

Oracle® Retail Enterprise Inventory Cloud Service

Security Guide

Release 19.1

F32615-01

July 2020

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Value-Added Reseller (VAR) Language

Oracle Retail VAR Applications

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

- (i) the **MicroStrategy** Components developed and licensed by MicroStrategy Services Corporation (MicroStrategy) of McLean, Virginia to Oracle and imbedded in the MicroStrategy for Oracle Retail Data Warehouse and MicroStrategy for Oracle Retail Planning & Optimization applications.
- (ii) the **Wavelink** component developed and licensed by Wavelink Corporation (Wavelink) of Kirkland, Washington, to Oracle and imbedded in Oracle Retail Mobile Store Inventory Management.
- (iii) the software component known as **Access Via**™ licensed by Access Via of Seattle, Washington, and imbedded in Oracle Retail Signs and Oracle Retail Labels and Tags.
- (iv) the software component known as **Adobe Flex**™ licensed by Adobe Systems Incorporated of San Jose, California, and imbedded in Oracle Retail Promotion Planning & Optimization application.

You acknowledge and confirm that Oracle grants you use of only the object code of the VAR Applications. Oracle will not deliver source code to the VAR Applications to you. Notwithstanding any other term or condition of the agreement and this ordering document, you shall not cause or permit alteration of any VAR

Applications. For purposes of this section, "alteration" refers to all alterations, translations, upgrades, enhancements, customizations or modifications of all or any portion of the VAR Applications including all reconfigurations, reassembly or reverse assembly, re-engineering or reverse engineering and recompilations or reverse compilations of the VAR Applications or any derivatives of the VAR Applications. You acknowledge that it shall be a breach of the agreement to utilize the relationship, and/or confidential information of the VAR Applications for purposes of competitive discovery.

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

Contents

Send Us Your Comments	vii
Preface	ix
Audience	ix
Documentation Accessibility	ix
Related Documents	ix
Improved Process for Oracle Retail Documentation Corrections	ix
Oracle Retail Documentation at the Oracle Help Center	x
Conventions	x
1 Overview	
Business Overview	1-1
Multiple Products	1-3
Cloud Deployment	1-3
EICS Client	1-3
SOCS Mobile Client	1-3
Web Services	1-3
WTSS / IDCS	1-3
EICS Application Server(s)	1-3
OBIEE Server	1-3
SFTP Server	1-4
Oracle DB Server (DBaaS)	1-4
Client-Server Communication	1-4
Client Service Security	1-4
Web Service Security	1-4
2 Security Model	
Terminology	2-1
User Access to Functionality	2-2
Security Groups	2-2
Application Roles	2-4
Role Permissions Configuration	2-4
User Types with Security Groups and Application Roles	2-4
User Provisioning	2-5
User Access	2-6

Oracle Identity Cloud Service User and Group Management	2-6
---	-----

3 Application Security

EICS Application Security.....	3-1
Role Management	3-2
Assigning Stores to a User.....	3-2
Assigning Roles to a User.....	3-2
Mass Assigning Roles and Stores	3-3
Deleting an EICS User Profile	3-3
Importing a Batch of User Accounts	3-3
Bulk Group Membership Update (Optional)	3-4
Nightly Batch File Uploads	3-5
Adding Authorized Keys.....	3-5
Logging In to WinSCP.....	3-8
Uploading the Batch File.....	3-10
Export File Downloads.....	3-11
Web Services Security	3-11
Personal Data	3-11
Regulatory Compliance	3-11

Send Us Your Comments

Oracle Retail Enterprise Inventory Cloud Service Security Guide, Release 19.1

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 Help Center (OHC) website. 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 describes the security aspects for Oracle Retail Enterprise Inventory Cloud Service.

Audience

This document is intended for administrators.

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

For more information, see the following documents in the Oracle Retail Store Inventory Operations Cloud Services Release 19.1 documentation set:

- *Oracle Retail Store Inventory Operations Cloud Services Release Notes*
- *Oracle Retail Store Inventory Operations Cloud Services Implementation Guide*
- *Oracle Retail Enterprise Inventory Cloud Service User Guide*
- *Oracle Retail Enterprise Inventory Cloud Service Administration Guide*
- *Oracle Retail Store Operations Cloud Service User Guide*
- *Oracle Retail Store Operations Cloud Service Mobile Guide*

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 at the Oracle Help Center (OHC) website, 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 at the Oracle Help Center at the following URL:

<https://docs.oracle.com/en/industries/retail/index.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 F123456-02 is an updated version of a document with part number F123456-01.

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

Oracle Retail Documentation at the Oracle Help Center

Oracle Retail product documentation is available on the following website:

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

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

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	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.

Business Overview

EICS is a cloud service platform helping a retailer track discrete store and warehouse inventory across the enterprise. In return this information can be provided to downstream systems for Omni-Channel purposes or even general merchandising.

The platform comes with a PC-based administration layer developed in Oracle JET.

