Oracle Fusion Service

How do I enable Digital Customer Service?

Oracle Fusion Service
How do I enable Digital Customer Service?

F89596-04

Author: David Yetter

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

Use help icons ⓘ to access help in the application. 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.

Get Support

You can get support at *My Oracle Support*. For accessible support, visit *Oracle Accessibility Learning and Support*.

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.

Learn About Accessibility

For information about Oracle's commitment to accessibility, visit the *Oracle Accessibility Program*. Videos included in this guide are provided as a media alternative for text-based topics also available in this guide.

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 Get Digital Customer Service Up and Running

Implementation Summary

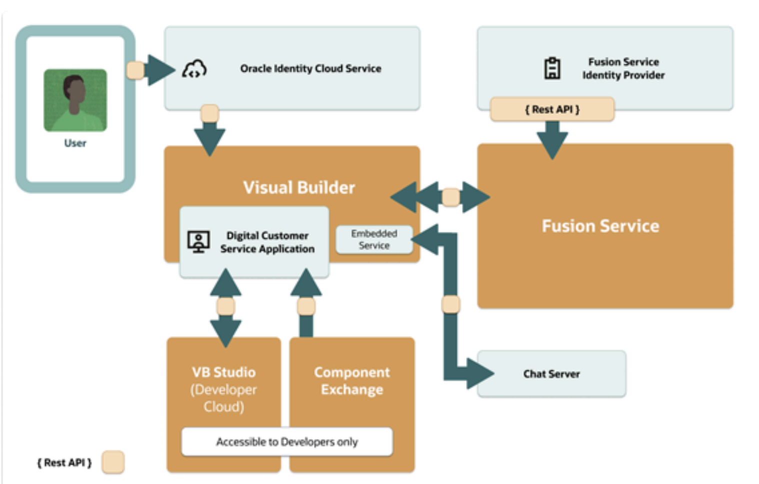
Before you start your Digital Customer Service implementation

Before starting with your implementation you must have subscribed to the service and received an email with the initial sign-on information.

Implementation overview

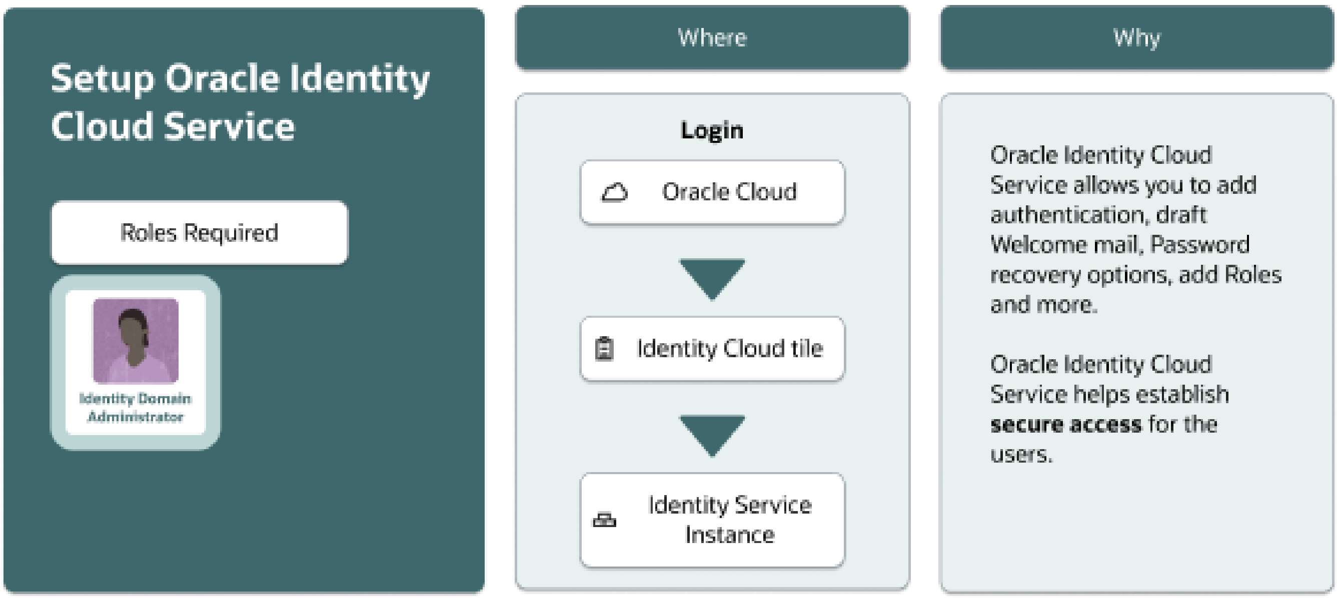
Use Digital Customer Service to provide your customer account users with a self-service web interface where they can access their service requests along with relevant knowledge articles.

With a configurable user interface and Oracle Visual Builder integration, you can create a user interface to reflect your company brand, and depending on your business needs, you can use Visual Builder to define root pages and styles. You can also implement Embedded Service, a syndicated widget, which provides users with multifunctional help at a point of need, where you can implement modular components such as Search Knowledge, Popular Articles, Live Chat, and others. For more information on implementing Embedded Service, see the Embedded Service playbook "How do I implement Embedded Service?"

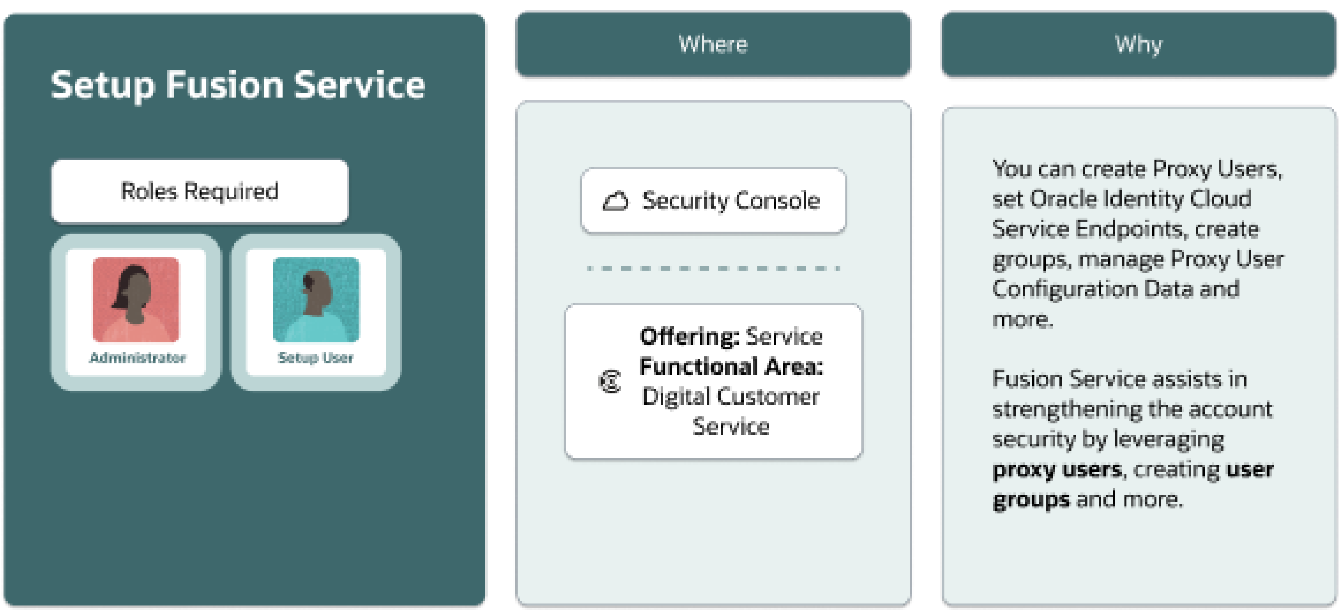


Use this playbook to get Digital Customer Service up and running. Here's a high level overview of what you need to do to get started:

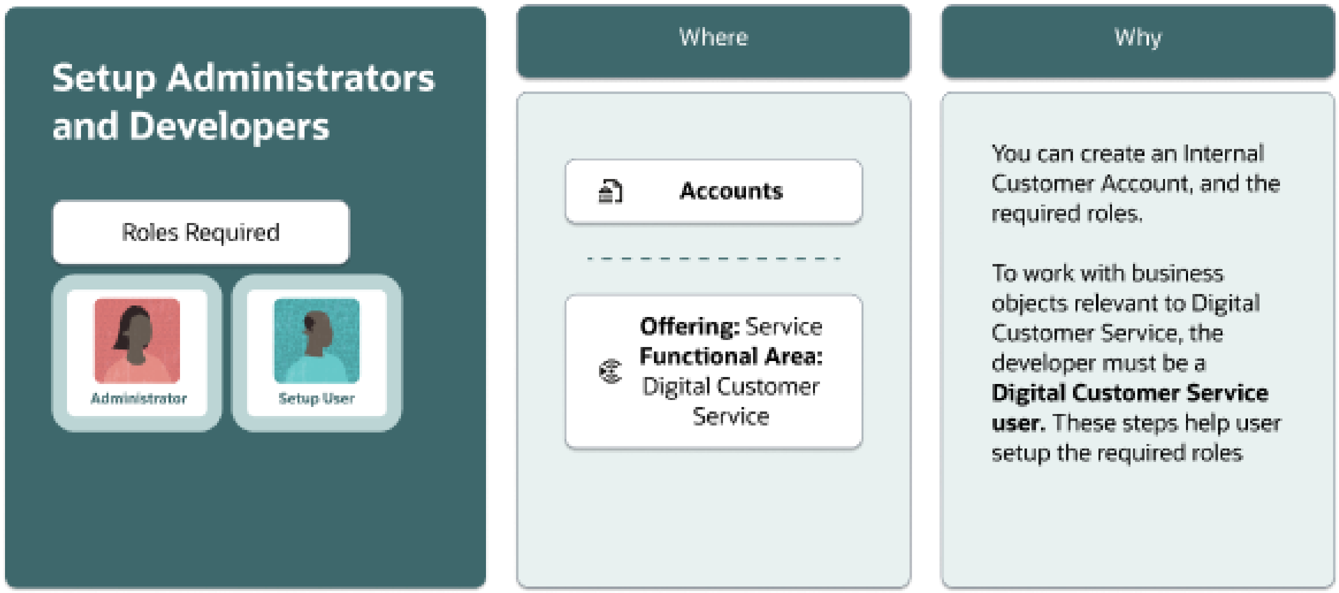
- **Set Up Oracle Identity Cloud Service**



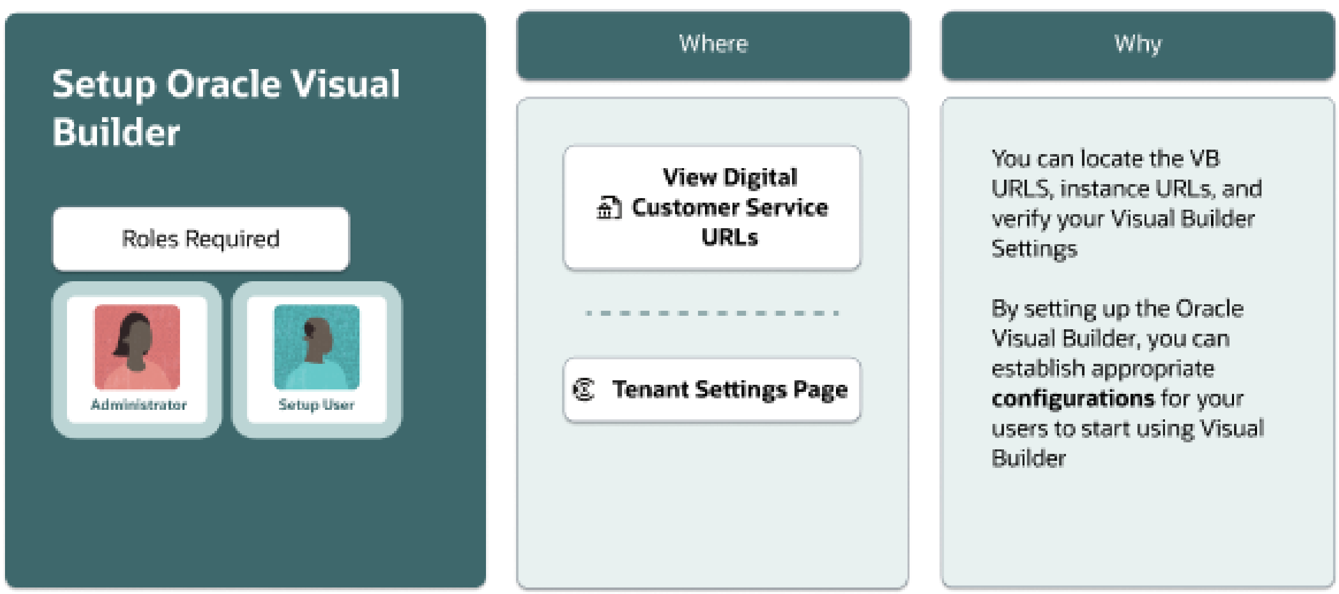
- **Set up Fusion Service**



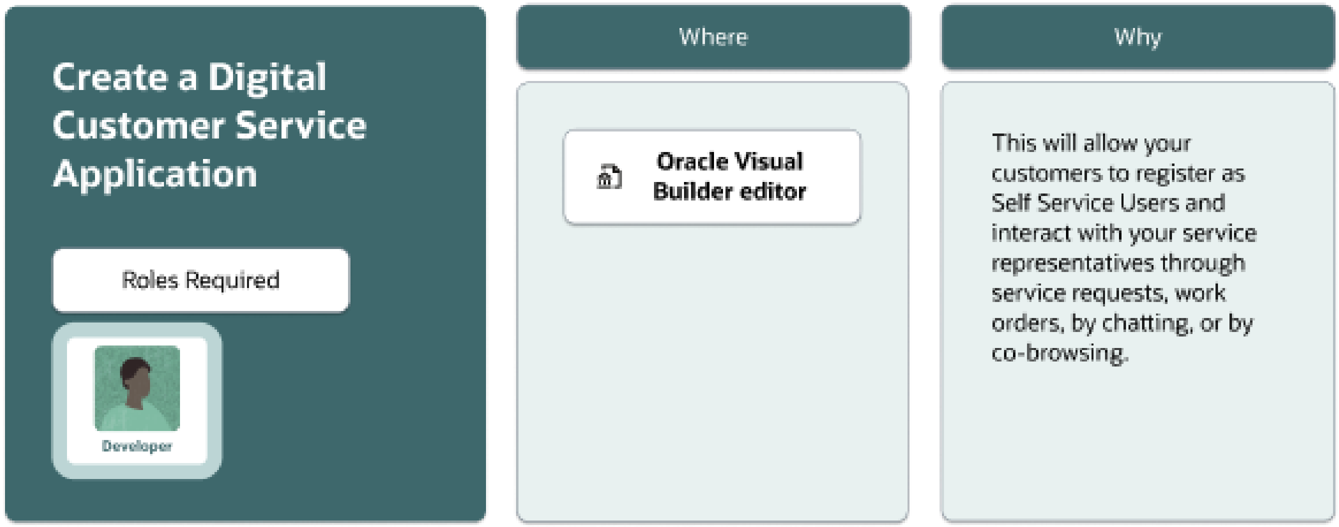
- **Set Up Administrators and Developers**



