Oracle® Retail Xstore Office Cloud Service 22.0

Security Guide

Release 22.0
F62083-03
April 2023

Oracle Retail Xstore Office Cloud Service 22.0 Security Guide, Release 22.0

F62083-03

Primary Author: Gerlinde Rust

Contributing Authors:

Contributors:

Contents

Send Us Your Comments

Oracle® Retail Xstore Office Cloud Service Security Guide, Release 22.0

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

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

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

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

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

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

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

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

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

Preface

The *Oracle Retail Xstore Office Cloud Service Security Guide* describes all available functions of Release 22.0.

Audience

This guide is for technical personnel who configure, maintain and support, or use Oracle Retail Xstore Office.

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

See the Oracle Retail Xstore Office Cloud Service documentation library at the following URL:

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

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

Review Patch Documentation

When you install the application for the first time, you install either a base release (for example, 22.0) or a later patch release (for example, 22.0.1). If you are installing the base release or additional patches, read the documentation for all releases that have occurred since the base release before you begin installation. Documentation for patch releases can contain critical information related to the base release, as well as information about code changes since the base release.

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 Help Center (docs.oracle.com) 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 Help Center (docs.oracle.com) 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 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 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.

Convention	Meaning
`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

This chapter provides a product and cloud deployment overview of Xstore Office Cloud Service.

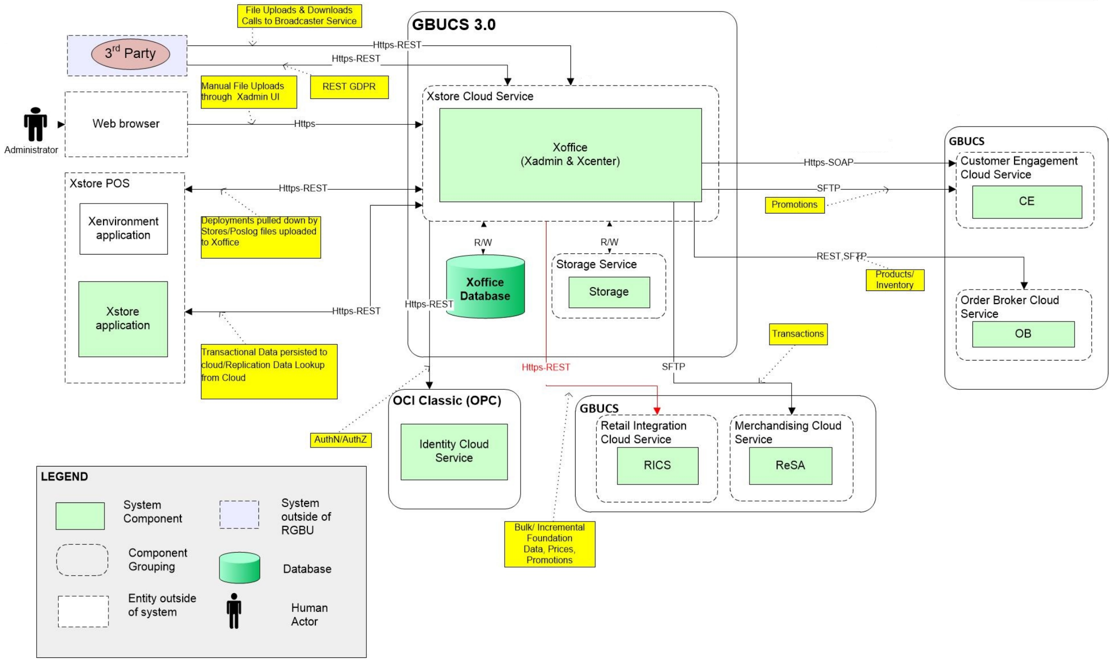
Product Overview

Oracle Retail Xstore Office Cloud Service is a web-based application used to administer corporate based functions such as Oracle Retail Xstore Point-of-Service configuration setup and maintenance, file management for the Oracle Retail Xstore Suite, viewing the electronic journal, viewing store reports, monitoring Oracle Retail Xstore Point-of-Service versions in use at the store and register levels, and monitoring alerts.

