Oracle® Retail Analytics and Planning

Security Guide

Release 24.1.201.0

F96001-01

April 2024

Oracle Retail Analytics and Planning Security Guide, Release 24.1.201.0

F96001-01

Contents

Send Us Your Comments

Oracle Retail Analytics and Planning Security Guide

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 RAP and RAP applications.

Audience

This document is intended to provide an overview of the security features of the RAP Platform and applications built upon it. It contains a set of best practices for administrators, developers, and system integrators who perform the following functions:

- Work with customers to configure and deploy RAP applications.
- Perform RAP Administration tasks such as user management, permissions, and system limits.

This document is not intended to describe in detail the processes of deploying and maintaining an RAP application. It is assumed that the readers have a general knowledge of administering the underlying technologies and applications.

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 Help Center (docs.oracle.com)

Oracle Retail product documentation is also available on the following Web site:

https://docs.oracle.com/en/industries/retail/index.html

(Data Model documents can be obtained 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

Retail Analytics and Planning Cloud Services Architecture

Retail Analytics and Planning (RAP) is a suite of applications deployed on Oracle's Cloud Infrastructure (OCI). The applications are deployed in a highly available, horizontally scalable architecture. These cloud services use Oracle Cloud Infrastructure Identity and Access Management (OCI IAM)) as an identity provider (IdP). Information about logical, physical, and data architecture in this document focuses on how this architecture supports security.

Architecture Overview

Most customer access to the RAP services is through the public web tier, which uses HTTPS/1.2 TLS encryption. The web tier contains the perimeter network services that protect the applications from the internet at large. All traffic from the web tier continues to the Web Tier Security Server that provides authentication (AuthN) and authorization (AuthZ) services, which in turn use the customer's Oracle IdP service within their OCI tenancy.

Further information about OCI IAM is available in the Oracle Retail Identity Management for OCI IAM Startup Guide.

The RAP applications are deployed within a managed Kubernetes cluster. Scheduling of batch processes is provided by Job Orchestration and Scheduling (JOS). Reporting is provided by a common Oracle Analytics Server (OAS) instance which can connect to the underlying RAP schemas.

The underlying database for RAP applications is provided by the OCI Autonomous Data Warehouse. Each RAP customer instance has an instance of OCI ADW, shared across RAP application schemas.

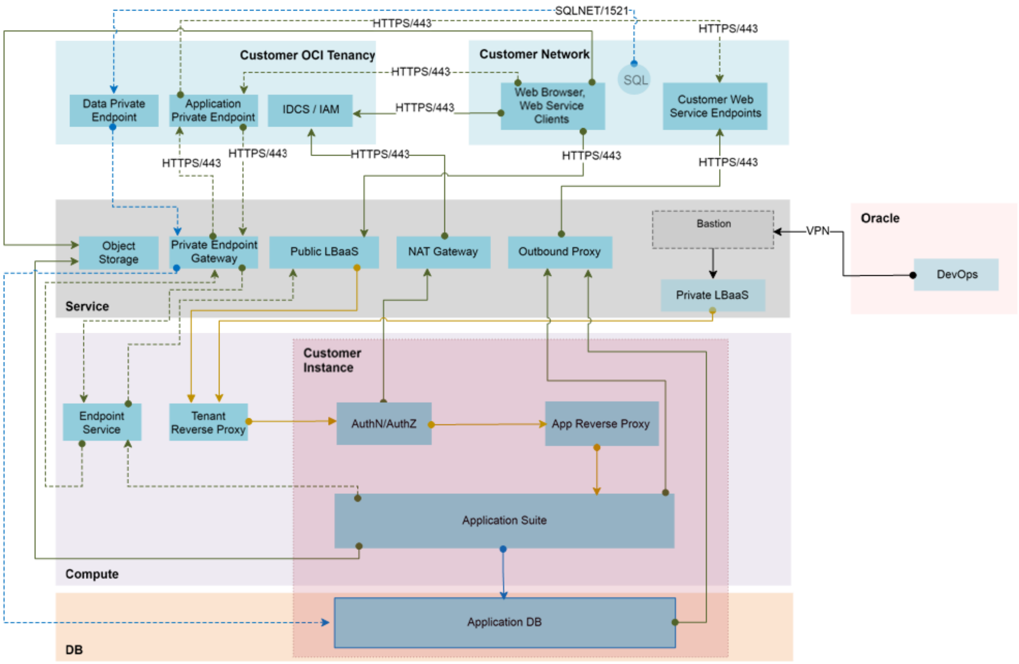
Transparent data encryption (TDE) is automatically set within ADW during provisioning. All tablespaces are encrypted. When data is otherwise stored at rest, it is encrypted using AES-256.

RAP applications primarily integrate with external business systems using files through a service-based upload to OCI Object Storage. All files are scanned by an anti-virus and anti-malware service. Other integration points are provided by RAP Innovation Workbench, using Oracle Restful Data Services (ORDS).

When RAP is integrated with Oracle Retail Merchandising Cloud Service (version 24 onwards) it is integrated through OCI GoldenGate.

RAP authenticates all REST services using OAuth2.0 through IdP. As a common authentication pattern is used, web service users are subject to the same security controls as application users. All service calls are recorded in the application security logs.

Application Data Flow



RAP services are deployed within a managed Kubernetes cluster, providing isolation for each customer instance. Each tier of the infrastructure is isolated by OCI Virtual Cloud Network (VCN) traffic ingress/egress lists.

Application traffic from a customer's network can ingress either through the public internet, or through an Application Private Endpoint within their own OCI tenancy. In either case, the traffic is encrypted. The traffic is routed to the customer's instance where authentication and authorization is verified against their IdP before reaching the relevant RAP service.

When file movement to or from OCI Object Storage is required, a time-limited Pre-authenticated Request (PAR) URL is issued subject to OAuth2.0 validation.

Typically, only HTTPS services are available to customers. Optionally, a customer can subscribe to the Data Private Endpoint service – this provides direct, encrypted SQL*Net access to the Innovation Workbench schema, but only to their OCI tenancy.

Oracle Application Management Services has limited access to the underlying application tiers to allow for service administration, deployment, and troubleshooting. This access is tightly controlled and granted to only a small number of Oracle employees as described in Oracle's Cloud Hosting and Delivery Policies.