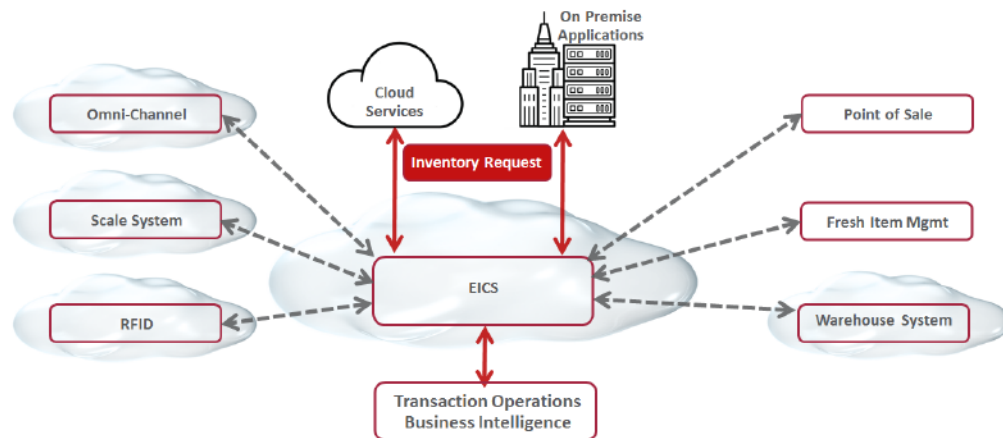
This administration layer allows:

- System and store business process configuration
- Setup of core data elements like reason codes, context values and tolerances for picking
- Configuration of printers
- Prioritizing the barcode parser
- Scheduling the batches and managing polling timers for the integration layer
- Management and scheduling of Product Groups to automate processes like stock counts
- Notification setup
- Extended Attributes setup and assignment to hierarchies
- Setup of server based translation values
- Printing reports
- Creation of roles and role user assignments

EICS leverages a host of APIs to allow a retailer to import and export data. The application it leverages is the Retail Integration Cloud Service (RICS), which consists of three integration methods:

- Retailer Integration Bus (RIB) for payload integration and continuous streaming between applications
- Retail Backbone Service (RSB) for web service integration to import, export and execute inventory business transactions
- Bulk Data Integration (BDI) is used to import start-up data

In addition to these integration tools, several batch processes also exist for operational bulk data processing.

Figure 1–1 EICS Platform

EICS does not have an operational transaction execution layer, and counts on the optional mobile UI of the Store Operations Cloud Services (SOCS) to execute store inventory transactions.

SOCS is a cloud service mobile UI which requires Enterprise Inventory Cloud Service (EICS) as a pre-requisite. It executes operational inventory transactions related to a store. The application itself is a fat client developed on Oracle's Mobile Application Platform (MAF).

The UI can be deployed on iOS, Android and Windows 10 mobile.

SOCS supports the following functions:

- Scanning of barcodes (GS1, VPN, item, container ID..) to identify a SKU or container
- Container, item and supplier lookup
- Inventory adjustment with appropriate reason codes
- Adhoc, unit, problem line and unit and amount Stock counts
- Creating, accepting, picking and rejecting transfer requests
- Shipping to another warehouse, store or external finisher
- Receiving from warehouse, store or external finisher
- Accepting Return to Vendor (RTV) request, creating RTVs and shipping to a vendor
- Direct Store Deliveries with Purchase order (PO), without PO and against an ASN
- In Store Replenishment from backroom to shop floor
- Management of inventory on shop floor and backroom
- Customer order Pick, pack and ship

Multiple Products

EICS (Enterprise Inventory Cloud Service) and SOCS (Store Operations Cloud Service) are two separately licensed products.

- EICS Browser Client
- EICS Web Services
- EICS Server Tier
- EICS Database tier with data access code, batches, reports

SOCS includes:

- Oracle MAF Client

In order to use SOCS, EICS needs to be deployed.

Cloud Deployment

EICS Client

Oracle Jet based browser application that allows the user to perform a wide range of administrative functions.

SOCS Mobile Client

The mobile client provides all the day-to-day transactional workflows within an Oracle Mobile Application Framework (MAF) platform. MAF is a hybrid-mobile platform that supports both iOS and Android devices. For more details, please see MAF Guide.

Web Services

There is no GUI for the SOAP web services APIs that are provided by EICS. These APIs allow customers to create or develop applications or add-ons that can replicate some or all of the steps of a transaction workflow.

WTSS / IDCS

WTSS: Web Traffic Security Service

IDCS: Identity Management Cloud Service is used to authenticate users.

EICS Application Server(s)

Server deployed as a J2EE application inside the WebLogic Application Server.

OBIEE Server

OBIEE / BIPublisher is used as reporting engine.

SFTP Server

The Secure File Transfer Protocol server is responsible for the moving of files from outside the internet firewall to within the internet firewall in a secure manner. This is used with File Storage Service.

Oracle DB Server (DBaaS)

Contains EICS schema. Uses JDBC to access data from the database.

WebLogic application server provides a connection pool to use database resources in an efficient fashion.

PL/SQL stored procedures are also used for high volume batch processing.

Client-Server Communication

Client(s) use ReST service calls to access the server.

External systems may use SOAP service calls to access the server.

All transactions are container managed.

Performance is sensitive to network latency (hence compression from client to server).

Client Service Security

The EICS Browser Client and SOCS MAF Client use REST services to communicate to the EICS server.

All service communication uses HTTPS with TLS for transport security.

These clients use either SSO authentication or OAUTH protocol.

Web Service Security

The EICS server provides and consumes SOAP web services, which are used for integration purposes with RIC (RSB).

For the cloud deployment the security policy A is supported, which uses a user name token policy with TLS.

See [Web Services Security](#) for more information.

Security Model

Terminology

This section defines Security Terms used.