- Set Up Oracle Visual Builder



- **Create a Digital Customer Service application**



What you can do after completing these steps

- Give your customer account users self-service access to their service requests and relevant knowledge articles through a web interface.
- Configure the user interface to reflect your company brand. If you want, you can also define root pages and styles, and include various UI components.
- Help your customers to search for knowledge articles, and solve problems through the self-service application.
- Enable your customers to register as Digital Customer Service self-service users so they can interact with your customer service representatives through service requests, work orders, or by chatting.

About the case study

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

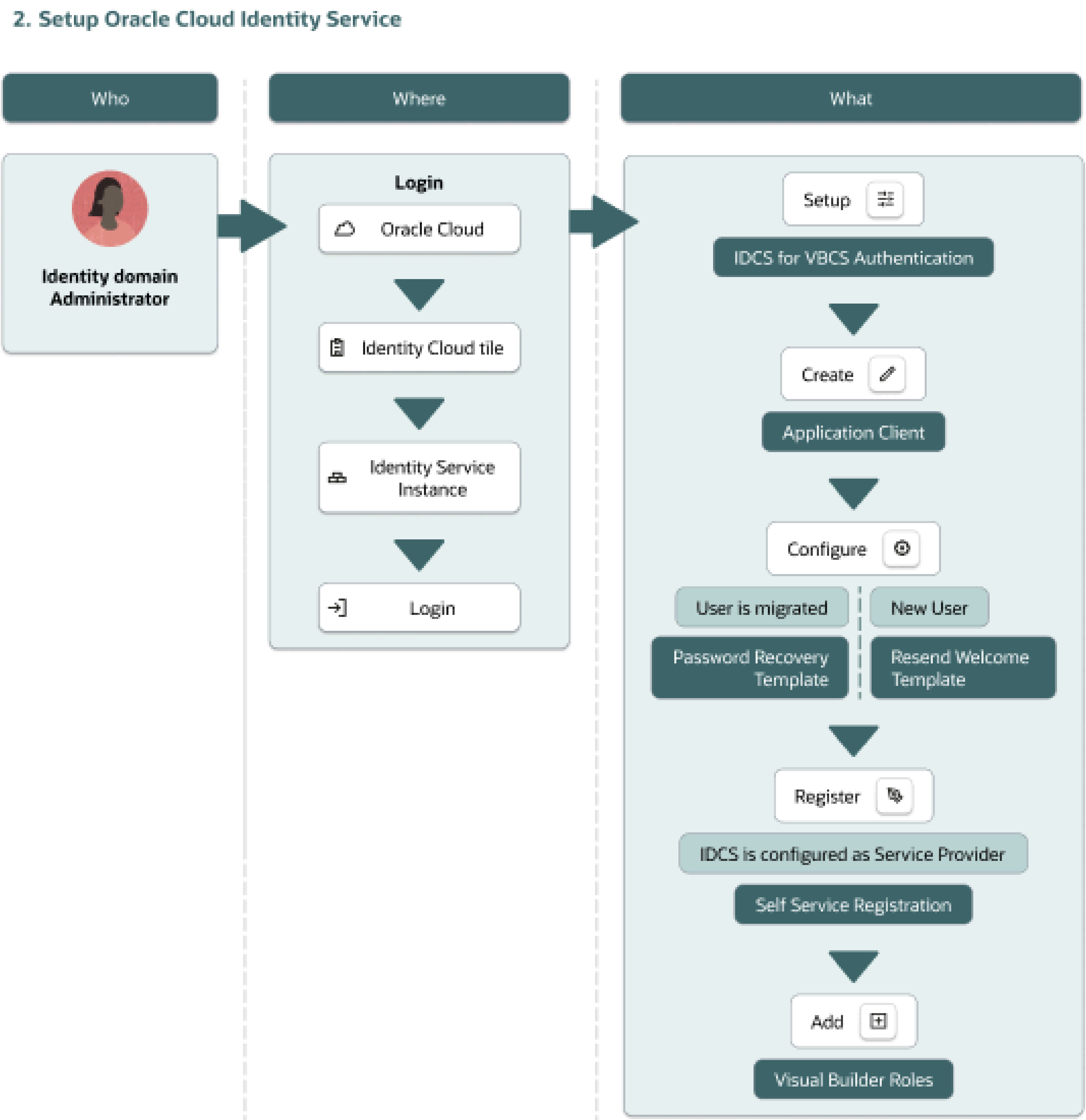
The case study is based on a fictitious company named Vision Corp, a global high-tech company that sells laptop and multiple server product lines to businesses and other organizations. Vision Corp would like to provide their customer account users self-service access to their service requests and relevant knowledge articles through a web interface to take advantage of the previously mentioned benefits.

Set up Oracle Identity Cloud Service

Overview of setting up Identity Cloud Service

You can set up Identity Cloud Service (IDCS) for Digital Customer Service by signing in as the Identity Domain Administrator and completing these steps:

- *Set Up Oracle Identity Cloud Service for authenticating your VBCS Application*
- *Create a Client application*
- *Configure the Resend Welcome and Password Recovery email templates*
- *Set up Self-Service registration when IDCS is configured as a service provider*
- *Add Visual Builder roles*


2. Setup Oracle Cloud Identity Service
Who
Where
What
Identity domain Administrator
Login
Oracle Cloud
Identity Cloud tile
Identity Service Instance
Login
Setup
IDCS for VBCS Authentication
Create
Application Client
Configure
User is migrated
New User
Password Recovery Template
Resend Welcome Template
Register
IDCS is configured as Service Provider
Self Service Registration
Add
Visual Builder Roles

Set Up Oracle Identity Cloud Service for authenticating your VBCS Application

By default the security policy defined is set up to use Fusion for sign in. For DCS applications created with VB, the policy should be changed to have IDCS provide the sign in. This is true for when using the DCS Custom Sign In components.

After this change, the new policy defined for VB will be for all VB applications. Optionally you can configure Identity Cloud Service. If there are VB applications embedded in Fusion, these should be explicitly listed in a new policy or added to the default policy.

This means two policies are created, one for IDCS sign in (user name-password) and one for Fusion sign in (Oracle Fusion Application). The non embedded Visual Applications should be selected to be used for IDCS sign in and the embedded Visual Applications should be selected for Fusion sign in respectively.

1. In your web browser, enter: `https://cloud.oracle.com` and sign in to your Oracle Cloud account.

   Note: This step is optional, and only required on your first use.

2. Sign in to Identity Cloud Service as the Administrator user.

   Note: Navigate to the domain first if required.

3. Click the Navigation drawer and then expand the **Security** list.
4. Click **IDP Policies**, and then click **Add**.
5. In the **Policy Name** field, enter a policy name, such as VBCS Sign in Policy, and click **Next**.
6. On the Add Identity Provider Roles page, click the **Add Rules** button.
7. In the Rule Name field, enter a rule name, then click the **Assign Identity Provider** field and choose an identity provider.
8. Click **Save**, and then click **Next**.
9. On the Apps page, click the **Assign Apps** button to add the VBCS application.
10. Select the application starting with VBINST_ or `<Fusion family name>*_vb_` and click **OK**.
11. Click **Finish** to complete and save the settings.

Create a Client application

A Confidential Client application must be created for use with Fusion Service when it interacts with IDCS. Use the IDCS Administrator Console to obtain appropriate application client credentials.

You'll either create an application client or get the Client ID and Client Secret of an existing client application.

If you need to create an application to use, follow these steps:

1. Sign in to Identity Cloud Service as the Administrator user.
2. Click the Navigation drawer and then expand the **Applications** list.
3. Click the **Add** icon.
4. Choose **Confidential Application**.
5. In the Name field enter **Proxy User Data Service App** and click **Next**.
6. Select **Configure this application as a client now** option.
7. In the Authorization area, select the **Client Credentials** option for Allowed Grant Types.

8. In the Token Issuance Policy area, for **Grant the client access to Identity Cloud Service Administrator APIs**, click **Add** or select all.
9. In the **Add App Role** dialog box, select **User Administrator**, and click **Add**.
10. Click **Next**, and then on the Resources page, click **Next** again.
11. In the **Web Tier Policy** page, click **Next** again.
12. On the **Authorization** page, click **Finish**.
13. From the **Application Added** dialog box, record the **Client ID** and **Client Secret** and then click **Close**.
14. Click **Activate**, and then in the confirmation dialog box, click **OK** to activate the application.

Configure the Resend Welcome and Password Recovery email templates

As part of user registrations, a user is created in IDCS and initially the user record is inactive.

After all the data related to the user is stored in the appropriate locations, the user is activated again and an API call is made to resend the Welcome email. To prevent a user from receiving multiple emails and to ensure the user sees the appropriate welcome message you've two configuration tasks depending on the scenario.

- You use the Resend Welcome template when a new user has signed up.
- You use the Password Recovery template when the user has been migrated.

Here are both tasks:

Configure the Resend Welcome Template

1. Sign in to Identity Cloud Service as a user with Administrative access
2. From the Navigation drawer, select **Settings**, and then **Notifications**.
3. Click the **Configure** tab.
4. Deselect the **Welcome** and **User Activation** check boxes.
5. Make sure the **Resend Welcome** check box is selected.
6. Click **Save**, then when the confirmation dialog box appears click **OK**.
7. Click the **Email Templates** tab.
8. Expand the **Resend Welcome** template, and replace the existing Subject line and message text with you own information and click **Save**.

Configure the Password Recovery Template

1. Sign in to Identity Cloud Service as a user with Administrative access
2. From the Navigation drawer, select **Settings**, and then **Notifications**.
3. Click the **Configure** tab.
4. Deselect the **Welcome** and **User Activation** check boxes.
5. Make sure the **Password Recovery Request** check box is selected.
6. Click **Save**, then when the confirmation dialog box appears click **OK**.
7. Click the **Email Templates** tab.
8. Expand the **Password Recovery Request** template, and replace the existing Subject line and message text with you own information and click **Save**.

Set up Self-Service registration when IDCS is configured as a service provider

You can configure Identity Cloud Service to act as a service provider to other external identity providers.

In this scenario the self-service registrations made when the value of the profile option SVC_CSS_USE_FA_AS_IDP is False will continue to create user accounts only in IDCS.

Depending on the identity provider, a custom process must be used to synchronize the user account with the external identity provider.

As the identity provider in this scenario isn't IDCS, the external provider will now have the responsibility for sending out the welcome email, managing the password cycle, and performing authentication. Also, IDCS must be configured to not send out the welcome email that allows a user to set the password.

Here's how you configure IDCS to not send the welcome email;

1. Sign in to Identity Cloud Service as a user with Administrative access.
2. From the Navigation drawer, select **Settings**, and then **Notifications**.
3. Click the **Configure** tab.
4. In the **End-User Notifications** work area, deselect the following check boxes:
    - Welcome
    - User Activation
    - Resend Welcome
5. Click **Save**, and when the confirmation dialog box appears click **OK**.

Add Visual Builder roles

You must add roles in Oracle Visual Builder and Oracle Visual Builder Studio to configure appropriate authorization for your Oracle Visual Builder platform and editor.

Instead of assigning roles to each user individually, you can simplify the process by creating groups and adding users to groups as a way to assign roles. Each time you add a user to a group, the user automatically gets the roles defined for the group. Or you can assign individual users to the Visual Builder roles.

Add Users to a Group

Add users to a group so that they automatically get the permissions defined for the group.

1. Sign in to Oracle Identity Cloud Service Console as an administrator.
2. From the Oracle Identity Cloud Service console, click the **Navigation menu** icon.
3. Click the **Groups** tab.
4. On the Groups page, click the group that you want to assign users to or add a new group.
5. On the Group Details page, select the **Users** tab.
6. Click **+ Assign**.
7. Select the users you want to add to the group, then click **OK**.
   The selected users are added to the group. You can now assign roles to all the users in the group, if required.