2 Responsibilities

As retailers migrate to the cloud, they must consider how the cloud, and more specifically Software-As-A-Service (SaaS), will impact their privacy, security, and compliance efforts. As the cloud service provider, Oracle Retail works together with customers to meet cloud security objectives.

Retailer Responsibilities

At a high level, retailers are responsible for:

- Understanding Oracle's security policies
- Implementing their own corporate policies via Oracle tools
- Creating and administering users via Oracle tools
- Ensuring data quality and enforcing end-user devices security controls, so that antivirus, malware, and other malicious code checks are performed on data and files before uploading data
- Ensuring that end-user devices meet the minimum security requirements
- Generating public/private key pairs as requested by Oracle Retail

To securely implement Retail Analytics & Planning applications, retailers and their implementation partners should read this document to understand Oracle's security policies. This document summarizes information and contains links to many other Oracle documents.

Oracle Responsibilities

As the cloud service provider, at the highest level Oracle Retail is responsible for:

- Building secure software
- Provisioning and managing secure environments
- Protecting the retailer's data

Retail Analytics & Planning applications fulfill their responsibilities by a combination of corporate level development practices and cloud delivery policies. Sections in this document will describe this information in great detail later in this document.

Security Category Definitions

To discuss Retail Analytics & Planning Cloud Services SaaS security, it helps to define and categorize the many aspects of security. For the purposes of this document, we discuss the following categories of SaaS security:

- Secure Product Engineering
- Secure Deployment
- Secure Management

- Assessment and Audit

Secure Product Engineering

Oracle builds secure software through a rigorous set of formal, always evolving security standards and practices known as Oracle Software Security Assurance (OSSA). OSSA encompasses every phase of the product development lifecycle.

More information about OSSA can be found at:

`https://www.oracle.com/corporate/security-practices/assurance/`

The cornerstones of OSSA are Secure Coding Standards and Security Analysis and Testing. Secure Coding Standards include both general use cases and language-specific security practices. More information about these practices can be found at:

`https://www.oracle.com/corporate/security-practices/assurance/development/`

Security Analysis and Testing includes product-specific functional security testing and both static and dynamic analysis of the code base. Static Analysis is performed through tools including both internal Oracle tools and HP's Fortify. Dynamic Analysis focuses on APIs and endpoints, using techniques like fuzzing to test interfaces and protocols.

`https://www.oracle.com/corporate/security-practices/assurance/development/analysis-testing.html`

Secure Deployment

Secure deployment refers to the security of the infrastructure used to deploy the SaaS application. Key issues in secure deployment include Physical Safeguards, Network Security, Infrastructure Security and Data Security.

Physical Safeguards

Retail Analytics & Planning Cloud Services are deployed through Oracle Cloud Infrastructure datacenters. Access to Oracle Cloud data centers requires special authorization that is monitored and audited. The premises are monitored by CCTV, with entrances protected by physical barriers and security guards. Governance controls are in place to minimize the resources that are able to access systems. Physical security safeguards are further detailed in Oracle's Cloud Hosting and Delivery Policies.

http://www.oracle.com/us/corporate/contracts/ocloud-hosting-delivery-policies-3089853.pdf

Network Security

The Oracle Cloud network is isolated from the Oracle Corporate Network. Customer instances are separated down to the VLAN level.

Infrastructure Security

The security of the underlying infrastructure used to deploy Retail Analytics & Planning Cloud Services is regularly hardened. Critical patch updates are applied on a regular schedule. Oracle maintains a running list of critical patch updates and security alerts. Per Oracle's Cloud Hosting and Delivery Policies, these updates are applied to all Oracle SaaS systems.

https://www.oracle.com/technetwork/topics/security/alerts-086861.html

Before our Cloud Services deploy code to SaaS, Oracle's Global Information Security team performs penetration testing on the cloud service. This penetration testing and remediation prevents software or infrastructure issues in production systems.

https://www.oracle.com/corporate/security-practices/assurance/development/ethical-hacking.html

Data Security

Retail Analytics & Planning Cloud Services uses a number of strategies and policies to ensure the retailer's data is fully secured.

- **Data Design** – Our applications avoid storing personal data unless required. Where PII data exists in a system, Data Minimization, Right to Access, and Right to Forget services exist to support data privacy standards.
- **Storage** - Our applications use encrypted tablespaces to store sensitive data.
- **Transit** - All data is encrypted in transit; Retail SaaS uses TLS for secure transport of data, as documented in Oracle's Cloud Hosting and Delivery policy:

  `https://www.oracle.com/assets/ocloud-hosting-delivery-policies-3089853.pdf`

Our cloud services also implement data filtering so that users see the data stripes relevant to their own jobs, as detailed later in this document.

Secure Management

Oracle Cloud Services manage SaaS based on a well-documented set of security-focused Standard Operating Procedures (SOPs). The SOPs provide direction and describe activities and tasks undertaken by Oracle personnel when delivering services to customers. SOPs are managed centrally and are available to authorized personnel through Oracle's intranet on a need-to-know basis.

All network devices, servers, operating systems, applications, and databases underlying our Cloud Services are configured and maintain auditing and logging. All logs are forwarded to a Security Information and Event Management (SIEM) system. The SIEM is managed by the Security Engineering team and is monitored 24*7 by the GBU Security Operations team. The SIEM is configured to alert the GBU Security Operations team regarding any conditions deemed to be potentially suspicious, for further investigation. Access given to review logs is restricted to a subset of security administrators and security operations personnel only.

Assessment and Audit

Oracle Cloud meets all ISO/IEC 27002 Codes of Practice for Information Security Controls. Third Party Audit Reports and letters of compliance for Oracle Cloud Services are periodically published.

3

Retail Predictive Application Server Cloud Edition Security Features

Overview

The Oracle Retail Predictive Application Server Cloud Edition (RPASCE) is a platform that provides a set of common components used by a number of applications (solutions). For these solutions, RPASCE provides the infrastructure needed to store, process, and produce information based on data input by the retailer.

This guide discusses security considerations pertaining to the end user maintenance of an RPASCE Server application and the users of an RPASCE application.

Terminology

The following section provides a brief introduction to RPASCE and its terminology.