Xstore Office Cloud Service consists of a User Interface component called Xadmin and a Web Services component called Xcenter, a Java and JSON-based messaging framework.

Xstore Office Cloud Service integrates with several other products as shown in the following Architecture Model. All incoming web services are RESTful and secured with OAuth 2.0. Outgoing web services are RESTful or SOAP based and secured with OAuth, Basic Auth or Custom Auth.

Figure 1-1   Architecture Model



Identity Cloud Service or Infrastructure Identity and Access Management

The Identity Cloud Service (IDCS) is an Identity Management Service and Authorization Server and has a host of other features and capabilities. For more information on IDCS, see the Oracle Identity Cloud Service documentation set, Get Started portal for IDCS.

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

Xstore Office Cloud Service integrates with Identity Cloud Service (IDCS). For Xstore Office Cloud, IDCS is primarily used for Identity Management (that is, storing user information), for securing REST services using the Open Authorization (OAuth) 2.0 and Login via the OAuth 2.0 and OpenID Connect (OIDC) protocols.

Oracle Cloud Infrastructure Identity and Access Management (OCI IAM) provides identity and access management features such as authentication, single sign-on (SSO), and identity lifecycle management for Oracle Cloud as well as Oracle and non-Oracle applications, whether SaaS, cloud-hosted, or on-premises.

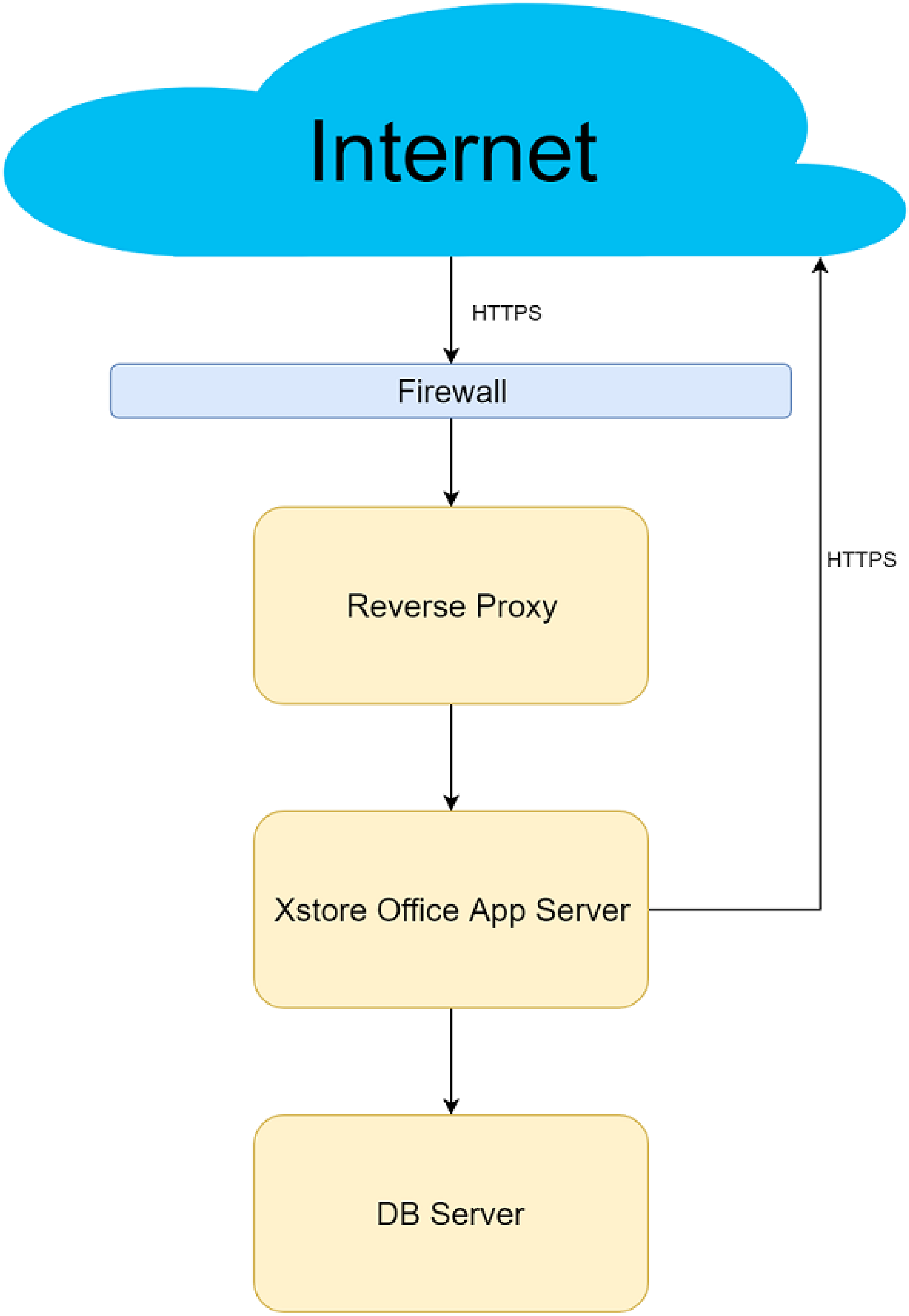
For more information, see the Oracle Cloud Infrastructure Documentation:

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

Cloud Deployment Overview

The following diagram describes an Xstore Office Cloud deployment.

Figure 1-2 Xstore Office Cloud Deployment Process



All incoming and outgoing service communication with the Cloud instance requires TLS for transport security.

Reverse Proxy: The Reverse Proxy intercepts all incoming requests to Xstore Office Cloud and authorizes and/or authenticates the requests based on the Xstore Office Cloud Web Tier Policy defined in IDCS or OCI IAM.

Xstore Office Application Server: The Application Server hosts the Xstore Office Cloud Service Applications including Xadmin which is the User Interface component and Xcenter which is the Web Services component (a Java and JSON-based messaging framework).

DB Server: The Oracle database server contains the database schemas required by the Xstore Office Cloud Service.

2 Security Features

This chapter describes the available security features of the Xstore Office Cloud Service.

Security Model

Xstore Office Cloud Service integrates with Identity Cloud Service (IDCS) or Oracle Cloud Infrastructure Identity and Access Management (OCI IAM) for Identity Management (that is, storing user information), for securing REST services using the Open Authorization (OAuth) 2.0 and Secure User Authentication via the OAuth 2.0 and OpenID Connect (OIDC) protocols.

A Reverse Proxy is in place that intercepts all incoming requests to Xstore Office Cloud Service and authorizes and/or authenticates the requests based on the Xstore Office Cloud Web Tier Policy defined in IDCS or OCI IAM.

Xstore Office Cloud Service Provisioning

During Xstore Office Provisioning, Xstore Office OAuth Clients (or Apps) are created in IDCS or OCI IAM with custom AppRoles. The Custom AppRoles are used to perform additional Application Level authorizations in addition to Application Level Privilege authorizations.

At the time of provisioning, a Customer Administration User is also created, who initially, is the sole user with access to the Xstore Office Cloud Service application. It is the responsibility of the Customer Administration User to create users with the appropriate privileges for functionality that will become available to them. It is recommended that users are granted the least level of access they require to perform their duties.

Authentication

Xadmin delegates the login to IDCS or OCI IAM. Therefore, it does not prompt the user to login and does not store any user credentials. Instead, when a user accesses Xadmin, the Reverse Proxy determines whether this user's session already exists in IDCS or OCI IAM. If so, it forwards to Xadmin. If this user's session does not exist, then the Reverse Proxy redirects to IDCS or OCI IAM prompting the user to enter their credentials. If the user successfully authenticates in IDCS or OCI IAM, then the request is forwarded to Xadmin. Once at Xadmin, additional application level authorization is performed to determine the user's role and privileges granted to the user in order to display the appropriate features that the user is authorized to access.

For details on how users are created and provisioned, see the Creation of Users section.

Multi-Factor Authentication (MFA)

IDCS or OCI IAM provides the ability to enable Multi-Factor Authentication. For more information on enabling Multi-Factor Authentication, see the *Oracle Cloud Administering Oracle Identity Cloud Service Guide* or the Oracle Cloud Infrastructure Documentation.

