Oracle Fusion Cloud Customer Experience

Getting Started with Your Customer Data Management (CDM) Implementation

Oracle Fusion Cloud Customer Experience
Getting Started with Your Customer Data Management (CDM) Implementation

F77895-11

Copyright © 2011, 2025, Oracle and/or its affiliates.

Author: Crescentia David

Contents

Get Help

There are a number of ways to learn more about your product and interact with Oracle and other users.

Get Help in the Applications

Some application pages have help icons to give you access to contextual help. If you don't see any help icons on your page, click your user image or name in the global header and select Show Help Icons. If the page has contextual help, help icons will appear.

Get Training

Increase your knowledge of Oracle Cloud by taking courses at *Oracle University*.

Join Our Community

Use *Cloud Customer Connect* to get information from industry experts at Oracle and in the partner community. You can join forums to connect with other customers, post questions, suggest *ideas* for product enhancements, and watch events.

Share Your Feedback

We welcome your feedback about Oracle Applications user assistance. If you need clarification, find an error, or just want to tell us what you found helpful, we'd like to hear from you.

You can email your feedback to *oracle_fusion_applications_help_ww_grp@oracle.com*.

Thanks for helping us improve our user assistance!

1 About this Guide

Audience and Scope

You can use this guide to get started with the implementation of Customer Data Management cloud service capabilities such as duplicate identification, duplicate resolution, address verification, and data enrichment.

This guide provides you with the concepts and procedures you need to quickly implement a simple customer data management solution in a test environment. We don't give you a comprehensive explanation of all the available features and options that you can find in other guides. Rather, we focus on key setups and leverage the default settings and on-boarding tools that Oracle provides to get you going.

We are dealing with a stand-alone customer data management implementation here. So, if you're implementing customer data management together with another service, you must follow a different set of steps for your initial setup.

This document supplements standard product documentation, which you're encouraged to review. To find complete documentation and other learning resources visit the Help Center for Oracle Customer Data Management Cloud.

Related Topics

How to Use This Guide

The chapters in this guide cover the setup in the recommended order. Each chapter assumes that you completed the steps in the previous chapters. Here's how to use this guide:

- Read the brief Setup Overviews at the beginning of each chapter to understand the setups the chapter covers.
- Use the Setup Overview as a guide to the setups you must perform. The remaining topics in the chapter provide the step-by-step details of how to perform each of those setups.
- Refer to other guides for full explanation of the different features and options.

Unless specified otherwise, you must be signed in as a setup user to complete the setups. A setup user has a broader set of security privileges than the initial user provided to you by Oracle.

What You Will Be Able to Do After Completing the Setups

After completing the setups described in this guide, you should be able to:

- Identify duplicates:
  - Identify potential duplicate account, contact, and address records in real time when your application users create a customer record, thus preventing entry of duplicate records.
  - Identify potential duplicates using batch processing for records already in the database or potential duplicates of the records in the database within an import batch
  - Identify duplicates during import of customer data for records already in the database.
- Resolve duplicates: Consolidate the identified duplicates by merging or linking them.
- Verify addresses: Cleanse an address to confirm to postal requirements and verify that the address is an actual postal address.
- Enrich Data: Enrich account and contact data to ensure it's comprehensive

Before You Start

We assume that you have subscribed to the service and have received the e-mail with your environment and initial sign-on information.

Case Study

This guide uses a case study to define the scope of the implementation tasks and illustrate their interdependence.

The case study is based on a fictitious company named Vision Corp., a global high-tech company that sells laptop and multiple server product lines to businesses and other organizations. With a view to diversify into software business, Vision Corp. has recently acquired a couple of software companies, First Software and Softgear, and their customers.

For the pilot implementation, Vision Corp would like to implement Customer Data Management Cloud to:

- Manage the quality of the acquired customer data.
- Manage the quality of its own existing data.
- Manage the quality of the new customer data entered real-time through its different touch points.

Related Guides

You can refer to the related guides listed in the following table to understand more about the tasks covered in this guide.

Title	Description
Implementing Customer Data Management	Describes tasks to configure and set up Oracle CX Customer Data Management capabilities, such as, duplicate identification, duplicate resolution, address verification, and data enrichment.

Title	Description
Using Customer Data Management	Describes how to manage customer information and identify and resolve duplicates, verify addresses, and enrich data.
Extending CX Sales and B2B Service	Describes how to use tools to configure and extend Oracle CX Sales and B2B Service.
Understanding Import and Export Management for CX Sales and B2B Service	Describes how to import legacy and other data into Oracle CX Sales and B2B Service using Import and Export Management, and export data out of these applications.
Using Oracle Account and Contact Enrichment by Dun & Bradstreet (D&B)	Describes how to use Oracle Account and Contact Enrichment by Dun & Bradstreet (D&B) to update company and contact data in your Oracle Cloud application
Using Oracle Address, Email, and Phone Verification	Describes how to use Oracle Address, Email, and Phone Verification to verify and standardize addresses in your Oracle Cloud application.

2 Sign In and Perform Preliminary Tasks

Overview of Preliminary Tasks

Before you start implementing your Customer Data Management application according to the instructions in this guide, complete these preliminary tasks.

Step	Description	Where to Get More Details
Complete the Service Administrator Action List	Before you sign in for the first time, complete the actions listed in the Service Administrator Action List provided by Oracle and create your account with My Oracle Support (support.oracle.com).	See the topic: How You Signing In for the First Time.
Sign in and reset your temporary password	If you haven't done so already, sign in and reset your temporary password. Click the user initials on the Welcome page, and select Set Preferences from the menu.	See the topic: How can I change or reset my password?
Enable the Customer Data Management offering for implementation	Enable the Customer Data Management offering and its functional areas for implementation in the Setup and Maintenance work area.	See the topic: Enable Customer Data Management Features for Implementation.
Ascertain that you have the required licenses	Verify that you have all the additional licenses required for your implementation of the Customer Data Management capabilities.	See the topic: Verify the Need for Additional Licenses.
Install the Customer Data Management Implementation Project	Install the Customer Data Management implementation project into your test environment to speed up your access to the implementation tasks. You can download the implementation project from My Oracle Support (support.oracle.com) and upload it into your environment.	See the topic: Enable Quick Access to Setup Tasks With an Implementation Project.

How You Sign In for the First Time

As part of your subscription, you're provisioned two Customer Data Management Cloud environments, production and test.

When your test environment is ready, Oracle sends a Welcome e-mail to the person designated as the administrator when you signed up with the Oracle Customer Data Management Cloud service.

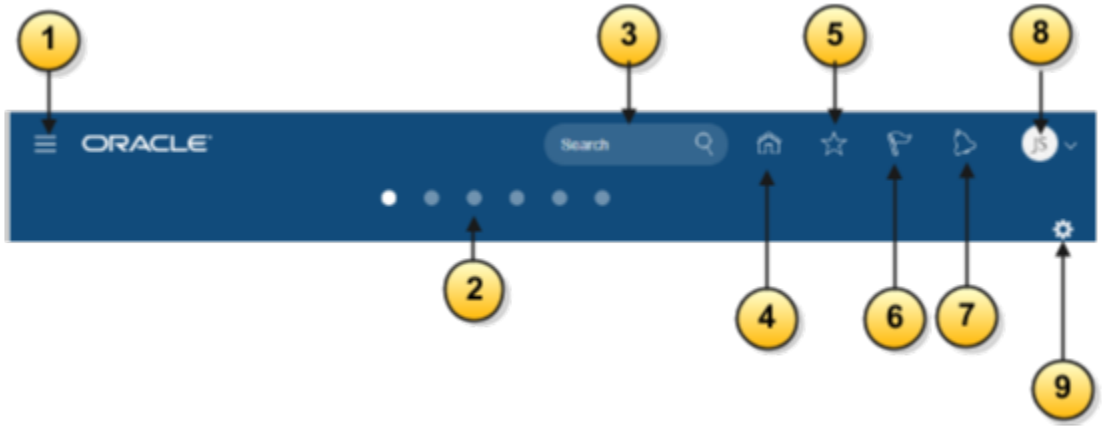
The Welcome e-mail to the administrator for the Oracle Customer Data Management Cloud contains all the details about your test and production environments, login credentials, and an Action List. Before you sign in for the first time, read the environment access e-mail, complete the tasks in the Service Administrator Action List, and familiarize yourself with the different user interfaces and basic navigation.

When you sign in for the first time, reset your password by clicking your user initials at the top-right of the Welcome page and selecting **Set Preferences** from the **Settings and Actions** menu.

Related Topics

Home Page Icons and What They Can Do

You can use the icons on your application's home page for navigation, search, configuration, and other tasks that are common across applications. Here are a few icons useful to your setup.



This table consist of a list of Home Page icons and their functions that will help you understand their usability::

Callout Number	Icon Name	Function
1	Navigator	You can use it to quickly get to the most frequently used work areas and tools.
2	Page Controls (The series of dots arranged horizontally in the center of the Home page.)	You can use these to toggle between the Welcome Springboard and the Quick Actions page. • The Welcome Springboard page has links to the most frequently used work areas and tools. • The Quick Actions page provides quick access to tasks. You can determine which of these pages should be displayed as the home page for users.

Callout Number	Icon Name	Function
3	Global Search	Let's you search transactional data across different objects. This field doesn't appear until you enable global search.
4	Home	Returns you to the page defined as the home page. By default, home is the Welcome Springboard page displaying the different work area icons.
5	Favorites and Recent Items	Marks a page as favorite and provides access to recently viewed pages.
6	Watchlist	Not used in the Customer Data Management Cloud application. Watchlist enables the tracking of business objects in some applications.
7	Notifications	Accesses application notifications. Some of these are also delivered using e-mail.
8	User image or Initials	Opens the Settings and Actions menu. From the menu, you can sign out, personalize and configure the User Interface, turn on and access help, and navigate to the Setup and Maintenance work area.
9	Personalize Springboard	Permits you to select which icons you want on the Welcome Springboard page. Your changes affect your springboard view only.

You can get more information on using common application features from the Oracle Applications Cloud Using Common Features guide.

How You Access Setup Tasks

You can access your set up tasks in several different ways:

- Use an implementation project provided by Oracle.
- Open tasks from the Customer Data Management offering Setup page, Setup: Customer Data Management, in the Setup and Maintenance work area.
- Use the Navigator to get to tasks from other work areas such as My Team, Tools, and Configuration.

Access Setup Tasks Using the Implementation Project

You can quickly access the setup tasks covered in the Getting Started with Your Oracle Customer Data Management Cloud Implementation guide by downloading and installing an implementation project provided by Oracle. The implementation project complements the structure of this guide and provides a direct link to each setup task.

If you don't use the implementation project, then you can navigate to some individual setup tasks from the functional areas on the **Setup: Customer Data Management**page and to others from the work areas on the **Navigator**.

Access Your Tasks Using the Setup Page

After you enable the Customer Data Management offering, you can open implementation tasks, including those not covered in this guide, from the Setup and Maintenance work area Setup page. Here is how:

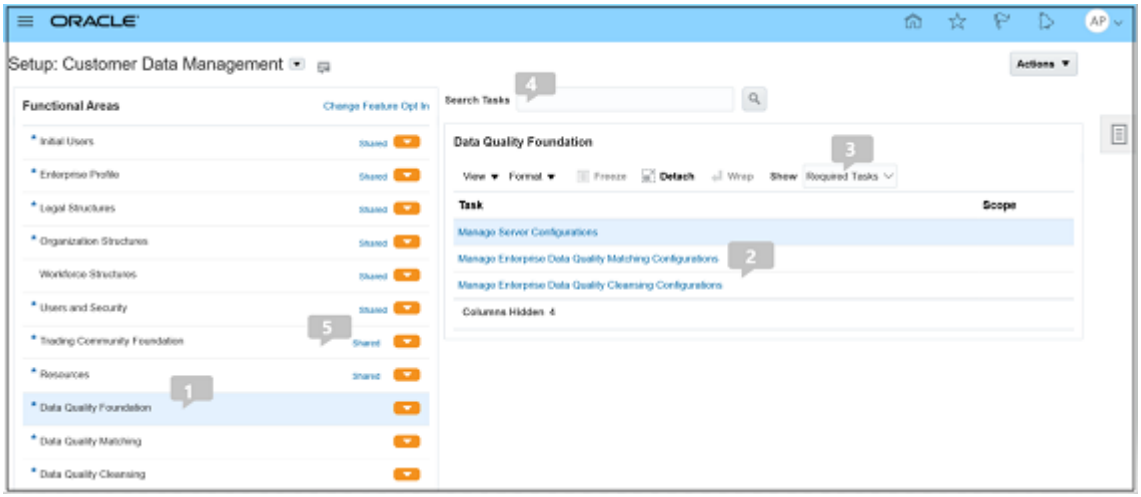
1. Click the **Setup and Maintenance** icon.

2. In the Functional Areas column, select the functional area you want to set up.

   Here's a description of the features on the Setup: Customer Data Management page.

Callout Number	Description
1	Selected functional area.
2	Listing of tasks for the functional area you selected.
3	By default, the page shows the required tasks for the functional area, but you can display all tasks.
4	You can search for tasks in the offering using the Search Tasks field.
5	Clicking the Shared link list other offerings using the same functional area.

Callout Number	Description



3. You can open tasks by clicking on their names in the **Task** list. By default, you see only the required tasks, but you can select All Tasks from the Show menu to see them all.
4. You can also search for tasks in the offering by name using Search Tasks. Use the percent sign (%) to represent missing letters or words. For example, to find the Run Maintain Geography Name Referencing task, you can search for Run % Geography % Referencing. The searches aren't case-sensitive.

Navigate to Other Work Areas for Setup

When you're not using the implementation project, you can use the Navigator to access setup tasks from other work areas involved in setup. You can open the Navigator by clicking its icon in the toolbar.

The Navigator doesn't display all the features, but only the ones that are available based on the permissions assigned to each pre-defined application user. Aside from the Setup and Maintenance work area, you use only a small number of the available work areas accessible from the Navigator menu. The most important of these include:

- My Team
  - Users and Roles
    Use this work area for creating and managing individual users in the UI. Another way of navigating to this work area is by using the Manager Users task in the Setup and Maintenance work area.
- Tools
  - Scheduled Processes
    Use this work area for scheduling and monitoring background processes.
- Configuration
  - Appearance
    Let's you control application appearance, including background color and icon shape.
  - Structure
    Let's you control the items that appear in the Navigator and on the Welcome page.

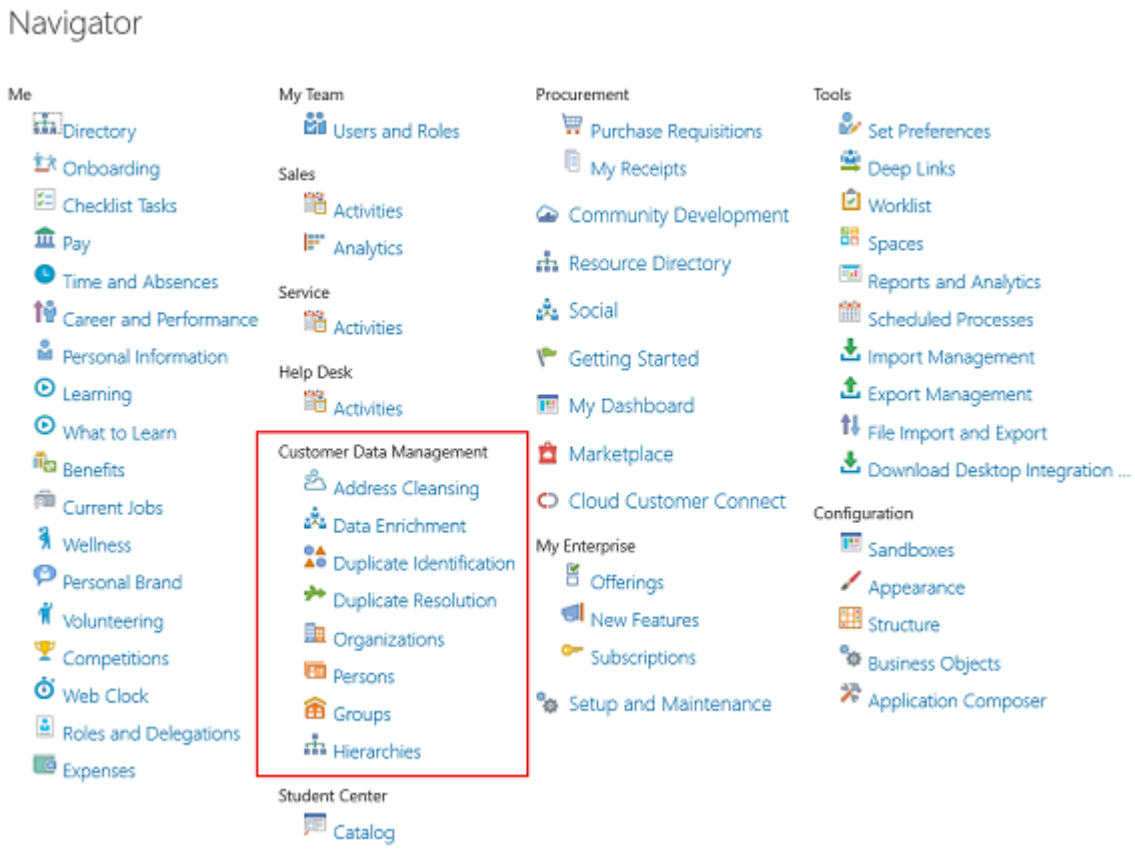
- Application Composer

  Use Application Composer to configure and enhance your application.

- Customer Data Management

  Use the different work areas under this heading for functional setup and to create data used to test your Customer Data Management application.

  Here's an image of a Navigator menu, which lists a set of tasks by default. You can configure the Navigator to show only the tasks that you need.



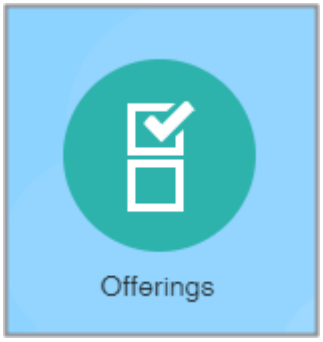
Enable Customer Data Management Features for Implementation

Before you start work, you must enable the Customer Data Management offering and its functional areas that you want to implement. Enabling the offering and its functional areas provides access to setup tasks.

You need to enable only the functional areas you're implementing now and, if required, add more later on.

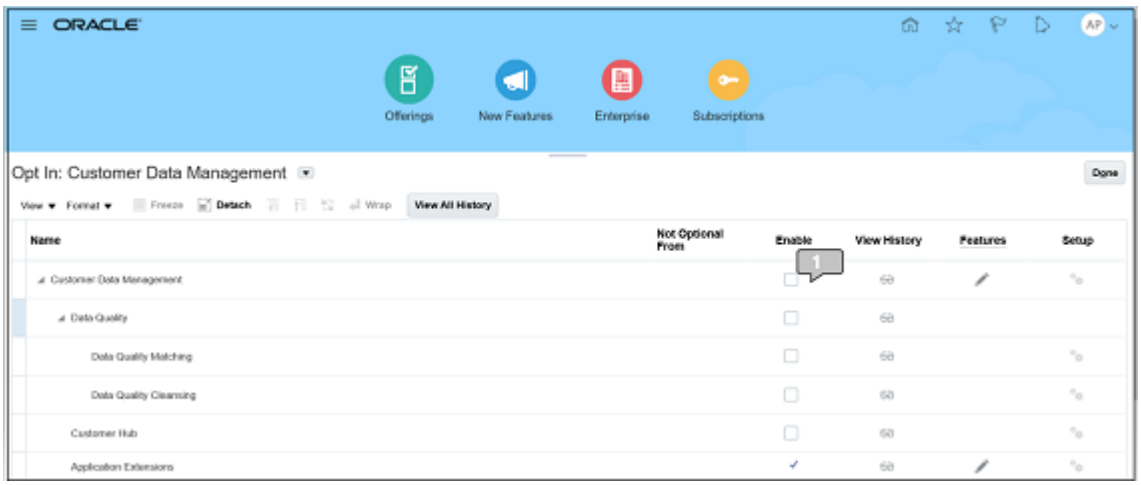
To enable the Customer Data Management offering and its functional areas:

1. Click the **My Enterprise** icon on the Home page, and select **Offerings**.



2. Click the **Customer Data Management** offering icon (callout 1 in the image below).

3. Click **Opt In Features** (callout 2).
4. On the Opt In: Customer Data Management page, select the **Enable** option for Customer Data Management, the folder at the top of the list (callout 1 in the image below). Your selection enables the offering.



5. Select the **Enable** option, for all the Customer Data Management functional areas you plan to set up. For the implementation of Customer Data Management documented in this guide, enable all of the functional areas: Data Quality, Data Quality Matching, Data Quality Cleansing and Customer Hub.

6. Click **Done**. You're returned to the Offerings page.
7. Click Home in the global header to return to the Welcome page.

Verify the Need for Additional Licenses

You can only enable the functional areas for which your company has purchased licenses.

Customer Data Management is shipped free of cost with some Oracle Cloud Services such as Sales and B2B Service. A Sales and B2B Service license provides you access to the following customer data management functionality:

- Data Steward Productivity Tools
- Reporting and Analytics
- Audit Reporting
- Customer Hub
- Customer Hierarchy Management

To make use of Data Quality, Enrichment, and Address Cleansing capabilities, you require the following additional licenses:

- Oracle Fusion Data Quality Cloud Service: This service enables you to identify and resolve potential duplicates records in the database or potential duplicates of the records in the database within an import batch. You can use this service for both real-time and batch duplicate identification.
- Oracle Address, Email, and Phone Verification: This service enables you to cleanse an address to conform to postal requirements and verify that the address is an actual postal address.
- Oracle Account Enrichment Cloud Service and Oracle Contact Enrichment Cloud Service: These services enable you to enrich account and contact data to ensure it's comprehensive.

Enable Quick Access to Setup Tasks with an Implementation Project

This guide describes how to speed up your initial setup using an implementation project supplied by Oracle.

The implementation project serves as a launch pad for many of the setup tasks covered in this guide, so you don't have to search for individual setup tasks or navigate to work areas, including the scheduled processes.

Downloading the Implementation Project to Your Desktop

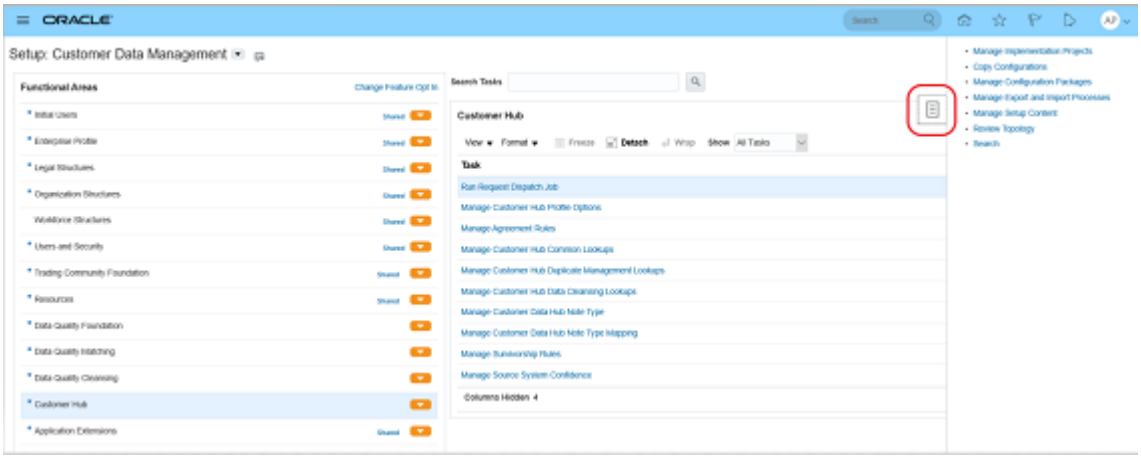
Download the implementation project to your desktop from the Oracle Customer Data Management Cloud: Quick Setup Customer Data Management Cloud Service: Implementation Project (Doc ID 2587374.1) available on support.oracle.com.

Install the Implementation Project You Downloaded

Use these steps to install the implementation project:

1. Navigate to the Setup and Maintenance work area.

2. Click the Tasks panel tab icon that's highlighted in the following image.



3. Click the Manage Configuration Packages task link in the panel tab.
4. On the Manage Configuration Packages page, click Upload.

   The Upload Configuration Package page appears.
5. On the Upload Configuration Package page, click Browse and select the compressed file with the implementation project you downloaded.
6. Click Get Details.

   Click Done on the Manage Configuration Packages page.
7. Click Submit.

   The application displays a message that the import is successful and the implementation project was created.
8. Click OK to close the message window.
9. Click Done on the Manage Configuration Packages page.

   You are returned to the Setup and Maintenance work area page.
10. Click the Tasks panel tab icon again and click Manage Implementation Projects.
11. On the Implementation Projects page, click the name link to open the implementation project.

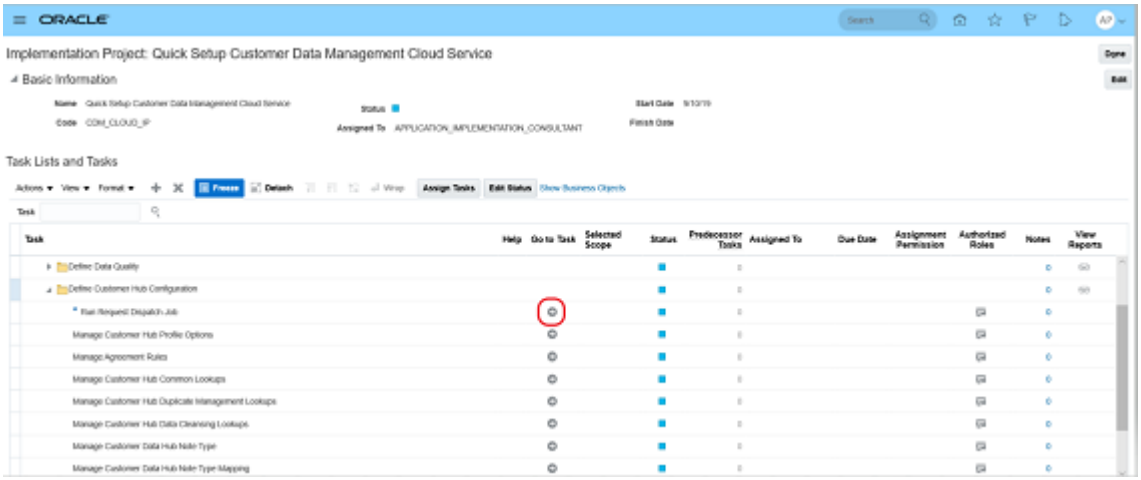
Use the Implementation Project As a Launchpad for Your Tasks

Complete these steps to use the implementation project to access your implementation tasks.

1. Navigate to the Setup and Maintenance work area by clicking the icon on the Welcome Springboard.
2. Click the Task panel tab icon.
3. In the panel tab, click Manage Implementation Projects.

4. On the Implementation Projects page, click the name link for the project.

   The implementation project displays the folders containing the individual tasks in the Task Lists and Tasks region. Here's an image of the Quick Setup Customer Data Management Cloud Service implementation project, highlighting the Go to Task icon.



5. Click a folder to open it and click the Go to Task icon for a task.

   When you complete a task, you are returned to the project.

3 Configure User Account Preferences

Overview of User Account Preference Setup

Review the settings for user name format and password strength and set up notifications before you create your first users. By default, the application uses the e-mail address to create user names and requires passwords with eight letters and one number.

You may want shorter user names and stronger passwords. You may also want to create your own versions of the notifications users receive regarding their accounts. Oracle provides sample notifications, but they include Oracle-specific language.

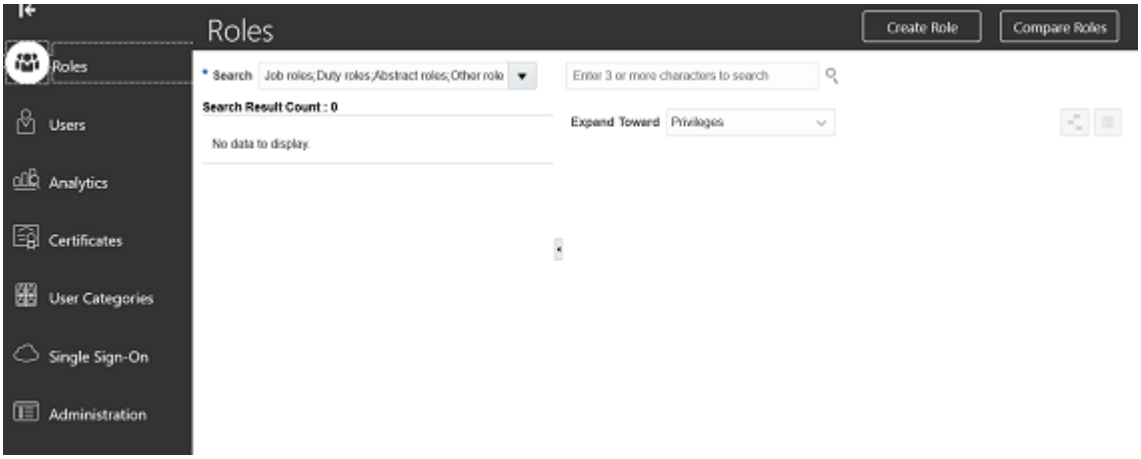
The Security Console you use for all these tasks includes many advanced features. Some don't even apply to your customer data management application. So, limit your use of the Security Console to the tasks listed here. You can open them from the implementation project.

Step	Description	Task Name	Where to Get More Details
Initialize the Security Console.	Initialize the Security Console by running the process Import Users and Roles into Application Security.	Import Users and Roles into Application Security	See the topic: How You Initialize the Security Console
Set up user account preferences.	Set up preferences for user name format, passwords, and create notifications.	Security Console	See the topic: Set Up User account preferences

Security Console Tabs and Their Uses

The Security Console is a powerful tool. Here's an overview of the Security Console tabs and their uses.

Only setup users, or other users with the IT Security Manager job role, can access the Security Console. Keep in mind that the initial setup comes with default settings but can be configured based on your needs.



Tab	Usage
Roles	Create your own roles as described in this guide.
Users	Manage user passwords and update user e-mail addresses. Don't use this tab to create users or to provision job roles. For customer data management, you must follow the instructions in the rest of this guide to create users, provision job roles, and change user names. Note that all users, even members of the resource organization who can't access the Security Console, can reset their own passwords. That's done by clicking the user name in the welcome page and selecting the Preferences option from the Settings and Actions menu.
Analytics	Review role assignments and compare roles.
Certificates	The customer data management application doesn't use this functionality.
User Categories	Specify password policies and manage notifications users receive about their accounts and passwords. You can specify different behavior for different categories of users. For the customer data management application, all the users you create are initially assigned to the Default category. But you can create additional user categories and move users to them.
Administration	Use to set role copying preferences and other advanced features.

How You Initialize the Security Console

You must initialize the Security Console before using it for the first time by running the process Import Users and Roles into Application Security.

The process copies users, roles, privileges, and data security policies from the LDAP directory, policy store, and Applications Core Grants schema to Oracle Cloud Applications Security tables. Having this information in the tables

makes the search feature of the Security Console fast and reliable. After the process completes the first time, Oracle recommends that you schedule the process to run daily.

1. Open the **Import Users and Roles into Application Security** task from the **Set Up Security Console and Preferences** folder in the implementation project. Alternatively, you can search for the task by name in the Setup and Maintenance work area using the following:
    - Offering: Customer Data Management
    - Functional Area: Initial Users
    - Task: Import Users and Roles into Application Security
2. On the Import Users and Roles into Application Security page, click **Submit**.

    This action starts the Import User and Role Application Security Data process. After the process completes, you can use the Security Console.
3. Now set up this same process to run daily:
    - On the Import Users and Roles into Application Security page, click **Advanced**.
    - Click the **Schedule** tab.
    - Select the Using a schedule option.
    - From the **Frequency** list, select **Daily**.
    - Enter an end date far in the future.
    - Click **Submit**.

Set Up User Account Preferences

Use the Security Console to set your preferences for user names, passwords, and user notifications. For example, you can require users to set stronger passwords, implement shorter user names, change the text of the notifications your users receive, or turn notifications off completely.

Specify Preferences for User Names and Passwords

You can set your preferences for user names, passwords, and user notifications by following the giving steps:

1. Open the Security Console using the **Manage Applications Security Preferences** task from the **Set Up Security Console and Preferences** folder in the implementation project. You can also click **Tools > Security Console** on the home page. Alternatively, you can search for the task by name in the Setup and Maintenance work area using the following.
    - Offering: Customer Data Management
    - Functional Area: Initial Users
    - Task: Manage Applications Security Preferences
2. Click **User Categories**.

    On the User Categories tab, you can set up different preferences and notifications for different categories of users. Since all of the customer data management users you create and import are created in the Default category, you set preferences for that category only.

3. Click **DEFAULT**.

   The DEFAULT User Category: Details page appears. Here you can set the user name format.
4. Click **Edit**.
5. Select the user name format you want to use from the **User Name Generation Rule** list.

   The application uses your selection to generate user names if you don't enter them manually or import them from a file. By default, the application uses the e-mail address as the user name. If you're implementing Partner Relationship Management, then you must use e-mail for creating partner contacts. Otherwise, you can use any of the three following options:

   - FirstName.LastName (First name.last name)
   - Email
   - FLastName (First initial and last name)

   Don't use **Person or party number** because numbers aren't easily remembered by users. For example, if the person number generated by the application for John Smith is 100000000178803, then the user name is 100000000178803 as well.
6. Select the **Generate system user name when generation rule fails** option to ensure the application generates a user name even if there is no information available for the option you selected.
7. Click **Save and Close.**
8. Click the **Password Policy** subtab.
9. Here you can specify password strength and expiration. For example, you can require users to use special characters in passwords and specify how frequently passwords must be changed.
10. Selecting the **Administrator Can Manually Reset Password** option, makes it possible for administrators to manually create new passwords for users.
11. Click **Save and Close**.

Configure the E-mail Notifications

In the Notifications subtab on the DEFAULT User Category tab, you can specify which e-mail notifications, if any, are sent to users and the text of those notifications. At present, the application supports text-only notifications in one language.

You can make these changes:

- Turn all notifications on or off.

  By default, all notifications are turned on. If you're setting up a test environment, turn off notifications while creating customer data management users to prevent the users from signing in to the application while you're setting it up.
- Turn individual notifications on or off.

  By default, all individual notifications are turned on.
- Create your own notifications.

  Oracle provides predefined English-language templates with Oracle-specific language. You can create your own templates.

Here's how to configure the e-mail notifications for the DEFAULT User Category:

1. Click the **Notifications** subtab.

The subtab lists the default notification templates provided by Oracle. The list includes the events that trigger the notifications and the e-mail subject lines.

2. To make changes, click **Edit**.
3. If you want to turn off all notifications, then deselect the **Enable Notifications** option under the **Notification Preferences** heading.
4. If you want to turn off individual notifications, then:
    - Click the template name link.
    - Deselect the **Enabled** check box.
    - Click **Save and Close**.
5. Here's how to create your own notification templates:
    a. Click **Add Template** and select the event.

    Selecting the event automatically copies over the text provided in the corresponding Oracle template that you can then edit.

    b. Edit the notification subject line and text.

    Here's a list of the tokens you can include in the message text. Each token must be within curly brackets and preceded by a dollar sign, for example: ${firstName}.

Token	Meaning
notificationUserName	User name to which notifications are sent
userEmailAddress	Address to which e-mail notifications are sent
userLoginId	User name
firstName	User's first name
lastName	User's last name
managerFirstName	Manager's first name
managerLastName	Manager's last name
loginURL	URL where you can sign in
resetURL	URL where you can reset the password
CRLFX	New line

Token	Meaning
SP4	Four spaces

c. Select the **Enabled** option.
d. Click **Save and Close**.

   The predefined template provided by Oracle is automatically disabled. You can only have one template for each event.

6. On the DEFAULT Category: Notifications page, click **Done**.

Set the Synchronization Process Frequency Warning

Whenever you navigate to the Security Console, the application warns you if the Import User and Role Application Security Data process wasn't run in the last six hours. If you scheduled the process to run daily, then it makes good sense to change the value of the warning as well.

1. Click the **Administration** subtab.
2. Change the value for the **Hours Since Last Synchronization Job Run Warning**.

4 Create Setup Users

Overview of Setup User Creation

As the initial user created by Oracle, you can perform security tasks, such as creating other users and granting setup permissions.

After you have signed in for the first time, you're ready to create any other users you need to help you with the application setup. You can also grant yourself the additional setup permissions you need to complete the setup tasks covered in this guide.

Here is a list of the setup tasks to create setup users. You can access these tasks from the Create Setup Users folder in your implementation project.

Step	Description	Task Name	Where to Get More Details
Create a job for Provisioning Setup Users	Create a job, Customer Data Management Setup User, which you can later assign to all users who are performing setup and aren't part of your resource organization. What you name the job doesn't matter. You use the job only as a condition in the rule to provision setup users with the permissions they require to complete all setups.	Manage Job	See the topic Create a Job for Provisioning Setup Users.
Create a rule to provision roles to that job	Create a role provisioning rule that automatically provisions the following job roles to all users with the Customer Data Management Setup User job: • Application Implementation Consultant • IT Security Manager • Application Diagnostic Administrator • Master Data Management Application Administrator	Manage HCM Role Provisioning Rules	See the topic Create the Provisioning Rule for Setup Users.
Create setup users and associate the job and roles to them.	Create each setup user as a user of type employee with the Customer Data Management Setup User job and associate the roles to them.	Manage Users	See the topic Creating Setup Users.
Grant the Initial User the Same Privileges as Other Setup Users	Grant yourself, the initial user, the same additional privileges the	Manage Users	See the topic Grant the Initial User the Same Privileges as Other Setup Users.

Step	Description	Task Name	Where to Get More Details
	other setup users have by editing the initial user profile.		

Setup Users and Security

Although the initial user can perform many of the setup tasks in this guide, this user can't perform all of them without additional privileges. For example, the initial user can't run scheduled processes.

How Permissions Are Grouped and Provisioned

Oracle follows the industry standard Role Based Access Control approach to security. In Oracle Applications Cloud, the privileges are bundled in:

- Job roles, which correspond to the jobs that the person is doing in your organization.
- Abstract roles, which permit users to carry on tasks that are common to all employees or resources.

For example, the Data Steward Manager job role makes it possible for a user to perform all of the customer data steward manager duties, such as reviewing and assigning duplicate identification batches and duplicate resolution requests to customer data steward. The Employee abstract role adds the ability to access reports and manage personal profile information. The Resource abstract role makes it possible for a user to be assigned as a resource to the customer data management department.

Security Roles Required by Setup Users

To perform the setup tasks mentioned in this guide, you must provision setup users with all the job roles granted to the initial user. These job roles are:

- Application Implementation Consultant (job role)
  Provides access to all the setup tasks across all products.
- IT Security Manager (job role)
  Provides access to the security tasks, including the ability to assign other enterprise roles.
- Application Diagnostics Administrator (job role)
  Provides access to the diagnostic tests and data.

In addition, you also need to provision them with:

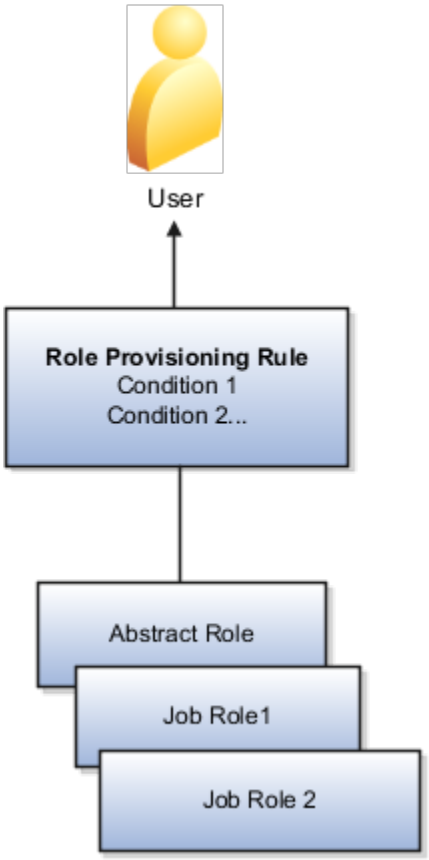
- Employee (abstract role)
  Provides the ability to run and monitor background processes and manage personal profile information.
- Master Data Management Application Administrator (job role)
  Permits the setup user to perform the same functional setups as a customer data management application administrator.

To perform the setup tasks in this guide as the initial user, you must provision these additional roles to yourself as well. While the initial user can create other users and perform many setup tasks, the initial user can't complete all the tasks without the additional security roles.

About Role Provisioning Rules

In Oracle Customer Data Management Cloud, you provision job roles and abstract roles to users using role provisioning rules. If users meet the conditions of the rule, the application provisions them with the job roles and abstract roles that you want to assign to the user.

The following figure shows how the role provisioning rule conditions must be met to provision the job roles and abstract roles.

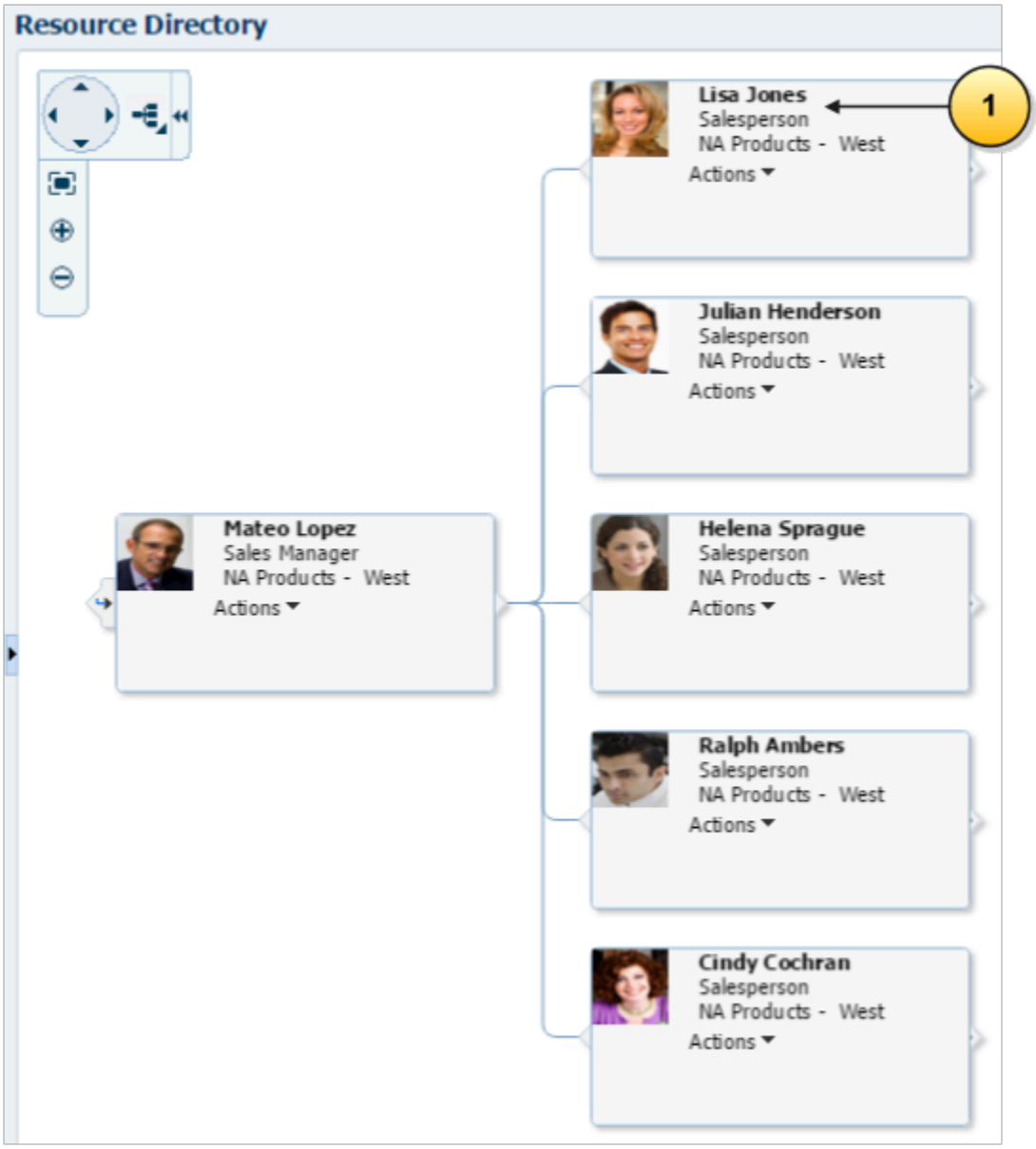


The role provisioning rules you use to provision customer data management application users and the initial setup users have different conditions.

How You Provisioning Customer Data Management Application Users

You provision job roles to customer data management users, such as data steward managers and customer data steward based on the role the user plays in the resource organization. This resource role is the job title, which appears under the user name in the Resource Directory.

The following figure shows resource directory page with the resource role appearing as job tittle under the user name highlighted with the callout 1.



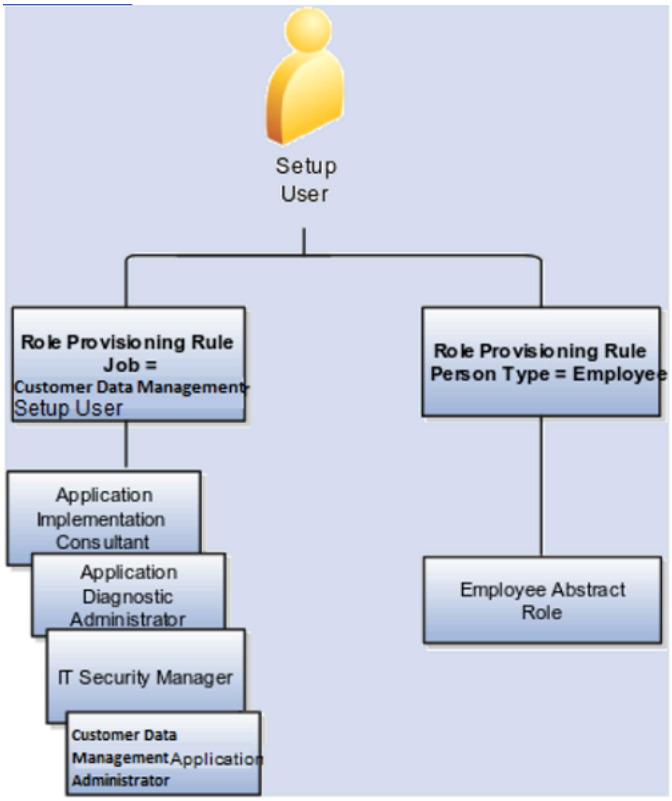
How You Create a Special Provisioning Rule for Setup Users

As users doing the initial setup aren't part of your company's resource organization, you don't want them to be a part of the resource hierarchy and you don't want them to appear in the Resource Directory. For these reasons, you don't create setup users as resources, and you don't assign them resource roles.

Because setup users don't have resource roles, you must create a special role provisioning rule that uses a different field as the condition. You create a Customer Data Management Setup User job, a field not normally used in Oracle Customer Data Management Cloud, and provision the setup user with job roles based on this job. You need to provision these roles to the Customer Data Management Setup User job: Application Implementation Consultant, Application Diagnostic Administrator, It Security Manager, and Master Data Management Application Administrator.

How You Provision Setup Users

The following figure illustrates the two provisioning rules used to provision the Customer Data Management Setup User job role and employee abstract role to the setup user. The employee role provisioning rule is already set up for you by Oracle unless you're implementing your application in a Global Single Instance environment. In GSI environments, you must set up all provisioning rules yourself.



What Happens When You Create Users

When you create users, Oracle Customer Data Management Cloud:

- Creates accounts, user names, and temporary passwords
- Provisions the job roles and abstract roles the users require to carry out their jobs
- Sends users an e-mail with their sign-in credentials

Tip: System notification e-mail, including the initial e-mail with sign-in information, don't include the URL for accessing Oracle Customer Data Management Cloud. You must provide this URL to users separately.

Create a Job for Provisioning Setup Users

Here's how you can create a job that you can use to assign setup users with implementation privileges. You use this job as a condition in the provisioning rule you create and assign the job to the users.

You can create a job by carrying out the given steps:

1. Sign in as the initial user.
2. If you have downloaded and imported the implementation project, then open the task Manage Job from the implementation project. Alternatively, you can access the Manage Job task from the Setup and Maintenance work area using the following:
    - Offering: Customer Data Management
    - Functional Area: Workforce Structures
    - Task: Manage Job

    Alternatively, you can search for the same task in the Setup and Maintenance work area using these steps:

    a. Click Navigator > Setup and Maintenance work area.
    b. In the Setup page, select Search from the Tasks panel tab.
    c. In the Search page, enter Manage Job and click the search icon

    To open the task from the implementation project:

    a. Navigate to the Setup and Maintenance work area by clicking the **Setup and Maintenance** icon on the springboard. The springboard is the page you see when you first sign in.
    b. Click **Implementation Projects**.
    c. In the Search Results region on the Implementation Projects page, click the name link for the project.
    d. Open the Create Setup Users folder.
    e. Click the **Go to Task** icon for the **Manage Job** task.

