Oracle® Retail Enterprise Inventory Cloud Service

Security Guide

Release 19.7

F70120-01

January 2023

ORACLE

Oracle Retail Enterprise Inventory Cloud Service Security Guide, Release 19.7

F70120-01

Primary Author: Tracy Gunston

Contributing Author: Bipin Pradhan

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

3 Application Security

Send Us Your Comments

Oracle Retail Enterprise Inventory Cloud Service Security Guide, Release 19.7

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 19.7 documentation set:

- *Oracle Retail Store Inventory Operations Cloud Services Release Notes*
- *Oracle Retail Store Inventory Operations Cloud Services Implementation Guide*
- *Oracle Retail Store Inventory Operations Cloud Services Data Model*
- *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.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Overview

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:

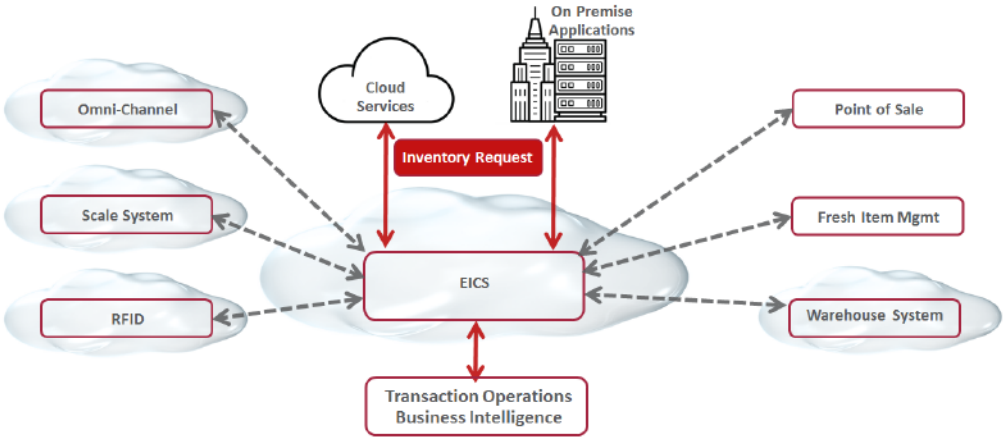
- System and store business process configuration
- Setup of core data elements like reason codes, context values and tolerances for picking
- Configuration of printers
- Prioritizing the barcode parser
- Scheduling the batches and managing polling timers for the integration layer
- Management and scheduling 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 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 the steps of a transaction workflow.

WTSS / IDCS or OCI IAM

WTSS: Web Traffic Security Service

Integration Cloud Services uses Oracle Identity Cloud Service (IDCS) as its identity provider (IDP) or Oracle Cloud Infrastructure Identity and Access Management (OCI IAM) as its identify provider (IDP).

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.

2

Security Model

This chapter covers the following sections:

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 SIOCS admin screen.
Application Implementer	System implementer is user who implements the application.
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.
IDCS or OCI IAM Application Role	IDCS or OCI IAM application roles are specific user entitlements that are created at the time of provisioning EICS application on IDCS or OCI IAM. Each IDCS or OCI IAM application role creates a security group.
Retail Home User	A user who can access SIOCS tile reports on Retail Home and navigate to related operational views in SIOCS from there.
Retail Home Service Admin User	A user who can access SIOCS tile reports and service admin screens in the Retail Home.
Security Group	A collection of users and groups. These groups are created automatically at the time of provisioning EICS application on IDCS or OCI IAM for each IDCS or OCI IAM application role. These groups are known to the Java EE server container.

Table 2–1 (Cont.) Security Terms

Term	Definition
SIOCS Application Role	SIOCS application role is a collection of users and other application roles. SIOCS Application roles are defined in the application and they are not necessarily known to a Java 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:

- IDCS or OCI IAM Application Roles
- SIOCS Application Roles
- User creations
- Assigning IDCS or OCI IAM Application Roles to corporate operational users
- Assigning SIOCS Application Roles to store users

IDCS or OCI IAM Application Roles

SIOCS comes with eleven IDCS or OCI IAM application roles used for special purpose access. These IDCS or OCI IAM application roles are defined inside EICS application on IDCS or OCI IAM.

All

The IDCS or OCI IAM application role *all_users* is required to access SIOCS.

This app role should be assigned to all users.

Admin

The IDCS or OCI IAM application role *admin_users* is required for access to administration tasks, such as managing configuration settings or translations.

The IDCS or OCI IAM application role should only be assigned to system operators and administrators.

