priv.

It is recommended that you implement LDAP policies to prevent reusing user names. This will prevent users from inheriting user role privileges. If other non-LDAP authentication provider is used then similar available mechanism should be deployed.

ReIM uses location criteria to limit the data set available for processing. Only the documents that are associated with the locations accessible to the user security group can be accessed by the user. ReIM uses RMS mechanism to associate location with the user group. See the RMS documentation for details on setting up location level security. It is important to note that if no locations have been defined for the user's group the use will have access to ALL location. At the same time if some locations have been assigned to the user's group then the user will have access just to those defined locations. Location security is used across the application, so all the workflows will adhere to the location restrictions, including batches. Because of this the batch user(s) should have access to ALL locations.

In addition to location security ReIM uses similar mechanism to restrict access to the reason codes and accordingly the resolution actions that the user can take. The access is defined manually via IM_SEC_GRP_REASON_CODE table. The table maintains mapping of the reason codes to the RMS security group. One difference of the reason code security from location security is that if no reason codes have been assigned to the user security group then no reason codes will be available for the user (no access by default). Reason code access needs to be explicitly granted to the user's security group.

Other Common Application Administration

As a part of the operational workflow, ReIM needs to have credential information to authenticate application users and to authenticate application itself with other dependent components such as Web Services. For the case of remote users connecting to ReIM servers through browsers, credentials are retrieved in real time through an online form. For all other cases the credentials are determined at installation and are stored in Secure Wallet by means of Credential Store Manager Component. At runtime the credentials are retrieved from the wallet and supplied to the component for authentication. The credentials can be updated if required. As part of installation ReIM provides convenience scripts that allow credential entries to be updated. The scripts allow the system administrator to see usernames stored in ReIM wallet partition and

to change the password if necessary. The script does not display original passwords. For more information, see the *Operations Guide*.

There are two sets of logs that are used by the ReIM application: Application and Batch client Execution Logs. The application logs are configured and maintained by Oracle Fusion Middleware Logging. Application log messages will be written to the server's diagnostic logs within the WebLogic directory structure. Such logs are owned by the OS users that own the WebLogic container. The logging level and other logging parameters can be adjusted through the Oracle Diagnostic Logging configuration as provided by Oracle Fusion Middleware. The batch client logs are not managed by Oracle Fusion Middleware and the logging level and other configurations are controlled through the Log4J properties within the batch client distribution. The default log path is the same directory as the batch client distribution. It is recommended that only administrative users are granted access to these log files, preferably the same OS users that would run the batch.

The ReIM application does not restrict concurrent sessions from the same user. It means that multiple users can log in to ReIM server with the same credentials. There will be more than one session from application standpoint, but there will be the same user from auditing standpoint of view. It is recommended not to use the same credentials for different sessions.

The session is maintained per browser instance. So if more than a single browser is used then the server will consider such scenario as multiple user logins. At the same time multiple tabs of the same browser would share the session.

Session timeout is defined at the application server level. It is 60 minutes by default, but can be changed through WebLogic configuration.

17

Extending/Customization

Customization and extending capabilities is an important part of any application. This chapter discusses how to securely implement customizations and extensions such that they do not jeopardize application security.

If customization is required it should be done in such a way that no built-in explicit security features would be circumvented. For example, many VO queries in ReIM use RMS data security views. These queries should not be modified to expose data by removing the usage of the view. It is recommended to perform secure code analysis after code customization to identify potential secure coding standard violations.

If additional integration credentials are required, the customization should store them in the Secure Credential Store along with all other ReIM credentials. Credential population should be done by the script provided with the application.

18

Securing the Database

The database should be secured using the recommendations from the *Oracle Database 12 C Release 1 Security Guide*.

The following sections provide additional application specific guidance for securing the database for use with Oracle Retail Invoice Matching application.

Application Schema Owners

As ReIM shares the schema owner with RMS, you need to follow the RMS security guidelines regarding schema owner permissions.

ReIM should not use schema owner for database communication. Instead a schema synonym should be used. The schema used for database interaction is stored in more than one place within the application (actually it is store in 2 configuration files and on the WebLogic Data Source). When you need to update the schema being used, make sure that all places have been updated.

Database Security Considerations

The following recommendations should be considered for the database:

- The database server should be on 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 through trusted network hosts.

- The database server should have minimal use of ports and any communications should be under secure protocols.

- The database should be on its own dedicated server (or a cluster of servers).

- The database server should be behind a firewall.

- Any database user should be audited.

- Only minimal rights should be granted to the owner of database processes and files such that only that 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.

Restricted Access to Purge Batches

ReIM uses a batch infrastructure for purging data. The purging processes should be scheduled and executing any individual data purging process outside of this schedule

should be avoided. Some of the purging is performed via truncating tables and as such no rollback is possible.

If some additional purging is required on a regular basis that is outside of the purging functionality provided by ReIM, it will need to be executed by a standard set of scripts that should have security built into it. In addition, any custom purging scripts should be executed under a separate schema.