    The Manage Jobs page appears.
3. Click **Create**.

    The Create Job: Basic Details page appears.
4. Enter **Customer Data Management Setup User** in the Name field.
5. Enter a name without spaces, for example **CDM_Setup_User**, in the Code field.
6. Enter Common Set in the Job Set Field.
7. You can keep the other field values as they're because you're creating this job only for the purposes of provisioning job roles to setup users.
8. Click **Next** until you reach the end of the process train.
9. Click **Submit** on the last page, and close the warning by clicking **Yes**.

The job may take a couple of minutes to create. You can use search on the Manage Job page to check that it has been created.

Create the Provisioning Rule for Setup Users

Here's how you can create the provisioning rule which automatically provisions users assigned the Customer Data Management Setup User job with the job roles required to perform the initial setup in this guide.

To create the provisioning rule:

1. Sign in as the initial user and open the **Manage HCM Role Provisioning Rules** task from the implementation project. Alternatively, you can search for the task by name in the Setup and Maintenance work area.
    - Offering: Customer Data Management
    - Functional Area: Users and Security
    - Task: Manage HCM Role Provisioning Rules
2. On the Manage Role Mappings page, click **Create**.
   The Create Role Mapping page appears.
3. In the **Mapping Name** field, enter **Customer Data Management Setup User**, or another name that will help you identify this mapping in the future.
4. In the Conditions region, select **Customer Data Management Setup User**, the job you created earlier, from the **Job** list. If the job doesn't appear in the list, click **Search** and search for it using the full name.
5. Select **Active** from the **HR Assignment Status** list.
   This additional condition ensures that any provisioned job roles are automatically removed if the user is terminated.
6. In the Associated Roles region, click **Add** and select each of the following job roles:
    - Application Implementation Consultant
    - IT Security Manager
    - Application Diagnostics Administrator
    - Master Data Management Application Administrator
7. Make sure the **Autoprovision** option is selected for all the job roles.
8. Click **Save and Close**.

Create Setup Users

After you have created the provisioning rules, you're ready to create other setup users in the UI.

To create a setup user:

1. Open the **Manage Users** task in the implementation project. You can also click the **Users and Roles** link under the **My Team** heading in the Navigator to access this task. Alternatively, you can access it from Setup and Maintenance work area using the following:
    - Offering: Customer Data Management
    - Functional Area: Users and Security
    - Task: Manage Users
2. On the Manage Users page, click **Create**.
   The Create User page appears.
3. Enter the user's name and a unique e-mail in the Personal Details region.
   The application automatically sends the initial sign-in credentials to this e-mail when you save the record.
4. In the User Details region, enter the user name.

> **Note:** If you leave the **User Name** field blank, then the application automatically creates a user name for you. By default, the application uses the e-mail as the user name.

5. In the User Notification Preferences region, select the **Send user name and password** option. The option to send the user name and password through e-mail is available only before you save the user record for the first time. You don't see the User Notification Preferences region and can't change your selection after you create the user.

> **Note:** If you don't select this option, the application doesn't send the initial password to the user and you must reset the user password manually using the procedure described in the Reset User Passwords topic.

6. In the **Employment Information** region, enter the following:
    - Select **Employee** from the **Person Type** list.
    - From the **Legal Employer** list, select the only value available, the legal employer Oracle created for you using the information you provided when you signed up with Oracle Customer Data Management Cloud. The Legal Employer name is typically your company name followed by the letters LE.
    - From the **Business Unit** list, select the only value available, the business unit created for you when you signed up. The Business Unit is typically your company name followed by the letters LE BU.
    - From the **Job** list, select **Customer Data Management Setup User**, the job you just created. If the job isn't in the list, then you must search for it by clicking **Search**.
7. Click **Autoprovision Roles**

    The **Role Requests** region displays the following roles:
    - Application Diagnostics Administrator
    - Application Implementation Consultant
    - IT Security Manager
    - Employee
    - Master Data Management Application Administrator
    - Human Resource Manager - View All

    The role request process may take a few minutes to complete because it's fulfilled by a process which is set to run periodically. You can view the status of the request any time you edit this user. When the process is complete, the roles appear in the Current Roles region.
8. Click **Save and Close**.

    If you haven't selected the **Send user name and password** option, then you must reset the password using the procedure described in the Reset User Passwords topic.

    Tip: The e-mail with the user name and password doesn't include the URL of your application. You must provide the URL to users separately.

Grant the Initial User the Same Privileges as Other Setup Users

Use this procedure to grant the initial user the same privileges as the other setup users:

1. Open the Manage Users task in the implementation project. You can also click the **Users and Roles** link under the **My Team** heading in the Navigator to access this task. Alternatively, you can access it from Setup and Maintenance work area using the following:
    - Offering: Customer Data Management
    - Functional Area: Initial Users
    - Task: Create Implementation Users
2. Enter the first name of the initial user in the **Keywords** field and click Search.
3. Select the name link in the Search Results.

    The Edit User page appears.
4. In the **Employment Information** region, select **Customer Data Management Setup User** (or the name that you gave for the job) from the Job list. This is the job you created earlier. If the job isn't listed, then click **Search** and search for it by name.
5. Click **Autoprovision Roles**.

    The **Role Requests** region displays the following roles:
    - Employee
    - Master Data Management Application Administrator

    Your role request process may take a few minutes to complete because it's fulfilled by a process which is set to run periodically. You can view the status of the request any time you edit this user. When the process is complete, the roles appear in the Current Roles region.
6. Click **Save and Close**.

    If you're signed in as the initial user, you must sign in again for the new privileges to take effect.

Reset User Passwords

You can use the Users tab in the Security Console work area to reset user passwords. Only setup users, and other users with the IT Security Manager job role, can access the Security Console.

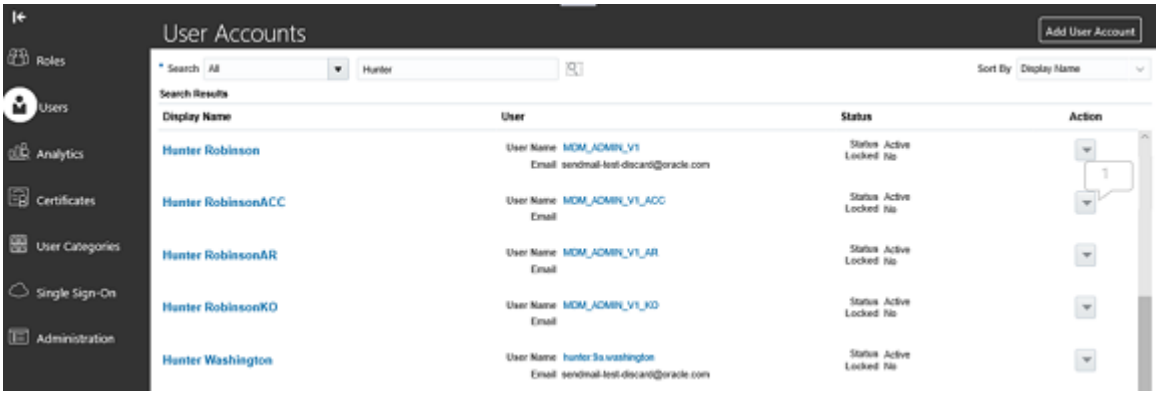
> **Note:** All users can reset their own passwords by clicking their user name or image, and selecting the Set Preferences link in the Settings and Actions menu. They can also reset their passwords by using Forgot Password on the sign-in page.

To reset password in the Security Console:

1. While signed in as a setup user, navigate to Tools and then to the Security Console work area. Alternatively, in **Setup and Maintenance**, go to the following:
    - Offering: Customer Data Management
    - Functional Area: Initial Users
    - Task: Create Implementation Users

    You can close any warnings regarding the scheduling of the Import Users and Roles Application Security Data job.
2. Click the **Users** tab.
3. Search for the user using one of the following:
    - First or last name, but not both
    - User name

    The following figure shows the Users tab in the Security Console work area.



4. From the **Action** menu (callout 1 in the preceding figure), select **Reset Password**.

    The Reset Password window displays the password strength policy.
5. If you want the application to send an e-mail to users with a URL that they can use to create their own passwords and sign in to the application, then select the **Automatically generate password** option.

    Note that you can select the option to manually reset your password while editing the password policy for the DEFAULT user category in the Security Console.
6. If you want to change the password yourself, then:
    a. Select the **Manually change the password** option
    b. Enter the new password twice.
7. Click **Reset Password**.

Update E-mail Addresses

Use the Users tab in the Security Console work area to change e-mail addresses for Customer Data Management Cloud users. Only setup users, and other users with the IT Security Manager job role, can access the Security Console.

1. Open the Security Console from under **Tools**. Alternatively, you can access it from Setup and Maintenance work area using the following:
    - Offering: Customer Data Management
    - Functional Area: Initial Users
    - Task: Create Implementation Users
2. Click the **Users** tab.
3. Search for the user using one of the following:
    - First or last name, but not both
    - User name
4. Click the user name link.
5. On the User Account Details window, click **Edit**.
6. In the Edit User Account window, edit the e-mail address.

    > **Note:** Don't edit any of the other information available on the Edit User Account page. Use the Manage Users task instead.

7. Click **Save and Close**.

Provide Users Permissions to View All Scheduled Processes

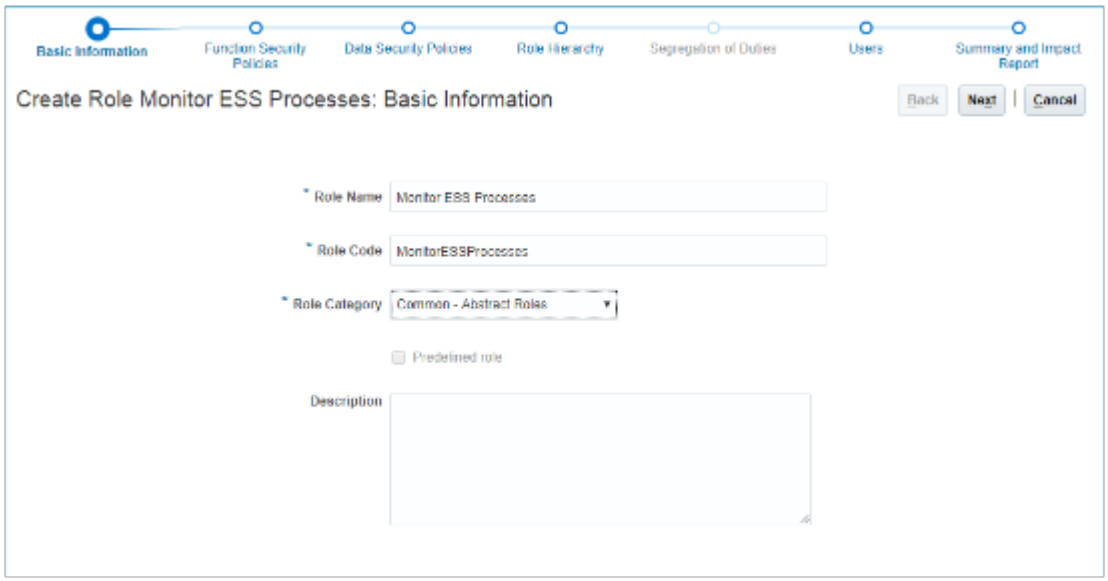
Your application setup requires you to run numerous scheduled processes and ensure they complete successfully.

By default, users can only see the scheduled processes they themselves submit. By creating a custom role in the Security Console and assigning all of the setup users to it, you ensure that everyone can see what processes are running and their status, no matter who submitted them.

1. Open the **Security Console** from under Tools. Alternatively, you can access it from Setup and Maintenance work area using the following:
    - Offering: Customer Data Management
    - Functional Area: Initial Users
    - Task: Create Implementation Users
2. Click the **Roles** tab.

3. On the Roles tab, click **Create Role**.

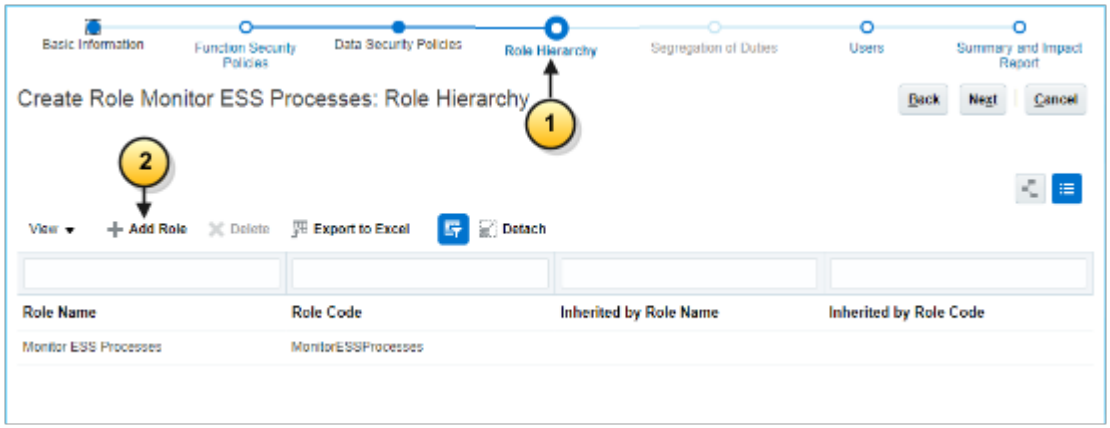
   The Create Role page displays a series of steps you can click directly or reach using the **Next** button.



4. In the Create Role: Basic Information step, make the following entries:

Field	Suggested Entry
Role Name	Monitor ESS Processes
Role Code	MonitorESSProcesses
Role Category	Common -Abstract Roles

5. Click the **Role Hierarchy** step (callout 1 in the following image).



6. Click **Add Role** (callout 2).
7. In the Add Role Membership window, search for ESS Monitor Role and click **Add Role Membership**.

8. Click **Cancel** when you're done.
9. Click the **Users** step.
10. Click **Add User** and add all of the setup users by searching for each by name and clicking Add User to Role.
11. Click **Cancel** when you're done.

    The Users step should list all of the users you added.
12. Click **Next** to get to the Summary and Impact Report step.
13. Click **Save and Close**.

    The users you added to the role can now monitor all of the scheduled processes in the Schedule Processes work area.

5 Create Customer Data Management Application Users

Overview of Application Users Creation

You can broadly categorize Customer data management application users into three groups::

- **Managers Users**: These have the job role Data Steward Managers
- **Individual Users**: These have the job role Customer Data Stewards
- **Administrator Users:** These have the job role Master Data Management Application Administrator

Here's a table that lists the steps to create Customer Data Management users in the **Manager Users** page, which you can open from the Manage Users task in the implementation project.

Step	Description	Task Name	Where to Get More Details
Create Data Steward Managers	Create one or more Data Steward Managers depending on your business requirements.	Manage Users	See the topic: Create Customer Data Management Application Users.
Create Customer Data Stewards	Create one or more Customer Data Stewards depending on your business requirements.	Manage Users	See the topic: Create Customer Data Management Application Users.
Create Master Data Management Application Administrator	Create one or more Master Data Management Application Administrators depending on your business requirements.	Manage Users	See the topic: Create Customer Data Management Application Users.

Create Customer Data Management Application Users

You can use this procedure to create customer data management application users in the UI. To create a user, complete these steps:

1. While signed in as a setup user, open the **Manage Users** task from the implementation project. You can also open this task by clicking **Users and Roles** under the My Team heading in the Navigator. Alternatively, you can access the Manage Users task from the Setup and Maintenance work area using the following.
    - Offering: Customer Data Management
    - Functional Area: Users and Security
    - Task: Manage Users

2. Click **Create**. The Create User page appears.
3. Enter the user's first and last names and a unique e-mail address in the Personal Details region.

   The application normally sends the initial sign-in credentials to this e-mail when you save the record.
4. The application automatically fills the current date in the Hire Date field and uses that date as the start date for the resource.

   In the User Details region, enter the user name.

   If you leave the User Name field blank, then the application automatically creates a user name for you. By default, the application uses the e-mail as the user name.

   In the User Notification region, select the Send User Name and Password option. The option to send the user name and password through e-mail is available only before you save the user record for the first time. You don't see the User Notification Preferences region and can't change your selection after you create the user.

   > **Note:** If you don't select this option, the application doesn't send the initial password to the user and you must reset the user password manually using the procedure described in the Reset User Passwords topic.
5. In the User Notification region, leave the Send User Name and Password option selected if you want the credentials e-mail to be sent to the alternate user you specified.
6. Make the following entries in the Employment Information region:

   - Select Employee from the Person Type list.
   - From the Legal Employer list, select the legal employer Oracle created for you using the information you provided when you signed up with Oracle Customer Data Management Cloud. There should be only one value available: your company name followed by the suffix LE.
   - From the Business Unit list, select the business unit created for you when you signed up. There should be only one value available: your company name followed by the suffix BU.

   Neither the legal employer name nor the business unit name is visible in the application, so the names need not correspond to actual entities in your company.
7. In the Resource Information region, from the Resource Role list, select the role the user plays in your implementation. For example:

   - For Manager, Customer Data Management, select the predefined resource role Data Steward Manager.
   - For Customer Data Steward, select the predefined resource role Customer Data Steward
   - For Master Data Management Application Administrator, select the predefined resource role Master Data Management Application Administrator.
8. Click **Autoprovision Roles**. The application provisions the job and abstract roles according to the predefined, out of the box role provisioning rules.
9. Click **Save and Close**.

   The application creates the user, and automatically sends an e-mail to the user with the user name and password, unless you deselect the Send User Name and Password option.

6 Set Up Geography Data

Overview of Geography Setup

You must import and set up reference geography data for the countries where you do business. You can use this data to set up validation for address elements, such as states and cities, to prevent address data entry errors.

Oracle licenses geography data from Loqate that you can import, at no additional cost. You can also license geography data from another supplier. For more information about importing third party geography data, see the Import Country Structure and Import Geographies topics of the Understanding Import and Export Management for Sales and Fusion Service.

Alternatively, you can verify your address data using Oracle Address, Email, and Phone Verification. This service lets you verify that an address is an actual postal address as well as cleanse the address to conform to postal requirements. However, note that you require a separate license for Oracle Address, Email, and Phone Verification.

Vision Corp., the organization in our case study, imports and sets up reference geography data from Loqate for the countries it's available. For the rest of countries where it does business, it uses Oracle Address, Email, and Phone Verification to prevent address data entry errors.

This table lists the tasks you must complete to set up geography data.

Step	Description	Task Name	Where to Get More Details
Set Up Geography Structure	You can define geography types and then define how the geography types are hierarchically related within the country structure.	Manage Geographies	See the topic: *Set Up Geography Structure*
Set Up Geography Hierarchy	After defining the geography structure, you can add geographies for each geography type in the geography hierarchy.	Manage Geographies	See the topic: *Set Up Geography Hierarchy*
Set up Geography Validation	For the countries for which you imported geography data, enable validation down to address level required for your business, such as sales territories, and specify which address elements require lists of values. When you enable validation on an address element, the application suggests alternatives during address entry. Enabling a list of values requires the user to make a selection from a list. Both validation and lists of values are enforced in the UIs.	Manage Geographies	See the topic: *Setting Up Geography Validation*
Import Geography Data	Import Oracle-licensed geography data for the countries you do	Manage Geographies	See the topic: *Import Geography Reference Data Licensed by Oracle*

Step	Description	Task Name	Where to Get More Details
	business from Loqate. Search for the country for which you want to import geography data on the Manage Geographies page and select the Import Geography Data action. The Import Geography Data action is disabled if Loqate doesn't support the country; or Oracle-licensed geography data or any third-party geography data is already imported for the country; or geography data and hierarchy data is already manually created for the country.		
Import Geography Zone Data	You can define zones that are specific to your business needs. For example, San Jose Tax zone or West Coast shipping zone.	Import Management	See the topic: *Import Your Geography Zone Data*
Import Territories	You can replicate your sales organization's regions by defining territory geography zones.	Manage Territory Geographies	See the topic: *How You Import and Export Territory Geography Zones*
Turn on Validation for Address Import	The validation selection you make on the Manage Geographies page affects entries made in the application UI only. You must use the task Manage Administrator Profile Values to set the profile option Geography Address Validation Enabled to Yes to validate the addresses you import. You must also make sure that the address data you import matches what the geography reference data expects. In case of data mismatch, add an alternate geography data in the Manage Geographies UI. For example, for the **Aosta** province in Italy, third-party geography data has a value of **AOSTA** and Loqate has a value of TR. To resolve this conflict, in case you imported the data from third-party earlier, add AO as an alternate province name in the Manage Geographies UI.	Manage Administrator Profile Values	See the topic: *Turn on Validation for Address Import*
Set up Geocoding	You can use the Geocoding feature to find the latitude and longitude coordinates of the locations where your business is operating.	Manage Geographies	See the topic: *Set Up Geocoding*
Enable Address Mapping	Enable the mapping of account and contact addresses. With mapping enabled, your salespeople on the go can view their contacts on a map and obtain directions on	Manage Geographies	See the topic: *Enable Address Mapping Using Geocoding*

Step	Description	Task Name	Where to Get More Details
	their mobile phones with the click of a button.		
Turn on Real Time Address Cleansing	Enable real time address cleansing to validate and correct geography attributes and the address line attributes as you enter address information in the application. **Note:** To use the address cleansing functionality, a separate license for Oracle Address, Email, and Phone Verification is required.	Manage Geographies	See the topic: *Enable Real Time Address Cleansing*

Import Geography Reference Data Licensed by Oracle

You can use this procedure to import geography reference data licensed by Oracle. If the data you want to import is unavailable in Loqate or is already imported, then the Import Geography Data action is disabled.

Note: The geography data is provided by Loqate and is third-party content. As per Oracle policy, this software and documentation may provide access to or information about content and services from third parties. Oracle and its affiliates aren't responsible for and disclaim all warranties of any kind with respect to the third-party content and services. Oracle and its affiliates aren't responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

To import geography data:

1. Sign in as a setup user having the role Master Data Management Applications Administrator.
2. Open the Manage Geographies task from the implementation project. Or you can go to **Navigator** > **My Enterprise** > **Setup and Maintenance** > **Tasks** and search for Manage Geographies. Alternatively, in the Setup and Maintenance work area, go to the following:
    - Offering: Customer Data Management
    - Functional Area: Enterprise Profile
    - Task: Manage Geographies
3. Enter either the country name in the **Country Name** field or the two-letter ISO code of the country in the **Country Code** field.

    Examples of ISO country codes include US (United States) and AT (Austria).
4. Click **Search**.

    The Search Results display the country.
5. Select the country in the search results. Don't click the link.
6. Select **Import Geography Data** from the **Actions** menu.

> **Note:** The Import Geography Data action is disabled if the country isn't available from Oracle Address, Email, and Phone Verification Loqate or if the country data is already imported.

7. Click **OK** to close the warning message.
8. Click **OK** to close the confirmation message.

The import of larger countries may require several hours to complete. You can track the progress of the import process by selecting **Scheduled Processes** from the Navigator menu.

After the import is complete, you can search for the country again in the Manage Geographies page. Check marks now appear in the **Structure Defined** and **Hierarchy Defined** columns indicating that the import completed successfully.

The **Geocoding Defined** and **Address Cleansing Defined** columns are used for additional features that you set up separately:

- Geocoding enables mapping features in your application, such as the display of customer locations on a map in the UI. For details, see the topic: Enable Address Mapping.
- Address cleansing makes it possible to validate addresses down to the street level. Address cleansing requires you to obtain a separate license for Oracle Address, Email, and Phone Verification.

> **Note:** Report any issues with Loqate data to Oracle Support who will contact the appropriate team for correction. Alternatively, you can make manual changes to the geography data by using the Manage Geographies task in the Setup and Maintenance work area. If you decide to use geography data from another data provider, then Oracle Support can delete the data and you can then load your data using Import Management.

List of Available Countries with Loqate Geography Reference Data

Oracle Applications Cloud provides third-party Loqate geography data for import. Here's the list of countries for which the Loqate geography data is available for import.

Country Name	Country Code
Andorra	AD
Angola	AO
Argentina	AR
Australia	AU
Austria	AT
Belgium	BE

Country Name	Country Code
Bolivia	BO
Bosnia and Herzegovina	BA
Brazil	BR
Bulgaria	BG
Canada	CA
Cayman Islands	KY
Chile	CL
China	CN
Croatia	HR
Cuba	CU
Cyprus	CY
Czech Republic	CZ
Denmark	DK
Dominican Republic	DO
Ecuador	EC
Estonia	EE
Finland	FI
France	FR
Germany	DE
Great Britain	GB
Greece	GR

Country Name	Country Code
Guadalupe	GP
Guam	GU
Guernsey	GG
Hungary	HU
Iceland	IS
India	IN
Indonesia	ID
Ireland	IE
Isles of Man	IM
Israel	IL
Italy	IT
Jamaica	JM
Japan	JP
Jordan	JO
Kenya	KE
Latvia	LV
Liechtenstein	LI
Lithuania	LT
Luxembourg	LU
Malaysia	MY
Malta	MT

Country Name	Country Code
Martinique	MQ
Mexico	MX
Netherlands	NL
New Zealand	NZ
Norway	NO
Oman	OM
Peru	PE
Poland	PL
Portugal	PT
Puerto Rico	PR
Qatar	QA
Reunion Island	RE
Romania	RO
Russia	RU
San Marino	SM
Singapore	SG
Slovakia	SK
Slovenia	SI
South Africa	ZA
South Korea	KR
Spain	ES

Country Name	Country Code
Sri Lanka	LK
Swaziland	SZ
Sweden	SE
Switzerland	CH
Taiwan	TW
Thailand	TH
Tunisia	TN
Turkey	TR
United Arab Emirates	AE
United States	US
Uruguay	UY
Vatican City	VA
Vietnam	VN

Import Third Party Geography Data Using Import Management

You can import Oracle-licensed Loqate data, shipped with the application, for those countries where the data is available. If the licensed data isn't available or is already set up for a particular country, then the Import Geography Data action is disabled.

In case the licensed data isn't available for a particular country, you must license geography data from another supplier and import it from a file.

Import Country Structures Using Import Management

A country structure is a hierarchical grouping of geography types for a country. For example, the geography structure for the United States has the geography type of State at the top, followed by the County, then the City, and finally the Postal Code.

You must import country structures before importing geographies. You can use the country structure to set up the following:

- The relationships between geographies within a country
- The types of geographies that you can define for a country

For more information, see the Import Your Country Structure Data topic of the Understanding Import and Export Management for CX Sales and B2B Service guide available on docs.oracle.com.

Import Geographies Using Import Management

A geography is any region with a boundary around it, regardless of its size. It might be a state, a country, a city, a county, or a ward. You must create or import geographies before you can associate them with company defined zones and addresses. For more information, see the Import Your Geography Data topic of the Understanding Import and Export Management for CX Sales and B2B Service guide available on docs.oracle.com. Also see the related links on importing geographies.

Related Topics

Enable Address Mapping Using Geocoding

You can quite literally put your accounts and contacts on the map by enabling geocoding as described in this topic. Geocoding turns the addresses you enter or import into longitude and latitude coordinates so that the locations can be displayed on a map.

> **Note:** Geocoding isn't the same as the Geo Code Types defined in Geography Hierarchies. Examples of Geo Code Types are FIPS code, ISO country code, and so on. You can view Geo Code Types on the Manage Geography Hierarchy page under the Code Type column.

Enabling address mapping involves two steps:

1. You turn on the geocoding feature
2. You run a process that converts the addresses into coordinates

Your sales team must enter valid postal addresses for geocoding to work, so it's a good idea for you to validate the addresses in your application by subscribing to Oracle Address, Email, and Phone Verification.

Geocoding Options

Salespeople can use geocoding in two ways:

- In the office, salespeople can view the location of an account address on the map while editing the account record.

- Using `Oracle CX Cloud Mobile` on their smartphones, salespeople can view a map showing the locations of accounts and contacts within a certain radius of their current location, or any other location they choose. They can obtain travel directions to any of the locations with the tap of a finger (`CX Cloud Mobile` passes the coordinates to the native mapping application on the phone).

Enable Geocoding

To enable Geocoding, click the arrow mark under the Geocoding Defined column header and make sure that the arrow mark transforms into a tick mark. Here are the steps:

1. Open the **Manage Geographies** task from the implementation project or from Setup and Maintenance work area using the following:
    - Offering: Customer Data Management
    - Functional Area: Enterprise Profile
    - Task: Manage Geographies
2. On the Manage Geographies page, search for a country you imported using either its name or its two letter ISO code. For example, you can search by entering either the country name United States or the two letter ISO code US, and clicking **Search**.
3. Select the **Geocoding Defined** icon.
4. Click **Done**.

Run the Populate Location Latitude and Longitude Process

Once geocoding is enabled, you can schedule the Populate Location Latitude and Longitude Information process to run at regular time intervals so that newly created or updated locations are selected and geocoded. Addresses that salespeople enter or addresses that you import don't show up on the map until the process completes, so schedule the process to run as frequently as necessary and each time you import. To schedule the geocoding feature to run at regular intervals, complete these steps:

1. Navigate to the **Scheduled Processes** from the **Tools** work area.
2. Click **Schedule New Process**.
3. Click the Name drop-down list icon and the **Search** link at the bottom of the list.
4. In the Search and Select: Name window, search for Populate Location Latitude and Longitude Information.
5. Select the process name form the search result and click OK.
6. Click OK in the Schedule new Process dialog box to confirm the name and description of the new process.
7. In the Process Details page, click **Advanced** to view the advanced options.
8. You can make the following entries on the Parameters Tab:

Parameter	What to Enter
Country Code	Leave this field blank if you want to generate the coordinates for all the countries you enabled for geocoding, or enter a specific country code.
Start Date, End Date, and Regenerate Geocode	Leave these fields blank. The geocoding process picks up any addresses that haven't been geocoded previously.
Batch Size	Leave this field blank. If the Populate Location Latitude and Longitude Information scheduled process is run without any parameters, the process picks all addresses of countries for which

Parameter	What to Enter
	geocoding is enabled. This scheduled process can populate a maximum of 10,000 address locations. If the total number of addresses to be geocoded are more than 10,000, you may have to run this scheduled process many times with each batch of size of 1000 addresses. This scheduled process populates Latitude and Longitude values in the HZ_LOCATIONS table. This scheduled process continues to pickup already processed addresses for which the latitude or longitude parameters are null.

9. Click Process Option to set options such as Language, Territory, Currency, and Time Zone.
10. Click OK to the Process Options page.
11. Schedule the process to run regularly:
    - Click the Schedule tab.
    - Select Using a Schedule and specify the frequency.
12. Click Submit. The application confirms your process was submitted.
13. Click OK to the confirmation message. You can monitor the process completion on the Overview page.

Enable Real Time Address Cleansing

Address cleansing validates, corrects, and standardizes address information that you enter in the application. Address cleansing, unlike geography validation, validates both the geography attributes and the address line attributes.

Note that you need a separate license for Oracle Address, Email, and Phone Verification, to use the address cleansing functionality.

Here's how you can define address cleansing for the countries in which you do business.

1. Open the **Manage Geographies** task from the implementation project or from Setup and Maintenance work area using the following:
    - Offering: Customer Data Management
    - Functional Area: Enterprise Profile
    - Task: Manage Geographies
2. Search for a country that you want to enable Address Cleansing using either by name or by its two letter ISO code. For example, you can search by entering either the country name United States or the two letter ISO code US, and clicking Search.
3. Select the country in the Search Results area.
4. Click the Go to Task button in the Address Cleansing Defined column to enable the Verify Address button for account, contact or household on the simplified UI.
5. In Address Cleansing Level dialog box, set the Real-Time Address Cleansing Level to Optional to enable the option to cleanse addresses. If the level is set to None, it specifies no real-time address cleansing.
6. Click Save and Close.

Set Up Geography Validation

You must set up geography validation for those geography elements that you plan to use in your business, for example your sales territories. Setting up validation also helps users fill in missing address information, and validate addresses during entry.

For example, you can have users select states or other address elements from lists to ensure accuracy during entry, and you can have the application fill in missing values. For example, when the user enters a Postal Code, the application can retrieve the city and state.

For each country, you must map the geography types to the address attributes. When you define geography validation, you need to verify the default mapping and update it if required.

Our example organization, Vision Corp. wants its salespeople to use a list of values to enter the states in their addresses and it plans to set up territories at the state level. So, validation must be set up at the state level.

Define Geography Validation

Perform the following steps to define geography validation:

1. Open the Manage Geographies task from the implementation project or from the Setup and Maintenance work area from Setup and Maintenance work area using the following:
    - Offering: Customer Data Management
    - Functional Area: Enterprise Profile
    - Task: Manage Geographies
2. Search for a country you imported using either its name or its two letter ISO code. For example, you can search by entering either the country name United States or the two-letter ISO code US.
3. Select the country from the Search Results area.
4. Click the Go to Task button in the Validation Defined column. Here's an image of the Manage Geographies page highlighting the Go to Task icon in the Validation Defined column.

5. On the Manage Geography Validation page, in the Address Style region, ensure that the No Styles Format address style is selected. You define validation for the No Styles Format address style so that the validations are performed for all addresses in the country.

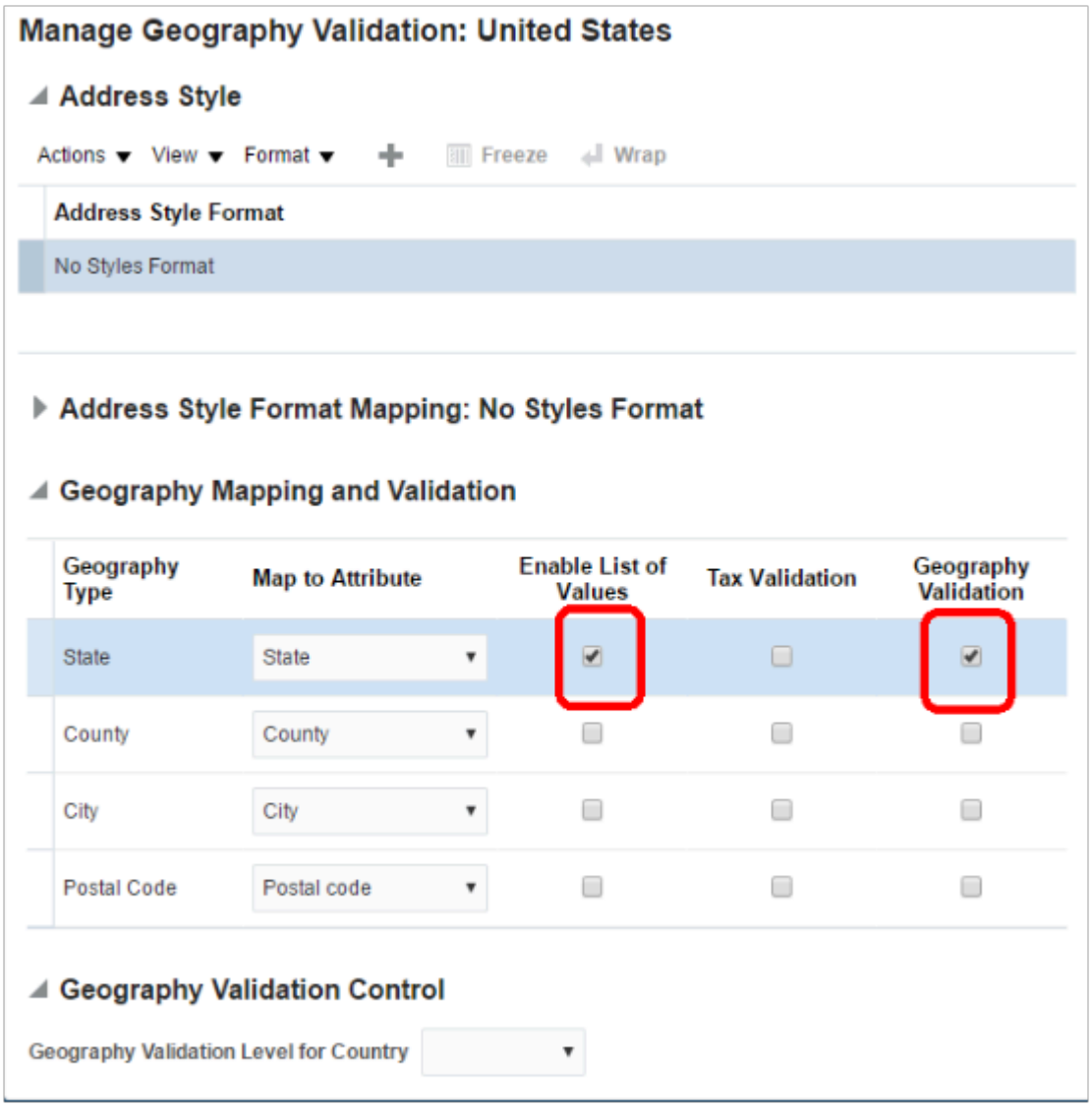
   > **Note:** The setup of address styles for your application is done elsewhere, using the Manage Address Formats task.

6. Select Enable List of Values in the Geography Mapping and Validation region to display the geography type as list of values during address entry in the classic and simplified UIs. For example, to have users select states from a list, select Enable List of Values for State.

   The example organization in our case study, Vision Corp., enables the list of values for State because it uses states for its sales territories and wants to assure that they are always entered correctly.

7. Select Geography Validation for all the geography types that you plan to use in territories.

   Our example organization, Vision Corp., plans to use set up geographies by state, so it selects Geography Validation for State. Here's an image of the Manage Geography Validation page highlighting the location of the Enable List of Values and Geography Validation options for the US State geography type.



> **Note:** If you don't select the validation for an address element, the application still suggests values to the user during address entry in the classic and simplified UIs, but it doesn't validate the address element.

8. Ensure that the mapping between **Geography Type** and **Map to Attribute** is valid in the Geography Mapping and Validation region and modify it if required. Oracle recommends that you use the following valid mapping for the countries that Loqate supports:

Country Name	Country Code	Geography Type	Map to Attribute
Andorra	AD	○ `Country`	○ `Country`

Country Name	Country Code	Geography Type	Map to Attribute
		o Parroqia o Settlement o Postal Code	o State o City o Postal code
Angola	AO	o Country o Provincia o Municipio o Comuna o Localidad	o Country o Province o County o City o Additional address attribute 2
Argentina	AR	o Country o Province o Department o Municipality o Postal Code	o Country o Province o County o City o Postal code
Australia	AU	o Country o State o City o Postal Code	o Country o State o City o Postal code
Austria	AT	o Country o Bundensland o Bezirk o Gemeinde o Postal Code	o Country o State o County o City o Postal code
Belgium	BE	o Country o Gewest o Provincie o Gemeente o Postal Code	o Country o Additional address attribute 1 o Province o City o Postal code
Bolivia	BO	o Country o Departmento o Provincia o Canton	o Country o Additional address attribute 1 o Province o City
Bosnia and Herzegovina	BA	o Country	o Country

Country Name	Country Code	Geography Type	Map to Attribute
		o District o Kanton o Opcine o Nasalje o Postal Code	o Additional address attribute 1 o Province o County o City o Postal code
Brazil	BR	o Country o State o City o Postal Code	o Country o State o City o Postal code
Bulgaria	BG	o Country o Oblast o Obshhina o Settlement o Postal Code	o Country o Additional address attribute 1 o Province o City o Postal code
Canada	CA	o Country o Province o City o Postal Code	o Country o Province o City o Postal code
Cayman Islands	KY	o Country o Island o District o Postal Code	o Country o State o City o Postal code
Chile	CL	o Country o Region o Provincia o Kommune o Postal Code	o Country o State o County o City o Postal code
China **Note:** China geography structure is supported but geocoding isn't supported.	CN	o Country o Province o City o Postal Code	o Country o Province o City o Postal code

Country Name	Country Code	Geography Type	Map to Attribute
Croatia	HR	o Country o Zupanije o Grad o Postal Code	o Country o Province o City o Postal code
Cuba	CU	o Country o Provincia o Municipio o City o Postal Code	o Country o Province o County o City o Postal code
Cyprus	CY	o Country o Periochi o Dimos o Postal Code	o Country o Province o City o Postal code
Czech Republic	CZ	o Country o Kraj o Okres o Obec o Postal Code	o Country o State o County o City o Postal code
Denmark	DK	o Country o Amt o Settlement o Postal Code	o Country o Province o City o Postal code
Dominican Republic	DO	o Country o Provincia o Municipio o Town o Postal Code	o Country o Province o County o City o Postal code
Ecuador	EC	o Country o Province o Canton o City o Postal Code	o Country o Province o County o City o Postal code

Country Name	Country Code	Geography Type	Map to Attribute
Estonia	EE	o Country o Maakond o Vald o Postal Code	o Country o State o City o Postal code
Finland	FI	o Country o Laani o Kunta o Postal Code	o Country o State o City o Postal code
France	FR	o Country o Region o Department o Commune o Postal Code	o Country o Additional address attribute 1 o State o City o Postal code
Germany	DE	o Country o Bundesland o Gemeinde o Postal Code	o Country o State o City o Postal code
Great Britain	GB	o Country o County o Township o Postal Code	o Country o State o City o Postal code
Greece	GR	o Country o Periferia o Nomi o Dimotika o Postal Code	o Country o State o County o City o Postal code
Guadalupe	GP	o Country o Commune o Postal Code	o Country o City o Postal code
Guam	GU	o Country o State o County	o Country o State o County

Country Name	Country Code	Geography Type	Map to Attribute
		○ Municipality ○ Village ○ Postal Code	○ City ○ Additional address attribute 2 ○ Postal code
Guernsey	GG	○ Country ○ City ○ Parishes ○ Villages ○ Postal Code	○ Country ○ City ○ Additional address attribute 2 ○ Additional address attribute 3 ○ Postal Code
Hungary	HU	○ Country ○ Megye ○ Jaras ○ Telepules ○ Settlement ○ Postal Code	○ Country ○ Additional address attribute 1 ○ Province ○ County ○ City ○ Postal code
Iceland	IS	○ Country ○ Jaras ○ Telepules ○ Settlement ○ Postal Code	○ Country ○ Province ○ County ○ City ○ Postal code
India	IN	○ Country ○ State ○ City ○ Postal Code	○ Country ○ State ○ City ○ Postal code
Indonesia	ID	○ Country ○ Province ○ Regency ○ City ○ Postal Code	○ Country ○ Province ○ County ○ City ○ Postal code
Ireland	IE	○ Country ○ Province ○ Post County ○ Post Code	○ Country ○ State ○ City ○ Postal Code

Country Name	Country Code	Geography Type	Map to Attribute
Isles of Man	IM	o Country o Locality o Settlement o Postal Code	o Country o City o Additional address attribute 2 o Postal code
Israel	IL	o Country o District o Subdistrict o City o Postal Code	o Country o State o County o City o Postal code
Italy	IT	o Country o Regione o Provincia o Comune o Postal code	o Country o Additional address attribute 1 o Province o City o Postal code
Jamaica	JM	o Country o Parish o Settlement	o Country o State o City
Japan	JP	o Country o Prefecture o City o Postal Code	o Country o State o City o Postal code
Jordan	JO	o Country o Muhafazat o Liwa o Tajma o Postal Code	o Country o State o County o City o Postal code
Kenya	KE	o Country o County o Division o Settlement	o Country o State o City o Additional address attribute 2
Latvia	LV	o Country o Rajons	o Country o State

Country Name	Country Code	Geography Type	Map to Attribute
		○ Pilseta ○ Postal Code	○ City ○ Postal code
Liechtenstein	LI	○ Country ○ Wahlkreis ○ Gemeinde ○ District ○ Postal Code	○ Country ○ Additional address attribute 1 ○ State ○ City ○ Postal code
Lithuania	LT	○ Country ○ County ○ Municipality ○ Ward ○ Postal Code	○ Country ○ State ○ County ○ City ○ Postal code
Luxembourg	LU	○ Country ○ Canton ○ Commune ○ Settlement ○ Postal Code	○ Country ○ State ○ County ○ City ○ Postal code
Malaysia	MY	○ Country ○ State ○ District ○ Subdistrict ○ Postal Code	○ Country ○ State ○ County ○ City ○ Postal code
Malta	MT	○ Country ○ Region ○ Local Council ○ Postal Code	○ Country ○ State ○ City ○ Postal code
Martinique	MQ	○ Country ○ Departmen ○ Arrondisement ○ Commune ○ Postal Code	○ Country ○ State ○ County ○ City ○ Postal code
Mexico	MX	○ Country	○ Country

Country Name	Country Code	Geography Type	Map to Attribute
		o State o Municipality o Locality o Postal Code	o State o County o Additional address attribute 2 o Postal code
Netherlands	NL	o Country o Province o Muncipality o Town o Postal Code	o Country o Province o County o City o Postal code
New Zealand	NZ	o Country o Region o Town o Postal Code	o Country o State o City o Postal code
Norway	NO	o Country o Fylke o Kommune o Postal Code	o Country o Province o City o Postal code
Oman	OM	o Country o Muhafazah o District o City	o Country o State o County o City
Peru	PE	o Country o Region o Provincia o Distrito o Postal Code	o Country o Province o County o City o Postal code
Poland	PL	o Country o Wojewodztwo o Powiat o Gmina o Postal Code	o Country o Province o County o City o Postal code
Portugal	PT	o Country	o Country

Country Name	Country Code	Geography Type	Map to Attribute
		o Distrito o Concelho o Settlement o Postal Code	o Province o County o City o Postal code
Puerto Rico	PR	o Country o Commonwealth o Municipio o Barrio o Postal Code	o Country o State o County o City o Postal code
Qatar	QA	o Country o Municipality o Zone	o Country o State o City
Reunion Island	RE	o Country o Region o Department o Commune o Postal Code	o Country o State o County o City o Postal code
Romania	RO	o Country o Regiune o Judet o Settlement o Comuna o Postal Code	o Country o Additional address attribute 1 o Province o County o City o Postal code
Russia	RU	o Country o Federal_District o Federal_Subject o Oblast o Postal Code	o Country o Additional address attribute 1 o State o City o Postal code
San Marino	SM	o Country o Comune o Postal Code	o Country o State o Postal code
Singapore	SG	o Country	o Country

Country Name	Country Code	Geography Type	Map to Attribute
		○ Region ○ District ○ Postal Code	○ State ○ City ○ Postal code
Slovakia	SK	○ Country ○ Kraj ○ Okres ○ Obec ○ Postal Code	○ Country ○ Province ○ County ○ City ○ Postal code
Slovenia	SI	○ Country ○ Regija ○ Upravna Enota ○ Obcina ○ Settlement ○ Postal Code	○ Country ○ Additional address attribute 1 ○ Province ○ County ○ City ○ Postal code
South Africa	ZA	○ Country ○ Province ○ District Municipality ○ Local Municipality ○ Postal Code	○ Country ○ Province ○ County ○ City ○ Postal code
South Korea	KR	○ Country ○ Jibang ○ Siti ○ Postal Code	○ Country ○ State ○ City ○ Postal code
Spain	ES	○ Country ○ Autonomous Community ○ Province ○ City ○ Postal Code	○ Country ○ Additional address attribute 1 ○ Province ○ City ○ Postal code
Sri Lanka	LK	○ Country ○ Province ○ District ○ Divisional Secretariat	○ Country ○ Province ○ County ○ City

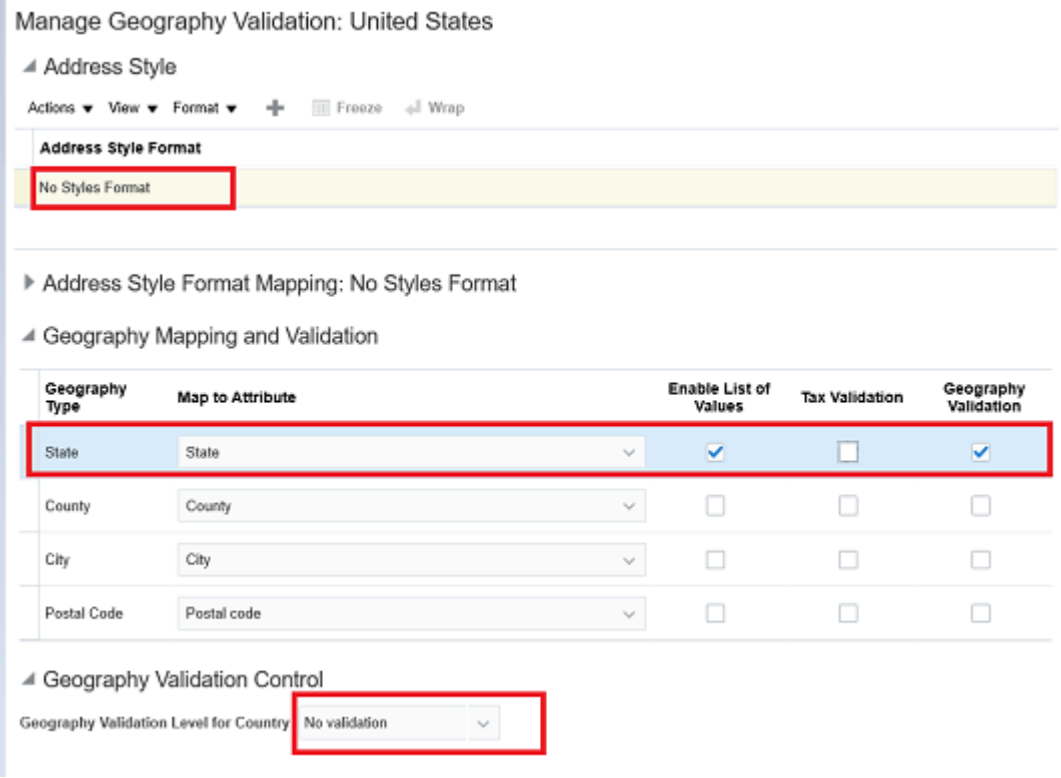
Country Name	Country Code	Geography Type	Map to Attribute
		o Postal Code	o Postal code
Swaziland **Note:** This country maybe labeled Eswatini in Manage Territories.	SZ	o Country o District o Inkhundla o Town o Postal Code	o Country o Province o County o City o Postal code
Sweden	SE	o Country o Lan o Settlement o Postal Code	o Country o Province o City o Postal code
Switzerland	CH	o Country o Kanton o Bezirk o Gemeinde o Postal Code	o Country o State o County o City o Postal code
Taiwan	TW	o Country o County o Town o Postal Code	o Country o State o City o Postal code
Thailand	TH	o Country o Region o Changwat o Amphoe o Postal Code	o Country o Additional address attribute 1 o State o City o Postal code
Tunisia	TN	o Country o Governorate o Delegation o Postal Code	o Country o State o City o Postal Code
Turkey	TR	o Country o Sehir o Ilce o Kasaba	o Country o Province o County o City

Country Name	Country Code	Geography Type	Map to Attribute
		o Postal Code	o Postal code
United Arab Emirates	AE	o Country o Emirate o City o Area	o Country o State o City o Additional address attribute 2
United States	US	o Country o State o County o City o Postal Code	o Country o State o County o City o Postal code
Uruguay	UY	o Country o Departamento o City o Postal Code	o Country o State o City o Postal code
Vatican City	VA	o Country o Municipal o Settlement o Postal Code	o Country o Province o City o Postal code
Vietnam	VN	o Country o Region o Tihn o Quan o Thank Pho o Postal Code	o Country o Additional address attribute 1 o Province o County o City o Postal code

9. Select the values from the Geography Validation Level for Country drop-down list to specify whether you want to permit the application to save addresses that aren't considered valid. The following are the available values in the Geography Validation Level for Country drop-down list:
    - No validation: The default value. Select to save incomplete or incorrect addresses. In case you have the license for Oracle Address, Email, and Phone Verification, you can select this option to verify the address data using this service.
    - Error: Select to verify address data against the master geography reference data. This value permits only valid addresses to be saved.