Batch

This IDCS or OCI IAM application role should only be assigned to system operators and batch administrators.

The IDCS or OCI IAM application role *batch_users* is required for access to batch related tasks, such as job management or scheduling.

Full Permission

The IDCS or OCI IAM application role *full_permission_users* allows the user to gain access to all available permissions without any database role assignment.

The IDCS or OCI IAM application role should only be assigned to system operator and initial customer admin user.

> **Note:** This full permissions IDCS or OCI IAM application role does not provide full data permission access. For performing administration operations, user should be assigned ADMINISTRATOR SIOCS application role in SIOCS application.

Global Store User

The IDCS or OCI IAM application role *global_store_users* grants the user access to all store locations.

This IDCS or OCI IAM application role should only be assigned to system operators, and administrators or special users requiring access to all store locations.

Integration

The IDCS or OCI IAM application role *integration_users* is required for accessing integration resources, such as web services.

This IDCS or OCI IAM application role should only be assigned to users designated for application integration, not those requiring access to the application UI.

Users that are only integrating with SIOCS 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 SIOCS client applications, and therefore do not require store assignments or role assignments (permissions).

MPS

The IDCS or OCI IAM application role *mps_users* is required for access to MPS (message processing service) related tasks, such as staged message maintenance or work type management.

This IDCS or OCI IAM application role should only be assigned to system operators and MPS administrators.

PSRAF

The IDCS or OCI IAM application role *psraf_users* is required to access platform features, for example, Favorites.

This app role should be assigned to all users.

PSRAF Admin

The IDCS or OCI IAM application role *psraf_admin_users* is required to access platform admin features, for example, Subscription Services.

Any user that needs access to the PSRAF admin functionality in the Retail Home should be a member of this role. The user belonging to this role will be able to access all PSRAF endpoints.

Retail Home

The IDCS or OCI IAM application role *retail_home_users* is required for retail home application to successfully call EICS APIs to fetch tile report data.

This IDCS or OCI IAM application role should only be assigned to retail home users.

Security

The IDCS or OCI IAM application role *security_users* is required for access to security management tasks, such as role maintenance and user role/store assignments.

This IDCS or OCI IAM application role 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 this assignment for accessing the application UI.

System Operator

The IDCS or OCI IAM application role *sysop_users* is required for access to restricted areas of the application, such as certain system configuration settings.

This IDCS or OCI IAM application role should only be assigned to system operators, which are typically the cloud operator.

Note: The *sysop_users* IDCS or OCI IAM application role is for internal use by Oracle team only and should not be assigned to customer users.

These IDCS or OCI IAM application roles are scoped to the EICS application on IDCS or OCI IAM. Since a new EICS application will be provisioned on IDCS or OCI IAM for each deployment type, there won't be any overlap in IDCS or OCI IAM application roles between different deployment types. This allows a Customer Security Admin to assign an IDCS or OCI IAM application role to a user on one deployment and not on others.

IDCS or OCI IAM application roles are assigned to users through IDCS or OCI IAM.

Each IDCS or OCI IAM application role creates one security group. These security groups are not visible on IDCS or OCI IAM, but the access can be managed via the associated IDCS or OCI IAM application role.

For example, assigning *admin_users* IDCS or OCI IAM application role to a user will automatically assign the associated security group, thus providing access to administration tasks to the user.

This table identifies IDCS or OCI IAM application roles:

Table 2–2 IDCS or OCI IAM Application Roles

Cloud Service or Options	IDCS or OCI IAM Application Roles
Admin Service	admin_users
Authenticated	all_users
Batch Service	batch_users
Initial user setup to login to EICS application	full_permission_users

Table 2–2 (Cont.) IDCS or OCI IAM Application Roles

Cloud Service or Options	IDCS or OCI IAM Application Roles
All store locations	global_store_users
Integration Service	integration_users
Message Processing Service	mps_users
Platform Service	psraf_users
Platform Service	psraf_admin_users
Retail Home Service	retail_home_users
Security Service	security_users
Perform application system configurations (both non-restricted and restricted)	sysop_users

SIOCS Application Roles

SIOCS 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 SIOCS security admin UI.

SIOCS has the following predefined application roles.