Assign Users or Groups to Roles in Visual Builder

After you create groups and add users to groups, you can assign roles and provide access to services and instances to all the members of the group at once.

Assign Roles to Users in Visual Builder

1. In Identity Cloud Service, click the **Navigation Drawer**, and select **Oracle Cloud Services**.
2. Select your Visual Builder instance.
   You can use the filter to help you find your instance. For Oracle Visual Builder Studio instances search for `visualbuilder`.
3. Click the **Application Roles** tab.
4. Click the menu options icon shown next to the role, and select **Assign Users**. To assign the role to a group, you need to select **Assign Groups**.
5. Assign the Oracle Visual Builder **Service Developer** role to the group or users that require Build and Maintain access in the Oracle Digital Customer Service applications.
6. Assign the Oracle Visual Builder **Service Administrator** role to the group or users that require Administrative access to configure instance-wide settings for the Oracle Visual Builder environment for all applications.

Assign Roles to Users in Visual Builder Studio

> **Note:** The following VB Studio steps apply only to one pod, typically your TEST instance. VBCS, however, is provisioned on all pods so those steps for the application roles are applicable to all instances.

1. Sign in to Identity Cloud Service, click the **Navigation Drawer**, and select **Oracle Cloud Services**.
2. From the Oracle Cloud console dashboard, navigate to the Identity Cloud console and click **Applications**.
3. Click the link for your Oracle Visual Builder Studio instance.
   You can use the filter to help you find your instance. For Oracle Visual Builder Studio instances search for your instance prefixed with "VBINST".
4. Click the **Application Roles** tab.
5. Click the menu options icon shown next to the role, and select **Assign Users**. To assign the role to a group, you need to select **Assign Groups**.
6. Select the check box next to the name of each user that you want to add to the role, and then click **Assign**.
   > **Note:** You must add the DEVELOPER_USER or the DEVELOPER_ADMINISTRATOR user roles.

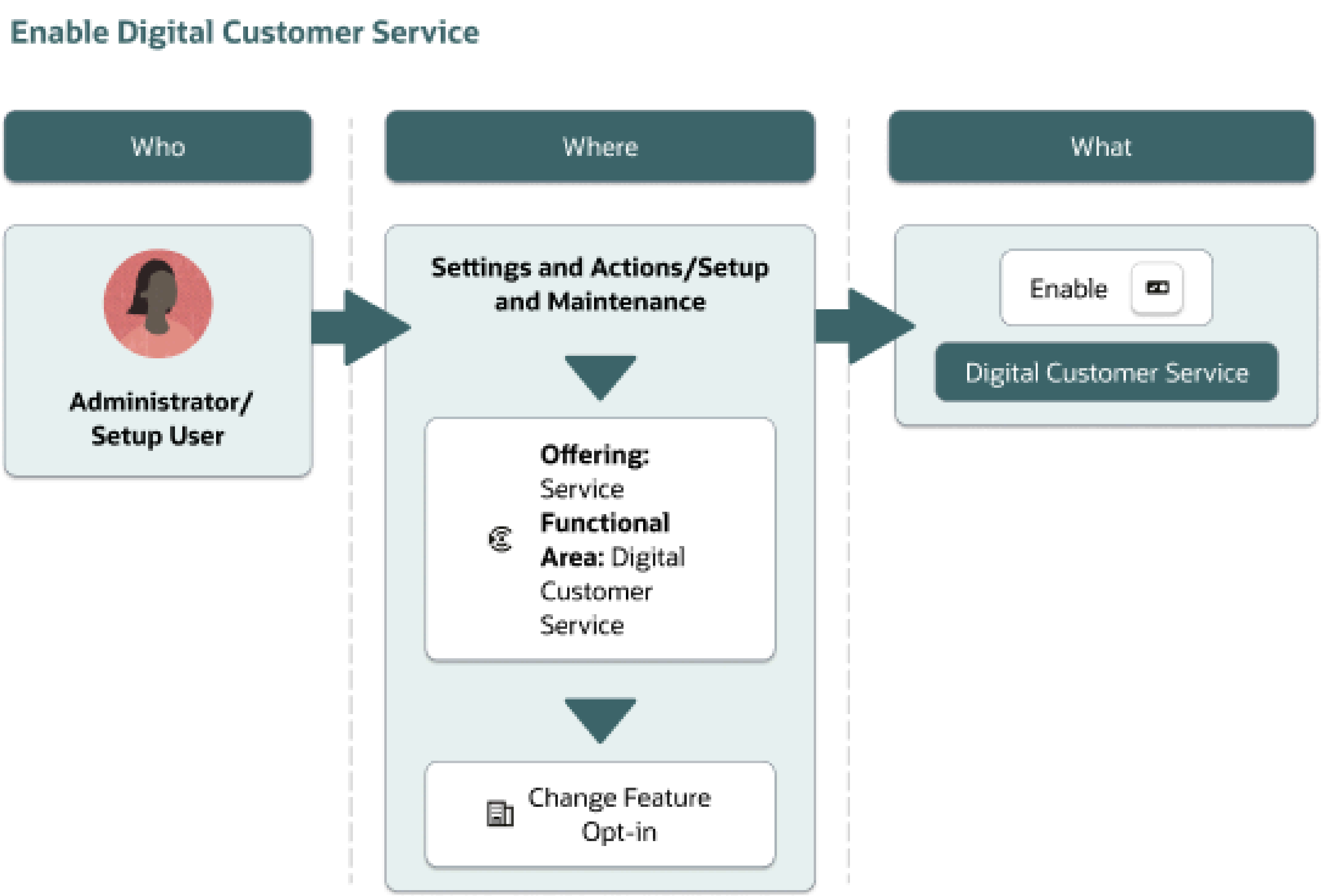
Enable Oracle Fusion Service

Overview of setting up Fusion Service for DCS

Here's a list of the steps required to set up Fusion Service for Digital Customer Service.

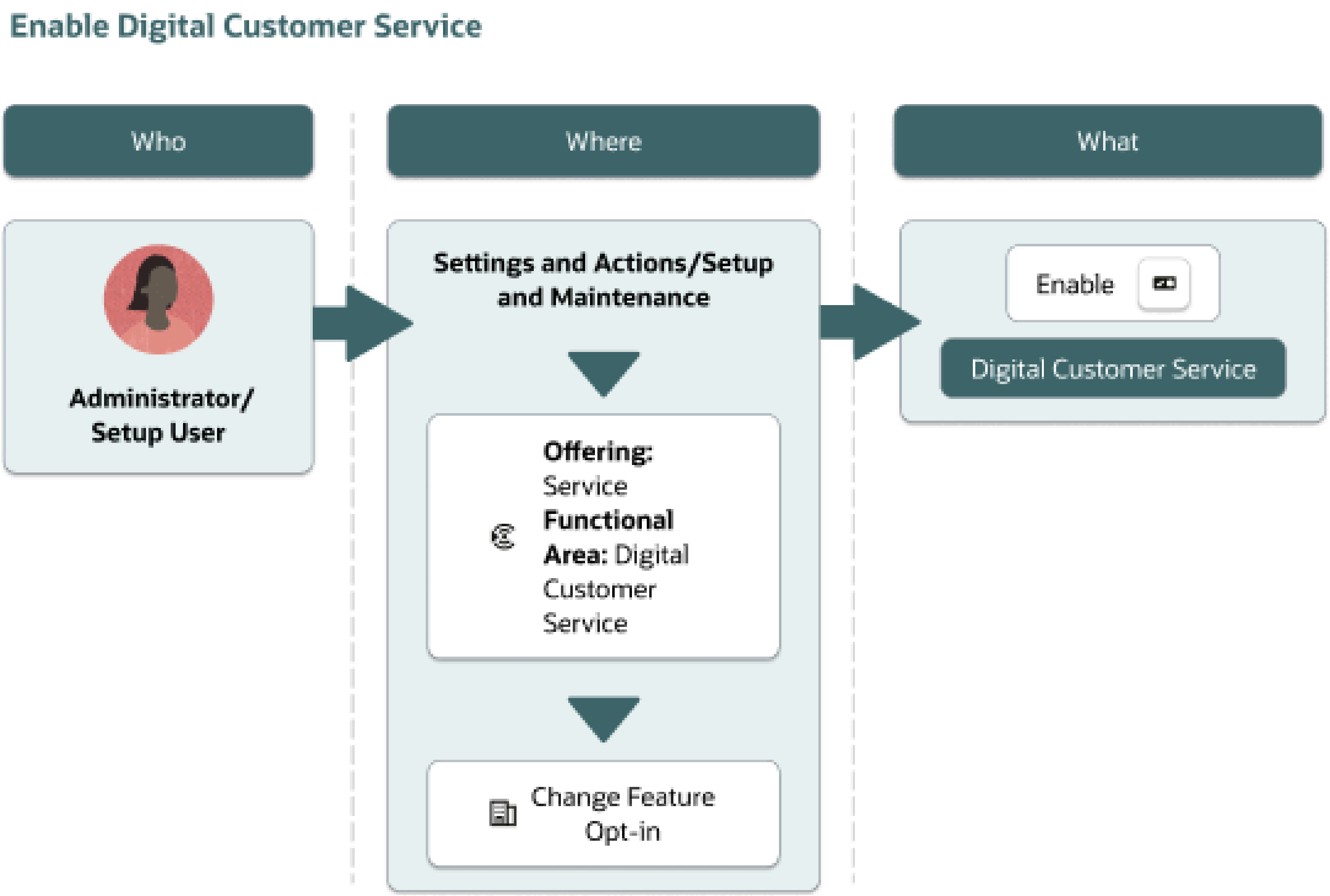
- *Enable Digital Customer Service*
- *Configure a user category for proxy users*
- *Create the proxy users*

- *Set profile options for Self-Service Optimization*
- *Set the Oracle Identity Cloud Service endpoint*
- *Configure the client ID and client secret*
- *Create groups in Fusion Service*
- *Manage the proxy user configuration data*
- *Set proxy user credentials*
- *Validate Self-Service Optimization setup*



Enable Digital Customer Service

You must enable Digital Customer Service in Fusion Service to have access to the profile options and work areas.



Here are the steps for enabling the Digital Customer Service application:

1. Sign in to Fusion Service as an administrator or a setup user.
2. Click the **Settings and Actions** drop-down list, and select **Setup and Maintenance**.
3. From the **Actions** drop-down list, select **Go to Offerings**, and then select **Service**.
4. In the **Setup and Maintenance** work area select the Service offering.
5. Click the **Opt In Features** button.

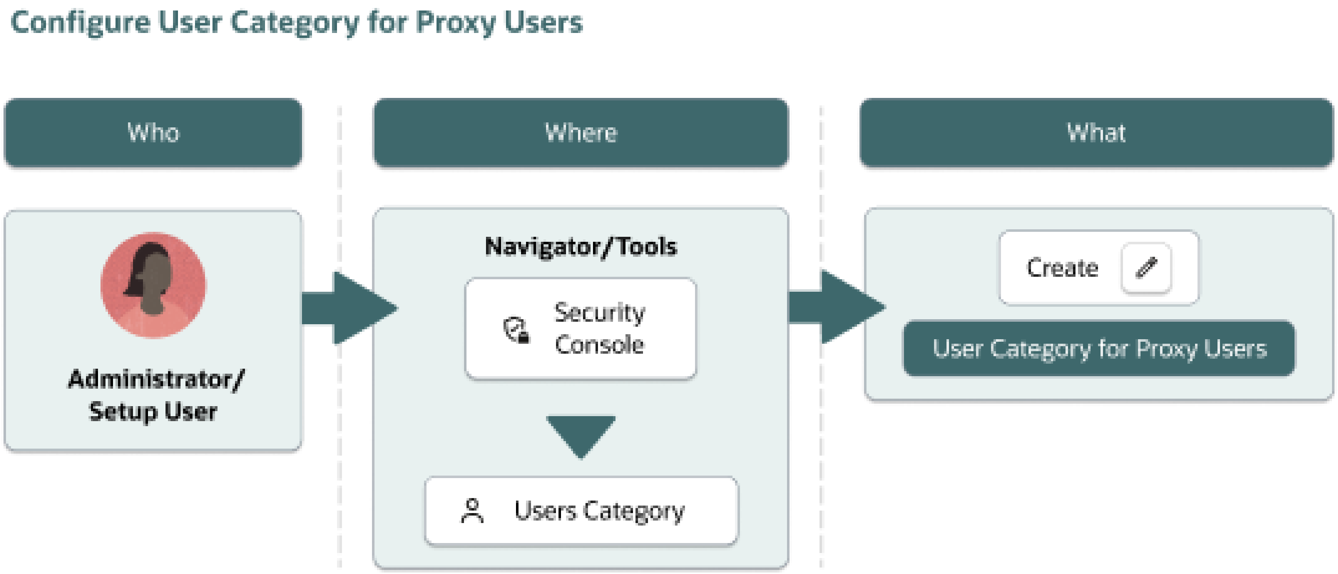
   The **Opt In: Service** page is displayed.
6. Find the **Digital Customer Service** row, then select the **Enable** check box.
7. Click **Done**.

Enabling Digital Customer Service will let you find these work areas grouped with the Service icon in Fusion Service:

- Self-Service Users
- Registration Requests

Configure a user category for proxy users

A proxy user account is used by multiple actual users to perform REST operations in Fusion Service.



You can configure the proxy users to have a different password expiry policy. You're strongly encouraged as it ensures that the regular password expiry rules don't apply to proxy users. You can create a different user category for the proxy users.

Follow these steps to create a category specific for proxy users that uses a password policy that doesn't expire passwords:

1. Sign in to Fusion Service.

   On the home page, select Tools, then **Security Console**.
2. In the **Security Console** work area, click the **User Categories** tab.
3. Click **Create**.