Table 2–1 Security Terms

Term	Definition
Application Administrator	A customer application admin user who can perform application configurations via EICS admin screen.
Application Implementer	System implementer is user who implements the application.
Application Role	An application role is a collection of users and other application roles. Application roles are defined in applications and they are not necessarily known to a Java Container.
Customer Cloud Administrator	A delegated customer cloud user for customer cloud management tasks, for example create customer security admin user, and other users.
Customer Security Admin	A customer security admin user who can create customer users and assign application roles. Please note that sometimes this may not be setup as a separate user than application administrator.
Retail Home User	A user who can access EICS tile reports on Retail Home and navigate to related operational views in EICS from there.
Security Group	A collection of users and groups. These groups are defined in security store, and are known to java EE server container.
Store Manager	A user who performs store manager role.
Store User	A user who performs store operations with assigned role permissions.
System Operator	Will be used by Oracle cloud team for debug.
User	A user is an end-user accessing a service or application.

In addition to application users, integration users need to be setup based on integrated applications.

User Access to Functionality

Users of SIOCS have roles through which they gain access to functions and data.

Security implementation involves the management of:

- [Security Groups](#)
- [Application Roles](#)
- User creations
- Assigning security groups to corporate operational users
- Assigning application roles to store users

Security Groups

EICS comes with 9 groups used for special purpose access, which are managed through IDCS.

Admin

The group *sim_admin_users* is required for access to administration tasks, such as managing configuration settings or translations.

This group should only be assigned to system operators and administrators.

Batch

This group should only be assigned to system operators and batch administrators.

The group *sim_batch_users* is required for access to batch related tasks, such as job management or scheduling.

Global Store User

The group *sim_global_store_users* grants the user access to all store locations.

This group should only be assigned to system operators, and administrators or special users requiring access to all store locations.

Integration

The group *sim_integration_users* is required for accessing integration resources, such as web services.

This group should only be assigned to users designated for application integration, not those requiring access to the application UI.

Users that are only integrating with EICS are considered integration users, for example, the RIB injection user is a typical case of an integration user.

These users do not require access to the EICS client applications, and therefore do not require store assignments or role assignments (permissions).

MPS

The group *sim_mps_users* is required for access to MPS (message processing service) related tasks, such as staged message maintenance or work type management.

This group should only be assigned to system operators and MPS administrators.

Security

The group *sim_security_users* is required for access to security management tasks, such as role maintenance and user role/store assignments.

This group should only be assigned to system operators and security administrators.

Users accessing application UI features that are restricted by group access must also be granted the relevant permissions through role and store assignments.

A regular store user should not require any security group assignments for accessing the application UI.

System Operator

The group *sim_sysop_users* is required for access to restricted areas of the application, such as certain system configuration settings.

This group should only be assigned to system operators, which are typically the cloud operator.

Full Permission

The group *sim_full_permission_users* allows the user to gain access to all available permissions without any database role assignment.

This group should only be assigned to system operator and initial customer admin user.

Note: This full permissions group does not provide full data permission access. For performing administration operations on EICS, user should be assigned administer role in EICS application.

Retail Home

The group *sim_retail_home_users* is required for retail home application to successfully call EICS APIs to fetch tile report data.

This group should only be assigned to retail home users.

For pre-production deployment, EICS provides the set of nine security groups as mentioned above but with PREPROD appended to the group names for easy differentiation.

Security Group assignments are typically used for special purpose access such as integration or various administration tasks. Enterprise Groups are assigned to users through IDCS.

This table identifies predefined application security groups:

Table 2–2 Predefined Application Security Groups

Cloud Service or Options	Predefined Group
Admin Service	sim_admin_users
Security Service	sim_security_users
Message Processing Service	sim_mps_users
Batch Service	sim_batch_users
All store locations	sim_global_store_users
Perform application system configurations (both non-restricted and restricted)	sim_sysop_users

Table 2–2 (Cont.) Predefined Application Security Groups

Cloud Service or Options	Predefined Group
Initial user setup to login to EICS application	sim_full_permission_users
Retail Home Service	sim_retail_home_users

Application Roles

Application roles are a collection of permissions that are assigned to users for specific or all of their assigned stores. These permissions are used to control access to application functionality and data. Roles are created, managed, and assigned to users through the EICS security admin UI.

EICS has the following predefined application roles.

Table 2–3 Predefined Application Roles

Operations	Role
Admin permission role	ADMINISTRATOR
Store Manager permission role	MANAGER
Retail Home permission role	RETAIL HOME

Role Permissions Configuration

There are 350+ configuration settings that decide how users access functionality. For details, see the *Oracle Retail Enterprise Inventory Cloud Service Administration Guide - Configuration* chapter.

User Types with Security Groups and Application Roles

Table 2–4 User Types with Security Groups and Application Roles

Application User Type	Job Duties	Application Roles Assigned (User Role Assignment is via EICS Security Admin Console)	Security Enterprise Group Assigned (User Security Group Assignment is via Oracle IDCS)
Initial Application Admin User	To access EICS application and create other application admin and store users.	N/A	sim_admin_users sim_security_users sim_mps_users sim_batch_users sim_global_store_users sim_full_permission_users
Application Admin User	Perform all administration activities, setup other customer application store users and perform application configuration.	ADMINISTRATOR	sim_admin_users sim_security_users sim_mps_users sim_batch_users sim_global_store_users

Table 2–4 (Cont.) User Types with Security Groups and Application Roles

Application User Type	Job Duties	Application Roles Assigned (User Role Assignment is via EICS Security Admin Console)	Security Enterprise Group Assigned (User Security Group Assignment is via Oracle IDCS)
Store Users	Perform store operations in store using Mobile client.	Custom Defined Role with selected role permissions.	N/A
Integration Users	External system invokes EICS provided Integration Services. See Integration Implementation sections for additional details.	N/A	sim_integration_users
Retail Home User	Access EICS tiles on retail home and navigate to related operational views in EICS.	RETAIL HOME	sim_retail_home_users