Table 2–3 Predefined Application Roles

Operations	SIOCS Application 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 IDCS or OCI IAM Application Roles and SIOCS Application Roles

Table 2–4 User Types with IDCS or OCI IAM Application Roles and SIOCS Application Roles

Application User Type	Job Duties	SIOCS Application Roles Assigned (User Role Assignment is via SIOCS Security Admin Screen)	IDCS or OCI IAM Application Role Assigned
Initial Application Admin User	To access SIOCS application and create other application admin and store users.	N/A	all_users admin_users batch_users full_permission_users global_store_users mps_users psraf_users security_users
Application Admin User	Perform all administration activities, setup other customer application store users and perform application configuration.	ADMINISTRATOR	all_users admin_users batch_users global_store_users mps_users psraf_users security_users
Store Users	Perform store operations in store using Mobile client.	Custom Defined Role with selected role permissions.	all_users psraf_users
Integration Users	External system invokes EICS provided Integration Services. See Integration Implementation sections for additional details.	N/A	integration_users
Retail Home User	Access SIOCS tiles on retail home and navigate to related operational views in SIOCS.	RETAIL HOME	all_users psraf_users retail_home_users
Retail Home Service Admin User	Access SIOCS tiles and service admin screens in Retail Home and navigate to related operational views in SIOCS		all_users psraf_admin_users retail_home_users

User Provisioning

Before users can access the Oracle Retail Stores Inventory and Operations Cloud Service applications, it is necessary to provision each user access to the system, and assign IDCS or OCI IAM application roles, stores, and SIOCS application roles to each user to control what functionality will be available to them. The access provisioning is done using Oracle Identity Cloud Service (IDCS) or Oracle Cloud Infrastructure Identity and Access Management (OCI IAM) for initial customer admin user. This user

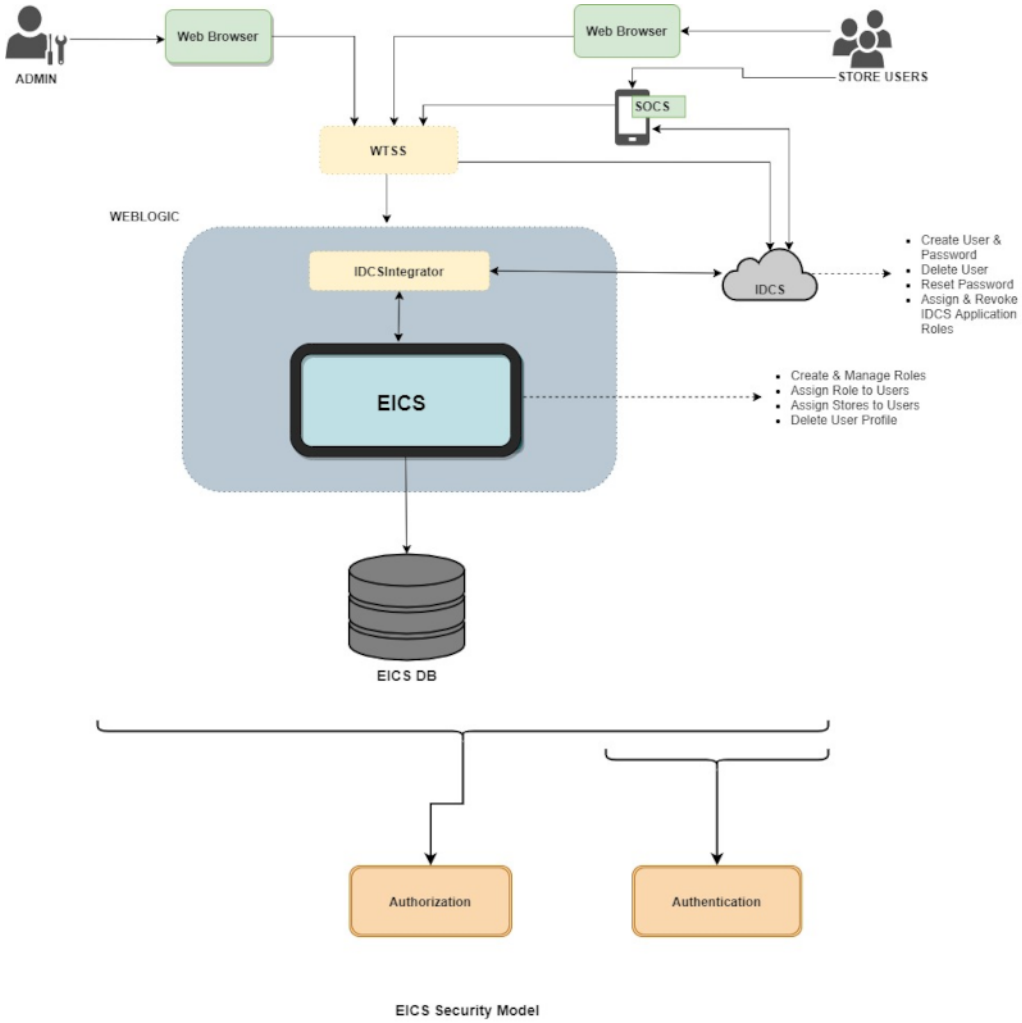
can create or manage other user provisioning via IDCS or OCI IAM and the SIOCS security admin UI.