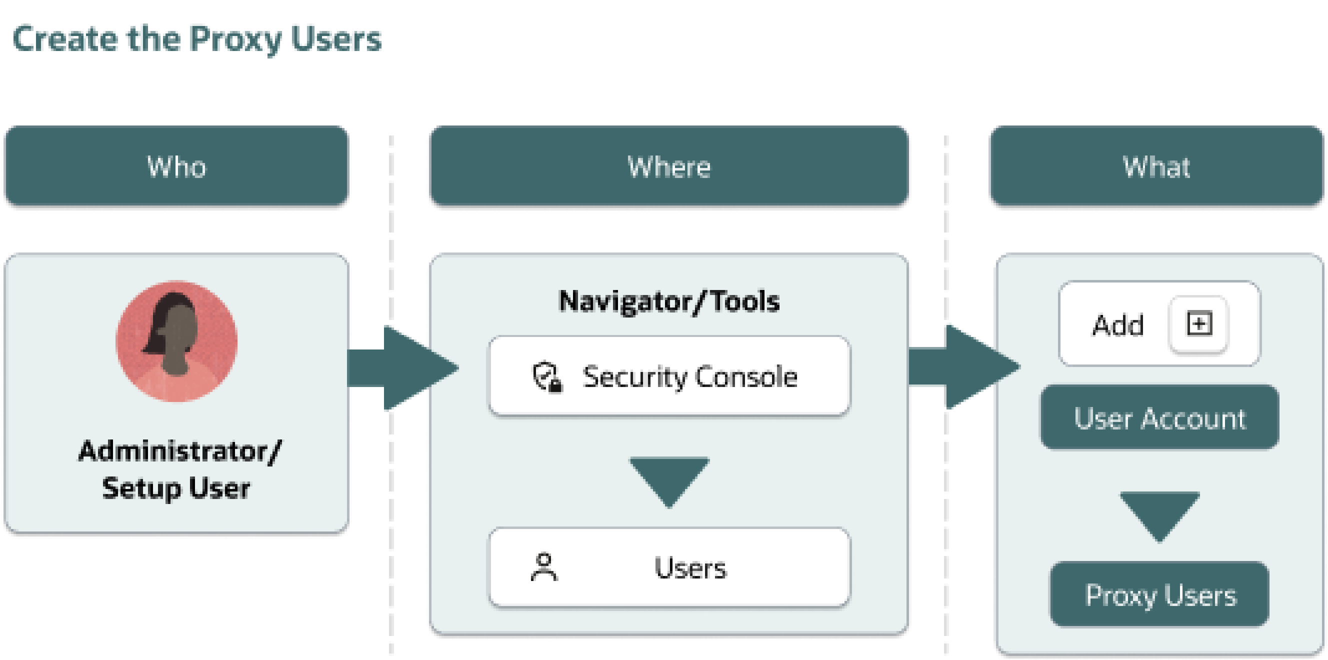
   The **User Category: Details** page appears.
4. Click **Edit**.
5. Enter a name in the **User Category Name** field, such as **ProxyUsers**.

   Note: Note this field can't contain spaces or special characters.
6. Click **Save and Close**.
7. Click **Password Policy**.
8. Click **Edit**.

9. Configure the fields for the proxy user password policy. In particular, you might want to set the **Days Before Password Expiration** to a relatively high number and give enough time for the **Days Before Password Expiry Warning**.
10. Click **Save and Close**.
11. Click **Done**.

Create the proxy users

A proxy user account is used by multiple actual users to perform REST operations in Fusion Service.



We recommend you use the syntax shown in the following table when you create your proxy user accounts.

1. Sign in to Fusion Service as an administrator or setup user.
2. Click Navigator, then from the Tools menu, select **Security Console**.
3. In the **Security Console** work area, click the **Users** tab.
4. Click **Add User Account**.
5. Now, one at time, add three separate users and grant them roles by doing the following:

    a. From the **User Category** drop-down list, select **ProxyUsers**.
    b. Fill in the **First Name**, **Last Name**, and **Email** fields.

    > **Note:** The **User Name** field auto fills with the email address user name. Overwrite that in the following step.

    c. In the **User Name** field, choose one of the entries:

User	Roles Granted	Role Code
PUDS_CSS_USER	Customer Self-Service Proxy User	ORA_SVC_CUSTOMER_SELF_SERVICE_PROXY_USER_ABSTRACT
PUDS_CSS_ADMIN	Customer Self-Service Proxy Account Administrator	ORA_SVC_CUSTOMER_SELF_SERVICE_PROXY_ACCOUNT_ADMINISTRATOR
PUDS_ANONYMOUS_USER	Customer Self-Service Proxy Anonymous User	ORA_SVC_CUSTOMER_SELF_SERVICE_PROXY_ANONYMOUS_USER

d. Enter a password, then confirm the password.

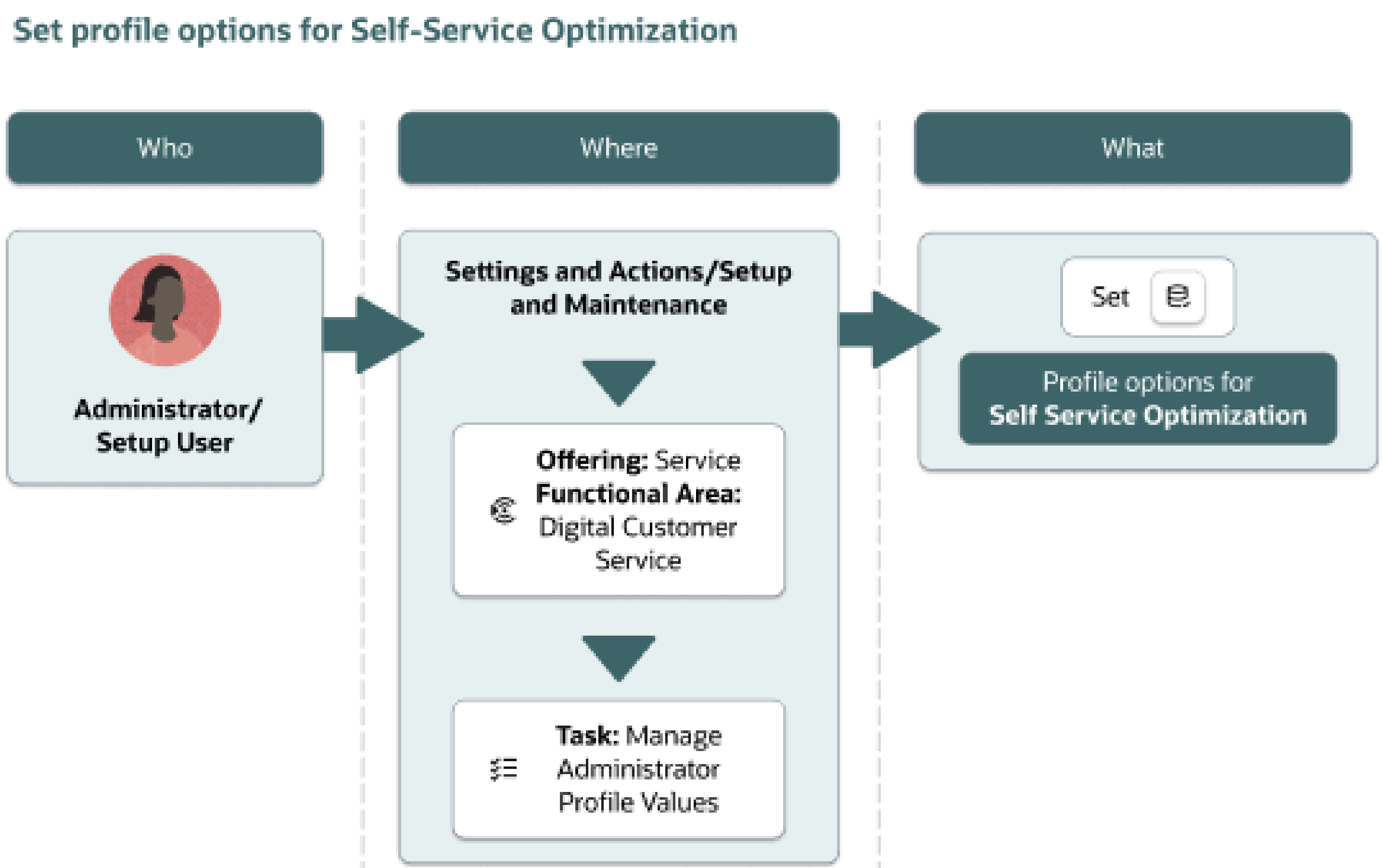
> **Note:** Passwords must be at least eight characters long.

e. Click **Add Role**.
f. In the Search field, enter the value listed in the **Roles Granted** column of the following table that corresponds with the user you've created.
g. When the role is found, click **Add Role Membership**, and then click **Done**.
h. Click **Save and Close** and repeat these steps for each of the three users you must create.

Set profile options for Self-Service Optimization

Self-Service Optimization gives you greater flexibility by using proxy users in Fusion Service

You must set the required profile options for Self-Service Optimization. There are also optional profile options for other functionality.



Set Required Digital Customer Service Profile Options

The profile options specific to Digital Customer Service are found in two task areas: Manage Digital Customer Service Profile Options and Manage Digital Customer Service Account Setup Profile Options.

1. Sign in to Oracle Fusion Service as administrator or a setup user.
2. In the **Setup and Maintenance** work area, go to the following:
   - Offering: Service
   - Functional Area: Digital Customer Service
   - Task: Manage Digital Customer Service Profile Options

     or
   - Task: Manage Digital Customer Service Account Setup Profile Options
3. Click the name of the profile option that you want to change.
4. Set the profile option value as needed.
5. Click **Save and Close**.

Required Profile Options and Descriptions	Default Value	Comments
FND_IDP_PROXY_USER_WHITELIST Used to identify the list of allowed proxy users.	None	Enter a comma-separated list of proxy user names. **Note:** There must be no spaces between the commas and the names.
ORA_CORS_ORIGINS List of trusted domains that can make requests.	None	*, or specific comma-separated fully qualified domain names.
CORS_ACCESS_CONTROL_ALLOW_HEADERS Specifies comma-separated list of headers that are allowed as part of a CORS request.		Add these values, in the comma separated list, if they're not present: Puds-Access-Token, kmauthtoken, content-language, X-Oracle-ABCS-SessionId, X-Oracle-ABCS-UserId
SVC_CSS_PUDS_CACHE_DURATION Decides the amount of time, in minutes, that Proxy User Data Service objects are cached.	15 minutes	Any changes to this parameter will force a refresh of the proxy users configuration data cache.
SVC_CSS_USE_FA_AS_IDP Identifies if self-service users are created in Fusion Service or in IDCS.	False.	Make sure this value is set to False for self-service optimization mode.

Set Optional Profile Options

Profile options enable you to configure and control application data centrally. They store user preferences, installation information, configuration choices, and processing options. Administrators and setup users manage profile options in the Setup and Maintenance work area.

Registration Profile Options

Profile Option	Default Value	Possible Values	Effect
`SVC_CSS_SELF_REGISTRATION`	New Or Existing	None New Or Existing Existing Only	Specifies which contacts can self-register. If Existing is specified, only existing contacts can self-register.
`SVC_CSS_SELF_REG_AUTO_APPROVE`	False	True False	Enables automatic approval of self-service registration requests that are associated with an account. If SVC_ CSS_ SELF_ REG_AUTO_ APPROVE is set to False and SVC_ CSS_ ACCT_ADMIN_APPROVE is set to True, then the Digital Customer Service Account

Profile Option	Default Value	Possible Values	Effect
			Administrators can approve user registration requests in the Digital Customer Service Customer user interface. Also, Digital Customer Service Administrators can approve registration requests in the Digital Customer Service Administration user interface.
`SVC_CSS_ACCT_ADMIN_APPROVE`	True	True False	Enables the approval of self-service user registration requests by users with Digital Customer Service Account Administrator roles. If set to True, Digital Customer Service Account Administrators can approve user registration requests in the Digital Customer Service customer user interface and Digital Customer Service Administrators can approve registration requests in the Digital Customer Service Administration user interface. If set to False, only Digital Customer Service Administrators can approve registration requests in the Digital Customer Service Administration user interface. **Note:** This option applies only when the SVC_ CSS_ SELF_ REG_ AUTO_APPROVE option is set to False.
`SVC_CSS_ACCT_KEY_FIELD`	OrganizationName	Any field in the Account object	Specifies a valid field name in the Account object. The field name is case sensitive. **Note:** You must create an attribute in the account object to be the account key, because the default account key of account name isn't secure.
`SVC_CSS_REG_CONT_MAP`	An empty string	An empty string. Any defined value, with a colon separating fields, and commas separating the pairs. For example, reg_field1:contact_ field1, reg_field2:contact_field2	You specify a value for this profile option only if the name of the attribute in the Self Registration object is different from the name in the Contact object. Cases where they might happen are if you've created a custom attribute for an object. Custom attributes are

Profile Option	Default Value	Possible Values	Effect
			designated with an _c, such as PlaceOfBirth_c. For this use case, you ignore the _c when decide whether an attribute maps or not. So, let's take the custom attribute in the Self Registration object **`PlaceOfBirth_c`**. Because the Contact object has a ready to use attribute called **`PlaceOfBirth`**no mapping is required because the two values match. If, however, the name of the custom attribute was **`BirthPlace_c`** the value of this profile option would then be **`BirthPlace_c:PlaceOfBirth`**. Here's an extra example with multiple mappings: First, you specify case sensitive name and value pairs to map the fields of the Registration View object to the Contact View object in the following way: **`reg_field1:contact_field1,reg_field2:contact_field2`**. The **`reg_field1`** is the PlaceOfBirth_c in the Registration View Object which is a custom object created in Application Composer. The **`contact_field`** is the **`PlaceOfBirth`** field in the Contact View object. This attribute is already present in the Contact object. So the mapping would be: **`reg_field1:contact_field1 LIKE BirthPlace_c:PlaceOfBirth`**
`SVC_CSS_SIGN_IN_ATTR_NAME`	EmailAddress	The value of the assigned attribute must be unique. Possible values include: EmailAddress	Specifies the sign-in attribute that users must specify in the Sign in ID field in the Self-Service Registration object. This field is used to decide whether the user exists in the Lightweight Directory Access Protocol server.
`SVC_CSS_REG_FLD_CONTACT`	EmailAddress	Any field on the Self-Service Registration object.	Specifies the field to use during the user registration process to decide if the registering user is an existing contact. The field names are case sensitive.