User Provisioning

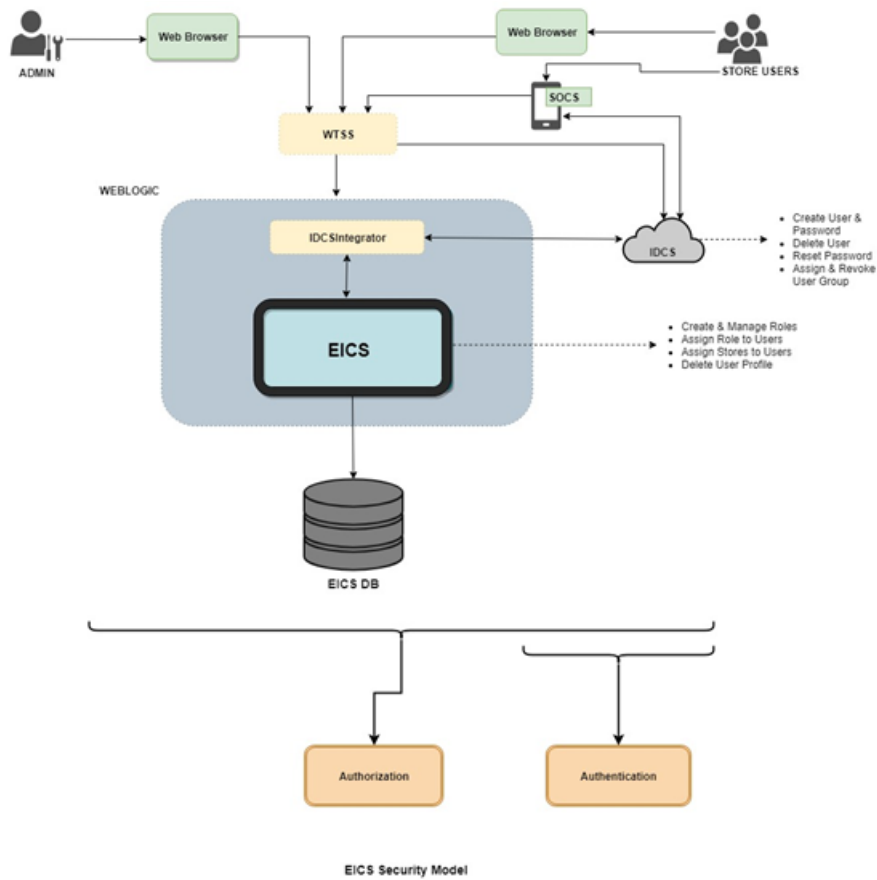
Before users can access the Oracle Retail Enterprise Inventory Cloud Service applications it is necessary to provision each user access to the system, and assign groups, stores, and roles to each user to control what functionality will be available to them. The access provisioning is done using Oracle Identity Cloud Service (IDCS) for initial customer admin user. This user can create or manage other user provisioning via IDCS and the EICS security admin UI.

Group assignments are typically used for special purpose access such as integration or various administration tasks. Groups are assigned to users through IDCS.

The application client uses store based sessions for performing business operations. Store assignments control the stores available for a user to login to. Users can be assigned access to specific stores through the EICS security admin UI.

Application roles are a collection of permissions that are assigned to users for specific or all of their assigned stores. These permissions are used to control access to application functionality and data. Roles are created, managed, and assigned to users through the EICS security admin UI.

Figure 2–1 EICS Security Model



User Access

It is recommended that users are granted the least level of access they require to perform their duties.

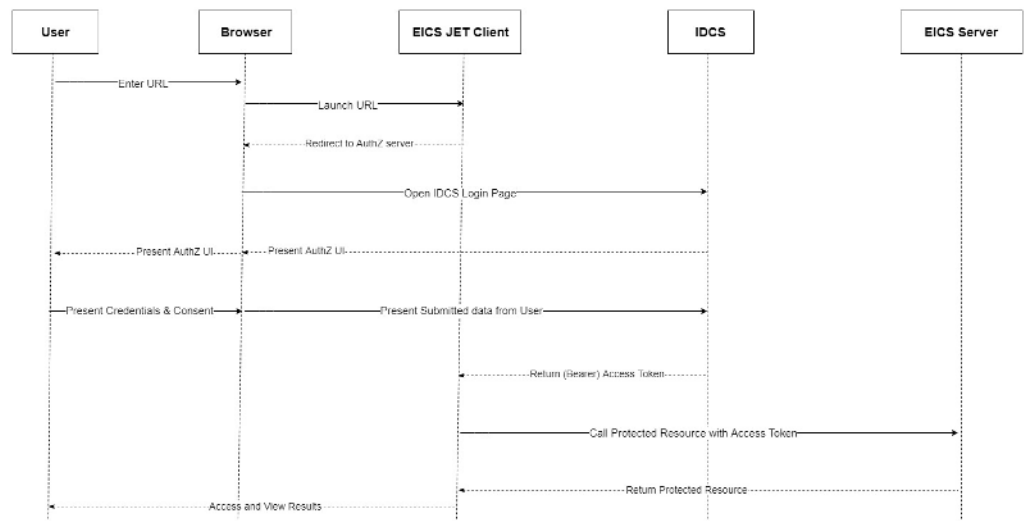
Users should not be reused or shared by multiple people or for multiple purposes.