19

Data Security

The following sections provide application specific guidance for securing data for use with the Oracle Retail Invoice Matching application.

Location Security

Quite often application users need to have access to a subset of locations within the Location Hierarchy. Retailers can assign a sub-tree of a location hierarchy to the application user group. Application users will have access only to the data (documents, discrepancies, etc.) associated with the locations that are assigned to the user's group. Data security is defined with the principle that the user just cannot act upon inaccessible data, but also cannot see that inaccessible data.

For example, if the application user User1 belongs to the group Group1 and the group has Store1, Store2, and Warehouse1 assigned to it, then the application user can see and act upon the documents related to those locations only. Document1 for Store1 can be found. Document2 for Store3 cannot even be found. Store3 also will not be listed anywhere in the location lists, LOVs, etc. when viewed by user User1. Another application user User2 that has access to the Store3 will be able to access and act on that document.

To assign the set of locations to the application user group, retailers would need to use standard Merchandising System mechanisms for data security.

Assignment of stores can be done at:

- Chain
- Area
- Region
- District
- Organizational Unit

To define store level security, the FILTER_GROUP_ORG table needs to be populated with a record associating the user's security group ID (from SEC_USER_GROUP) with the FILTER_ORG_LEVEL representing the location hierarchy level and FILTER_ORG_ID representing ID at that level. For example, to allow the user from the secure group 1 access to the stores in the district 123, a record would be created in FILTER_GROUP_ORG with '1', 'D', '123'.

Assignment of warehouses can be done at:

- Warehouse
- Organizational Unit

To define warehouse level security, FILTER_GROUP_ORG table needs to be populated with a record associating the user's security group ID (from SEC_USER_GROUP) with the FILTER_ORG_LEVEL representing the location hierarchy level and FILTER_ORG_ ID representing ID at that level. For example, to allow the user from the secure group 1 access to the warehouse 123, a record would be created in FILTER_GROUP_ORG with '1', 'W', '123'.

Reason Code Security

Reason code data security is provided via the Reason Code Maintenance screen by assigning a security group id to the reason code. This assignment is stored in the IM_ SEC_GRP_REASON_CODE table.

Part V

Oracle Retail Price Management (RPM)

The following chapters provide guidance for administrators, developers, and system integrators who securely administer, customize, and integrate the Oracle Retail Price Management (RPM) application.

Part V contains the following chapters:

- General Security Considerations
- Understanding Security
- Post Installation - Application Administration
- Extending/Customization
- Securing the Database

20

General Security Considerations

This chapter discusses how to securely install the Oracle Retail Price Management (RPM) application. To obtain a secure configuration, follow the instructions and advice provided below.

The RPM application is installed on the server; however it is used in the distributed environment. Both client and server security must be taken into consideration when hardening application deployment. You need to reference your desktop and server operation system security guides, if available for more information on reinforcing security for the execution environment.

In particular, only valid users should have access to the client workstations running clients for the application. Since the RPM user interface has no inactivity timeouts, a reasonable locking policy should be established to lock out computer screens after some time of inactivity. Security policy should be established at the desktop level to monitor unsuccessful login attempts. System administrator should guarantee that the operation system has the latest mandatory update patches.

As RPM client executes in the Java sandbox, it is important to keep Java runtime up-to-date with the latest security patches. Java runtime can be provided by either a browser plug-in or by standalone JVM such as the one shipped with JDK. You need to make sure that runtime configuration for appropriate Java version is correct. See Figure 20–1 for example on how Java runtime environment settings window looks like.

Figure 20–1   Java Runtime Environment Settings Window
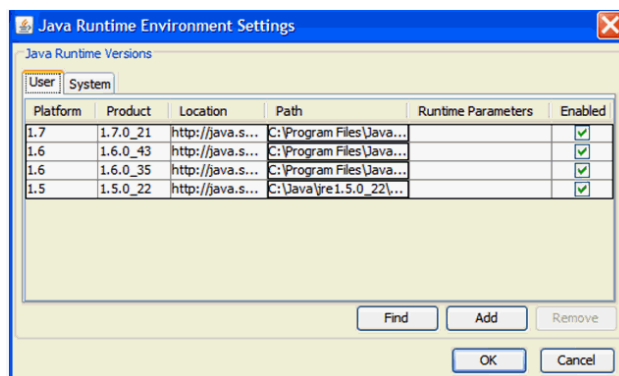
Ensure the following:

■   The product identifier matches actual version of the runtime pointed by path

■   Disable runtimes that are not up-to-date are not required

- The configuration is correct at both system and user level (for each user on the workstation)

- The network configuration is correct and connection will go either directly or through authorized proxy

- Verify that the runtime configuration has enough temporary space allocation to download and keep RPM client (see RPM distribution for the latest client size)

- The correct certificates are installed on client's workstations. As RPM installation requires signing of distributed ears and jar files and self-generated keys are not allowed anymore, make sure that retailer certificate is used for signing and that the certificate is installed correctly

- Double-check that Java runtime is configured to allow JNLP file invocation - the best setting would be to prompt user

System administrator should restrict users from modifying security setting for Java runtime. At the same time the user should be allowed to accept JNLP security requests. Only signed trusted code should be downloaded and run. The system should check that the certificate matches hostname of the server. The retailer should be registered as a trusted publisher with the workstation. SSL should be enabled on the client.

