Oracle® Retail Insights Cloud Service

Security Guide

Release 23.2.301.0
F84674-01
July 2023

Oracle Retail Insights Cloud Service Security Guide, Release 23.2.301.0

F84674-01

Primary Author: Nathan Young

Contents

List of Figures

List of Tables

Send Us Your Comments

Oracle Retail Insights Security Guide, Release 23.2.301.0

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

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

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

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

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

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

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

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

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

Preface

This document serves as a guide for administrators, developers, and system integrators who securely administer, customize, and integrate Oracle Retail Insights Cloud Service application.

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 above mentioned product, 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.

We assume 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.

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/technetwork/documentation/oracle-retail-100266.html

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

Conventions

The following text conventions are used in this document:

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

1

Overview of Security Features

This chapter provides an overview of the security features included with Oracle Retail Insights.

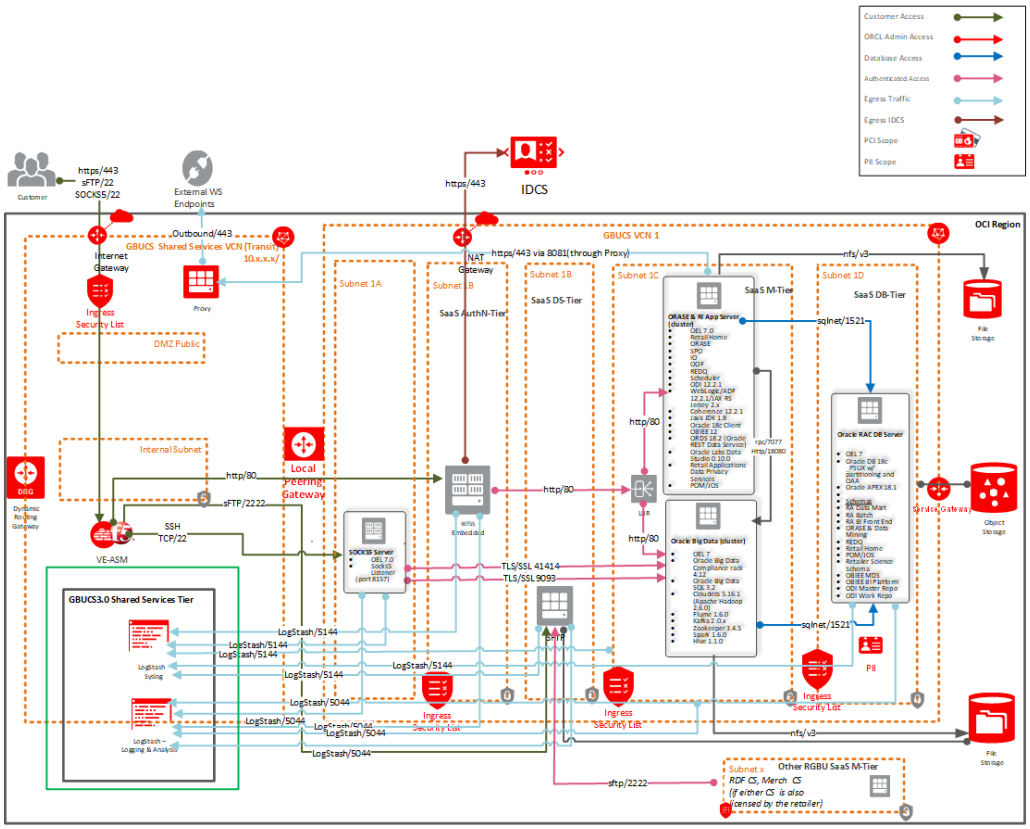
Retail Analytics and Planning

As part of the Retail Analytics and Planning cloud services, the latest version of Retail Insights shares many common components, tools, and processes with other applications like AI Foundation Cloud Services. This document is specific to the version of RI deployed in 1st Generation architecture, which is not part of the RAP platform and maintains its own deployment model and security features.

Retail Insights Physical Deployment

The following diagram provides a high-level overview of the physical deployment of Retail Insights.

Figure 1-1 Physical Deployment



Retail Insights

The PC user interface for the Oracle Retail Insights application is web-based, normally accessed through a browser. RI does not provide it's own user interface, but instead leverages the Oracle Analytics Server product for all it's interface needs.

The minimal configuration of the Oracle Retail Insights application runs on three types of servers: one for the reporting user interface via Oracle Analytics Server (OAS), one for the batch execution via Oracle Data Integrator (ODI), and one for the Oracle database. The batch execution and ODI metadata can be on the same server with Oracle database. Using same Oracle database server for ODI metadata and RI data mart can improve batch performance due to less network traffic. The storage of executables, scripts, configurations and data for each can reside on a central mirrored disk array cabinet unit or can be segregated by server type, with the file system configured as a shared mount point for relevant servers. All the servers and disk storage units are inter-connected by one or more high speed optical fiber channels where appropriate to insure quickest data communication relative to time critical processes occurring on each server. For connectivity to Retail Insights data source systems and Retail Insights hosted in the corporate data center, a LAN is sufficient. And for systems external to the data center, a WAN is usually sufficient.

The data aggregation logic is found on the batch server while the reporting logic for the application is customized by users and stored on the application server.

The U.I. server setup involves Oracle Analytic Server (OAS), which support horizontal scaling to provide some higher availability, load balancing and fail-over, and visualization. To fully enable clustering requires a Web Load Balancer servicing HTTP requests from PC clients, and the cohabitation of OAS on the multiple servers.

The database server hosts the Oracle database instance for the application. The database server can optionally be RAC enabled, using Oracle Clusterware, to provide high availability and fail-over, without which a fail-over backup server (potentially idle) would be required.

The Retail Insights application has numerous ODI batch jobs. The scheduling can be performed by the same scheduler installed for the core Merchandising applications. The processing architectures of most batch jobs do not naturally lend themselves to horizontal scaling across multiple servers. However in the event of a batch server hardware failure, a backup server connected to the same file system may be needed to facilitate quicker restart of aborted jobs. Alternatively, batch jobs could be executed on the database server and/or ODI batch server if ODI is installed on the different server with Retail Insights database server, but with a RAC setup the load balancing of multiple jobs, across multiple servers is not straightforward. In addition, jobs run on RAC database servers, will cause uneven contention for resources with the Oracle database instances that would partially defeat the load balancing efforts of RAC for Oracle database instances.

All of the batch jobs except data mining related batch jobs should run daily during a nightly batch window with no user access availability for the application. Data mining batch jobs should run weekly.

Oracle Analytics

The standard reporting tool for Retail Insights is Oracle Analytics Server (OAS). The version of OAS used is the standalone enterprise edition platform, not the cloud-hosted OCI version (known as OAC). Using OAS allows for full control over the configurations, metadata, and support process within our own hosted cloud environments.

Dependent Applications

- Oracle® Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition
- Oracle WebLogic Server Documentation Library
- Oracle® Database 2 Day + Security Guide, 12c Release 1
- Oracle® Fusion Middleware Developer's Guide for Oracle Data Integrator

Secured setup of Retail Insights Infrastructure in WebLogic

Retail Insights is deployed in Oracle Analytics Server (OAS) on top of WebLogic (WLS). The security of Oracle Analytics can be configured at different levels based on security requirements.

This document provides steps of securing the WebLogic infrastructure where OAS has been installed.

To learn about security at different layers of OAS, please refer to *Managing Security for Oracle Analytics Server*.

WebLogic Server supports SSL on a dedicated listen port. Oracle Analytics can be configured to use SSL as well. To establish an SSL connection, a Web browser connects to WebLogic

Server by supplying the SSL listen port and the HTTPs protocol in the connection URL, for example, https://myserver/analytics.

Retail Insights setup is supported in WebLogic in secured mode. For enterprise deployment, it uses SSL certificates signed by certificate authorities. The process in the following sections describes how SSL certificates are obtained and used with WebLogic. No action is needed outside of Oracle when interacting with OAS deployed as part of Retail Insights in the cloud, this is mainly for informational purposes.

> **Note:**
>
> Separate signed SSL certificates needs to be obtained for each host where application is being deployed.

Obtain an SSL Certificate and Setup a Keystore

1. Obtain an identity (private key and digital certificates) and trust (certificates of trusted certificate authorities) for WebLogic Server. 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 reputable vendor such as Entrust or Verisign to perform this step.
   a. Set appropriate JAVA_HOME and PATH to java.

      Example:

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

   b. Create a new keystore.

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

      Example:

      ```
      keytool -genkey -keyalg RSA -keysize 2048 -keystore
      [SERVERNAME].keystore -alias [SERVERNAME]
      ```

   c. Generate the signing request.