For example, users created for integration purposes should not be granted access required for application UI usage.

Oracle Identity Cloud Service User and Group Management

Oracle Identity Cloud Service (IDCS) provides a fully integrated service that delivers all the core identity and access management capabilities through a multi-tenant Cloud platform.

Figure 2–2 IDCS User and Group Management



For instructions on managing users and groups in IDCS, follow the Manage Users and Groups IDCS document at the following URL:

<https://docs.oracle.com/en/cloud/paas/identity-cloud/index.html>

Application Security

For information on the administrative tasks, see the following sections:

- [EICS Application Security](#)
- [Role Management](#)
- [Assigning Stores to a User](#)
- [Assigning Roles to a User](#)
- [Mass Assigning Roles and Stores](#)
- [Deleting an EICS User Profile](#)
- [Importing a Batch of User Accounts](#)
- [Bulk Group Membership Update \(Optional\)](#)
- [Nightly Batch File Uploads](#)
- [Export File Downloads](#)
- [Web Services Security](#)
- [Personal Data](#)
- [Regulatory Compliance](#)

EICS Application Security

Users are required to have store access and permissions in order to use the EICS client applications.

For access to special areas, group assignment in IDCS is also required as mentioned in previous sections.

Users that are assigned the global store users group (*sim_global_store_users*) automatically have access to all store locations in EICS. Users that do not have global store access require store assignments, which are setup through the EICS security admin UI.

EICS implements fine grained permissions for controlling access to functionality and data. All users accessing the EICS client application must have valid role assignments in order to be granted access to permissions. Users are assigned roles through the EICS security admin UI.

Application roles are created and managed through the EICS security admin UI by assigning permissions to the role.

For detailed information regarding user and role management with the EICS security admin UI, please see the *Oracle Retail Enterprise Inventory Cloud Services User Guide*.

Role Management

1. Log into the EICS admin UI.
2. Navigate to Security \ Role Maintenance.
3. Click **Create New** or the name of an existing role.
4. For new roles, enter the name, description, type.
5. Assign permissions to the role using the table.
6. Click **Save** when changes are complete.

Assigning Stores to a User

1. Log into the EICS admin UI.
2. Navigate to Security \ User Assignment.
3. Locate the user in the table, using filters as needed.
4. Click on the username.
5. Click on the **Stores** tab.
6. Assign stores to the user using the table.
7. Click **Save** when changes are complete.

Assigning Roles to a User

1. Log into the EICS admin UI.
2. Navigate to Security \ User Assignment.
3. Locate the user in the table, using filters as needed.
4. Click on the username.
5. Click on the **Roles** tab.
6. Click **Create New** to assign roles to the user.
7. Select the store scope and store(s) for the role assignment(s).
8. Select the role(s) to assign.
9. Enter start and end dates if needed.
10. Click **Apply** to create the selected assignments.
11. Click **Save** when changes are complete.

Mass Assigning Roles and Stores

1. Log into the EICS admin UI.
2. Navigate to Security \ User Assignment.
3. Click **Import**.
4. Click **Download Template** on the **Import Data File** dialog.
5. Fill data in the downloaded template.
6. Drag and drop the filled template file or click to select the file.
7. Click **Import**.

Deleting an EICS User Profile

The EICS user profile will be automatically deleted through a scheduled batch job if the user is deleted in IDCS.

However, an EICS user profile can be manually deleted without deleting the user in IDCS. This should be done if the user no longer requires access to EICS, or if the same username is used for a new user before the batch job has executed.

The EICS User Assignment table displays users stored in IDCS as well as EICS user profile information, such as the create date and login date. These refer to the EICS user profile creation and client login, not IDCS user information.

Users with a create date have an existing EICS user profile, which can be deleted with the following steps.

1. Log into the EICS admin UI.
2. Navigate to Security \ User Assignment.
3. Locate the user in the table, using filters as needed.
4. Select the row(s) in the table.
5. Click **Delete Profile**.

Deleting an EICS user profile includes all store and role assignments for that user. It does not affect group assignments or other user information managed through IDCS.

If a user account needs to be deleted or all access disabled it is recommended to use IDCS to perform the user management.

If a user only needs access to certain stores or permissions within EICS removed then the EICS security admin UI should be used.

Importing a Batch of User Accounts

If you have batch of users that have to be created, the Oracle team can bulk load the users into the IDCS application. When users are bulk loaded, each initial password is set to the current password of a template user. The new users are required to change the password on their first login.

To request the creation of accounts by bulk loading:

1. Create a CSV file listing all users to create. Following is an example of this file.

```
#####
filename.csv
```

```
#####  
#####  
USR_LOGIN,USR_FIRST_NAME,USR_LAST_NAME,USR_EMAIL,ORG_NAME  
CE.ADMIN1,ce,admin1,CE.ADMIN1@oracle.com,Retail  
CE.ADMIN2,ce,admin2,CE.ADMIN2@oracle.com,Retail  
CE.ADMIN3,ce,admin3,CE.ADMIN3@oracle.com,Retail  
CE.ADMIN4,ce,admin4,CE.ADMIN4@oracle.com,Retail  
CE.ADMIN5,ce,admin5,CE.ADMIN5@oracle.com,Retail  
CE.ADMIN6,ce,admin6,CE.ADMIN6@oracle.com,Retail  
CE.ADMIN7,ce,admin7,CE.ADMIN7@oracle.com,Retail  
CE.ADMIN8,ce,admin8,CE.ADMIN8@oracle.com,Retail  
CE.ADMIN9,ce,admin9,CE.ADMIN9@oracle.com,Retail  
CE.ADMIN10,ce,admin10,CE.ADMIN10@oracle.com,Retail  
#####
```

2. Create or identify a user whose password will be used as the initial password for all created users.
3. Open an SR with Oracle Support and provide the CSV file and user from Steps 1 and 2.