For more information of how secure the internal network used to access RPM server(s), see *Network Security Configuration Guide.* This should include both physical and logical security of the network. Only SSL enabled communication should be used.

Only the desktops on the intranet should be allowed accessing the application server. The best approach is to limit the set of client computers on the network that can access the application server. That can be done at the network level to prevent guest users on the local network from even seeing the application server.

Only system administrators should have access to the application server(s). Business users (even power users) should not have accounts on the application server computers. If such accounts do exist, the OS account privileges should prevent business user from accessing application server files/directories associated with RPM application.

The users running batches should not be system administrators. The best approach is to have a single dedicated user for running batches, rather than having multiple users running batches ad hoc. At the same time RPM application does not prevent any valid application user from running batches. The main difference between batch user and regular users is that batch user credentials exist in the Secure Wallet. Installer is the one responsible for placing batch user credentials into the wallet, so by default there will be only a single batch user. At the same time nothing is preventing the system admin from adding additional valid RPM users into Secure Wallet (by running provided scripts).

RPM both consumes and produces data files. File consumption is done on the client side where a user can select a file on the file system containing a Price Event Item List. Only CSV and Excel file types are allowed. It is recommended that the file transfer to the client workstation is done through secure FTP (in case the file is not generated on the same workstation). File generation is done on the server. It is recommended to keep the file being uploaded for audit purposes. It is up to the retailer to provide the process for that. The files can be kept in an audit directory or using any other appropriate document management system that would allow easy retrieval later on. Generated price event files are transmitted through secure FTP.

21

Understanding Security

This chapter provides an overview of all the security features available in the RPM application. It is provided as a reference for how the application securely communicates with other applications; how the application authenticates, authorizes, and audits users; and the encryption and hashing mechanisms used by the application.

The following topics are covered in this chapter:

- Security Features Overview
- Dependent Applications
- Discussion of Dependencies on Underlying Platform
- Technical Overview of the Security Features
- Security Features of the Application
- Encryption and Hashing

Security Features Overview

Figure 21–1 shows the physical deployment of RPM.

Figure 21–1   RPM Physical Deployment
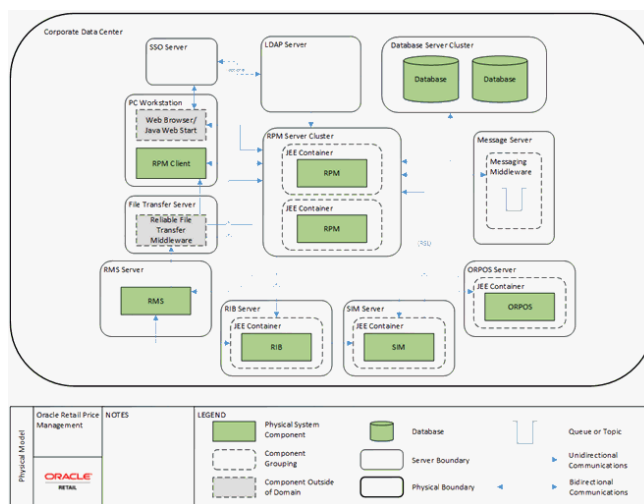
The Application server is deployed on the corporate intranet on WebLogic cluster. The Application server is connected to a cluster of Oracle databases and a corporate LDAP

server. Optionally Single Sign-On infrastructure can be deployed. In addition secure FTP server is responsible for transferring files in/out of the application on the server and on the client (if required). Optionally 3rd party batch running infrastructure can be deployed to run batch scripts (for example, Appworx, and so on). The client workstation should be at the corporate data center. The client workstations need to run supported Java runtime.

WebLogic Application server executes server side of the application logic. Oracle Database provides data handling functionality. An LDAP server provides user attributes handling. Single Sign-On infrastructure provides capability to share authentication tokens across multiple retail applications. An FTP server provides delivery for incoming/outgoing files. Workstation Java runtime executes client side application logic.

RPM is exchanging data with other retail applications that are part of the Oracle Retail Suite, such as RMS, SIM, and POS.

Each component of the deployment should be secured to provide minimum required access. This includes OS security, network security, browser security, LDAP security, WebLogic security, database Security and FTP server security. For information on how to secure each component, see the reference documentation.

Dependent Applications

Security Guides for dependent applications are found at the following Web sites:

- Oracle Database 12 C Release 1:

  http://docs.oracle.com/database/121/TDPSG/E17609-19.pdf

- Oracle WebLogic 12.2.1:

  https://docs.oracle.com/middleware/1221/wls/wls-secure.htm

Contact your vendor for other components of security guides.