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

      Example:

      ```
      keytool -certreq -keyalg RSA -file [SERVERNAME].csr -keystore
      [SERVERNAME].keystore -alias [SERVERNAME]
      ```

   d. Submit the certificate request to Certificate authority.
2. Store the identity and trust. Private keys and trusted CA certificates which specify identity and trust are stored in a keystore.

   In following examples, we are using same keystore to store all certificates.

   a. Import the root certificate into the keystore.

      Example:

```
keytool -import -trustcacerts -alias verisignclass3g3ca -file Primary.pem-
keystore  [SERVERNAME].keystore
```

b. Import the intermediary certificate (if required) into the keystore.

Example:

```
keytool -import -trustcacerts -alias oracleclass3g3ca -file Secondary.pem-
keystore  [SERVERNAME].keystore
```

c. Import the received signed certificate for this request into the keystore.

Example:

```
keytool -import -trustcacerts -alias [SERVERNAME] -file cert.cer -keystore
```

Configure the Application Server for SSL

Follow the below steps to configure both the **Administration** server and managed server of Oracle Analytics (**bi_server1**). You can choose to disable the non-SSL ports (HTTP). It is highly recommended to secure the Node Manager. The steps to secure Node Manager as provided in the next section.

1. Configure the identity and trust keystores for WebLogic Server in the WebLogic Server Administration Console.
   a. In the Change Center of the Administration Console, click **Lock & Edit**.
   b. In the left pane of the Console, expand **Environment** and select **Servers**.
   c. Click the name of the server for which you want to configure the identity and trust keystores. For Forms server, it would be typically WLS_FORMS.
   d. Select **Configuration > Keystores**.
   e. In the **Keystores** field, select **Custom Identity and Custom Trust**.
   f. In the **Identity** section, define attributes for the identity keystore.

      Custom Identity Keystore: The fully qualified path to the identity keystore created above.

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

      Custom Identity Keystore Passphrase: The password you will 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.

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

      Custom Trust Keystore: The fully qualified path to the trust keystore.

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

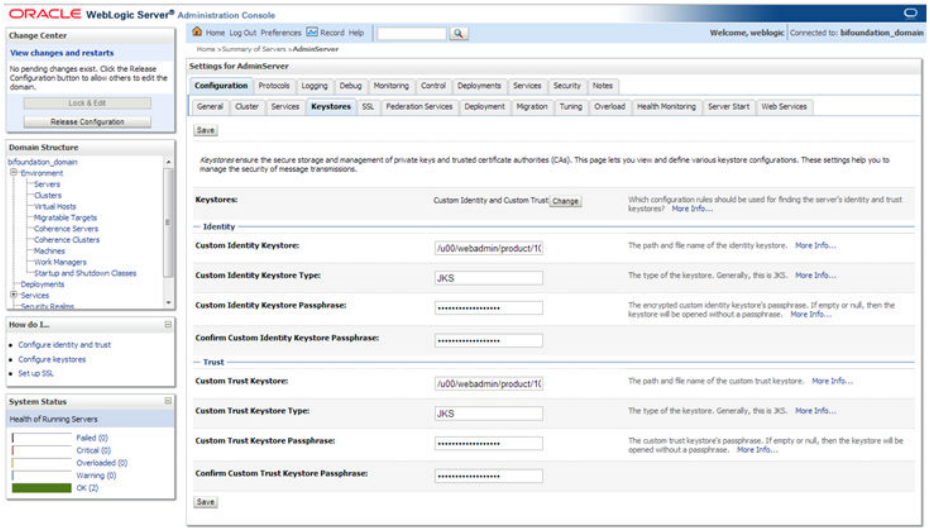
      Custom Trust Keystore Passphrase: The password you will enter when reading or writing to the keystore. This attribute is optional or required depending on the type of keystore. All keystores require the passphrase in order to write to the keystore. However, some keystores do not require the passphrase 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.

h. Click **Save**.

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

Not all changes take effect immediately-some require a restart.

Figure 1-2 Keystores Window



> **Note:**
>
> See "Configure Keystores" in the *Administration Console Online Help* for more information.

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

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

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

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

d. Select **Configuration > SSL**.

e. In the **Identity and Trust Locations**, defaults to **Keystores**.

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

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

h. Save the changes.

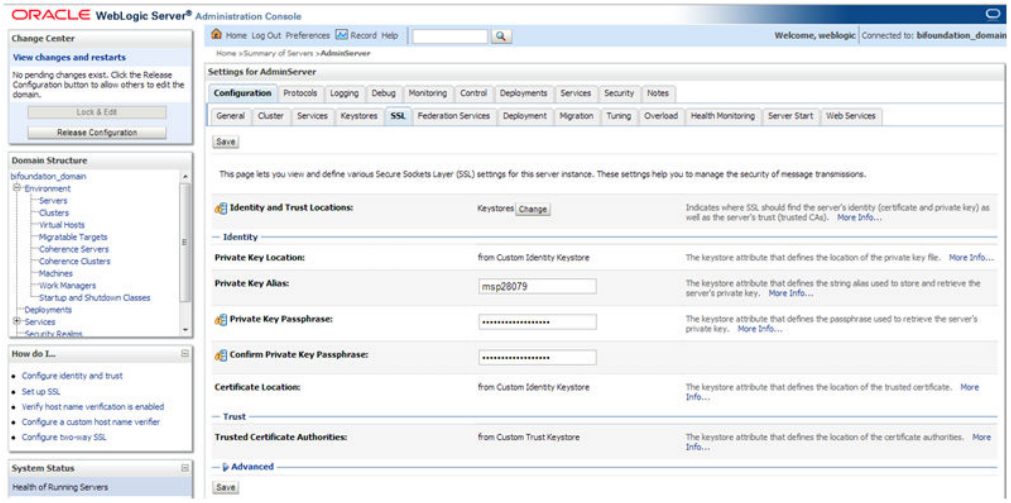
i. Click on **Advanced** section of SSL tab.

j. In the **Hostname Verification**, select as **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).

k. Save the changes.

Figure 1-3 SSL Window



> **Note:**
>
> See "Configure SSL" in the *Administration Console Online Help* for additional information.

Post Setup

All the server SSL attributes are dynamic; when modified via 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. To ensure that all the SSL connections exist according to the specified configuration, you must reboot WebLogic Server.

Use the **Restart SSL** button on the Control: Start/Stop page to restart the SSL server when changes are made to the keystore files and need to be applied for subsequent connections without rebooting WebLogic Server.

Upon restart you can see 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 listening on ip.to.your.server:57002 for protocols iiops, t3s,
ldaps, https.>
<Mar 11, 2013 5:18:27 AM CDT> <Notice> <Server> <BEA-002613> <Channel
"DefaultSecure[1]" is now listening 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>
```

Configuring WebLogic Scripts if Administration Server is Secured

WebLogic startup/shutdown scripts should be updated with secured port and protocol to start/stop services.

Backup and update following files in <DOMAIN_HOME>/bin with correct Admin server URLs.

Update the following files:

startManagedWebLogic.sh: echo "$1 managedserver1 http://[SERVERNAME].us.oracle.com:7001" **stopManagedWebLogic.sh**: echo "ADMIN_URL defaults to t3://[SERVERNAME].us.oracle.com:7001 if not set as an environment variable or the second command-line parameter."
stopManagedWebLogic.sh: echo "$1 managedserver1 t3://[SERVERNAME].us.oracle.com:7001 weblogic weblogic"
stopManagedWebLogic.sh: ADMIN_URL="t3://[SERVERNAME].us.oracle.com:7001"
stopWebLogic.sh: ADMIN_URL="t3://[SERVERNAME].us.oracle.com:7001"

Change the URLs to the values below wherever applicable.

t3s://[SERVERNAME].us.oracle.com:7102 https://[SERVERNAME].us.oracle.com:7102

Adding a Certificate to the JDK Keystore

Retail application installer will need Java to run. In situation where Administration server is secured using signed certificate, the Java keystore through which the installer is launched must have the certificate installed.

Example:

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

Enforcing Stronger Encryption in WebLogic

Upgrading JDK to use Java Cryptography Extension

If you want to use the strongest Cipher suite (256 bit encryption) you have to install the unlimited encryption JCE policy. It is dependent on the JDK version.

Using the following URL, download and install the Java Cryptography Extension (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 http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html and replace the files in JDK/jre/lib/security directory.

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

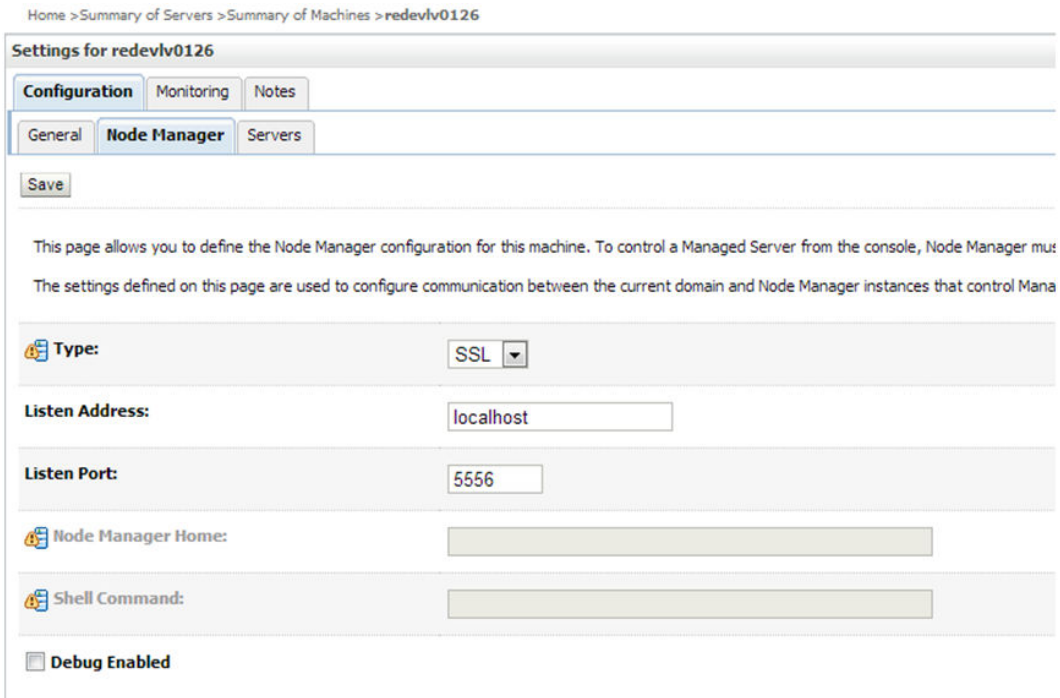
Securing Nodemanager with SSL Certificates

1. Navigate to **<DOMAIN_HOME>/nodemanager** and take a backup of nodemanager.properties.
2. Add similar entry to **nodemanager.properties**:

```
KeyStores=CustomIdentityAndCustomTrust CustomIdentityKeyStoreFileName=/u00/
webadmin/ssl/[SERVERNAME].keystore CustomIdentityKeyStorePassPhrase=[password to
keystore, this will get encrypted]
CustomIdentityAlias=[SERVERNAME]
CustomIdentityPrivateKeyPassPhrase=[password to keystore, this will get encrypted]
CustomTrustKeyStoreFileName=/u00/webadmin/ssl/[SERVERNAME].keystore
SecureListener=true
```

3. Login to WebLogic console, navigate to **Environment** > **Machines**. Select the nodemanager created already and navigate to **Node Manager** tab. In the Change Center, click **Lock and Edit**.
4. For Type, select **SSL** and save and activate (this may already be set to SSL).
5. "Listen Address" must be set to the server name used for the certificate request.

Figure 1-4 Nodemanager Window



6. After activating the changes, you need to bounce entire Weblogic Domain for changes to take effect. Verify the nodemanager is reachable in **Monitoring** tab after restart.

Advanced Infrastructure Security

Depending upon your security need for your production environment, infrastructure where retail applications are deployed can be secured. Following should be secured to ensure complete protection of environment.

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

Please refer to Ensuring the Security of Your Production Environment section in the *Oracle® Fusion Middleware Securing a Production Environment for Oracle WebLogic Server 12c (12.2.1)* for more information.

Troubleshooting

Java 8 SSL handshake issue while using self signed certificates

Java 8 may have issues using self signed certificates. The self-signed root certificate may not be recognized by Java 1.8 and a certificate validation exception might be thrown during the SSL handshake. To fix this problem, the private key must be created with Subject Key Identifier. An option "-addext_ski" must be included when the orapki utility is used to create the private key in the root wallet.

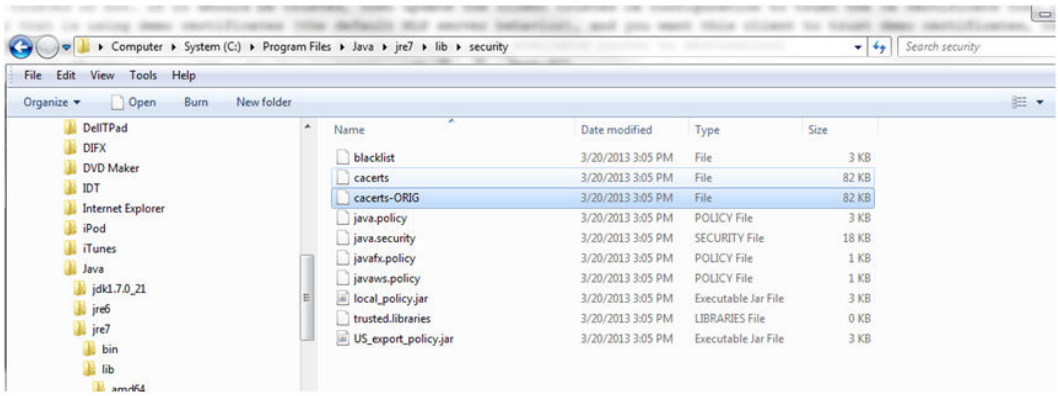
Import the root certificate in local client JRE

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 error with 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. In order to import the root certificates, follow the steps similar to below.

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

Figure 1-5 Backup the CA Certificate



2. Import the certificate using the keytool utility.

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

Enter keystore password: [default is changeit]
Owner: CN=[SERVERNAME].us.oracle.com, OU=RGBU, O=Oracle Corporation,
L=Minneapolis, ST=Minnesota, C=US
Issuer: CN=[SERVERNAME].us.oracle.com, OU=RGBU, O=Oracle Corporation,
L=Minneapolis,
ST=Minnesota, C=US 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\jre7\lib\security>
```

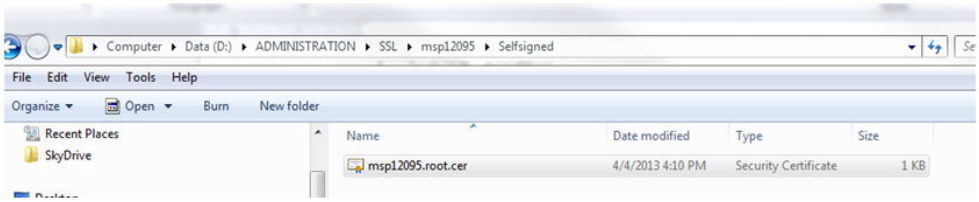
Import the Root Certificate to the Browser

If the Root Certificate that signed WebLogic server certificate is not in that list of trusted CAs, you need to add it in the browser to avoid certificate verification error.

For Internet Explorer, that requires the following steps:

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 1-6 Rename Root Certificate

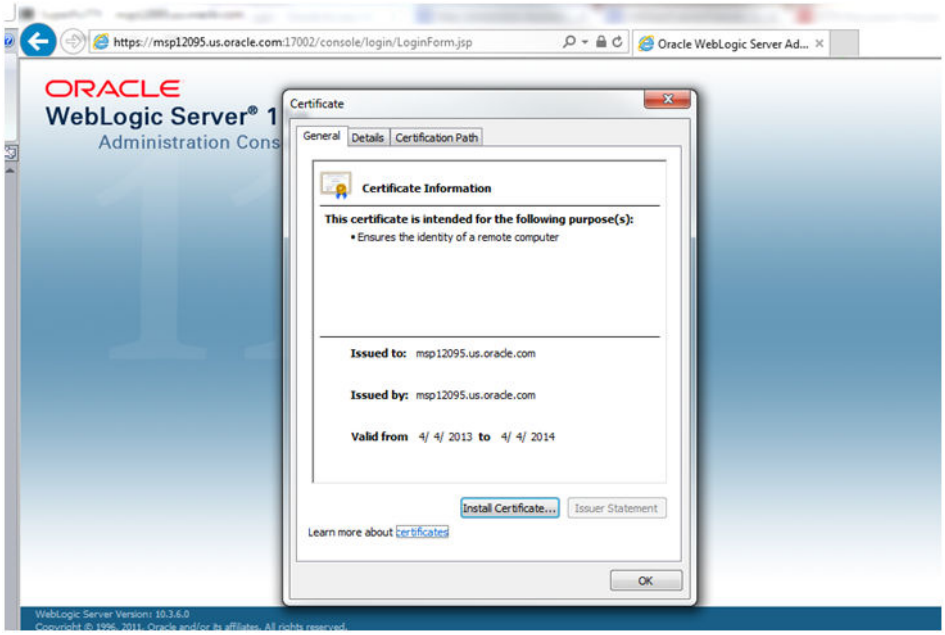


3. Double-click on the file.
4. Click **Install Certificate** and click **Next**.
5. Select Place all certificates in the following store and click **Browse**.
6. Select **Trusted Root Certification Authorities** and click **OK**.
7. Click **Next**.
8. Click **Finish** and then **Yes** at the Security Warning prompt.
9. Click **OK** to close the remaining open dialog boxes.