IDCS or OCI IAM application roles assignments are typically used for special purpose access such as integration or various administration tasks. IDCS or OCI IAM application roles are assigned to users through IDCS or OCI IAM.

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 SIOCS security admin UI.

SIOCS 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 SIOCS security admin UI.

Figure 2–1 EICS Security Model



EICS Security Model

User Access

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

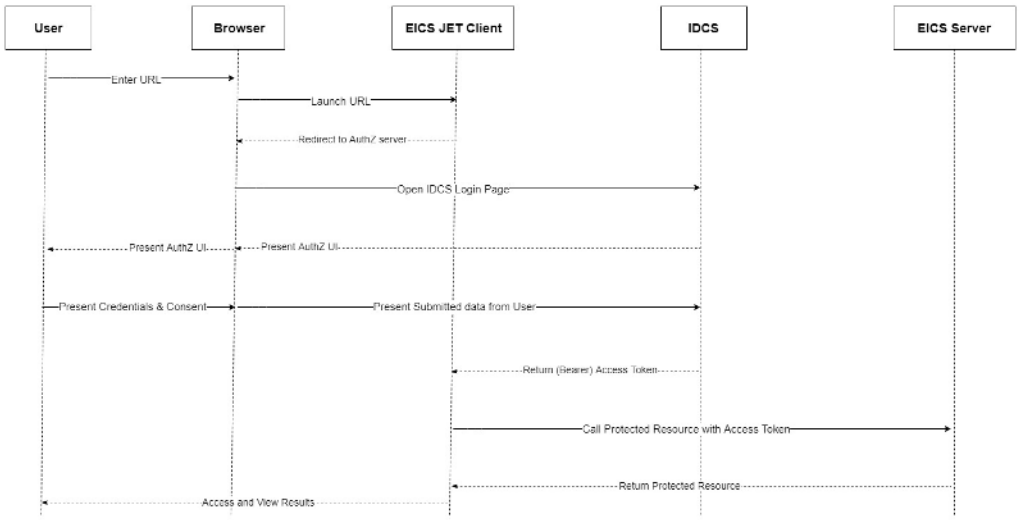
Users should not be reused or shared by multiple people or for multiple purposes.

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

Oracle Identity Cloud Service Access 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 Access Management



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

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

IDCS Application Roles are used for special purpose access. A Customer Security Admin can assign IDCS application roles to users on IDCS as follows:

1. Log into the IDCS console.
2. Select **Oracle Cloud Services** from the Navigation Drawer.
3. Locate and click on the EICS application for your deployment.
4. Navigate to the **Application Roles** tab.
5. Open the application role menu (☰) for the role you want to assign and select **Assign Users**.
6. Select the users that you want to assign the IDCS application role to and click **Assign**.

You can also use the IDCS application role menu to revoke a role from a team member.

Assigning an IDCS application role will automatically assign the associated security group to the user. These security groups are not visible on the IDCS UI and are only maintained internally.

Oracle Cloud Infrastructure Identity and Access Management

Oracle Cloud Infrastructure Identity and Access Management (IAM) provides identity and access management features such as authentication, single sign-on (SSO), and identity lifecycle management for Oracle Cloud.

For instructions on managing users in OCI IAM, follow the Manage Users OCI IAM document at the following URL:

https://docs.oracle.com/en-us/iaas/Content/Identity/home.html

3

Application Security

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

EICS Application Security

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

For access to special areas, IDCS or OCI IAM application role assignment in IDCS or OCI IAM is also required as mentioned in previous sections.

Users that are assigned the global store users IDCS or OCI IAM application role (*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 SIOCS security admin UI.

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

Application roles are created and managed through the SIOCS 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 SIOCS 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 SIOCS 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 SIOCS Application Roles to a User

1. Log into the SIOCS 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 SIOCS Application Roles and Stores

1. Log into the SIOCS 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 or OCI IAM.

However, an EICS user profile can be manually deleted without deleting the user in IDCS or OCI IAM. 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 SIOCS User Assignment table displays users stored in IDCS or OCI IAM 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 or OCI IAM 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 SIOCS 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 IDCS or OCI IAM application role assignments or other user information managed through IDCS or OCI IAM.