Discussion of Dependencies on Underlying Platform

RPM relies on Java runtime on the client workstations to provide client side code execution.

RPM replies on WebLogic to provide authorization for accessing application services. Only authenticated authorized users should be allowed to access Enterprise JavaBeans (EJBs) and data sources installed as part of RPM installation on WebLogic servers. For more information, see the Authorization section.

Technical Overview of the Security Features

The following section describes the authentication, authorization, audit, and user management.

Security Features of the Application

The relevant security features fall into one or more of the following categories. For information on these categories, see the following sections:

- Authentication
- Authorization
- Audit

- User Management

Authentication

Only authentication users should have access to RPM application. By the point of application authentication the user potentially successfully authenticates with the network and/or the workstation OS.

RPM supports the following two types of authentication:

- Dedicated

- Single Sign-On

Dedicated authentication - User credentials (username and password) are verified by WebLogic Authenticator. For information on registering an Authenticator with WebLogic, see the *Oracle Retail Price Management Installation Guide*. LDAP authenticator should be used where actual authentication data is provided by LDAP.

> **Note:** Even though LDAP provides the data, the actual verification of provided credentials is done by WebLogic.

If the WebLogic has been successfully verified the user credentials then the user has passed the first step of authentication. For the authentication to complete successfully the user should also have all the mandatory attributes defined within LDAP entity. If some mandatory attributes are missing then the authentication process will fail.

All LDAP attribute mappings are defined in the security.properties file. The following attributes (besides user identifier attribute) have to be defined for a user to be able to successfully authenticate with RPM:

- ldap.firstname.attrname

- ldap.lastname.attrname

The attributes listed are not actual attribute name, but rather logical name and should be mapped to actual attribute name within security.properties configuration file.

Dedicated authentication credentials are either provided by the application online user in real time (entering the user name and password on the RPM provided login page) or are retrieved by the application server from the Secure Wallet in the case of batch process. The batch user still needs to provide credentials alias, so that appropriate username and passwords are retrieved from the Secure Wallet.

Single Sign-On authentication - In case of Single Sign-On authentication happens only once per application suite. Authentication is performed by Single Sign-On infrastructure (potentially backed by the same LDAP server as the case for dedicated authentication). In this case login page is provided by the Single Sign-On infrastructure. The second step of authentication is exactly the same as in dedicated authentication - mandatory user attributes should be present in LDAP server.

In both cases of authentication, the authentication is performed when it is determined that the session is not authenticated or the session has been invalidated (in case of dedicated authentication).

Authorization

RPM supports the following two types of authorization:

- Enterprise

■   Business

Enterprise authorization - This is performed by application server logic. WebLogic will make sure (if configured correctly - see the *Oracle Retail Price Management Installation Guide* for more information on required WebLogic configuration) that already authenticated user is the member of RPM user role/group (Role is created LDAP). Only the users who are members of RPM groups are allowed to get access to RPM functionality. All EJBs and data sources are accessible to RPM Secure User.

When the user submits a request to the server, the request (after authentication) is handled by a Controller EJB. This controller EJB will determine appropriate EJB to perform the action. When controller EJB will issue another request to Worker EJB, this request will be performed under RPM Secure User principal. Same discussion applies to accessing Data sources.

Business authorization - This is performed by Oracle Retail Security Management (RSM) logic. RSM is a part of RPM distribution. RMS will define what action each user role can perform and in what mode those action can be performed (allowed modes are Edit, View, None, Emergency). In addition to action security RSM provides ability to define data security. Data security allows system to associate appropriate level of location and merchandising hierarchy with a user role. Note that RSM operates on the user role level and not on the user level.

Audit

RPM does not provide extensive audit capabilities. Only price event tables carry the user information. The user information is relevant only as the creation identifier and does not guarantee that the final price event was completed by the same user who created the price event. Hence if auditing is required, it should be done at the database level. For information on how to turn on the database auditing, see the Oracle database documentation. The database auditing will be not be able to differentiate application users modifying data, as it is done at the database user level and all RPM application users share the same database user.

User Management

RPM does not store or maintain users. Instead RPM relies on LDAP to provide user management functionality on its behalf.

To create a new user to be used within RPM application, a new user should be created in LDAP; the user should be assigned to LDAP RPM role. Through backend the newly created user should be associated with a user role. If a new user role is required, it should be created through RSM screen first. It is recommended to create user roles with the minimum set of user privileges required for the user.

In order to remove the user from RPM, you need to first remove the user from the user group within RSM, then remove the user from a group in LDAP, and finally delete the user from LDAP.

Encryption and Hashing

This section covers securing the applications using encryption and hashing.

RPM uses encryptions as part of a security key generated on the server to deliver a client to the user workstation. To access RMS the user issues a requests to the server for Java Network Launch Protocol (JNLP) file. The server will generate temporary token based on the encryption method configured in the security.properties file.

user.signature.cipher.algorithm

By default HmacSHA1 is used, but the algorithm can be changed if required.