To do the same thing in Firefox, you follow a similar set of steps:

1. Start Firefox.
2. Select Tools > Options from the main menu.
3. Click on **Advanced** and then the Encryption tab.
4. On the Encryption tab, click **View Certificates**.
5. In Certificate Manager, click the Authorities tab and then the **Import** button.
6. In the Downloading Certificate dialog, choose **Trust this CA to identify websites** and click **OK**.
7. Click **OK** in Certificate Manager and then in Options.
8. Open a browser and test you URL using the SSL port.

Figure 1-7 Test the Firefox URL



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.

To disable hostname verification for testing purposes, follow these steps:

1. Go to Environment -> Domain -> Servers -> AdminServer.
2. Click the SSL tab.
3. Click **Advanced**.
4. On Hostname Verification, select **NONE**.
5. Click **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 like this:
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 Certificate Content

In situations where the certificate gets expired or may belong to other hosts, the certificates become unusable. To determine the details of the certificate keytool utility can be used. If the certificates are expired, they should be renewed or new certificates should be obtained from appropriate certificate authorities.

Example:

```
[SERVERNAME]:[10.3.6_apps] /u00/webadmin/ssl> keytool -printcert -file cert.cer
Certificate[1]:
Owner: CN=[SERVERNAME].us.oracle.com, OU=FOR TESTING PURPOSES ONLY, O=Oracle
Corporation, L=Redwood City, ST=California, C=US
Issuer: CN=Oracle SSL CA, OU=Class 3 MPKI Secure Server CA, OU=VeriSign Trust
Network, O=Oracle Corporation, C=US
Serial number: 8878deb9f2a1a44e3cd6d92a3987296
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:
EC:A7:16:DF:B6
         Signature algorithm name: SHA1withRSA
         Version: 3

Extensions:
```