    Our example organization wants to save all addresses including incomplete and invalid addresses, so it keeps the No validation which is the default value.

    The following figure shows the Manage Geography Validation page when the task is completed.



10. Click Save and Close.

Turn on Validation for Address Import

By default, the validation you specified on the Manage Geography Validation page is enforced for creating addresses in the UI only. You must set the profile option Geography Address Validation Enabled to Yes for the validation to be enforced during import.

Follow these steps to set the profile option:

1. Open the **Manage Administrator Profile Values** task from the implementation project or by searching for it in the Setup and Maintenance work area. The Manage Administrator Profile Values page appears.

2. In the Profile Display Name field located in the Search: Profile Option region, enter Geography Address Validation Enabled.
3. Click **Search**.
4. With the profile option selected in the search results, select **Yes** from the Profile Value list.
5. Click Save and Close.

7 Import Your Data

Set Up Source Systems

You set up source systems to import data into the application from other systems and identify the source of the data that you're importing.

> **Note:** You must setup source systems before importing your organization (account) and person (contact) data. The next step is to setup source system confidence to determine the relative reliability of a particular organization (account) or person (contact) attribute (standard or custom) from a particular source system. This allows the preservation of data from the most reliable source in the master record during the merge operation. See the topic: *Manage Source System Confidence*.

You can specify whether the source system is a spoke system, such as a legacy system, or a purchased system, such as data from a third party provider. You can also specify what types of entities can be imported from a source system. For example, you can enable a source system for importing trading community members such as organizations (accounts) and persons (contacts).

> **Note:** You can select multiple source references in the Manage Source System Entities task to allow multiple source system records to map to a single record.

For example, consider Vision Corp., a software company which acquires a couple of software companies, First Software and Softgear, and their customers. So we will have to setup the following three source systems:

- Vision Corp.
- Softgear
- First Software

Here is how you can go about setting up these source systems:

1. In the Setup and Maintenance work area, navigate to the following:
    - Offering: Customer Data Management
    - Functional Area: Trading Community Foundation
    - Task: Manage Trading Community Source Systems
2. From the Actions menu, click Create. The Create Source System UI page appears.
3. Enter the following information:
    - Code: VC
    - Name: Vision Corp.
    - Type: Spoke
4. Enable the source system for Trading Community Members. You can enable it for other entity types also depending on your business requirements.
5. Click Save and Create Another.
6. Enter the following information:

- Code: SG
- Name: Softgear
- Type: Spoke

7. Enable the source system for Trading Community Members. You can enable it for other entity types also depending on your business requirements.
8. Click Save and Create Another.
9. Enter the following information:
   - Code: FS
   - Name: First Software
   - Type: Spoke
10. Enable the source system for Trading Community Members. You can enable it for other entity types also depending on your business requirements.
11. Click Save and Close.

About Import Management

How do I import data?

Use Import Management from the Tools work area, to import data from text files. This topic is your guide to importing data in sales, service, and incentive compensation.

You can create, update, or delete records through import.

The import options and other details differ by the type of data that you're importing. Before importing, understand how the data in your file maps to the attributes in Oracle Applications Cloud and what values are expected in the import file. The data records in the CSV source file may not be processed in the listed order. To learn how to monitor the status of your import, see the topic How You Monitor Your Import Activities in the Related Topics section.

Note: Don't submit duplicate import jobs for the same import object as they create duplicate object records.

To help you get started, you can use the example import object templates described in the related topics.

Import Data from a File

To import data:

1. Click **Tools** > **Import Management**.
2. On the **Manage Imports** page, click the **Create Import Activity** button.
3. On the **Enter Import Options** page provide values for each field as shown in the following table:

Field	Description of the value
Name	Name of the import.

Field	Description of the value
Object	Object that you're importing. If you can't find your object, then search for it by clicking the **Search** link. In the **Search and Select** dialog box, enter the object name in the **Object** text box and click the **Search** button. Select your object from the result list and click **OK**. You can also use the advanced search option by clicking the **Advanced** button. Here you can search based on various filter criteria such as object name, Attachment supported, creation date, and so on. If the object you're importing isn't listed then verify if you have the roles and privileges required to import the object. For information on the roles, see the topic Roles Required for Import and Export Management referenced in the Related Topics section.
Attachment Object	To import an attachment for an existing object record in the database select the Attachments object from the **Object** drop-down list. Next select the object from the **Attachment Object** drop-down list. For more details on importing attachments, review the topic Import Attachments.
File Name	Browse and select a text file in CSV format. The first row of the source file is treated as the header row. Provide a file name within 40 characters. **Note:** If your source file has more than 50,000 records, then you must manually split the file into several smaller files with less than 50,000 records each. The file import page only permits 50,000 records for each import job. Alternatively, you can use the External Cloud Data Loader Client, which can accept files with more than 50,000 records. See the My Oracle Support (support.oracle.com) document External Data Loader Client (document ID 2325249.1) for more information about this tool.
Import Object Hierarchy	To import a hierarchy of objects, such as child and grandchild objects, click on the **Import Object Hierarchy** link after you upload the source file for the parent object. Next select the Enabled check box for the child object you want to import, and select the related source file. **Note:** When importing child records for a parent object, ensure that the child records and the parent records are imported in the same batch (using the same import file). If you import child records in batches using parallel jobs, then the import job may fail because the parent object record may be locked during the import process.

4. Optionally, to set additional import configurations, click the **Advanced Options** section. Here you can configure settings under **Source File**, **Import Options**, or **Create Schedule** sections.

    a. In the **Source File** and **Import Options** regions, some of the options in the following table might not be available depending on the object that you're importing:

Option	Description
Import Mode	You can specify whether you want to create and update records or update them only. - **Update and create records** - a new record is created if a matching record isn't found. This is the default option. - **Create records** - all the records in the file are new records which have to be created. If there are any existing matching records, then they're marked as errors. - **Delete records** - all the records in the file are deleted.
Enable High-Volume Import	The high-volume import mode is designed to import millions of records at once. This mode doesn't trigger any custom logic configured through the application composer. For a list of supported objects, see the topic Data Import Options. By default, this mode is enabled for the supported objects. **Note:** If ZCA_FILE_IMPORT_ENABLE_CUSTOM_BUSINESS_LOGIC is set to “Yes”, then you won’t be able to use High Volume import.
Enable Survivorship	Survivorship on update is available for Account, Organization, Contact, and Person. The check box is visible if the attribute survivorship is configured on the objects. You can use high-volume import mode, only when the survivorship configuration uses only Source Confidence. You can't use the high-volume import mode when Data Quality Rules are enabled.
Notification email	The email of the individual who receives import processing notifications. The user submitting the import receives an email notification automatically. To have more than one email recipient, separate the email addresses with a semicolon. If you don't want to receive the notification, then set the profile option ORA_ZCA_IMPEXP_ENABLE_EMAIL_NOTIFY to 'N' at user level.
Enable Custom Business Logic	If you select this check box, then any custom triggers and validations configured for the object are enabled. This may affect import performance, because of configurations. Hence, disable this option for better performance. To enable this check box by default, set the profile option ZCA_FILE_IMPORT_ENABLE_CUSTOM_BUSINESS_LOGIC to 'Yes' by navigating to the Manage Administrator Profile Values task.

Option	Description
	Note: If ZCA_FILE_IMPORT_ENABLE_CUSTOM_BUSINESS_LOGIC is set to “Yes”, then you won’t be able to use High Volume import. **Note:** This selection has no effect on events and object workflows, and is applicable only on triggers and validations.
Delimiter	If your file doesn't use a comma to separate values, then select the correct delimiter in the **Delimiter** drop-down list. Possible values are: - Caret Symbol - Closing Curly Bracket - Closing Parenthesis - Closing Square Bracket - Colon - Comma - Exclamatory Mark - Minus - Opening Curly Bracket - Opening Parenthesis - Opening Square Bracket - Pipe Symbol - Plus - Question Mark - Semi-Colon - Star Symbol - Tilde Symbol
Decimal Separator	The decimal separator used in your import file.
Date Format	The format of the date fields in your file.
Time Stamp Format	The format of the time fields in your file.
File Encoding	The format in which your source file is encoded. The possible values are: - Chinese Simplified - GB, CP936 - Chinese Traditional - CP950 - Eastern European - Win, CP1250 - Greek - MS Windows, CP932

Option	Description
	- Japanese - Shift- JIS, CP932 - Unicode - UTF-16 - Unicode- UTF-16BE, Mac, Unix - Unicode - UTF-16LE, MS Windows - Unicode - UTF-8 - Western European - Win, CP1252 **Note:** The above mentioned encoding formats are the only ones supported. Importing file with any other format, such as ANSI, will cause unexpected characters to be imported.

b. In the **Create Schedule** region, schedule the import to run immediately or at a future date. If you select a future date, then provide the date and time to start the import.

You can save the Advanced Options for subsequent reuse by clicking on the **Save advance options** link in the UI. The options are retained until you click the **Reset** link and reset the options to application defaults.

> **Note:** All fields except Import Mode, Enable Custom business Logic, Enable High-Volume Import, Enable Survivorship Logic, Schedule Mode, and Schedule Start Time will be saved.

5. Click **Next**. The **Map Fields** page shows the first row of the data from your source file. By default, the application tries to automatically map each of the source file columns to the appropriate target object attribute. If some of the columns in your file couldn't be mapped, then drag the target attribute onto the **Attribute Display Name** column in the **Source File** region.

   The data in unmapped columns aren't imported.

   You can save your import map by clicking on **Save As** in the Create Import Activity page. You can use the saved map for future imports. You can view your saved maps by clicking on the **Import Mapping** drop-down list in the Create Import Activity page.

   Also, you can select and then edit your saved maps for the specific objects in the Import Objects page.
6. You select a predefined mapping from the list of available mappings in the **Import Mapping** drop-down list. If you're reusing an import mapping, then both the source and target columns are already populated.

   Leave the Attribute Display Name field blank for any column that you don't want to import.

   Click **Validate Data** to check the field mapping.
7. In the case of hierarchical import, you can see the mapping information for child objects in the subsequent tabs. Note that data validation isn't done for these objects.
8. Click **Next**. On the **Review and Submit** page, review the import activity configuration. If you had not run the prevalidation on the **Map Fields** page, then you get a notification message to run the validation process. You can view any unmapped columns of parent or child objects on this page.
9. Click **Validate Data** to check the data in your source file. Validation errors, if any, are displayed on the Mapping Validation screen. If you get warnings about unmapped columns, then you can ignore these columns, and

proceed to submit the import job. Validations are for informational purposes and applicable only for low-volume imports.

> **Note:** In import activity with single CSV hierarchical records, explicit validation from the mapping UI isn't supported. For example, while importing the sales territory object, if there are matching values for the attributes ParentUniqueTerritoryNumber and UniqueTerritoryNumber, then validation isn't supported.

> **Note:** During the import validation process on the Mapping page, the following custom triggers aren't supported:
>
> - Before InValidate
> - Before Remove
> - Before Insert in Database
> - Before Update in Database
> - Before Delete in Database
> - Before Rollback in Database
> - After Changes Posted to Database

10. Click **Submit** to queue the import.
    Note that business events aren't fired when using Import Management.

Automating and Scheduling Import Jobs

You can automate import jobs using the import REST services. The import REST services let you manage import activities, manage activity maps, and export object metadata. You can use an external scheduler that uses these REST services to run recurring import jobs, create and run import activities, manage maps, and review object metadata.

You can use the Oracle WebCenter Content Document Transfer Utility to manage the import files used by the scheduler. You can download the Oracle WebCenter Content Document Transfer Utility by navigating to the My Oracle Support (support.oracle.com) document Oracle WebCenter Content Document Transfer Utility Readme (document ID 1624063.1). Once downloaded, you can run the tool by navigating to the ridc folder after extraction.

For detailed instructions on automating and scheduling file import using REST API, see Oracle CX Sales and Fusion Service: Automating and Scheduling File Import Activity Using REST API (Doc ID 2308691.1) article on My Oracle Support (support.oracle.com).

Set Up Event Notifications for Resources

In file-based data import, the `SendCredentialsEmailFlag` attribute allowed the import to specify the notification setting for each employee resource. You can do this in Import Management using the User Category option but this applies to all resources in a single import.

To set up notifications for all events:

1. Navigate to **Tools** > **Security Console** on the home page.
2. Click the **User Categories** tab.
3. Click DEFAULT. Click the **Notifications** tab.
4. Click the **Edit** button. To turn on all notifications, then select the **Enable Notifications** checkbox in the Notification Preferences heading.
5. Click the Save button.

6. Click the Done button.

To set up notifications for a specific event:

1. Navigate to **Tools** > **Security Console** on the home page.
2. Click the **User Categories** tab.
3. Click DEFAULT. Click the **Notifications** tab.
4. Click the Edit button.
5. To turn on a specific event notifications, click the template for the desired event.
6. On the **Template Information** page, select the **Enabled** checkbox and click **Save and Close**.
7. Click the **Save** button.
8. Click the **Done** button.

Import FCLs and DCLs

Setting FCL Field values

You must pass the lookup code in order to set the FCL field using import management.

Setting FCL and DCL Fields to Null

You must pass #NULL value for the FCL field in order to nullify a value for an FCL using Import Management.

Here is an example to nullify TargetGlobalPJDetailFlag1_c field:

PartyId	TargetGlobalPJDetailFlag1_c
100000001527765	#NULL

Related Topics

- How do I import attachments?
- How do I monitor import activities?
- How do I map import fields?
- What are my data import options?
- What are the roles required to import or export data?

How do I import attachments?

You can import attachments associated with any supported object.

Supported Objects and File Types

The following objects support importing attachments:

- Account
- Activity
- Asset

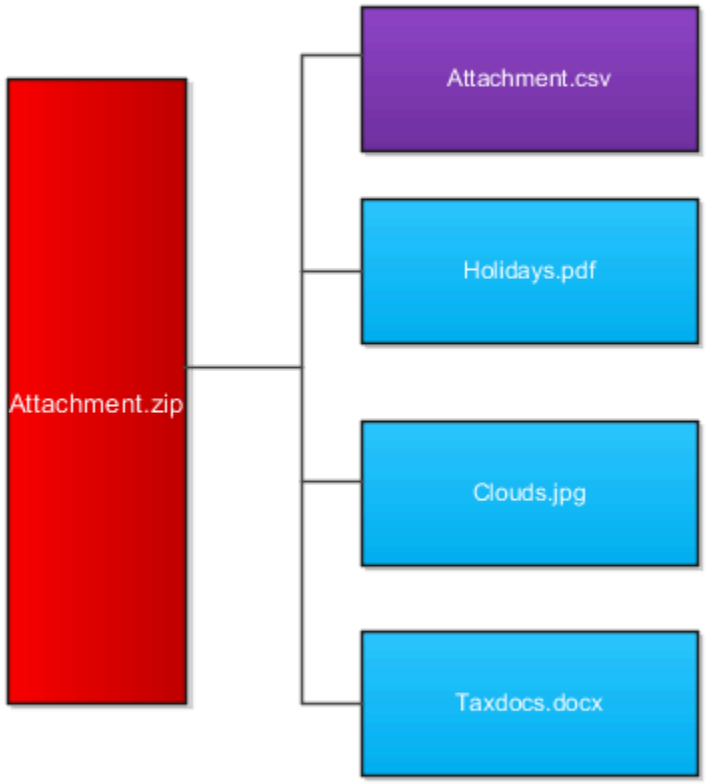
- Business Plan
- Contact
- Custom Object
- Deal Registration
- Household
- Message
- Objective
- Opportunity
- Opportunity Revenue
- Partner
- Partner Program
- Product
- Sales Lead
- Sales Lead Product
- Service Request

The following file types are supported for attachment files:

- CSV
- DOC
- DOCX
- JPG
- PDF
- PNG
- PPTX
- TIF
- TEXT
- XLSX
- XML
- ZIP

How to Create ZIP File

To import an attachment, you must create a ZIP file that contains the source data file and optionally one or more attachment files. Make sure you always name the source file as 'Attachment.csv'. You must mention each of the attachment file names in the Attachment.csv file. The Attachment.zip file has the structure shown in the following image:



Here are the examples for the attachment.csv file shown in purple box in the image above:

Pk1Value	ObjectPuid	FileName	Url
100100004247330			http://www.yahoo.com
100100004247330		Clouds.jpg	
100100004247330		Taxdocs.docx	
	CDRM_6493		http://www.google.com

Pk1Value	ObjectPuid	FileName	Url
	CDRM_6493	Holidays.pdf	

Note:

- Pk1Value and ObjectPuid column values uniquely identify an existing object record. FileName indicates the name of attachment files. Url indicates the value of URL attachment to import.
- The exact file name must exist in the zip file such as Document.pdf
- The attachment ZIP file name can include characters such as parenthesis (), ampersand (&), dots (.), and apostrophe (') only. You shouldn't have more than one period (.) in your attachment name. Also, the rootname.extension shouldn't be more than 80 characters.
- An attachment can only be associated with an existing record of the object. A single record can be associated with multiple attachments by having multiple rows in the CSV file. You can import any number of attachments in an import job, but the ZIP file should not exceed 250 MB in size.
- A record in the CSV file can't have values for both FileName and Url columns. You can pass either the Primary key or the PUID for an object record. If you pass both Primary key and PUID values, then Primary key will be considered and PUID will be ignored.
- The AttachedDocumentId should be left blank.
- The DatabaseTitle shouldn't be higher than 79 character.

How to Import Attachments

To import attachments:

1. Click **Tools** > **Import Management**.
2. On the **Manage Imports** page, click **Create Import Activity**.
3. On the Enter Import Options page, enter a name for your import. From the **Object** drop-down list select **Attachments**.
4. In the **Attachment Object** drop-down list that appears, select the object associated with the attachment.
5. Select the ZIP file that you created in the previous section.
6. Click **Next**. On the **Map Fields** page, click the **Apply** button next to the **Import Mapping** drop-down list to map the source and target attributes automatically.
7. Click **Next** to navigate to the **Review and Submit** page.

Review the import activity configuration and click **Submit** to activate the import. The **Manage Imports** page shows the status of the submitted import. The topic Import Data in the related topics section contains more details about the import process.

Related Topics

- How do I import data?

Import Data

How do I import account data?

You can use Import Management to create, update, or delete your account data.

You can import account records using these steps:

1. Map your source account data to Oracle Applications Cloud object attributes. This way the import process would know where to insert each of the information bits.
2. Create the source CSV file with the account data you want to import.
3. Kick off an import activity.
4. Check the import results to know if the import went well.

How You Map Your Source Data to Target Object Attributes

You import account data into Oracle Applications Cloud from a CSV file containing your source data that's mapped to target Oracle Applications Cloud object attributes.

You need to do the following before creating the .csv file for data import:

- Identify how your source data attributes map to the target object attributes in Oracle Applications Cloud.
- Ensure prerequisite steps are complete, such as understanding what attributes are required for importing your objects.
- Understand your options for uniquely identifying the records.
- Ensure parent records exist before importing child records.
- Identify the target object attributes that are required in the .csv file for a successful import

> **Note:** You can enable automatic territory-based assignment after sales accounts are imported. You can enable this feature by turning the profile option ZCA_BATCH_ASSIGN_ON_BULK_IMPORT ON. If the profile option is disabled, then you must manually run a batch assignment or assign each sales account individually.

To better manage your account information, the account object has the following child objects:

- Address
- Classification
- Relationship
- Sales Team Member

Note: You can't set an attribute value to NULL in high-volume import (import management with the option **Enable High-Volume Import** selected). However, when updating a record, you can change an attribute value from NOT NULL to NULL

If you're importing account records with attributes specific to the parent account object or along with single child record details (like phone, email, address, and so on), then you can include the child record details in the same .csv file for account object. However, if you're importing multiple records of any child object, then you must create multiple .csv files to import- one for each child which has multiple records that you're importing. For example, if you're importing 5 emails, 5 phones, and 5 addresses for an account, then you must create three import files - one for Account object, one for Contact Point object (phone and email), and one for Address object. There are separate help topics describing how to import each of these child objects. For more information, see the related topics section.

Note: High-volume import for accounts now supports hierarchy management and generation.

Before You Start

You must do some basic checks before starting your import. For example, make sure that:

- You have completed all the prerequisites for importing each attribute in your source data. For example, when using source system reference information to identify your account records, the source system of the account object should be enabled for parties using the Manage Trading Community Source Systems task.
- You have all parent records in place before importing child records. For example, when importing the address of an account, ensure the account exists.

Select a Unique Identifier for Your Records

All records must be unique in the application. You can use one of these to identify records:

- Public unique identifiers: If you're creating records, then you can provide an easily understandable public unique identifier. These are, usually, denoted with 'Number' and visible in the business object's UI. PUID attributes are usually named <object> Number. If you're updating a record with a Number attribute, then use the Number attribute to identify the record. For account object, the attribute is PartyNumber and shows up in the UI as Party Number. For more information about public unique identifiers, see the topic "How You Use Alternate Keys to Import Records" in Related Topics section.
- Source system and source system reference: Source system is an identifier for the external system, and source system reference is a unique identifier within the external system. If you're importing new accounts or are updating accounts that have source system reference data, then provide the source system and source system reference values. For account object, these are SourceSystem and SourceSystemReferenceValue and show up as Party Source System and Party Source System Reference Value in the UI.

Review Required Attributes and Validations for Account Object

To import data successfully into Oracle Applications Cloud, your CSV file must include the required attributes. Make sure that you provide valid values for these attributes so that they pass import validations inbuilt into the application.

This table lists the required attributes for account records, prerequisite setup tasks and specific validations, if any:

Attribute	Description	Prerequisite Setup Tasks or Import Validations	Creating an Account Record	Updating an Existing Account Record	Deleting an Existing Account Record
SourceSystem	The source system for the sales account.	Know the source system. To view source systems, use the Manage Trading Community Source System task.	Conditionally Required To identify an account record, use one of these: • SourceSystem and SourceSystemRefe • PartyNumber	Conditionally Required To identify an account record, use one of these: • SourceSystem and SourceSystemRefe • PartyNumber	Conditionally Required To identify an account record, use one of these: • SourceSystem and SourceSystemReferenceValu • PartyNumber
SourceSystemReferenc	The reference number or text representing the source system unique ID for the party (account or contact) to which the sales profile belongs.	Know the source system reference value. To view the source systems reference, use the Manage Trading Community Source System task.	Conditionally Required To identify an account record, use one of these: • SourceSystem and SourceSystemRefe • PartyNumber	Conditionally Required To identify an account record, use one of these: • SourceSystem and SourceSystemRefe • PartyNumber	Conditionally Required To identify an account record, use one of these: • SourceSystem and SourceSystemReferenceValu • PartyNumber
PartyNumber	The public unique identifier of the party.	The party must exist. You get a list of all party IDs and party numbers by exporting the Party object.	Conditionally Required	Conditionally Required	Conditionally Required
OrganizationName	The name of the party of the Organization party type.	Organization names are listed in the Resource Directory.	Required	Conditionally Required	Conditionally Required
OwnerPartyId	The identifier of the account owner.	This attribute is required only in import management, but optional in high-volume import.	Required	Not Required	Not Required

Note: When deleting or updating accounts, you must ensure that the account related to the party number provided has the Sales Account usage. If you provide the party number of an account that doesn't have the Sales Account usage, then the relationships for that account are also deleted. For example, if you provide the party number ORA17292 that doesn't have a Sales Account usage, then the related partners, contacts, and so on are also deleted.

For the extension child objects of account, RecordName field isn't unique. Hence you can't update the records only by passing RecordName.

You can use the profile option ORA_HZ_IMPORT_MULTI_ADDRESS_TYPE to control how address types are entered. By default this profile option is set to Yes, so you can enter multiple address types, during high-volume import of Account,

Contact, and Household objects . You can disable this profile option to improve the import performance. When you set this profile option to No, you can enter only a single address type.

> **Note:** When importing accounts or legal entities, you can retrieve duplicates using the Customer Data Management Duplicates LOV only if you have licensed the data quality functionality. Once licensed, you must rebuild the keys for your matching configuration using the Manage Enterprise Data Quality Matching Configurations task. After the keys are rebuilt, the matching functionality uses the settings in the match configuration to identify duplicates.

Go to **Navigator** > **Tools** > **Import Management** > **Import Objects** to see all the attributes of the account object. The page also lists attribute information like type, length, description, and so on.

Create the Source CSV File

You include the data that you want to import into CX Sales and Fusion Service in a source CSV file.

You can use the templates available in the Import Objects UI page to create the source CSV file. To download a template:

1. Go to **Navigator** > **Tools** > **Import Management** > **Import Objects**.
2. Select the **Account** object in the table and click **Download**.

You can now edit the downloaded file and provide valid values for the required attributes.

Providing the ZIP and Country Code values in the import CSV file won't automatically populate the State/County/City fields. Values for these fields should be separately provided in the import file.

> **Note:** For help in populating the CSV file and to avoid any issues in entering values, see the topic Potential Issues When Opening CSV Files With Excel in Related Topics section.

Create the Import Activity

After you have the CSV file ready, create an import activity to import the account information. To create an import activity:

1. Go to **Navigator** > **Tools** > **Import Management** > **Import Queue**.
2. Click **Create Import Activity** in the **Manage Imports** page.
3. In the **Enter Import Options** page, provide a name for the import activity, and select Account from the **Object** drop-down list.
4. Select the CSV file in the **File Name** field, and click **Next.**
5. You would see that the source and target attributes are automatically mapped in the **Map Fields** page. Review and edit the mappings if required.
6. Check the file for unmapped columns or data format issues by clicking **Validate Data**. Click **Next.**
7. Review the import details on the **Review and Submit** page, and click **Submit** when you're ready.

Review the Import Results

Check if your import succeeded on the **Manage Imports** page. This page shows the status of all active, completed, and unsuccessful imports. To check the status of the import activity:

1. Go to **Navigator** > **Tools** > **Import Management** > **Import Queue**.
2. Click All Imports and search for the import activity that you created earlier.
3. Check the **Status** column for the import activity. The import is successful if the status displays as **Completed**. You can drill down on the import activity to go to the **Import Status** page which provides the status details of the import activity.

Note: After importing your data successfully, you need to run a couple of post processing jobs for duplicate identification, duplicate resolution, and account assignment. For more information on import management post processing jobs, see the topic *Import Management Post Processing Jobs*

When importing accounts you can now load the account hierarchy data. Use the following attributes to import accounts:

- ParentAccountPartyId
- ParentAccountPartyNumber
- ParentAccountSourceSystem
- ParentAccountSourceSystemReferenceValue

You can load account hierarchy data. To load the account hierarchy data:

1. Load the account data without providing values for the parent attributes mentioned above.
2. Load the account hierarchy using the Hierarchy and Hierarchy Member import objects. For more information, see *How do I import hierarchy data?* and *How do I import hierarchy member data?*

Delete an Account

Related Topics

- How do I import data?
- Import Your Address Data
- How do I import contact point data?
- How You Use Alternate Keys to Import Records
- Potential Issues When Opening CSV Files in Excel
- How You Enable Automatic Account Assignment

How do I import contact data?

You can use the Import Management to create, update, or delete contact records.

You can import contact records using these steps:

1. Map your source contact data to Oracle Applications Cloud object attributes. This way the import process would know where to insert each of the information bits.
2. Create the source CSV file with the contact data you want to import.
3. Kick off an import activity.
4. Check the import results to know if the import went well.

How You Map Your Source Data to Target Object Attributes

To import your contact data into Oracle Applications Cloud, you must populate a .csv file with your source data and map that source data to target object attributes in Oracle Applications Cloud.

You must do the following before creating the .csv file for data import:

- Identify how your source data attributes map to the target object attributes in Oracle Applications Cloud.

- Ensure prerequisite steps are complete, such as understanding what attributes are required for importing your objects.
- Understand your options for uniquely identifying the records.
- Ensure parent records exist before importing child records.
- Identify the target object attributes that are required in the .csv file for a successful import

To better manage your contact information, the contact object has the following child objects:

- Address
- Classification
- Relationship
- Sales Team Member

Note: You can't set an attribute value to NULL in optimized import (standard import with the option **Enable High-Volume Import** selected). However, when updating a record, you can change an attribute value from NOT NULL to NULL

If you want to import only a few records, then you can create a single CSV file for all contact attributes. However if you want to import a large number of records, then you may decide to create multiple CSV files, one for each of the contact child objects. Note that you must have imported the CSV file for contact object successfully before trying to import the CSV files for the child objects. There are separate help topics describing how to import each of these child objects. For more information, see the related topics section.

Before You Start

You must do some basic checks before starting your import. For example, make sure that:

- You have completed all the prerequisites for importing each attribute in your source data.
- You have all parent records in place before importing child records.

Select a Unique Identifier for Your Records

All records must be unique in the application. You can use one of these to identify records:

- Public unique identifiers: If you're creating records, then you can provide an easily understandable public unique identifier. These are, usually, denoted with 'Number' and visible in the business object's UI. PUID attributes are usually named <object> Number. If you're updating a record with a Number attribute, then use the Number attribute to identify the record. For more information about public unique identifiers, see the topic "How You Use Alternate Keys to Import Records" in Related Topics section.
- Source system and source system reference: Source system is an identifier for the external system, and source system reference is a unique identifier within the external system. If you're importing new contacts or are updating contacts that have source system reference data, then provide the source system and source system reference values.

Required Attributes and Validations for the Contact Object

To import data successfully into Oracle Applications Cloud, your .csv file must include the required attributes. Ensure that you provide valid values for the attributes.

This table lists the required attributes for contact records, prerequisite setup tasks and specific validations, if any:

Attribute	Description	Prerequisite Setup Task or Import Validations	Creating a Contact Record	Updating an Existing Contact Record	Deleting an Existing Contact Record
`SourceSystem`	The code representing the source system for the contact.	Identify the source system or configure source systems either by using the Manage Trading Community Source System task, or by importing the source system information into Oracle Applications Cloud using the Source System Reference import object.	Conditionally Required For uniquely identifying a contact record, provide one of the following reference information: • SourceSystem and SourceSystemRefe • PartyNumber	Conditionally Required For uniquely identifying a contact record, provide one of the following reference information: • SourceSystem and SourceSystemRefe • PartyNumber	Conditionally Required For uniquely identifying a contact record, provide one of the following reference information: • SourceSystem and SourceSystemReferenceValu • PartyNumber
`SourceSystemRefere`	The reference number or text representing the source system unique ID for the contact.	Identify the source system or configure source systems either by using the Manage Trading Community Source System task, or by importing the source system information into Oracle Applications Cloud using the Source System Reference import object.	Conditionally Required For uniquely identifying a contact record, provide one of the following reference information: • SourceSystem and SourceSystemRefe • PartyNumber	Conditionally Required For uniquely identifying a contact record, provide one of the following reference information: • SourceSystem and SourceSystemRefe • PartyNumber	Conditionally Required For uniquely identifying a contact record, provide one of the following reference information: • SourceSystem and SourceSystemReferenceValu • PartyNumber
PartyNumber	The public unique identifier of the contact.	No prerequisite tasks	Conditionally Required	Conditionally Required	Conditionally Required
FirstName	First name of a person party.	No prerequisite tasks	Required	Not required	Not required
LastName	Last name of a person party.	No prerequisite tasks	Required	Not required	Not required

Note: For the **Time Zone** import attribute, specify the time zone of the contact to know the preferred time to call or send e-mail to the contact.

You can use the profile option ORA_HZ_IMPORT_MULTI_ADDRESS_TYPE to control how address types are entered. By default this profile option is set to Yes, so you can enter multiple address types, during high-volume import of Account, Contact, and Household objects . You can disable this profile option to improve the import performance. When you set this profile option to No, you can enter only a single address type.

Go to **Navigator** > **Tools** > **Import Management** > **Import Objects**, to see all the attributes of the contact object. The page also lists attribute information like type, length, description, and so on.

Create the Source CSV File

You include the data that you want to import into CX Sales and Fusion Service in a source CSV file.

You can use the templates available in the Import Objects UI page to create the source CSV file. To download a template:

1. Go to **Navigator** > **Tools** > **Import Management** > **Import Objects**.
2. Select the **Contact** object in the table and click **Download**.

You can now edit the downloaded file and provide valid values for the required attributes.

Providing the ZIP and Country Code values in the import CSV file won't automatically populate the State/County/City fields. Values for these fields should be separately provided in the import file.

> **Note:** For help in populating the CSV file and to avoid any issues in entering values, see the topic Potential Issues When Opening CSV Files With Excel in Related Topics section.

Create the Import Activity

After you have the CSV file ready, create an import activity to import the contact information. To create an import activity:

1. Go to **Navigator** > **Tools** > **Import Management** > **Import Queue**.
2. Click **Create Import Activity** in the **Manage Imports** page.
3. In the **Enter Import Options** page, provide a name for the import activity, and select Contact from the **Object** drop-down list.
4. Select the CSV file in the **File Name** field, and click **Next.**
5. You would see that the source and target attributes are automatically mapped in the **Map Fields** page. Review and edit the mappings if required.
6. Check the file for unmapped columns or data format issues by clicking **Validate Data**. Click **Next.**
7. Review the import details on the **Review and Submit** page, and click **Submit** when you're ready.

Review the Import Results

Check if your import succeeded on the **Manage Imports** page. This page shows the status of all active, completed, and unsuccessful imports. To check the status of the import activity:

1. Go to **Navigator** > **Tools** > **Import Management** > **Import Queue**.
2. Click All Imports and search for the import activity that you created earlier.
3. Check the **Status** column for the import activity. The import is successful if the status displays as **Completed**. You can drill down on the import activity to go to the **Import Status** page which provides the status details of the import activity.

> **Note:** After importing your data successfully, you need to run a couple of post processing jobs for duplicate identification, duplicate resolution, and account assignment. For more information on import management post processing jobs, see the topic: Import Management Post Processing for Accounts and Contacts.

Related Topics

- Potential Issues When Opening CSV Files in Excel
- How You Use Alternate Keys to Import Records

How do I import organization data?

You can use Import Management to create or update Organization records.

To import Organization records, perform the following tasks:

1. Map your source data to Oracle Applications Cloud object attributes.
2. Create source Comma Separated Values (CSV) file for import.
3. Create the import activity.
4. Review the import results.

How You Map Your Source Data to Target Object Attributes

To import your Organization data into Oracle Applications Cloud, you need to populate a CSV file with your source data and map that source data to target object attributes in Oracle Applications Cloud.

You need to do the following before creating the CSV file for data import:

- Identify how your source data attributes map to the target object attributes in Oracle Applications Cloud.
- Ensure prerequisite setups are done, if applicable.
- Understand your options for uniquely identifying the records.
- Ensure parent records exist before importing child records.
- Identify the target object attributes that are required in the CSV file for a successful import.
- Ensure that you don't insert duplicate addresses while importing, to avoid redundant data.

Before You Start

You must do some basic checks before starting your import. For example, make sure that:

- You have completed all the prerequisites for importing each attribute in your source data.
- You have all parent records in place before importing child records.

Select a Unique Identifier for Your Records

All records must be unique in the application. You can use one of these to identify records:

- Public unique identifiers: If you're creating records, then you can provide an easily understandable public unique identifier. These are, usually, denoted with 'Number' and visible in the business object's UI. PUID attributes are usually named <object> Number. If you're updating a record with a Number attribute, then use the Number attribute to identify the record. For more information about public unique identifiers, see the topic "How You Use Alternate Keys to Import Records" in Related Topics section.
- Source system and source system reference: Source system is an identifier for the external system, and source system reference is a unique identifier within the external system. If you're importing new organizations or are updating organizations that have source system reference data, then provide the source system and source system reference values.

Required Attributes and Validations for Organization Object

To import data successfully into Oracle Applications Cloud, your CSV file must include the required attributes. Ensure that you provide valid values for the attributes. This table lists the required attributes for importing new Organization records, required attributes for updating Organization records, prerequisite setup tasks for the attributes, and specific validations, if any, for Organization import:

Attribute	Description	Prerequisite Setup Task/ Import Validations	Creating an Organization Record	Updating an Existing Organization Record
SourceSystem	The original source system name	Know the source system. To view source systems, use the Manage Trading Community Source System task.	Conditionally Required To identify an organization record, use one of these: • Combination of SourceSystem and SourceSystemReferenc • PartyNumber	Conditionally Required To identify an organization record, use one of these: • Combination of SourceSystem and SourceSystemReferenceValue • PartyNumber
SourceSystemReferenceValu	The identifier in the original source system	Know the source system reference value. To view the source systems reference, use the Manage Trading Community Source System task.	Conditionally Required To identify an organization record, use one of these: • Combination of SourceSystem and SourceSystemReferenc • PartyNumber	Conditionally Required To identify an organization record, use one of these: • Combination of SourceSystem and SourceSystemReferenceValue • PartyNumber
PartyNumber	The public unique identifier of the party.	Know party number. To obtain a list of all party IDs and party numbers, export the Party object.	Conditionally Required	Conditionally Required
OrganizationName	The name of the party of the Organization party type.	The organization names are listed in the Resource Directory.	Required	Conditionally Required
PartyUsageCode	Specifies the party usage code to which the organization is associated	This should be an active value in the HZ_PARTY_USAGES_B table.	Required	Not required
CleanlinessScore	The overall score for the account or contact record for the category **Cleanliness**	No validation	Optional	Optional
CompletenessScore	The overall score for the account or contact record for the category **Completeness**	No validation	Optional	Optional

Attribute	Description	Prerequisite Setup Task/ Import Validations	Creating an Organization Record	Updating an Existing Organization Record
DataConfidenceScore	The overall data confidence score that indicates the level of data quality for a record	No validation	Optional	Optional
DuplicateIndicator	Signifies the duplicate status of the record that's determined as follows: • A null value indicates that the record isn't a duplicate or hasn't been evaluated. • The record can also have one of 2 other values - DUPE (record is a duplicate) or LINK (record is linked to another record).	No validation	Optional	Optional
DuplicateScore	The overall score for the account or contact record for the category **Duplicate**	No validation	Optional	Optional
EnquiryDuns	A unique identifier used to query the Dun and Bradstreet data. If the location is a branch, in some countries the "DUNS" number of the headquarters is used to run the query. Otherwise, the "DUNS" number is considered.	No validation	Optional	Optional
EnrichmentScore	The overall score for the account or contact record for the category **Enrichment**	No validation	Optional	Optional
LastScoreUpdateDate	The date and time at which this record was updated by the source system in the last update source system column	No validation	Optional	Optional
RecencyScore	The overall score for the account or contact record for the category **Recency**	No validation	Optional	Optional
ThirdPartyFlag	This option tracks if a party has a direct relationship with the organization using Oracle receivables	No validation	Optional	Optional

Attribute	Description	Prerequisite Setup Task/ Import Validations	Creating an Organization Record	Updating an Existing Organization Record
	or through a third party supplier. The value Y denotes third party relationship, while the value N denotes direct relationship. If Oracle Service is installed, the Third Party field in the Customers window is mandatory.			
ValidatedFlag	Indicates if the party was validated. The value Y denotes a validated party, while the value N denotes a party that's not validated.	No validation	Optional	Optional
ValidityScore	The overall score for the account or contact record for the category **Validity**	No validation	Optional	Optional

You can view the Organization object along with all its child objects and attributes in the Manage Import Objects page of the Import Management flow. You can find attribute information like type, length, description, and so on, on this page.

Create the Source CSV File

You include the data that you want to import into CX Sales and Fusion Service in a source CSV file.

You can use the templates available in the Import Objects UI page to create the source CSV file. To download a template:

1. Go to **Navigator** > **Tools** > **Import Management** > **Import Objects**.
2. Select the **Organization** object in the table and click **Download**.

You can now edit the downloaded file and provide valid values for the required attributes.

> **Note:** For help in populating the CSV file and to avoid any issues in entering values, see the topic Potential Issues When Opening CSV Files With Excel in Related Topics section.

Create the Import Activity

After you have the CSV file ready, create an import activity to import the information. To create an import activity:

1. Go to **Navigator** > **Tools** > **Import Management** > **Import Queue**.
2. Click **Create Import Activity** in the **Manage Imports** page.
3. In the **Enter Import Options** page, provide a name for the import activity, and select Organization from the **Object** drop-down list.
4. Select the CSV file in the **File Name** field, and click **Next.**
5. You would see that the source and target attributes are automatically mapped in the **Map Fields** page. Review and edit the mappings if required.
6. Check the file for unmapped columns or data format issues by clicking **Validate Data**. Click **Next.**
7. Review the import details on the **Review and Submit** page, and click **Submit** when you're ready.

Review the Import Results

Check if your import succeeded on the **Manage Imports** page. This page shows the status of all active, completed, and unsuccessful imports. To check the status of the import activity:

1. Go to **Navigator** > **Tools** > **Import Management** > **Import Queue**.
2. Click All Imports and search for the import activity that you created earlier.
3. Check the **Status** column for the import activity. The import is successful if the status displays as **Completed**. You can drill down on the import activity to go to the **Import Status** page which provides the status details of the import activity.

Related Topics

- How do I import data?
- Potential Issues When Opening CSV Files in Excel
- How You Use Alternate Keys to Import Records

How do I import person data?

You can use import management to create or update Person data.

You can import Person records using these steps:

1. Map your source data to Oracle Applications Cloud object attributes. This way the import process would know where to insert each of the information bits.
2. Create the source CSV file with the Person data you want to import.
3. Kick off an import activity.
4. Check the import results to know if the import went well.

How You Map Your Source Data to Target Object Attributes

You import Person data into Oracle Applications Cloud from a CSV file containing your source data that's mapped to target Oracle Applications Cloud object attributes.

Before you create the source data file, you should:

- Know how your source data attributes map to the target object attributes in Oracle Applications Cloud. Match each column from the source file to an attribute in the Person import object.
- Finish all prerequisite steps, such as understanding what attributes are required for importing your objects.
- Know how you can uniquely identify the records.
- Check the target object attributes required in the CSV file for a successful import.
- Ensure that you don't insert duplicate Person while importing, to avoid redundant data.

Before You Start

You must do some basic checks before starting your import. For example, make sure that:

- You have completed all the prerequisites for importing each attribute in your source data.
- You have all parent records in place before importing child records.

Select a Unique Identifier for Your Records

All records must be unique in the application. You can use one of these to identify records:

- Public unique identifiers: You can pass the PUID when creating Person records. If the PUID isn't passed, it will be auto generated. You can optionally provide the PUID when creating Person records. If you're updating records, then you can provide an easily understandable public unique identifier. These are, usually, denoted with 'Number' and visible in the business object's UI. PUID attributes are usually named <object> Number. If you're updating a record with a Number attribute, then use the Number attribute to identify the record. For more information about public unique identifiers, see the topic "How You Use Alternate Keys to Import Records" in Related Topics section.
- Source system and source system reference: Source system is an identifier for the external system, and source system reference is a unique identifier within the external system. If you're importing new Persons or are updating Persons that have source system reference data, then provide the source system and source system reference values.

Required Attributes and Validations for Person Object

To import data successfully into Oracle Applications Cloud, your .CSV file must include the required attributes. Ensure that you provide valid values for the attributes.

This table lists the required attributes for Person records, prerequisite setup tasks and specific validations, if any:

Attribute	Description	Prerequisite Setup Task/ Import Validations	Creating a Person record	Updating an Existing Person record
PartyId	The internal ID for the Person type party	When updating the record, this should already exist.	Not required	Conditionally required. To identify a person record, use one of these: • Combination of SourceSystem and SourceSystemReferenceValue • PartyNumber • PartyId
Country	The country code of the postal address	Identify valid country codes using the Setup and Maintenance, Manage Territories task.	Conditionally required A value is required only when you're creating an address for the Person record.	The attribute is neither required nor conditionally required.
AddressNumber	The internal unique identifier that's internally generated when creating an address	No validation	This is a PUID for Address. If a value is passed, it will be imported. Otherwise, it will be auto-generated.	Pass the AddressNumber.
OrganizationPartyNumber	The party number of the organization to which the person is related	This should already exist.	Not required	Not required

Attribute	Description	Prerequisite Setup Task/ Import Validations	Creating a Person record	Updating an Existing Person record
DeceasedFlag	The option that indicates whether the person imported is deceased	Y or N The default value is N.	Not required	Not required
PartyNumber	The unique identifier of the party	Know the party number. To obtain a list of all party IDs and party numbers, export the Person object.	This is a PUID for Person. If a value is passed, it will be imported. Otherwise, it will be auto-generated.	Conditionally required To identify a person record, use one of these: • Combination of SourceSystem and SourceSystemReferenceValue • PartyNumber • PartyId
FirstName	The first name of the person	No validation	Required. A value is required for the FirstName, MiddleName, or LastName.	Not required
MiddleName	The middle name of the person	No validation	Required. A value is required for the FirstName, MiddleName, or LastName.	Not required
LastName	The last name of the person	No validation	Required. A value is required for the FirstName, MiddleName, or LastName.	Not required
PartyUsageCode	Specifies the party usage code to which the person is associated	Select one of the following values: • EXTERNAL_PAYEE • CONTACT • PAYMENT_ISSUING_AUTHORITY • PARTY_OF_INTEREST • VIRTUAL_ASSISTANT • FS_TECH You can assign a limited set of unrestricted party usages through the Person import object. To create persons of other types, use the specific import objects created for those purposes.	Required	Not required
SourceSystem	The original source system name	Know the source system. To view source systems, use the Manage Trading Community Source System task.	Conditionally required To identify a person record, use one of these:	Conditionally required To identify a person record, use one of these:

Attribute	Description	Prerequisite Setup Task/ Import Validations	Creating a Person record	Updating an Existing Person record
			• Combination of SourceSystem and SourceSystemReferenc • PartyNumber	• Combination of SourceSystem and SourceSystemReferenceValue • PartyNumber • PartyId
SourceSystemReferenceValu	The identifier in the original source system	Know the source system reference value. To view source system reference, use the Manage Trading Community Source System task.	Conditionally required To identify a person record, use one of these: • Combination of SourceSystem and SourceSystemReferenc • PartyNumber	Conditionally required To identify a person record, use one of these: • Combination of SourceSystem and SourceSystemReferenceValue • PartyNumber • PartyId

Go to **Navigator** > **Tools** > **Import Management** > **Import Objects**, to see all the attributes of the Person object. The page also lists attribute information like type, length, description, and so on.