RPASCE Concepts

This section describes RPASCE concepts.

- **RPASCE**: A platform that provides a foundation to run solutions used for retail planning. RPASCE provides those solutions with a common interface based on wizards, templates, workbooks, and batch processes.
- **RPASCE Solution**: An application running on top of RPASCE that provides solutions for retail activities such financial planning or forecasting demand.
- **Planning Data Schema:** The Planning Data Schema (PDS) is a schema created within the Oracle Database containing the tables that contain application metadata, a customer's planning data, and the procedures used to access and manipulate that data. The majority of user interactions with customer information are performed in workspaces; however, data load and other offline batch activities operate directly on the PDS.
- **Workspaces:** Users perform application tasks inside workspaces. A workspace is a sandbox built by pulling data from the PDS; it supports the operations a user requires to perform a given task within the application. Once a task is complete, the changes made within the workspace sandbox can be applied to update the information contained within the PDS.

RPASCE Applications

Users access an RPASCE solution through the RPASCE client, a web-based client.

In addition, Administrators can access the **Configuration Tools**. This is a Windows-based set of utilities used to configure and maintain a RPASCE solution.

Secure Deployment

Secure deployment refers to the security of the infrastructure used to deploy the SaaS application. Key issues in secure deployment include Physical Safeguards, Network Security, Infrastructure Security, and Data Security.

RPASCE applications are deployed via Oracle Cloud Infrastructure datacenters. Access to Oracle Cloud data centers requires special authorization that is monitored and audited. The premises are monitored by CCTV, with entrances protected by physical barriers and security guards. Governance controls are in place to minimize the resources that are able to access systems. Physical security safeguards are further detailed in Oracle's Cloud Hosting and Delivery Policies.

http://www.oracle.com/us/corporate/contracts/ocloud-hosting-delivery-policies-3089853.pdf

The above referenced document also contains information about practices concerning Network, Infrastructure, and Data Security for applications deployed in the Oracle Cloud Infrastructure datacenters.

General Security Principles

The following principles are fundamental to using any application securely.

Keep Software Up to Date

One of the principles of good security practice is to keep all software versions and patches up to date. Since all interactions with RPASCE applications occur through a web browser (either through the RPASCE Client or through the Object Store web interface), these must be maintained at their latest release level to ensure the security of customer information.

Follow the Principle of Least Privilege

The principle of least privilege states that users must be given the lowest privilege level required to perform their jobs. Overly ambitious granting of responsibilities, roles, grants, and so on, especially early on in an organization's life cycle when people are few and work must be done quickly, often leaves a system wide open for abuse. User privileges must be reviewed periodically to determine relevance to current job responsibilities.

Monitor System Activity

System security stands on three legs: good security protocols, proper system configuration, and system monitoring. Auditing and reviewing audit records address this third requirement. Each component within a system has some degree of monitoring capability. Follow the audit advice in this document and regularly monitor audit records.

Keep Up to Date on Latest Security Information

Oracle continually improves its software and documentation. Check this note yearly for revisions.

Client Tier Security

This chapter discusses security for the RPASCE Client.

Factors Affecting Security

The factors affecting security within the RPASCE Client are Authentication and Authorization.

Authentication

It is a requirement that user names and passwords for RPASCE users must be created in an Oracle Cloud Infrastructure Identity and Access Management (OCI IAM) instance. RPASCE Client uses perimeter authentication. The Oracle software product, Web Tier Security Service (WTSS), is used to field all HTTP requests. WTSS redirects the browser to an OCI IAM login page if a request lacks the OCI IAM session cookie.

Users authenticated by OCI IAM and assigned the authentication role for the RPASCE application will be granted access to the RPASCE application with a set of application permissions based upon the application roles granted them in OCI IAM

Users can be added through the OCI IAM Admin Console and can be added in bulk using a CSV file. For more information on using OCI IAM, see the Oracle Identity Cloud Service online help at `https://docs.oracle.com/en-us/iaas/Content/Identity/home.htm`.

User accounts will be automatically created in the RPASCE application when a new user logs in for the first time if an account does not exist. However, this is not recommended, as there are some administrative tasks required to fully set up a new user account, so those tasks should be performed before they login. For AIF and RI applications, users do not exist in those systems independently of OCI IAM, all authentication is managed through direct communications between OCI IAM and the application client and there are no administrative steps in AIF/RI to separately configure user access.

To address the additional steps in Planning applications, the Online Administrative Tools (OAT) contain tasks to facilitate the addition of new users after they have been created in OCI IAM but prior to their first time logging into the system. Information about these tasks can be found in the *Oracle Retail Predictive Application Server Cloud Edition Administration Guide*.

Authorization

Authorization refers to the selective provisioning of data and the functional access to different classes of users.

Authorization Within an RPASCE UI Application

Once a user has been granted both the application authentication role and the administrator role in IAM, that user can log into the system as an administrative user.

The administrative user can log in to the application and see the functional groups within the application. Various application features such as workbook templates can be assigned to these functional groups. (We call this RPASCE capability “Security Administration”). He or she can then log in to IAM Console and assign users to *the like-named IAM groups*.

This will allow users to access those application features that he or she has been authorized to access, based on the memberships of functional groups (indirectly through their membership of the like-named IAM groups), and the access control established in the Security Administration process.

For more information on users, user groups, and granting privileges, see Compute Tier Security.

Authorization for Retail Home Metric Tiles

For each RPASCE solution, there is a Retail Home configuration file. A tile contains several “tile states” (accessed from the small round buttons at the bottom of the tile. This file defines the metadata for the Retail Home metric tiles, including the assignment of OCI IAM groups to tile states.

The user will only see those tile states for which he or she has been authorized, by way of their IAM group memberships.

Password Policies

The customer administrator user can define password complexity and rotation rules. All application user maintenance is performed by Customer Administrators via OCI IAM.

The following guidelines are useful.

- Automatic lock out occurs after a certain number of failed login attempts.
- Password expiration may be enabled.
- The password reuse time can be set.

Browser Security

Update the browser when new versions are released; they often include new security features.

Check the browser for built-in safety features.