Verifying Keystore Content

Keystores are repository of the certificates. In situations when we are facing issues related to SSL Certificates, once can check the certificates which are available in the keystore. In case the certificates are not missing, they should be imported. 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/[SERVERNAME].keystore
```

Integration Issues

Retail applications can be deployed across different hosts and even behind network behind firewalls. Ensure that 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. Refer to Enforcing stronger encryption in WebLogic section in Pre-install steps for Secured setup of Retail Infrastructure in WebLogic chapter on steps to specify secured protocol.

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. Refer to Import the root certificate in local client JRE section in Troubleshooting chapter for steps to import root certificates.

Technical Overview of the Security Features

Retail Insights Security Features

- Authentication is required when Retail Insights end users run Retail Insights front-end report or Retail Insights batch users execute Retail Insights batch in the back-end. For front-end, the authentication, including the storage of the credential of database connection, is managed by Oracle OAS, WebLogic, and Oracle IDCS or OCI IAM. For the back-end, the authentication, including the storage of the credentials of the database connection, is managed by ODI and Oracle DB Wallet.
- During Retail Insights installation, it is required to create different Retail Insights database users with different permissions. Within these database users, the Retail Insights data mart user is the user who owns data. The Retail Insights batch user is the user who executes Retail Insights batch. The batch user is granted with SELECT, UPDATE/ INSERT, and DELETE permissions to the resources owned by the Retail Insights data user. The Retail Insights front-end user is the database user who will query Retail Insights data through the front-end report. This user is granted with SELECT permission to the resources owned by the Retail Insights data user.
- The Universal Adapter is an optional ETL component which facilitates the loading of flat files generated from source system into Retail Insights database staging tables. The Universal Adapter is dependent on the Oracle Client installed on the Application server, so a sqlldr utility can be used to load data from files to RI staging tables. The credentials used in the sqlldr are stored in the Oracle Wallet.
- The Aggregation Framework is an optional ETL component which facilitates the loading of aggregation data into client customized aggregation tables. The Aggregation Framework is PL/SQL based programs. It requires that the Retail Insights batch user be granted read+write access to the UTLFILE folder on the database server. The framework can be uninstalled from the batch schema by dropping procedures RA_AGGREGATION_DAILY and RA_AGGREGATION_REC.

2

Application Administration

Oracle Retail Insights integrates tightly with Oracle Analytic Server (OAS) to allow the right content to be shown to the right user.

All components of Oracle Analytic Server are fully integrated with Oracle Fusion Middleware security architecture. OAS authenticates users using an Oracle WebLogic Server authentication provider against user information held in an identity store (IDCS or OCI IAM). User and group information is held within the Oracle Identity Cloud Service (IDCS) or Oracle Cloud Infrastructure Identity and Access Management (OCI IAM).

Ensure that you are familiar with the security features of Oracle Analytic Server before you begin working with Oracle BI Applications.

Security settings for Oracle Analytics Server are documented in *Managing Security for Oracle Analytics Server*.

Security Types

Security in Oracle Retail Insights can be classified into the following types. By default, Retail Insights does not provide these security features. You can choose to implement it based on the implementation requirements:

- **Data-level security** – controls the visibility of data (content rendered in subject areas, dashboards, Oracle BI answers, and so on) based on the user's association to data in the transactional system.
- **Object-level security** – controls the visibility to business logical objects based on a user's role. You can set up object-level security for metadata repository objects, such as subject areas and presentation folders, and for web objects, such as dashboards and dashboard pages, which are defined in the presentation catalog.

Data-Level Security in Retail Insights

This section describes the data-level security features in Retail Insights. Group IDs from the source system control access to certain levels of data, such as which Merchandising Department, or which Organization District. Data level security mapping is provided by users though interface files RAF_SEC_USER.dat, RAF_SEC_GROUP.dat, RAF_SEC_USER_GROUP.dat, RAF_FILTER_GROUP_MERCH.dat, RAF_FILTER_GROUP_ORG.dat.

- RAF_SEC_USER.dat contains USER_ID (LDAP ID) who has data access limit in OBIEE reporting.
- RAF_SEC_GROUP.dat contains GROUP_ID defined in the source system.
- RAF_SEC_USER_GROUP.dat contains mapping between USER and GROUP from the source system.
- RAF_FILTER_GROUP_MERCH.dat contains access mapping between Merch hierarchy level, Merch ID on that level, and the GROUP.

- RAF_FILTER_GROUP_ORG.dat contains access mapping between Organization hierarchy level, Org ID on that level, and the GROUP.
- User, whose USER_ID does not exist in the mapping, will have unlimited data access.

Object-Level Security in Retail Insights

This section describes the object-level security features in Retail Insights. It contains the following topics:

- Metadata Object-Level Security (Repository Groups)
- Metadata Object-Level Security (Presentation Services)

Metadata Object-Level Security (Repository Groups)

Application roles control access to metadata objects, such as subject areas, tables, and columns. For example, certain Retail Insights roles may not have access to view certain presentation tables. Metadata object security is configured in the Oracle BI Repository, using the Oracle BI Administration Tool. The Authenticated User group is denied access to some of the presentation tables and only related roles have explicit read access. This access can be extended to subject areas and columns.

> **Note:**
>
> By default in Oracle Retail Insights, only permissions at the presentation tables level have been configured.

For the full list of Retail Insights application roles and the associated enterprise roles, Refer to the Oracle Retail Insights Administration Guide. You have to create these enterprise roles in your authentication provider, such as WebLogic, Oracle Identity Cloud Service (IDCS), or Oracle Cloud Infrastructure Identity and Access Management (OCI IAM). For more information on how to set-up roles, refer to the *Oracle® Fusion Middleware - Security Guide for Oracle Business Intelligence Enterprise Edition*. In new Retail Insights Cloud Service environments, the default set of enterprise roles will be created in IDCS or OCI IAM and should be added to users and groups following the *Oracle Retail Insights Cloud Service Suite Administration Guide* instructions.

Except for core presentation tables available to all roles (such as Item dimension) presentation tables will be hidden by default, unless the user is granted the specific role necessary for that table. This permissions structure allows for strict control over which users can access data from different areas of RI based on their business needs. Note that the Retail Analyst role is a super-user role with visibility to all presentation tables. This role should be granted only to system administrators and implementers.

Metadata Object-Level Security (Presentation Services)

Oracle BI Presentation Services objects are controlled using Presentation Services groups. Access to these objects, such as dashboards and pages, reports, and Web folders, is controlled using the Presentation Services groups. Presentation Services groups are customized in the Oracle BI Presentation Services interface. For detailed

information about Presentation Services groups, see the *Oracle Business Intelligence Presentation Services Administration Guide*.

By default, users of Retail Insights will only have write-access to two folders in the presentation catalog:

- My Folders (personal storage for each user)
- Shared Folders > Custom (business objects which can be shared with the company)

All other folders, reports, dashboards, and related presentation objects in the RI catalog will be read-only to business users. Users may view or copy the provided presentation objects into one of their folders for their own use. RI application administrators can control the permissions on objects in Shared Folders > Custom as they see fit, such as by limiting the folder to read-only for other users or creating specific sub-folders for each business group.

Other Common Application Administration

- Retail Insights front-end clients access Retail Insights stored data through Oracle OAS. The credentials for Oracle OAS and Retail Insights Database access are managed through Oracle OAS security system. In Retail Insights front-end, some security features, such as session timeout set, are also managed by Oracle OAS and WebLogic server. See *Managing Security for Oracle Analytics Server* for the detail information.
- Retail Insights batch users access Retail Insights stored data through ODI. Then credentials for ODI and Retail Insights Database access are managed through ODI security system. See ODI Security Guide for the detail information.
- Configuration and logs files protection
  - Batch process:

    To execute Retail Insights batch, Retail Insights batch scripts, Retail Insights source data files, Retail Insights configuration files, and Retail Insights batch log files need to be placed under Retail Insights base home directory. These files are protected with secured permission. There is no world read for these files. Retail Insights batch scripts have 750 file permission Retail Insights configuration files have 660 permission, and Retail Insights static data files have 640 permission.
  - Front-end process:

    The default permission for OAS configuration files and log files are 640.

Application Specific Feature Administration

- The security and data access for Retail Insights goes beyond simple role based associations. Typically users and groups are associated with roles. The setup of each role determines what object is accessible by the users.
- Retail Insights batch user is the only one who can run the batch scripts and the connections managed by ODI are used by the batch processes to access data sources.
- For file permission, by default the following permissions are given to users to access files packaged with Retail Insights once installation is completed.
  - All Retail Insights scripts should at least have 750 permission
  - All configuration files should at least have 660 permission
  - All static data (csv files) should at least have 640 permission

Based on the permission above, besides owner (the installer user), the group member can also view and execute scripts, read and modify the configuration files, and read the static file. A user out of the group cannot do anything to Retail Insights files and explicit permission needs to be given by the Administrator to users outside of the group.

3
General Privacy and Security Information

Privacy by Design

As a Data Privacy enhancements, retail applications have created a data privacy web service interface and command line tool to provide retailers with services for requesting access to personal information for review and forget/update the personal information if requested.

Some of the examples of the personal information can be:

- Full Name
- Home address
- Email address
- Date of birth

The following features are handled as part of Retail Insights data privacy the using data privacy command line the tool:

- Right to Access (RTA)

  Enable retailers to accept and respond to end-user requests for data access, correction, and deletion for individual end-user data records they store in the Oracle service.

- Right to be Forgot (RTF)

  Based on end-users right to request to forget/update their personal information, enable the retailers to delete/update (mask) end-users personal data during the services period. Some of the data critical for the business or is part of the legal requirement might not be deleted.

Data Minimization

RI uses database role, enterprise role, and application role to control who has access to the data. At the front-end side, RI provides default enterprise roles based on their corresponding application roles provided by RI. Users assigned with a specific enterprise role can only access specific function area. For detail, see the User Creation and the Assign members to a role sections in the *Oracle Retail Insights Cloud Service Administration Guide*. At the database level, different database roles are assigned to different type of users. The front-end user role only has read permission to RI data. Batch user role has read, insert, update, and delete permission to RI data.

Data Deletion

The data deletion concept has always been of high importance in RI. The Retail Insights product is a Business Intelligence system which stores the customer centric/ Merchandising data for a specified time limit only, as this is required for making business decisions. When data reaches the threshold it can be deleted from the system to release the memory occupied by stale data. This will not be automatic unless already agreed on during setup.

Right to Access / Right to Forget

RI provides a web service interface (file RetailAppsDataPrivServices-7.0.1-RetailAppsDataPrivServices.ear) for right to access and right to forget. The service provides a REST call to return end-user information based on a provided key and provides a REST call to forget the end-user based on a provided key. See Retail Insights Installation Guide on how to deploy the service. The feature is also available via the command line by using jar file RetailAppsDataPrivServices-7.0.1-RetailAppsDataPrivTool.jar

RI provides three groups (type_id) for right to access and right to forget. See Appendix C for how type_id is used.

- CustomerRecord

  By providing customer number as key, the end user can access or forget the PII data for the customer, customer address, and history sales information related with this customer.

- Employee

  By providing employee number as key, the end user can access or forget the PII data for the employee.

- Supplier

  By providing primary contact name as key, the end user can access or forget supplier contact name and supplier contact phone number information.

See Appendix C on how to use command line for the right to access and right to forget feature. See the Data Privacy Services REST Endpoints section in Appendix C for service REST Endpoints

Data Portability

RI provides the capability for the end users to export the downloaded report to transmit data to another controller.

Encryption

RI uses Oracle Transparent Data Encryption TDE tablespace encryption to encrypt entire RI tablespaces.

Data Masking

Oracle data redaction is used for RI data masking. A data redaction policy has been created in RI on the W_PARTY_PER_D. ETHNICITY_NAME and W_PARTY_PER_D. ETHNICITY_CODE columns. Only users that are granted EXEMPT REDACTION POLICY can view the data. Out of the box, only the RI batch user is granted EXEMPT REDACTION POLICY.

A

Appendix: Database Security Guide

The database should be secured using the recommendations from the *Oracle Database 12c Release 1 Security Guide*. The following sections provide additional application specific guidance for securing the database for use with Oracle Retail products.

Application Schema Owners

The following recommendations should be considered for the schema owners:

- Database Administrators should create an individual schema owner for each application, unless the applications share the same data.

  For example, the Oracle Retail Point-of-Service and Back Office applications share the same database.
- The schema owners should only have enough rights to install the applications.
- Set the following rights when using an Oracle database:
  - CREATE TABLE
  - CREATE VIEW
  - CREATE INDEX
  - CREATE SEQUENCE
  - CREATE PROCEDURE
  - ALTER SESSION
  - CONNECT
- After the database objects are created, the following rights are no longer needed, and should be revoked:
  - When using an Oracle database, revoke CREATE PROCEDURE.

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 via 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 internal database JVM is required to be Java JVM v7.0 in order to run the optional Universal Adapter ETL component
  - Note that in Oracle 12c, the internal JVM version is configurable
  - For more information regarding the internal JVM, please refer to the Oracle Database Java Developer's Guide

The purge script is usually put into an automation script, which runs once per day. As described above, this script is usually run by a user with limited access (only execute procedure and connect access).

B

Appendix: References

Information in the following documents can be used to supplement the information contained in this guide:

- Oracle® Fusion Middleware Administering Security for Oracle WebLogic Server 12.2.1: 28 Overview of Configuring SSL in WebLogic Server

  http://docs.oracle.com/middleware/1221/wls/SECMG/ssl_overview.htm#SECMG718

- Oracle® Fusion Middleware Administering Security for Oracle WebLogic Server 12.2.1: 29 Configuring Keystores

  http://docs.oracle.com/middleware/1221/wls/SECMG/identity_trust.htm#SECMG365

- Oracle® Fusion Middleware Guide for Oracle Business Intelligence Enterprise Edition: 5 Configuring SSL in Oracle Business Intelligence

  https://docs.oracle.com/middleware/1221/biee/BIESC/ssl.htm#BIESC374

C

Appendix: Data Privacy Installation

The services that are part of data privacy command line tool are executable though a command line executable JAR file RetailAppsDataPrivTool.jar

Setting up the Java Development Kit (JDK)

Java 1.8 is a prerequisite to install and test the data privacy command line tool. This section contains instructions on how to set up the Java Development Kit (JDK).

Download and Install Java 8

Download the latest 64-bit version of Java SE Development Kit 8. Install in a location on your machine. Ensure that the installation folder name does not contain any whitespaces (example: Program Files)

Define Environment Variables for JDK

To effectively use the JDK on your workstation you need to define environment variables on your system.

Define the JAVA_HOME Variable

Define a new environment system variable named JAVA_HOME with a value referring to the path where your JDK is installed. Example:

```
JAVA_HOME=D:\Java\jdk1.8_66
```

Modify the PATH Variable

Modify your system's existing PATH variable to include executable program location on your JDK installation. These executables are located under %JAVA_HOME%\bin.

```
PATH=%JAVA_HOME%\bin;%PATH%
```

Testing Your JDK Installation

1. Start a new command line window by selecting Start ->Run -> Open -> type `cmd.exe`.
2. Go to the root directory by typing:

   ```
   cd c:\ <enter>
   ```

3. Run the Java compiler and query its version by typing:

   ```
   javac -version
   ```

   The command should return with the Java version information similar to shown below. Make sure it matches with the JDK version you just installed.