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

If a user only needs access to certain stores or permissions within EICS removed, then the SIOCS 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 or OCI IAM 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 IDCS or OCI IAM Application Role Membership Update (Optional)

If a considerable number of users need to have roles to be assigned, the Customer Security Admin can bulk import the role membership into the IDCS or OCI IAM application.

Bulk Update

To update the membership by bulk update:

1. Use these sample files as a starting point.
2. Extract the compressed file and then open the AppRoleMembership.csv file.
3. Review and then delete any demo data in the AppRoleMembership.csv file.
4. Create an import file using the AppRoleMembership.csv file. The AppRoleMembership.csv file is a simple text file in a tabular format (rows and columns). The first row in the file defines the columns (fields) in your table. At a minimum, the file must have these exact column headings.
   - **Entitlement Value** - Name of the IDCS or OCI IAM application role
   - **Grantee Name** - Name of the user
   - **Grantee Type** - Type should be fixed to 'User' (without quotes)

   For each membership, you create a new row (line) and enter data into each column (field). Each row equals one record.

   Important: The maximum number of membership roles that can be imported in a single job must not exceed 10,000.
5. Save your file in a CSV format.

Important: If you do not save the file in a CSV format with UTF-8 encoding, the import fails.

Bulk Import

IDCS

To import users and groups for Oracle application roles:

1. Log into the IDCS console.
2. Navigate to **Oracle Cloud Services** from the Navigation Drawer.
3. Locate and click on the EICS application for your deployment.
4. Click **Application Roles**.
5. Click **Import**.
6. In the Import Application Roles window, click **Browse** to locate and select the CSV file that contains the users and groups to import.

> **Note:** Click **Download sample file** in the dialog box to download a sample file.

7. Verify that the path and name of the CSV file that you selected appear in the **Select a file to import** field.
8. Click **Import**.
9. If Oracle Identity Cloud Service can't import a membership record, then it evaluates the next record in the CSV file.
10. After Oracle Identity Cloud Service evaluates all records, review the job results.
    - If the job can be processed immediately, then a dialog box appears with the **Job ID** link for your import job. Click the link. Review the details that appear on the **Jobs** page.
    - If the job cannot be processed immediately, then a message appears with a **Schedule ID** in it. Copy that ID and use it to search for the job on the **Jobs** page. The job will appear when processing completes. Go to Step 9.
11. On the **Jobs** page, locate the job that you want to view, and then click **View Details**. If the job failed, then click on **Export Errors** to export all the rows that the job was not able to process.

> **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.

OCI IAM

To import users and groups for Oracle application roles:

1. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Domains**.
2. Select the identity domain you want to work in and click **Applications**.
3. In the **Applications** page, click the Oracle application that has roles to which you want to assign users and groups.

Note: Importing application roles imports application roles memberships only. The application roles must already exist in the identity domain. If the application roles don't exist, you will receive an error for the membership import for that application role.

4. Click **Import**.
5. In the **Import application roles** window, drag and drop the file or click **Select one** to browse for the file.

Note: Click **Download sample file** in the dialog box to download a sample file.

6. Verify that the path and name of the CSV file that you selected appear in the **Select a file to import** field.
7. Click **Import**.

   If a user or a group is missing a required value, such as the user name or the group name, then that user or group can't be imported. If the user or group can't be imported, then the next user or group is evaluated in the CSV file.
8. After the job completes, review the job results.
   - If the job can be processed immediately, then a dialog box appears with the **Job ID** link for your import job. Click the link. Review the details that appear on the **Jobs** page.
   - If the job cannot be processed immediately, then a message appears with a **Schedule ID** in it. Copy that **Schedule ID** and use it to search for the job on the **Jobs** page. The job will appear when processing completes.
9. On the **Jobs** page, locate the job that you want to view. A table appears that displays the user names or group names, classification types (User or Group), and status of the users and groups that you imported and assigned to Oracle application roles in the identity domain.

Nightly Batch File Uploads

The following steps describe the file upload process.