Access Control

Xcenter REST APIs are secured with OAuth 2.0 protocols and use OAuth tokens. When Xcenter REST Services are invoked, the Reverse Proxy intercepts the requests, uses the OAuth 2.0 protocol to authorize the OAuth tokens and forwards the request to Xcenter. Xcenter then examines the tokens and performs additional application level authorization by examining the tokens to see if they were requested by an OAuth Client that was granted specific AppRoles defined in IDCS or OCI IAM when Xstore Office OAuth Clients were provisioned. If the token contains the necessary AppRole Grants, Xcenter provides access to the endpoint and the appropriate response is returned.

For details on how users are created and provisioned, see the Creation of Users section.

Security Audit

User Identity (account name or IP address) is recorded in the application logs when accessing Xadmin or invoking Xcenter REST APIs. In addition, date, time, information, software or configuration changes are also recorded in the application logs.

IDCS or OCI IAM provides several reports that are detailed in the *Oracle Cloud Administering Oracle Identity Cloud Service Guide* or the Oracle Cloud Infrastructure Documentation.

Credential Rotation

All credentials in use within the Xstore Office Cloud Service will be rotated on a regular schedule.

3

Security Considerations for Developers

This chapter describes security considerations for developers.

Creation of Users

A Customer Administration User will be created as part of the Xstore Office Cloud Service provisioning process. Before end users can access the Xstore Office Cloud Service application it is necessary to create and provision users. This includes provisioning access to the system, assigning organizations, a role and org nodes to each user to control what functionality will be available to them. This will need to be done by the Customer Administration User.

IDCS or OCI IAM

> **Note:**
>
> While users can be created using the IDCS or OCI IAM UI, it is important to note that they must still be provisioned through the Xadmin UI. This includes provisioning access to the system, assigning organizations, a role and org nodes to each user to control what functionality will be available to them.

Manual Creation

Users can be created manually (that is, one at a time) in IDCS or OCI IAM by following the instructions on how to create user accounts in the *Oracle Cloud Administering Oracle Identity Cloud Service Guide* for IDCS or the Oracle Cloud Infrastructure Documentation for OCI IAM.

Bulk Import

Users can be bulk imported into IDCS or OCI IAM by following the instructions on how to import user accounts in the *Oracle Cloud Administering Oracle Identity Cloud Service Guide* for IDCS or the Oracle Cloud Infrastructure Documentation for OCI IAM.

REST APIs

Users can also be imported (either individually or in bulk) into IDCS or OCI IAM by invoking IDCS or OCI IAM REST APIs. For more information about the REST APIs, see the *Oracle Cloud REST API for Oracle Identity Cloud Service Guide* for IDCS or the Oracle Cloud Infrastructure Documentation for OCI IAM.

User Access AppRole

When a user is created using IDCS or OCI IAM (either manually or via bulk import, or via REST APIs), it is the Customer Admin's responsibility to grant the User the *User Access* AppRole. This can be done in the IDCS or OCI IAM UI as follows:

- Click on Oracle Cloud Services in the menu/left frame.
- Click on the Xstore Office App:
  - For XOCS 20.x environments:

    The App will typically be of the format RGBU_XTROFFCS_{ENV}_XOFFICE:
    - where {ENV} can be PRDXX or STGXX or DEVXX (or UATXX)
    - where XX represents an index number

      For example, RGBU_XTROFFCS_PRD1_XOFFICE or RGBU_XTROFFCS_STG2_XOFFICE and so on.
  - For XOCS 19.x environments:

    The App will typically be of the format RGBU_XTROFFCS_{ENV}_XOFFICE.
    - where {ENV} can be PRD, UAT or DEV
- Click on the Application Roles tab.
- Select the menu icon on the far right of the *User Access* AppRole.
- Select **Assign Users** and select the Users in the popup to be granted this AppRole.

Xadmin

Refer to the *Oracle Retail Xstore Office/Xstore Office Cloud Service User Guide* for details on how to provision users via the Xadmin User Management UI.

Xoffice OAuth Client AppRoles

AppRoles have been created in Xoffice OAuth Clients in order to perform additional App Level Authorization.