```
D:\gdpr>java -version
java version "1.8.0_66"
Java(TM) SE Runtime Environment (build 1.8.0_66-b18)
Java HotSpot(TM) 64-Bit Server VM (build 25.66-b18, mixed mode)

D:\gdpr>javac -version
javac 1.8.0_66
```

Data Privacy Command Line Tool

Download the following RA/RI files:

- RetailAppsDataPrivTool.jar
- ContextOverride.properties
- DATAPRIV-Global.xml
- DATAPRIV-ValidateForget.xml
- DATAPRIV-Get.xml
- DATAPRIV-Forget.xml

1. Create a folder DataPrivacy and copy the RetailAppsDataPrivTool.jar into this folder.
2. Create a folder RIDataPrivConfig under the DataPrivacy folder and copy DATAPRIV-Global.xml, DATAPRIV-ValidateForget.xml, DATAPRIV-Get.xml and DATAPRIV-Forget.xml into this folder.

Configure the Configuration Files

Perform the following changes to the specified configuration files:

- ContextOverride.properties - Contains details of the connection string to be used in case of using oracle wallet. This needs to be modified to enter the correct database information.
  - The JDBC URL must comply with the following format to reference Oracle Wallet credentials at runtime:
  - A forward slash "/" must be specified BEFORE the "@" character. This instructs the Oracle database driver to be aware of Oracle Wallet aliases.
  - The identifiers following the "@" character must be registered as an alias in the Oracle Wallet. The wallet creation and configuration steps is explained in the next section.
  - Datasoure string format - datasource-url=jdbc:oracle:thin:/@hostname:port/SID e.g. - datasource-url=jdbc:oracle:thin:/@myhost:1521/mydb
- DATAPRIV-Global.xml - Contains DB connection details as well as details of customer-id-format. No changes necessary for this file.
- DATAPRIV-Get.xml - Contains the SQL query or function to perform the right to access. No changes necessary for this file.

- DATAPRIV-Forget.xml - Contains the SQL query or function to perform the right to forget. No changes necessary for this file.
- DATAPRIV-ValidateForget.xml - Contains validations to perform prior to right to forget. No changes necessary for this file.

Creating and Configuring Oracle Wallet

Data privacy command line tool uses oracle wallet to securely store the database credentials. The wallet can be created using the RetailAppsDataPrivTool.jar.

Perform the following steps to create and configure the Oracle wallet for the data privacy command line tool.

1. Create an empty wallet file in a DataPrivacy directory by running the below command in a command prompt (cmd) in DataPrivacy folder.

   ```
   java -classpath RetailAppsDataPrivTool.jar
   oracle.security.pki.OracleSecretStoreTextUI      -wrl <wallet directory> -create
   ```

   For example:

   ```
   java -classpath ./RetailAppsDataPrivTool.jar
   oracle.security.pki.OracleSecretStoreTextUI -wrl ./tmp_wallet -create
   ```

   You are prompted for a password. This will be the password to manage the contents of the wallet files. Note this password as it will be needed in succeeding commands against the wallet files.

2. Add the database credentials into the wallet by running the below command in the command prompt (cmd) in the DataPrivacy folder. This will prompt to enter the password you created in step 1.

   ```
   java -classpath RetailAppsDataPrivTool.jar
   oracle.security.pki.OracleSecretStoreTextUI
        -wrl <wallet directory>
        -createCredential  <db connect string>  <db user>  <db password>
   ```

   <db connect string> - is the database connection string included in a JDBC connection url in the ContextOverride.properties.xml. It is the part of the JDBC url after the "@" character.

   It is specified using the format: <hostname>:<port>/<SID>

   Example:

   ```
   myhost:1521/mydb
   <db user> - DB user to connect to the RI DB.
   <db password> - password to connect to the RI DB.
   ```

   For example:

   ```
   java -classpath ./RetailAppsDataPrivTool.jar
   oracle.security.pki.OracleSecretStoreTextUI -wrl ./tmp_wallet -createCredential
   myhost:1521/mydb rmsuser password
   ```

3. Verify the database credentials in the wallet by running the following command in the command prompt (cmd).

   ```
   java -classpath RetailAppsDataPrivTool.jar
   oracle.security.pki.OracleSecretStoreTextUI
   ```

```
-wrl <wallet directory>
-listCredential
```

For example:

```
java -classpath ./RetailAppsDataPrivTool.jar
oracle.security.pki.OracleSecretStoreTextUI -wrl ./tmp_wallet -listCredential
```

Make sure the credential information shown by the command is as expected.

Using the Data Privacy Command Line Tool

The Private Data Services command line tool is an executable JAR file that uses the "java -jar" option:

```
java  -DContextOverride.properties=<Context Override Properties file>
      -Duse.jdbc.oracle.wallet=true
      -Doracle.net.wallet_location=<Oracle wallet directory>
      -Dconfig.xml.dir=<configration files directory>
      -Ddatapriv.action=<action>
      -Dcustomer.id=<query parameters for the tool>
      -Did.type=<table_used>
      -Dinvoked.by=<user ID>
      -Doutput.file.dir=<output file directory>
      -jar RetailAppsDataPrivServices-7.0.1-RetailAppsDataPrivTool.jar
```

The parameters are given to the command line via system property JVM arguments (-D options).

Understanding the Command Line Parameters

Table C-1 Command Line Parameters

System Property/ Parameter	Required	Description
ContextOverride.properties	Always	The path to a Java properties file that will contain the connection details of the database the data privacy command line tool will connect to. Refer to Configure the Configuration Files for additional details.
use.jdbc.oracle.wallet	Always	Set to true to use Oracle Wallet files as a source for database credentials. Refer to Creating and Configuring Oracle Wallet for additional details.
oracle.net.wallet_location	Always	The path to the Oracle Wallet directory. Refer to Creating and Configuring Oracle Wallet for additional details.
config.xml.dir	Always	The directory that contains the DATAPRIV configuration XML files.

Table C-1 (Cont.) Command Line Parameters

System Property/ Parameter	Required	Description
datapriv.action	Always	The data privacy action to be performed: Valid values: • access • forget
customer.id	Always	The input parameters to the query/update the personal data.
id.type	Always	The table for which the data privacy action will be performed.
invoked.by	Always	The ID of the user calling the command line tool (for audit purposes).
output.file.dir	No	The output files directory. Default is the user's home directory.

Command Query

Format for datapriv.action=access (Right to Access)

example:

Employee

```
java -DContextOverride.properties=D:\EU-GDPR\RI\ContextOverride.properties -
Duse.jdbc.oracle.wallet=true -Doracle.net.wallet_location=./tmp_wallet -
Dconfig.xml.dir=D:\EU-GDPR\RI\RIDataPrivConfig -Ddatapriv.action=access -
Dcustomer.id="-1" -Did.type=employee -Dinvoked.by=user -Doutput.file.dir=D:\EU-
GDPR\RI\out -jar RetailAppsDataPrivServices-7.0.1-RetailAppsDataPrivTool.jar
```

Supplier

```
java -DContextOverride.properties=D:\EU-GDPR\RI\ContextOverride.properties -
Duse.jdbc.oracle.wallet=true -Doracle.net.wallet_location=./tmp_wallet -
Dconfig.xml.dir=D:\EU-GDPR\RI\RIDataPrivConfig -Ddatapriv.action=access -
Dcustomer.id="123" -Did.type=supplier -Dinvoked.by=user -Doutput.file.dir=D:\EU-
GDPR\RI\out -jar RetailAppsDataPrivServices-7.0.1-RetailAppsDataPrivTool.jar
```

Customer

```
java -DContextOverride.properties=D:\EU-GDPR\RI\ContextOverride.properties -
Duse.jdbc.oracle.wallet=true -Doracle.net.wallet_location=./tmp_wallet -
Dconfig.xml.dir=D:\EU-GDPR\RI\RIDataPrivConfig -Ddatapriv.action=access -
Dcustomer.id="-1" -Did.type=customerRecord -Dinvoked.by=user -Doutput.file.dir=D:\EU-
GDPR\RI\out -jar RetailAppsDataPrivServices-7.0.1-RetailAppsDataPrivTool.jar
```

Customer.id format for datapriv.action= forget (Right to Forget)

Query example:

Employee

```
java -DContextOverride.properties=D:\EU-GDPR\RI\ContextOverride.properties -
Duse.jdbc.oracle.wallet=true -Doracle.net.wallet_location=./tmp_wallet -
Dconfig.xml.dir=D:\EU-GDPR\RI\RIDataPrivConfig -Ddatapriv.action=forget -
Dcustomer.id="-1" -Did.type=employee -Dinvoked.by=user -Doutput.file.dir=D:\EU-
GDPR\RI\out -jar RetailAppsDataPrivServices-7.0.1-RetailAppsDataPrivTool.jar
```

Supplier