Setting Policy For Unattended PC Sessions

Others may try to access an unattended workstation while the user is still logged into the system. Users must never leave their workstation unattended while logged into the system because it makes the system accessible to others. Organizations must set a corporate policy for handling unattended PC sessions. Users must use the password-locked screen savers feature on all PCs.

Compute Tier Security

This chapter contains information on security activities carried out in the Compute Tier.

User and Group Management

Users of RPASCE applications are created and managed within OCI IAM. RPASCE allows administrators to create user groups within the application that correspond to roles defined in OCI IAM. When a user logs into the RPASCE application, the application will check to see if that user belongs to any roles that correspond to a group defined in the application and assign the user the privileges granted to those groups.

User groups are typically assigned based on a common business role such as Planners in order to facilitate managing the authorization settings at the group level. However, users will also have certain roles that server non-business purposes, as described "Non-Business Roles".

When a user is added, either through the Synch Users task or when a user logs into the application for the first time, a position is created for the user in the metadata dimension User. Similarly, when a group is added, that group is assigned a position in the metadata dimension Group.

User Life Cycle

As users enter the OCI IAM system, they can be granted both the application authorization role and one or more of the business roles. Once granted appropriate roles, users will be able to access the RPASCE application with the corresponding access rights. However, some additional administrative setup is required for a user accessing the system for the first time.

Position security is not role-based and is not managed through OCI IAM. It is therefore necessary for an administrative user to set the position access rights for a new user in order for that user to be able to interact with data in the application. Additionally, new users will not have access to the Dashboard in the RPASCE client until a dashboard workbook has been prepared for them. When a new user first logs in, that user will receive a message from the application to contact their administrator to complete these setup processes.

During the lifetime of a user within the system, any changes to that user's responsibilities can be accommodated by updating the set of roles assigned to the user in OCI IAM. If the set of roles possessed by a user change, those changes will automatically result in a change to that user's access rights when that user next logs in that reflect the access rights of the new set of roles they possess.

When a user should no longer be granted access to the application, the application authorization role can be revoked in OCI IAM or, if appropriate, the user can be dropped from OCI IAM entirely. No subsequent login attempts by that user will succeed, and they will no longer have access to the application and its data.

When a user is removed from the system, the system may continue to hold resources created by and for that user in the form of workbooks, saved formatting, and so on. To allow these resources to be reclaimed, a pair of administrative utilities can be run. First, the Sync Users from OCI IAM utility will query OCI IAM for the set of users authorized for the application. Any users who are no longer authorized for the application because of role changes, or as a result of being removed from OCI IAM, will be flagged within the application as expired.

A second utility, Manage Users, can then be executed. This utility will drop all workbooks and reclaim all other resources associated with the expired users and will purge them from the system. The purpose of this two-step process is to safeguard against the loss of user information as a result of accident. Purging a user from the system and deleting all that user's work may result in a significant loss of time and effort. As such, it is recommended that the two utilities be scheduled to run separately in order to provide a chance for error remediation prior to the irrevocable deletion of user data.

Non-Business Roles

Two special roles are associated with an RPASCE application using Atomic User Management (AUM): the first is the authentication role and the second is the application administration role. These roles are do not relate to the business processes of the application, but are instead used to manage access to the application and determine which users have administrative privileges within the application.

The names for these roles are not fixed and will vary between RPASCE applications and between the different environments (production, stage, and so on) making up a customer instance. For new customers, the role names will be provided during the provisioning and deployment process. For existing customers migrating to AUM, they are created as a part of the migration process.

Application Authorization Role

In order for users authenticated by OCI IAM to be allowed access to the RPASCE application, they must belong to the application authorization role. Users who do not possess the authentication role will not be allowed access to the application, even if they possess one or more of the roles defined and granted rights in the application. In this way, a single set of business-related roles can be managed across multiple RPASCE application instances but access can still be limited for an application instance to a subset of all users. It can be useful, for example, to share user roles between a stage and a production environment but grant access to the stage environment to a subset of users.

Application Administrative Role

Under the AUM model, users are no longer granted administrative privileges through the setting of the admin flag within the user management templates. Instead, users possessing the administrative role for a given application instance will be granted admin rights for that application instance. These rights can then be managed by assigning a user the administrative role or revoking that role, with the changes taking effect automatically when the user next accesses the RPASCE application.

Deactivating User Accounts

User accounts can be marked as deactivated by the administrator in the OCI IAM console. This prevents the user from logging on with the RPASCE Client. The account remains locked until the administrator re-activates the user.

Roles Created in OCI IAM

A number of roles are created within OCI IAM as part of the provisioning process that are used to support the RPASCE Cloud subscriptions. Some of these roles are created to support user operations and must be assigned to users in the system. Other roles are created within OCI IAM to support the integration of the RPASCE systems with other systems and components within the Cloud environment. These roles are used by the internal processes of the system and, in general, do not need to be assigned to users of the system.

Information on the roles created for the various components of an Oracle Retail cloud subscription can be found in the *Oracle Retail Identity Management for OCI IAM*. Readers are encouraged to review not only the sections pertaining to the cloud services for which they have subscriptions but also the sections detailing role information for common components that are a part of every subscription, such as Retail Home, Process Orchestration and Monitoring, and Retail AI Foundation Cloud Service.

Authorization

This section deals with authorizing access. The workbook template security and position-level security are managed in the security administration workbook through various Workbook Template Rights and Position Security views. See the “Security Administration Workbook” section in the *Oracle Retail Predictive Application Server Cloud Edition Administration Guide* for more information.

Workbook Template Security

Workbook template access can be granted as Full Access or Read-Only. Full Access enables the user to build, open, modify, and commit the workbook. Read-Only access allows the user to open and view the workbook only. Workbook access is automatically granted to the user who builds a workbook, and the workbook can be shared by that user with other users in the system who are authorized to view that workbook and the data contained within it. The user who receives access to a shared workbook has the same access granted to the user on the workbook template. That is, Full Access users can modify and commit the shared workbook while Read-Only users can only view the workbook.

For guidance on assigning permissions to workbooks by role and group, see the Implementation Considerations chapter, section "Security," of each RPASCE Application's Implementation Guide. All recommendations in the guides are for the GA solution. If a customer chooses to customize permissions, keep in mind that the Principle of Least Privilege: only provide users with sufficient permissions to do their job and nothing more.