Bulk Group Membership Update (Optional)

If a considerable number of users need to have roles to be assigned, the Oracle team can bulk update the role membership into the IDCS application.

To update the membership by bulk update:

1. Create a CSV file with the user role mapping. Note that the user name must be in upper case format. See the example below.
2. Open an SR with Oracle Support and provide the CSV file and user name from Step 1.

```
#####  
role.csv  
#####  
#####  
UGP_NAME,USR_LOGIN  
Role1,CE.ADMIN1  
Role2,CE.ADMIN1  
Role1,CE.ADMIN2  
Role3,CE.ADMIN3  
Role4,CE.ADMIN4  
Role5,CE.ADMIN5  
Role6,CE.ADMIN6  
Role7,CE.ADMIN7
```

Role8,CE.ADMIN8

Role2,CE.ADMIN8

Role2,CE.ADMIN9

#####

Note: If more than one role is to be attached to a particular user, add one more row with the role that the user is to have and the user name. Refer to the CE.ADMIN1 in the above example.

Nightly Batch File Uploads

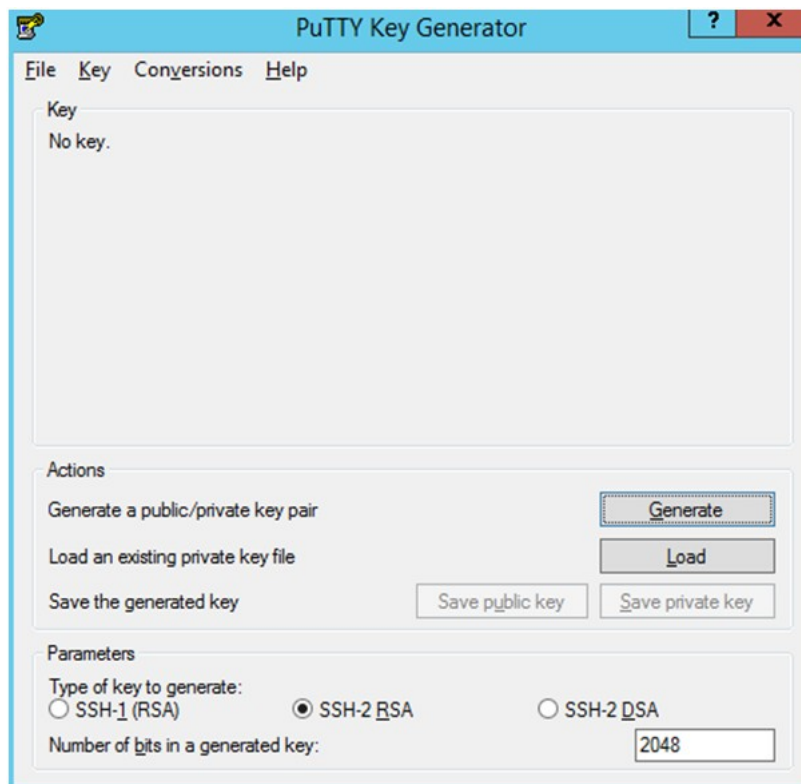
The following steps describe the file upload process.

The Private/Public keys must be generated and the Public key must be associated with your SFTP Account for the file uploads. The [Adding Authorized Keys](#) section describes the step-by-step method to generate the keys (2048 bit RSA Keys).

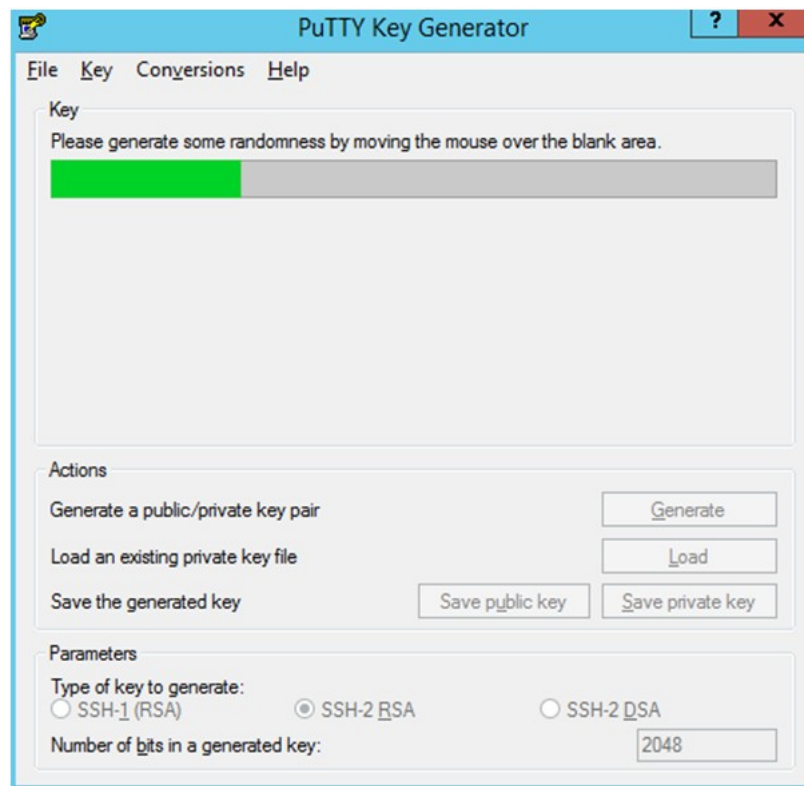
Adding Authorized Keys

The following process is used to generate a 2048 bit RSA key and to add the same to the SFTP server. This is done with the help of the WinSCP tool on Windows. However, the same can be done using ssh-keygen on Linux as well.