Create the Source CSV File

You include the data that you want to import into CX Sales and Fusion Service in a source CSV file.

You can use the templates available in the Import Objects UI page to create the source CSV file. To download a template:

1. Go to **Navigator** > **Tools** > **Import Management** > **Import Objects**.
2. Select the Person object in the table and click Download.

You can now edit the downloaded file and provide valid values for the required attributes.

> **Note:** For help in populating the CSV file and to avoid any issues in entering values, see the topic Potential Issues When Opening CSV Files With Excel in Related Topics section.

Create the Import Activity

After you have the CSV file ready, create an import activity to import the Person information. To create an import activity:

1. Go to **Navigator** > **Tools** > **Import Management** > **Import Queue**.
2. On the **Manage Imports** page, click **Create Import Activity**.
3. In the **Create Import Activity: Enter Import Options** page, provide a name for the import activity, and select **Person** from the **Object** drop-down list.
4. Select the CSV file in the File Name field, and click Next.
5. You would see that the source and target attributes are automatically mapped in the Map Fields page. Review and edit the mappings if required.
6. Check the file for unmapped columns or data format issues by clicking Validate Data. Click Next.
7. Review the import details on the Review and Submit page, and click Submit when you're ready.

Review the Import Results

Check if your import succeeded on the Manage Imports page. This page shows the status of all active, completed, and unsuccessful imports. To check the status of the import activity:

1. Go to **Navigator** > **Tools** > **Import Management** > **Import Queue**.
2. Click All Imports and search for the import activity that you created earlier.
3. Check the Status column for the import activity. The import is successful if the status displays as Completed. You can drill down on the import activity to go to the Import Status page which provides the status details of the import activity.

Related Topics

- How You Use Alternate Keys to Import Records
- Potential Issues When Opening CSV Files in Excel
- Why can't I see the people I just imported?

8 Configure Profile Options

Overview of Profile Options Setup

Profile options are a set of preferences that you can use to centrally manage the user interface settings, data access and processing, and application action.

Customer data management profile options let you view or change the address cleansing configuration, matching configuration, duplicate resolution request options, and various thresholds such as auto link, auto merge, and batch sizes. You can set these profile option values only at the site level.

Note that you don't have to change the default values of any profile options to use Customer Data Management for the basic implementation case study described in this guide. However, you should be familiar with them to make sure that the correct configurations, actions, and thresholds are selected for your business requirements.

Here's a table that lists the setup tasks that you can use to configure these profile options to your business requirements:

Step	Description	Task Name	Where to Get More Details
Configure the customer hub profile options	Configure the customer hub profile options to calibrate address cleansing configuration, matching configuration, duplicate resolution request options, and various thresholds such as auto link, auto merge, and batch sizes per your business requirements	Manage Customer Hub Profile Options	See the topic: • Manage Customer Hub Profile Options
Setup Duplicate Resolution Simplified Profile Options	Setup duplicate resolution simplified profile options to: • Fine-tune the performance and control the flow and level of automation of your duplicate resolution processes • Control the processing logic that governs the final outcome of a merge request	Manage Customer Data Management Options	See the topic: How You Setup Duplicate Resolution Simplified Profile Options

Key Customer Data Management Profile Options

Here's a table that lists some important Customer Data Management profile options, along with their names, descriptions and default values.

Profile Option Name	Profile Option Definition	Description	Default Value
ZCH_CLNS_PROC_BT_SIZE	Data Cleansing Process Batch Size	The transaction batch size for the data cleansing process. Set this value based on available system resources.	10000
ZCH_DEDUP_REQUEST_TYPE_OPTION	Resolution Request Type Default	The default request type for the duplicate resolution requests.	Merge
ZCH_DI_PROC_BT_SIZE	Duplicate Identification Process Batch Size	The transaction batch size for the duplicate identification process. It's used to group records in the batch and process each group in a loop as a separate transaction.	100
ZCH_USER_MERGE_REQUESTS	User Merge Requests	The processing options for merge requests. This option applies only for merge requests submitted from FUSE UI or EUM UI in Enter Merge Request setup task.	Unspecified (NULL)
ZCH_ENABLE_SURVIVORSHIP	Survivorship Enabled	The option to enable survivorship rules for duplicate resolution.	Yes
ZCH_AUTO_LINK_THRESHOLD	Auto Link Threshold	The threshold for auto link. Data stewards review link requests with lower scores.	0
ZCH_AUTO_MERGE_THRESHOLD	Auto Merge Threshold	The threshold for auto merge. Data stewards review merge requests with lower scores.	100
ZCH_DI_MERGEREQ_REC_SIZE	Duplicate Set Record Number	The maximum number of records in a duplicate set that can be automatically converted to duplicate resolution requests.	10
ZCM_ACC_EXACT_NAME_MATCH	Exact Account Name Match	This option controls the display of duplicate accounts based on an exact name match when no duplicate accounts were found from data quality configuration.	FALSE
ZCM_CON_EXACT_NAME_MATCH	Exact Contact Name Match	This option controls the display of duplicate contacts based on an exact name match when no duplicate contacts were found from data quality configuration.	FALSE
ZCM_ACC_DUP_NOTIFICATION	Duplicate Account Notification	This option controls whether the UI that shows notifications for duplicate accounts should be enabled or not.	TRUE

Profile Option Name	Profile Option Definition	Description	Default Value
		This option is available only if you have Oracle Fusion Data Quality.	
ZCM_CON_DUP_NOTIFICATION	Duplicate Contact Notification	This option controls whether the UI that shows notifications for duplicate contacts should be enabled or not. This option is available only if you have Oracle Fusion Data Quality.	TRUE
ORA_ZCH_OPTIMIZE_LOAD	Optimized Mode Enabled	Enable the optimized mode for merge to prevent the triggering of non-essential business events.	N

You must consider the following point while setting the values of the Customer Hub profile options:

- The profile option User Merge Requests is set to Unspecified (NULL) by default. You can set the following values for this profile option:
  - **Allow Processing Without Approval**: Merge requests are processed immediately without approval by the data steward.
  - **Process Subject to Approval**: Merge requests are reviewed by the data steward, who can decide to approve or not.
  - **Unspecified**: Merge requests are processed immediately without data steward approval. This indicates that the Customer Hub isn't configured. The option is enabled only if the user has the Submit Trading Community Merge Request and Enter Trading Community Merge Request privileges.
- Data stewards must review merge requests initiated from the Simplified UI, Enter Merge Request setup task, Automerge web service, or the Duplicate Resolution Request web service. Data stewards can review merge requests only if the profile option User Merge Requests is set to Process Subject to Approval, else the merge requests returns an error.
- Auto Link Threshold is set to 0 by default, which means auto link never occurs automatically. Maximum auto merge threshold is 100, which means unless there is a 100 percent match, there is no auto merge. You need to change the threshold based on customer implementation.

Data Quality Profile Options

Data quality profile options configure data access and processing for duplicate identification processes and data cleansing processes.

The following table lists data quality profile options, descriptions, and default values.

To view the details of these profile options:

1. Click **Navigator** > **My Enterprise** > **Setup and Maintenance** work area.
2. Click the Tasks menu and click **Search**. Search for **Manage Profile Options** task and open it.
3. Search using the profile option code.

To change the default values of these profile options

1. Click **Navigator** > **My Enterprise** > **Setup and Maintenance** work area.
2. Click the Tasks menu and click **Search**. Search for **Manage Administrator Profile Values** task and open it.
3. Search using the profile option code.
4. Change the profile value.

Profile Option Code	Profile Option Name	Default Value	Description
ORA_ZCQ_MAX_CANDIDATES	Interactive Duplicate Identification List Size	20	This profile option lets you limit the number of possible duplicates which may be returned by the interactive duplicate identification interface.
ORA_ZCQ_BATCHMATCH_DEBUG_LEVEL	Batch Duplicate Identification Debug Level	INFO	This profile option controls the level of diagnostic logging for batch duplicate identification processes.
ORA_ZCQ_LEVEL_OF_INDIRECTION	Indirect Duplicate Candidates Level	0	This profile option controls the extent to which indirect duplicate candidates are considered during duplicate identification.
ORA_ZCQ_CONVERTER_FINEST_LOGGING	Data Quality Match Value Conversion Logging	N	This profile options controls the logging on the data quality match value conversion process. When this profile option is set to Y, data quality logs are written in the log file.
ORA_ZCQ_CS_DATA_REFRESH_TIME_HRS	Refresh Duplicate Identification Custom Scoring Dictionary Cache	12	This profile option controls the frequency in hours for refreshing the custom scoring data dictionary cache.
ORA_ZCQ_CHUNK_SIZE_FOR_CLEANSE_BATCH	Address Cleansing Batch Transaction Size	200	This profile option controls the number of records that are saved per transaction during batch address cleansing.
ORA_ZCQ_ENABLE_ADDR_MATCH_OBJECT	Address Duplicate Identification Match Configuration Enabled	No	This profile option enables the display of inactive Address Duplicate Identification configuration in Manage Enterprise Data Quality Matching Configurations UI page. This profile option works with the Data Quality Caching and Refresh Enabled (ORA_ZCQ_ENABLE_CACHE) profile option.
ORA_ZCQ_ENABLE_CACHE	Data Quality Caching and Refresh Enabled	500	This profile option enables the caching and refresh of frequently used data, such as server address,

Profile Option Code	Profile Option Name	Default Value	Description
			in the data quality matching processes.
ORA_ZCQ_CUSTOMSCORING_CLUSTER_COUNT	Batch Duplicate Identification Custom Scoring Candidate Keys		Specify the number of match key candidates per driver record key during batch duplicate identification candidate selection for custom scoring. **Note:** This is an Oracle internal setting. We recommend that you don't change this value unless instructed by Oracle Support.

Manage Customer Hub Profile Options

Here's how you can set up customer hub profile options.

You can configure these profile options by completing the following steps:

1. Open the Manage Customer Hub Profile Options task from the implementation project. Alternatively, Alternatively, in the Setup and Maintenance work area go to the following:
    - Offering: Customer Data Management
    - Functional Area: Customer Hub
    - Task: Manage Customer Hub Profile Options
2. Search for and select the profile option that you want to configure on the Manage Customer Hub Profile Options page.
3. Select the appropriate profile option value, in the Profile Values area of the page.
4. Click Save and Close.

Duplicate Identification Simplified Profile Options

How do I set up duplicate identification simplified profile options?

You can configure the duplicate identification simplified profile options in the Setup and Maintenance work area.

Navigate as follows:

- Offering: Customer Data Management
- Functional Area: Customer Hub
- Task: Manage Customer Data Management Options

Click the Duplicate Identification tab.

You can use these profiles options to specify:

Tuning

You can use this group of profile options to fine-tune the performance of your duplicate identification processes. The profile options under this category are:

- Enable Real-Time Key Generation
- Number of Batch Key Generation Jobs
- Number of Batch Matching Jobs
- Number of Real-Time Possible Duplicates

Advanced Options

You can use this set of profile options to configure diagnostic profile options that aren't related to the standard configuration activities. The profile options under this category are:

- Batch Duplicate Identification Debug Level
- Enable Fine Logging for Match Value Conversion

You can find more details about the duplicate identification simplified profile options in the individual topics about them.

Enable Real-Time Key Generation

This setting controls whether CDM generates real-time business events for updating cluster keys whenever a customer record is created or modified. The underlying profile option is ORA_ZCQ_ENABLE_REALTIME_KEYGEN.

The options are:

- Yes: Specifies that the real-time business events trigger cluster key generation whenever a record is created or modified.
- No: Specifies that the real-time business events aren't triggered.

Consider these points when working with this setting:

- A recurring incremental batch key generation job is always required, regardless of this setting.
- Not all processes generate cluster key generation events, regardless of this setting. For example, file-based record creation and updating don't generate key generation events.
- We recommend that you review the best practices before changing this setting listed in the Related Topics section.

Number of Batch Key Generation Jobs

This setting controls whether CDM specifies the maximum number of batch cluster key generation child jobs. The underlying profile option ZCQ_BATCH_KEYGEN_NUMJOBS.

Number of Batch Matching Jobs

This setting controls whether CDM specifies the maximum number of batch duplicate identification child jobs. The underlying profile option ZCQ_BATCH_MATCH_NUMJOBS.

Number of Real-Time Possible Duplicates

This setting controls the maximum number of possible duplicates that can be presented through a real-time interface, such as the Possible Duplicated popup window in Customer Center or the response to the REST findDuplicates API. The underlying profile option is ORA_ZCQ_MAX_CANDIDATES.

Before changing the Number of Real-Time Possible Duplicates setting, you must consider these points:

- The default value of 20 candidates is usually an optimal balance of performance, completeness, and usability.
- Increasing the number of returned candidates above the default value may affect the performance of real-time interfaces.
- Possible Duplicates are returned in descending order of their match score, thus the highest quality match candidates are presented first.
- Keep in mind how many possible duplicates your users are likely to review.

Batch Duplicate Identification Debug Level

This setting controls whether CDM specifies the level of diagnostic logging for batch duplicate identification processes. The underlying profile option is ORA_ZCQ_BATCHMATCH_DEBUG_LEVEL. The options are:

- Debug: Specifies that the diagnostic logging for batch duplicate identification processes is debug.
- Informational: Specifies that the diagnostic logging for batch duplicate identification processes is collecting information.

Enable Fine Logging for Match Value Conversion

This setting controls whether CDM enables fine logging for the data quality match value conversion process. The underlying profile option is ORA_ZCQ_CONVERTER_FINEST_LOGGING. The options are:

- Yes: Specifies that the fine logging for the data quality match value conversion process is enabled.
- No: Specifies that the fine logging for the data quality match value conversion process isn't enabled.

Duplicate Resolution Simplified Profile Options

How You Setup Duplicate Resolution Simplified Profile Options

You can configure the duplicate resolution simplified profile options in the Setup and Maintenance work area using the following:

- Offering: Customer Data Management
- Functional Area: Customer Hub
- Task: Manage Customer Data Management Options

You can use these profiles options to specify:

- Tuning

  You can use this group of profile options to fine-tune the performance of your duplicate resolution processes. These settings work together to provide multiple ways to optimize your performance based on your implementation scenario, project phase, and data shape. The profile options under this category are:

  - Maximum Concurrent Resolution Request Jobs Setting
  - Merge Mode Setting
  - Resolution Request Job Size Setting
  - Merge Scope Setting
  - Merge Request Notifications

- Duplicate Resolution Control

  Use the profile options belonging to this category to control the flow and level of automation of your duplicate resolution processes. These settings let you define where merge requests can originate and when data stewards need to be involved in duplicate resolution activities. The profile options under this category are:

  - Automerge Threshold Setting
  - Customer Center Merge Requests Setting
  - Default Resolution Type Setting
  - Data Steward Resolution Request Handling Setting
  - User Resolution Request Handling Setting

- Merge Behavior

  You can use this set of profile options to configure how the merge process handles the records in a duplicate resolution request. These settings let you control the processing logic that governs the final outcome of a merge request, such as which record is retained as the master and how the process derives its final attributes. The profile options under this category are:

  - Agreement Rules Type Setting
  - Attribute Selection Type Setting

    - Enable Attribute Source Tracking Setting
    - Master Record Selection Setting
    - Merge Identical Child Records Setting
    - Add Groovy to Attribute Selection Setting

- Link Behavior

  You can use this set of profile options to configure how the link process handles the records in a duplicate resolution request. These settings let you control the processing logic that governs the final outcome of a link request, that is, which record is selected as the master. The profile options under this category are:
    - Main Record Selection Setting
    - Autolink Threshold Setting

You can find more details about the duplicate resolution simplified profile options in the individual topics about them.

Add Groovy to Attribute Selection Setting

Controls whether logic written with Application Composer Data Quality Rules are used to determine which attribute values are selected for the master record.

The underlying profile option is ZCH_GROOVY_RULE. The options are:

- No: Use only the option selected for the Attribute Selection Type setting to determine which attribute values are selected for the master record.
- Yes: Combine logic written with Application Composer Data Quality Rules with the option selected for the Attribute Selection Type setting to determine which attribute values are selected for the master record.

Consider these points:

- You can't combine Data Quality Rules with the Oracle business rules Attribute Selection Type setting option.

Agreement Rules Type Setting

Controls the method used to prevent records from being merged into other records incorrectly.

The underlying profile option is ZCH_AGREEMENT_TYPE. The options are:

- Default agreement rules: Only the seeded agreement rules are processed. These rules can't be edited or disabled.
- Default agreement rules with Oracle business rules: In addition to the default rules, merge incorporates logic written with Oracle business rules using the Manage Agreement Rules setup task.
- Default agreement rules with Data Quality Rules: In addition to the default rules, merge incorporates logic written with Application Composer Data Quality Rules.

Consider these points:

- You can't use Oracle business rules to configure agreement rules or Data Quality Rules to configure agreement rules, if you have set the Merge Scope to Customer data management specific areas with restrictions.

Attribute Selection Type Setting

Controls the method used to coalesce attribute values from the different records in a merge set onto the master record.

The underlying profile option is ZCH_SETATTRIBUTE_TYPE. The options are:

- No attribute survivorship rules selected: Merge only replaces null values on the master with non-null values from the duplicates.
- Use source confidence with oldest record as the tie breaker: In addition to replacing nulls with non-nulls, merge picks the attributes for the master based on the source confidence values configured using the Manage Source System Confidence setup task. In the case of multiple records in the duplicate set sharing the highest source confidence value for a given attribute, the value created at the earliest point in time is selected.
- Use source confidence with newest record as the tie breaker: In addition to replacing nulls with non-nulls, merge picks the attributes for the master based on the source confidence values configured using the Manage Source System Confidence setup task. In the case of multiple records in the duplicate set sharing the highest source confidence value for a given attribute, the value created at the most recent point in time is selected.
- Use Oracle business rules: In addition to replacing nulls with non-nulls, merge picks the attributes for the master based on logic configured with Oracle business rules using the Manage Survivorship Rules setup task.

Consider these points:

- The source confidence-based survivorship methods use optimized internal processes and may offer the best performance.
- The Attribute Selection Type can't be Oracle business rules if the Merge Scope is set to Customer data management specific areas with restrictions.

Autolink Threshold Setting

Defines the match score at or above which a duplicate resolution request of type Link is processed without requiring a data steward to review the request. The underlying profile option is ZCH_AUTO_LINK_THRESHOLD.

Consider these points:

- The highest possible match score is 100. So, if you set this value to 101, you can prevent any automatic Link processing.
- Use this setting only when the Default Duplicate Resolution type is Link.

Automerge Threshold Setting

Defines the match score at or above which a duplicate resolution request of type Merge is processed without requiring a data steward to review the request. The underlying profile option is ZCH_AUTO_MERGE_THRESHOLD.

Consider these points:

- The highest possible match score is 100. So, if you set this value to 101, you can prevent automatic Merge processing.

- Use this setting only when the Default Duplicate Resolution type is Merge.

Customer Center Merge Requests Setting

Controls whether you can submit merge requests directly from the Customer Center Account and Contact list pages.

Consider these points:

- If this option is enabled, the User Merge Handling setting controls whether or not those requests require a data steward's review before being processed.

Data Steward Resolution Request Handling Setting

You can select the Data Steward Resolution Request Handling setting to specify if a batch duplicate resolution request job automatically processes records or requires a review by a data steward.

The underlying profile option for this setting is ORA_ZCH_DS_MERGE_REQUESTS. The options for this setting are:

- Allow Processing Without Approval: batch duplicate resolution requests are automatically processed without any intervention from the data steward.
- Process Subject to Approval: Data steward reviews manually the batch duplicate resolution requests before processing.

Consider these points:

- Use the Create Resolution Request task in Party Center pages to create manual resolution requests.

Default Resolution Type Setting

Controls which duplicate resolution process type are assigned to new duplicate resolution requests. The underlying profile option is ZCH_DEDUP_REQUEST_TYPE_OPTION.

The options are:

- Merge: New duplicate resolution requests are queued for merging the duplicates into one master record.
- Link: New duplicate resolution requests are queued for linking the duplicates to each other without merging the records. The records to remain active.
- Generic: The data steward selects the duplicate resolution process type before processing the resolution requests.

Consider these points:

- To implement automatic duplicate resolution request processing, you must select either Merge or Link for the Default Duplicate Resolution setting.
- A data steward can change the duplicate resolution request type while reviewing a duplicate resolution request.

Enable Attribute Source Tracking Setting

Controls whether the attribute-level change by source system is tracked. This tracking is required for survivorship processes that use source confidence configuration to determine which attribute values in a duplicate set are ultimately written onto the master record. The underlying profile option is ZCH_ENABLE_SURVIVORSHIP.

Consider these points:

- The 'Use source confidence with oldest record as the tiebreaker' and 'Use source confidence with newest record as tiebreaker' attribute selection options require Attribute Source Tracking to be enabled.
- Attribute selection options that use Oracle Business Rules can be used without enabling Attribute Source Tracking but those rules can't access source confidence values.
- Once enabled, Enable Attribute Source Tracking can't be disabled because breaks in the source tracking history invalidate source confidence-based logic.

Maximum Concurrent Resolution Request Jobs Setting

You can use the Maximum Concurrent Resolution Request Jobs setting to control the number of resolution request jobs that can be processed at any given time. If you don't set the maximum limit, all resolution request jobs are submitted for concurrent processing.

A greater number of concurrent resolution request jobs may clear a duplicate resolution request queue more quickly but may impact other processes and functions that use customer records. The underlying profile option is ORA_ZCH_MERGE_MAX_REQUEST_LIMIT.

Before specifying the limit for Maximum Concurrent Resolution Request Jobs, you must consider these points:

- The default value is 10 concurrent resolution request jobs.
- Increasing the number of concurrent resolution request jobs can be helpful during high-volume data initialization scenarios when processing the duplicate resolution queue is a high priority.
- The Maximum Concurrent Resolution Request Jobs setting and the Resolution Request Job Size setting work together to let you control the resolution request system better.

Main Record Selection Setting

Controls the method used to identify which record in a duplicate set becomes the main during a link. The underlying profile option is ORA_ZCH_LINK_SETMAIN_TYPE.

The options are:

- Main account is based on duplicate identification result: Internal logic of the duplication identification process determines the master.
- Select highest Customer Profile Quality Score as main: The record with the highest customer profile quality score is selected as the main record.
- Select the main record for link type using groovy scripts: Logic groovy script configured with Application Composer Data Quality Rules determines the main.

- Select the newest sales account as main: The record with the most recent creation date is the main.
- Select the oldest sales account as main: The record with the oldest creation date is the main.

Consider these points:

- The Select the older record as master and Select the latest record as master options use optimized internal processes and may offer the best performance.
- The Duplicate Identification batch process identifies a preliminary master record, but the final determination of master record occurs within duplicate resolution processing per the Master Record Selection Setting. Select the Select master based on duplicate identification results option if you want to retain the master record selection from the duplicate identification results.

Note: If the creation date value is exactly same for the records, then the party with the lowest party ID is chosen as the master record.

Merge Mode Setting

You can use the Merge Mode setting to select the optimized mode for merge to prevent the triggering of non-essential business events. This setting controls whether the merge uses preconfigured processing logic or workflows and generates integration events for Oracle Integration Cloud services.

Ideally, you should enable optimized mode for merge to improve application performance when:

- you're not integrating merge events with external systems.
- you don't need groovy scripts or object workflows to run when a master record is updated by a merge.

Merge Scope Setting

You can use the Merge Scope setting to specify the business areas to be processed during a merge. This setting optimizes the size of the merge memory and execution profile and application performance. The underlying profile option is ORA_ZCH_MERGE_SCOPE.

You can specify any of these areas as the merge scope:

- Customer data management specific areas: Merges Customer Data Management foundation entities such as Organizations, People, Addresses, Phone Numbers, and Email Addresses.
- Customer data management specific areas with restrictions: Merges the same entities as the CDM scope. However, processing throughput is maximized by not invoking survivorship rules, integration events, or extended processing logic. You can use this option for high-volume data initialization scenarios.
- All customer relationship management related areas: Merges Customer Data Management foundation entities and transfers CRM transactional data, such as Opportunities, Activities, or Service Requests, from duplicate records to the master record.
- All functional areas: Merges Customer Data Management foundation entities and all merge-enabled entities on the point of deployment.

Before specifying the merge scope, you should consider these points:

- Select the appropriate merge scope to get the best performance.
- When you use Customer Data Management specific areas with restrictions merge scope, you must only select compatible options for other settings:
    - Master Record Selection can't be survivorship rule.
    - Attribute Selection Type can't be Oracle business rules.
    - Agreement Rules Type can't be Oracle business rules.

Merge Identical Child Records Setting

Controls whether the merge process merges or transfer certain types of child records when they have the same values. This setting currently controls the processing of addresses, phone contact points, and email contact points. The underlying profile options is ORA_ZCH_MERGE_IDENTICAL.

Merge Request Notifications

Controls whether notifications are sent when duplicate resolution requests are assigned and processed.

The options are:

- Send notifications for new requests: User created merge requests are created with the Send Notifications parameter set to Yes.
- Don't send notifications for new requests: User created merge requests are created with the Send Notifications parameter set to No.
- Don't send any notifications: Merge notifications aren't sent regardless of the Send Notifications parameter value on individual merge requests.

Consider these points:

- The Send Notifications parameter of merge requests created through the Duplicate Identification Batch process can be set at the Duplicate Identification Batch level.
- The Send Notifications parameter value of individual merge requests can be modified on the Duplicate Resolution list page.

Resolution Request Job Size Setting

You can use the Resolution Request Job Size to specify the number of requests that each resolution request job can handle.

A greater number of resolution requests per resolution request job may increase resolution request processing throughput when the Merge Mode is optimized or the Merge Scope is set to Customer data management specific areas with restrictions. The underlying profile option is ORA_ZCH_MERGE_REQUEST_BATCH_SIZE_LIMIT.

Consider these points before specifying the resolution request job size:

- The default value is 100 resolution requests per resolution request job.
- Increasing the number of resolution requests per resolution request job can be helpful during high-volume data initialization scenarios when processing the duplicate resolution queue is a high priority.
- The Resolution Request Job Size setting and the Maximum Concurrent Resolution Request Jobs setting work together to let you have a fine-grained control of the resolution request system.
- Setting no value (null) for the Resolution Request Job Size setting distributes all pending resolution requests to the available resolution request jobs. If the ratio of resolution request to resolution request jobs is too high, system performance may be adversely affected.

What's the master record selection setting?

Controls the method used to identify which record in a duplicate set becomes the master during a merge.

The options are:

- Select master record using survivorship rule: Logic configured with Oracle business rules using the Manage Survivorship Rules setup task determines the master.
- Select the oldest record as master: The record with the earliest creation date is the master.
- Select the latest record as master: With the most recent creation date is the master.
- Select master based on duplicate identification results: Internal logic of the duplication identification process determines the master.
- Select master record using Data Quality Rules: Logic configured with Application Composer Data Quality Rules determines the master.

Consider these points:

- The Select the older record as master and Select the latest record as master options use optimized internal processes and may offer the best performance.
- Master Record Selection can't be survivorship rule or Data Quality Rules if the Merge Scope has been set to Customer data management specific areas with restrictions.
- The Duplicate Identification batch process identifies a preliminary master record, but the final determination of master record occurs within duplicate resolution processing per the Master Record Selection Setting. Select the Select master based on duplicate identification results option if you want to retain the master record selection from the duplicate identification results.

Note: If the creation date value is exactly same for the records, then the party with the lowest party ID is chosen as the master record.

User Resolution Request Handling Setting

Controls whether manually created resolution requests are processed automatically or require review by a data steward.

The underlying profile option is ZCH_USER_MERGE_REQUESTS. The options are:

- Allow Processing Without Approval: Manually created resolution requests are processed automatically.

- Process Subject To Approval: Data steward reviews manually created resolution requests before processing.

Consider these points:

- Use the Account and Contact list pages in Customer Center if Customer Center Merge Requests have been enabled to create manual merge requests or create requests automatically using duplicate resolution web services.

9 Configure Data Enrichment

Overview of Data Enrichment Setup

Data enrichment improves the quality of your existing organization (account) and person (contact) data, and it also enriches the data with additional information.

> **Note:** You require separate licenses for **Oracle Account Enrichment Cloud Service** and **Oracle Contact Enrichment Cloud Service** to be able to do data enrichment in the Customer data Management Cloud. These services are also known as Oracle Account and Contact Enrichment by Dun & Bradstreet (D&B).

You can use Oracle Account and Contact Enrichment by Dun & Bradstreet (D&B) to enrich your organization (account) and person (contact) data. Oracle Account and Contact Enrichment by Dun & Bradstreet (D&B) has the most up-to-date data for over 300 million companies and over 100 million contacts worldwide.

Data Stewards can enrich data in bulk in Customer Data Management Cloud using batch data enrichment in the Data Enrichment work area. Note that batch enrichment is only supported for Oracle Account and Contact Enrichment by Dun & Bradstreet (D&B) attributes that are mapped out of the box to the organization (account) and person (contact) attributes. Batch enrichment of custom attribute isn't supported. The batch data enrichment option lets you enrich data in bulk by creating and submitting batch-processing jobs in the Data Enrichment work area. Configuring this enrichment process requires the completion of the following set-up steps:

Step	Description	Task Name	Where to Get More Details
Subscribe to Oracle Account and Contact Enrichment by Dun & Bradstreet (D&B)	Purchase a subscription to Oracle Account and Contact Enrichment by Dun & Bradstreet (D&B)	N/A	See the topic: Configure Oracle Account and Contact Enrichment by Dun & Bradstreet (D&B)
Create Users	Create application users and administrators	N/A	See the topic: Configure Oracle Account and Contact Enrichment by Dun & Bradstreet (D&B)
Configure Customer Data Management Cloud to Oracle Account and Contact Enrichment by Dun & Bradstreet (D&B) Integration	Enter the URL of your Oracle Account and Contact Enrichment by Dun & Bradstreet (D&B) instance, security policy, and login credentials on the Manage Data Enrichment Integration page	Manage Data Enrichment Integration **Note:** We use Manage Data Enrichment Integration task instead of the Manage Integration with Oracle Data as a Service task for configuring enrichment. The Manage Integration with Oracle Data as a Service task isn't supported in later releases.	See the topic: Configure Oracle Account and Contact Enrichment by Dun & Bradstreet (D&B)
Manage Administrator Profile Values	Set the Profile Value for the `DAAS_PRODUCTION_MODE` profile option to NO to configure Customer Data	Manage Administrator Profile Values	See the topic: Configure Oracle Account and Contact Enrichment by Dun & Bradstreet (D&B)

Step	Description	Task Name	Where to Get More Details
	Management Cloud to Data Cloud Integration		

For more information on the setup process, let's see the topic Overview of the setup process in the Related Topics section.

Related Topics

- Overview of the Setup Process

Configure Oracle Account and Contact Enrichment by Dun & Bradstreet (D&B)

You can configure Oracle Account and Contact Enrichment by Dun & Bradstreet (D&B) by completing the following tasks:

1. Setup Your Account.
2. Create Users.
3. Configure the Manage Data Enrichment Integration task in the application.
4. Configure Manage Administrator Profile Values task in the application.

Set Up Your Account

Here are the steps that you can follow to setup your account for Oracle Account and Contact Enrichment by Dun & Bradstreet (D&B):

1. Subscribe to Oracle Account and Contact Enrichment by Dun & Bradstreet (D&B):
   a. Log on to the Oracle Cloud Application Console at https://cloud.oracle.com/sign-in. In case you don't yet have an Oracle Cloud account, you can sign up for Oracle Cloud.
   b. Purchase a subscription account for Oracle Account and Contact Enrichment by Dun & Bradstreet (D&B).
2. Add subscription to your Oracle Cloud account.

   You'll receive an email titled “Action Required: Welcome to New Oracle Cloud Service Subscription(s).” Follow the instructions in the email:

   - If you have an Oracle Cloud account, then click the **Add to existing cloud account** button. We recommend using your existing Oracle Cloud account to manage all your Oracle services.
     i. Specify your cloud Tenant name and click **Continue**
     ii. Specify your username and password and click **Sign In**.

     The **Add Subscription** page is displayed.
     iii. Add the new subscription to your tenancy. This page indicates the subscription name, subscription ID, and subscription description (with product SKU).

     > **Note:** Adding a subscription to a tenancy can't be done.

- If you're a new customer, then click the **Create new cloud account** button. The New Cloud Account Information sign up form is displayed.
  i. Specify your First name, Last name, and Email address. The email address is also the username for signing into the account. The person you specify here is the first administrator who can access the account and can create other users. This role also has full administrator permissions in your account.
  ii. Specify a password and confirm.
  iii. Specify a Tenancy Name. This is also called your cloud account name. When choosing a tenancy name, note the following:
    - The tenancy name or cloud account name is used to identify your account. The name is also used to create the URLs to access your cloud services. For example, if you call your tenancy "abccorp", an application URL might look like: https://abccorp-oracleservice.service.us.phoenix-1.ocs
    - The tenancy name must be unique, start with a lowercase letter and have no more than 25 lowercase letters or numbers. You can't use spaces or special characters.
  iv. Select a Home region where your services will be hosted.

  > **Note:** Your home region is the geographic location where your account and identity resources will be created. You can't change this after signing up. If you are not sure which region to select as your home region, contact your sales representative before you create your account.

  v. Read the terms of use and click Create Tenancy.

3. Create the Data Environment.
   You'll receive a another email titled “Get Started Now with Oracle Cloud”. Click the Sign In button in the email. The Create environment page is displayed.
   a. Specify the cloud account name, credentials that you provided while creating cloud account and click **Create**.
   b. On the Create environment page, specify the admin email and click **Create**.

   > **Note:** Ensure that you don’t select the Update option.

   A page containing the environment information is displayed.
   c. Click the environment name to view the environment details.
   d. Copy the Service console URL from the Environment information tab and other links you need from the Additional links tab.
4. Log on to the Oracle Cloud Applications Console to get the Oracle Account and Contact Enrichment by Dun & Bradstreet (D&B) API URL. When you sign in successfully, the Oracle Cloud Dashboard page displays a list of your activated services and the REST service endpoint URLs.
5. Create the OAuth client credentials as follows:
   a. In the Oracle Cloud Console home page, login to your cloud account.
   b. Click **Navigator** > **Account Management** > **Users**.
   c. On the User Management page, click the link on the message that the page is part of the new identity and access management experience.
   d. Click **Integrated applications** and click **Add application**.
   e. On the Add application popup, select **Confidential Application** and then click **Launch app catalog**.
   f. Type the name on the Add Confidential Application and click **Next**.
   g. On the Client configuration section, select **Configure this application as a client now** and select Resource Owner, Client credentials, and Refresh token options.

h. Click **Next**.
i. On the Web tier policy page, click **Finish**. You are now directed back to your application's Cloud Console.
j. Scroll up and click the **Activate** button.
k. Click the **Activate application** on the Activate application popup.

> **Note:** For any integration or using Oracle Account and Contact Enrichment by D&B APIs, you require the client credentials. Use these steps:
>
> a. Scroll down to the General Information section and copy the Client ID.
> b. Click **Show secret** in the **Client secret** section.
> c. Click the **Copy** link in the Client secret popup and click **Close** to copy the password.

Create Users

As part of creating users, you need to create administrators as well as application users.

Here is how you can go about creating administrators:

1. Log in as the Account Administrator to My Account.
2. Assign a Service Administrator (to monitor the service) and an Identity Administrator (to manage users). Service Administrator and Identity Administrator get activation emails with credentials to access the Oracle Cloud console.

Here is how you can go about creating application users:

1. Log in as the Identity Administrator to the Oracle Cloud Applications Console.
2. On the Users page, click Add.
3. Enter the data center where Oracle Account and Contact Enrichment by Dun & Bradstreet (D&B) is located, your identity domain and your temporary password. (This information is listed in your Welcome email. If you can't find this email, the account administrator can resend it from My Account.)
4. Expand the Advanced Roles section, and add the Data Service Client AppID role for this user.
5. Click Add to create this user.

If the new users don't already have a password for this domain, they get an email with a temporary password. They can reset the password in the Oracle Cloud Applications Console. (The user now has credentials, but still needs to know the service URLs to log on. The Service administrator or the Identity administrator can provide this from the Welcome email.)

Configure Customer Data Management Cloud to Account and Contact Enrichment by Dun & Bradstreet Integration

Here are the steps that you can follow to configure Customer Data Management Cloud to Account and Contact Enrichment by Dun & Bradstreet Integration to do batch data enrichment in the Data Enrichment work area:

1. Sign in to Customer Data Management Cloud as a setup user.
2. Navigate to Setup and Maintenance.
3. Click the Tasks side panel to open it, and click Search.
4. Search for and go to the task: Manage Data Enrichment Integration.
5. Do the following on the Manage Data Enrichment Integration:
   Select OAuth Authentication in the DaaS Credentials section.

For information about adding a confidential application and getting the Client ID and Secret, see Add a Confidential Application topic in the Administering Oracle Identity Cloud Service guide.

> **Note:** On the Client page of the Add Confidential Application wizard, in the Authorization section, select Resource Owner, Client Credentials, Authorization Code, and Refresh Token as Allowed Grant Types. Leave Redirect URL blank.

> **Note:** We strongly recommend that you use OAuth authentication method because Basic authentication isn't supported in later releases. If you use Basic Authentication, don't include the question mark special character (?) in the password. For URL, remove /data/ui from the end of the instance address listed in your Welcome email and in the Cloud Console.

For URL, remove /data/ui from the end of the instance address listed in your Welcome email and in the Cloud Console.

For example, https://mydataservice-myidentitydomain.data.us2.oraclecloud.com.

6. Click Save and Close.

Requesting the Welcome Email to be Resent

Setup steps for this service are sent through a welcome email to the customer when the license is purchased. If the URL of Oracle Account and Contact Enrichment by Dun & Bradstreet (D&B) instance is missing and the customer administrator has already activated the service, then the customer administrator can request resend of the Welcome email by going to http://cloud.oracle.com > My Account (see the following figure).

The following figure highlights the Resend Welcome Email button on the My Accounts page.

However, if the customer administrator didn't receive a welcome email with links to activate the service, then the customer will have to log a service request to have Oracle Support resend the welcome email so that the customer administrator can activate the service. Instructions on how to log a service request and the Customer Support Identifier associated to the service request are described in the FAQ section of Getting Started with Oracle Cloud in the Help Center.

Manage Administrator Profile Values

Here are the steps that you can follow to manage administrator profile values:

1. Navigate to Setup and Maintenance.
2. Search for and go to the Manage Administrator Profile Values task.
3. Enter DAAS_PRODUCTION_MODE as the Profile Option Code on the Manage Administrator Profile Values page.
4. Click Search. The specified Profile Option appears as the search result.
5. Make sure that the Profile Level is Site and the Profile Value is set to No.

   > **Note:** Do not set the Profile Level Site value to Yes. The only supported value today is No.

6. Click Save and Close.

   The integration between Oracle Account and Contact Enrichment by Dun & Bradstreet (D&B) and Oracle Customer Data Management Cloud is now complete. You can find more information about Oracle Account and

Contact Enrichment by Dun & Bradstreet (D&B) in the Using Oracle Account and Contact Enrichment by Dun & Bradstreet (D&B) guide.

Configure Enrichment Preferences

Specify if you want to enable enrichment of accounts, contacts, or both, and configure enrichment preferences to define what data is updated in an enriched account or contact.

CAUTION: Ensure that you configure attribute mappings before you start configuring enrichment preferences.

1. Click **Navigator** > **My Enterprise** > **Setup and Maintenance** work area.
2. Click the Tasks menu and click Search. Search for Manage Oracle Data as a Service Attribute Mapping and Preferences and open it.

   This page includes two tabs, one for accounts and another one for contacts. You can use these to enable enrichment for accounts and contacts, and configure the data that should be included in the enriched account.
3. Select **Account** or **Contact** to enable enrichment for accounts or contacts, respectively.
4. Enter a match threshold for accounts and contacts in the **Match Threshold** field.
5. Enter the maximum number of records that should be enriched in the **Maximum Number of Accounts for Real-Time Enrichment** and **Maximum Number of Contacts for Real-Time Enrichment** fields.
6. In case of contact enrichment, enter the maximum number of new contacts to create during enrichment in the **Maximum Number of New Contacts** field.
7. Map the source attributes with the required sales attribute. You can also select preferences for each attribute. For example, you can set an attribute to be displayed during real-time enrichment. Note that the preferences aren't available for child fields.

   Note: Click Reset to revert back to the default mapping and preferences.
8. Click **Save and Close**

If you have a preproduction or staging environment, then test the service association between your sales preproduction environment and your Oracle Account and Contact Enrichment by Dun & Bradstreet (D&B) subscription. You must limit testing to 500 records. When you go to production, do the service association between your production environments and your Oracle Account and Contact Enrichment by Dun & Bradstreet (D&B) production environment. The service association steps are the same, but the test and production service URLs are different. The service URLs are listed in your welcome email and in the Unified Console application.

10 Configure Data Verification and Validation

Overview of Data Verification and Validation Setup

Data verification includes verification of addresses, phones, and email addresses.

Address verification is the process to verify that the address data entered for an organization (account) or person (contact) is a confirmed postal address. This includes the first line of the address, which includes a premise or building number and street name.

You can use address verification to verify, correct, and complete your address data, based on postal requirements. Here's an example wherein if you enter some of your address details, such as Address Line 1, and country, and then click the Verify Address button on the Create Organization or Create Person UIs, then the application may suggest a full address that you can accept or reject. Similarly, verification of phone numbers and email addresses ensures that the phone number and the email addresses exist.

Note that for data verification you require a separate license for Oracle Address, Email, and Phone Verification. Oracle Address, Email, and Phone Verification, ensures that you have the correct postal addresses, that your emails don't bounce, and your calls go through.

The data verification functionality is available:

- Real-time, on the Create Organization (Create Account) or Create Person (Create Contact) UIs
- In batch mode in the Data Verification work area
- During the import of data

Address validation is a process that you can use to check whether the address data that you enter real-time on the UI or import is valid. The application validates the address elements against your master reference geography data, ensuring that the data entered or imported is consistent with your reference geography data.

Address validation kicks in on the UI when you try to save the address data entered by you on the Create Organization (Create Account) or Create Person (Create Contact) UIs. The application also attempts to complete the address data, provided you had selected the Enable List of Values option on the Manage Geography Validation page. For example, if you enter postal code and country, then address validation may return a value for the city and the state. Likewise, if you enter city and country, then address validation supplies a value for the state.

Note that you may already have set up real time address validation during geographies setup while setting up geography validation using reference geography data. In case you plan to use Oracle Address, Email, and Phone Verification to validate address, you require a separate license for Oracle Address, Email, and Phone Verification. You also need to modify your earlier address validation setup as described in this chapter.

Here's a table that lists the configurations that you must complete to enable data verification and validation using Oracle Address, Email, and Phone Verification.

Step	Description	Task Name	Where to Get More Details
Configure Oracle Address, Email, and Phone Verification	Subscribe to Oracle Address, Email, and Phone Verification. Set the value for the **DAAS_PRODUCTION_MODE** profile option to NO to	• Manage Integration with Oracle Verification Services	See the topic: Configure Oracle Address, Email, and Phone Verification

Step	Description	Task Name	Where to Get More Details
	configure Applications Cloud to Data Cloud Integration.	• Manage Administrator Profile Values	
Manage Address Cleansing Configurations	You can use either the predefined cleansing configuration shipped ready-to-use, or duplicate and edit that configuration to meet your cleansing requirements. You can duplicate an available configuration to modify it according to your geography, address, and cleansing requirements. **Note:** You must save a duplicated configuration before you can edit it.	Manage Address Cleansing Configurations	See the topic: Manage Address Cleansing Configurations.
Set Up Real Time Address Cleansing	Enable real time address verification for the countries in which you do business.	Manage Geographies, Address Cleansing Defined	See the topics: • Set Up Real Time Address Cleansing to Enable Verify Address Button • How You Enable Search Mode for Oracle Address, Email, and Phone Verification
Set Up Address Validation	Enable address validation for the countries in which you do business.	Manage Geographies, Validation Defined	Define Real Time Address Validation

How do I configure Oracle Address, Email, and Phone Verification service?

You can configure Oracle Address, Email, and Phone Verification by completing the following tasks:

1. Setup Your Account.
2. Create Users.
3. Configure the Manage Integration with Oracle Verification Service task in the application.
4. Configure Manage Administrator Profile Values task in the application.

Set Up Your Account

Complete these steps to setup your account for Oracle Address, Email, and Phone Verification:

1. Subscribe to Oracle Address, Email, and Phone Verification:
    a. Log on to the Oracle Cloud Application Console at https://cloud.oracle.com/sign-in. In case you don't yet have an Oracle Cloud account, you can sign up for Oracle Cloud.
    b. Purchase a subscription account for Oracle Address, Email, and Phone Verification.
2. Add subscription to your Oracle Cloud account.

    You'll receive an email titled “Action Required: Welcome to New Oracle Cloud Service Subscription(s).” Follow the instructions in the email:

    - If you have an Oracle Cloud account, then click the **Add to existing cloud account** button. We recommend using your existing Oracle Cloud account to manage all your Oracle services.

        i. Specify your cloud Tenant name and click **Continue**
        ii. Specify your username and password and click **Sign In**.

        The **Add Subscription** page is displayed.
        iii. Add the new subscription to your tenancy. This page indicates the subscription name, subscription ID, and subscription description (with product SKU).

        > **Note:** Adding a subscription to a tenancy can't be done.

    - If you're a new customer, then click the **Create new cloud account** button. The New Cloud Account Information sign up form is displayed.

        i. Specify your First name, Last name, and Email address. The email address is also the username for signing into the account. The person you specify here is the first administrator who can access the account and can create other users. This role also has full administrator permissions in your account.
        ii. Specify a password and confirm.
        iii. Specify a Tenancy Name. This is also called your cloud account name. When choosing a tenancy name, note the following:
            - The tenancy name or cloud account name is used to identify your account. The name is also used to create the URLs to access your cloud services. For example, if you call your tenancy "abccorp", an application URL might look like:

              https://abccorp-oracleservice.service.us.phoenix-1.ocs
            - The tenancy name must be unique, start with a lowercase letter and have no more than 25 lowercase letters or numbers. You can't use spaces or special characters.
        iv. Select a Home region where your services will be hosted.

        > **Note:** Your home region is the geographic location where your account and identity resources will be created. You can't change this after signing up. If you are not sure which region to select as your home region, contact your sales representative before you create your account.

        v. Read the terms of use and click Create Tenancy.

3. Create the Data Environment.

   You'll receive a another email titled “Get Started Now with Oracle Cloud”. Click the Sign In button in the email. The Create environment page is displayed.

   a. Specify the cloud account name, credentials that you provided while creating cloud account and click **Create**.
   b. On the Create environment page, specify the admin email and click **Create**.

      > **Note:** Ensure that you don’t select the Update option.

      A page containing the environment information is displayed.
   c. Click the environment name to view the environment details.
   d. Copy the Service console URL from the Environment information tab and other links you need from the Additional links tab.
4. Create the OAuth client credentials as follows:
   a. In the Oracle Cloud Console home page, login to your cloud account.
   b. Click **Navigator** > **Account Management** > **Users**.
   c. On the User Management page, click the link on the message that the page is part of the new identity and access management experience.
   d. Click **Integrated applications** and click **Add application**.
   e. On the Add application popup, select **Confidential Application** and then click **Launch app catalog**.
   f. Type the name on the Add Confidential Application and click **Next**.
   g. On the Client configuration section, select **Configure this application as a client now** and select Resource Owner, Client credentials, and Refresh token options.
   h. Click **Next**.
   i. On the Web tier policy page, click **Finish**. You are now directed back to your application's Cloud Console.
   j. Scroll up and click the **Activate** button.
   k. Click the **Activate application** on the Activate application popup.

> **Note:** For any integration or using Oracle Cloud service with Address, Email, and Phone Verification APIs, you require the client credentials. Use these steps:
>
> a. Scroll down to the General Information section and copy the Client ID.
> b. Click **Show secret** in the **Client secret** section.
> c. Click the **Copy** link in the Client secret popup and click **Close** to copy the password.

Create Users

As part of creating users, you need to create administrators and application users.

Here is how you can go about creating administrators:

1. Log in as the Account Administrator to My Account.
2. Assign a Service Administrator (to monitor the service) and an Identity Administrator (to manage users).