User Access

Typically, the IDCS or OCI IAM tenant will represent several applications which are independent of each other. The *User Access* AppRole has been created in the Xstore Office App.

For XOCS 20.x environments:

The Xstore Office App typically has a display name of either RGBU_XTROFFCS_PRDXX_XOFFICE or RGBU_XTROFFCS_STGXX_XOFFICE or RGBU_XTROFFCS_DEVXX_XOFFICE (or RGBU_XTROFFCS_UATXX_XOFFICE) depending on the environment where XX represents an index number.

For XOCS 19.x environments:

The Xstore Office App typically has a display name of either RGBU_XTROFFCS_PRD_XOFFICE or RGBU_XTROFFCS_UAT_XOFFICE or RGBU_XTROFFCS_DEV_XOFFICE depending on the environment.

The User Access AppRole is used to link IDCS or OCI IAM users with the Xstore Office Cloud Service Application.

When Xadmin performs a user sync against IDCS or OCI IAM, it will do the sync based on the users that have been granted this *User Access* AppRole. Refer to the *Oracle Retail Xstore Office/Xstore Office Cloud Service User Guide* for details on the user sync between Xadmin and IDCS or OCI IAM.

When a user is created using the IDCS or OCI IAM UI (either manually or via Bulk Import), it is the Customer Admin's responsibility to grant the user the *User Access* AppRole. This can be done as follows:

- Click on Oracle Cloud Services in the menu/left frame.
- Click on the Xstore Office App:
  - For XOCS 20.x environments:

    The App will typically be of the format RGBU_XTROFFCS_{ENV}_XOFFICE:
    - where {ENV} can be PRDXX or STGXX or DEVXX (or UATXX)
    - where XX represents an index number

      For example, RGBU_XTROFFCS_PRD1_XOFFICE or RGBU_XTROFFCS_STG2_XOFFICE and so on.
  - For XOCS 19.x environments:

    The App will typically be of the format RGBU_XTROFFCS_{ENV}_XOFFICE.
    - where {ENV} can be PRD, UAT or DEV
- Click on the Application Roles tab.
- Select the menu icon on the far right of the *User Access* AppRole.
- Select **Assign Users** and select the Users in the popup to be granted this AppRole.

Xstore Access

The *Xstore Access* AppRole is used for additional App Level Authorization. This authorization is done when Xstore Office REST APIs are invoked. Therefore, if the Xstore Office REST APIs are to be invoked, then they must be done by using an OAuth Client (App) that has been granted the *Xstore Access* AppRole. For instance, refer to Xstore Office Setup App in the Creation of the Setup OAuth Client in IDCS or OCI IAM section. This AppRole should not be granted to any users, groups or apps. Any granting that is required will be done automatically by the system.

Data Privacy Access

The *Data Privacy Access* AppRole is used for additional App Level Authorization. This authorization is done when the Data Privacy REST APIs are invoked. Therefore, if the Data Privacy REST APIs are to be invoked, they must be done by using an OAuth Client (App) that has been granted the *Data Privacy Access* AppRole. Refer to the Creation of the Setup OAuth Client in IDCS or OCI IAM section. This AppRole should not be granted to any users, groups or apps. Any granting that is required will be done automatically by the system.

Enhanced Email Access

The Enhanced Email Access AppRole is used for additional App Level Authorization. This authorization is done when the Email Receipt REST API is invoked. Therefore, if the Email Receipt REST API is to be invoked, it must be done by using an OAuth Client (App) that has been granted the Enhanced Email Access AppRole. Refer to the Creation of the Setup OAuth Client in IDCS or OCI IAM section. This AppRole should not be granted to any users, groups or apps. Any granting that is required will be done automatically by the system.

Service Access

The *Service Access* AppRole is used for internal manipulation of the OAuth Clients. This is also needed in case OAuth Clients need to be deleted. This AppRole should not be granted to any users, groups or apps. Any granting that is required will be done automatically by the system.