22

Post Installation - Application Administration

This chapter provides information about application administrative tasks related to security. How to manage users and roles as well as some other common application administrative tasks such as secure credential management and logging are discussed.

This chapter discusses post installing the application administration.

The following topics are covered in this chapter:

- Roles and Permission Grants
- Other Common Application Administration

Roles and Permission Grants

RPM uses the following two kinds of user roles:

- Enterprise
- Business

There should be only a single enterprise user role created and it is defaulted to rpm_secure_users. This role is created in LDAP by the system administrator. Any LDAP user that should be considered for RPM processing should be made a member of this role. RPM makes an assumption that LDAP implementation will have groups that keep track of its member and the users will not be aware about their group membership. It implies that there will be a reference maintained by the user group to the user group member by means of a static member DN attribute. For example if this attribute is **uniqueMember**, then **uniqueMember** attribute will point to the group member. The user, on the other hand does not have any attributes pointing to the rpm_secure_users group. RPM does not provide any LDIF scripts to create the rpm_secure_users role.

If the data seeding script has been run, then the script would create a single business user role - Administrator Role. If the script has not been run, then no user roles exist by default and the retailer is responsible for creating the groups manually by inserting data into appropriate table (demo data script can be used as a starting point). The role Administrator Role, as the name suggests, has the highest level of privileges. The name of the group is completely arbitrary. Retailers can create as many additional roles as they require. The best approach when creating a user role is to define it based on the set of task the role members are supposed to perform and assign only the minimum required set of privileges to that group. For example, an employee can be part of a group which only allows the submission of price events and does not allow direct approval. This allows users with approval privileges the chance to review submitted price events and decide whether or not to approve them.

Despite it being the only role created by the data seed script, try to avoid assigning all users to Administrator Role. This will grant all users more privileges than is likely required. Create user roles that best fit the user's requirements and assign them only the privileges they require.

It is recommended to create the Administrator Role and an Admin user through a script and then to use Application logic (RSM Role Administration Screen) to maintain user roles.

The application logic allows the following actions:

1. Create/delete/update a user group

2. Assign/remove users to/from a role

3. Define a role's workflow permissions

4. Assign Location Hierarchy to the role

5. Assign Merchandise Hierarchy to the role

You cannot delete a user role from the UI, however it is possible to remove all the privileges from the role effectively eliminating it.

Other Common Application Administration

As a part of the operational workflow, RPM needs to have credential information to authenticate application users or to authenticate application itself with other dependent components such as database, LDAP or Oracle Retail Integration Bus (RIB). For the case of remote users connecting to RPM servers through RMI credentials are retrieved in real time through client provided form. For all other cases the credentials are determined at installation and are stored in Secure Wallet by means of Credential Store Manager Component. At runtime the credentials are retrieved from the wallet and supplied to the component for authentication. The credentials can be updated if required. As part of installation RPM provides convenience scripts that allow credential entries to be updated. The scripts allow the system administrator to see usernames stored in RPM wallet partition and to change the password if necessary. The script does not display original passwords. For more information, see the *Operations Guide*.

There are two set of logs that are generated by RPM application - infrastructure logs and actual Application logs. Infrastructure logs are configured and maintained by appropriate tools for infrastructure component. An example of infrastructure log would be WebLogic application server various logs. The logging level and other logging parameters can be adjusted through WebLogic component. Such logs are owned by the OS user that own WebLogic process. WebLogic log files are located within WebLogic directory structure. Application logs are generated by RPM application logic. RPM log configuration is done through RPM log configuration file (on the client and on the server). The administrator has the rights to configure the location of the RPM log files. RPM log files are also owned by the OS user that own WebLogic process (on the server) and OS user running client Java runtime (on the client workstation). It is recommended to grant access to log files only to the administrators.

RPM application does not restrict concurrent sessions from the same user. It means that more than a single user can log in to RPM server with the same credentials. There will be more than one session from application standpoint, but there will be the same user from database standpoint of view. It is recommended not to use the same credentials for different sessions.

Session timeout is defined at the application server level. It is 60 minutes by default, but can be changed through WebLogic configuration.

23

Extending/Customization

Customization and extending capabilities is an important part of any application. This chapter discusses how to securely implement customizations and extensions such that they do not jeopardize application security.

If customization is required it should be done in such a way that no built-in explicit security features would be circumvented. Customization should be done using provided customization toolkit.

It is recommended to perform secure code analysis after code customization to identify potential secure coding standard violations.

If additional integration is required and credentials are required then the customization should store those additional credentials in the Secure Wallet along with all other RPM credentials (in RPM partition). Credential population should be done by a script provided with RPM. If additional EJB are required, they should be protected by the same authorization as pre-existing EJBs. For more information, see the *Oracle Retail Price Management Installation* Guide.

24

Securing the Database

The database should be secured using the recommendations from the *Oracle Database 12 C Release 1 Security Guide*.