Profile Option	Default Value	Possible Values	Effect
			The SVC_CSS_REG_CONT_MAP profile option is used to find the name of the attribute on the Contact.
`SVC_CSS_SEND_WELCOME_EMAIL`	True	True False	Enables sending a welcome email when a new user account is created.
`SVC_CSS_USER_ROLE_COMMON_NAME`	`ORA_SVC_CUSTOMER_SELF_SERVICE_USER_ABSTRACT`	A string representing the name of the role that's set up for Customer Self-Service users. Typically, this is a copy of a Customer Self-Service User with extra privileges added.	Specifies the common name of the role granted to previously created Customer Self-Service Users.
`SVC_CSS_ACCT_ADMIN_ROLE_COMMON_NAME`	`ORA_SVC_CUSTOMER_SELF_SERVICE_ACCOUNT_ADMINISTRATOR_ABSTRACT`	A string representing the name of the role that's set up for Customer Self-Service Account Administrator. Typically, this is a copy of a Customer Self-Service Account Administrator with extra privileges added.	Specifies the common name of the role granted to the previously created Customer Self-Service Account Administrators.
`SVC_CSS_USER_CATEGORY`	An empty string	A string	Specifies the user category that defines the URL to which the self-service user is redirected after a password reset. The user category is defined in the Security Console.
`SVC_CSS_IMP_SIGN_IN_ATTR_NAME`	`PrimaryEmailAddress`	Any field on the Contact object.	Specifies a field in the Contact object to be used as the sign-in attribute when importing data into the Self-Service Roles object. The field name is case sensitive.
`SVC_CSS_USE_FA_AS_IDP`	False	True False	Specifies whether the identity provider is Oracle Fusion Applications or Oracle Identity Cloud Service. When set to True, Oracle Fusion Applications is used.
`ORA_SVC_CSS_SELF_REG_B2C_AUTO_APPROVE`	True	True False	Enables automatic approval of self-service registration requests that aren't associated with an account. If set to True, users who register without an account will be auto approved to become self-service users. If set to False, users who register without an account

Profile Option	Default Value	Possible Values	Effect
			will need to be approved by an administrator before they can become self-service users.
SVC_CSS_PUDS_CACHE_DURATION	15	Integer in minutes	Decide the amount of time, in minutes, that Self-Service Optimization objects are cached.
SVC_CSS_ALLOW_CONTACT	True	True False	Enables the self-service registration of B2C Service contacts.
SVC_CSS_ALLOW_CONSUMER	True	True False	Enables the self-service registration of consumers.
SVC_CSS_CONSUMER_USER_CATEGORY	An empty string	A string	Specify the user category for consumers defining the redirect URL for self-service users after a password reset.

Knowledge Setup Profile Options

Profile Option	Default Value	Possible Values	Effect
CSO_CONTENT_RATING_TYPE	None	True and False	Enables content rating for Knowledge.

Use custom job roles

You can create a custom job role for Customer Self-Service users. It lets you create a custom object and assign privileges to that object.

Note: This step is optional for advanced setup of your application.

There are many reasons why you might create a custom job role for Customer Self-Service users. One possible reason is when you create a custom object and want to assign privileges to that object.

Follow these steps to assign custom job roles for use in Digital Customer Service:

1. Create a custom role by making a copy of one of the following predefined roles:
    - Customer Self-Service User
    - Customer Self-Service Account Administrator

2. Set the value of the appropriate Digital Customer Service profile option to the name of the custom role you created. The following profile options can be set to the name of the custom role:
    - `SVC_CSS_USER_ROLE_COMMON_NAME` If the value of this profile option is set to the name of a custom role, then all Customer Self-Service Users will be assigned this role when they're provisioned.
    - `SVC_CSS_ACCT_ADMIN_ROLE_COMMON_NAME` If the value of this profile option is set to the name of a custom role, then all self-service users who are assigned the Customer Self-Service Account Administrator role will receive this custom role.

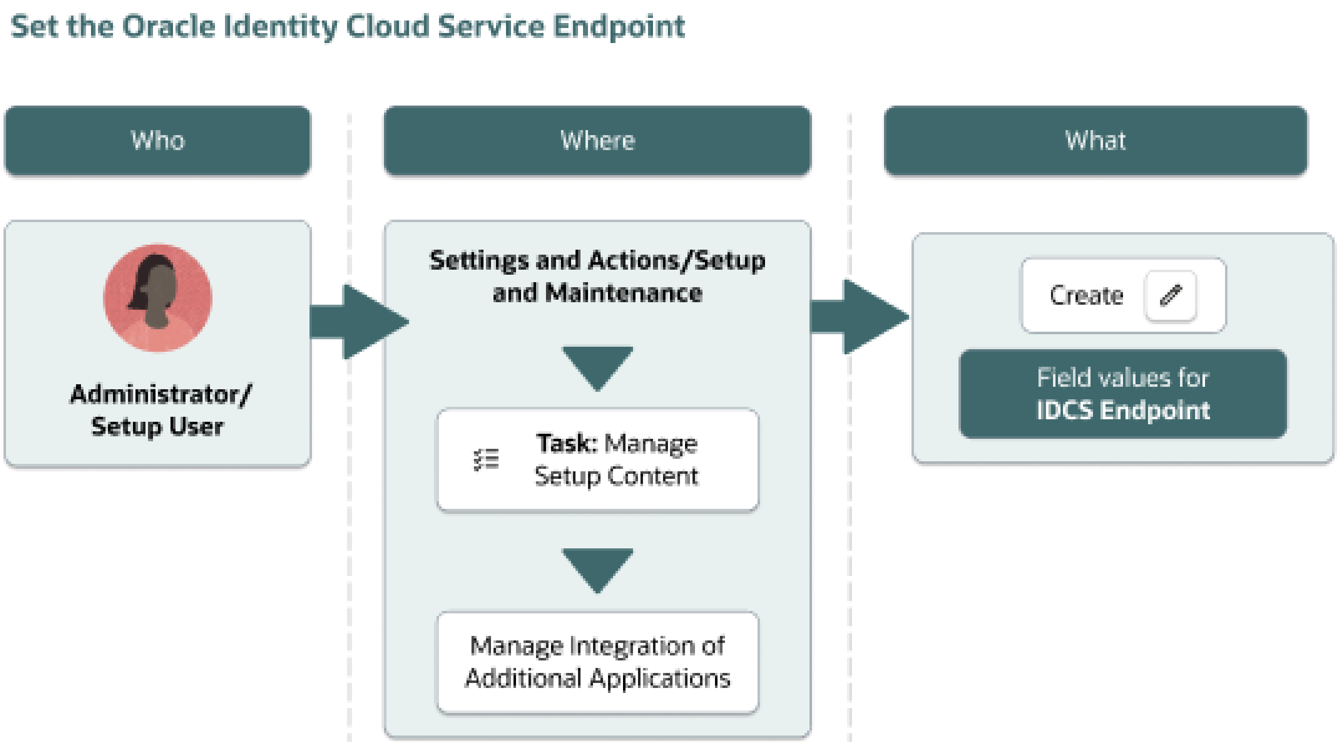
    For more information about setting profile options, see *Set profile options for Self-Service Optimization*.

    > **Note:** If you update these profile options to specify a custom role once your Digital Customer Service application is in use, you must perform a mass update of any existing users from the old roles to the new roles.

For each custom job role you create, you also must create a group in Identity Cloud Service. The external ID of the IDCS group you create must match the code of the Fusion Service custom job role that you created. For more information about creating IDCS groups, see *Set profile options for Self-Service Optimization*.

Set the Oracle Identity Cloud Service endpoint

You can configure Fusion Service to enable back end communication with IDCS.



Here are the steps:

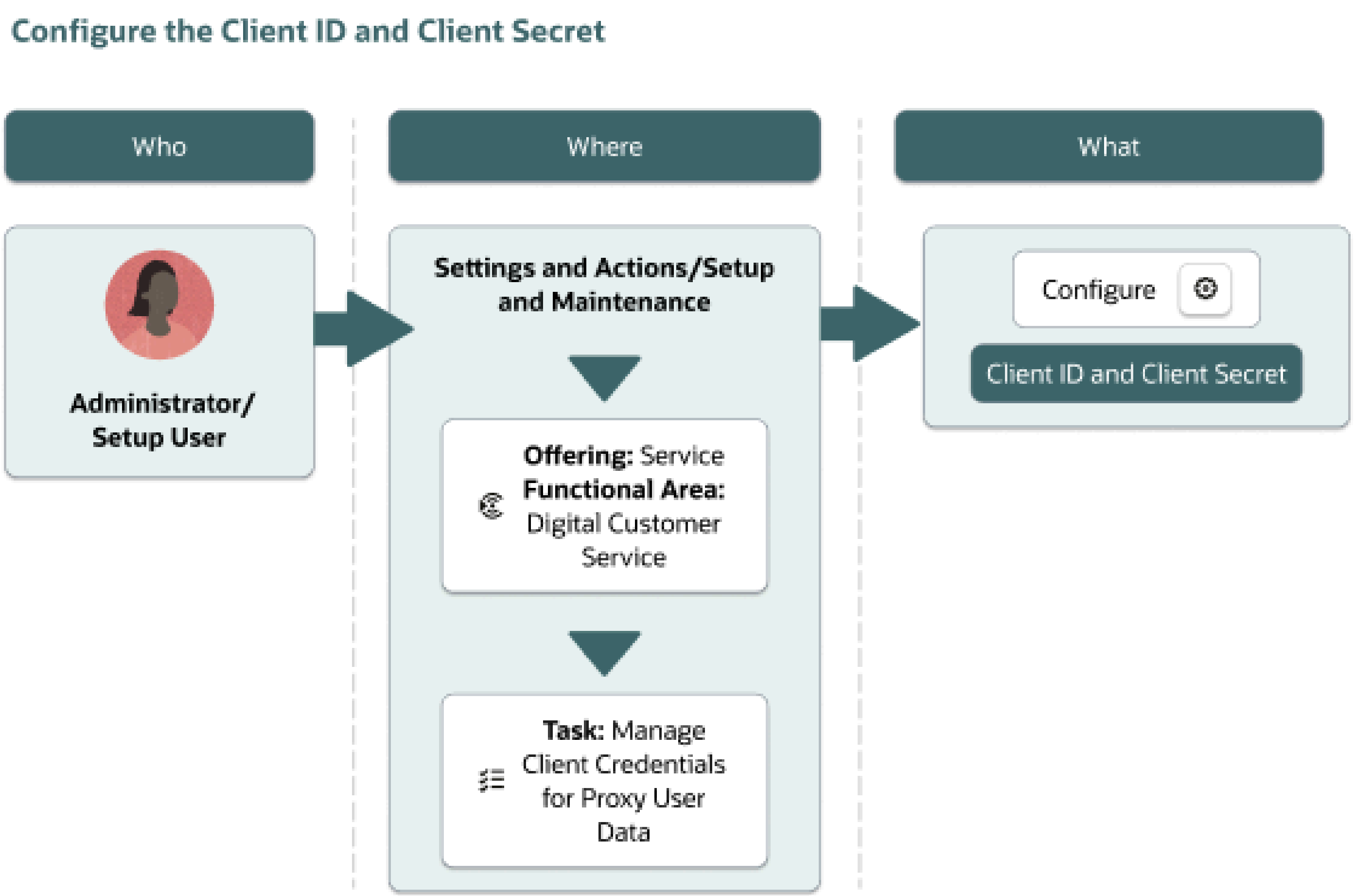
1. Sign in to Fusion Service as administrator or setup user.
2. Click the Settings and Actions menu, and select Setup and Maintenance.
3. Click the **Tasks** icon, then click **Manage Setup Content**.
4. Click **Manage Integration of Additional Applications**.
5. In the Search Results area, click the **Actions** menu, and select **Create**.
6. In the Create Application Integration form, enter the following:

Field	Enter this value
Application Name	IDCS_REST_ENDPOINTAPP
Full URL	For example: **https://<IDCS HOST>/admin/v1** **Note:** This is the IDCS host that authenticates the Visual Builder instance.
Partner Name	IDCS

7. Click the **Apply** button and then verify the Protocol, Server Host and Context Root details are populated in the **Server Details** area.
8. Click **Save and Close**.

Configure the client ID and client secret

Add the client ID and client secret that you created using the steps from *Create a Client application* to your Fusion Service configuration.



Follow these steps to configure the client ID and client secret.