1. Launch WinSCP and select Tools\ Run PuttyGen.
2. Select **SSH-2 RSA** for the type of key to generate and enter 2048 for the number of bits in a generated key field. Click **Generate**.

Figure 3–1 Key Generator

3. Move the mouse over the blank space in the window until the key is generated. Moving the mouse over the blank space creates a random pattern which is used for key generation.

Figure 3–2 Key Generator Progress

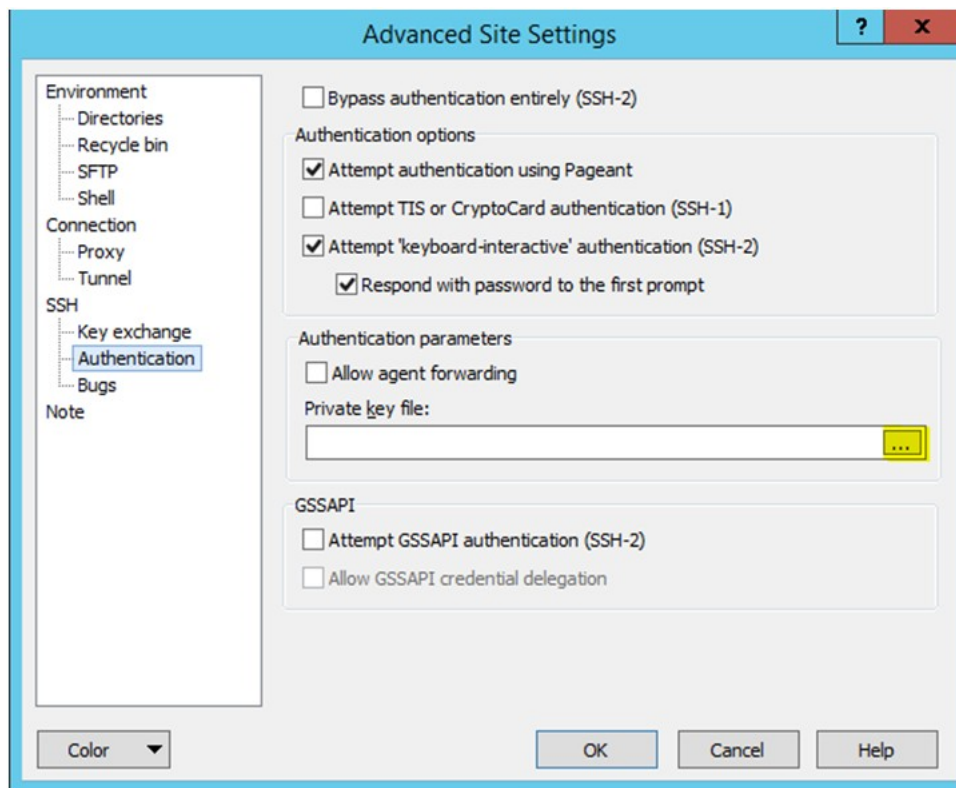
4. Once the key is generated, click **Save public key** to save the public key to a file.
5. Click **Save private key** to save the private key to a file. Confirm to save it with or without a passphrase.
6. Open an SR with Oracle Support, to associate the public key with your SFTP account (attach the key with the SR).

Logging In to WinSCP

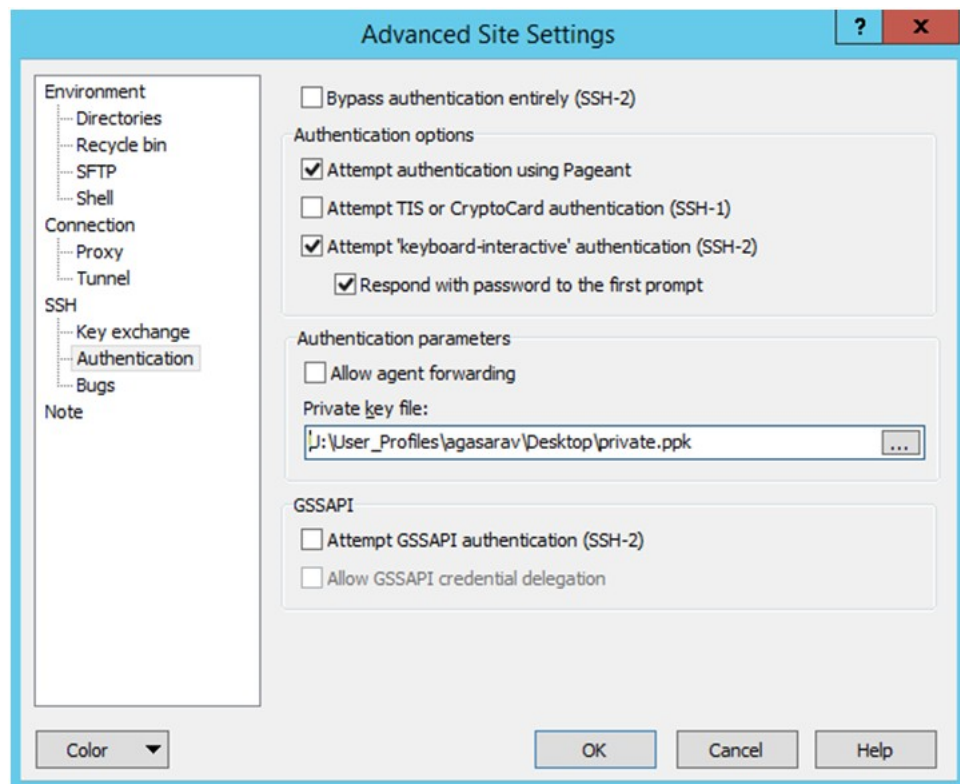
The upload steps use the private key generated in the [Adding Authorized Keys](#) section.