> **Note:**
>
> A user must have access to the workbook template in order to access the workbook, even if the workbook has world or group access rights.

A user’s workbook template access rights can be inherited from the user’s groups. If any group a user belongs to has Full Access to a workbook template, the user also has Full Access. If one or more of the user’s groups have Read-Only access and the others have no access, the user inherits the Read-Only access which is then combined with their own access rights to become the final access rights. That is, if the user themselves has no access rights, the heritance grants Read-Only rights. If the user themselves already has Read-Only or Full Access rights, the heritance has no effects.

By default, the group template rights inheritance is enabled. It can be turned on/off on a user-by-user basis through the “Manage Users” OAT task.

Users with administrator status automatically have access to all workbook templates. By default, administrators have access to all workbooks that are saved with world access. If a workbook is saved with group access, administrators can only access the workbook if they are members of the default user group of the user who saved the workbook.

Another aspect of workbook security is the ability to set limits for the number of workbooks that a user can have saved at any given time. Limits can be set for a user per template, for a user group per template, or for a template for all users. The limits are evaluated in the above order, which means that a limit defined at user-template overrides any values defined at group-template or template. If the above limits are not defined, the default value is one billion.

The limits are checked when the workbook build process is initiated. When the limit is reached, an error message displays informing the user that the workbook build process cannot complete because the limit has been reached. The message also lets the user know what that limit is. The wizard process then terminates.

Administrative users have full access to all workbook templates, regardless of the access rights that other administrative users may assign to them in the Security workbook. The administrative user can build the Security workbook to change the access right back, so the nominal assignment does not matter for administrative users.

Non-administrative users do not have access to the Security template and User Administration template groups even if the administrator inadvertently assigns them access rights.

Position Level Security

Position Level Security allows access control for dimensions on a position-by-position basis. This capability is completely optional. If position level security is not explicitly defined and configured, all users in an application have access to all positions in all hierarchies. After the position level security is defined, access to a position can be granted or denied for individual users, users in a group, or for all users.

Position level security can be defined at levels at or above base (such as class in the product dimension) in any dimension other than calendar. As positions are added at a level lower in the dimension than where the position level security is maintained, access to those positions is automatically granted if a user has access to the parent position.

For example, if security is maintained at the subclass level, users are automatically granted access to all the SKUs in a given subclass if they have access to that subclass. This includes those that were added after security was established.

Exactly one level in each dimension can be defined as the security level for the dimension. If a security level is defined for the dimension, all levels in the dimension have position level security enabled, but position security is set at or above the designated level. For example, if the class level is designated as the security level, an administrator can maintain access to positions in the class level or at any level above class.

To specify the security level for a dimension, the application designer must update the configuration and either rebuild or patch the application. After a security level is defined for a dimension, all users in the application default to having access to all positions in any level in the dimension. Additionally, users automatically have access to newly added positions. Views in the Security Administration workbook are used to control position access for individual users, user groups, or all users (referred to as world or default access). Three views are provided in this workbook for each dimension with a defined security level. The default view controls access to positions for all users (for instance, Prod Security Default); one view controls access to positions by user group (for instance, Prod Security Group); and the last view controls access to positions by individual users (for instance, Prod Security User).

Access must be granted at all levels for a user to have access to a position. This means that a position must have a value of true at the levels default/world, group, and user. The table below demonstrates how access is granted or denied based on all combinations of settings.

In the table, security is set by Position. Denied = False and Granted = True. Based on the settings for User, User Group, and World, the user is either granted or denied access, as shown in the Resulting Access column.

> **Note:**
>
> A user can belong to multiple user groups (primary and other groups of the user), The user is granted access on the user group level as long as one of their groups is granted.

Table 3-1 Granting Access

User	User Group	World	Resulting Access
Denied	Denied	Denied	Denied
Denied	Denied	Granted	Denied
Denied	Granted	Denied	Denied
Granted	Denied	Denied	Denied
Denied	Granted	Granted	Denied
Granted	Denied	Granted	Denied
Granted	Granted	Denied	Denied
Granted	Granted	Granted	Granted

Position-level security is used when a user selects positions in the wizard process before building a workbook. Only positions to which a user has access are available for selection in the 2-tree, which are then included in the build of the workbook.

Setting Proper Resource Limits

This section specifies how to set resource limits. The views described in the subsections below - WorkbookTemplate Limits, Max Domain Session Limit, Max User Session Limit and Dimension Modification Rights are the views present in the security administration workbook. These resource limits can also be viewed in the PDS Explorer. See the “Security Administration Workbook” and “PDS Explorer” sections in the *Oracle Retail Predictive Application Server Cloud Edition Administration Guide* for more information.

WorkbookTemplate Limit Views

The Workbook Template Limit views are used to limit the number of workbooks that the user can have saved. Limits can be set for a user per template, for a user group per template, or for a template for all users. The limits are evaluated in the above order, which means a limit defined in a user-template overrides any values defined at group-template or template. If the above limits are not defined, the default value is one billion, but it is not displayed in the workbook.

The limits are checked when the user begins the workbook build process. If the limit has been reached, an error message appears that informs the user that the workbook build process cannot completed because the limit has been reached. The wizard process then terminates.

Max Domain Session Limit View

The Max Domain Session Limit view is used to limit the number of user sessions that can be attached to a single application by all users of that application. The limit is set at the application level. This limit is checked during user login. If the limit has been reached, an error message appears to inform the user that the login has failed because this limit has been reached.

Max User Session Limit View

The Max User Session Limit view is used to limit the number of concurrent user sessions that can be attached to a single application by the same user at the same time. The limit is set per user so that the administrator can control the maximum number of concurrent sessions that are allowed for an individual user.

This limit is checked during user login. If the limit has been reached, an error message appears to inform the user that the login has failed because this limit has been reached.

Dimension Modification Rights View

The Dimension Modification Rights view allows the administrator to determine which user-defined dimensions, if any, a user can modify. Its purpose is to provide a filtered list of user-defined dimensions to be shown on the dimension selection wizard page of the Hierarchy Maintenance template. The view contains a check box for each available user and dimension combination. A check mark in the cell indicates that the user is permitted to modify the specified dimension.