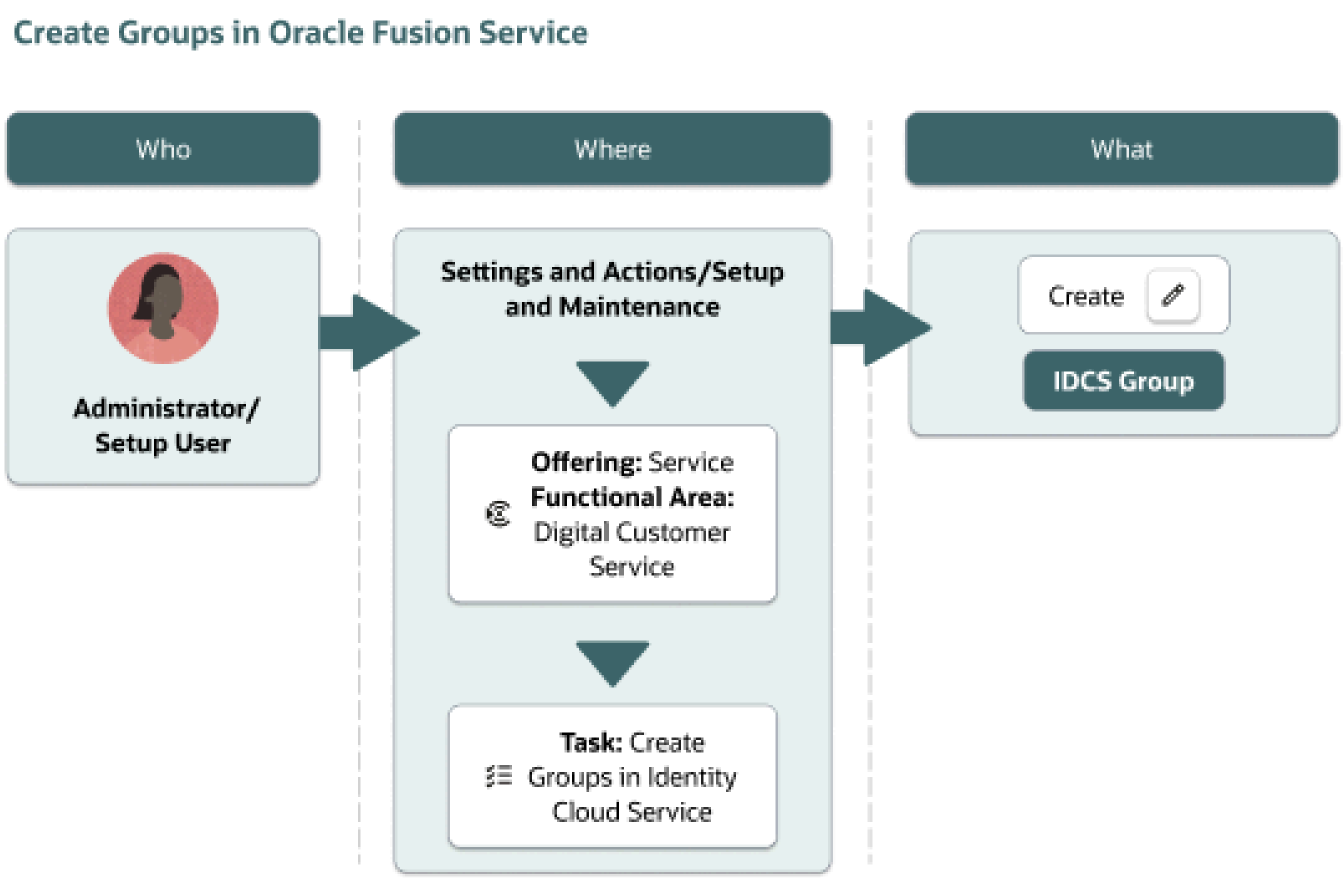
1. Sign in to Fusion Service as an administrator or a setup user.
2. In the Setup and Maintenance work area, go to the following:
   - Offering: Service.
   - Functional Area: Digital Customer Service.
   - Task: Manage Client Credentials for Proxy User Data
3. Enter the Client ID and Client Secret.

4. Click **Test** to make sure the values you entered are valid, and then click **OK** if so.
5. Click **Save and Close**.

Note: The credentials are cached by the Proxy User Data Service. These credentials can be cleared or refreshed by changing the value of SVC_CSS_PUDS_CACHE_DURATION profile option.

Create groups in Fusion Service

The groups should already be in place in the Identity Cloud Service from the synchronisation of roles from Fusion. If they're not, you can create them manually by working through the following steps.



Note: If you delete a group that's in use and then at another time recreate it we recommend that you clear the cache by adjusting the value of SVC_CSS_PUDS_CACHE_DURATION profile option.

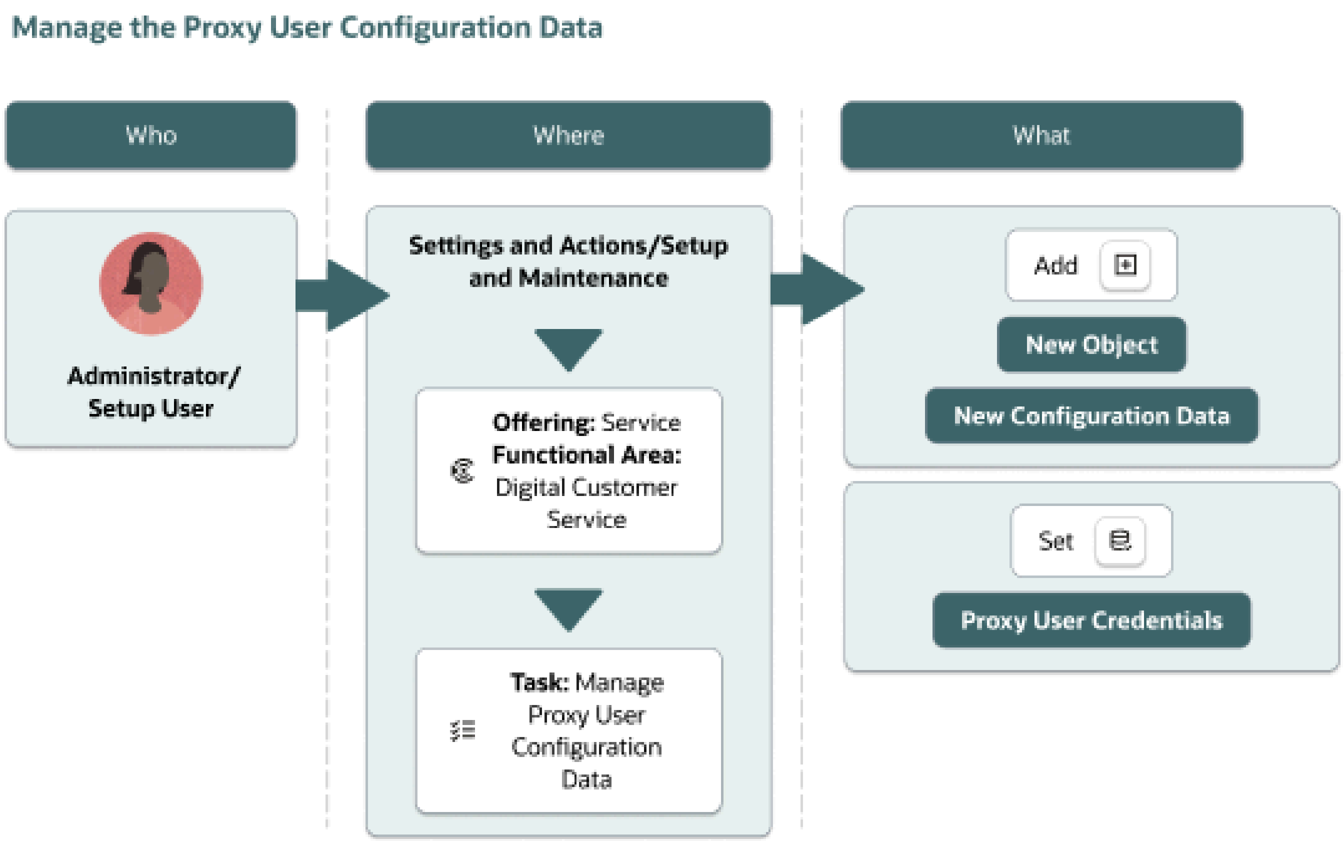
Role Name	External ID	Related Profile Option
Customer Self-Service User	ORA_SVC_CUSTOMER_SELF_SERVICE_USER_ABSTRACT	SVC_CSS_USER_ROLE_ COMMON_NAME
Customer Self-Service Account Administrator	ORA_SVC_CUSTOMER_SELF_SERVICE_ACCOUNT_ADMINISTRATOR_ABSTRACT	SVC_CSS_ACCT_ADMIN_ROLE_ COMMON_NAME

> **Note:** If you've changed the value of the profile options listed in the last column of the following table, then don't use the external ID and role name shown in the table, instead the external ID and role name will depend on the value of your change profile option.

> **Note:** By default, the related profile options reflect the preceding table. If you use custom roles, the Role Name and the Display Name values must match the value of the relevant profile option. If you need to create a new group, you do it using the **Create Groups in Identity Cloud Service** task in Functional Setup Manager. Here are the steps for you to create groups:
>
> 1. Sign in to Fusion Service as an administrator or setup user.
> 2. In the Setup and Maintenance area, go to the following:
>   - Offering: Service.
>   - Functional Area: Digital Customer Service.
>   - Task: Create Groups in Identity Cloud Service.
>
>   **Note:** Select **All Tasks** from the **Show** drop-down list to display the task.
> 3. Click the link for the task.
> 4. Select the appropriate Fusion Service role from the table.
> 5. If the corresponding Identity Cloud Service role doesn't exist, click the **Create** button to create the IDCS group.
>
>   **Note:** If the corresponding IDCS group already exists, you'll see information about the existing role instead of the Create button.

Manage the proxy user configuration data

Perform these steps to manage all the URL patterns that you need to reach in Fusion Service through the proxy user data service.



The fields are pre populated in Fusion Service with all the endpoints that are used in the Digital Customer Service reference implementation. The standard use case it to set up the proxy user credentials.

If you need to add more objects, here are the steps:

1. Sign in to Fusion Service as administrator or setup user.
2. In the Setup and Maintenance work area, go to the following:
   - Offering: Service.
   - Functional Area: Digital Customer Service.
   - Task: Manage Proxy User Configuration Data.
3. For predefined configuration data note the following:
   - You can add new configuration data.
   - Only allowlisted resources can be exposed to anonymous users. The following resources are on the allowlist:
     - categories
     - catalogProductItems
     - catalogProductGroups

        - productGroupHierarchies
        - fndStaticLookups
        - selfRegistrations
        - chatAuthenticate
        - dynamicLinkPatterns
    - Custom objects that you create with Application Composer can be exposed to Anonymous users even though they're not on the allowlist.
4. To add new objects, do the following:
    a. In the Search Results area, click the **New (+)** icon.
    b. Add the URL pattern.
    c. Click the drop-down list and add the HTTP method.
    d. Click the drop-down list and choose the appropriate user role.

        Note: This is the same user role from Identity Cloud Service.

    e. Add the appropriate proxy user key.
    f. Click **Active**.
5. Click **Save and Close**.

Note: Proxy user configuration data is cached for a duration specified by the SVC_CSS_PUDS_CACHE_DURATION profile option.

If this value is changed then the cache is cleared. For changes made using this UI to be read immediately, the value of SVC_CSS_PUDS_CACHE_DURATION profile must be altered. The recommended action is to add or subtract 1 minute from the existing value.

Set proxy user credentials

Complete the configuration of the proxy user configuration data for the Self-Service Optimization feature, you need to set the user credentials for the proxy users.

1. Sign in to Fusion Service as an administrator or setup user.
2. In the Setup and Maintenance work area, go to the following:
    - Offering: Service.
    - Functional Area: Digital Customer Service.
    - Task: Manage Proxy User Configuration Data.
3. Find any line referencing the following proxy user keys:
    - PUK#_ANONYMOUS_USER
    - PUK#_SELF_SERVICE_USER
    - PUK#_SELF_SERVICE_ACCOUNT_ADMIN

4. Do the following with each of the three user keys:

    a. Select the entry, then from the **Actions** menu, click **Edit**.
    b. In the Edit Proxy User Configuration Data workspace, enter the Proxy User Name if it's different from the default name.

        Note: It's recommended that you retain the proxy user names.

    c. Enter the password for the proxy user.
    d. Click **Save and Close**.

Because the same proxy user key is used by multiple URLs, you can edit any one URL that uses this proxy user key to set the proxy user credentials associated with that key.

Note: Proxy user configuration data is cached for a duration specified by the SVC_CSS_PUDS_CACHE_DURATION profile option.

Validate Self-Service Optimization setup

Now that you've enabled Fusion Service, you can verify the setup.

You can use a set of validation checks Functional Setup Manager by providing certain basic configuration parameters. The checks are grouped by task and have a set of tests associated with them. Some tests requires you to enter parameters. If so, the Supply Parameters tab is enabled. The Test Results tab is enabled once all required parameters have been populated.

Here's an overview of all the tests you can run:

Validate Self-Service Optimization Tests

Setup Task	Tests	Description
Set Profile Options for Self-Service Optimization	Verify profile option: SVC_CSS_USE_FA_AS_IDP	Verifies the value of the SVC_CSS_USE_FA_AS_IDP profile option.
	Verify profile option: FND_IDP_PROXY_USER_WHITELIST	Verifies the value of the FND_IDP_PROXY_USER_WHITELIST profile option.
	Verify profile option: ORA_CORS_ORIGINS.	Verifies the value of the ORA_CORS_ORIGINS profile option.
	Verify profile option: CORS_ACCESS_CONTROL_ALLOW_HEADERS	Verifies the value of the CORS_ACCESS_CONTROL_ALLOW_HEADERS profile option.
Configure the Client ID and Client Secret	Get IDCS client access token	Retrieves the client access token for use in other tests.
Create Groups in Oracle Identity Cloud Service	Verify customer self-service user group in IDCS	Verifies that the Customer Self-Service User group is available in Identity Cloud Service.