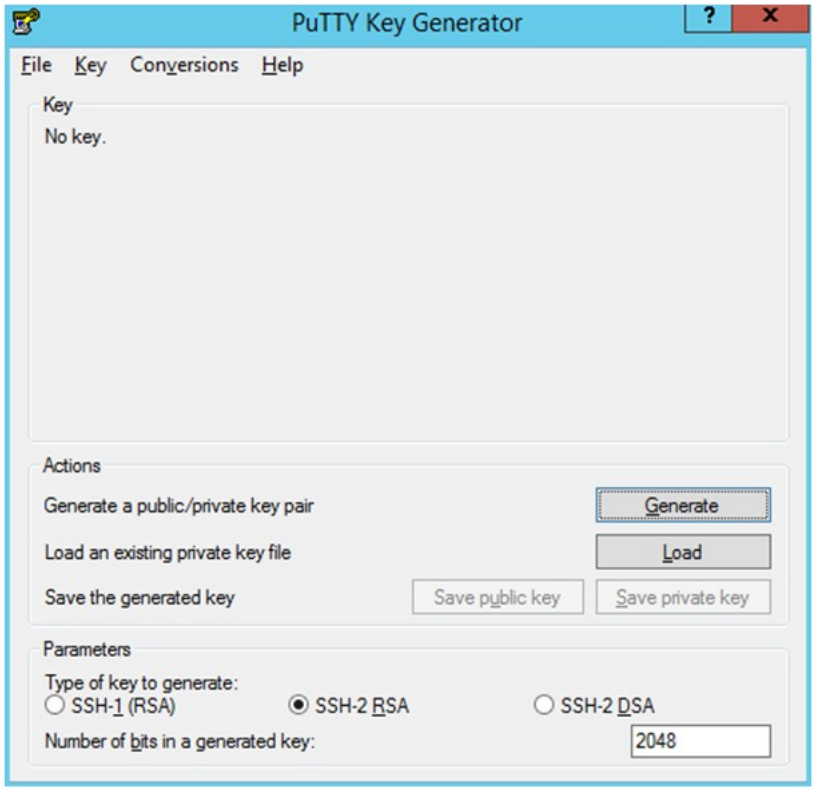
The Private/Public keys must be generated and the Public key must be associated with your SFTP Account for the file uploads. The Adding Authorized Keys section describes the step-by-step method to generate the keys (2048-bit RSA Keys).

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.

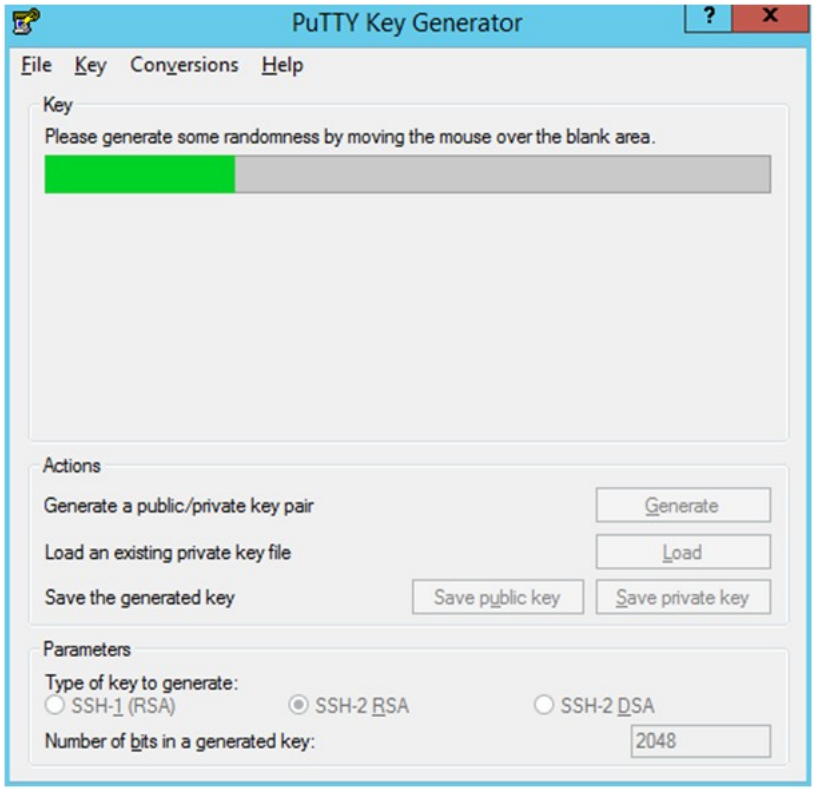
1. Launch WinSCP and select Tools\ Run PuttyGen.
2. Select **SSH-2 RSA** for the type of key to generate and enter 2048 for the number of bits in a generated key field. Click **Generate**.