The following sections provide additional application specific guidance for securing the database for use with Oracle Retail Price Management application.

Application Schema Owners

As RPM shares schema owner with RMS, follow RMS security guidelines regarding schema owner permissions.

RPM should not use schema owner for database communication. Instead a schema synonym should be used.

Database Security Considerations

The following recommendations should be considered for the database:

- 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 through trusted network hosts.

- The database server should have minimal use of ports and any communications should be under secure protocols.

- The database should be on its own dedicated server.

- 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 that 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.

The purge script is usually put into an automation script, which runs once a day. As described above, this script is usually run by a user with limited access (only execute procedure and connect access).

Restricted Access to Purge Batches

RPM will use batch infrastructure for purging data. As such the user authentication is required. The purging processes should be scheduled and executing any individual data purging process outside of this schedule should be avoided.

If some additional purging is required on a regular basis that is outside of the purging functionality provided by RPM, do that through standard set of scripts that should have security built into it. Run the custom purging scripts under a separate schema.

Part VI

Oracle Retail Allocation

This Security Guide is for users and administrators of Oracle Retail Allocation. This includes merchandisers, buyers, business analysts, and administrative personnel.

Part VI contains the following chapter:

- Allocation Security Considerations

For more information on Allocation Security Considerations, see Chapter 8, "Functional Security for Applications Using Fusion Middleware".

25

Allocation Security Considerations

The chapter provides guidance for administrators to understand, configure, and customize functional security for the Oracle Retail Allocation application.

The following topics are covered in this chapter:

- Technical Overview of the Security Features
- Security Configuration
- JMS Security
- Security in Allocation Reports Launching RMS Screens

Technical Overview of the Security Features

The section describes the authentication, authorization, audit, and user management.

Security Features of the Application

The relevant security features fall into one or more of the following categories. For information on these categories, see the following sections:

- Authentication
- Authorization
- Audit
- User Management

Authentication

Only authenticated users should have access to Allocation. By the point of application authentication the user potentially successfully authenticates with the network and/or the workstation OS.

Allocation supports the following two types of authentication:

- Dedicated
- Single Sign-On

Dedicated Authentication: User credentials (username and password) are submitted by the Application Server to the LDAP server or any other configured authentication provider. If the authentication provider can successfully identify the user, then that user is considered authenticated with the Allocation application. Dedicated authentication credentials are either provided by the online application user in real time (entering user name and password on the Allocation provided login page) or are

retrieved by the client from the Secure Wallet in the case of batch process. The batch user still needs to provide credentials alias, so that the appropriate username and passwords is retrieved from the Secure Wallet.

Single Sign-On authentication: In case of Single Sign-On, authentication happens only once per application suite. Authentication is performed by Single Sign -On infrastructure (potentially backed by the same LDAP server as the case for dedicated authentication). In this case login page is provided by the Single Sign - On infrastructure.

In both cases of authentication, the authentication is performed when it is determined that the session is not authenticated or the session has been invalidated (in case of dedicated authentication).

Authorization

Only application users that belong to one of the Allocation user roles are authorized to use functionality provided by Allocation. If the user is a valid enterprise user, login may be successful but authorization may prevent access to specific workflows based on the user's assigned role. Authorization is performed for each user driven operation. It is assumed that the batch user is assigned to the administrator role which is authorized to perform all operations.

Audit

Auditing can be performed at the application level and at the infrastructure level. The operating system (OS) can be configured to audit user access and processes invoked. The network layer can be configured to audit entire communication data set. The application server can be configured to audit access to the application, including all URLs requested. The database can be configured to audit each table separately or entire sessions. Allocation also has some limited auditing capabilities.

The application will maintain some level of audit trail by keeping track of the last user modifying data and the date and time it was done.

- LAST_UPDATED_BY

- LAST_UPDATE_DATE

- CREATED_BY

- CREATED_DATE

Additional audit can be performed by decreasing logging level of the application. In this case additional information is reported into logs. The drawback is that performance can suffer and that amount of log entries to be recorded will increase. You can selectively decrease logging (see Log4J and Java Logging documentation on logging configuration for more information). Also make sure that the log files generated by the application are secure and are accessible to authorized OS users only.

User Management

Allocation does not store or maintains users. Instead, Allocation relies on external systems such as LDAP to provide user management functionality on its behalf.

To create a new user to be used within Allocation, you need to create a new user in the LDAP or whatever data store the configured authentication provider relies on. To access Allocation workflows, the user should be assigned to a valid Allocation user role.

Security Configuration

Access control of system resources is achieved by requiring users to authenticate at login and by restricting users to only those resources for which they are authorized. A default security configuration is available for immediate use after the Oracle Retail Fusion application is installed and is configured to use the Oracle Fusion Middleware security model. The default configuration includes three predefined security roles for application specific permission grants. Users can be added to predefined groups that are mapped to preconfigured application roles. Allocation is preconfigured to grant specific application permissions.