Here is how you can go about creating application users:

1. Log in as the Identity Administrator to the Oracle Cloud Applications Console.
2. On the Users page, click Add.

3. Enter the data center where Oracle Address, Email, and Phone Verification is located, your identity domain and your temporary password. This information is listed in your Welcome e-mail. If you can't find this e-mail, the account administrator can resend it from My Account.
4. Expand the Advanced Roles section, and add the Data Service Client AppID role for this user.
5. Click Add to create this user.

If the new users don't already have a password for this domain, they get an e-mail with a temporary password. They can reset the password in the Oracle Cloud console. (The user now has credentials, but still needs to know the service URLs to log on. The Service administrator or the Identity administrator can provide this from the Welcome e-mail.)

Configure Customer Data Management Cloud to Verification Services Integration

Complete these steps to configure Customer Data Management Cloud to Data Cloud Integration:

1. Sign in to Customer Data Management Cloud as a setup user.
2. Navigate to Setup and Maintenance.
3. Click the Tasks side panel to open it, and click **Search**.
4. Search for and go to the task: Manage Integration with Oracle Verification Services.
5. Enter the following information on the Manage Integration with Oracle Verification Services page:

   Select OAuth Authentication.

   For information about adding a confidential application and getting the Client ID and Secret, see Add a Confidential Application topic in the Administering Oracle Identity Cloud Service guide.

   > **Note:** On the Client page of the Add Confidential Application wizard, in the Authorization section, select Resource Owner, Client Credentials, Authorization Code, and Refresh Token as Allowed Grant Types. Leave Redirect URL blank.

   > **Note:** We strongly recommend that you use OAuth authentication method because Basic authentication isn't supported in later releases. If you use Basic Authentication, don't include the question mark special character (?) in the password. For URL, remove /data/ui from the end of the instance address listed in your Welcome email and in the Cloud Console.

   For URL, remove /data/ui from the end of the instance address listed in your Welcome email and in the Cloud Console.

   For example, https://mydataservice-myidentitydomain.data.us2.oraclecloud.com.
6. Click Save and Close.

Requesting the Welcome E-mail to be Resent

Setup steps for this service are sent through a welcome e-mail to the customer when the license is purchased. If the Oracle Address, Email, and Phone Verification URL is missing and the customer administrator has already activated the service, then the customer administrator can request resend of the Welcome e-mail by going to http://cloud.oracle.com > My Account (see the following figure).

The following figure highlights the Resend Welcome E-mail button on the My Accounts page. 

However, if the customer administrator didn't receive a welcome e-mail with links to activate the service, then the customer will have to log a service request to have Oracle Support resend the welcome e-mail so that the customer

administrator can activate the service. Instructions on how to log a service request and the Customer Support Identifier associated to the service request are described in the FAQ section of Getting Started with Oracle Cloud in the Help Center.

Manage Administrator Profile Values

Complete the following steps to manage administrator profile values:

1. Navigate to Setup and Maintenance.
2. Search for and go to the Manage Administrator Profile Values task.
3. Enter DAAS_PRODUCTION_MODE as the Profile Option Code on the Manage Administrator Profile Values page.
4. Click Search. The specified Profile Option appears as the search result.
5. Make sure that the**Profile Level** is Site and the **Profile Value** is set to No.

   > **Note:** Don't set the Profile Level Site value to Yes. The only supported value today is No.

6. Click Save and Close.

The integration between Oracle Address, Email, and Phone Verification and Oracle Customer Data Management Cloud is now complete.

You can find more information about Oracle Address, Email, and Phone Verification in the Using Oracle Address, Email, and Phone Verification guide.

Related Topics

How do I enable the verification of addresses, emails, and phone numbers?

This step is a prerequisite to verifying addresses, emails, and phone numbers. You can enable or disable address, phone, and email verification services in the Configure Verification Services page. The Address Verification service is enabled by default.

You can access Address, Email, and Phone Verification service only if you have already purchased Address Verification.

> **Note:** Currently, email and phone validations aren't supported in Customer Data Management UI.

1. You can configure the Verification Services in the Setup and Maintenance work area using the following:
   - Offering: Customer Data Manager
   - Functional Area: Data Quality Verification Services
2. Click the Quick Setup icon.

   The Configure Verification Services page appears.
3. Select the verification services you want to enable.
4. Specify if the validity status of email and phone must be displayed.

5. (Optional) If you selected Yes in the previous step, specify the number of days since the last valid verification status was run that the verification status must be displayed. For example, if you set this value to 60, then 60 days after the last valid verification was run the verification status is displayed.
6. Click Save and Close.

Manage Address Cleansing Configurations

Address cleansing configuration maps the Customer Data Management application address attributes to Oracle Address, Email, and Phone Verification attributes.

As part of managing an address cleansing configuration, you can:

- Use the predefined address cleansing configuration shipped ready-to-use with the application.
- Adapt the predefined address cleansing configuration to your address cleansing requirements by duplicating and editing it.

Copy a Predefined Address Cleansing Configuration

To copy or make a duplicate of a predefined address cleansing configuration, complete these steps:

1. Sign is as a setup user having the role Master Data Management Applications Administrator.
2. Open the Manage Address Cleansing Configurations task from the implementation project. Alternatively, in the Setup and Maintenance work area, go to the following:
    - Offering: Customer Data Management
    - Functional Area: Data Quality Foundation
    - Task: Manage Address Cleansing Configurations
3. Select the Address Cleansing configuration, and click Duplicate.
4. Enter a name, such as Vision Corp. Address Cleansing Configuration, in the Name field. In case you don't enter a unique name, the application defaults the auto-generated configuration code for example, C1_DQ_SEED_LOC_CLEANSE, as the name.
5. Click Save.

Adapt a Copy of the Predefined Address Cleansing Configuration

To edit a copy of the predefined address cleansing configuration to your cleansing requirements, you need to:

> **Note:** You can't edit a predefined address cleansing configuration. You can only make a copy of it and edit it by following this procedure.

1. Sign in as a setup user having the role Master Data Management Applications Administrator.
2. Open the Address Cleansing Configurations task from the implementation project. Alternatively, in the Setup and Maintenance work area, go to the following.
    - Offering: Customer Data Management
    - Functional Area: Data Quality Foundation
    - Task: Manage Address Cleansing Configurations

3. Select the copy of the predefined Address Cleansing configuration that you created earlier, in our example, Vision Corp. Address Cleansing Configuration, and click Edit. The Edit EDQ Cleansing configuration page appears.

   Note that the Usage option is set to Both, which indicates that configuration makes Address Cleansing available real-time in the UI when creating or editing Organizations (Accounts) or Persons (Contacts), as well as for batch matching.
4. Select the Active check box to activate your copy of the address cleansing configuration, Vision Corp. Address Cleansing Configuration.

   By default, the predefined configurations are set to active. If there are copies of the predefined configurations, then you can set any of them to active by selecting the Active check box.

   > **Note:** You can activate only one configuration at a time. You must rebuild the keys when you activate a configuration.
5. Click Yes in the warning dialog box to activate this configuration.
6. In the Cleansing Attributes Mapping section, to modify the existing mapping, change the mapping between Oracle Address, Email, and Phone Verification attribute and address attribute to your business requirements by selecting appropriate attributes from the Address Attribute drop down.

   For more information about mapping cleansing attributes, see the topic How You Map Address Cleansing Attributes.
7. In the Cleansing Configuration Parameters section, you can carry out the given tasks:

   a. In the Default Country drop-down list, select the relevant country name. In our case study it's United States.
   b. In the Output Casing drop-down list, select Upper Case to print the addresses in upper case.
   c. In the Minimum Verification Level drop-down list, select `5-Verified` to Delivery Point or PostBox Level.
   d. In the Minimum Verification Score drop-down list, select 80.
   e. If you're configuring real-time processing, select Search or Verify for Processing Mode. This option isn't available for batch processing.
   f. Select the Correct Partially Verified Addresses.
   g. Select the Correct Ambiguous Addresses.
   h. Select Return Verified Address in Native Script to display verified addresses in the language native to the country selected in sub step a.

   For more information, let's see the topic How You Define Address Cleansing Configuration Parameters.
8. Click Save.
9. Review Configuration Results.

   For more information, let's see the topic Reviewing Matching Configuration Results.
10. Click Save and Close.

How You Map Address Cleansing Attributes

An Address Cleansing configuration comes with the following two sets of attributes:

- Address Attribute: The application attribute used to describe the address submitted for address cleansing.
- DaaS Attribute: The Oracle Address, Email, and Phone Verification attribute that's mapped with the application address attribute for cleansing.

You can determine which Oracle Address, Email, and Phone Verification Attribute you want to map to an Address Attribute depending on your address cleansing requirements. A Oracle Address, Email, and Phone Verification attribute is used to describe a distinct item of information that relates to a record. For example a City attribute might describe the city details of a customer record. Once the mapping is established, the input address is verified, and cleansed.

How You Define Cleansing Configuration Parameters

Cleansing configuration parameters are system-level parameters that control aspects of the data quality cleansing services. An address cleansing configuration includes both real-time and batch cleansing configuration parameters.

These parameters control real-time and batch address cleansing, standardization, and validation operations for a subset or all of the address records in the database, or as part of a data import process. The following table describes theses parameters and provides the supported parameter values where applicable.

Parameter	Description	Parameter Value
Default Country	Used to specify the country to cleanse the address, if no identifiable country can be found in an input address.	• Possible Values: Names of different countries • Default Value: United States
Output Casing	Used to specify the letter case for an output address.	• Possible Values: Upper case, Lower case, Mixed case. • Default Value: Mixed
Minimum Verification Level	Used to specify the level of verification to which the input data matches the available reference data during the verification process. Ranges from Verified to Administrative Area Level to Verified to Delivery Point, or Postbox level.	• Possible Values: Between 1 and 5. • Default Value: 4. **Note:** The higher the value, the more precise is the address. For a description of what each level means, see the topic: Notes on Minimum Verification Levels.
Minimum Verification Score	Used to specify the similarity between the input address and closest reference data match as a percentage between 0 (no match) and 100 (perfect match).	• Possible Values: Between 0 and 100. • Default Value: 80
Correct Partially Verified Addresses	Determines if you want to correct the addresses that you entered.	• Possible Values: Yes/No • Default Value: No
Correct Ambiguous Addresses	Determines if you want to correct the address that you entered if it's unclear and resolve it to the correct address.	• Possible Values: Yes/No • Default Value: No
Processing Mode	Use Verify mode to see the verified addresses. The Address Verification usage counter increases when you use the Verify mode. Use Search mode to get a list of verified addresses from which you can select the correct address.	• Possible Values: Verify and Search • Default Value: Search

Notes on Minimum Verification Levels

The verification level sets the level at which the input data is verified against the available reference data during the verification process. The 'post processed verification level achieved after standardization and parsing of the input address, is used as the second character of the Accuracy Code returned by the Address Verification processor.

Here's a table that lists the possible verification levels. The maximum verification level that it's possible to reach varies by country. For information on the maximum level in each country, see the Oracle Portal website at: http://www.loqate.com/oracle

Verification Level	Description
1	Verified to Administrative Area (State, Region or County) level
2	Verified to Locality (City or Town) level
3	Verified to Thoroughfare (Street) level
4	Verified to Premise (Building Number) level
5	Verified to Delivery Point (Sub-Building Number) level

Review Configuration Results

The Review Configuration Results option lets you check if the address attributes entered for cleansing in the Edit EDQ Cleansing Configuration page return the expected cleansed address. Here's a list of the cleaning configuration parameters that you can use to test the results:

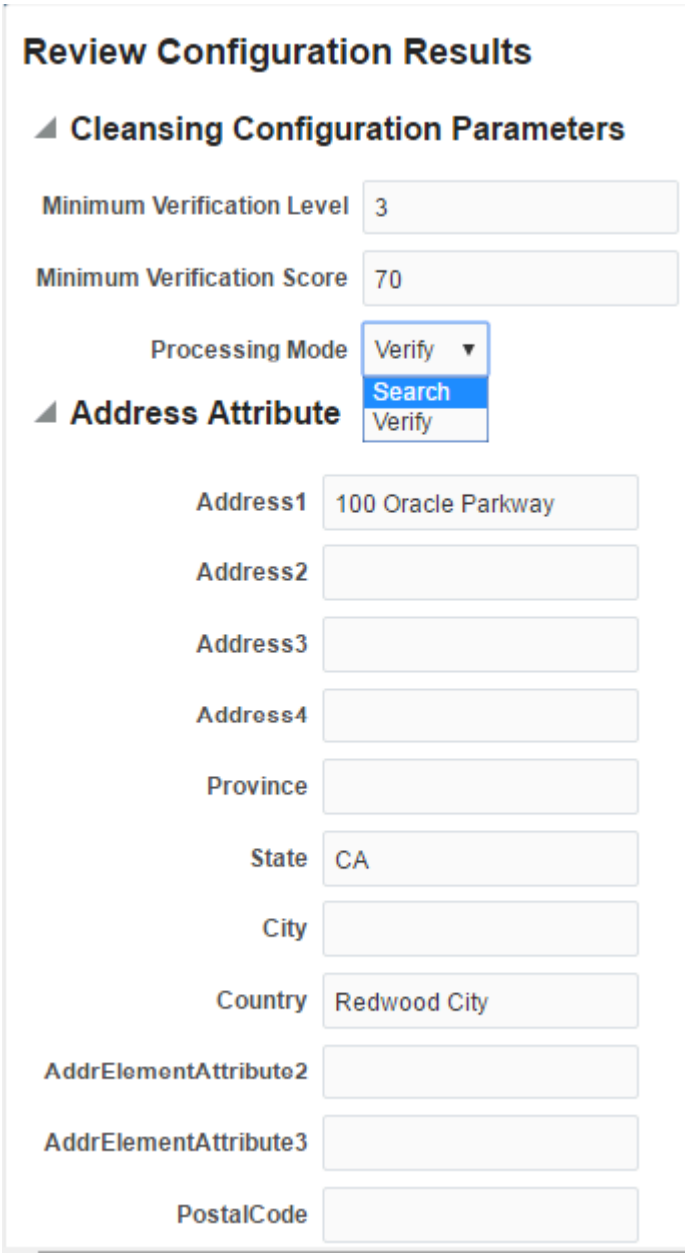
- Minimum Verification Level: Returns records based on the selected minimum verification level.
- Minimum Verification Score: Returns records based on the selected minimum verification score.
- Processing Mode: Use Search mode to search for valid addresses from Oracle Address, Email, and Phone Verification. If you use Verify mode, the Address Verification usage counter increases. In this mode, for every verified address the customer is charged.

You can review configuration results by completing the following steps:

1. Sign in as a setup user having the role Master Data Management Applications Administrator.
2. Open the Manage Address Cleansing Configurations task from the implementation project. Alternatively, in the Setup and Maintenance work area, go to the following.
    - Offering: Customer Data Management
    - Functional Area: Data Quality Foundation
    - Task: Manage Address Cleansing Configurations
3. Click the Review Configuration Results button on the Edit EDQ Cleansing Configuration page.
   Clicking the Review Configurations Result button verifies your connection with the Oracle Address, Email, and Phone Verification server. Select the process mode as **Search** to see multiple valid address results and **Verify** to see the verified address.

4. Enter values for the Cleansing Configuration parameters as required.
5. Enter some sample address data into Review Configuration Results page:
    a. Address 1: 100 Oracle Parkway
    b. State: CA
    c. Country: Redwood City
6. Click Find to verify whether the cleansed address record meets your expectations.

    The following figure shows the Review Configurations Results page.



For more information about address cleansing configuration template, see Implementing Customer Data Management, Address Cleansing Setup, Address Cleansing Configurations.

Set Up Real Time Address Cleansing to Enable Verify Address Button

You can setup real time address cleansing to enable the Verify Address button on the Organization (Account), Person (Contact), and Group (Household) UIs.

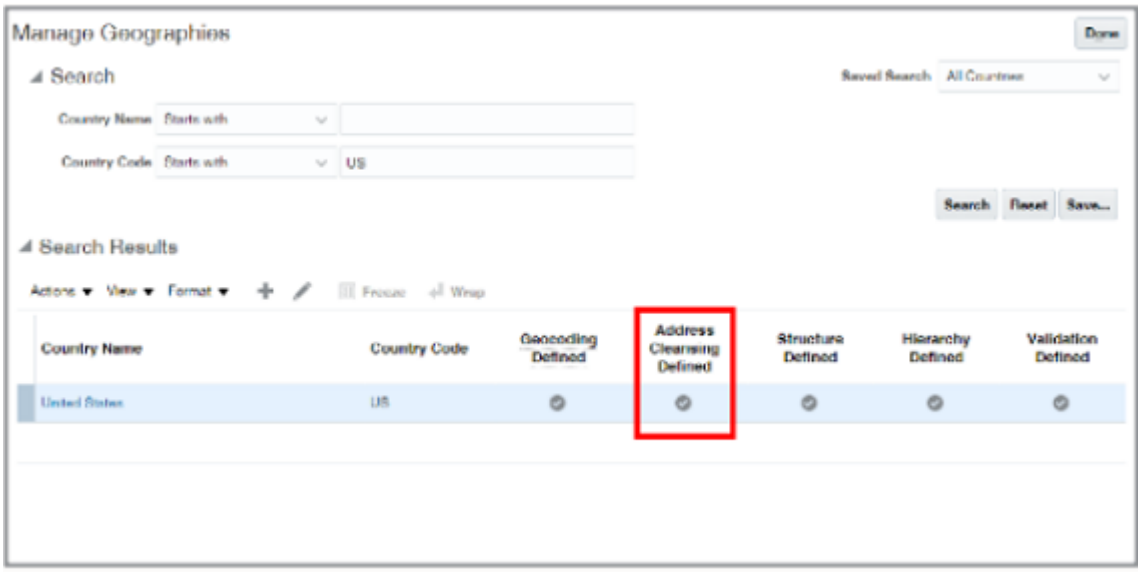
You can use the Verify Address button to validate, correct, and standardizes address information that you enter in the application down to the street level. Address cleansing, unlike geography validation, validates both the geography attributes and the address line attributes.

> **Note:** You need a separate license for Oracle Address, Email, and Phone Verification, to use the address cleansing functionality. You may have already set up real time address cleansing as a part of your geographies setup. If so, you don't have to set it up again.

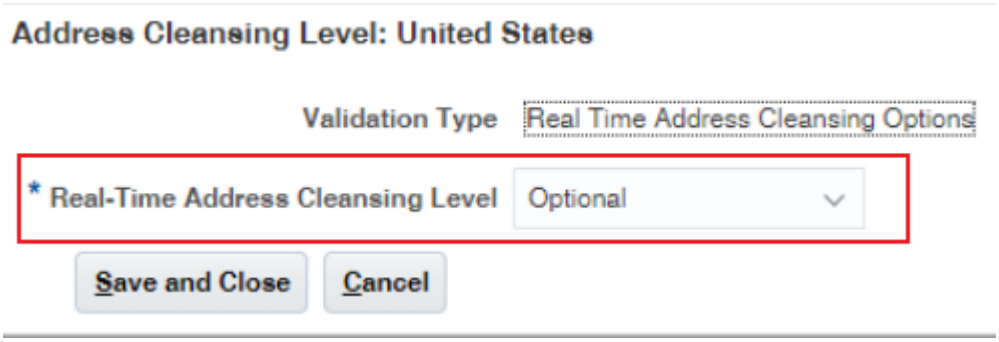
Here are the steps to define address cleansing for the countries in which you do business.

1. Open the Manage Geographies task from the implementation project or from Setup and Maintenance work area using the following:
    - Offering: Customer Data Management
    - Functional Area: Enterprise Profile
    - Task: Manage Geographies
2. Search for a country that you want to enable Address Cleansing using either by name or by its two letter ISO code. For example, you can search by entering either the country name United States or the two letter ISO code US, and clicking Search.
3. Select the country in the Search Results area.
4. Click the Go to Task button in the Address Cleansing Defined column to enable the Verify Address button on the Create Organization (Create Account), Create Person (Create Contact, and Create Group (Create Household)

UIs. Here's a screenshot of the Manage Geographies page highlighting the Go to Task icon and the Address Cleansing column.



5. In Address Cleansing Level dialog box, set the Real-Time Address Cleansing Level to Optional to enable the option to cleanse addresses. If the level is set to None, it specifies no real-time address cleansing. Here's a screenshot of the Address Cleansing Level dialog box highlighting the Real-Time Address cleansing Level field.



6. Click Save and Close.

Related Topics

- What are the best practices for managing Geography mismatches?

Define Real Time Address Validation

You must set up real time address validation for address elements, such as states and cities, for the countries in which you do business.

You need to do this to prevent address data entry errors and also to help users fill in missing address information, and validate addresses during entry.

Note that you may already have set up real time address validation during geographies setup while setting up geography validation using reference geography data. In case you plan to use Oracle Address, Email, and Phone

Verification to do address validation, you require a separate license for Oracle Address, Email, and Phone Verification. You also need to modify your earlier address validation setup as described in this topic.

Use the following steps to define real time address validation for the countries in which you do business.

1. Open the Manage Geographies task from the implementation project or from the Setup and Maintenance work area using the following:
    - Offering: Customer Data Management
    - Functional Area: Enterprise Profile
    - Task: Manage Geographies
2. Search for a country for which you want to enable Address Validation using either its name or its two letter ISO code. For example, you can search by entering either the country name United States or the two letter ISO code US, and clicking Search.
3. Select the country in the Search Results area.
4. Click the Go to Task button in the Validation Defined column to enable address validation for the country.

5. On the Manage Geography Validation page, in the Address Style region, ensure that the No Styles Format address style is selected. You define validation for the No Styles Format address style so that the validations are performed for all addresses in the country.

> **Note:** The setup of address styles for your application is done elsewhere, using the Manage Address Formats task. The format of addresses for Accounts and Contacts on the Create and Edit UI pages may not map perfectly to master geography structure.

6. Deselect Enable List of Values option in the Geography Mapping and Validation region to avoid Oracle Address, Email, and Phone Verification data conflicts with master reference geography data. By deselecting this option you can avoid any UI level validation against master reference geography data while adding address.

> **Note:** The Enable List of Values option is used to display the geography type as list of values during address entry in the classic and simplified UIs. For example, to have users select states from a list, select Enable List of Values for State. If the Enable List of Values check boxes are selected then, in case of data conflicts, Geography Naming References records won't be created.

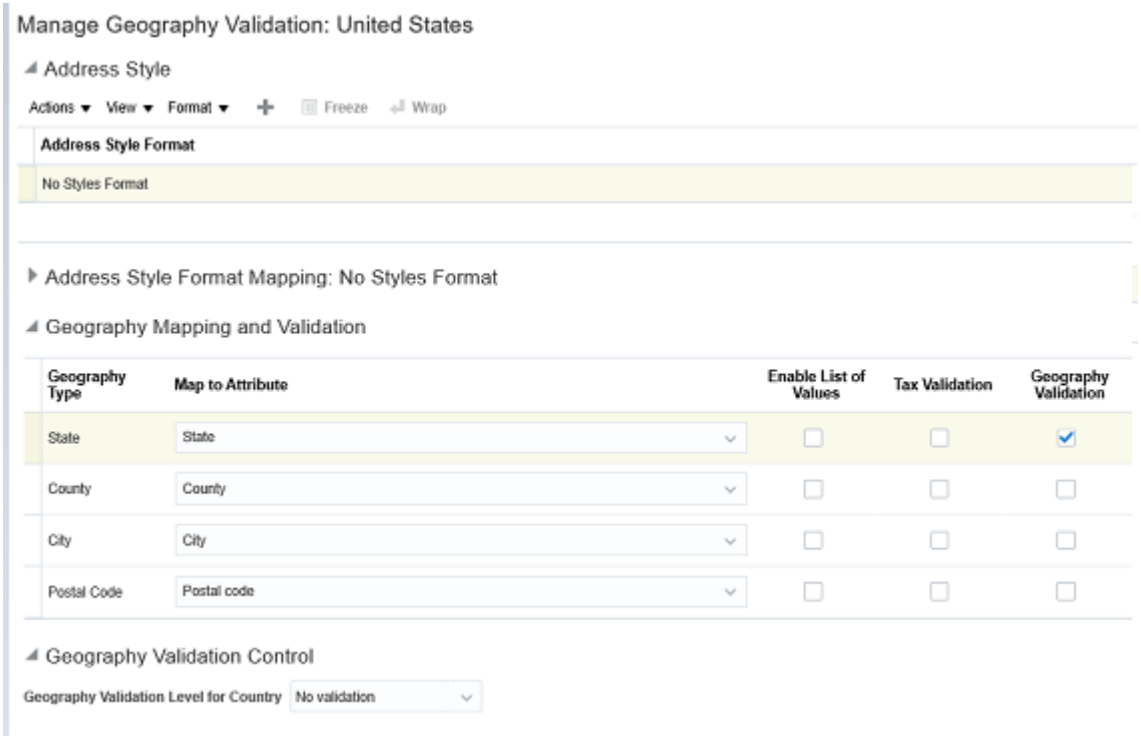
If Oracle Address, Email, and Phone Verification is used, the check boxes for Enable List of Values should be deselected to avoid data conflicts with master geography data. Tax Validation and Geography Validation are used for tax validation and territory management, respectively.

7. Select Geography Validation for all the geography types that you plan to use in territories. Our example organization, Vision Corp., plans to use set up geographies by state, so it selects Geography Validation for State. You must enable geography validation for all geography levels above the level you're planning to use for territories. For example, if an organization decided to set up territories at the Postal Code level, it must select Geography Validation for state, city, county, and Postal Code.

   > **Tip:** If you don't select the validation for an address element, the application still suggests values to the user during address entry, but it doesn't validate the address element.

8. Select Geography Validation Level for Country as **No validation** to verify address data by Oracle Address, Email, and Phone Verification.

   > **Tip:** If you want to verify address data against the master geography reference data, then set Select Geography Validation Level for Country to Error, it means that you want to verify. Here's a figure of the Manage Geography Validation page highlighting the Geography Validation options for the US State geography type.



9. Click Save and Close.

For more information about setting up Master Reference Geographies and Address Cleansing, see the MOS document Best Practices for Setting up Master Reference Geographies, in the Related Links section of this topic.

Turning on Validation for Address Import

By default, the validation you specified on the Manage Geography Validation page is enforced for creating addresses in the UI. You must set the profile option Geography Address Validation Enabled to Yes for the validation to be enforced during import. Here are steps to set the profile option:

1. Navigate to the Setup and Maintenance work area.

2. Search for and go to the Manage Administrator Profile Values task.
   The Manage Administrator Profile Values page appears.
3. In the Profile Display Name field located in the Search: Profile Option region, enter Geography Address Validation Enabled.
4. Click Search.
5. With the profile option selected in the search results, select Yes from the Profile Value list.
6. Click Save and Close.

Related Topics

- What are the best practices for managing Geography mismatches?

How You Enable Search Mode for Oracle Address, Email, and Phone Verification

Oracle Address, Email, and Phone Verification comes with two processing modes for address verification, Verify and Search. You can use this functionality to verify an address in real-time while entering information on the create or edit pages of Accounts or Contacts.

Out of the box, the Verify mode is enabled. When the Verify mode is enabled and you verify addresses in real-time on the create or edit pages of Accounts or Contacts, the service returns a single verified address that matches the address information you entered on the page.

The search mode is available in address cleansing configuration as a processing mode. When the Search mode is enabled and you do real-time address verification on the Create or Edit Accounts or Contacts page, the service returns a list of the suggested verified addresses that match the address information you entered. You can then select the appropriate address from the list.

Configure Address Verification Processing Mode

You can configure the address verification process mode by performing the following tasks:

1. In the Setup and Maintenance work area, go to the following:
   - Offering: Customer Data Management
   - Functional Area: Data Quality Foundation
   - Task: Manage Address Cleansing Configurations
2. On the Manage Address Cleansing Configurations page, click **Address Cleansing**.
   The Edit Address Cleansing Configuration: Address Cleansing page appears.
3. Select Search from the **Processing Mode** list in the **Cleansing Configuration Parameters** section.

   > **Note:** You can select either Verify or Search mode form the Processing Mode list according to your requirements. Select Verify mode if you want only one verified address to be returned while verifying an address on the Create Accounts or Create Contacts page. Select Search mode to get a list of the suggested verified addresses that match the address you entered so that you can select the appropriate address from the list.

4. Click **Save and Close**.

Verify Search Mode on Account or Contact Creation Page

You can verify the functionality of the Search mode while creating a new account or contact. Perform the following steps to verify an address in the search mode while creating a new account:

1. Navigate to Accounts work area.
2. Click **Create Account**.
3. Enter Address Line 1, City, and State of the account that you want to create on the Create Accounts page.
4. Click **Verify Address**.

> **Note:** If you click Verify Address after populating all the fields in the Address section of the Create Address page, you will get only one verified address with the complete match.

5. Select the correct address by clicking **Select** for the appropriate address from the list of suggested verified addresses.
6. Click **OK**.

   When you click OK the selected address gets populated in the Address section of the Create Account page.
7. Enter account details on the Create Account page.
8. Click **Save and Close**.

11 Configure Duplicate Identification

Overview of Duplicate Identification Setup

Duplicate identification is a process that identifies potential duplicate records for organization (account) and person (contact) records. You can use this process to identify duplicates in the following situations:

- Identify potential duplicate account and contact records in real-time when your salespeople create a customer record. This prevents the entry of duplicate records.
- Identify potential duplicates in batch mode for records already in the database or within the batch file itself.
- Identify duplicates during import of customer data for records already in the database or within the import batch file itself.

Duplicate identification uses the Enterprise Data Quality (EDQ) service. You require a separate license for the Oracle Fusion Data Quality Cloud Service.

You can enable Duplicate Identification by configuring the following tasks in the Setup and Maintenance work area:

Step	Description	Task Name	Where to Get More Details
Enable the Server Configuration for Matching	Enable the check box for EDQ Real-time and Batch Match Server configuration. Ensure that the Server Parameter Values (Server Address and Server Port) are complete.	Manage Server Configurations	See the topic: Enable the Server Configuration for Matching
Manage Enterprise Data Quality Matching Configurations	You can use either the predefined matching configuration shipped ready-to-use, or copy and edit these configurations to meet your matching requirements.	Manage Enterprise Data Quality Matching Configurations	See the topics: • Manage Enterprise Data Quality Matching Configurations • Key Generation • Considerations for Selecting Sources of Match Rules and Scoring • Manage Custom Match Rules and Scoring • Create Custom Match Rules

Enable the Server Configuration for Matching

The first step to configure duplicate identification is to enable the Enterprise Data Quality (EDQ) server configuration for matching.

Here's how you can enable the EDQ server configuration for matching:

1. Open Manage Server Configurations task from the implementation project. Alternatively, in the Setup and Maintenance work area , go to the following:
    - Offering: Customer Data Management
    - Functional Area: Data Quality Foundation
    - Task: Manage Server Configurations
2. Select the EDQ Real-time and Batch Basic Match Server configuration to enable it.
3. Ensure that the Server Parameter Values (Server Address and Server Port) are complete.
4. Click Save and Close.

For more information about managing EDQ server configurations, see Enterprise Data Quality Server Configurations, Define Data Quality, Implementing Customer Data Management.

Related Topics

- Enterprise Data Quality Server Configurations

Manage Enterprise Data Quality Matching Configurations

To help you identify duplicate records, the application comes with three predefined ready-to-use matching configurations, one each for the records of type organization (account) and person (contact). These ready-to-use configurations are read-only.

As part of managing Enterprise Data Quality (EDQ) matching configurations, you have the following options:

- Use the predefined matching configurations shipped ready-to-use with the application.
- Adapt the predefined matching configurations to your matching requirements by duplicating and editing them.

Note: There can be only one active matching configuration per object.

Copy a Predefined Enterprise Data Quality Matching Configuration

You can copy or make a duplicate of a predefined Enterprise Data Quality matching configuration by completing the following steps.

Note: This example demonstrates the procedure for duplicating the matching configuration for the account object. You can use these steps to also create copies of the predefined matching configurations for the contact objects.

1. Sign in as a setup user having the role Master Data Management Applications Administrator.
2. Open the Manage Enterprise Data Quality Matching Configurations task from the implementation project. Alternatively, in the Setup and Maintenance work area, go to the following:
    - Offering: Customer Data Management

- Functional Area: Data Quality Foundation
- Task: Manage Enterprise Data Quality Matching Configurations

3. Select the Account Duplicate Identification match configuration, and click Duplicate.
4. Click Yes in response to the warning message.
5. Click Save to save the copy of the predefined configuration. When saved you can rename the configuration appropriately. You can enter a name, such as Vision Corp. Account Duplicate Identification Configuration, in the Name field. In case you don't enter a unique name, the application defaults the auto-generated configuration code, for example, C1_DQ_SEED_ACCT_DUP_IDENTIFICATION, as the name.
6. Repeat steps 2 to 4 to create copies of the predefined match configurations for the contact objects, such as Vision Corp. Contact Duplicate Identification Configuration.

Adapt a Copy of the Predefined Enterprise Data Quality Matching Configuration

You can edit a copy of the predefined Enterprise Data Quality matching configuration, for example a copy of the the matching configuration for the account object, by completing the following steps:

> **Note:** You can't edit a predefined Enterprise Data Quality configuration. You can only make a copy of it and edit it by following this procedure.

1. Sign in as a setup user having the role Master Data Management Applications Administrator.
2. Open the Manage Enterprise Data Quality Matching Configurations task from the implementation project. Alternatively, in the Setup and Maintenance work area, go to the following:
   - Offering: Customer Data Management
   - Functional Area: Data Quality Foundation
   - Task: Manage Enterprise Data Quality Matching Configurations
3. Select the copy of Account Duplicate Identification match configuration that you created earlier, in our example, Vision Corp. Account Duplicate Identification Configuration.
4. Click Edit.
5. Select the Active check box to activate the new configuration.

   > **Note:** By default, the predefined configurations are set to active. If there are one or more copies of the predefined configurations, then you can activate any of the copies by selecting the Active check box. You must build the keys before you can set a configuration to active. Only one configuration can be activated at a time. Make sure that the Usage option is set to Both, which indicates that the configuration is for both for real-time and batch matching.

6. Click Yes in response to the warning message to set this configuration as active.
7. In the Match Attributes section, you can edit the mapping between EDQ Match Identifier and application attributes as follows:
   a. Select a row and click the attribute drop-down list arrow of the selected row.
   b. Select the relevant attribute from the list.
   c. If the list doesn't display the attribute that you want to map, then click Search in the drop-down list to search for the attribute.
   d. Select the relevant option and click OK.

   For more information about mapping matching attributes, see Mapping Matching Attributes.
8. You can set the real-time and batch key generation options and matching configuration parameters as follows:

a. Select Typical in the Cluster Key Level drop-down list of the Key Generation Options section.
b. In the Score Threshold field, enter 85.
c. In the Match Results Display Threshold field, enter 20.

> **Note:** The Match Results Display Threshold option isn't available for Batch. For more information, see the section: Best Practices for Mapping Matching Attributes.

9. Click Save.
10. At this point, you can Click Review Configuration Results from the Actions menu to review the results of your matching configuration. Alternatively, at any point, you can click Preview Configuration from the Actions menu to test your matching configurations definition without rebuilding the keys. For more information, see the section: How You Preview and Review Configuration Results.
11. Click Save and Close.

How You Preview and Review Matching Configuration Results

At any point, during the definition of the matching configuration, you can click Preview Configuration from the Actions menu to test your matching configuration definition without rebuilding the keys. Once you're satisfied with the definition of the matching configuration, you can build the keys and set the configuration to active. You can then click Review Configuration Results from the Actions menu to review the results of your matching configuration:

The Review Configuration Results option lets you evaluate if the attributes and parameters entered for matching in the Edit EDQ Matching Configuration page return the expected results. You can also test the results of one or more of the following matching configuration parameters:

- Cluster Key Level
- Score Threshold
- Maximum Candidates
- Match Results Display Threshold

You can review the configuration results of the Contact Duplicate Identification matching configuration by completing the following steps:

1. Click the Review Configuration Results button on the Edit EDQ Matching Configuration page for the Vision Corp. Contact Duplicate Identification Configuration.
2. Enter values for the Matching Configuration parameters as required.
3. Enter some sample data into Review Configuration Results UI page, for example, as follows:

   Match Configuration Parameters
   - Cluster Key Level: Exhaustive
   - Score Threshold: 50
   - Maximum Candidate: 99
   - Match Results Display Threshold: 20

   Match Attributes
   - PersonFirstName: Lisa
   - PersonLastName: Jones
   - Address1: 300 Oracle Pkwy

4. Click Find to verify whether the records returned as potential duplicates meet your expectations.

For more information about managing EDQ server configurations, see Enterprise Data Quality Matching Configurations, Define Data Quality, Implementing Customer Data Management.

Related Topics

- Enterprise Data Quality Server Configurations
- Enterprise Data Quality Matching Configurations

Best Practices for Mapping Matching Attributes

Match attributes, such as name, country, and postal code are used for real-time and batch matching of the account and contact records. You map the attributes in Customer Data Management application with the corresponding Enterprise Data Quality (EDQ) attributes to create an attribute mapping.

For example, for account matching, map the EDQ Attribute, name, to the Account Attribute, OrganizationName. When you map the attributes in the CDM application with the corresponding EDQ attributes, you create a matching configuration setting for identifying duplicate entries. These settings are stored as matching keys in CDM.

You can use two types of EDQ Match Identifiers to include or exclude records from matching.

- Unique Identifier: Records that have the same Unique Identifiers always match, regardless of all other data.
- Elimination Identifier: Records that have different Elimination Identifiers never match.

Examples of attributes that could be used for Unique Identifier or Elimination Identifier are Social Security Number for contact or D-U-N-S number for account. You can use up to 3 Unique Identifier and 3 Elimination Identifier attributes in your matching configuration.

Note: Key considerations for managing key generations:

- When you change the attribute mappings you must regenerate matching key values for the new or updated accounts and contacts.
- A key generation failure is logged for records having a null or empty string value for a mapped attribute.
- Consider using a Unique Identifier for cases where an exact match on a single attribute value will always signify duplication. In other words, a single-value exact match rule would be configured with a match score of 100.

Matching configuration parameters are system-level parameters that control aspects of the data quality matching services. An Enterprise Data Quality (EDQ) matching configuration includes both real-time and batch matching configuration parameters.

The following table describes the real-time and batch configuration parameters and provides the supported parameter values where applicable.

Parameter	Description	Parameter Value
Cluster Key Level	Returns records based on the cluster key level.	• Possible Values: Limited (loose matching), Typical or Exhaustive (tight matching). • Default Value: Typical (recommended)
Score Threshold	Specifies the score above which the matched records are returned by the matching service. Records equal to or greater than the score are considered as matches and the records with scores less than the threshold are rejected.	• Possible Values: Between 0 and 100. • Default Value: 50
Match Results Display Threshold	Controls the number of matched records that are returned by the real-time matching. Note: This match configuration parameter is enabled only for real-time matching.	• Possible Values: Between 0 and 100. • Default Value: 20

Key Generation

The EDQ matching process for real-time and batch matching makes use of the EDQ Cluster Key Generation service and the EDQ matching service for duplicate identification. Successful key generation is critical to duplicate identification.

Key generation identifies similar parties and assigns a key to each. When a matching configuration is made active, the application passes a set of keys (subset of parties) to the EDQ matching service to process for duplicate identification.

The EDQ Cluster Key Generation service must be run whenever a record is added or updated in the application. This service generates keys for records added as well as for the records that are updated in the application. If keys aren't generated, duplicate identification fails.

How You Configure Key Generation

The duplicate identification process uses matching keys, which must be maintained through a key generation process. You need to set up a recurring, incremental key generation job for each active data quality matching configuration for batch duplicate identification. You also may want to configure real-time key generation for immediate matching of new data as soon as new data is entered.

How You Setup Recurring Incremental Key Generation (Required)

You can schedule incremental key generation for an active matching configuration using the schedule key generation option on the Edit Matching Configuration page. This generates keys for records that don't have a key or if the key time stamp is older than that of the records. You must incrementally generate matching key values for the new or updated accounts and contacts.

To assure your duplicate identification processes use up-to-date matching keys, check if the following setup tasks have been completed.

1. In the Setup and Maintenance work area, go to the following:
    - Offering: Customer Data Management
    - Functional Area: Data Quality Foundation
    - Task: Enterprise Data Quality Matching Configuration
2. Click the name of the required active match configuration.
3. Click Scheduled Key Generation.
4. Click Advanced.
5. Select Using a schedule option in the Advanced Options section.
6. Specify the frequency, the start date, and end date to run the scheduled process.

    You may want to select a distant end-date to reduce how often you must run this task and to help assure that the recurring schedule doesn't lapse.
7. Click Submit.

    The recurring incremental key generation scheduled process is submitted.

How You Specify Real-time Key Generation (Optional)

You may want to configure keys to be generated for immediate matching of new data as soon as new data is entered. For example, different users may be entering duplicate records at nearly the same time and you may want the keys to be generated immediately. Real-Time key generation process is available to handle such scenarios.

Follow these steps to enable real-time key generation:

1. Search and navigate to the Manage Administrator Profile Values task.
2. Search for the ORA_ZCQ_ENABLE_REALTIME_KEYGEN profile option.
3. Set the Site level profile option value to Yes.
4. Click Save and Close.

Best Practices for Real-Time Key generation

Here are guidelines to help you decide if real-time key generation is right for your business needs:

- Use Real-Time key generation only if an appropriately scheduled incremental key generation process doesn't support your business process needs.
- Certain processes, such as batch address cleansing, don't trigger real-time key generation events. Real-time key generation isn't sufficient to replace recurring incremental key generation, but it may be used as a complement for certain business scenarios.
- If possible, disable update events for higher-volume data creation and update processes, such as web service-based data integration flows.

To disable high-volume user accounts from generating update events:

1. Search and navigate to the Manage Administrator Profile Values task.
2. Search for the ZCA_PUBLIC_BUSINESS_EVENTS profile option.
3. Click **Actions** > **New** in the Profile Values section.
4. Specify the following values:

- Set the Profile Level to User.
- Select the User Name for which you want to suppress business events.
- Set the Profile Value to No.

5. Click Save and Close.

How You Rebuild Keys

You must rebuild keys before activating a new configuration. You must rebuild keys if you change match configuration mappings or if you think that the keys are no longer valid because of updates to the records. You can regenerate matching key values using the Rebuild Keys option in the Edit Matching Configuration page.

How You Specify Real-time and Batch Key Generation Options

You can specify different key generation options for batch matching and real-time matching. Take for example the cluster key level parameter that has the values, limited, typical, or exhaustive. It's possible to select one value of this parameter, say limited, for batch matching and another, say exhaustive, for real-time matching, depending on how tightly you want the data quality engine to match records.

How You Review Key Generations Status

You can search for key generation jobs and review the status of each key generation job on the Manage Key Generation page. The following table describes the various possible key generation statuses for a matching configuration.

Key Generation Status	Description
Pending	Key generation for the configuration is required.
Processing	Key generation for the configuration is in progress.
Review Required	Key generation for this configuration needs review.
Ready	Key generation for this configuration is complete.

Considerations for Selecting Sources of Match Rules and Scoring

The Customer Data Quality application comes with two options for match rules and scoring, predefined match rules (EDQ match rules) and custom match rules (Customer Data Management match rules).

You can use a drop-down button on the Enterprise Data Quality Matching Configuration page to select the match rules and scoring option best suited for your business requirements.

The predefined EDQ match rules include a single, view-only matching rule for each object such as account and contact. These match rules can't be edited, scores can't be changed, and no new rules can be added.

In case the predefined match rules aren't suitable for your business requirements, you should enable custom match rules and scoring. You should be able to turn on custom scoring by selecting Custom from the Scoring Type drop-down list on the Manage Enterprise Data Quality Matching Configurations UI page. You can use this functionality to create your own match rules and scores.

Manage Custom Match Rules and Scoring

This topic describes how to enable the custom match rules and scoring functionality.

Use the following procedure to enable custom match rules for account and contact. Note that custom match rules are available only for account and contact.

1. In the Setup and Maintenance work area, go to the following:
    - Offering: Customer Data Management
    - Functional Area: Data Quality Foundation
    - Task: Manage Enterprise Data Quality Matching Configurations
2. On the Manage Enterprise Data Quality Matching Configurations page, drill down on the predefined or the user-defined matching configuration, for which you want to enable or disable custom match rules and scoring.
3. Scroll down to the **Scoring Type** drop-down list and select Custom from the Real-Time or Batch tabs on the Edit Match Configuration page.
4. Click **Save** or **Save and Close**

How do I create custom match rules?

You can use the custom match rule and scoring functionality to create your own match rules and scores based on your business requirements.

Use the following procedure to create custom match rules.

1. In the Setup and Maintenance work area, go to the following:
    - Offering: Customer Data Management
    - Functional Area: Data Quality Foundation
    - Task: Manage Enterprise Data Quality Matching Configurations
2. On the Manage Enterprise Data Quality Matching Configurations page, drill down on the predefined or the user-defined matching configuration for which you want to create or update predefined rules.
3. Click **Manage Match Rules** on the Edit Match configuration page.
4. On the Manage Match Rules page click New. Alternatively, you can click Duplicate to create a new rule based on an existing predefined or user-defined match rule.
5. Enter the following values for the newly created or copied match rule:

- **Rule Name:** The name of the new rule. There's no restriction for the rule name.
- **Match Rule Score:** The score that you assign to the rule. The value must be between 1 and 100.
- **Rule Attribute:** The standard or predefined attributes that must be used in the custom match rules. Specify an attribute name followed by either Exact or Fuzzy to find exact matches or closer to the attribute value matches. You can specify any number of rules separated by commas but you must ensure that the rule is logical. Ensure that the syntax and spelling are exact. The following are examples:
  - `name:Exact,address:Exact,taxnumber:Exact`
  - `name:Exact,address:Fuzzy,taxnumber:Exact`

> **Note:** Address:Exact match returns a match when all three of the following match:
> - Address lines 1, 2, 3 and 4, postal code
> - Country
> - State or City
>
> City need not match exactly but the address is considered an exact match if the address lines fields, state, and country match.

6. Click **Save** or **Save and Close**.

12 Configure Duplicate Resolution

Overview of Duplicate Resolution Setup

Duplicate resolution is a set of processes that you can use, after duplicate records are identified, to consolidate those records. You can resolve duplicates in two ways, either by linking them or by merging them. Linking involves associating the duplicate records.

The linked records are treated as unique records in the data registry, and have their own unique identifiers. Merging involves combining duplicate records into one new master record.

The duplicate resolution functionality comes with tools and rules that you can use to determine whether to merge records or not. These rules can also help determine the record that should be kept as the golden master (the surviving record) and the record that should be deleted (the non-master record).

You can setup linking by configuring a couple of profile options discussed in the topic Duplicate Resolution Simplified Profile Options. However, the setup for merging is a bit more elaborate. It consists of configuring logic to:

1. Determine which record from a set of identified duplicates should be designated as the master record. You can set this up by configuring Set Master Record Rules.
2. Determine which attribute value instances from across the set of duplicates the master record should have. You can set this up by configuring Set Attribute Value Rules. The Set Master Record Rules and Set Attribute Value Rules are collectively called Survivorship Rules.
3. Determine whether the merge is violating any of the conditions under which a merge should be prohibited. You can set this up by configuring Agreement Rules.

You can easily setup survivorship and agreement rules in Application Composer using Groovy Script.

An alternative to using Groovy Scripts based survivorship and agreement rules is to configure them using Oracle Business Rules. You can do this configuration in the Setup and Maintenance work area using the Manage Survivorship Rules and Manage Agreement Rules setup tasks.

Note that if you're already using Oracle Business Rules, you can migrate from Oracle Business Rules to Groovy Script incrementally. For example, you could continue to use Oracle Business Rules to define agreement rules while using Groovy Script for your set master rules.

You can setup duplicate resolution by configuring the tasks listed in the following table.