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



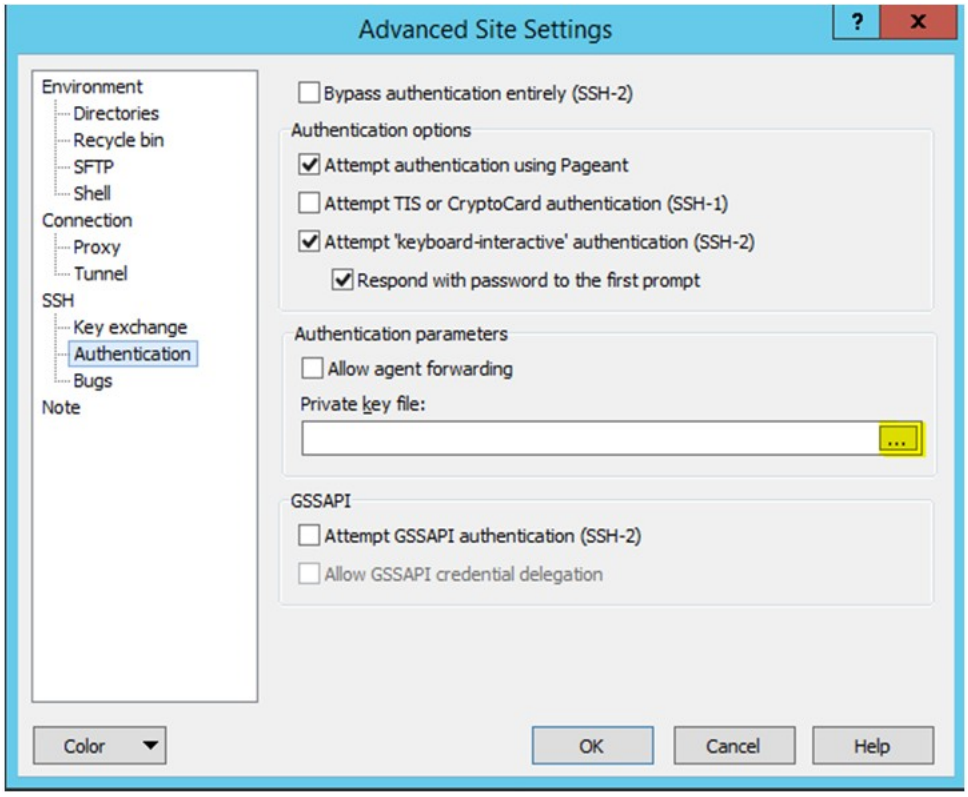
4. Once the key is generated, click **Save public key** to save the public key to a file.
5. Click **Save private key** to save the private key to a file. Confirm to save it with or without a pass phrase.
6. Open an SR with Oracle Support, to associate the public key with your SFTP account (attach the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

Logging In to WinSCP

The upload steps use the private key generated in the Adding Authorized Keys section.

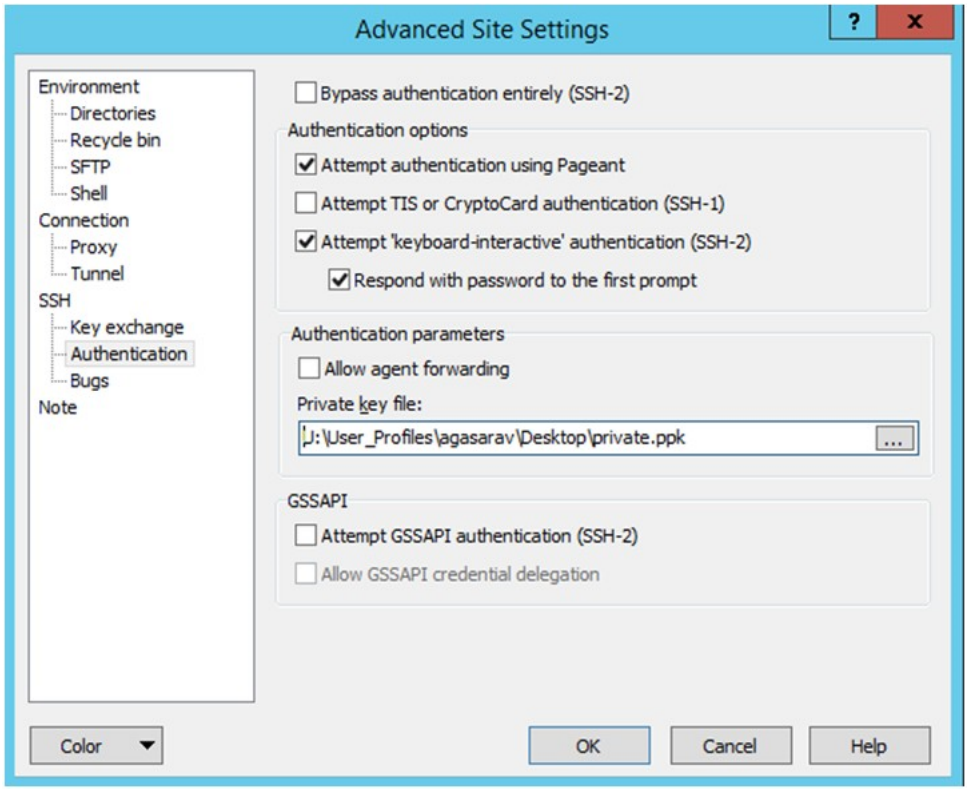
1. Launch WinSCP and connect to <SFTP Server> using port 22.
2. Enter the user name and click **Advanced**.
3. Click **Authentication**.
4. In the Private Key File field, click **Browse** and select the private key created in the Adding Authorized Keys section.