Table 25–1   Privileges

Name	Description
Search Allocations Priv	A privilege for searching for allocations.
Maintain Allocation Priv	A privilege for creating, maintaining, and editing an allocation.
Delete Allocation Priv	A privilege for deleting an allocation.
View Allocation Priv	A privilege for viewing an allocation.
Submit Allocation Priv	A privilege for submitting an allocation for approval.
Review Allocation Priv	A privilege for approving or reserving an allocation.
Batch Allocation Priv	A privilege for running batch jobs.
Search Allocation Location Groups Priv	A privilege for searching for allocations.
Maintain Allocation Location Group Priv	A privilege for creating and editing and an allocation location group.
Delete Allocation Location Group Priv	A privilege for deleting an allocation location group.
View Allocation Location Group Priv	A privilege for viewing an allocation location group.
Search Allocation Policy Templates Priv	A privilege for searching for allocations.
Maintain Allocation Policy Template Priv	A privilege for creating and editing a Policy Template.
Delete Allocation Policy Template Priv	A privilege for deleting a Policy Template.
View Allocation Policy Template Priv	A privilege for viewing a Policy Template.
Search Size Profile Priv	A privilege for searching Size Profiles.
Maintain Size Profile Priv	A privilege for creating and editing and a Size Profile.
Delete Size Profile Priv	A privilege for deleting a Size Profile.
View Size Profile Priv	A privilege for viewing a Size Profile.
Maintain System Options System Properties Priv	A privilege for editing the System Properties for System Options.
Maintain System Options User Group Properties Priv	A privilege for editing the user group properties for System Options.
View System Options Priv	A privilege for viewing System Options.
Search Auto Quantity Limits Priv	A privilege for searching for Auto Quantity Limits

Table 25–1   (Cont.) Privileges

Name	Description
Maintain Auto Quantity Limits Priv	A privilege for editing for Auto Quantity Limits.
View Auto Quantity Limits Priv	A privilege for Viewing for Auto Quantity Limits.
Maintain Allocation Dashboard Priv	A privilege for maintaining the Allocation Dashboard.
Maintain Allocation Buyer Dashboard Priv	A privilege for maintaining the Allocation Dashboard.

Table 25–2   Duties

Duty	Description	List of Privileges
Allocation Management Duty	A duty for managing allocations. This duty is an extension of the Allocation Inquiry Duty.	All privileges found in the Allocation Inquiry Duty. Maintain Allocation Priv, Delete Allocation Priv,
Allocation Inquiry Duty	A duty for viewing allocations.	View Allocation Priv, Search Allocations Priv,
Allocation Submit Duty	A duty for submitting allocation for approval.	Submit Allocation Priv,
Allocation Review Duty	A duty for approving or rejecting an allocation.	Review Allocation Priv,
Allocation Batch Duty	A duty for running batch process.	Batch Allocation Priv,
Allocation Location Groups Management Duty	A duty for managing allocation location groups. This duty is an extension of the Allocation Location Groups Inquiry Duty and Allocation Location Group Search Duty.	All privileges found in the Allocation Location Groups Inquiry Duty and the Allocation Location Groups Search Duty. Maintain Allocation Location Groups Priv, Delete Allocation Location Groups Priv,
Allocation Location Groups Inquiry Duty	A duty for viewing allocation location groups.	View Allocation Location Groups Priv, Search Allocation Location Groups Priv,
Allocation Policy Template Management Duty	A duty for managing allocation policy template. This duty is an extension of the Allocation Policy Template Inquiry Duty and Allocation Policy Template Search Duty.	All privileges found in the Allocation Policy Template Inquiry Duty and the Allocation Policy Template Search Priv, Maintain Allocation Policy Template Priv, Delete Allocation Policy Template Priv,
Delete Allocation Location Group Priv	A duty for viewing allocation Policy Template.	View Allocation Policy Template Priv, Search Allocation Policy Template Priv,
Size Profile Management Duty	A duty for managing size profile. This duty is an extension of the Size Profile Inquiry Duty.	All privileges found in the Size Profile Inquiry Duty. Maintain Size Profile Priv, Delete Size Profile Priv,
Size Profile Inquiry Duty	A duty for viewing allocation Policy Template.	View Size Profile Priv, Search Size Profiles Priv,

Table 25–2   (Cont.) Duties

Duty	Description	List of Privileges
System Options System Properties Management Duty	A duty for managing the system properties in system options. This duty is an extension of the System Options Inquiry Duty.	All privileges found in the System Options Inquiry Duty. Maintain System Options System Properties Priv,
System Options User Group Properties Management Duty	A duty for managing user group properties system options. This duty is an extension of the System Options Inquiry Duty.	All privileges found in the System Options Inquiry Duty. Maintain System Options User Group Properties Priv,
System Options Inquiry Duty	A duty for inquiring on profile. This duty is an extension of the Size Profile Inquiry Duty.	All privileges found in the System Options Inquiry Duty. Maintain System Options Priv,
Auto Quantity Limits Duty	A duty for managing Auto Quantity Limits. This duty is an extension of the Auto Quantity Limits Duty.	All privileges found in the Auto Quantity Limits Inquiry Duty. Maintain Auto Quantity Limits Priv.
Auto Quantity Limits Inquiry Duty	A duty for viewing Auto Quantity Limits.	View Auto Quantity Limits Priv. Search Auto Quantity Limits Priv.
Allocation Dashboard Duty	A duty for maintaining the Allocation Dashboard.	Maintain Allocation Dashboard Priv.
Allocation Buyer Dashboard Duty	A duty for maintaining the Allocation Buyer Dashboard.	Maintain Allocation Buyer Dashboard Priv.