Managing Sensitive Data

While RPASCE can be configured to store any type of data, it is designed to be used with sales history, inventory, and other business-related information with low security requirements. It is not intended to be used with any sensitive data, such as personally identifiable information or credit card information. It does not have any mechanisms to protect this data, such as encryption, and therefore must not be used in this manner.

Online Administration Tools

In order to be able to run and schedule administrative tasks in a cloud environment where the administrator has no access to the back-end servers, RPASCE Online Administration Tools provide an interface that allows authorized users to launch back-end processes from the RPASCE UI. It also provides a dashboard-like interface for the administrator to monitor the status of the tasks whose requests have been submitted.

Planning Data Schema Security

This chapter of the security guide covers Planning Data Schema (PDS) creation and maintenance.

Configuration Management

The process of RPASCE application configuration can be performed by an RPASCE administrator, an application expert, a consultant or a third-party implementation team. In all cases, the process of creating or modifying the configuration of an RPASCE application is performed using a stand-alone Java application known as the RPASCE Configuration Tools.

The RPASCE Configuration Tools work with an XML representation of the content of an application known as the application configuration. Using the Configuration Tools, an application configuration can be inspected and modified. The configuration is then used as an input to the application deployment process, which creates and modifies RPASCE PDS.

Because the RPASCE Configuration Tools are supported only on the Windows platform, there is a need to manage the transfer of that configuration between the system being used for the configuration and the system on which the RPASCE PDS will be built and maintained.

Although the configuration itself does not contain any sensitive information, it does contain information about the meta-data of the application and the processes used to maintain and modify that application data. As such, it is prudent to secure the representation of the application contained within the configuration.

To that end, there are three areas in which the security of a configuration can be discussed. These areas are:

- Upon the system on which the configuration process is performed.
- Upon the system on which the RPASCE PDS is deployed.
- Upon the transfer of the configuration between the above two systems.

In each of these areas, precautions can be taken to maintain the integrity and confidentiality of the information represented within the configuration.

Securing the Configuration System

Because the RPASCE Configuration Tools do not interact directly with the RPASCE PDS, they cannot be used to inspect or modify PDS information. However, because the configuration describes the information in the PDS and the processes used to maintain and modify that information, it should be viewed as proprietary information. As such it should be subjected to the appropriate considerations employed to protect other proprietary information present on user systems.

The considerations include safeguarding the physical security of systems that store proprietary information, encryption of storage devices for these systems and limiting risk of exposure through controlling access to the information contained within the configuration.

Securing the Deployment System

Once uploaded to the OCI environment, the configuration is protected by the same safeguards present to secure all application resources residing within the host environment. No additional protections are required.

Securing the Transfer of Configurations

Configuration is performed on one or more users' individual systems. In order to build or update an RPASCE PDS with that configuration, it is necessary to transfer the configuration to the system upon which the PDS will be deployed. This transfer is accomplished using the

Oracle Cloud Infrastructure Object Storage service. OCI Object Storage provides a reliable and secure method of moving information into and out of RPASCE application instances.

Information on use of OCI Object Storage in conjunction with RPASCE applications can be found in the *Oracle Retail Predictive Application Cloud Service Implementation Guide.* Information on OCI Object Storage itself, including information on security best practices, can be found here:

`https://docs.oracle.com/en-us/iaas/Content/Object/Concepts/objectstorageoverview.htm`

Dynamic Position Maintenance

The creation of positions within the dimensions of an RPASCE application is a process that is performed by loading the position information from flat files or through the integration of an RPASCE application with other Oracle Retail applications. However, the business processes performed by some RPASCE applications make deferring position creation and management to an off-line process unacceptable.

Dynamic Position Maintenance (DPM) allows user to create and manage certain positions in an online process while working within a workbook. Users can create positions within constraints based on application security settings and the workbook configuration and enforced by the RPASCE Server instance.

Users can also modify and or delete existing positions created through DPM operations within constraints based on application security settings and the workbook configuration and enforced by the RPASCE Server instance.

Users are not allowed to modify or delete positions which the application's security settings do not grant them access to; they may also not modify positions of levels and dimensions not allowed by the configuration of the workbook in which they are working. Finally, formal positions managed through data load or integration with other Oracle Retail applications cannot by modified in any circumstances through DPM operations.

Enabling DPM functionality within a workbook involves the following process:

1. Configurator must enable DPM on particular dimensions in the application.
2. Configurator must enable DPM on the specific workbook template.
3. Configurator or system administrator must ensure there is enough space to accommodate the volume of DPM position given by the bitsize of the dimension.
4. Administrator must give WRITE permission on that workbook template to the user. Any users granted WRITE permission to the workbook template can create DPM positions.

When a user creates DPM positions, they are treated as temporary positions; flat file operations and integration with other Oracle Retail applications do not update these positions. Online Administration Tools (OAT) contains a Manage Informal Positions task that can be used for maintaining the informal positions of any levels in the application. This task can convert positions from formal to informal or from informal to formal. It can also remove informal positions, create informal positions in bulk, and copy data slices between positions in measures.

RPASCE Maintenance

PDS maintenance is a periodic operation that must be performed by the administrator. Many of these operations can improve overall performance of data access operations. This can result in fewer contention issues which improves accessibility.

In addition, many of these operations involve removing data from the PDS when that data is no longer needed by the operations being performed by the PDS. This periodic cleansing serves to remove data from the system and addresses the need to retire data as a part of the data management life cycle. Some of the PDS maintenance tasks that can be performed periodically are:

Purging Unused and Inactive Hierarchy Positions

All measure data within the PDS is stored in either scalar or dimensional measures. As positions are introduced to the hierarchies of the PDS, these positions become available for the storage of measure data. When a position is no longer required by the PDS, it can be purged. This hierarchy purging will result in the measure data associated with the retired positions being cleaned from the PDS.

The purging process is performed via the Load Dimension Data OAT task, which has a purgeAge option that can be used for purging unused hierarchy positions.

Clean Up Old Workbooks

It is possible to list all the workbooks in the application and determine which ones are old. "Managing Workbooks Using wbmgr", found in the *Oracle Retail Predictive Application Server Administration Guide*, describes using the option Manage Workspaces to list all the workbooks in the application. From this output, all the old and obsolete workbooks can be found. These old workbooks can be removed using the same Managing Workbooks task. Removing only the workbook and keeping the associated segment can help to rebuild the workbook later using the same selections if required. Segments without their workbooks do not require much space. Alternately, the entire segment can be removed using the Managing Segments task.