1. Launch WinSCP and connect to <SFTP Server> using port 22.
2. Enter the user name and click **Advanced**.
3. Click **Authentication**.
4. In the Private Key File field, click **Browse** and select the private key created in the [Adding Authorized Keys](#) section.

Figure 3–3 Advanced Site Settings Dialog



5. After loading the private key file, click **OK**.

Figure 3–4 Private Key File Loaded

6. Click **Login**. The window does not prompt for a password and logs in to the SFTP server. Provide a passphrase if one has been set up.

Note: Login can only be performed using the authorized keys. Login with username / password is not supported.

Uploading the Batch File

To upload the batch file:

1. Log in to WinSCP. Follow the steps in [Logging In to WinSCP](#).
2. Transfer the file to be copied (for example, test) to /<SFTP User>.

Figure 3–5 <SFTP User> Directory

Name	Type	Changed	Name	Changed
..	Parent directory	2/9/2017 4:36:54 PM	..	2/8/2017 2:49:59 PM
test.complete	COMPLETE File	11/28/2016 9:43:43 PM	COMMAND	2/9/2017 4:36:48 PM
test	File	11/28/2016 9:43:43 PM	COMPLETE	11/28/2016 9:43:43 PM
			test	11/28/2016 9:43:43 PM

3. Transfer an empty file <filename>.complete (for example, test.complete) to the directory /<SFTP User>.

Figure 3–6 Transferring Empty File

Name	Type	Changed	Name	Changed
..	Parent directory	2/9/2017	..	2/8/2017 2:49:59 PM
test.complete	COMPLETE File	11/28/2016	COMMAND	2/9/2017 4:36:48 PM
test	File	11/28/2016	COMPLETE	11/28/2016 9:43:43 PM
			test	11/28/2016 9:43:43 PM
			test.complete	11/28/2016 9:43:43 PM

4. If multiple files have to be transferred, copy all the files to /<SFTP_user>.

Figure 3–7 Transferring Multiple Files

Name	Type	Changed	Name	Changed
..	Parent directory	2/9/2017	..	2/8/2017 2:49:59 PM
test	File	11/28/2016	COMMAND	2/9/2017 4:36:48 PM
test1	File	11/28/2016	COMPLETE	11/28/2016 9:43:43 PM
test2	File	11/28/2016	test	11/28/2016 9:43:43 PM
			test1	11/28/2016 9:43:43 PM
			test2	11/28/2016 9:43:43 PM

5. Transfer all the corresponding <filename>.complete files to the /<SFTP_user> directory for the transfer to complete.

Figure 3–8 Transferring .complete Files

Name	Type	Changed	Name	Changed
..	Parent directory	2/9/2017	..	2/8/2017 2:49:59 PM
test.complete	COMPLETE File	11/28/2016	COMMAND	2/9/2017 4:36:48 PM
test1.complete	COMPLETE File	11/28/2016	COMPLETE	11/28/2016 9:43:43 PM
test2.complete	COMPLETE File	11/28/2016	test	11/28/2016 9:43:43 PM
			test.complete	11/28/2016 9:43:43 PM
			test1	11/28/2016 9:43:43 PM
			test1.complete	11/28/2016 9:43:43 PM
			test2	11/28/2016 9:43:43 PM
			test2.complete	11/28/2016 9:43:43 PM

Export File Downloads

To export file downloads:

1. Log in to WinSCP. Follow the steps in [Logging In to WinSCP](#).
2. Change the directory to /<SFTP User>/EXPORT.
3. Download all data files.

Web Services Security

The SOAP web services provided and consumed by EICS can be configured with security policies by the installer. These web services are designed to participate in Retail Service Backbone (RSB) flows which support two distinct Oracle WebLogic WS-Policy configurations. These are referred to as Policy A and Policy B.

Note: Cloud deployment supports only Policy A for SOAP web services.

On the provider side of the communication, Policy A and Policy B are configured using one or more Oracle WebLogic WS-Policy configurations defined in the xml files included in Oracle WebLogic:

- Policy A
 - Description: Message must be sent over SSL and requires authentication of a plain text UsernameToken.
 - Configuration: Wssp1.2-2007-Https-UsernameToken-Plain.xml
- Policy B
 - Description: Message body must be encrypted and signed, and requires authentication of an encrypted UsernameToken.
 - Configuration:
 - * Wssp1.2-2007-Wss1.1-UsernameTokenPlain-EncryptedKey-Basic128.xml
 - * Wssp1.2-2007-EncryptBody.xml
 - * Non-RSB Web ServicesWssp1.2-2007-SignBody.xml

Personal Data

Personal data is not stored within EICS.

Regulatory Compliance

EICS does not store any credit card data.

EICS does not store any HIPPA/health related data.

EICS does use Oracle TDE (Transparent Data Encryption) for portion of schema that stores users' passwords.