```
java -DContextOverride.properties=D:\EU-GDPR\RI\ContextOverride.properties -
Duse.jdbc.oracle.wallet=true -Doracle.net.wallet_location=./tmp_wallet -
Dconfig.xml.dir=D:\EU-GDPR\RI\RIDataPrivConfig -Ddatapriv.action=forget -
Dcustomer.id="123" -Did.type=supplier -Dinvoked.by=user -Doutput.file.dir=D:\EU-
GDPR\RI\out -jar RetailAppsDataPrivServices-7.0.1-RetailAppsDataPrivTool.jar
```

Customer

```
java -DContextOverride.properties=D:\EU-GDPR\RI\ContextOverride.properties -
Duse.jdbc.oracle.wallet=true -Doracle.net.wallet_location=./tmp_wallet -
Dconfig.xml.dir=D:\EU-GDPR\RI\RIDataPrivConfig -Ddatapriv.action=forget -
Dcustomer.id="-1" -Did.type= customerRecord -Dinvoked.by=user -
Doutput.file.dir=D:\EU-GDPR\RI\out -jar RetailAppsDataPrivServices-7.0.1-
RetailAppsDataPrivTool.jar
```

Understanding the command output files

The command line tool produces the output files after execution.

All files are generated by default in the user's home directory. Parameters are available to configure the directory.

Data Privacy Services REST Endpoints

Resource URL

```
http://<server>:<port>/RetailAppsDataPrivServicesRESTApp/rest/privatedata
```

Required Request Headers

Table C-2 Required Request Header List

Header	Values
Accept	application/json or application/xml Refer to endpoint documentation below to see what the endpoint requires.
Authorization	Base 64 encoded authorization string representation of the user credentials.

List of Resource Endpoints

Table C-3 List of Resource Endpoints

Operation	Path	Method	Accept	Description
Access customer's information (JSON)	/privatedata/{id_type}	GET	application/json	Returns customer information in the system in JSON formats Path Parameters • id_type: The type of query to be executed. This is matched against the query group type defined in the RTA Get configuration XML.Refer to the RAF DATAPRIV Services Configuration XML Files for details Query Parameters • customer_id: (required) The customer ID string to be used in looking up the customer. The format of this string must conform to the format indicated in the context parameter • customer-id-format" defined in the RTA Get Configuration XML for the input type (id_type). Refer to the RAF DATAPRIV Services Configuration XML Files for details. • jsonFormat : The type of JSON format to return. Valid values: "concise" (default) , "full". See Access Output Formats for details. Input Payloads • None Response Codes and Error Messages • 200 - Success • 400 - Bad Request - Produced for the following situations: - Customer ID does not match the required format - Invalid input type - Missing customer ID - Invalid jsonFormat • 500 - Internal Server Errors - for all other types of errors (e.g. config errors, sql errors, etc). Success Payloads • JSON payload depending on input jsonFormat. See Access Output Formats for details.

Table C-3 (Cont.) List of Resource Endpoints

Operation	Path	Method	Accept	Description

				Error Payload
				• See Error Payloads for information.
				Examples
				`GET http://127.0.0.1:7101/RetailAppsDataPrivServicesRESTApp/rest/privatedata/customer?customer_id=12::12::12`
				
				`GET http://127.0.0.1:7101/RetailAppsDataPrivServicesRESTApp/rest/privatedata/raf?customer_id=benny_anderson::benny_anderson@acme.com`
				
				`GET http://127.0.0.1:7101/RetailAppsDataPrivServicesRESTApp/rest/privatedata/raf?customer_id=12::12::12&jsonFormat=full`

Access customer's information (HTML)	/privatedata/{id_type}	GET	application/XML	Returns customer information in the system in HTML format. Same parameters as getting customer information in JSON format (see above) except that the "jsonFormat" query paramete is not applicable. Note that the Accept value MUST be application/XML to access this endpoint. The Output Payload generated in HTML format instead of JSON. See Access Output Formats for details.

Table C-3 (Cont.) List of Resource Endpoints

Operation	Path	Method	Accept	Description
Remove customer's information	/privatedata/{id_type}	DELETE	application/json	Removes the customer from the system. Path Parameters • id_type: The type of query to be executed. This is matched against the query group type defined in the Forget configuration XML.Refer to the RAF DATAPRIV Services Configuration XML Files for details Query Parameters • customer_id: (required) The customer ID string to be used in looking up the customer. The format of this string must conform to the format indicated in the context parameter "customer-id-format" defined in the Forget Configuration XML for the input type (id_type). Refer to the RAF DATAPRIV Services Configuration XML Files for details. Input Payloads • None Response Codes and Error Messages • 200 - Success - Delete successful • 412 - Precondition Failed - Unable to delete. • 400 - Bad Request - Produced for the following situations: - Customer ID does not match the required format - Invalid input type - Missing customer ID • 500 - Internal Server Errors - for all other types of errors (e.g. config errors, sql errors, etc). Error Payload • See Error Payloads for information. Examples: `DELETE http://127.0.0.1:7101/RetailAppsDataPrivServicesRESTApp/rest/privatedata/customer?customer_id=12::12::12`

Table C-3 (Cont.) List of Resource Endpoints

Operation	Path	Method	Accept	Description
Validate if customer's information can be removed	/privatedata/{id_type}/validateForget	GET	application/json	Validates whether a customer can be removed from the system. Path Parameters • id_type: The type of query to be executed. This is matched against the query group type defined in the Validate Forget configuration XML.Refer to the RAF DATAPRIV Services Configuration XML Files for details Query Parameters • customer_id: (required) The customer ID string to be used in looking up the customer. The format of this string must conform to the format indicated in the context parameter "customer-id-format" defined in the ValidateForget Configuration XML for the input type (id_type). Refer to the RAF DATAPRIV Services Configuration XML Files for details. Input Payloads • None Response Codes and Error Messages • 200 - Success - Person can be deleted • 412 - Precondition Failed - Person cannot be deleted • 400 - Bad Request - Produced for the following situations: - Customer ID does not match the required format - Invalid input type - Missing customer ID • 500 - Internal Server Errors - for all other types of errors (e.g. config errors, sql errors, etc). Error Payload • See Error Payloads for information. Examples: `GET http://127.0.0.1:7101/RetailAppsDataPrivServicesRESTApp/rest/privatedata/customer/validateForget?customer_id=12::12::12`

Table C-3 (Cont.) List of Resource Endpoints

Operation	Path	Method	Accept	Description
Get query group types for Access requests	/privatedata/config/access	GET	application/json	Returns the valid ID types that can be used in access calls. Path Parameters • None Query Parameters • None Input Payloads • None Response Codes and Error Messages • 200 - Success • 500 - Internal Server Errors - for all other types of errors (e.g. config errors, sql errors, etc). Success Payloads `{ "types": [ "raf", "supplier", "customer" ] }`

Table C-3 (Cont.) List of Resource Endpoints

Operation	Path	Method	Accept	Description

Get query group type information for access requests	/privatedata/config/access/{id_type}	GET	application/json	Returns details of the id type to be used for access requests.
				Path Parameters
				• id_type: The type of query to be executed. This is matched against the query group type defined in the Get configuration XML.Refer to the RAF DATAPRIV Services Configuration XML Files for details
				Query Parameters
				• None
				Input Payloads
				• None
				Response Codes and Error Messages
				• 200 - Success
				• 400 - Bad Request - Produced for the following situations:
				Invalid input type
				• 500 - Internal Server Errors - for all other types of errors (e.g. config errors, sql errors, etc).
				Success Payloads
				`{ "customerIdFormat": "{%customerId%}::{%divisionId%}::{%groupId%}", "type": "customer" }`
				Error Payload
				• See Error Payloads for information.
				Examples:
				`GET http://127.0.0.1:7101/RetailAppsDataPrivServicesRESTApp/rest/privatedata/config/access/customer`
				`GET http://127.0.0.1:7101/RetailAppsDataPrivServicesRESTApp/rest/privatedata/config/access/supplier`

Get query group types for Forget Access requests	/privatedata/config/forget	GET	application/json	Similar to "Get query group types for Access requests" but retrieves types from the Forget configuration xml

Table C-3 (Cont.) List of Resource Endpoints

Operation	Path	Method	Accept	Description
Get query group type information for Forget requests	/privatedata/config/forget/{id_type}	GET	application/json	Similar to "Get query group type information for access requests" but retrieves type information from the Forget configuration xml
Get query group types for Validate Forget Access requests	/privatedata/config/validateForget	GET	application/json	Similar to "Get query group types for Access requests" but retrieves types from the Validate Forget configuration xml
Get query group type information for Validate Forget requests	/privatedata/config/validateForget/{id_type}	GET	application/json	Similar to "Get query group type information for access requests" but retrieves types from the Validate Forget configuration xml

Access Output Formats

The following output formats are supported by the REST endpoint for Access requests:

Table C-4 Access Output Format List

Format	Description
Concise JSON (default)	Human readable JSON format. Concise but cannot be parsed into a generic stucture at runtime.
Full JSON	Full JSON format that can be parsed as a generic QueryGroupResult object. Ideal for importing data into the system (a future functionality)
Human Readable HTML	Human readable HTML format.

Concise JSON