Step	Description	Task Name	Where to Get More Details
Setup Source Systems	Set up source systems to import data into the application and identify the source of the data that you're importing. You can select multiple source references in the Manage Source System Entities task to allow multiple source system records to map to a single record. You must setup source systems before importing your organization (account) and person (contact) data	• Manage Trading Community Source Systems • Manage Source System Entities	See the topic: Setup Source Systems

Step	Description	Task Name	Where to Get More Details
Manage Source System Confidence	Source system confidence levels or scores are used as criteria in survivorship rules for: • Comparing the reliability of information from different source systems • Preserving the data from the most reliable source in the master record during merge operations You can set the source confidence score per source system for attributes in the organization (account) and person (contact) objects.	Manage Source System Confidence	See the topic: Manage Source System Confidence
Enable Groovy Script-based Survivorship and Agreement Rules	You must enable groovy scripting, before you can start using groovy scripts to configure survivorship and agreement rules. You can do so in the in Setup and Maintenance work area by setting the appropriate profile options.	Manage Customer Data Management Options	See the topic: How You Enable Groovy Script-based Survivorship and Agreement Rules
Create an Application Composer Sandbox	Create a separate, dedicated sandbox for survivorship and agreement rules. This approach gives you the greatest flexibility for iterative design, testing, and deployment of your survivorship and agreement rules.	N/A	See the topic: Create an Application Composer Sandbox
Configure Predefined Data Quality Rules to Your Requirements	Customer data management comes with six predefined data quality merge event points, three for the Account (Organization) entity and three for the Contact (Person) entity. You must configure these predefined rules to your unique business requirements.	N/A	See the topics: • Configure Predefined Data Quality Rules to Your Requirements in Application Composer • Configure Groovy Script Based Set Master Record Rules • Configure Groovy Script Based Set Attribute Value Rules • Configure Groovy Script Based Agreement Rules
Test Your Survivorship and Agreement Rules Configuration	Create a Test Merge Request in the Duplicate Resolution work area to test your groovy script-based survivorship and agreement rules configuration in real time.	N/A	See the topic: Test the Survivorship and Agreement Rules Configuration

Step	Description	Task Name	Where to Get More Details
Deploy Your Survivorship and Agreement Rules Configuration	You must publish your dedicated Application Composer sandbox for survivorship and agreement rules to deploy the configuration.	N/A	See the topic: Deploy the Survivorship and Agreement Rules Configuration
(Applicable only if you're using Oracle Business Rules) Manage Oracle Business Rules Based Survivorship Rules	Survivorship rules determine the master or surviving customer record and its attributes during the merge operations for duplicate resolution. You can enable survivorship rules by setting the ZCH_ENABLE_SURVIVORSHIP profile option to Yes	• Manage Survivorship Rules • Manage Customer Hub Profile Options	See the topics: • How You Enable and Manage Survivorship Rules • Define Survivorship Rules • Define Set Master Record Rules • Define Set Attribute Value Rules
(Applicable only if you're using Oracle Business Rules) Manage Oracle Business Rules Based Agreement Rules	Agreement rules determine whether a merge request should be vetoed by the application or not. Merge requests that violate agreement rules don't complete successfully	Manage Agreement Rules	See the topics: • How You Manage Agreement Rules • Define Agreement Rules
Run Request Dispatch Job	Run this process to manage and monitor resolution requests in pending or submitted statuses	Run Request Dispatch Job	See the topic: Run the Request Dispatch Job

Note: In case of Accounts, Customer Profile Quality Scoring is an additional method to resolve duplicates. This method helps in assigning scores to records and identifying a record with the highest score. This record with the highest score can be used as the single account record, instead of multiple duplicate records. For more information about Customer Profile Quality Scoring, see the Implementing Customer Data Management guide.

Set Up Source Systems

You set up source systems to import data into the application from other systems and identify the source of the data that you're importing.

Note: You must setup source systems before importing your organization (account) and person (contact) data. The next step is to setup source system confidence to determine the relative reliability of a particular organization (account) or person (contact) attribute (standard or custom) from a particular source system. This allows the preservation of data from the most reliable source in the master record during the merge operation. See the topic: *Manage Source System Confidence*.

You can specify whether the source system is a spoke system, such as a legacy system, or a purchased system, such as data from a third party provider. You can also specify what types of entities can be imported from a source system. For

example, you can enable a source system for importing trading community members such as organizations (accounts) and persons (contacts).

> **Note:** You can select multiple source references in the Manage Source System Entities task to allow multiple source system records to map to a single record.

For example, consider Vision Corp., a software company which acquires a couple of software companies, First Software and Softgear, and their customers. So we will have to setup the following three source systems:

- Vision Corp.
- Softgear
- First Software

Here is how you can go about setting up these source systems:

1. In the Setup and Maintenance work area, navigate to the following:
    - Offering: Customer Data Management
    - Functional Area: Trading Community Foundation
    - Task: Manage Trading Community Source Systems
2. From the Actions menu, click Create. The Create Source System UI page appears.
3. Enter the following information:
    - Code: VC
    - Name: Vision Corp.
    - Type: Spoke
4. Enable the source system for Trading Community Members. You can enable it for other entity types also depending on your business requirements.
5. Click Save and Create Another.
6. Enter the following information:
    - Code: SG
    - Name: Softgear
    - Type: Spoke
7. Enable the source system for Trading Community Members. You can enable it for other entity types also depending on your business requirements.
8. Click Save and Create Another.
9. Enter the following information:
    - Code: FS
    - Name: First Software
    - Type: Spoke
10. Enable the source system for Trading Community Members. You can enable it for other entity types also depending on your business requirements.
11. Click Save and Close.

Manage Source System Confidence

Source system confidence is used to determine the relative reliability of a particular organization (account) or person (contact) attribute (standard or custom) from a particular source system.

This allows the preservation of data from the most reliable source in the master record during the merge operation. Each attribute is given its own source system confidence score. Source system confidence levels range from 0 to 100, and are set by default to 0. When all source system confidence levels are set to 0, all conflicts are listed for the Master Data Management Applications Administrator. The Master Data Management Applications Administrator reviews the list and decides the source system attributes that must be included into the master record.

Here's how you can define source system confidence:

1. Open the Manage Source System Confidence task from the implementation project. Alternatively, in the Setup and Maintenance work area go to the following:
    - Offering: Customer Data Management
    - Functional Area: Customer Hub
    - Task: Manage Source System Confidence
2. From the Actions menu, click New. The Define Source System Confidence UI page appears.
3. Click Object Type drop-down list and select an object type.
4. Select and move the attributes for which you want to set the source system confidence scores from the Available Attributes list to the Selected Attributes list.
5. Select a source system code from the Source System Code drop-down list for each attribute. In our implementation case study, we set up three source systems:
    - Vision Corp. (code: VC)
    - First Software (code: FS)
    - Softgear (code: SG)
6. Enter a value in the Source Confidence field. The value of the source system confidence can range from 0 to 100.
7. Click New to define the source confidence score for the selected attributes for different systems.
8. Click Save and Close after defining source system confidence score. All attributes, their source system, and confidence scores are visible in the Manage Source System Confidence UI page.

Configure Duplicate Resolution Using Groovy Scripts

How you Configure Merges Using Groovy Scripts

A merge request consists of configuring logic to:

- Determine which record from a set of identified duplicates should be designated as the master record. You can set this up by configuring Set Master Record Rules.

- Determine which attribute value instances from across the set of duplicates the master record should contain. You can set this up by configuring Set Attribute Value Rules. The Set Master Record Rules and Set Attribute Value Rules are collectively called Survivorship Rules.
- Determine whether the merge is violating any of the conditions under which a merge should be prohibited. You can set this up by configuring Agreement Rules.

The linked records are treated as unique records in the data registry, and have their own unique identifiers. Merging involves combining duplicate records into one new master record.

You can setup duplicate resolution using Groovy scripts by configuring a couple of profile options discussed in the topic Duplicate Resolution Simplified Profile Options and specify the scripts in the Application Composer.

You can easily setup survivorship and agreement rules using Groovy Script in Application Composer. If you already have defined survivorship and agreement rules without using the Groovy Scripts, you can migrate them to Groovy Script incrementally. For example, you could continue to use your existing agreement rules while also using Groovy Script for your set master rules.

How You Enable Groovy Script-based Survivorship and Agreement Rules

Before you can start using groovy scripts to configure survivorship and agreement rules, you must enable groovy scripting in Setup and Maintenance.

Follow these steps to enable Groovy Script-based survivorship and agreement rules:

1. In the Setup and Maintenance work area, go to the following:
    - Offering: Customer Data Management
    - Functional Area: Customer Hub
    - Task: Manage Customer Data Management Options
2. In the Merge Behavior section under the Duplicate Resolution Options tab, select the groovy script options as the value for one or more of the following fields as required:
    - Master Record Selection: Select the Select master record using groovy scripts option to define the rules for selecting master records using Groovy Scripts.
    - Attribute Selection Type: To define attribute selection rules using Groovy Scripts, select the following options:
        - Select either Use source confidence with newest record as the tie breaker or Use source confidence with oldest record as the tiebreaker.
        - Select Yes for the Add Groovy to Attribute Selection field.
    - Agreement Rules Type: Select the Default agreement rules with groovy scripts option to define agreement rules using Groovy Scripts.

Create an Application Composer Sandbox

The configuration of Groovy Script survivorship and agreement rules is done in Application Composer using the standard Unified Sandbox framework for developing and testing your scripts.

We recommend that you create a separate, dedicated sandbox for survivorship and agreement rules rather than combine survivorship and agreement rule configuration with other types of Application Composer configuration activities. This approach gives you the greatest flexibility for iterative design, testing, and deployment of your survivorship and agreement rules.

To create an Application Composer Sandbox:

1. Click **Navigator** > **Configuration** > **Application Composer** > **Sandboxes**
2. Click Create Sandbox.
3. Specify a name and select Application Composer All Tools. Also select the Publishable option as Yes.
4. Click Create and Enter.
5. Click the Application Composer icon.
6. Go to Common Setup and click Data Quality Rules.

   On the Data Quality Rules page, you should can see six predefined templates for survivorship rules of the type set master and set attributes and agreement rules. You should can see three rules for the Contact (Person) entity and three for the Account (Organization) entity.

You're now ready to configure the survivorship or agreement rules using Groovy Scrip for accounts or contacts. For more information about creating sandboxes, see the Related Topics section.

Related Topics

- Overview of Sandboxes

Configure Predefined Data Quality Rules to Your Requirements in Application Composer

You can configure predefined data quality rules to your requirements in the application composer.

Follow these steps:

1. In your Sandbox dedicated for Data Quality rules, click the Application Composer icon.
2. Go to Common Setup and click Data Quality Rules to view the predefined data quality rules. You should be able to see six predefined templates for data quality rules, three for the Contact (Person) entity and three for the Account (Organization) entity. These templates are:
   - ContactSetMaster: Configure rules for determining the master record in contact merges.
   - ContactSetAttribute: Configure attribute survivorship rules for contact merges.
   - ContactMergeAgreement: Configure merge agreement rules for contact records.
   - AccountSetMaster: Configure rules for determining the master record in account merges.
   - AccountSetAttribute: Configure attribute survivorship rules for account merges.
   - AccountMergeAgreement: Configure merge agreement rules for account records.
3. To configure the merge processing logic for any of these templates, you can:
   - Click the required template.
   - Select the desired row and click **Actions** > **Edit**.
4. Create and save your scripts in the Groovy Script editing interface that's displayed when you click edit for a given survivorship or agreement rule.

Configure Groovy Script Based Set Master Record Rules

In this example, you will learn how to create a set master record rule to select the master record in a resolution request, with different logic depending on whether the resolution request is merge request.

The logical requirements of the scenario are as follows:

- Records integrated with RNOW source system are the top priority to be master record.

- If multiple records are present from a prioritized source system, use the most recently updated record as the tiebreaker.
- If no RNOW-integrated records are present in the merge, take whatever record had been designated as master by the upstream process.

Steps to Perform

1. Enable Groovy Scripts to select master records:
   a. In the Setup and Maintenance work area, go to the following:
      - Offering: Customer Data Management
      - Functional Area: Customer Hub
      - Task: Manage Customer Data Management Options
   b. In the Merge Behavior section, select the Select master record using groovy scripts option for the Master Record Selection field.
2. Create an Application Composer sandbox. Refer to the Create an Application Composer Sandbox topic for the steps.
3. Populate the sample script in the AccountSetMaster template:
   - Navigate to **Common Setup** and click **Data Quality Rules**.
   - Click AccountSetMaster.
   - Copy and paste the code given in the Sample Code section in the Edit Data Quality Rules page.
   - Click Save and Close.
4. Test the code. Refer to the Test the Survivorship and Agreement Rules Configuration topic to test the code.
5. Deploy the Code, after you're satisfied with the results of the Set Master Record Rules. See the topic: Deploy the Survivorship and Agreement Rules Configuration.

What the Sample Script Does

The script begins by calling the getRows() input function to access the records in the resolution request. After initializing additional variables, the script calls getAttribute("ResolutionType") to determine what type of resolution request is being processed.

If the Resolution Type is MERGE, the script loops through the records in the resolution request to inspect which source system reference assignments exist for each record. When a record with an RNOW source system reference is found, the row is added to the list of records having the given source system reference assignment.

Once all the rows in the resolution request have been tested for their source system reference values, the script tests whether any records from the prioritized source system reference were found. If records are found in the top priority list, they're tested by last updated date. Then the most recently updated record having the highest priority source system reference is designated to become the master record.

Finally, the script calls the selectMaster() output function to designate the master record. If a top-priority or second-priority record was identified earlier in the script, that record is provided to the selectMaster() function. If no priority record was identified, then the default master record specified by the upstream process will be retained as the master record for the resolution request.

Sample Code

```
try {
 def requestRows = getRows();
 def rowMaster = false;
 def osrMap = ['RNOW': []];
 def rowDefaultMaster = getMaster();
 def iHighestAccountScore = 0;
```

```
def resolutionType = getAttribute("ResolutionType");

if (resolutionType == "MERGE") {
for (row in requestRows) {
def osrRows = row.getAttribute("OriginalSystemReference");
osrRows.reset();
while (osrRows.hasNext()) {
def osrRow = osrRows.next()
if (osrRow.OrigSystem == "RNOW") {
osrMap['RNOW'].add(row);
}
}
}

if (rowMaster == false && osrMap['RNOW'].size() > 0) {
rowMaster = osrMap['RNOW'][0];
for (row in osrMap['RNOW']) {
if (row.LastUpdateDate > rowMaster.LastUpdateDate) {
rowMaster = row;
}
}
}
}

if (rowMaster) {
selectMaster(rowMaster);
} else {
selectMaster(rowDefaultMaster);
}

} catch (Exception e) {
def sMsg = "Exception in Account Set Master: " + e.getMessage();
println(sMsg);
}
```

Configure Groovy Script Based Set Attribute Value Rules

In this example, you will learn how to create a set attribute value rule to override the standard attribute source confidence-based survivorship processing with groovy script based on the classification code assignment of the records.

The logical requirements of the scenario are as follows:

- If the merge contains a record that has been classified as `OFN Category One account`, use that `OFN Category One record's value` for a set of key fields regardless of the attribute source confidence score.
- If multiple rows in the merge have been classified as `OFN Category One`, use the attribute values from the most recently updated row.

Steps to Perform

1. Enable Groovy Scripts to select master records:
    a. In the Setup and Maintenance work area, go to the following:
        - Offering: Customer Data Management
        - Functional Area: Customer Hub
        - Task: Manage Customer Data Management Options
    b. In the Merge Behavior section under the Duplicate Resolution Options tab, select the following options:
        - Select either Use source confidence with newest record as the tie breaker or Use source confidence with oldest record as the tiebreaker for the Attribute Selection Type field.
        - Select Yes for the Add Groovy to Attribute Selection field.
    c. Create an Application Composer sandbox. Refer to the Create an Application Composer Sandbox topic for the steps.
2. Populate the sample script in the `AccountSetAttribute` template:
    a. Navigate to **Common Setup** and click **Data Quality Rules**.
    b. Copy and paste the code given in Sample Code section in the Edit Data Quality Rules page.
    c. Click Save and Close.
3. Test the code. Refer to the Test the Survivorship and Agreement Rules Configuration section to test the code.
4. Deploy the code after you're satisfied with the results of the attribute value rules, you can. See the topic: Deploy the Survivorship and Agreement Rules Configuration.

What the Sample Script Does

The script begins by calling the `getRows()input function` to access the records in the merge request. Next, the script loops through each of the row records and accesses its Code Assignment collection. The script then loops through the code assignments to test whether the specified code assignment value is present. When a row having the specified code assignment is identified, the row is copied into an array of prioritized records for subsequent processing.

Once all the rows in the merge request have been tested for their code assignment values, the list of prioritized records is sorted based on the records' last update date. Finally, the script identifies the most recently updated row having the specified code assignment value. After this row is identified, the script calls the `selectAttribute() output function` to designate that priority row as being the attribute value source for a set of defined attributes.

Sample Code

```
try {
 def rowDuplicates = getRows();
 def rowPriorities = [];
 def exceptionAttributes = ['BusinessScope', 'CeoTitle'];
 def CAs;
 def CAi;
 for(row in rowDuplicates){
 CAs = row.getAttribute("CodeAssignment");
 if(CAs){
 for(CA in CAs){
 CA.reset();
 while(CA.hasNext()) {
 CAi = CA.next();
 if(CAi.ClassCategory == "OFN" && CAi.ClassCode == "OFN1") {
 rowPriorities.add(row);}
 }
 }
 }
 }
```

```
    if(rowPriorities.size()){
    def rowPriority = rowPriorities[0];
    for (row in rowPriorities){
    if (row.LastUpdateDate > rowPriority.LastUpdateDate){
    rowPriority = row;}
    }

    for (a in exceptionAttributes){
    selectAttribute(a, rowPriority);
    }
    }
  }

  catch(Exception e) {
    def sMsg = "Exception in Account Set Attribute: " + e.getMessage();
    println(sMsg);
  }
```

Configure Groovy Script Based Agreement Rules

In this example, we are operating in a complex business ecosystem where it's not always appropriate to merge certain accounts that have been identified as duplicates.

When the conditions that prohibit a merge from happening are encountered, the data steward needs to see an informative message explaining exactly which records blocked the merge, and for what reasons. The conditions that can prevent a merge are as follows:

When the conditions that prohibit a merge from happening are encountered, the data steward needs to see an informative message explaining exactly which records blocked the merge, and for what reasons. The conditions that can prevent a merge are as follows:

- A non-master record is integrated with the Legal Hold system
- A non-master record has a Certification Score value of 100

Steps to Perform

1. Enable Groovy Scripts to select master records:
    a. In the Setup and Maintenance work area, go to the following:
        - Offering: Customer Data Management
        - Functional Area: Customer Hub
        - Task: Manage Customer Data Management Options
    b. In the Merge Behavior section under the Duplicate Resolution Options tab, select the Default agreement rules with groovy scripts option for the Agreement Rules Type field.
2. Create an Application Composer sandbox. Refer to the Create an Application Composer Sandbox topic for the steps.
3. Populate the sample script in the `AccountMergeAgreement` template:
    a. Navigate to **Common Setup** and click **Data Quality Rules**.
    b. Click `AccountMergeAgreement`.
4. Copy and paste the code given in the Sample Code section in the Edit Data Quality Rules page.
5. Click Save and Close.
6. Test the code. Refer to the Test the Survivorship and Agreement Rules Configuration topic to test the code.
7. Deploy the code after you're satisfied with the results of the agreement rules. See the topic: Deploy the Survivorship and Agreement Rules Configuration.

What the Sample Script Does

The script begins by calling the `getNonMasters()input function` to access the non-master records in the merge request. Note that the result of a Set Master groovy scripts is expressed in `getMaster()` and `getNonMasters()` responses in Agreement Rule and Attribute Selection scripts. Next, the script loops through each of the row records to test for the two different conditions that would lead to the merge being rejected. The first test is to evaluate the source system reference assignments of the records to determine if the record is integrated with the Legal Hold system. The second test is to check the Certification Level value of the non-master records. If a given record matches either of the tests, a partial rejection message is added to the `vetoMessages` array.

After all the non-master rows in the merge request have been tested, the script checks to see if the `vetoMessages` array has any data in it. If it does, then a final rejection message is constructed from the data in the `vetoMessages` array and the merge is rejected with that constructed message being displayed to the data steward in the duplicate resolution UI.

Sample Code

```
try {
 def rowNonMasters = getNonMasters();
 def sMsg = "";
 def rejectMsg = "";
 def vetoMessages = [];
 for (row in rowNonMasters){
 def OSRs = row.getAttribute("OriginalSystemReference");
 OSRs.reset();
 sMsg = "";
 while(OSRs.hasNext()) {
 def OS = OSRs.next();
 if (OS.getAttribute("OrigSystem") == "LEGAL_HOLD" && sMsg == "") {
 sMsg = "A legal hold has been placed on Account " + row.getAttribute("PartyNumber");
 vetoMessages.add(sMsg);}
 }
 sMsg = "";
 if (row.getAttribute("CertificationLevel") == "100") {
 sMsg = "A Certification Level of 100 was found on Account " + row.getAttribute("PartyNumber");
 vetoMessages.add(sMsg);}
 }

 if (vetoMessages.size()) {
 rejectMsg = "Merge rejection reasons: ";
 vetoMessages.eachWithIndex { item, index ->
 rejectMsg += ((index +1) + ") " + item + " ");
 }
 rejectRequest(rejectMsg);
 }
}

catch(Exception e) {
 def sMsg = "Exception in Account Merge Agreement: " + e.getMessage();
 println(sMsg);
}
```

Test the Survivorship and Agreement Rules Configuration

You can test your Groovy Script-based survivorship and agreement rules configuration while working inside of the sandbox by creating a Test Merge Request in the Duplicate Resolution work area.

A Test Merge Request invokes whatever survivorship and agreement rules have been configured inside the current sandbox. For more information about creating test merge requests, see Related Topics section.

After you have identified potential duplicates in your database through a duplicate identification batch, you can resolve these duplicate sets by creating and submitting a duplicate resolution request.

To create and submit a resolution request:

1. Navigate to the Create Resolution Request UI page as follows: **Navigator** > **Customer Data Management** > **Duplicate Resolution** > **Tasks**
2. Click **Create Resolution Request**.
3. Search for and multi-select the duplicate records using the shift key.
4. Click Create Request.
5. Click Test Merge and click OK.

   You can optionally select one of the records as master. Once the request is submitted, the application generates a Request ID, which you can use to track the status of the duplicate resolution process.
6. You can tweak your survivorship and agreement rules configuration and retest your code using new test merge requests to ensure that the code is working as expected.

   > **Note:** This process tests the merge request configuration without changing your application data.

Deploy the Survivorship and Agreement Rules Configuration

When you're satisfied with your configured survivorship and agreement rules, you can deploy the configuration by using the standard sandbox publication process.

When you publish the sandbox, whatever Groovy Script-based rules were previously in the mainline configuration are replaced with whatever scripts are in the sandbox. Once the sandbox has been published, the Request Dispatch scheduled process begins to use the new Groovy Scripts during the processing of regular merge requests.

To publish a sandbox to deploy your survivorship and agreement rules configuration:

1. Click **Navigator** > **Configuration** > **Sandboxes**
2. On the Sandboxes page, click the name of the sandbox you want to publish.
3. Click Publish.

   > **Note:** The Publish button might be disabled for your sandbox because of various reasons. For example, you haven't yet made any changes in your sandbox, or the Control Publish Sandbox Action in Production Environment profile option (FND_ALLOW_PUBLISH_SANDBOX) is set to No.
4. Click Continue to Publish. The sandbox is published.
5. Click Done.

Best Practices for Configuring Groovy Scripts Based Survivorship and Agreement Rules

In this topic we discuss the best practices for configuring groovy scripts.

- If you configure your implementation to use Groovy Scripts for Set Master rules, merges aren't processed until a valid Set Master script has been deployed.
- Any survivorship rules written using the Manage Survivorship Rules setup task which uses the Oracle Business Rules framework, continues to function if you don't enable groovy script survivorship rules.
- For a given survivorship process type, such as Set Master or Agreement Rules, you can either use Groovy script or Oracle Business Rules. You can't combine the two frameworks for a single process type. For example you can't define one Set Master rule using Groovy Script and another Set Master rule using Oracle Business rules.
- You can combine Oracle Business Rules and Groovy script between different survivorship process types, such as using Oracle Business Rules for Set Master logic and Groovy script for Set Attribute logic.

- For best performance with attribute survivorship processing, try to use attribute source confidence as much as possible for your Set Attribute survivorship logic.
- Merge request processing may handle very large volumes of records, so groovy scripts should be as fast and efficient as possible. Avoid using `newView()` functions and web service calls unless absolutely necessary; and if necessary, assure that these types of operations will be fast and reliable.
- Select one of the Use source confidence Attribute Selection Type options from the Manage Customer Data Management Options setup page.
- If needed, use Groovy script along with your source confidence configuration to handle exception scenarios.

Overview of Groovy Scripting Functions

Groovy Script support for configuring survivorship and agreement rules is based on a specific set of functions that let you interact with the data records in the context of a merge request. These functions are of the following categories:

- Functions that let you inspect the records in the merge requests
- Functions that let you define the result of the merge request

These categories of specialized functions help you to create survivorship and agreement rules using standard Groovy Script syntax and operations.

`Input Functions`

These functions provide the data that your survivorship and agreement rules evaluate. Generally, these functions are called at the beginning of your script to instantiate the information required to determine the proper merge process outputs.

`getRuleType()`

This function lets you determine the functional context of the script. This function returns `SetAttribute, SetMaster,` or Agreement depending on which type of script calls it. It's generally not necessary to programmatically determine the rule type because the script types are presented as distinct functions within the Application Composer Data Quality Rules task. But there may be cases where it's helpful for logging or testing.

`getObjectType()`

This function lets you determine what type of party the merge request is processing. This function returns PERSON or ORGANIZATION depending on which type of script calls it. It's generally not necessary to programmatically determine the object type because the scripts for Persons and Organizations are clearly differentiated as distinct functions within the Application Composer Data Quality Rules task. But there may be cases where it's helpful for logging or testing.

`getMaster()`

This function lets you access the data record that has been identified as the master record for the merge request. The function is called without parameters and it returns a single Row object that contains the details of the master record. The following example shows a typical usage of this function:

```
def rowMaster = getMaster();
def masterName = rowMaster.getAttribute("OrganizationName");
// etc...
```

`getNonMasters()`

This function lets you access the set of data records that have been identified as the non-master records for the merge request because the merge process inactivates them. This function is called without parameters and it returns a list of row objects consisting of one list entry for each non-master record. It's important to note that the `getNonMasters` list isn't an `ADF recordset object. ADF recordset functions` such as reset() and first() don't work with the list. The following example shows a typical usage of this function:

```
 getNonMasters()
def rowNonMasters = getNonMasters();
 def nonmasterName;
 for (nonmaster in rowNonMasters) {
 nonmasterName = nonmaster.getAttribute("OrganizationName"); }
 // etc...
```

`getRows()`

This function lets you access the full set of customer records for the merge request, which is the union of the master and non-master sets of rows. This function is called without parameters and it returns a list of row objects consisting of one list entry for each non-master record. Like the `getNonMasters` function, it's important to note that the `getRows` list isn't an `ADF recordset object`. `ADF recordset functions` such as reset() and first() don't work with the list. The following example shows a typical usage of this function:

```
def rowDuplicates = getRows()
 def duplicateName;
 for (duplicate in rowDuplicates) {
 duplicateName = duplicate.getAttribute("OrganizationName"); }
 // etc...
```

`getSourceInfo(Row row, String attributeName)`

This function lets you access information about which source system provided the current value of an attribute for a given master or non-master row. This function is called using the following parameters:

- A row object for the non-master or master row of interest
- The name of a source-confidence configured attribute

This function returns a source information record for the attribute in question. The structure of the source information record is as follows:

Attribute	Definition	Example
`RecordId`	The party ID of the person or organization record referenced by the row object parameter.	300100184760397
`AttributeName`	The name of the attribute parameter.	OrganizationName
`AttributeValue`	The current value of the attribute on the row.	Pinnacle Systems
`Source`	The code of the registered source system for the attribute value.	RNOW
`SourceConfidenceLevel`	The configured attribute source confidence value of the given attribute for the given source system.	90
`SourceUpdateDate`	The time stamp when the person or organization record was updated with the current value.	1/24/2020 11:48:03 PM

Note: The `getSourceInfo` function is only available for attributes that have been configured with source system confidence using the Manage Source System Confidence setup task.

The following example shows a typical usage of this function:

```
def rowDuplicates = getRows();
def rowSource;
def bestSource;
def bestValue;
bestSource = getSourceInfo(rowDuplicates[0],"OrganizationName");
for (row in rowDuplicates) {
rowSource = getSourceInfo(row,"OrganizationName");
if(rowSource.SourceConfidenceLevel > bestSource.SourceConfidenceLevel) {
bestSource = rowSource;
}
}
bestValue = bestSource.AttributeValue;
```

Output Functions

Output functions create the final behavior of the merge process based on the logic of a survivorship or agreement rule script. Generally, these functions are called at the end of the script after the data provided by the input functions has been evaluated with scripted logic.

`selectMaster(Row row)`

This function is used in Contact Set Master and Account Set Master scripts to specify which record from the merge request should be retained as the master record after the merge. This function takes a data Row instance as its only parameter, and whatever row is passed to the function is the record that's retained as the master. All other records in the merge request are inactivated during merge processing. The following example shows a typical usage of this function:

```
...
def masterRow = rowDuplicates[0];
for (row in rowDuplicates) {
if row.LastUpdateDate > masterRow.LastUpdateDate {
masterRow = row;
}
}
selectMaster(masterRow);
```

`selectAttribute(String attributeName, Row row)`

This function is used in Contact Set Attributes and Account Set Attributes scripts to define which attribute value instances from across the records in the merge should be used to build the master record. This function takes the name of an attribute and a Row instance as its parameters. The value for the given parameter that's found in the given row is retained on the master record. This function is logically equivalent to using the Duplicate Resolution override flow to select the source record for a given attribute. The following example shows the syntax of this function:

```
def rowDuplicates = getRows();
def bestSourceRow;
def fieldName = "OrganizationName";
rowBestSource = rowDuplicates[0];
for (row in rowDuplicates) {
if(getSourceInfo(row, fieldName).SourceConfidenceLevel > getSourceInfo(rowBestSource,
fieldName).SourceConfidenceLevel) {
rowBestSource = row;}
}
selectAttribute(fieldName, rowBestSource);
```

`overrideAttribute(String attributeName, Object attributeValue)`

This function is used in Contact Set Attribute and Account Set Attribute rules to specify an attribute value for the master record, which can't be derived in the normal fashion from the records in the merge request. This function takes the name of an attribute and the value for the attribute as its parameters and sets the final value of the master record's given field to the given value. This function is logically equivalent to using the Duplicate Resolution Override flow to enter your own value for a given attribute.

Note: Ensure that the value's data type and format are correct because this function sets an externally-defined value.

The following example shows the syntax for this function:

```
def fieldName = "OrganizationName";
 def fieldValue = "Pinnacle Systems";
 overrideAttribute(fieldName, fieldValue);
```

This function is used in Contact Agreement Rule and Account Agreement Rule scripts to veto a merge request if a specified set of conditions are observed in the merge request's records. This function takes a single parameter which defines the rejection message that's displayed on the merge request if the rejection criteria are met. The following example shows the syntax for this function:

```
def rowNonMasters = getNonMasters;
 for (row in rowNonMasters) {
 if (row.value != null) {
 rejectRequest("Unable to merge contacts that have this value");}
 }
```

Evaluating the Data

Once you have called the appropriate functions, your survivorship or agreement rules script need to evaluate the data to determine the correct merge result. This evaluation process uses standard Groovy Script operators and functions. For more information about Groovy scripts, see the Oracle Applications Cloud Groovy Scripting Reference guide.

Putting It Together

You can generally follow this pattern in groovy scripting:

1. `Call Input Functions`
2. `Evaluate the Data`
3. `Call Output Functions`

To further illustrate this concept, the following is a simple script to determine the master record for a merge request based on the most recent Last Updated Date from the records:

```
/* Input Functions: call getRows() to initialize a list of the party records in the merge request and then
define a variable to designate the Master record and set it to the first record in the list of Rows */
 def rowDuplicates = getRows();
 def masterRow = rowDuplicates[0];
/* Evaluate the Data: iterate through the list of records to determine if the current list item
was more recently updated than whatever record has been designated the master. If the current record was
 more recently updated,
promote it to become the new Master */
 for (row in rowDuplicates) {
 if (row.LastUpdateDate > masterRow.LastUpdateDate) {
 masterRow = row;
 }
 }
/* Call Output Functions: use the selectMaster() function to dictate which record from the merge set
should become the master */
 selectMaster(masterRow);
```

Best Practices for Groovy Scripting

Consider the following points when planning and configuring your survivorship and agreement rules using groovy scripts:

- The Rows returned by the `getRows()`, `getNonMasters()`, and `getMaster()` functions is a standard Groovy Script list object, not an `Oracle ADF recordset object`. You must use standard Groovy methods for traversing the `recordset` such as for (item in list) instead of ADF functions such as `reset()`, `first()`, or `hasNext()`.
- The responses of the `getRows()`, `getNonMasters()`, or `getMaster()` functions are cached for each script execution. So the data state of row objects of your scripts don't show any changes within the scope of a script execution.
- The result of a Set Master script is reflected in the response to `getNonMasters() or getMaster()` functions called in Set Attribute or Agreement Rules scripts.
- You can't access the Resolution Request header object in your survivorship scripts. The only supported means for initializing data objects in your scripts are the `input functions` described in this topic.
- The `selectAttribute()` and `overrideAttribute()` functions can be used on top-level attributes of the Row object. Fields that contain embedded child record collections can't be manipulated with these functions.
- You can interact with custom attributes and custom child objects by using the API name for the attribute or object that was specified when the custom entity was created in Application Composer.
- The script fragments provided in this topic are intended to illustrate the syntax and usage of the `Input and Output functions`. Refer to the Sample Scripts section for examples of complete scripts.
- Some Best Practices for writing Groovy Scripts are available in the Performance Best Practices for Using Scripts section of Performance Best Practices for Extending Oracle CX Sales and Fusion Service (Doc ID 2170121.1) on My Oracle Support: https://support.oracle.com/epmos/faces/DocumentDisplay?id=2170121.1
- The Groovy Script survivorship and agreement rule templates should only be used to configure Set Master, Attribute Survivorship and Agreement rules. Use of these templates for general processing extension or automation isn't supported and may cause incorrect or unpredictable behavior.

How you Configure Link Using Groovy Scripts

Link requests consist of configuring logic to:

- Specify that Groovy script will manage linking.
- Enter the Groovy script in Application Composer.

How You Enable Groovy Script-based Linking

Before you can start using groovy scripts to configure link, you must enable groovy scripting in Setup and Maintenance.

Follow these steps to enable Groovy Script-based linking:

1. In the Setup and Maintenance work area, go to the following:
    - Offering: Customer Data Management
    - Functional Area: Customer Hub
    - Task: Manage Customer Data Management Options

2. In the Link Behavior section under the Duplicate Resolution Options tab, select the groovy script options as the value for the Main Record Selection setting.

Configure Predefined Data Quality Rules to Process Link Requests in Application Composer

The configuration of Groovy Script for linking is done in Application Composer using the standard Unified Sandbox framework for developing and testing your scripts.

We recommend that you create a separate, dedicated sandbox for linking rather than combine this configuration with other types of Application Composer configuration activities. This approach gives you the greatest flexibility for design and deployment of your linking configuration.

In this example, you will learn how to create a set main link record rule to select the main record in a link request:

- The record with the highest Customer Profile Quality Score should be selected as the main record.
- If multiple records are tied for the highest Customer Profile Quality Score, use the most recently updated record as the tiebreaker.
- If none of the records in the link request have been assigned a Customer Profile Quality Score, take whatever record had been designated as main by the upstream process.

To create an Application Composer Sandbox:

1. Click **Navigator** > **Configuration** > **Application Composer** > **Sandboxes**.
2. Click Create Sandbox.
3. Specify a name and select Application Composer under All Tools. Also select the Publishable option as Yes.
4. Click Create and Enter.
5. Click the Application Composer icon.
6. Go to Common Setup and click Data Quality Rules.
7. Click the AccountSetMainLink template.
8. Copy and paste the code given in Sample Code section in the Edit Data Quality Rules page.
9. Click Save and Close.

Deploy the code. See the topic: Deploy the Link Request Configuration.

What the sample script does

The script begins by calling the getRows() input function which returns all the Parties selected in the link request.

The script loops through the records in the resolution request to inspect each record's Customer Profile Quality Score value. Each record's value is compared to the highest value found so far, and if the current row has a higher value than the highest value found so far, that row is promoted to become the master record of the link set.

Finally, the script calls the selectMaster() output function to designate the main record. If a top-priority or second-priority record was identified earlier in the script, that record is provided to the selectMaster() function. If no priority record was identified, then the default master record specified by the upstream process will be retained as the master record for the resolution request.

Sample Script:

```
try {
def requestRows = getRows();
def rowMaster = false;
def rowDefaultMaster = getMaster();
def iHighestAccountScore = 0;
for (row in requestRows)
{
```

```
if (nvl(row.getAttribute("ProfileQualityScore"), 0) > iHighestAccountScore) {
rowMaster = row;
iHighestAccountScore = row.getAttribute("ProfileQualityScore");
}
}
if (rowMaster) {
selectMaster(rowMaster);
} else {
selectMaster(rowDefaultMaster);
}
} catch (Exception e) {
def sMsg = "Exception in Account Set Master: " + e.getMessage();
println(sMsg);
}
```

Deploy the Link Request Configuration

When you're satisfied with your configured link logic, you can deploy the configuration by using the standard sandbox publication process.

When you publish the sandbox, whatever Groovy Script-based rules were previously in the mainline configuration are replaced with whatever scripts are in the sandbox. Once the sandbox has been published, the Request Dispatch scheduled process begins to use the new Groovy Scripts during the processing of regular link requests.

To publish a sandbox to deploy your link management configuration:

1. Click **Navigator** > **Configuration** > **Sandboxes**.
2. On the Sandboxes page, click the name of the sandbox you want to publish.
3. Click Publish.

   > **Note:** The Publish button might be disabled for your sandbox because of various reasons. For example, you haven't yet made any changes in your sandbox, or the Control Publish Sandbox Action in Production Environment profile option (FND_ALLOW_PUBLISH_SANDBOX) is set to No.

4. Click Continue to Publish. The sandbox is published.
5. Click Done.

Best Practices for Configuring Groovy Scripts for Link Requests

In this topic we discuss the best practices for configuring groovy scripts.

- If you configure your implementation to use Groovy Scripts for linking, your duplicate resolution requests aren't processed until a valid link management script has been deployed.
- Link request processing may handle very large volumes of records, so groovy scripts should be as fast and efficient as possible. Avoid using newView() functions and web service calls unless absolutely necessary; and if necessary, assure that these types of operations will be fast and reliable.

Overview of Groovy Scripting Functions

Groovy Script support for configuring link requests is based on a specific set of functions that let you interact with the duplicate data records. These functions are of the following categories:

- Functions that let you inspect the records in the link requests
- Functions that let you define the result of the link request

These categories of specialized functions help you to process link requests using standard Groovy Script syntax and operations.

Input Functions

These functions provide the data that your logic evaluates. Generally, these functions are called at the beginning of your script to instantiate the information required to determine the proper link process outputs.

`getObjectType()`

This function lets you determine what type of party the link request is processing. This function returns PERSON or ORGANIZATION depending on which type of script calls it. It's generally not necessary to programmatically determine the object type because the scripts for Persons and Organizations are clearly differentiated as distinct functions within the Application Composer Data Quality Rules task. But there may be cases where it's helpful for logging or testing.

`getMaster()`

This function lets you access the data record that has been identified as the master record for the link request. The function is called without parameters and it returns a single Row object that contains the details of the master record. The following example shows a typical usage of this function:

```
Copy
 def rowMaster = getMaster();
 def masterName = rowMaster.getAttribute("OrganizationName");
 // etc...
```

`getNonMasters()`

This function lets you access the set of data records that have been identified as the non-master records for the link request. This function is called without parameters and it returns a list of row objects consisting of one list entry for each non-master record. It's important to note that the **`getNonMasters`** list isn't an **`ADF recordset object`**. **`ADF recordset functions`** such as reset() and first() don't work with the list. The following example shows a typical usage of this function:

```
Copy
 getNonMasters()
def rowNonMasters = getNonMasters();
 def nonmasterName;
 for (nonmaster in rowNonMasters) {
 nonmasterName = nonmaster.getAttribute("OrganizationName"); }
 // etc...
```

`getRows()`

This function lets you access the full set of customer records for the link request, which is the union of the master and non-master sets of rows. This function is called without parameters and it returns a list of row objects consisting of one list entry for each non-master record. Like the **`getNonMasters`** function, it's important to note that the **`getRows`** list isn't an **`ADF recordset object`**. **`ADF recordset functions`** such as reset() and first() don't work with the list. The following example shows a typical usage of this function:

```
Copy
def rowDuplicates = getRows()
 def duplicateName;
 for (duplicate in rowDuplicates) {
 duplicateName = duplicate.getAttribute("OrganizationName"); }
 // etc...
```

`getSourceInfo(Row row,String attributeName)`

This function lets you access information about which source system provided the current value of an attribute for a given master or non-master row. This function is called using the following parameters:

- A row object for the non-master or master row of interest

- The name of a source-confidence configured attribute

This function returns a source information record for the attribute in question. The structure of the source information record is as follows:

Attribute	Definition	Example
`RecordId`	The party ID of the person or organization record referenced by the row object parameter.	300100184760397
`AttributeName`	The name of the attribute parameter.	OrganizationName
`AttributeValue`	The current value of the attribute on the row.	Pinnacle Systems
`Source`	The code of the registered source system for the attribute value.	RNOW
`SourceConfidenceLevel`	The configured attribute source confidence value of the given attribute for the given source system.	90
`SourceUpdateDate`	The time stamp when the person or organization record was updated with the current value.	1/24/2020 11:48:03 PM

The following example shows a typical usage of this function:

```
Copy
 def rowDuplicates = getRows();
 def rowSource;
 def bestSource;
 def bestValue;
 bestSource = getSourceInfo(rowDuplicates[0],"OrganizationName");
 for (row in rowDuplicates) {
 rowSource = getSourceInfo(row,"OrganizationName");
 if(rowSource.SourceConfidenceLevel > bestSource.SourceConfidenceLevel) {
 bestSource = rowSource;
 }
 }
 bestValue = bestSource.AttributeValue;
```

Output Functions

Output functions create the final behavior of the based on the logic of a link process script. Generally, these functions are called at the end of the script after the data provided by the input functions has been evaluated with scripted logic.

`selectMaster(Row row)`

This function is used in Contact Set Master and Account Set Master scripts to specify which record from the link request should be selected as the master record. This function takes a data Row instance as its only parameter, and whatever row is passed to the function is the record that's retained as the master. The following example shows a typical usage of this function:

```
Copy
...
 def masterRow = rowDuplicates[0];
 for (row in rowDuplicates) {
 if row.LastUpdateDate > masterRow.LastUpdateDate {
 masterRow = row;
 }
 }
```

```
selectMaster(masterRow);
```

Evaluating the Data

Once you have called the appropriate functions, your script needs to evaluate the data to determine the correct link result. This evaluation process uses standard Groovy Script operators and functions. For more information about Groovy scripts, see the Oracle Applications Cloud Groovy Scripting Reference guide.

Putting It Together

You can generally follow this pattern in groovy scripting:

1. Call Input Functions
2. Evaluate the Data
3. Call Output Functions

```
Copy
/* Input Functions: call getRows() to initialize a list of the party records in the merge request and then
define a variable to designate the Master record and set it to the first record in the list of Rows */
 def rowDuplicates = getRows();
 def masterRow = rowDuplicates[0];
/* Evaluate the Data: iterate through the list of records to determine if the current list item
was more recently updated than whatever record has been designated the master. If the current record was
 more recently updated,
promote it to become the new Master */
 for (row in rowDuplicates) {
 if (row.LastUpdateDate > masterRow.LastUpdateDate) {
 masterRow = row;
 }
 }
/* Call Output Functions: use the selectMaster() function to dictate which record from the merge set
should become the master */
 selectMaster(masterRow);
```

Best Practices for Groovy Scripting

Consider the following points when planning and configuring your survivorship and agreement rules using Groovy scripts:

- The Rows returned by the getRows(), getNonMasters(), and getMaster() functions is a standard Groovy Script list object, not an Oracle ADF record set object. You must use standard Groovy methods for traversing the record set such as for (item in list) instead of ADF functions such as reset(), first(), or hasNext().
- The responses of the getRows(), getNonMasters(), or getMaster() functions are cached for each script execution. So, the data state of row objects of your scripts don't show any changes within the scope of a script execution.
- You can't access the Resolution Request header object in your survivorship scripts. The only supported means for initializing data objects in your scripts are the input functions described in this topic.
- You can interact with custom attributes and custom child objects by using the API name for the attribute or object that was specified when the custom entity was created in Application Composer.
- The script fragments provided in this topic are intended to illustrate the syntax and usage of the Input and Output functions. See the Sample Scripts section for examples of complete scripts.
- Some Best Practices for writing Groovy Scripts are available in the Performance Best Practices for Using Scripts section of Performance Best Practices for Extending Oracle CX Sales and Fusion Service (Doc ID 2170121.1) on My Oracle Support: https://support.oracle.com/epmos/faces/DocumentDisplay?id=2170121.1
- The Groovy Script templates should only be used to configure Set Master. Use of these templates for general processing extension or automation isn't supported and might cause incorrect or unpredictable behavior.

Configure Duplicate Resolution Using Oracle Business Rules

How You Enable and Manage Survivorship Rules

Survivorship rules are a collection of business rules that create the best version of a record from multiple source systems.

These business rules use Source System Confidence scores as well as other criteria to determine the master or surviving record and its attributes that should be retained during merge operations.

Survivorship Rules Types

The two types of survivorship rules that are used together to define the best version of a surviving record are as follows:

- Set master record: Defines the criteria for selecting the master record at the record level.
- Set attribute value: Defines the criteria for selecting the best attribute values for the master record at the attribute level.

How You Enable Survivorship Rules

You can enable the survivorship functionality by setting the **ZCH_ENABLE_SURVIVORSHIP** profile option to Yes in the Setup and Maintenance work area, using the following:

- Offering: Customer Data Management
- Functional Area: Customer Hub
- Task: Manage Customer Hub Profile Options

How You Manage Survivorship Rules

You can create, edit, and delete survivorship rules in the Setup and Maintenance work area by going to the following:

- Offering: Customer Data Management
- Functional Area: Customer Hub
- Task: Manage Survivorship Rules

The rules use source system confidence level and other criteria to determine the attributes of the record that should be retained from a particular source system. Survivorship rules are stored in the rules dictionary XML file. The dictionary can be exported and imported through the Export Survivorship Rules Dictionary web service and the Import Survivorship Rules Dictionary web service.

> **Note:** The application doesn't support changing survivorship rules inside the Application Composer sandbox. Therefore, the merge engine doesn't pick up the changes made to these rules inside the Application Composer sandbox. When you define custom attributes or custom objects in an Application Composer sandbox, you should Publish and Exit the sandbox before changing a survivorship rule in the Manage Survivorship Rules setup task.

Predefined Survivorship Rules

Six predefined set attribute value rules are provided ready-to-use with the application:

- **Least Recently Updated Organization Attribute (History Wins):** This rule selects the organization attributes that have the oldest updated date.
- **Most Recently Updated Organization Attribute (Recent Wins):** This rule selects the organization attributes that have the most recent updated date.
- **Highest Source Confidence Level Wins for Organization:** This rule selects the organization attribute values that have the highest source confidence.
- **Least Recently Updated Person Attribute (History Wins):** This rule selects the person attributes that have the oldest updated date.
- **Most Recently Updated Person Attribute (Recent Wins):** This rule selects the person attributes that have the most recent updated date.
- **Highest Source Confidence Level Wins for Person:** This rule selects the person attribute values that have the highest source confidence.

In addition, you can use predefined templates to create new Set Attribute Value rules.

> **Note:** To see these predefined attribute rules, click Search button on the Manage Survivorship Rules task. You can use these predefined survivorship rules as a starting point to define the survivorship criteria that's best for your business. These rules are updated with every release. You can also create, edit, and delete these rules. However, deleting an existing rule isn't recommended. By default, these predefined survivorship rules are in the inactive status and you can activate these rules from the Manage Survivorship Rules task.

Define Survivorship Rules

This example demonstrates how to create a survivorship rule. Survivorship rules enable intelligent creation of the best version record, especially from multiple source systems, by specifying criteria for selecting the record to be retained during a merge operation.

Create A Survivorship Rule

To create a survivorship rule:

1. In the Setup and Maintenance work area, go to the following:
    - Offering: Customer Data Management
    - Functional Area: Customer Hub
    - Task: Manage Survivorship Rules
2. On the Manage Survivorship Rules page, click **Add** from the Actions menu.
3. Enter the sample information provided in the following table on the Create Survivorship Rule page.

Field	Value
Rule Name	PickPersonMasterRule

Field	Value
Description	Select the master person record based on original source system of the record.
Rule Type	Set master record **Note:** Note: You can create the following two types of survivorship rules: Set Master Record and Set Attribute Value. You can use predefined templates to create the Set Attribute Value rules.
Object Type	Person **Note:** You can create a survivorship rule for the following two types of party records: Person and Organization.

4. Click **Apply**. The Define Survivorship Rules: Select Master Record page appears.

Specify Criteria for Selecting the Master Record

The following are the steps to specify criteria for selecting the master record:

1. Navigate to the Define Survivorship Rules: Select Master Record page.
2. Enter the information provided in the following table as IF/THEN rules condition in the Define Survivorship Rules: Select Master Record page.