Setup Task	Tests	Description
	Verify customer self-service account administrator group in IDCS	Verifies that the Customer Self-Service User group is available in Identity Cloud Service.
Set Proxy User Credentials	Get IDCS user access token	Retrieves the user access token for use in other tests.
	Verify IDCS and Fusion Service integration	Verifies the Identity Cloud Service and Fusion Service Integration.
	Verify anonymous proxy user setup	Verifies the Anonymous Proxy User setup.
	Verify customer self-service proxy user setup	Verifies the Customer Self-Service Proxy User setup.
	Verify customer self-service proxy account administrator setup	Verifies the Customer self-service proxy account administrator setup
	Get categories as anonymous user	Verifies the categories are available to an anonymous user

Run pre validation setup in IDCS

1. Sign in to IDCS as the Administrator user.
2. Click the Navigation drawer and then expand the **Applications** list.
3. Search for **Proxy User Data Service App** and select it.
4. Select the **Configure** tab, and expand the **Client Configuration** menu item.
5. In the Authorization area, select the **Resource Owner** along with the already selected **Client Credentials** option for Allowed Grant Types.
6. Click the **Test Results** step.

Run validations tests in Fusion Service

1. Sign in to Fusion Service as an administrator or setup user.
2. In the Setup and Maintenance work area, go to the following:
   - Offering: Service.
   - Functional Area: Digital Customer Service.
   - Task: Validate Self-Service Optimization Setup for Digital Customer Service.

     > **Note:** To show this task, you might need to select **All Tasks** from the **Show** drop-down list.
3. On the **Select Test** page, select the tests that you'd like to run.

   If a given test request requires parameters, the **Supply Parameters** step will be enabled.
4. If required, enter parameters in the **Value** field on the **Supply Parameters** page.

   > **Note:** The **Supply Parameters** step is only enabled if parameters are required for the chosen test.
5. Click the **Test Results** step.

The tests are automatically run and the results displayed. You can return to the **Select Test** page as often as necessary until you've fully performed your validations.

Run post validation tests in IDCS

1. Sign in to IDCS as the Administrator user.
2. Click the Navigation drawer and then expand the **Applications** list.
3. Search for **Proxy User Data Service App** and select it.
4. Select the **Configure** tab, and expand the **Client Configuration** menu item.
5. In the Authorization area, deselect the **Resource Owner** option for Allowed Grant Types.

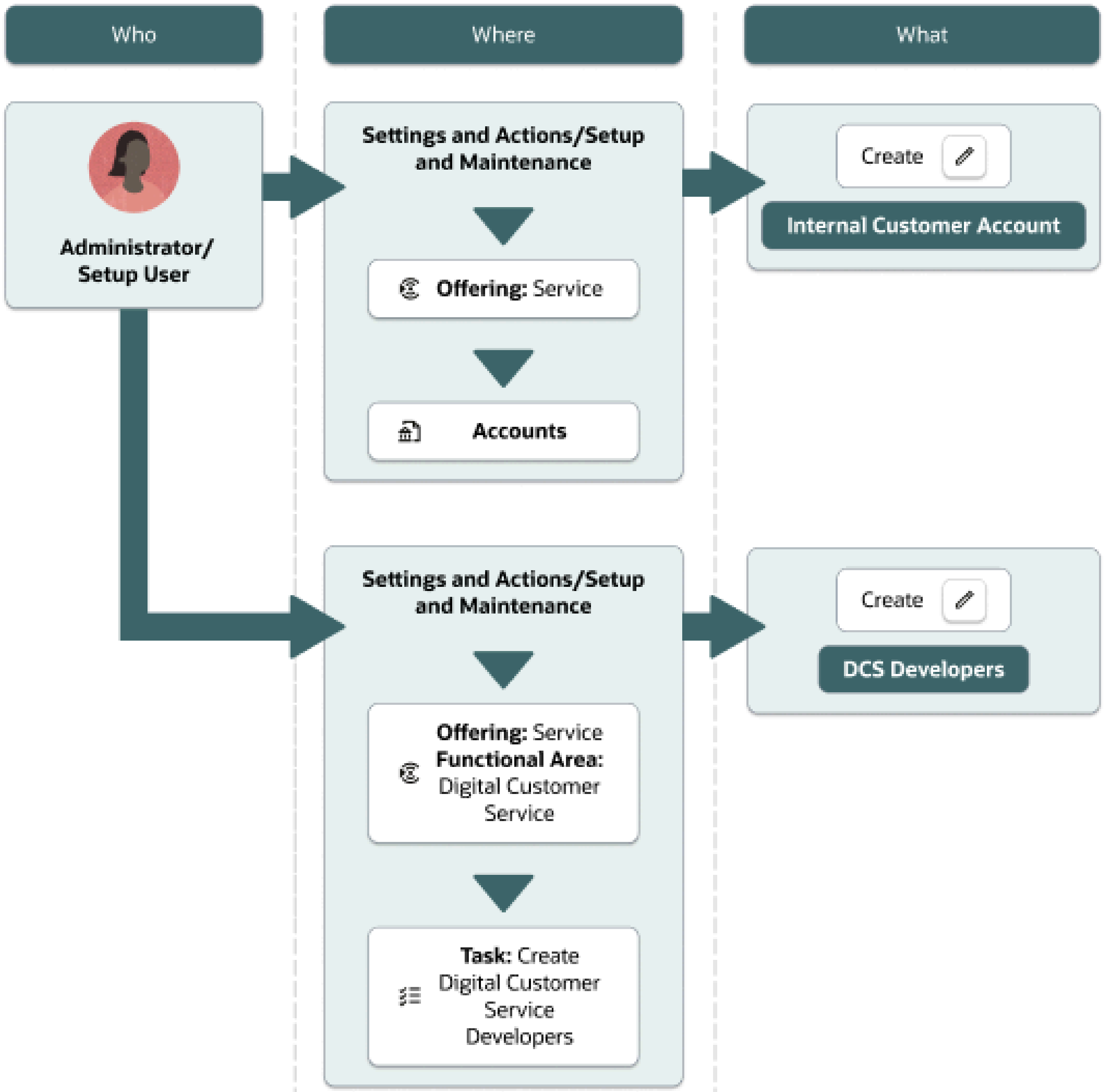
Set up Administrators and Developers

Overview of setting up Administrators and Developers for DCS

Here's a list of the steps required to set up administrators and developers for Digital Customer Service.

- *What are the Digital Customer Service Developer roles?*
- *Create an Internal Customer account*
- *Create Digital Customer Service Developers*

4. Setup Administrator and Developers



What are the Digital Customer Service Developer roles?

To work with business objects relevant to Digital Customer Service, the developer must be a Digital Customer Service user and must be granted the appropriate roles. Here are thee tasks you'll need to perform:

1. Create an Internal Customer Account (This task only needs to be done once). *Create an Internal Customer account*.
2. Register the Developer as a Self-Service User. *Create an Internal Customer account*.
3. Add User Roles. *Add Visual Builder roles*.

Create an Internal Customer account

Before creating the Digital Customer Service developer or administrator users, an internal customer account must be created for these users.

The internal customer account lets you associate your staff to a specific account. An account key is required when creating a new Digital Customer Service user.

> **Note:** You only need to create the internal customer account once. This internal customer account can be used by all Developers and Administrators.

To create an internal customer account:

1. Sign in to Oracle Fusion Service.
2. Navigate to the **Service** work area and click **Accounts**.
3. Click **Create Account**.
4. Enter the **Name**.

   > **Note:** The name that you enter in this field represents the **AccountKey** that you need to use in the Create Digital Customer Service Developers topic. This is true only if the value of the profile option SVC_CSS_ACCT_KEY_FIELD hasn't been changed.

5. Select **Customer** from the **Type** menu.
6. Click **Save and Close**.

Create Digital Customer Service Developers

Here's how you create Digital Customer Service Developer users.

1. Sign in to Oracle Fusion Service as an administrator or a setup user.
2. Click the Settings and Actions menu, and select **Setup and Maintenance**.
3. In the **Setup and Maintenance** work area, go to the following:
   - Offering: Service
   - Functional Area: Digital Customer Service
   - Task: Create Digital Customer Service Developers

> **Note:** To access this task, click the **Show** drop-down list, and select **All Tasks**.

4. In the Create Developers for Digital Customer Service page, fill in each field.

   The default value of the account key is the account name you created in *Create an Internal Customer account* . You're encouraged to make the account key more secure by creating a custom account key here: *Create a custom Account Key field*.

   > **Note:** The sign in ID is optional. To use your email address as the sign in ID, just click the check box.

5. Click **Save** when you're finished.

   The user account is created in both Fusion Service and IDCS. You'll then receive an email from IDCS prompting you to reset your password.

Create a custom Account Key field

Use this topic to create a custom Account Key field for Digital Customer Service.

The value of the new Account Key field must be unique to each account and can be set to any value. If the value is set to a string that's easy to guess then someone could guess the value and create for themselves a user account. This is a particular problem if automatic approval is set to true. If the account key is set to a string that's difficult to guess then only those to whom the string is sent can successfully submit a registration request.

End user customers are required to have a known account key. Users must also specify an appropriate account key when they register for a self-service user account.

Multiple tasks must be completed to create a custom Account Key field for Digital Customer Service. To create a custom Account Key field for Digital Customer Service, complete these tasks in the order that they appear in this topic:

1. Add the Account Key to the Account Object
2. Add the Account Key to Pages
3. Populate the Account Key for Existing Accounts
4. Publish the Sandbox
5. Set a Profile Attribute for the Account Key

Add the Account Key to the Account Object

To add a custom field for the Account Key to the Account object, you'll need to use the Application Composer in Oracle Fusion Service.

1. Sign in to Oracle Fusion Service as an administrator or a setup user.
2. Create a sandbox for adding the Account Key field:
   a. Click **Navigator > Configuration > Sandboxes**.
   b. Click the **+** icon (**New**) to create the new sandbox.

      The **Create Sandbox** dialog appear.
   c. Enter a name in the **Sandbox Name** field.
   d. Click **Save and Close**.

      A confirmation dialog appears.
   e. In the **Manage Sandboxes** list, click the line item with the sandbox name that you specified in step c.

   f. Click **Set as Active**.
3. Navigate to the **Application Composer**.
4. Expand **Objects**, then **Standard Objects**, then **Account**, and then click **Fields**.

   The **Select Field Type** page appears.
5. Click the **Action** menu, and select **Create**.

   The **Select Field Type** dialog appears.
6. Click the **Text** option, then click **OK**.

   The **Create Text Field** page appears.
7. Specify the following for the Account Key text field options:
   - In the **Display Label** field, enter the following string:

     `Account Key`
   - The **Name** field will be pre populated based on the name that you entered for the **Display Label**, without any spaces.
   - The **API Name** field will be pre populated based on the name that you entered for the **Display Label**, without any spaces, and typically with the following suffix: `_c`

     > **Tip:** You'll need to note the value assigned to the **API Name** field, because it will be assigned to the `SVC_CSS_ACCT_KEY_FIELD` profile option in the Set a Profile Attribute for the Account Key task, later in this topic.

   - In the **Display Type** option, click the **Simple Text Box** option.
   - Deselect the **Required** option in the **Constraints** section.
   - Select the **Updatable** option in the **Constraints** section.
   - Select the **Searchable** option in the **Constraints** section.
   - Select the **Include in Service Payload** option in the **Constraints** section.
8. Click **Save and Close**.

Add the Account Key to Pages

In this task, you'll add the Account Key field that you created in the previous task to the necessary pages in the Oracle Fusion Service Application Composer.

1. Sign in to Oracle Fusion Service as an administrator or a setup user.
2. Navigate to the **Application Composer**.
3. Expand **Objects**, then **Standard Objects**, then **Account**, and then click **Pages**.

   The **Account: Pages** page appears.
4. In the **Creation Page Layouts** section, select a layout to base your page on, such as **Standard layout**.
5. In the **Creation Page Layouts** section, click the **Actions** menu, and select **Duplicate**.

   The **Duplicate Layout** dialog appears.
6. Enter a name in the **New Layout Name**.
7. Click **Save and Edit**.
8. Click the **Pencil** icon (**Edit**) next to `FUSE Customer ObjectCreation View.`
9. The **Creation Layout** page appears.
10. From the **Available Fields** column, click the `AccountKey` field that you created in the previous task, then click the arrow to move it to the **Selected Fields** column.

11. Click **Save and Close**.
12. Click the `AccountKey` link, then set the following options on the **Edit UI Properties** dialog:
    - Set **Required** to **No**.
    - Set **Updatable** to **Yes**.
    - Set **Hidden** to **No**.
13. Click **Save and Close**.
14. Click **Done**.
15. In the **Details Page Layouts** section, click the **Actions** menu, and select **Duplicate**.
    The **Duplicate Layout** dialog appears.
16. Enter a name in the **New Layout Name**.
17. Click **Save and Edit**.
18. In the **Subtabs Region**, click the **Profile** subtab.
19. Click the **Pencil** icon (**Edit**) next to `SummaryEdit Summary Subtab`.
    The **Details Layout Edit Summary** page appears.
20. From the **Available Fields** column, click the **Account Key** field that you created in the previous task, then click the arrow to move it to the **Selected Fields** column.
21. Click **Save and Close**.
22. Click the **Account Key** link.
    The **Edit UI Properties** dialog appears.
23. Set **Required** to **Expression**, then click the `xyz` next to the **Required** field.
    The **Advanced Expression** dialog appears.
24. In the **Edit Script** text box, add the following expression:

    ```
    if (SalesProfileType == "ZCA_CUSTOMER") {return true} else {return false}
    ```

    > **Note:** This makes the Account Key required if the **Account Type** is **Customer**. Self-service registration only works for **Customer** accounts.