Cloud Enrollment of Xstore Clients

Any Xstore register (desktop, thin client, tablet, or mobile) or other client (like Xenvironment or Xservices) that communicates with Xstore Office Cloud Service must first be enrolled in IDCS or OCI IAM via Xstore Office Cloud Service. This can be done either via Xadmin or Xenvironment. The sections below contain information about the steps to be followed for Cloud Enrollment of Xstore Clients.

For more information about how to configure web service authentication for the Retail Omnichannel products, see the *Oracle Retail Omnichannel Web Service Authentication Configuration Guide* (Doc ID 2728265.1) on My Oracle Support.

Xadmin

Xstore Stores can be enrolled in Xstore Office Cloud Service via Xadmin On-Premise, if the retailer has an existing Xadmin On-Premise application 18.0.1 or higher. Refer to the on-premise *Oracle Retail Xstore Office User Guide* for these steps.

Xenvironment

Xstore stores can be enrolled in the Xstore Office Cloud Service via Xenvironment by following these steps.

> **Note:**
>
> Collect the following data prior to starting the Cloud Enroll process via Xenvironment.
>
> 1. Xstore Office Cloud Service hostname, port and tenancy ID. The Customer Administrator can look this up by logging into their Cloud Service Account.
> 2. IDCS or OCI IAM User credentials: Username and password of any IDCS or OCI IAM user belonging to the provisioned IDCS or OCI IAM tenant.
>
>   Note that the user whose credentials are used here MUST NOT have Multi Factor Authentication (MFA) enabled. This same user's credentials can then be used for all Store Enrollments. Whenever Store Enrollments are completed, MFA can be enabled for this user.

1. Once the Xenvironment installation is complete, open a web browser on the same system where Xenvironment is installed, that is on the lead register. The enrollment process only works when performed on the lead register. Go to the following URL: https://<lead_register_hostname>:9096/cloudenroll.
2. Log in as the user that runs Xstore Point of Service.
3. In the form that is presented, enter the Xcenter Application Server Settings for Xstore Office Cloud.
   - Host: Xstore Office Cloud Hostname
   - Port: Xstore Office Cloud Port
   - Username: Username of an IDCS or OCI IAM user (This is typically an email address)
   - Tenancy ID: References the prod, stage or dev (or uat) environment. It will be of the format rgbu-omni-<cust>-<env><num>-xocs and is part of the application url.
   - Password: Password of an IDCS or OCI IAM user
4. Click **Enroll Location**. This will validate the user credentials and enroll the location.
5. Once the enrollment is complete the systems will be restarted. When the registers start up again they will be configured for Xstore Office Cloud Service.
6. At Store close all the registers, Xenvironment, and Xservices will be enabled with Xstore Office Cloud Service configurations and all systems will be restarted.

Creation of OAuth Clients in IDCS or OCI IAM

OAuth Clients (also called Apps) are required in order to invoke REST Services exposed by Xstore Office.

A new REST API has been exposed for creating OAuth Clients to be able to perform initial setup of the Xstore Office Cloud Service.

> **Note:**
>
> While OAuth Clients can be created via the IDCS or OCI IAM User Interface, the resulting OAuth Clients do not have all the needed properties in order to be able to function accurately. Instead, follow the steps detailed below in order to create the OAuth Clients using the IDCS or OCI IAM REST APIs.

Prerequisites

- It is very helpful to understand tools and terminologies such as Basic Auth, OAuth, curl, json and their usage.
- For example, knowing that OAuth uses Bearer Tokens in the HTTP Authorization Header whereas Basic Auth uses Base 64 encoded credentials will help you understand the commands below.
- Authorization Header for an OAuth Token would look like this: "Authorization: Bearer <token>"
- Authorization Header for a Basic Auth Token would look like this: "Authorization: Basic <Base64_encode(client_id:client_secret)>"

> **Note:**
>
> 1. OAuth Clients are also called Apps. These terms are used interchangeably.
> 2. Be sure to use the correct App Client IDs and Client Secrets based on the environment. These steps will have to be repeated for each environment. Using the artifacts from one environment in another environment can lead to unexpected results.

Required Data

Collect the following data prior to creation of the OAuth Clients.