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.

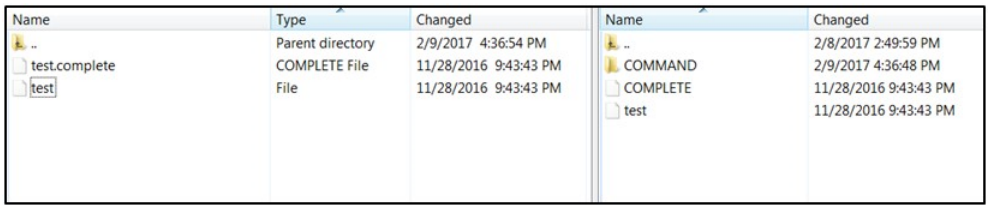
Note: Login can only be performed using the authorized keys. Login with username / password is not supported.

Uploading the Batch File

To upload the batch file:

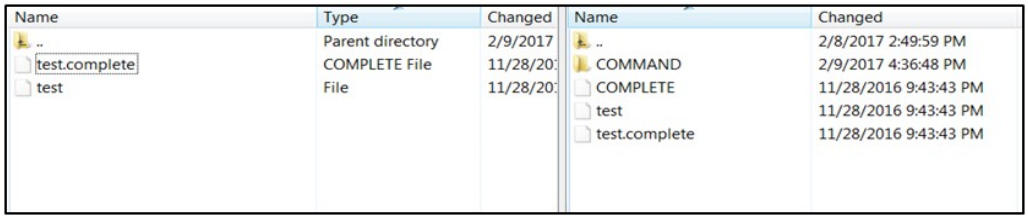
1. Log in to WinSCP. Follow the steps in Logging In to WinSCP.
2. Transfer the file to be copied (for example, test) to /<SFTP User>.

Figure 3–5 <SFTP User> Directory



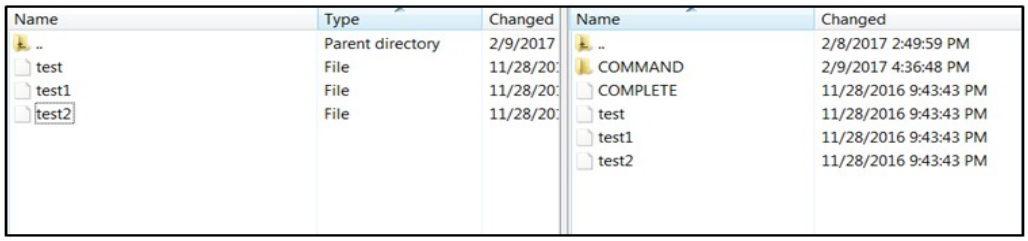
3. Transfer an empty file <filename>.complete (for example, test.complete) to the directory /<SFTP User>.

Figure 3–6 Transferring Empty File



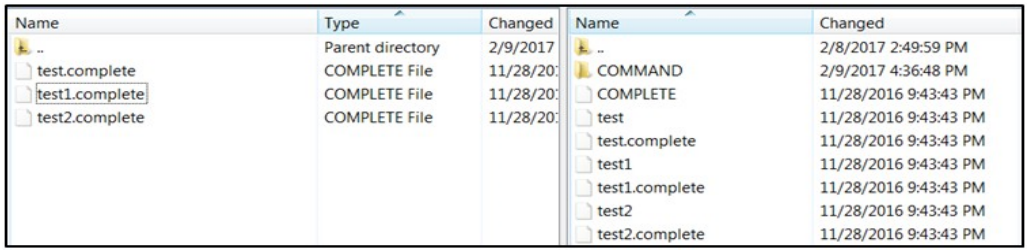
4. If multiple files must be transferred, copy all the files to /<SFTP_user>.

Figure 3–7 Transferring Multiple Files



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

Figure 3–8 Transferring .complete Files



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.