Clean Up Old Administration Tasks

The tasks in the OAT dashboard grow over time and take up valuable system resources. It is recommended that an Admin user periodically purge unused admin tasks. The task to perform the purge operation is described in "Purge Tasks from Task Status Dashboard Task", found in the *Oracle Retail Predictive Application Server Administration Guide*.

Performance Diagnostic Tool

The performance diagnostic tool contains valuable options to analyze system resources. See "Analyzing Workbook Performance", found in the *Oracle Retail Predictive Application Server Administration Guide*, regarding how to efficiently find workbooks that can be cleaned up.

RPASCE Integration

This chapter covers integrating information across multiple RPASCE applications.

Data and Metadata Integration

The client/server interactions of RPASCE define how users may access the system but are not effective for larger scale modification of the data of the system. To allow for these operations, RPASCE supports bulk data load and export operations. Even though RPASCE supports file-based integration, we recommend that the customer load data through importer. These files are provided to and retrieved from the system through the use of an Object Storage Cloud Service server that is part of the provisioned environment.

Integrating User Information

RPASCE applications rely on OCI IAM for user authentication and authorization. Users are created, deleted, and assigned roles within OCI IAM. Those users who have been granted the authentication role for an RPASCE application are given access to the application with the set of application privileges granted by the user roles that user has been granted in OCI IAM. Additionally, users granted the administrator role in OCI IAM are also allowed access to the administrative functions of the RPASCE application and granted super user rights that supersede the rights of the application roles they may have.

As a result, the integration of user information between multiple RPASCE applications or between an RPASCE application and another Oracle Retail application is entirely a matter of role membership within OCI IAM. Users granted the authorization role for multiple RPASCE applications will have access to those applications, with application privileges determined by the application roles for those applications.

Object Store

RPASCE uses object storage for interacting with incoming and outgoing files in the cloud. Object storage is available from Oracle for cloud customers and is documented at the link below.`https://docs.oracle.com/en-us/iaas/Content/Object/Concepts/objectstorageoverview.htm`

Interface Configuration File

Data from all pre-defined planning interfaces to external systems such as RMFCS (Oracle Retail Merchandising Foundation Cloud Service) or internal systems like Retail Insight/Science is pulled through importers from RAP Data Exchange (RDX) schema. Any data that is going from Planning to external systems can also be exported through importers from the RDX schema. Though interface tables in the RDX schema will not change quite often, as defined by the interface contracts between respective applications, the planning/forecast application that is implemented on PDS supports extensibility and enterprise edition (EE) configuration. Therefore, importers and exporters must be configurable, since dimensions and fact names can be different for different customers. To provide for the configurability of importers and exports, the `interface.cfg` file (interface configuration file) is used. It is a free-form text file similar to the batch control file, and contains the mapping of dimension/facts in PDS to columns mapped to external tables for each interface.

Both importers and exporters are commonly referred as interfaces within PDS; each interface has a unique interface ID. Interfaces are classified as one of three types: dimension importers, data importers, or data exporters. Customer can create or modify entries only for the available list of interfaces. They can configure the interface to match and pull the required dimension/fact data per the dimension/fact names configured with in their application when those interfaces are executed in batch. For general availability applications, the pre-configured `interface.cfg` file is readily available, and customer can customize the file for any required extensibility changes, similar to an EE customer.

For more information about uploading the custom `interface.cfg` file, see the Load Interface Mappings task in the *Oracle Retail Predictive Application Cloud Edition Administration Guide*.

Use of ORDS in Conjunction with the Planning Data Schema

Customers can make use of Oracle ReSTful Data Services (ORDS) to invoke web services that supply the data stored in the Planning Data Schema. Several standard web service endpoints are provided, and it is possible to create additional endpoints to supplement those provided.

The access provided to ORDS by the Planning Data Schema allows only for reading data; there is no capability for modification of the data contained within the Planning Data Schema. The endpoints provided are intended for use by external systems that connect to ORDS through the use of system accounts.

In order to connect to the Planning Data Schema through ORDS, the account representing the external process must exist within the OCI IAM instance associated with the application. Additionally, that account must belong to the group RPAS_ORDS_GROUP. All unauthenticated access requests and any requests made by a user who is not a member of the RPAS_ORDS_GROUP will be denied.

Creation of Additional Service Endpoints

In order to create additional service endpoints, it is necessary for a user to gain limited administrative access to ORDS. First, the user must exist within the OCI IAM instance and belong to the RPAS_ORDS_GROUP role. Second, a service request must be created to give that user access to the ORDS administrative UI.

Once access is granted, authorized users will be able to access parts of the ORDS administrative UI that allow the creation and registration of endpoints. However, they will not have access to other administrative functions (such as security policy management) of the ORDS instance.

4

AI Foundation Security Features

Technology-Specific Security Features

Oracle Retail AI Foundation Cloud Services uses several common technologies and services and provides specific security features as described below.

Web Services

The web services in Oracle Retail AI Foundation Cloud Services are stateless, so state is not stored or managed. Pagination such as the batch size of data and parameters such as export data time, product, location, and so on are used to manage payload size and to handle session timeouts only.

SOAP

Oracle Retail AI Foundation Cloud Services has an Outbound Interface to push Customer Segment and its members to Oracle Retail Customer Engagement (ORCE). This interface supports the following security features:

- Message authentication is enabled in ORCE, and the Oracle Retail AI Foundation Cloud Services message includes authentication information in the HTTP header for the message. This authentication information is specific to ORCE and is stored in the Credential Stores. The Credential Stores are created or updated from the Data Management task, which is enabled for an Administrator. The Base64 encoding tool is used to encode the authorization key that is sent as part of the Message HTTP Header request. The Credential Stores use APIs that applications can use to create, read, update, and manage credentials securely and mark code as being "privileged", thus affecting subsequent access determinations.
- Oracle Retail AI Foundation Cloud Services provides configuration to set up proxy settings for both HTTP and HTTPS.
- XML sent as part of the message relies on marshalling and un-marshalling to and from Java Objects generated using the WSDL/Schema exposed through ORCE. This ensure that the XML generated is well formed and valid. It is the responsibility of ORCE to convert XML; Oracle Retail AI Foundation Cloud Services does not perform any XML Conversion. There are no concerns regarding XXE and XEE.