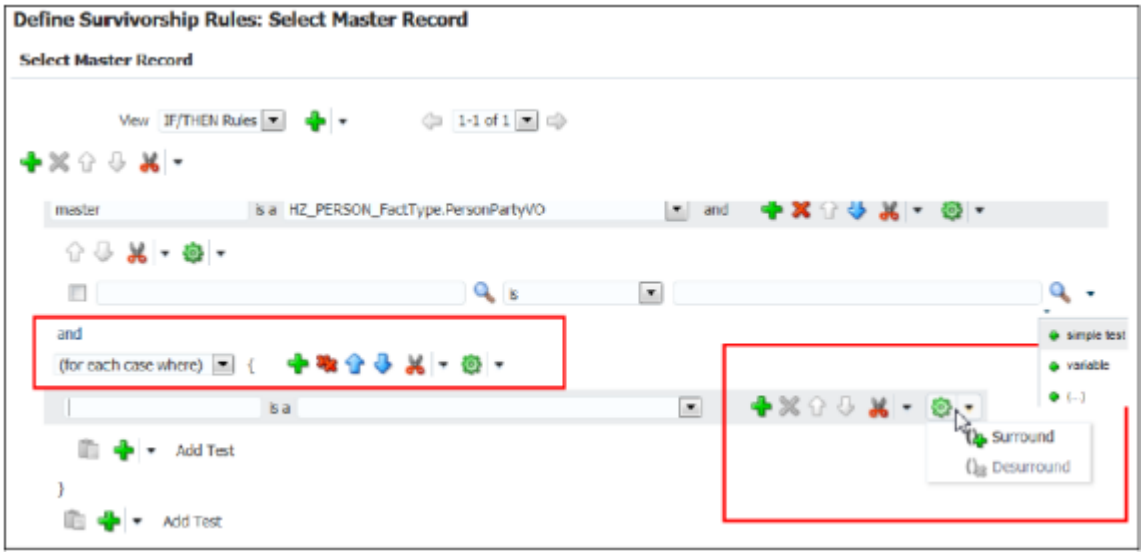
Rule Condition	Value
IF Condition	`IF PersonParty is a TCHFactTypeDictionary.PersonPartyVO and there's a case where {OrigSourceSystem} != null and OrigSourceSystem.OwnerTableId == PersonParty.PartyId and OrigSourceSystem.OrigSystem == "GSI"}`
THEN Condition	`THEN Assert new Result (name:"masterId", value:"PersonParty.PartyId)`

Rule Condition	Value

Note the following specification in the Define Survivorship Rules: Select Master Record page.

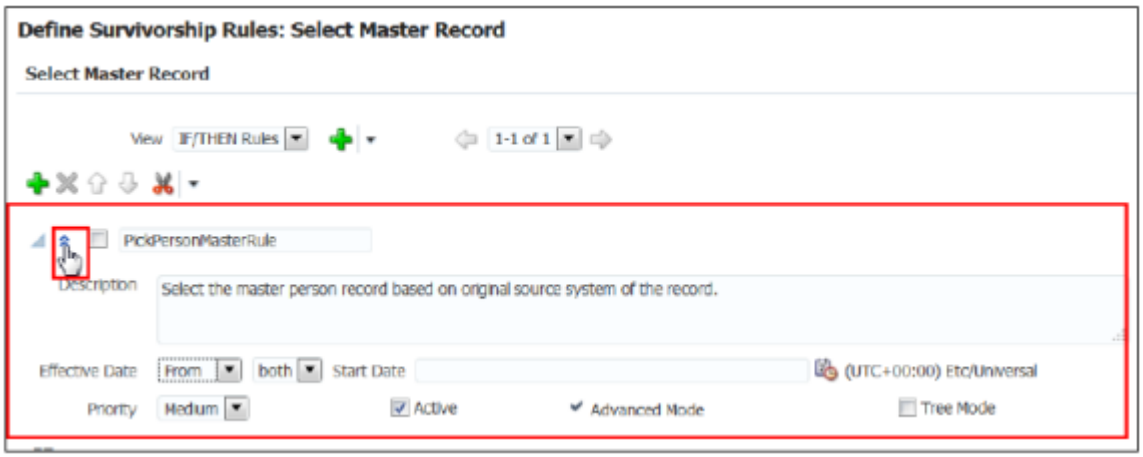
- Click the + icon to add additional patterns to include additional conditions
- Click the Surround with Parenthesis option to add more features to the conditions
- Select the + Simple Test option to add additional clauses

The following figure shows the Define Survivorship Rules: Select Master Record page with the Surround icon highlighted.



3. Click the Advanced Settings button to verify the effective date of the rule that you're going to create.

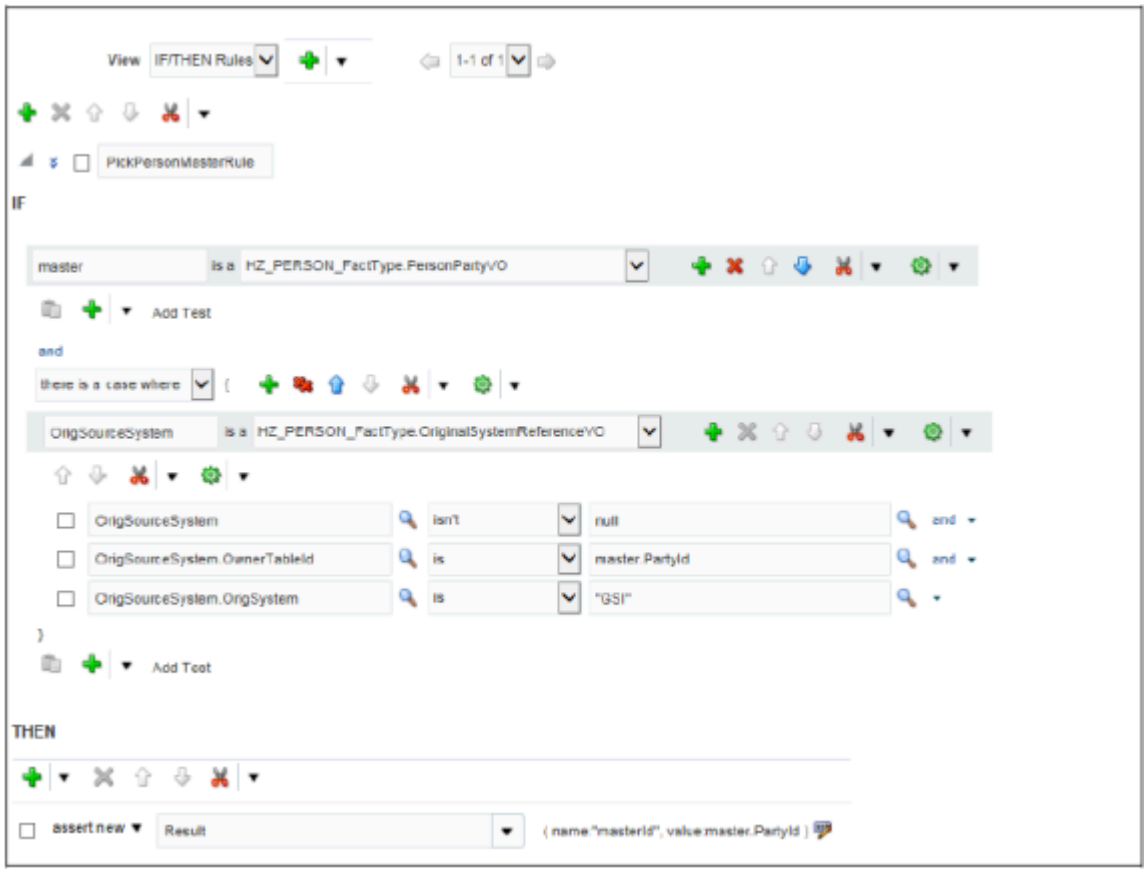
   The following figure shows Advanced Settings icon on the Define Survivorship Rule: Select Master Record page.



4. Select an effective date, as appropriate. The default effective date is Always. You can select an Effective From or Effective To date, or you can select an Effective Date range.
5. Select a priority for the rule, as appropriate.

   The default priority of the Survivorship rules is Medium. These rules get executed in the order of their priority.
6. Ensure that the Rules Active option is selected.

The following figure shows how the survivorship rule looks like when fully defined. The details include the rule name and the IF and THEN conditions for determining the master.



7. Click Save and Close. You can view the newly created rule in the Manage Survivorship Rules page by searching for it.
8. Click Submit.

> **Tip:** To activate the rule you must click Submit. You may have selected the Active mode, but that doesn't activate a rule unless submitted.

Related Topics

- MOS document: Define Survivorship Rules

Define Set Master Record Rules

This procedure demonstrates how to create a survivorship rule of the type Set Master Record.

You can determine survivorship at the record level using the set master record rule type. Set master rules are used in party merge to set a single record as the master record.

Create Set Master Record Rules

The input to the survivorship rule is given in the IF clause. In a set master rule, the input is a set of party records. The THEN clause contains the output that determines the master record. In the Set Master Record rule, the output is a result object that contains a specific Party ID. If multiple records with different Party IDs are returned, then it results in a conflict error. To create Set Master rules, you may perform the following steps:

To create Set Master rules, you perform the following steps:

1. Navigate to the Manage Survivorship Rules task.
2. Click Add. The Create Survivorship Rule page appears.
3. Enter the information provided in the following table on the Create Survivorship Rule page.

Field	Value
Rule Name	PickOrganizationMasterRule
Description	Select the master organization record based on the specified criteria for setting the master record.
Rule Type	Set master record
Object Type	Organization

4. Click Apply. You're taken to the Define Survivorship Rules: Select Master Record page.

In the Define Survivorship Rules: Select Master Record page, you specify criteria for picking the master record. The criteria that you define in this page determine the output of the rule.

The following topics contains three worked examples that show different ways of defining criteria in the Define Survivorship Rules: Select Master Record page to set a master records:

- Set the Record with Oldest Creation Date as Master
- Set the Record with D-U-N-S Number and Smallest Party ID as Master
- Set the Record with D-U-N-S Number and Highest Number of Party Site as Master

How You Set the Record with the Oldest Creation Date as Master

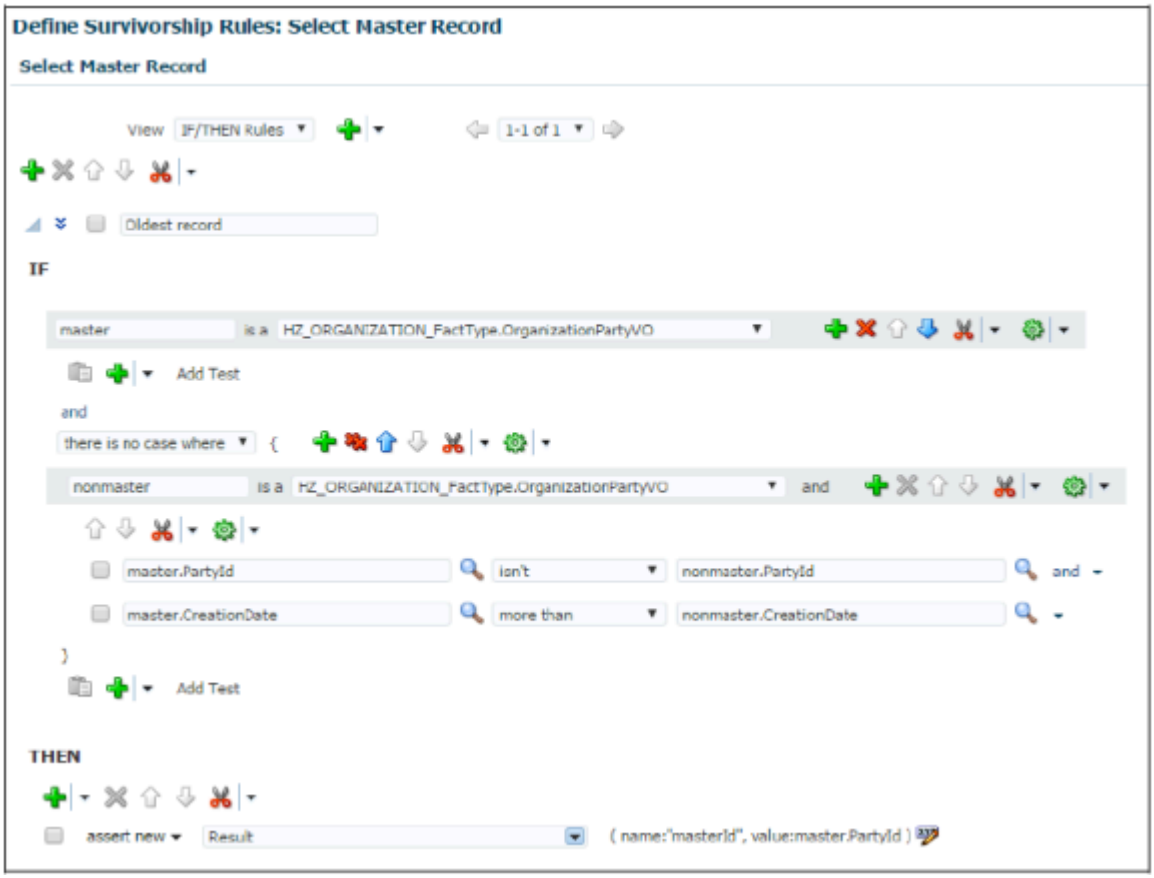
This rule has a single condition to set a record that has the oldest creation date as the master.

1. Navigate to the Define Survivorship Rules: Select Master Record page.
2. Enter the information provided in the following table as IF/THEN rules condition in the Define Survivorship Rule: Select Master Record page.

Rule Condition	Value
IF Condition	`IF master is an HZ_PERSON_FactType.PersonPartyVO`

Rule Condition	Value
	`and there is no case where {nonmaster == HZ_PERSON_FactType.PersonPartyVO and master.PartyId isn't nonmaster.PartyId and master.creationDate is more than nonmaster.CreationDate}`
THEN Condition	`THEN Assert new Result (name:"masterId", value:" master.PartyId)`

The following figure displays the Define Survivorship Rules: Select Master Record page with completely filled IF and THEN rules conditions for setting a record that has the oldest creation date as the master.



How You Set the Record with D-U-N-S Number and Smallest Party ID as Master

This rule identifies and returns the master record based on the following three conditions in the order of priority listed:

1. Pick master that has D-U-N-S Number.
2. If more than one record has D-U-N-S Number, pick one based on the smallest Party ID.
3. If no record has D-U-N-S Number, pick one based on the smallest Party ID.

The following are the use cases for a set master record rule to pick the master based on the D-U-N-S number and the smallest Party ID.

Use Case 1

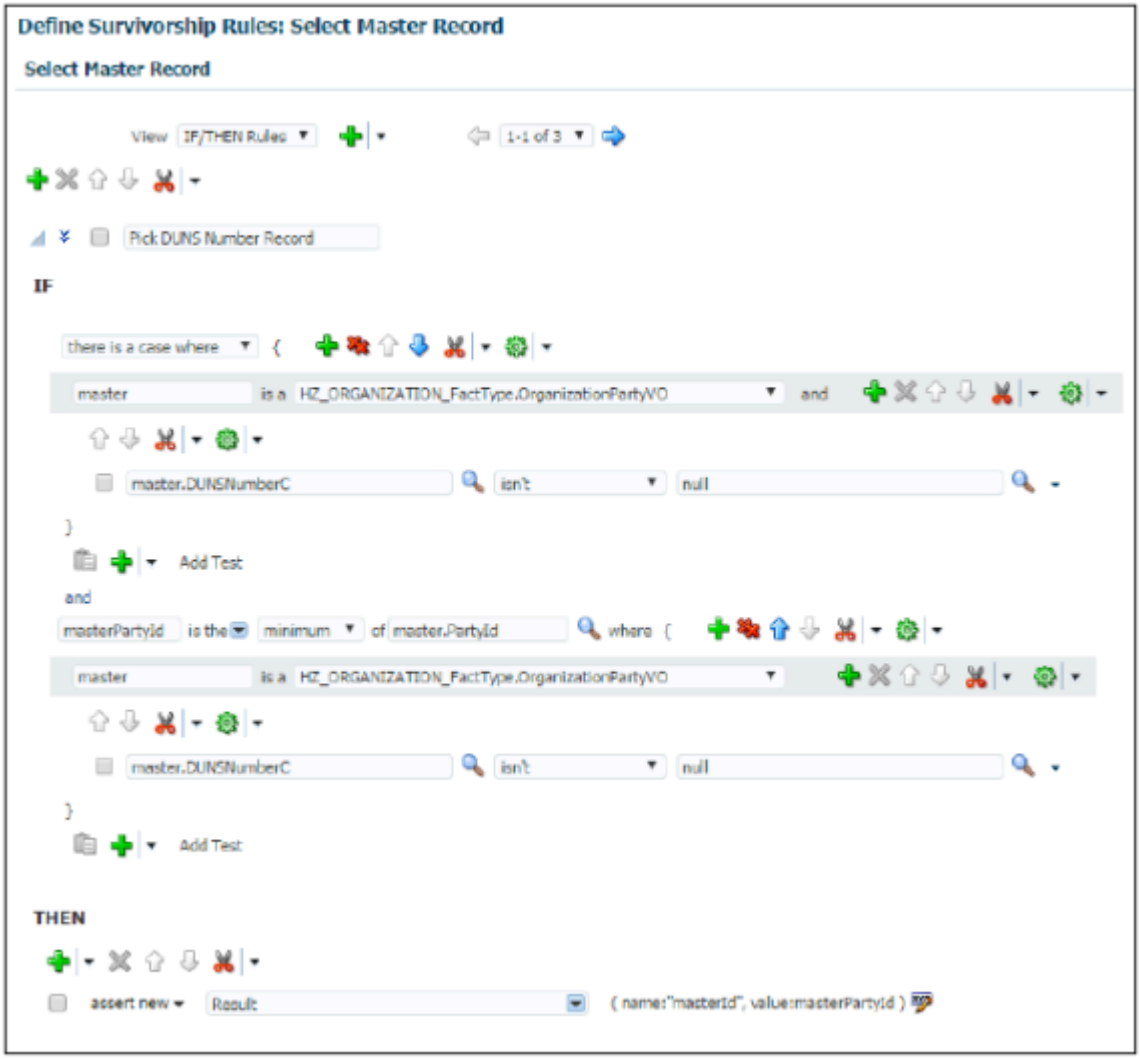
In this case, there are two records with D-U-N-S number. Therefore, the record with the smaller party ID is picked as the master record. The following table contains the sample record information for this use case.

Record Name	Party ID	D-U-N-S Number	Master
Record 1	11	998837472	Yes
Record 2	12	null	No
Record 3	13	984939234	No

The following table lists the IF and THEN rules condition values that you must enter on the Define Survivorship Rules: Select Master Record page for this use case.

Rule Condition	Value
IF Condition	`Pick D-U-N-S number{IF master is an HZ_PERSON_FactType.OrganizationPartyVO master.DUNsNumberC isn't null} masterPartyID is the minimum of masterPartyID where {master= HZ_PERSON_FactType.OrganizationPartyVO and master.DUNsNumberC isn't null}`
THEN Condition	`THEN Assert new Result (name:"masterId", value:" master.PartyId)`

The following figure shows the Define Survivorship Rules: Select Master Record page with IF and THEN rules conditions for picking the record with D-U-N-S number and minimum party ID as master.



Use Case 2

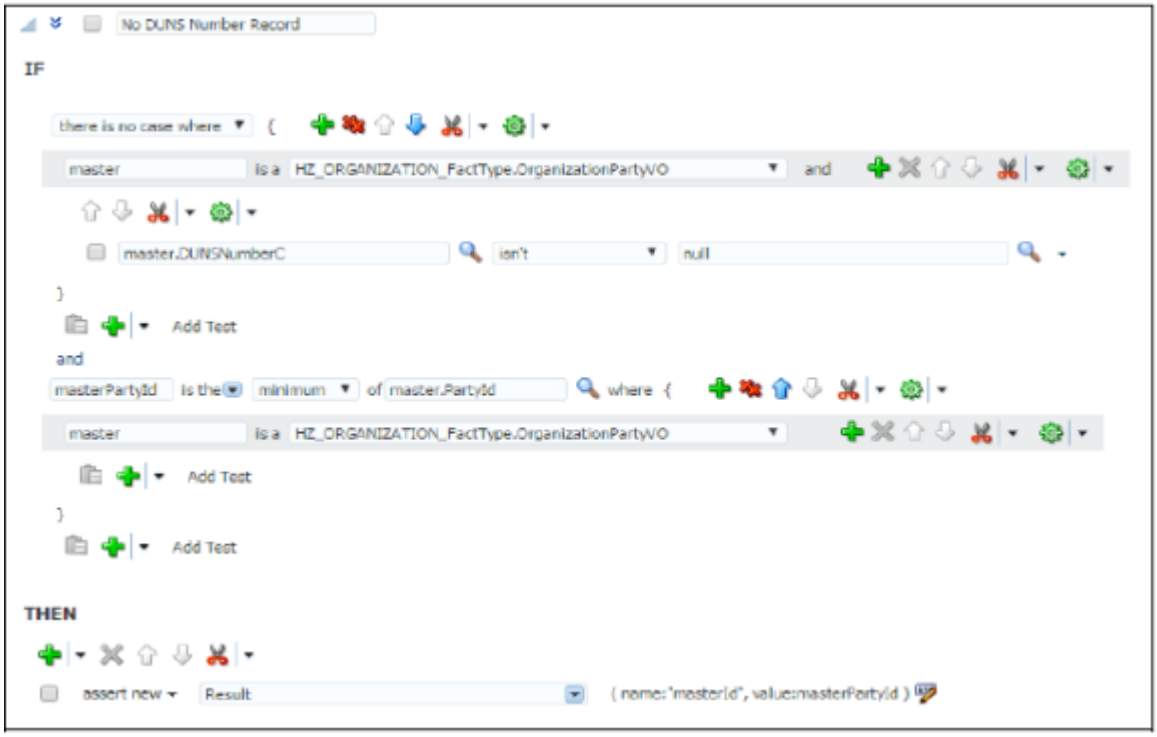
In this case, there is no record with D-U-N-S number. Therefore, the record with smallest party ID is picked as the master record. The following table lists the sample record information for this use case.

Record Name	Party ID	D-U-N-S Number	Master
Record 1	21	null	Yes
Record 2	22	null	No
Record 3	23	null	No

The following table lists the IF and THEN rules condition values that you must enter on the Define Survivorship Rules: Select Master Record page for this use case.

Rule Condition	Value
IF Condition	**Pick D-U-N-S number** **{IF master is an HZ_PERSON_FactType.OrganizationPartyVO** **master.DUNsNumberC isn't null}** **and** **masterPartyID is the minimum of masterPartyID** **where** **{master= HZ_PERSON_FactType.OrganizationPartyVO and** **master.DUNsNumberC isn't null}**
THEN Condition	**THEN** **Assert new Result (name:"masterId", value:" master.PartyId)**

The following figure displays the Define Survivorship Rules: Select Master Record page with completely filled IF and THEN rules conditions to set the record that has the smallest party ID as the master when no record with D-U-N-S number is found.



In this example, you have created two set master rules for Organization. First rule is for the cases where the input records have at least one record with D-U-N-S number. The second is for the case where no records have D-U-N-S Number.

> **Note:** You can activate more than one survivorship rule at a time. When you activate multiple rules, make sure that the rules aren't conflicting and the conditions in the rule are set according to the priority.

How You Set the Record with D-U-N-S Number and Highest Number of Party Sites as Master

This rule identifies and returns the master record based on the following three conditions in the order of priority listed:

1. Pick master that has D-U-N-S Number.
2. Pick master that has more party sites.
3. Pick master that has the smallest Party ID.

The following are two use cases for creating a set master rule to select the master record based on D-U-N-S number, number of party sites, and party ID:

Use Case 1

In this case, there are three records with D-U-N-S number and two records with highest number of party sites. Among those two records, the one with the lower value for party ID is selected as master. The following table contains the sample record information for this use case.

Record Name	Party ID	Number of Party Sites	D-U-N-S Number	Master
Record 1	11	3	198837472	Yes
Record 2	12	3	489203901	No
Record 3	13	2	384792392	No
Record 4	14	1	null	No

Use Case 2

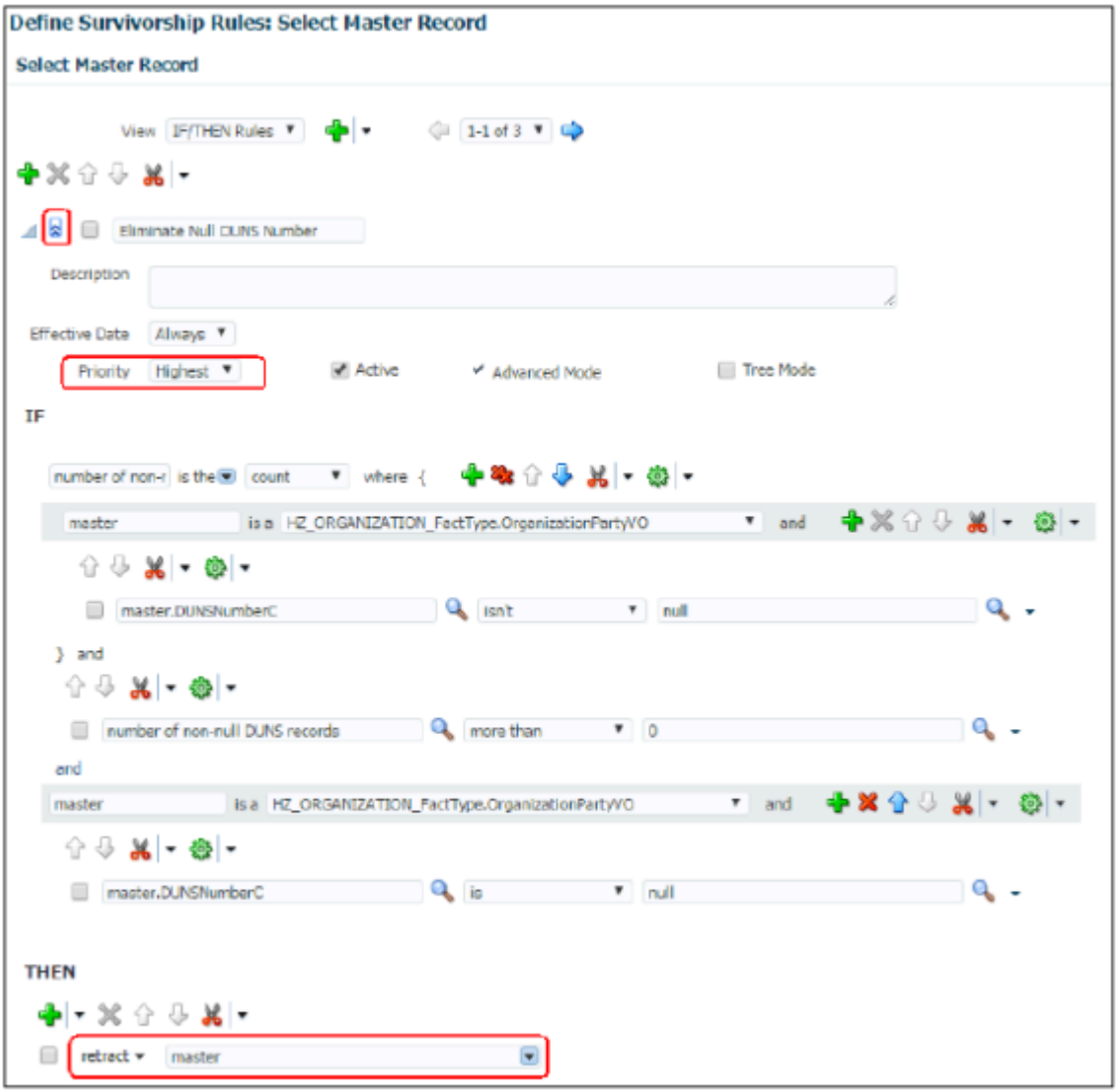
In this case, there are no records with D-U-N-S number. So, among the two records with higher number of party sites, the record with the smaller party ID is picked as the master record. The following table contains the sample record information for this use case.

Record Name	Party ID	Number of Party Sites	D-U-N-S Number	Master
Record 1	21	1	null	No
Record 2	22	2	null	Yes
Record 3	23	3	null	No

To create a master record with D-U-N-S number, number of party sites, and party ID, you add one more condition to the previous example where you set a master record with D-U-N-S number. Adding a condition to the previous example makes the rules complicated and cumbersome. Instead, you can create a simple rule for each condition to narrow down the list of potential master records and create another simple rule in the end to pick one record from the remaining potential master records.

> **Note:** You can activate more than one survivorship rule at a time. When you activate multiple rules, make sure that the rules aren't conflicting and the conditions in the rule are set according to the priority.

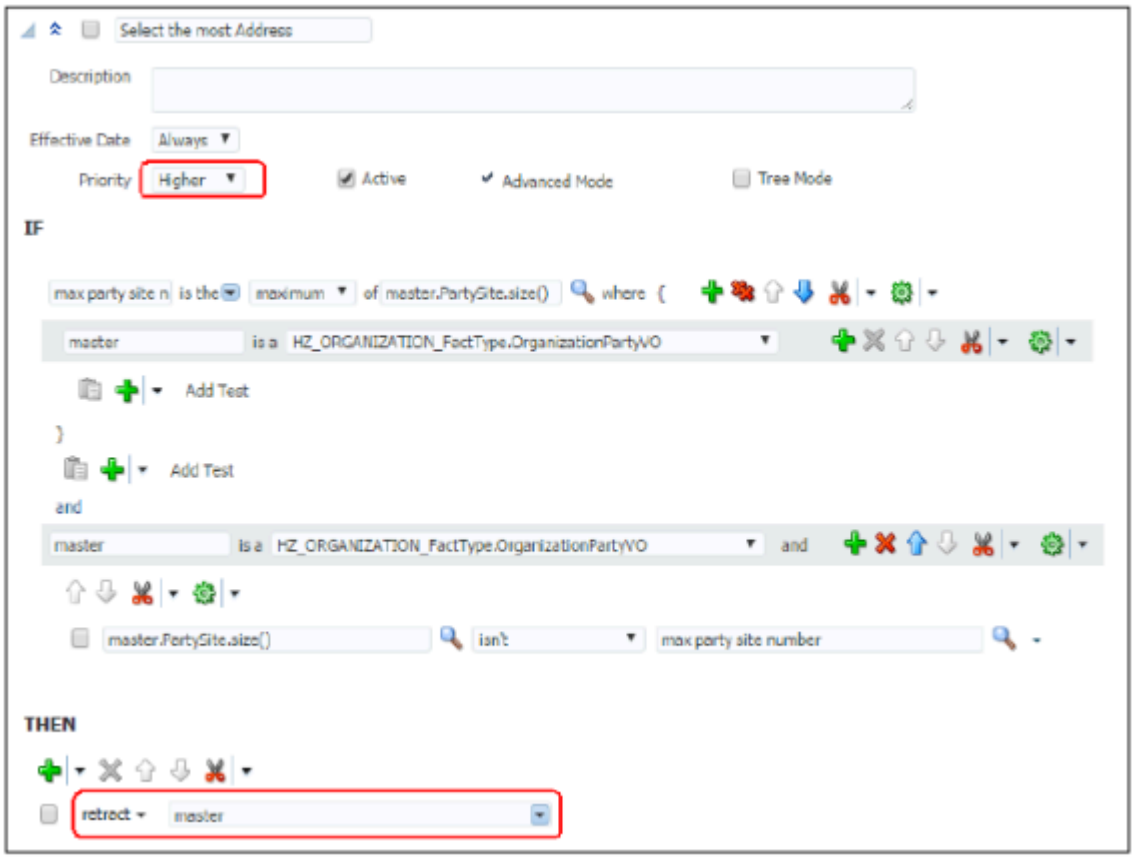
The following figure displays the Survivorship Rules: Select Master Record page with the IF and THEN rules condition values for creating a set master rule to set the record that has D-U-N-S Number as master. The priority of the rule is set as highest. The details of the conditions are as follows:Priority: HighestIF condition: If number of non-null DUNS records is the count where {master is a HZ_ORGANIZATION_FactType.OrganizationPartyVO and master.DUNSNumberC isn't null} and number of non-null DUNS records more than 0 and master is a HZ_ORGANIZATION_FactType.OrganizationPartyVO and master.DUNSNumberC is nullTHEN condition: Then retract master



Now, you set the conditions to set the record with the maximum number of party sites as the master.

The following figure shows the Survivorship Rules: Select Master Record page with the IF and THEN condition values to set the record with the maximum number of party sites as the master from the remaining potential records. The priority of the rule is set as higher. The details of the conditions are as follows.Priority: HigherIF condition: If maximum party site number is the maximum of master.PartySite.size() where {master is a HZ_ORGANIZATION_FactType.OrganizationPartyVO} and master is a HZ_ORGANIZATION_FactType.OrganizationPartyVO and master.PartySite.size() isn't maximum party site numberTHEN

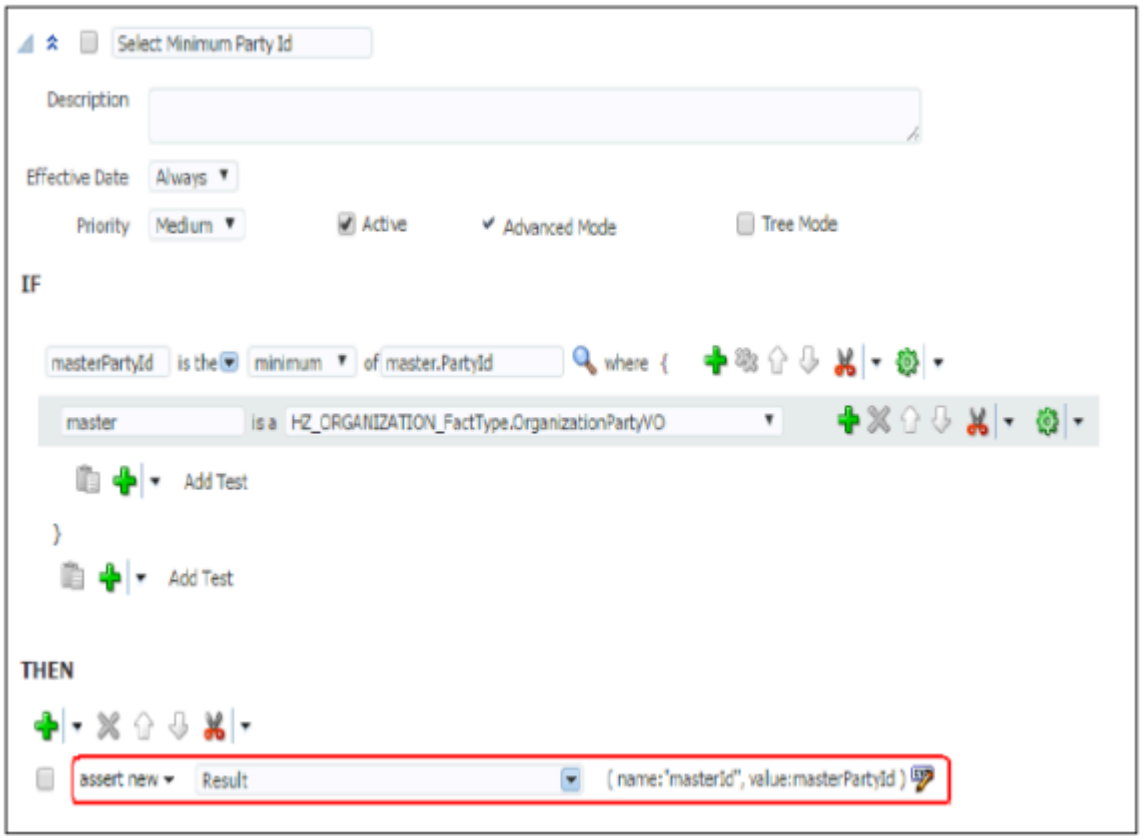
condition: Then retract master



When the records are screened with two previous conditions, you create a third condition to screen all remaining potential records with the smallest party ID.

The following figure shows the Survivorship Rules: Select Master Record page with the IF and THEN condition values for creating a set master rule to set the record with the smallest party ID as the master. The priority of the rule is set as medium. The details of the conditions are as follows.Priority: MediumIF condition: If masterPartyId is the minimum of master.PartyId where {master is a HZ_ORGANIZATION_FactType.OrganizationPartyVO}THEN condition: Assert new Result(name:

"masterId",value:masterPartyId)



In this example, the rules are created to narrow down the list of potential master records. When you activate more than one rule at a time you should set the conditions for the rule according to the priority to narrow down the list of potential master records. In this example Eliminate Null D-U-N-S Number rule is executed first to select records with D-U-N-S Number. Select the Most Address rule is executed next to find the master record with most number of party sites among the potential master records having D-U-N-S Number. Finally, Select Minimum Party ID rule is executed at the end to pick the minimum party ID from the remaining party records.

How do I define set attribute value rules?

This example demonstrates how to create a survivorship rule of the type Set Attribute Value.

You can determine survivorship at the attribute level using the set attribute value survivorship rule type. Set attribute value rules are used in party merge to determine which attribute value should come from which record.

The input to the survivorship rule is given in the IF clause. In a set attribute value rule, the inputs are the party records and their source information. The source information contains information about all attributes for each record in the database. If you're creating rules that use the Source information VO, you define it in the Define Source Systems Confidence page of the Manage Source System Confidence task. You must map each attribute to its source system and given a Source Confidence score on a scale of 1 to 100.

The following table lists the attributes in the source information VO to create a set attribute value rule.

Attribute Name	Description
RecordId	The record ID of a specific attribute.
AttributeName	The name of the attribute.
Source	The source system from where the attribute is updated.
SourceConfidenceLevel	The source confidence level assigned to the source system.
SourceUpdateDate	The date when the attribute was last updated.

The THEN clause determines the output object that picks the master record. In this case, setAttribute function creates the output object. To create Set Attribute Value rules, you perform the following steps:

1. Navigate to the Manage Survivorship Rules task.
2. Click Add. The Create Survivorship Rule page appears.

   > **Tip:** You can select attributes from the available attributes in the Create Survivorship Rule page. It pre-populates the rule template with the selected attributes. It's not mandatory to set attributes from the available attribute.

3. Enter the sample information provided in the following table on the Create Survivorship Rule page.

Field	Value
Rule Name	PickAttributeValueRule
Description	Select the master value for a specific attribute based on specified master selection criteria.
Select the master value for a specific attribute based on specified master selection criteria.	Set attribute value
Object Type	Organization
Template	Select the Attribute Based template to select the surviving value based on the characteristic of the attributes. For example, you need an Attribute Based template to pick an attribute with the highest or lowest value such as a party number, or salary, or the earliest incorporated year. Select the Source Confidence Based template to select the surviving value based on the confidence in the source information.

4. Select attributes from the available attributes to pre-populate the rules template. In case you want to use the predefined set attribute rules, don't select any attributes.
5. Click Apply. You're taken to the Define Survivorship Rules: Select Attribute Value page.

In the Define Survivorship Rules: Select Attribute Value page, you specify criteria for selecting the master attribute value. The criteria that you define in this page determine the feature of the rule. You also have the option of using one of the following three predefined templates:

- Highest Source Confidence Level Wins for Organization (or Person): Use this rule to select the attribute values with the highest source confidence level.
- Most recently updated Organization (or person) attribute: Use this rule to select the attribute values with the most recently updated date.
- Least recently updated Organization (or person) attribute: Use this rule to select the attribute values with the oldest updated date.

The following sections of this topic contain three worked examples that show different ways of manually setting master attribute values in the Define Survivorship Rules: Select Attribute Value page. They are as follows:

- Set the Values with the Earliest Update Date as the Surviving Attribute Values
- Set the Value with the Highest Source Confidence Level as the Surviving Attribute Value for D-U-N-S Number
- Set the Values with the Earliest Incorporated Year as the Surviving Attribute Values

How You Set the Values with the Earliest Update Date as Surviving Attribute Values

This rule has a single condition to set all the surviving attribute values based on the earliest update date. The following is a use case for a set attribute rule to select the values with the earliest update date as surviving attribute values:

Use Case 1

Party Record

The following table contains information for party records.

Record Name	Party ID	Party Name	D-U-N-S Number
Record 1	1	Oracle Corp	198837472
Record 2	2	Oracle USA Corp	489203901
Record 3	3	Oracle	null

Source Information

The following table contains information for source information records.

Record ID	Attribute Name	Source	Source Confidence Level	Source Update Date
1	Party Name	FUSION	95	1/5/2016
2	Party Name	FUSION	95	1/5/2010
3	Party Name	SIEBEL	90	1/5/2000

Record ID	Attribute Name	Source	Source Confidence Level	Source Update Date
1	D-U-N-S Number	DNB	100	2/5/1990
2	D-U-N-S Number	FUSION	95	1/5/2016

In this case:

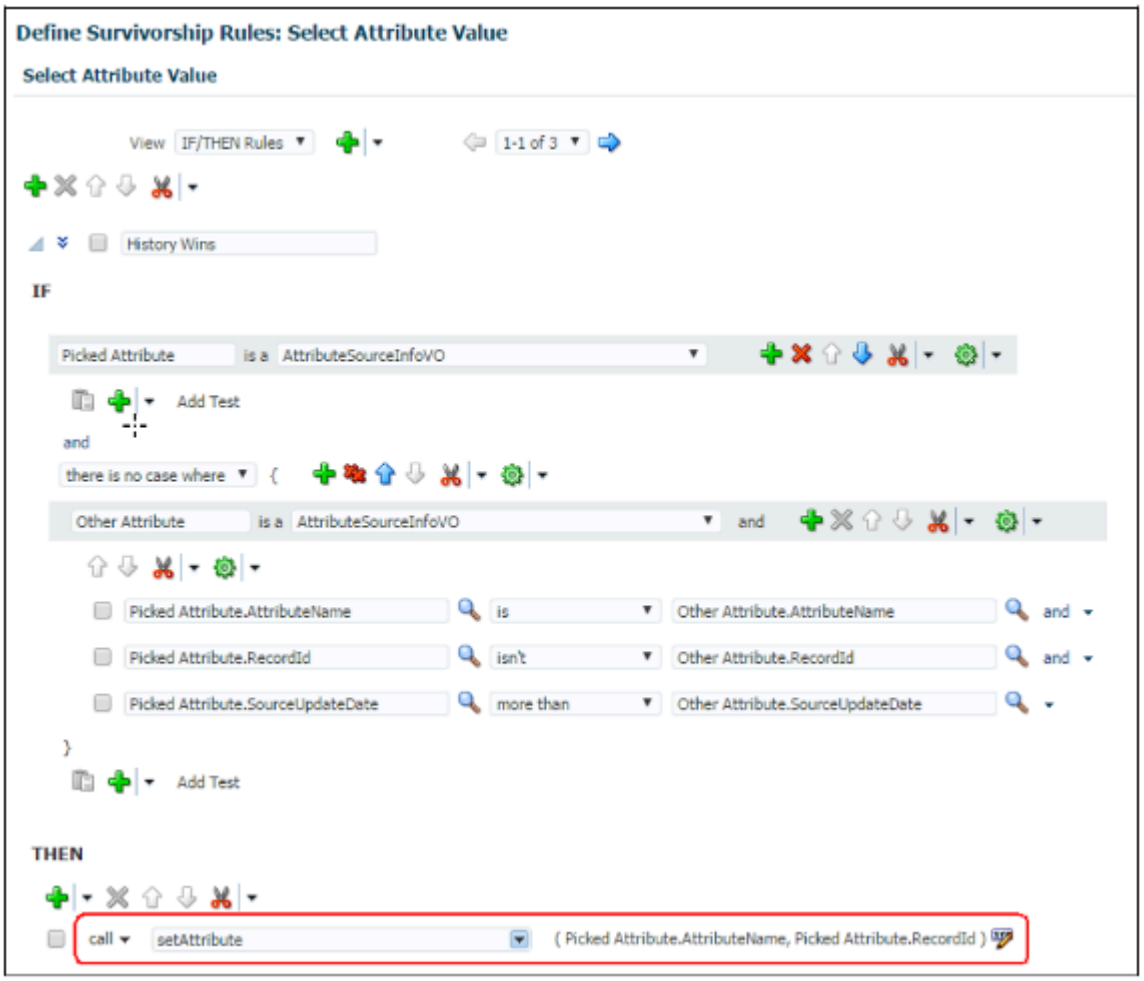
- The D-U-N-S number attribute value from the record with ID 1 is selected as master because the source information indicates that it has the earliest source update date.
- The Party Name attribute value from the record with the ID 3 is selected as master because the source information indicates that it has the earliest source update date.

Populate the Define Survivorship Rules: Select Attribute Values page with the IF and THEN rules condition values provided in the following table.

Rule Condition	Value
IF Condition	`IF picked attribute is a AttributeSourceInfoVO and there is no case where { Other Attribute == AttributeSourceInfoVO and there is no case where Other Attribute is a AttributeSourceInfoVO Picked Attribute.Attributename is OtherAttributename and PickedAttribute.RecordId isn't Other Attribute.recordId and Picked Attribute.SourceUpdateDate more than OtherAttribute.SourceUpdateDate}`
THEN Condition	`THEN call setAttribute (picked attribute.Attributename, Picked Attribute.RecordId)`

The following figure displays the Define Survivorship Rules: Select Attribute Values page with the IF and THEN rules conditions to create the set attribute value rule that selects the values with the earliest source update date as the surviving attribute value. The figure provides the following details. Name of the rule: History WinsIF condition: If picked attribute is a AttributeSourceInfoVO and there is no case where {Other Attribute is AttributeSourceInfoVO and Picked Attribute.AttributeName is Other Attribute.AttributeName and PickedAttribute.RecordId isn't Other Attribute.RecordId and Picked Attribute.SourceUpdateDate more than Other

Attribute.SourceUpdateDate}THEN condition: Then call setAttribute (Picked Attribute.AttributeName, Picked Attribute.RecordId)



How You Set the Value with the Highest Source System Confidence Level as the Surviving Attribute Value for D-U-N-S Number

This rule has a single condition to select the D-U-N-S number value with the highest source confidence level as the surviving attribute value for the D-U-N-S number attribute. The following is a use case for a set attribute rule to select the D-U-N-S number value with the highest source confidence level as the surviving attribute value:

Use Case

Party Record

The following table contains information for party records.

Record Name	Party ID	Party Name	D-U-N-S Number
Record 1	1	Oracle Corp	198837472
Record 2	2	Oracle USA Corp	489203901

Record Name	Party ID	Party Name	D-U-N-S Number
Record 3	3	Oracle	null

In this case, the party record contains three records with the attribute Party Name and two records with D-U-N-S number. These attributes are picked to create the source information. The source information table defined using the attributes from this party record table is as follows:

Source Information

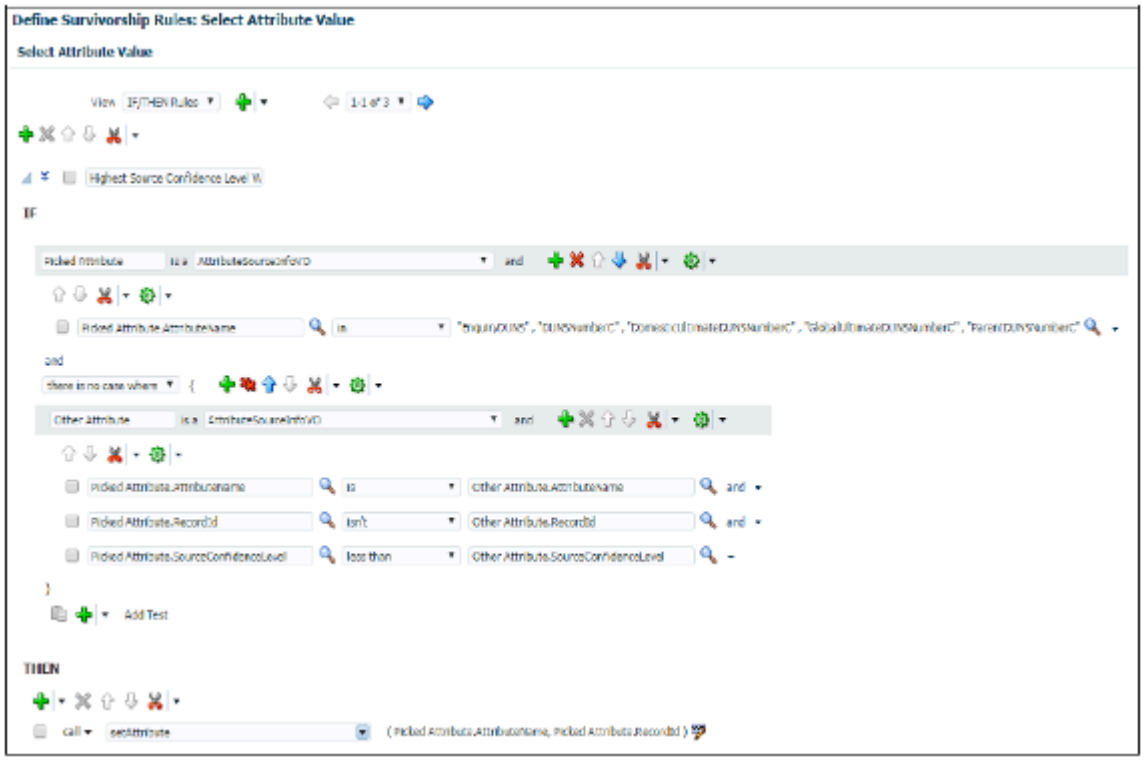
The following table contains information for source information records.