1. IDCS_TENANT_HOST: The Customer Administrator can look this up by logging into their Cloud Service Account.
2. IDCS or OCI IAM User credentials: Username and Password of an IDCS or OCI IAM user belonging to the provisioned IDCS or OCI IAM tenant who is either an Identity Domain Administrator or an Application Administrator, or both. An IDCS or OCI IAM user who is neither an Identity Domain Administrator nor an Application Administrator will not be authorized to invoke this API.

Tools

The following steps are executed using curl. However, any similar tool such as SoapUI or Postman can be used.

Creation of the Setup OAuth Client in IDCS or OCI IAM

Xstore Office Setup App

Before the newly provisioned Xstore Office Cloud Service can be used, some initial setup is required. For instance, the Xstore Office database needs Tax Location data to be present in order to be able to setup new stores or organization hierarchy via the Xadmin UI. This can be achieved by using the Xcenter auto deployment functionality via REST services. In order to utilize the Xcenter REST services, an OAuth Client is required. This client can also be used to insert any other seed Xstore Office data that needs to be present in the database besides the Tax Location data.

This Xstore Office Setup OAuth Client can be created by invoking the Enroll Client API as described below.

> **Note:**
>
> 1. This OAuth Client can also be used to invoke RTLog Generator REST APIs.
> 2. This OAuth Client credentials can also be used to configure the Data Migration Utility.
> 3. This OAuth Client can also be used to invoke Data Privacy APIs.
> 4. This OAuth Client can also be used for any additional recurring customer operations where Xcenter REST Services need to be invoked.

> **Note:**
>
> The intent of this API is to create an OAuth Client for the setup of Xstore Office Cloud Service, primarily for Data Migration purposes, uploading "seed" data and for invoking the Data Privacy API. It is not intended to be used for integration with other systems.

1. Request creation of the Setup OAuth Client. The response will contain the client id, client secret of the OAuth Client as well as the IDCS_TENANT_HOST (which is already known to the Customer Admin).

   Replace the <IDCS_username> and <IDCS_password> with those of an IDCS user who is either an Identity Domain Administrator or an Application Administrator or both.

   Note that the user whose credentials are used here MUST NOT have Multi Factor Authentication (MFA) enabled. If it is enabled, please disable MFA for only this user temporarily in order to invoke this API. Once the API returns the OAuth Client credentials, please re-enable MFA for this user. If the API needs to be invoked at a future time, please follow the same MFA disable/enable process described above for the user.

   ```
   curl -i -H "Authorization: Basic
   <Base64_encode(<IDCS_username>:<IDCS_password>)>" "https://
   <XSTORE_OFFICE_HOST>/<tenancy_id>/xcenter/rest/Default/21/enrollclient?
   type=setup"
   ```

where <tenancy_id> references the prod, stage or dev (or uat) environment.

2. Request an Access token using the Setup OAuth Client credentials (from the previous step).

   Replace the <client_id> and <client_secret> with those of the Setup OAuth Client (App).

   ```
   curl -i -H "Authorization: Basic
   <Base64_encode(<client_id>:<client_secret>)>" -H "Content-Type:
   application/x-www-form-urlencoded;charset=UTF-8" https://
   <IDCS_TENANT_HOST>/oauth2/v1/token -d
   "grant_type=client_credentials&scope=urn:opc:idm:__myscopes__"
   ```

3. This token can now be used to invoke Xoffice REST APIs in order to configure Xstore Office Cloud Service.

4. RTLog Generator REST APIs:

   a. The credentials (Client Id and Client Secret) of the Setup OAuth Client (App) can be similarly used to obtain a token in order to invoke RTLog Generator REST APIs.

5. Data Migration Utility:

   a. The credentials (Client Id and Client Secret) of the Setup OAuth Client (App) can be used when configuring the Data Migration Utility (to update idp.properties) in order to migrate data from an existing Xstore Office to Xstore Office Cloud Service.

6. Data Privacy API:

   a. The credentials (Client Id and Client Secret) of the Setup OAuth Client (App) in conjunction with an IDCS or OCI IAM user's userid/password can be used in order to request an Access token to invoke the Data Privacy REST API.