REST

Oracle Retail AI Foundation Cloud Services has an Outbound Interface to export data (GET request), and it uses REST to expose data. These web services are REST-based; it is assumed that callers are familiar with the basic REST principles (such as the usage of HTTP verbs). AC and ASO export web services can serve as a means of obtaining incremental update data from a specified point in time. All services support the query parameter `contentType` and the HTTP header Content-Type, with supported values `application/json` and `application/xml`. The query parameter takes precedence; if no content type is supplied, then `application/json` serves as the default. Basic authentication is used, so you may use any client software that supports it. Authorization is done for ADF-LDAP (OID) mapped roles, and only administrator roles are used (that is, the calling user must be in a duty that is mapped to the defined administrator roles). JSON/XML parsing is done using standard JAXB request parameters that are validated before data is fetched.

ORDS

The following three security features are provided:

- **Single Sign On (SSO)** - AIF integration with ORDS supports SSO, using ORDS-provided authentication schemes called the HTTP Header Variable. User credential verification is performed by OCI IAM, which passes the user's name to Oracle Application Express using an HTTP header variable such as `IDCS REMOTE_USER`. While setting up the scheme in ORDS, the logout URL is also configured by Oracle.
- **Schema used in the ORDS Workspace** - AIF integration with ORDS includes defining a new schema called Retail Workspace Schema (`RTLWSP01`) in the ORDS workspace. This is provided to the retailer, and in turn is associated with the AIF product schema. The retailer may not create other workspaces; they are expected to use only the provided one in conjunction with AI Foundation applications.
- **Declarative REST API** – AIF integration with ORDS also provides the retailer with a declarative way to create new service endpoints in the system. Access to such endpoints are enabled through oAuth2.0. This REST API request is authorized using the OCI IAM client credential grants type, where the retailer requests an access code from OCI IAM and passes the token in subsequent calls to access data.

Authentication and Authorization

For authorization, Oracle Retail AI Foundation Cloud Services modules have been built with role-based access. Access to application user interface components is done by assigning application roles. Application roles are defined as part of the application and deployed as part of the installation process. Application roles are mapped to enterprise roles during the initial environment provisioning. For Oracle Cloud Infrastructure Identity and Access Management (OCI IAM) users, the enterprise roles are available from the user interface and are managed in the same way as other security groups. Refer to the *Retail Identity Management Startup Guide for OCI IAM* for details on all available enterprise roles for each AIF application and module.

Analytics Client Security

The Oracle Analytics Server (OAS) client used for BI reporting and data analysis has additional client-side security measures, mainly for the Retail Insights (RI) application usage.

Authentication for OAS is automatically sourced from OCI IAM; however, the application also uses authorization roles, which are defined within the products themselves (such as Retail Insights). These application roles are linked to OCI IAM user groups, but do not share the same naming structure. For example, the OCI IAM group `swef98w4f4nf009-SalesInsights_JOB` appears simply as the “Sales Insights” group within OAS. The relationship between OCI IAM groups and OAS application roles is covered in more detail in the *Identity Management for OCI IAM Startup Guide*.

OAS also provides object-level security within the application UI. Example objects are reports, datasets, dashboards, and connections. Object-level security is managed from the OAS user interface by right-clicking an object and inspecting it for access and sharing permissions. More details can be found in the Oracle Analytics Server User Guides.

Retail Insights includes metadata security in OAS, which restricts the metrics and attributes a user has access to based on their OCI IAM group assignments. For example, the Sales folder of metrics is not available to all users; it requires one of a set list of OCI IAM groups to be assigned first. The mapping between application roles and metadata objects is provided in the Metrics and Attributes Catalog (MAC) document in My Oracle Support (Doc ID 2539848.1).

Hierarchy Position Security

In the Retail Insights (RI) and AI Foundation (AIF) applications, position-level security is managed using database tables and associated flat file loads. Unlike RPAS application position security, the data provided through this process is more like data filtering; it is not a guaranteed limit to the user's access in all cases. The data-level security mapping is provided though interface files: `RAF_SEC_USER.dat`, `RAF_SEC_GROUP.dat`, `RAF_SEC_USER_GROUP.dat`, `RAF_FILTER_GROUP_MERCH.dat`, and `RAF_FILTER_GROUP_ORG.dat`. If you are accessing the tables from APEX, then the table name is the same as the filename without the extension (such as `RAF_SEC_USER`). The security tables exist in multiple database schemas, so specify the application user when querying or writing to the tables (`RADM01` or `RASE01` user schemas for RI and AIF, respectively).

- `RAF_SEC_USER.dat` contains the `USER_ID` (LDAP ID) for any user who has data access limits defined
- `RAF_SEC_GROUP.dat` contains the `GROUP_ID` to group together multiple sets of users having the same access levels.
- `RAF_SEC_USER_GROUP.dat` contains the mapping between `USER_ID` and `GROUP_ID`. Individual users are not assigned data permissions, it is done with security groups.
- `RAF_FILTER_GROUP_MERCH.dat` contains the access mapping between any merchandise hierarchy level, Merch ID on that level, and the GROUP IDs. This mapping defines what the group is allowed to access. Anything not included is restricted.
- `RAF_FILTER_GROUP_ORG.dat` contains the access mapping between Organization hierarchy level, Org ID on that level, and the GROUP IDs. This mapping defines what the group is allowed to access. Anything not included is restricted.

If a user is not mapped into any of these files, then they have full access to the data in RI and AIF applications. If a user runs a report in RI that is above the security level (such as a Division level report when the security settings are at Department level) then they will get all data from the database returned without restriction, as it is not possible to filter the report at levels above the security level. The data filtering does not apply to custom datasets built using DV, nor does it apply to queries run in Innovation Workbench. You are expected to limit the user's access to these tools if you do not want them to have unrestricted data access.

If you do not wish to use the files and want to populate the data from APEX instead, separate functionality is provided to do so. Refer to the “Extensibility” chapter of the *RAP Implementation Guide* for more details.