Table 25–3   Function Security Mapping

Role	Duty	Privileges
Administrator	Allocation Management Duty, Allocation Submit Duty, Allocation Review Duty, Allocation Location Groups Management Duty, Allocation Policy Template Management Duty, Size Profile Management Duty, System Options System Properties Management Duty, System Options User Group Properties Management Duty, Allocation Batch Duty, Auto Quantity Limits Management Duty, Allocation Dashboard Duty	Search Allocations Priv, Maintain Allocation Priv, Delete Allocation Priv, Submit Allocation Priv, Review Allocation Priv, View Allocation Priv, Search Allocation Priv, View Allocation Location Groups Priv, Search Allocation Location Groups Priv, View Allocation Policy Template Priv, Search Allocation Policy Templates Priv, View Size Profile Priv, Search Size Profile Priv, View System Options Priv, Maintain System Options User Group Properties Priv, Batch Allocation Priv, Maintain Auto Quantity Limits Priv, View Auto Quantity Limits Priv, Search Auto Quantity Limits Priv, Maintain Allocation Dashboard Priv

Table 25–3   (Cont.) Function Security Mapping

Role	Duty	Privileges
Allocation Manager	Allocation Management Duty, Allocation Submit Duty, Allocation Review Duty, Allocation Location Groups Management Duty, Allocation Policy Template Management Duty, Size Profile Management Duty, System Options User Group Properties Management Duty, Auto Quantity Limits Management Duty, Allocation Dashboard Duty	Search Allocations Priv, Maintain Allocation Priv, Delete Allocation Priv, Submit Allocation Priv, Review Allocation Priv, View Allocation Priv, Search Allocation Priv, View Allocation Location Groups Priv, Search Allocation Location Groups Priv, View Allocation Policy Template Priv, Search Allocation Policy Templates Priv, View Size Profile Priv, Search Size Profile Priv, View System Options Priv, Maintain System Options User Group Properties Priv, Maintain Auto Quantity Limits Priv, View Auto Quantity Limits Priv, Search Auto Quantity Limits Priv, Maintain Allocation Dashboard Priv
Allocator	Allocation Management Duty, Allocation Submit Duty, Allocation Review Duty, Allocation Location Groups Inquiry Duty, Allocation Policy Template Inquiry Duty, Size Profile Management Duty, System Options Inquiry Duty Auto Quantity Limits Management Duty, Allocation Dashboard Duty.	Search Allocations Priv, Maintain Allocation Priv, Delete Allocation Priv, Submit Allocation Priv, Review Allocation Priv View Allocation Priv, Search Allocation Priv, View Allocation Location Groups Priv, Search Allocation Location Groups Priv, View Allocation Policy Template Priv, Search Allocation Policy Templates Priv, View Size Profile Priv, Search Size Profile Priv, View System Options Priv, Maintain Auto Quantity Limits Priv, View Auto Quantity Limits Priv, Search Auto Quantity Limits Priv, Maintain Allocation Dashboard Priv
Buyer	Allocation Inquiry Duty, Allocation Policy Template Inquiry Duty, Allocation Location Groups Inquiry Duty, Allocation Size Profile Inquiry Duty, Allocation Buyer Dashboard Duty.	View Allocation Priv, Search Allocation Priv, View Allocation Location Groups Priv, View Allocation Policy Template Priv, Search Size Profile Priv, View Size Profile Priv, Maintain Allocation Buyer Dashboard Priv

For more information about the Oracle Fusion Middleware security model and the authenticated role, see *Oracle Fusion Middleware Application Security Guide*.

JMS Security

Allocation utilizes a JMS Queue for long running processes. This queue can and should be secured. To do this, see Chapter 3, Asynchronous Task JMS Queue Security section.

> **Note:** When step 9 is reached in Securing the Asynchronous Task JMS Queue, you need to name the JMS Queue Role as AllocJMSQueueAccessRole for security to work.

Security in Allocation Reports Launching RMS Screens

Some Oracle Retail Allocation Reports include in-context launch of RMS screens functionality to display specific orders or shipments information. This feature allows users to gain access to data which may be restricted by RMS permissions. It is therefore necessary that users with access to this property also have the proper role in RMS to access these screens.

The Allocation reports that contain the attribute that allows direct launch into RMS screens are:

- PO Arrival Report
- Shipment Arrival Report