Record ID	Attribute Name	Source	Source Confidence Level	Source Update Date
1	Party Name	FUSION	95	1/5/2016
2	Party Name	FUSION	95	1/5/2010
3	Party Name	SIEBEL	90	1/5/2000
1	D-U-N-S Number	DNB	100	2/5/1990
2	D-U-N-S Number	FUSION	95	1/5/2016

In this case, the D-U-N-S attribute value for the record with ID 1 is selected as master because the source information indicates that it has the highest source confidence level among all records that have the D-U-N-S Number attribute.

The following figure displays Define Survivorship Rules: Select Attribute Values page with the IF and THEN rules condition values to set the attribute value with the highest source system confidence level as the master. The figure provides the following details.Name of the rule: Highest Source Confidence LevelIF condition: If picked attribute is a AttributeSourceInfoVO andPicked Attribute.ArrtibuteName is EnquireDUNSNumberC and there is no case where {Other Attribute is a AttributeSourceInfoVO and Picked Attribute.AttributeName is Other Attribute.AttributeName and Picked Attribute.RecordId isn't Other Attribute.RecordId and Picked Attribute.SourceConfidenceLevel is less than

OtherAttribute.SourceConfidenceLevel}THEN condition: Then call setAttribute (Picked attribute.AttributeName, Picked Attribute.RecordId)



How You Set the Values with the Earliest Incorporated Year as the Surviving Attribute Values

This rule has a single condition to select values with the earliest incorporated year as the surviving attribute values. The following is a use case for creating such a set attribute value rule:

Use Case 1

Party Record

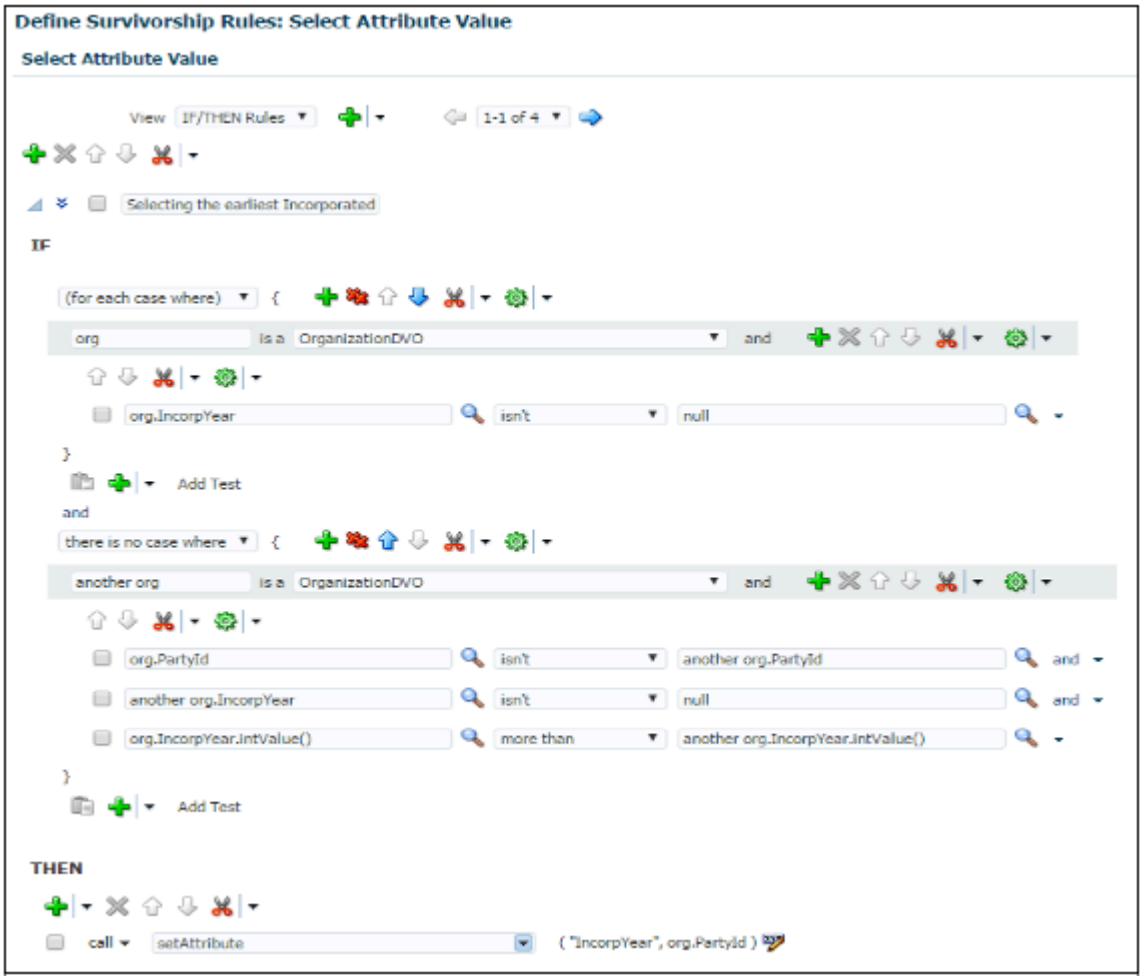
The following table contains information for party records.

Record Name	Party ID	Party Name	Incorporated Year
Record 1	1	Oracle Corp	1980
Record 2	2	Oracle USA Corp	1990
Record 3	3	Oracle	2000

In this case, the party record table contains three records with the attributes Party Name, Party ID, and Incorporated Year. The attribute values for the record with the earliest incorporated year are picked as master attribute values.

The following figure displays Define Survivorship Rules: Select Attribute Values page with the IF and THEN rules condition values to set the attribute with the earliest incorporated year as the master. The figure provides the following details.Name of the rule: Selecting the Earliest Incorporated YearIF condition: If for each case where org

is a OrganizationDVO and org.IncorpYear isn't null and there is no case where another org is a OrganizationDVO and org.PartyId isn't another org.PartyId and another org.IncorpYear isn't null and org.IncorpYear.intvalue() is more than another org.incorpyear.intValue()THEN condition: Then call setAttribute ("IncorpYear", org.PartyId)



How You Manage Agreement Rules

An agreement rule is a collection of patterns and conditions that are defined to determine whether a merge request should be vetoed by the application or not. Merge requests that violate these rules are either automatically rejected or end in error.

An example of an Agreement Rule is CUST_CONTACT_DIFF_RESOURCE_ORG_VETO, which prevents two partner-owned contacts belonging to different resource organizations from being merged.

You can create and edit Agreement Rules in the Setup and Maintenance work area by going to the following:

- Offering: Customer Data Management
- Functional Area: Customer Hub
- Task: Manage Agreement Rules

Agreement rules let you check a merge request for any veto conditions that can prevent a merge from occurring. These rules save resources and time by obviating the task of reviewing merge requests to prevent undesired merges from

being processed. Besides, agreement rules prompt you to consider alternative duplicate resolution mechanism such as linking. Note that Agreement Rules can't be set up in sandbox mode. Agreement rule can be of the following two types:

- Predefined: These are shipped out of the box with the application and are available in the predefined Agreement Rules Dictionary shipped with the application.
- User-defined: You can create your own Agreement Rules using the Manage Agreement Rules setup and maintenance task.

To know more about the two types of agreement rules see the Overview of Agreement Rules topic in the related links.

Related Topics

Define Agreement Rules

This example demonstrates how to create user-defined agreement rules that you can use to prevent a merge request from being processed.

Agreement rules are collections of patterns and conditions that are defined to determine whether a merge request should be vetoed by the application or not. Perform the following tasks to define agreement rules:

- Review and refresh terms in the predefined agreement rules dictionary shipped out of the box
- Add a new agreement rule

For more information on agreement rules, see *Oracle Fusion Middleware User's Guide for Oracle Business Rules* on Oracle Technology Network at http://www.oracle.com/technetwork.

Review and Refresh Terms in the Predefined Agreement Rules Dictionary

The Customer Hub application is shipped with a predefined agreement rules dictionary that contains all the predefined Agreement Rules shipped out of the box with the application. Before using this dictionary to define custom agreement rules, you must review whether the agreement rule terms and term attributes existing in the predefined agreement rules dictionary are sufficient to define custom agreement rules needed to meet your business requirements. If required, refresh terms to import the latest terms, term attributes, and related metadata, for example, fact types such as entities and objects. Refreshing the dictionary helps you pull in all the newly added custom attributes for accounts and contacts. Use the following steps to review and refresh the agreement rules dictionary:

1. In the Setup and Maintenance work area, go to the following:
    - Offering: Customer Data Management
    - Functional Area: Customer Hub
    - Task: Manage Agreement Rules
2. On the Manage Agreement Rules page, review whether the agreement rule terms and term attributes existing in the predefined agreement rules dictionary are sufficient to define custom agreement rules needed to meet your business requirements.
3. Click **Refresh Terms** to import the latest terms, term attributes, and related metadata.
4. Click **OK** in response to the confirmation message.

Add a New Agreement Rule

After reviewing and refreshing the Agreement Rules Dictionary using the earlier steps, perform the following steps to create a new custom agreement rule:

1. On the Manage Agreement Rules page, click **Next** to navigate to the Manage Agreement Rules: Define Rules page.
2. Click **Add** form the Actions menu to add a new rule.
3. Enter a rule name.
4. Click **Define Rule**.
5. Enter the reason for creating the agreement rule in the **Justification Reason**.
6. Click **Add** form the Actions menu to create a new pattern.
7. Complete the fields in the new pattern field using the sample information provided in the following table. Use the default values except where indicated. Note that the relation is always AND between patterns and can't be edited. You must include the Dictionary Terms OrganizationPartyVO and PersonPartyVO, with defined MergeType, into the Define Patterns column. These patterns determines the master and nonmaster records.

Pattern	Dictionary Term	Term Alias	Relation
for each case where	PersonPartyVO	Person	AND
for each case where	OrganizationPartyVO	NonmasterParty	AND
there is a case where	PartyUsageAssignmentVO	PartyUsageAssignment	AND

8. Navigate to the Conditions table.
9. Click **Add** from the Actions menu to add a new condition and complete the fields using the sample information provided in the following table. Use the default values except where indicated.

Term Attribute	Operator	Value	Relation
Person.PartyNumber	is not	1234	AND
NonmasterParty.MergeType	=	Nonmaster	AND
UsageAssignment.PartyUsag	=	HR_APPLICANT	AND

10. Click **Save** or **Save and Close**.
11. Click **Submit**.

Run the Request Dispatch Job

The Dispatch Job processes duplicate resolution requests in Pending or Submitted status. Run this process to manage and monitor resolution requests. Running the Dispatch Process You can run this job in two modes:

- On demand. Complete the following steps to run the job on an ad-hoc basis:
  a. Open the Run Request Dispatch Job task from the implementation project. Alternatively, in the Setup and Maintenance work area, go to the following:
     - Offering: Customer Data Management
     - Functional Area: Customer Hub
     - Task: Run Request Dispatch Job
  b. Click Submit and make a note of the Process ID.
- Per a specific schedule. Do the following steps to set up a recurring job:
  a. Open the Run Request Dispatch Job task from the implementation project. Alternatively, in the Setup and Maintenance work area, go to the following:
     - Offering: Customer Data Management
     - Functional Area: Customer Hub
     - Task: Run Request Dispatch Job
  b. Click Advanced on the Run Request Dispatch Job task.
  c. Click Schedule tab and select the Using a Schedule radio button.
  d. Select the frequency and start date that you want and click Submit and make a note of the Process ID.

Review the Status of the Process

To see the list of dispatch jobs, and their statuses:

1. Go to the Tools section on the Navigator.
2. Click the Scheduled Processes link under Tools.
3. Use the Process ID that you noted earlier to search and view the status of the Schedule Duplicate Resolution Requests process.

High Volume Batch Deduplication

Batch deduplication of account or contact records in Oracle Customer Data Management Cloud Service by duplicate identification or resolution.

Batch deduplication consists of the following two steps:

- Duplicate Identification: This step includes the identification of duplicate records by submitting a Duplicate Identification Batch job.

  You can define and submit this job from the Duplicate Identification page.

- Duplicate Resolution: This step includes the resolution of the duplicates, typically by merging each set of duplicate records.

  You can resolve the duplicates either automatically by submitting the Duplicate Identification Batch job (called Automerge) or manually by submitting records in bulk from the Duplicate Identification Batch results review page.

For more details on these steps and for configuration of Automerge, see Merge Requests, Implementing Customer Data Management.

Both of these jobs are data-intensive operations that can read or update millions of rows of data in various Oracle Application Cloud tables. This document is intended to provide the guidelines and best practices for planning the data-sets, and applying appropriate configurations to achieve optimal throughput for high volume deduplication in Oracle Customer Data Management Cloud Service. Each customer's data set is unique. The time required to process a duplicate identification batch varies on the data shape.

Best Practices for High Volume Batch Deduplication

Customer Data Management merge is a data-intensive process that scans and updates a large number of tables in Oracle Applications Cloud, to correctly merge two or more Accounts or Contacts.

This section describes how you can use the following profile options to optimize the merge process:

- **Scope of Merge Process** (ORA_ZCH_MERGE_SCOPE): You can use this profile option to define the scope of the merge process.
- **Master Record Selection Method** (ORA_ZCH_SETMASTER): You can use this profile option to specify the method for selecting the master record in a merge request.
- **Create Automerge with Review** (ORA_ZCH_AUTOMERGE_REVIEW): You can use the profile option to select an appropriate processing option for Automerge.
- **Maximum Number of Concurrent Merge Jobs** (ORA_ZCH_MERGE_MAX_REQUEST_LIMIT): Specify the maximum number of merge jobs to be processed at a time. If you don't set the maximum limit, all merge jobs are submitted for concurrent processing.

You can set these profile options in the Setup and Maintenance work area using the following:

- Offering: Customer Data Management
- Functional Area: Customer Hub
- Task: Manage Customer Hub Profile Options

How You Define the Scope of the Merge Process

When you merge two or more records, the application scans hundreds of transactional and reference tables across all modules in the Oracle Applications Cloud such as, Core Customer Data Management, CRM, Financials, and Manufacturing. This can make merge a data-intensive and time consuming process. However, you can use the Scope of Merge Process (ORA_ZCH_MERGE_SCOPE) profile option to define and limit the scope of merge process in an implementation so that the application scans only the necessary business areas. This optimizes the size of the merge memory and execution profile.

The following options are supported by the Scope of Merge Process profile option:

- All Functional Areas (ALL): This is the default option and scans across all areas of Oracle Applications Cloud. You use this option when there's a global implementation running various modules of Oracle Applications Cloud such as, Core Customer Data Management, CRM, Financials, and Manufacturing.
- All Customer Relationship Management Related Areas (CRM): This option limits the scope of the process to handle all the CRM entities such as, Opportunities, and Leads, core Customer Data, Common Entities such as, Notes, and Activities, and Custom Objects. You use this option when there's a CRM implementation along with the use of Customer Data Management functionality.
- Customer Data Management Specific Areas: This option limits the scope of the process to core Customer Data, Common Entities such as Notes and Activities, and Custom Objects. You use this option during the initial customer data consolidation and to achieve best performance for Customer Data management, implementations.

Note: The profile option settings can be changed at any time, if additional modules are turned on the instance. For instance, the Customer Data Management option might be used during initial consolidation and cleanup of customer data and then changed to CRM or ALL options if other modules are implemented later.

How You Define the Master Record Selection Method

The performance of the merge process also depends on the method used to select the master record. You can use the Master Record Selection Method (ORA_ZCH_SETMASTER) profile option to specify an appropriate option for selecting the master party automatically during merge. The following options are supported by the Master Record Selection Method profile option:

- Select master record using survivorship rule (RULE): This is set as the default master selection option. This option selects the master record based on the Set Master rules defined in the Manage Survivorship task. These rules are applied using the Oracle Business Rules component. You use this option when there are complex business rules required to pick the master.
- Select the oldest record as master (OLDEST): This option selects the party with the earliest creation date as the master.
- Select the newest record as master (NEWEST): This option selects the party with the newest creation date as the master.
- Select master based on duplicate identification results (ANY) - This option randomly selects one of the parties in the set as a master.

How you Configure Automerge Action

Automerge is the process of automatically merging identified duplicate sets that exceed the automerge threshold. The process is initiated by creating a duplicate identification batch with the Create Merge Request option. You can use the Create Automerge with Review (ORA_ZCH_AUTOMERGE_REVIEW) profile option that has Yes and No values to select an appropriate processing option for Automerge:

- Create merge requests only for duplicate sets exceeding the automerge threshold: To enable this processing option, select No as the value for the Create Automerge with Review (ORA_ZCH_AUTOMERGE_REVIEW) profile option. If you select this option, the application processes duplicate sets as follows:
    - The application preprocesses the duplicate sets exceeding the automerge threshold and merges them into a single job. This option is ideal for processing high volumes of merge requests when the duplicate sets require no review or any further action.

- Duplicate sets not exceeding the automerge threshold remain in Not Reviewed status in the Duplicate Identification page, from where they can be manually converted to merge requests, or rejected, if needed.

- Create Merge Requests for all duplicate sets: To enable this processing option, select Yes as the value for the Create Automerge with Review (ORA_ZCH_AUTOMERGE_REVIEW) profile option. If you select this option, merge requests are created for all duplicate sets. All requests are first pre-processed. Then they're either merged (if they exceed the automerge threshold), or put in "New" status (so that they can be reviewed) if they don't exceed automerge threshold.

How you Control the Concurrency of Merge Processes

Each merge request executes as a single batch process in the Enterprise Service Scheduler (ESS). The number of merge requests executing concurrently is limited by the number of batches being concurrently processed. Therefore, if there are other ESS processes competing for threads when there are a large number of merge requests queued up, then the scheduling of those jobs could get delayed.

During initial consolidation of customer data, it's advantageous to use the maximum available threads. However, in steady state when there are other processes running in the background, it may be necessary to limit and control the number of concurrent merge ESS jobs.

To achieve this, set the following profile option to an appropriate value:

- **Profile Option Name**: Maximum Number of Concurrent Merge Jobs
- **Profile Option Code**: ORA_ZCH_MERGE_MAX_REQUEST_LIMIT

  - When the profile option value is left blank or when no value is defined, the ESS will allocate merge requests according to the threads available. This is recommended during initial high volume data processing.
  - After initial data load, set the profile option value to ten or lower if other processes such as Web services or other ESS jobs are running.

How You Purge Duplicate Resolution Data

Legacy duplicate resolution data, such as resolution logs and legacy duplicate resolution batches and requests can clutter the duplicate resolution work area and affect the performance of the application.

Use the Purge Duplicate Resolution Data scheduled process to purge the duplicate resolution data, such as resolution logs and to delete duplicate resolution batches and requests. You can schedule this process from the Scheduled Processes work area. You can navigate to this work area as follows:**Navigator** > **Tools** > **Scheduled Processes** .

This scheduled process lets you purge duplicate resolution data based on status and date range. You can specify the status of the duplicate resolution requests to be purged, such as duplicate resolution requests in Completed, Error, Pending, New, or Rejected status. You can also specify a date range by specifying the start and an end date to select duplicate resolution requests to be purged. For more information, see: Submitting Scheduled Processes and Process Sets: Procedure

Related Topics

- Submit Scheduled Processes and Process Sets
- Process Sets
- View Status and Other Details for Scheduled Processes

13 Configure Automerge

Overview of Automerge Setup

The automerge functionality merges duplicate records without any approval or intervention from the data steward. Automatic processing of merge requests is critical when processing large volumes of customer data because automerge can expedite the resolution of duplicate records without manual review.

Note that during automerge, the child entities of the duplicate records, such as contact points, relationships, classifications, and cross references, become the child entities of the master record.

Enabling Automerge involves several implementation steps that you have probably already completed while setting up duplicate identification and duplicate resolution. However, review the following list to ensure these setups are indeed complete.

You can enable automerge by configuring the tasks listed in the following table in the Setup and Maintenance work area:

Step	Description	Task Name	Where to Get More Details
Manage Customer Hub Profile Options	Set up the following profile options appropriately: • Auto Merge Threshold (ZCH_AUTO_MERGE_THRESHOLD) • Record Size Limit of Duplicate Set (ZCH_DI_MERGEREQ_REC_SIZE) • Survivorship Enabled (ZCH_ENABLE_SURVIVORSHIP)	Manage Customer Hub Profile Options	See the following topics in the Configure Profile Options chapter of the Getting Started with Your Customer Data Management Implementation guide: • Key Customer Data Management Profile Options • Manage Customer Hub Profile Options • How You Setup Duplicate Resolution Simplified Profile Options
Define Survivorship	Survivorship rules determine the master or surviving record and its attributes during the merge operations for duplicate resolution. Enable survivorship rules by setting the ZCH_ENABLE_SURVIVORSHIP profile option to Yes.	• Manage Survivorship Rules • Manage Customer Hub Profile Options	See the following topics in the Configure Duplicate Resolution chapter of the Getting Started with Your Customer Data Management Implementation guide: • How You Enable and Manage Survivorship Rules • Define Survivorship Rules • Define Set Master Record Rules • Define Set Attribute Value Rules
Manage Server Configuration	Enable the EDQ Real-time and Batch Match Server configuration. Ensure that the Server Parameter	Manage Server Configuration	See the following topic in chapter Configure Duplicate Identification of the Getting Started with Your

Step	Description	Task Name	Where to Get More Details
	Values (Server Address and Server Port) are complete.		Customer Data Management Implementation guide: • Enable the Server Configuration for Matching
Manage Enterprise Data Quality Matching Configuration	Create an active Match Configuration in Manage Enterprise Data Quality Matching Configurations task or use a predefined Match Configuration. Rebuild the keys if necessary.	Manage Enterprise Data Quality Matching Configurations	See the following topic in chapter Configure Duplicate Identification of the Getting Started with Your Customer Data Management Implementation guide: Manage Enterprise Data Quality Matching Configurations
Create a duplicate identification batch with the appropriate processing option	Create a duplicate identification batch and select Create Merge Request as the Automatic Processing Option.	N/A	See the following topic in the Identify Duplicates chapter of the Using Customer Data Management guide: Create Duplicate Identification Batches and Define Subset Rules

How Records are Selected for Automerge

Records are selected for automerge based on the following criteria:

- Score threshold: The score threshold is defined in the Match Configuration and determines whether a record is included in a duplicate set or not.
- Automerge threshold: The automerge threshold is defined by the ZCH_AUTO_MERGE_THRESHOLD profile option and determines whether the merge request for a duplicate set is processed automatically or if it must be reviewed manually.

The three possible outcomes for each record with regard to duplicate identification and merging are as follows:

- Low score below score threshold: The record isn't included in duplicate set and in the merge request for that duplicate set.
- Medium score above score threshold and below automerge threshold: The record is included in duplicate set but merge request for that duplicate set must be reviewed manually.
- High score above score threshold and above automerge threshold: The record is included in duplicate set and merge request is processed automatically.

The score for all the records in a duplicate set must be above the automerge threshold for automated processing. If one record in the duplicate set is below automerge threshold, and the other records are above the automerge threshold, the merge request must be reviewed manually.

Note: When you merge two or more records with exactly same children information under phone, email, or address the children information is merged and rolled up as one record.

Implement Automerge

Automatic processing of merge requests is critical when processing large volumes of customer data.

Automerge can expedite the resolution of duplicate records without any manual review or approval from the data steward.

How You Enable Automerge

You can enable Automerge by completing the following implementation tasks in the Setup and Maintenance work area:

- Manage Customer Hub Profile Options: Navigate to this task either from the implementation project or through the Setup and Maintenance work area as follows: Offering: Customer Data Management > Functional Area: Customer Hub > Task: Manage Customer Hub Profile Options. Perform the following implementation steps:
    - Set Auto Merge Threshold profile option (ZCH_AUTO_MERGE_THRESHOLD) to the required value. This profile option specifies the threshold for auto merge. Merge requests with lower scores need data steward's review. An exact match is 100.
    - Review the Record Size Limit of Duplicate Set (ZCH_DI_MERGEREQ_REC_SIZE). This profile option determines the maximum number of records in the duplicate set that can be merged automatically. By default, the value is set to 10 records.
    - Set the Survivorship Enabled profile option (ZCH_ENABLE_SURVIVORSHIP) to Yes. This profile option enables the survivorship rules to select the master record and retain the attributes during a merge or update operation.
- Manage Survivorship Rules: Navigate to this task either from the implementation project or through the Setup and Maintenance work area as follows: Offering: Customer Data Management> Functional Area: Customer Hub > Task: Manage Survivorship Rules. Create Set Master survivorship rules or activate the predefined survivorship rules, base on your business requirements. Set Master survivorship rules are used to choose the master record for merge requests created from the duplicate identification batch.

  If there are no active Set Master rules or if the Set Master rules did not trigger, then the merge request must be reviewed manually. Even if the ZCH_AUTO_MERGE_THRESHOLD profile option is set, the score for all records is above the threshold value, and the number of records is below the record size limit you must activate Set Master rules to complete the automerge without manual review.

  > **Note:** You can use the Set Attribute rules with Set Master rules to determine the Golden Master record. For automerge, Set Master rule is required.

- Define Data Quality: Perform the following implementation steps:
    - Enable EDQ Real Time and Batch Basic Match Server in Manage Server Configurations task. Navigate to this task either from the implementation project or through the Setup and Maintenance work area as follows: Offering: Customer Data Management > Functional Area: Data Quality Foundation > Task: Manage Server Configurations.
    - Create an active Match Configuration in Manage Enterprise Data Quality Matching Configurations task or use a predefined Match Configuration. Rebuild the keys if necessary. Navigate to this task either from the implementation project or through the Setup and Maintenance work area as follows: Offering: Customer

Data Management > Functional Area: Data Quality Foundation > Task: Manage Enterprise Data Quality Matching Configurations.

Run Automerge

Running automerge involves the following two tasks:

1. Create a duplicate identification batch and select Create Merge Request as the Automatic Processing Option.
2. Run the task Run Request Dispatch Job from the Setup and Maintenance work area as follows to disposition the duplicate resolution sets.

The Run Request Dispatch Job processes all resolution requests in Pending or Submitted status. You can run this job in two modes:

- On demand. Complete the following steps to run the job on an ad-hoc basis:
    a. Open the Run Request Dispatch Job task from the implementation project. Alternatively, in the Setup and Maintenance work area, go to the following:
        - Offering: Customer Data Management
        - Functional Area: Customer Hub
        - Task: Run Request Dispatch Job
    b. Click Submit and make a note of the Process ID.
- Per a specific schedule: You can set up a recurring job when you:
    a. Open the Run Request Dispatch Job task from the implementation project. Alternatively, in the Setup and Maintenance work area, go to the following:
        - Offering: Customer Data Management
        - Functional Area: Customer Hub
        - Task: Run Request Dispatch Job
    b. Click Advanced.
    c. Click Schedule tab and select the Using a Schedule radio button.
    d. Select the required frequency and start date and click Submit and make a note of the Process ID.

To see the list of dispatch jobs, and their statuses:

1. Go to the Tools section on the Navigator
2. Click the Scheduled Processes link under Tools.
3. Use the Process ID that you noted earlier to search and view the status of the Schedule Duplicate Resolution Requests process.

Troubleshoot Automerge Issues

After you create your Duplicate Identification Batch, drill down into the completed batch to see the results. If duplicate sets have been found, and automerge is enabled, resolution requests are automatically submitted for merging.

If the resolution request wasn't submitted automatically, you can drill down to the duplicate set and compare the score for each record with the threshold in the ZCH_AUTO_MERGE_THRESHOLD profile option and the number of records with the limit in the ZCH_DI_MERGEREQ_REC_SIZE profile option. If all scores are above the threshold and the number of records is below the limit, verify that Set Master rules are active. These rules trigger you to choose a master for the

records in the duplicate set. One last thing that you would have to check is that the ZCH_ENABLE_SURVIVORSHIP is set to yes.

14 Integrate Customer Data Management with Other Cloud Services

Customer Data Management Integration Approaches

You can integrate the Customer Data Management functionality of Oracle CX Sales and Fusion Service with other cloud services using REST APIs and SOAP APIs to provide address cleansing, duplicate identification, and duplicate resolution capabilities.

Alternatively you can use the Integration Cloud Service to develop work flows to integrate Customer Data Management with other cloud based or on-premise applications.

Customer Data Management Integration Using REST APIs

The Oracle Customer Data Management functionality of Oracle CX Sales and Fusion Service provides multiple public REST APIs that can be used to access data stored in the Customer Data Management database and construct integrations to other systems. The APIs include resources to Get, Post (create), Patch (update), and Delete organizations (accounts) and persons (contacts). Also there are resources to identify and create resolution request for duplicate parties.

For more information on public REST APIs, see REST API for CX Sales and Fusion Service.

Customer Data Management Integration Using SOAP APIs

The Customer Data Management functionality of Oracle CX Sales and Fusion Service provides SOAP services to create and update organizations (accounts) and persons (contacts). You can also use these services to identify and resolve duplicate parties.

For more information on SOAP APIs, see Oracle CX SOAP Web Services for CX Sales and Fusion Service.

Customer Data Management Integration with Import and Export

You can use Import and Export Management, and Data Import to import and export application data using text or XML files into and out of the Customer Data Management registry.

You can also import attachments using Import and Export Management. Note that the imported attachments aren't visible in Customer Data Management if you used the Account or the Contact import objects but can be viewed in Customer Center. To import attachments in Customer Data Management, using Import and Export Management you must use the Organization and Person import objects. For more information about importing attachments, see the Related Topics section.

You can also use import to create or update records in the Customer Data Management registry.

Customer Data Management Integration Using the Integration Cloud Service

You can use the Integration Cloud Service to leverage predefined integrations between Customer Data Management, other cloud services, and on premise applications. For example, you can integrate Oracle Service Cloud with Customer

Data Management to provide the duplicate resolution capability. Using this capability, you can merge an Oracle Sales and Fusion Service account (organization) or contact (person) with an Oracle B2C Service account (organization) or contact (person).

For more information on the Integration Cloud Service, see Oracle Integration Cloud Service in the Related Topics section.

Customer Data Management Integrations for Accounts (Organization) and Contacts (Persons)

The following table shows the possible integrations options for Oracle Customer Data Management. The table also lists the available REST and SOAP web services that you can use to perform the different Customer Data Management processes.

Customer Data Management Process (Batch Job)	REST Service	Data Import (for account Receivables only)	Data Import	Data Export	ICS Events	Comments
Address Cleansing	Address Cleansing is available by the REST service from Oracle Address, Email, and Phone Verification only.	No	No	Yes (Batch Summary only). Doesn't include child object such as duplicate address and relationships.	No	None
Duplicate Identification	Yes. The 'accounts', 'contacts', 'hubOrganizations', and 'hubPersons' REST resources all support the findDuplicates action for API-based real-time duplicate identification.	No	No	Yes (Batch Summary only). Doesn't include child object such as duplicate address and relationships.	No	None
Duplicate Resolution and Merging	Yes. The `crmRestApi/resources/latest/resolutionReque` REST service can create new resolution request and query existing resolution requests but can't update the existing requests.	No	No	Yes. The Resolution Details object which is a child of the resolution request header export object. The resolution details object provides the full details for child objects in the merge scope.	Yes. Public Resolution Request Updated.	None
Data Enrichment	Data enrichment is available by REST service from Oracle Account	No	No	Yes	No	None

Customer Data Management Process (Batch Job)	REST Service	Data Import (for account Receivables only)	Data Import	Data Export	ICS Events	Comments
	and Contact Enrichment by Dun & Bradstreet (D&B) only.					
Non-Duplicate	`crmRestApi/resources/latest/nonDuplicates`	N/A	Yes	Yes	N/A	None
Resolution Link	`crmRestApi/resources/latest/resolutionLinks`	N/A	Yes	Yes	N/A	None

Related Topics

- How do I import attachments?
- Oracle Integration Cloud Service
- Import Your Resolution Link Data
- Import Your Nonduplicate Data

Merge Operation Process During Integration Cloud Service Based Integration

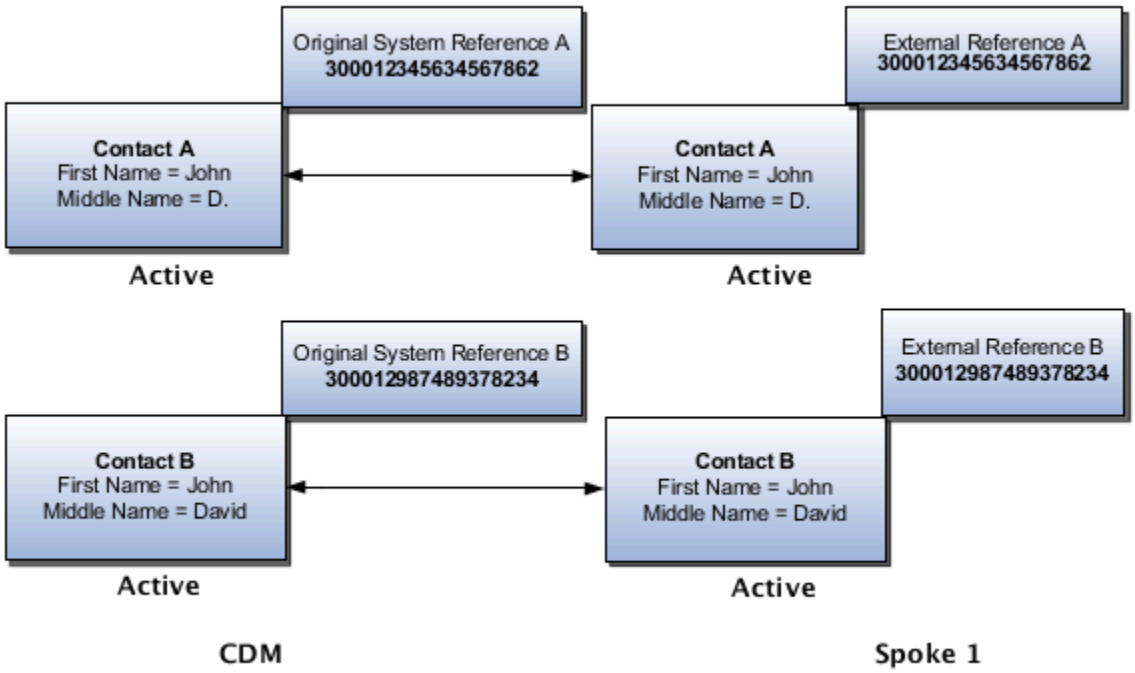
The Customer Data Management functionality of Oracle CX Sales and Fusion Service acts as the customer master during Integration Cloud Service based integration between different cloud services (also known as spoke systems).

You can use Customer Data Management to cleanse, consolidate, and share customer data across integrated cloud services. This topic explains how the duplicate resolution capability of the Customer Data Management functionality merges records across integrated cloud services, for example, how it merges an Oracle CX Sales and Fusion Service account or contact with an Oracle Service Cloud account or contact.

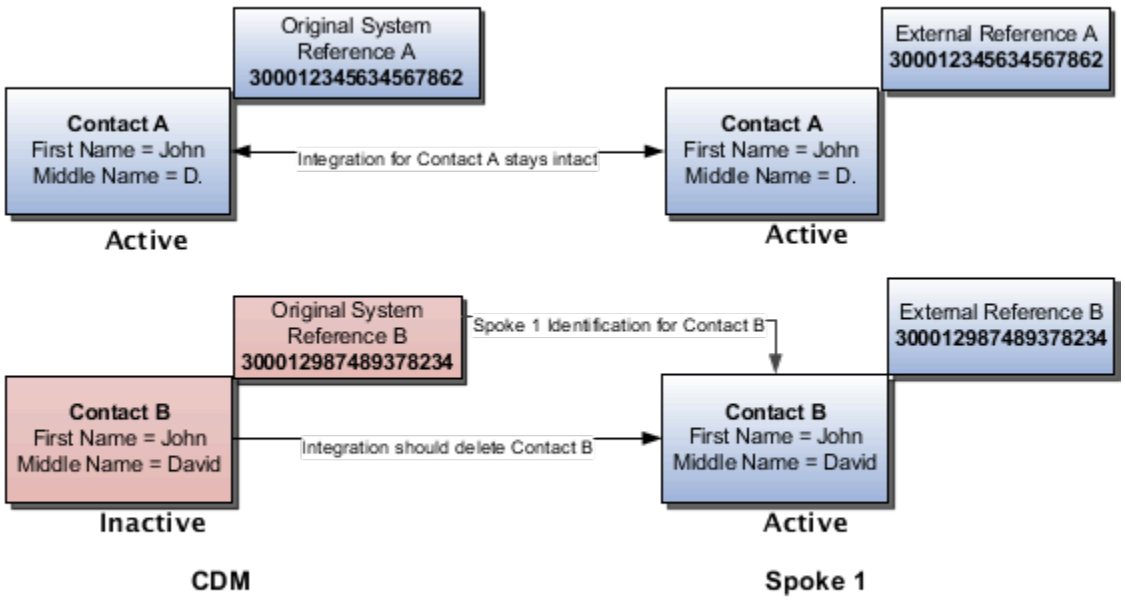
Merge Operation Process for Point to Point Integration

In this integration scenario, Customer Data Management provides the duplicate resolution capability to a single spoke system.

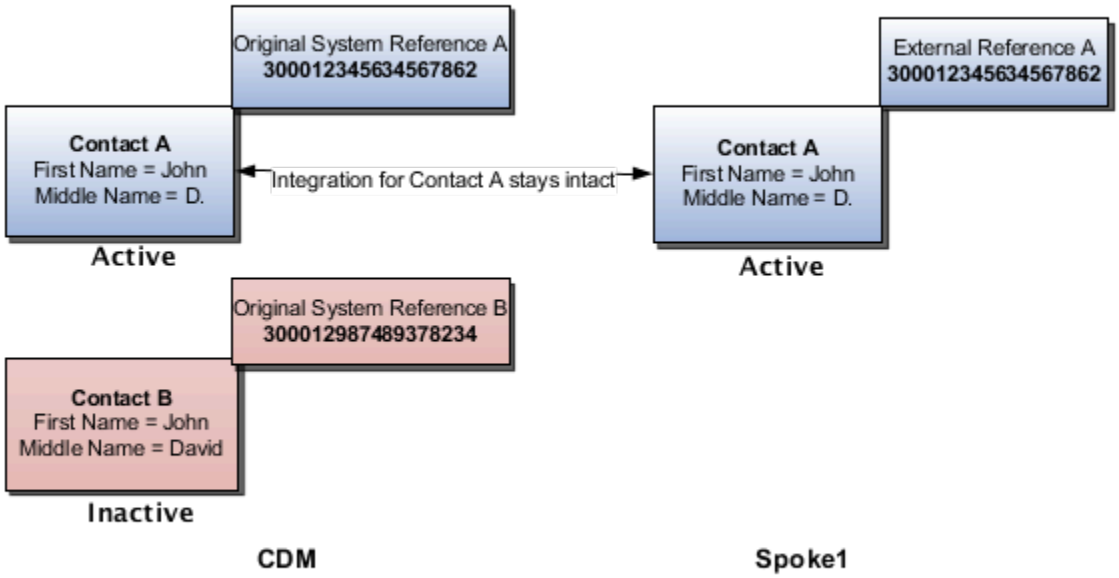
The following diagram shows the before merge status of two contacts, Contact A and Contact B, of an account from Spoke 1.



The following diagram illustrates how the two contacts, A and B, of the account from Spoke 1 are being merged in CDM and how the Contact A emerges as the master and the Contact B becomes the non-master.



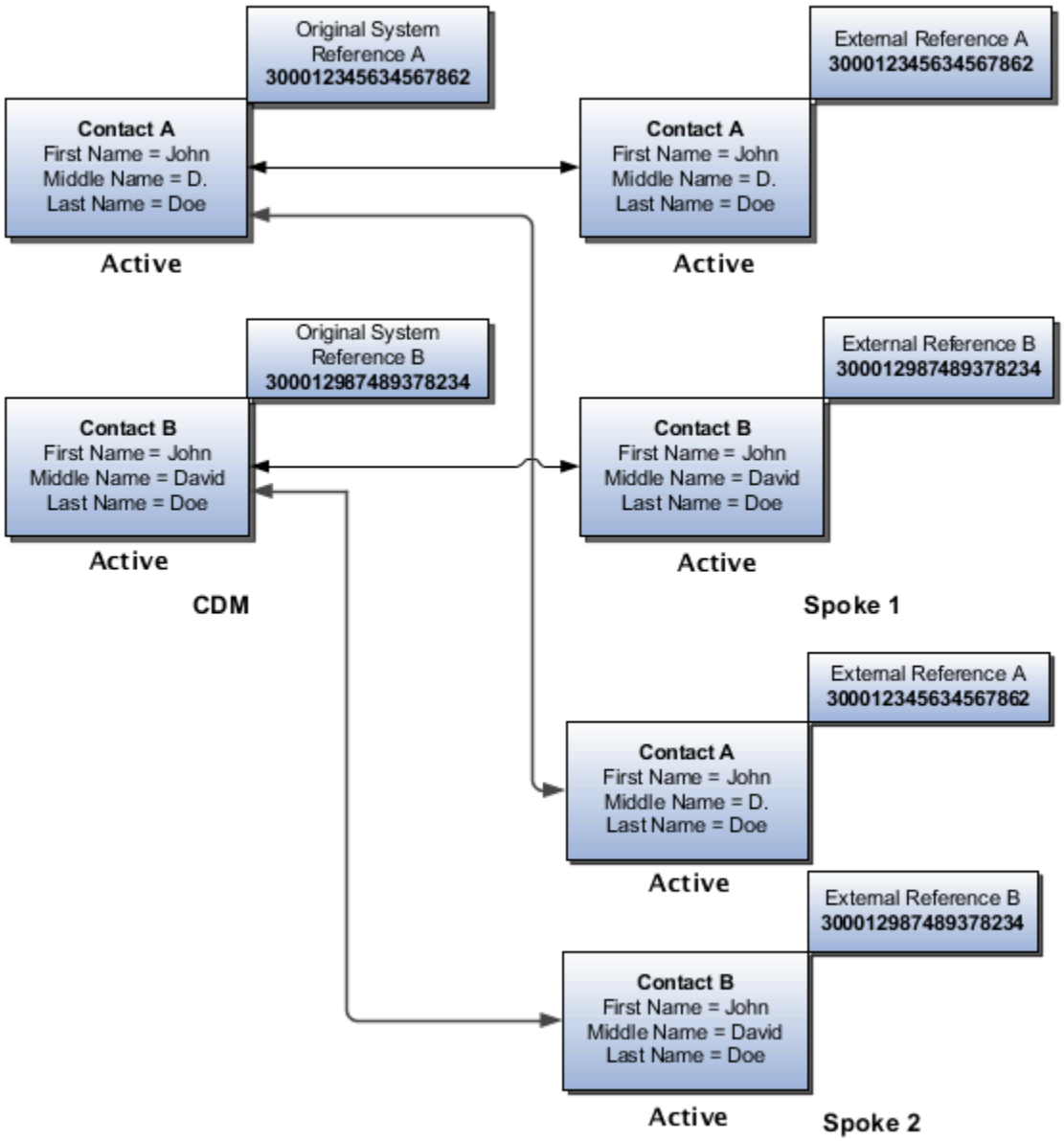
The following diagram shows the after merge status of two contacts, A and B, of the account. Note that in Spoke 1 only Contact A has survived and remained active after the merge.



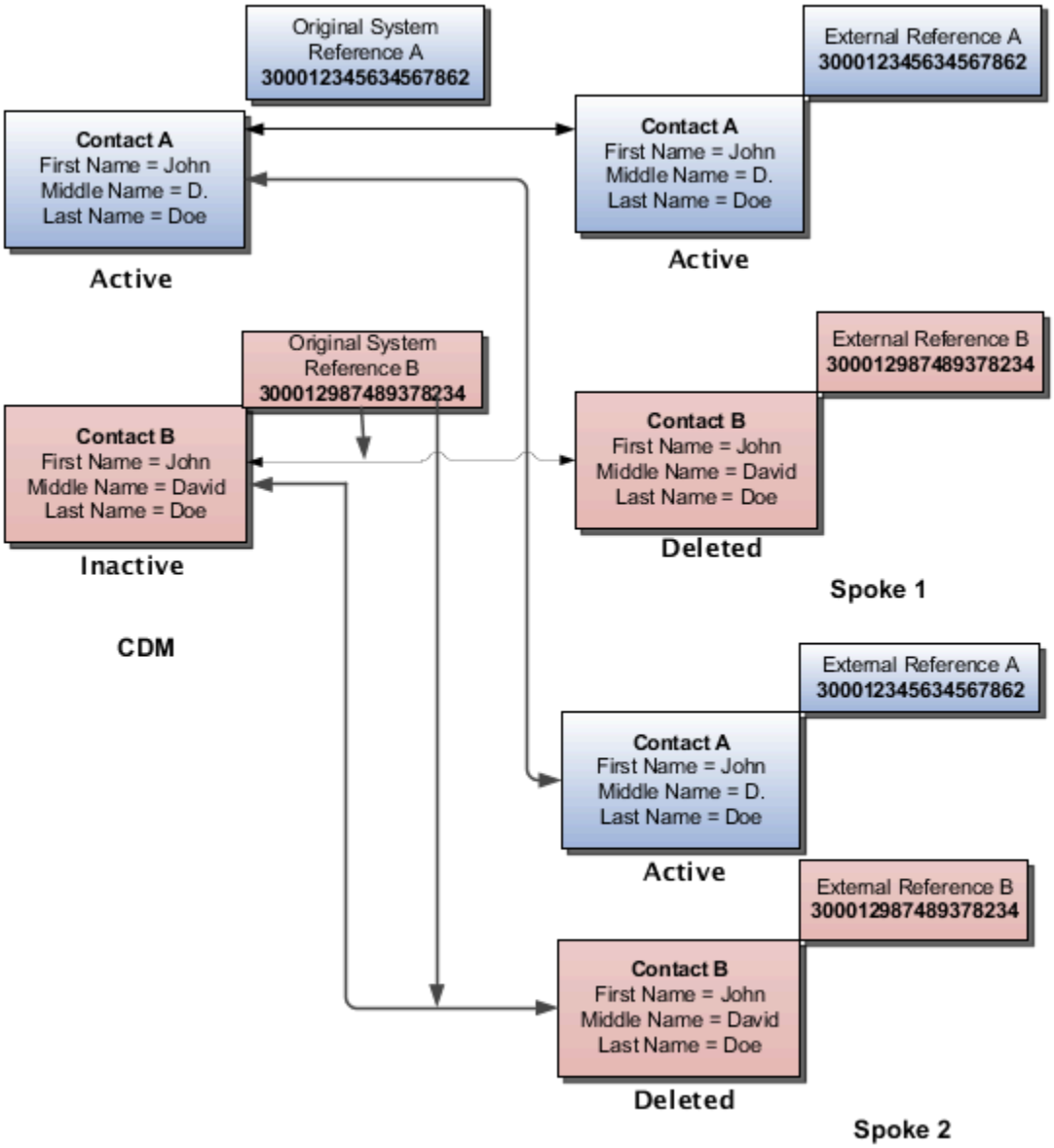
Merge Operation Process for Publish and Subscribe Integration

In this integration scenario, Customer Data Management provides the duplicate resolution capability to two or more integrated cloud services or spoke systems. Duplicate data from spoke systems is consolidated in CDM and the mastered data is published to the subscribing spoke systems.

The following diagram shows the before merge status of two contacts, A and B, of an account that exists both in Spoke 1 and Spoke 2.



The following diagram shows the after merge status of two contacts, A and B, of the account.



Take note of the following:

- Data about Contacts A and B comes in Customer Data Management registry from both the spoke systems.
- The merge is taking place in Customer Data Management registry and any owned objects by the non-masters are moved (re-parented) to master record in CDM.
- The mastered data is published to both the spoke systems and, consequently, Contact B is deleted from both the spoke systems.
- When performing merge across different cloud services using ICS based integration, you should explicitly publish to merge events and not rely on account, contact, and household composite events. You can publish merge events by implementing the Resolution Request Updated business event in ICS.