      Replace the <client_id> and <client_secret> with those of the Data Privacy OAuth Client (App).

      Replace the <IDCS_username> and <IDCS_password> with those of an IDCS user.

      Note that the user whose credentials are used here MUST NOT have Multi Factor Authentication (MFA) enabled. If it is enabled, please disable MFA for only this user temporarily in order to invoke this API. Once the API returns the OAuth token, please re-enable MFA for this user. If the token API needs to be invoked at a future time, please follow the same MFA disable/enable process described above for the user.

      ```
      curl -i -H "Authorization: Basic
      <Base64_encode(<client_id>:<client_secret>)>" -H "Content-Type:
      application/x-www-form-urlencoded;charset=UTF-8" https://
      <IDCS_TENANT_HOST>/oauth2/v1/token -d
      "grant_type=password&username=<IDCS_username>&password=<IDCS_passwo
      rd>&scope=urn:opc:idm:__myscopes__"
      ```

   b. Invoke the Data Privacy endpoint (example – replace with appropriate data).

      Replace <token> with the token from the previous step.

      ```
      curl -i -H "Authorization: Bearer <token>" "https://
      <XSTORE_OFFICE_HOST>/<tenancy_id>/xcenter/rest/privatedata/
      1000::100?type=employee"
      ```

where <tenancy_id> references the prod, stage or dev (or uat) environment.

Creation of the Enhanced Email OAuth Client in IDCS or OCI IAM

Xstore Office Enhanced Email App

The Enhanced Email App is intended to be created by the Retailer and the credentials are to be given to a third party to invoke the Email Receipt REST API. This Xstore Office Enhanced Email OAuth Client can be created by invoking the Enroll Client API as described below.

> **Note:**
>
> A pre-requisite here is that the Setup OAuth Client must have already been created because those credentials are needed to retrieve a token to invoke the Enroll Client API. In other words, while the Setup OAuth App is created using the Enroll Client API secured via Basic Auth, the Enhanced Email App is also created using the Enroll Client API but it is secured via OAuth (using a token obtained by using the Setup OAuth App credentials).

> **Note:**
>
> The intent of this API call is to create an Enhanced Email OAuth Client to invoke the Email Receipt REST API and cannot be used to invoke any other APIs.

1. Request creation of the Setup OAuth Client as described in the previous section. The response will contain the client id, client secret of the OAuth Client as well as the IDCS_TENANT_HOST (which is already known to the Customer Admin).
2. Request an Access token using the Setup OAuth Client credentials (obtained from the previous step).

   Replace the <client_id> and <client_secret> with those of the Setup OAuth Client (App).

   ```
   curl -i -H "Authorization: Basic
   <Base64_encode(<client_id>:<client_secret>)>" -H "Content-Type:
   application/x-www-form-urlencoded;charset=UTF-8" https://<IDCS_TENANT_HOST>/
   oauth2/v1/token -d
   "grant_type=client_credentials&scope=urn:opc:idm:__myscopes__"
   ```
3. This token can now be used to invoke the Enroll Client API to request creation of the Enhanced Email OAuth Client. The response will contain the client id, client secret of the OAuth Client as well as the IDCS_TENANT_HOST (which is same as what was used/returned earlier).

   ```
   curl -i -H “Authorization: Bearer <token>” "https://<XSTORE_OFFICE_HOST>/
   <tenancy_id>/xcenter/rest/Default/21/enrollclient?type=email"
   ```

   where <tenancy_id> references the prod, stage or dev (or uat) environment.
4. Request an Access token using the Enhanced Email OAuth Client credentials (from the previous step).

Replace the <client_id> and <client_secret> with those of the Enhanced Email OAuth Client (App).

```
curl -i -H "Authorization: Basic
<Base64_encode(<client_id>:<client_secret>)>" -H "Content-Type:
application/x-www-form-urlencoded;charset=UTF-8" https://
<IDCS_TENANT_HOST>/ oauth2/v1/token -d
"grant_type=client_credentials&scope=urn:opc:idm:__myscopes__"
```

This token can now be used to invoke the Email Receipt REST API once the Email Receipt Service Broadcaster has been correctly setup via the Xadmin UI.