```
{
    "Customer Information": {
        "Basic Information": {
            "list": [
                [
                    {
                        "Customer ID": "12344",
                        "First Name": "Joe",
                        "Middle Name": "Steven",
                        "LastName": "Smith",
                        "Division": "Division 4444",
                        "Group": "Group 5555"
                    },
                    {
                        "Customer ID": "12344",
                        "First Name": "Joseph",
```

```
                "Middle Name": "Steven",
                "LastName": "Smith",
                "Division": "Legacy Division 89-4444",
                "Group": "Legacy Group 76-5555"
            }
        ]
    ],
    "Phone Numbers": {
        "list": [
            [
                {
                    "Home Phone": "123-123-1234",
                    "Mobile Phone": "123-123-1234"
                }
            ]
        ]
    },
    "Addresses": {
        "list": [
            [
                {
                    "Address Line 1": "123 Stoney Lake Road",
                    "Address Line 2": "Apartment 2C30",
                    "City": "Toledo",
                    "State": "Ohio",
                    "Postal Code": "85225",
                    "Country": "United States"
                },
                {
                    "Address Line 1": "444 Hill Trail Road",
                    "Address Line 2": "null",
                    "City": "Cleveland",
                    "State": "Ohio",
                    "Postal Code": "44444",
                    "Country": "United States"
                },
                {
                    "Address Line 1": "123 Lyndale Avenue",
                    "Address Line 2": "Apartment 5B",
                    "City": "Minneapolis",
                    "State": "Minnesota",
                    "Postal Code": "554333",
                    "Country": "United States"
                }
            ]
        ]
    },
    "Email Addresses": {
        "list": [
            [
                {
                    "Email": "jssmith@gmail.com"
                },
                {
                    "Email": "j.s.smith@yahoo.com"
                },
                {
                    "Email": "joe.steven.smith@aol.com"
                },
                {
                    "Email": "joe.s.smith@outlook.com"
```

```
                        },
                        {
                            "Email": "the.smithster@yahoo.com"
                        }
                    ]
                ]
            }
        }
    }
}
```

Full JSON

```
[
    {
        "name": "Customer Information",
        "type": "customer",
        "showAsList": false,
        "queryResults": [],
        "subgroups": [
            {
                "name": "Basic Information",
                "type": null,
                "showAsList": false,
                "queryResults": [
                    {
                        "rows": [
                            {
                                "attributes": [
                                    {
                                        "name": "Customer ID",
                                        "value": "12344"
                                    },
                                    {
                                        "name": "First Name",
                                        "value": "Joe"
                                    },
                                    {
                                        "name": "Middle Name",
                                        "value": "Steven"
                                    },
                                    {
                                        "name": "LastName",
                                        "value": "Smith"
                                    },
                                    {
                                        "name": "Division",
                                        "value": "Division 444"
                                    },
                                    {
                                        "name": "Group",
                                        "value": "Group 5555"
                                    }
                                ]
                            },
                            {
                                "attributes": [
                                    {
```

```
                                    "name": "Customer ID",
                                    "value": "12344"
                                },
                                {
                                    "name": "First Name",
                                    "value": "Joseph"
                                },
                                {
                                    "name": "Middle Name",
                                    "value": "Steven"
                                },
                                {
                                    "name": "LastName",
                                    "value": "Smith"
                                },
                                {
                                    "name": "Division",
                                    "value": "Legacy Division 89-444"
                                },
                                {
                                    "name": "Group",
                                    "value": "Legacy Group 76-5555"
                                }
                            ]
                        }
                    ],
                    "rowLimitReached": false,
                    "maxRowLimit": 5
                }
            ],
            "subgroups": [
                {
                    "name": "Phone Numbers",
                    "type": null,
                    "showAsList": true,
                    "queryResults": [
                        {
                            "rows": [
                                {
                                    "attributes": [
                                        {
                                            "name": "Home Phone",
                                            "value": "123-123-1234"
                                        },
                                        {
                                            "name": "Mobile Phone",
                                            "value": "123-123-1234"
                                        }
                                    ]
                                }
                            ],
                            "rowLimitReached": false,
                            "maxRowLimit": 5
                        }
                    ],                          "subgroups":
[]                  },                      {                       "name":
"Addresses",                            "type": null,
"showAsList": true,                             "queryResults":
[                           {                               "rows":
[                                {                                          "at
tributes":
```

```
[                                                    {
       "name": "Address Line 1",
"value": "123 Stoney Lake
Road"                                                    },
        {                                                       "name": "Address Line
2",                                                       "value": "Apartment
2C30"                                                    },
        {                                                       "name":
"City",                                                      "value":
"Toledo"                                                    },
         {                                                         "name":
"State",                                                     "value":
"Ohio"                                                   },
         {                                                        "name": "Postal
Code",                                                    "value":
"85225"                                                   },
          {                                                       "name":
"Country",                                                   "value": "United
States"                                                  }
     ]                                              },
{                                                   "attributes":
[                                                       {
       "name": "Address Line 1",
                              "value": "444 Hill Trail
Road"                                                    },
        {                                                       "name": "Address Line
2",                                                       "value":
null                                                    },
       {                                                       "name":
"City",                                                      "value":
"Cleveland"                                                 },
              {                                                        "name":
"State",                                                     "value":
"Ohio"                                                   },
         {                                                        "name": "Postal
Code",                                                    "value":
"44444"                                                   },
          {                                                       "name":
"Country",                                                   "value": "United
States"                                                  }
     ]                                              },
{                                                   "attributes":
[                                                       {
       "name": "Address Line 1",
"value": "123 Lyndale
Avenue"                                                  },
         {                                                       "name": "Address Line
2",                                                       "value": "Apartment
5B"                                                   },
      {                                                       "name":
"City",                                                      "value":
"Minneapolis"                                               },
                {                                                       "name":
"State",                                                     "value":
"Minnesota"                                                 },
              {                                                         "name": "Postal
Code",                                                    "value":
"554333"                                                  },
           {                                                       "name":
"Country",                                                   "value": "United
States"                                                  }
```

```
    ]                                   }                                   ],
                            "rowLimitReached":
false,                                   "maxRowLimit":
5                            }                          ],
"subgroups": []                      },
{                         "name": "Email Addresses",
"type": null,                        "showAsList": true,
"queryResults":
[                            {                                  "rows":
[                                    {                                        "at
tributes":
[                                              {
             "name": "Email",
"value":
"jssmith@gmail.com"                                             }
                        ]                                     },
                  {                                        "attributes":
[                                              {
             "name": "Email",
"value":
"j.s.smith@yahoo.com"                                           }
                          ]                                   },
                    {                                       "attributes":
[
                {                                                  "name":
"Email",                                              "value":
"joe.steven.smith@aol.com"                                        }
                                ]                                  },
                          {                                       "attributes":
[                                              {
             "name": "Email",
"value":
"joe.s.smith@outlook.com"                                         }
                                ]                                 },
                          {                                      "attributes":
[                                              {
             "name": "Email",
"value":
"the.smithster@yahoo.com"                                         }
                                ]                                 }
                  ],                                  "rowLimitReached":
true,                                "maxRowLimit":
5                            }                          ],
"subgroups": []                    }                ]            }        ]    }]
```

Human Readable HTML

Customer Information

Basic Information

Customer ID	First Name	Middle Name	LastName	Division	Group
12345	Joe	Steven	Smith	Division 555	Group 8888
12345	Joseph	Steven	Smith	Legacy Division 89-555	Legacy Group 76-8888

Phone Numbers

Home Phone	Mobile Phone
123-123-1234	123-123-1234

Addresses

Address Line 1	Address Line 2	City	State	Postal Code	Country
123 Stoney Lake Road	Apartment 2C30	Toledo	Ohio	85225	United States
444 Hill Trail Road		Cleveland	Ohio	44444	United States
123 Lyndale Avenue	Apartment 5B	Minneapolis	Minnesota	554333	United States

Email Addresses

Email
jssmith@gmail.com
j.s.smith@yahoo.com
joe.steven.smith@aol.com
joe.s.smith@outlook.com
the.smithster@yahoo.com

Error Payloads

For Bad Request and Precondition Failure Errors (400, 412)

```
{
    "errors": [
        "Invalid value for query parameter, jsonFormat. Expecting 'concise' or 'full'
but received 'saf'."
    ]
}
```

For Internal Server Errors (500):

```
{
    "errors": [
        "ORA-123:  SQL not properly terminated"
    ],
    "stackTrace": [
```

```
            "sun.reflect.NativeConstructorAccessorImpl.newInstance0(Native Method)",
               ::
        ]
    }
```