25. Click **OK**.
26. Set **Updatable** to **Yes**.
27. Set **Hidden** to **Expression**, then click the `xyz` next to the **Required** field.
    The **Advanced Expression** dialog appears.
28. In the **Edit Script** text box, add the following expression:

    ```
    if (SalesProfileType != "ZCA_CUSTOMER") {return true} else {return false}
    ```

    > **Note:** This hides the field if it's not a **Customer** account type.

29. Click **OK**.
30. Click **Save and Close**.

Populate the Account Key for Existing Accounts

If you already have existing Customer accounts, you'll need to edit the accounts, and add the required Account Key field.

> **Note:** Make sure to assign unique values to each account.

1. Sign in to Oracle Fusion Service as an administrator or a setup user.
2. Navigate to **Accounts**.
3. Search for, then select the account.

   The **Edit Account** dialog appears.
4. In the **Account Key** field, enter a value that uniquely identifies the Customer account.
5. Click **Save and Close**.
6. Repeat steps 3-5 for all previously existing Customer accounts.

Publish the Sandbox

To ensure that the configuration that you applied in the previous tasks takes effect, you must now publish the sandbox.

1. Sign in to Oracle Fusion Service as an administrator or a setup user.
2. Click **Navigator > Configuration > Sandboxes**.
3. Select the name of the sandbox created in step 2 of the Add the Account Key to the Account Object task.

   The **Sandbox Details** dialog appears.
4. Click **Publish**.

Set a Profile Attribute for the Account Key

The account key is used to uniquely identify an account, and is decided by the value assigned to the SVC_CSS_ACCT_KEY_FIELD profile option.

By default, the SVC_CSS_ACCT_KEY_FIELD profile option is set to the **organizationName** field, which appears as **Name of the Account** in the Oracle Fusion Service User Interface for account management. You must create an attribute to be the account key: the default account key of **organizationName** isn't secure because it can be easily guessed.

You must set the `svc_css_ACCT_KEY_FIELD` profile option to the **API Name** field of the Account Key created in step 7 of the Add the Account Key to the Account Object task in this topic.

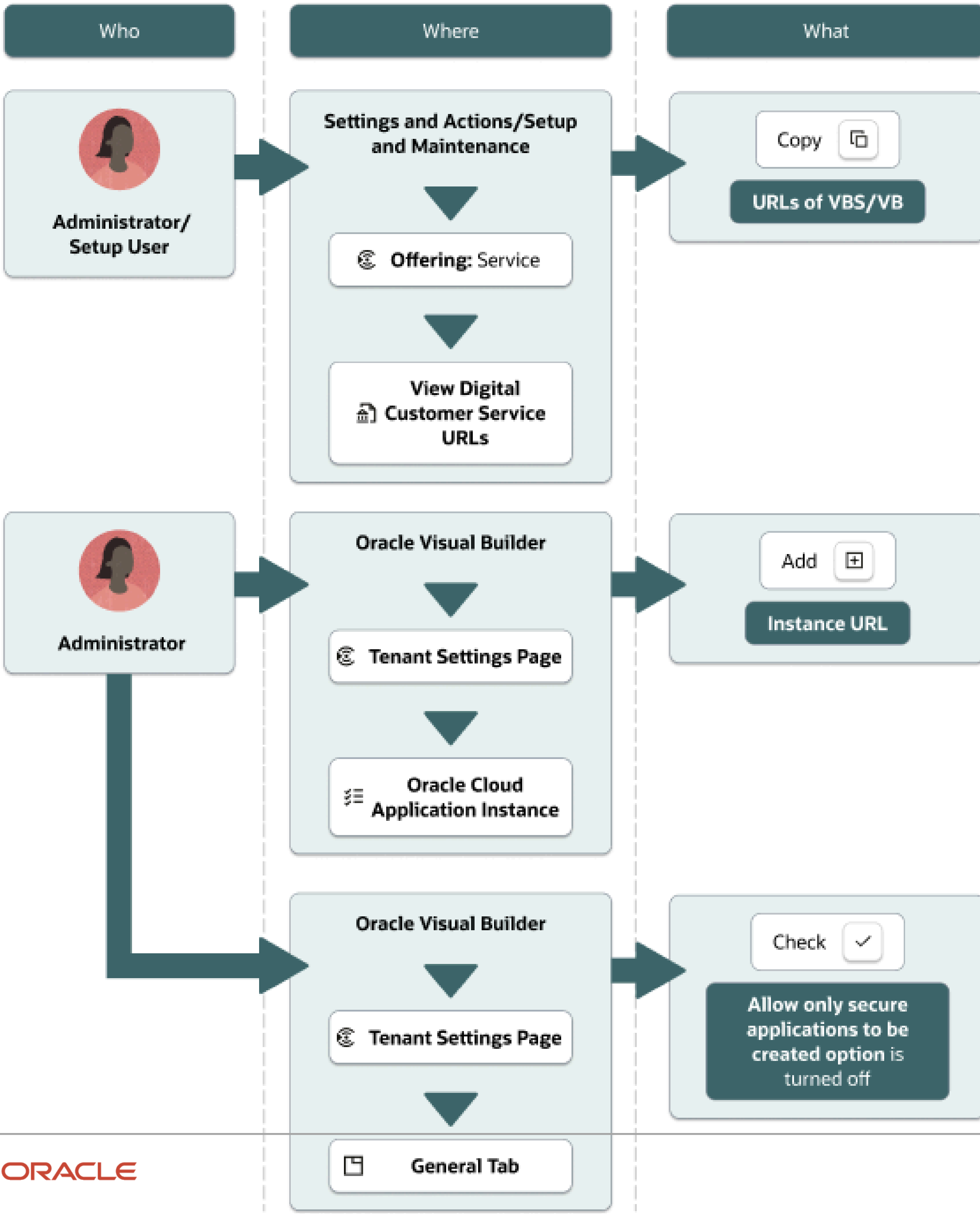
Set up Oracle Visual Builder

Overview of steps for setting up Visual Builder for DCS

Here's a list of the steps required to set up Visual Builder for Digital Customer Service.

- *Retrieve the Oracle Visual Builder URLs*
- *Specify the Fusion Service Details in Oracle Visual Builder*
- *Verify Your Oracle Visual Builder Settings*

5. Set up Oracle Visual Builder



Retrieve the Oracle Visual Builder URLs

You must have access to Oracle Visual Builder to perform setup tasks for Visual Builder.

Use these steps to find URLs for:

- Oracle Visual Builder. Use for your application development and its lifecycle. VBCS has a 1:1 mapping with the Fusion Service Production, Test and Development environments.
- Oracle Visual Builder Studio (optional). You can use Visual Builder Studio for source control and to build pipelines. You can integrate VB Studio with Visual Builder.

> **Note:** Only 1 instance of VB Studio is provisioned for each Cloud Account and is associated with the **Test Fusion Service** instance.

1. Sign in to Fusion Service as an administrator or setup user.
2. In the Setup and Maintenance work area, go to the following:

- Offering: Service.
- Functional Area: Digital Customer Service.
- Task: View Digital Customer Service URLs.

> **Note:** To view the task, select **All Tasks** from the **Show** drop-down list.

1. In the View Digital Customer Service URLs page, copy the URLs by finding the entry or either:
    a. Oracle Visual Builder
    b. Oracle Visual Builder Studio
2. When you've found the entry you want, click the **Copy** button.

Configure Source Control for Applications

Configuring Git for source control of your application is optional.

1. In Visual Builder Studio, set up a Git repository.

    > **Note:** For groups that will be collaborating, when you're creating your project, select the **Shared** option when defining **Security**.

    > **Note:** It's recommended that you create a branch for each developer to enable your developers to work independently and then merge to the main branch when they want their changes to be shared.

2. In Oracle Visual Builder, integrate your application with a Git repository.

Specify the Fusion Service Details in Oracle Visual Builder

To specify Fusion Service details in Oracle Visual Builder:

1. Sign into Oracle Visual Builder as an administrator.
2. Click the **Menu** icon, and select **Settings** to open the Tenant Settings page.
3. Click the Services tab, then click the **Back ends** icon (**+**)
4. In the Back end Service Type window, select **Oracle Cloud Application Instance**.
5. In the Instance URL field of the Create Oracle Cloud Application Instance window, enter the instance URL of your Fusion Service back end service.
6. From the Authentication drop-down list, select **Oracle Cloud Account**.
7. Click **Create**.

   Note: You must set the Instance URL field with the fully qualified domain name of your Oracle Applications Cloud Fusion Service instance.

Verify Your Oracle Visual Builder Settings

Here's how to verify your Oracle Visual Builder settings:

1. Sign in to Oracle Visual Builder as a Service Administrator.
2. Click the **Home** menu.
3. Click **Settings**.

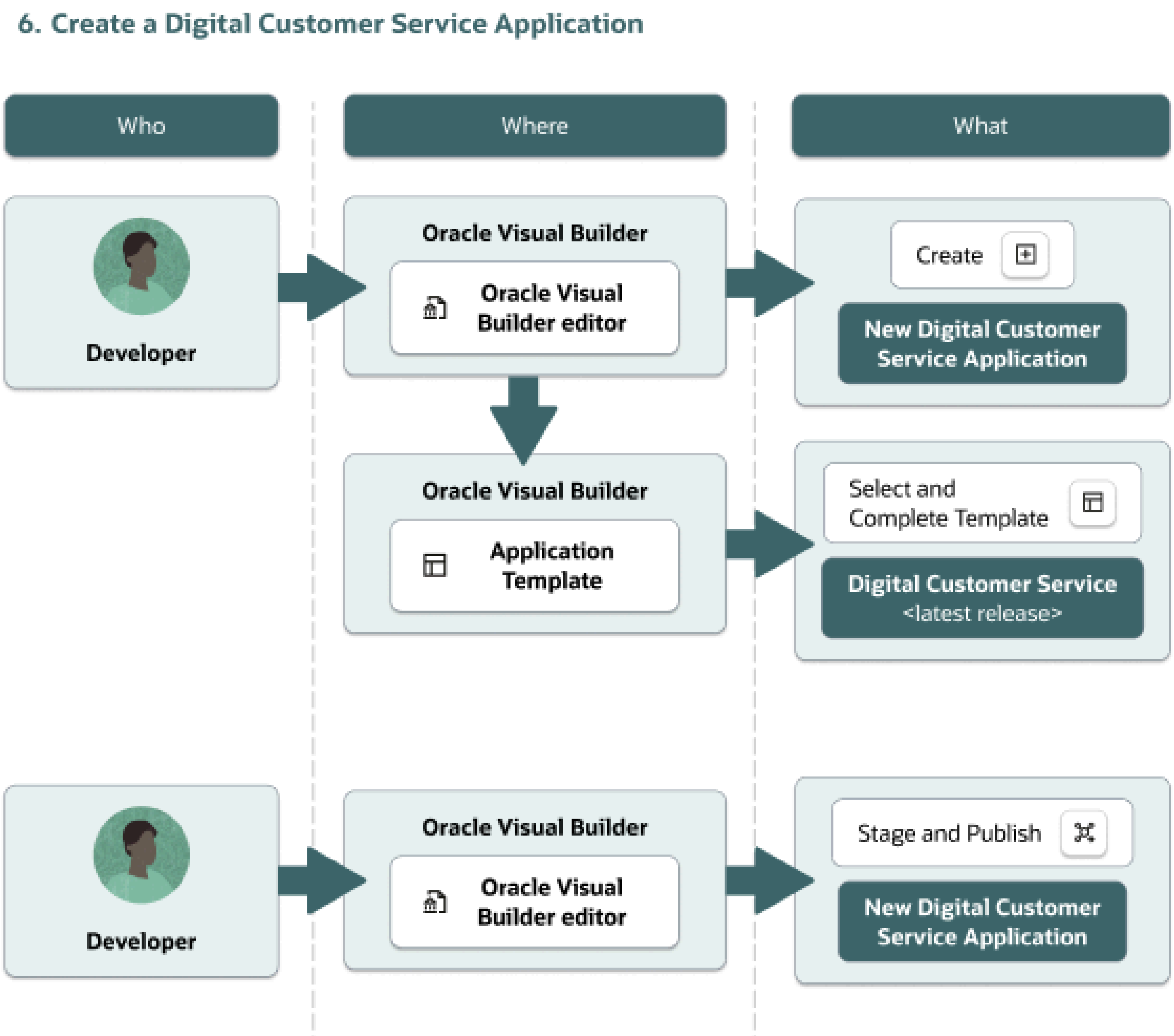
   The **Tenant Settings** screen appears.
4. On the **General** tab, find the **Allow only secure applications to be created** option, and ensure that it's turned off.

Create a Digital Customer Service Application

Overview of steps to create a Digital Customer Service application

Here's a list of the steps required to create a Digital Customer Service application.

- *Create a New Digital Customer Service application*
- *Stage and Publish the Digital Customer Service application*



Create a New Digital Customer Service application

The steps that follow assume that you've selected the current Reference Implementation template.

1. Sign in to the Oracle Visual Builder editor as a user with the Developer role.

2. Click **New**.

   > **Note:** If no applications have been created yet, the button will read **New Application**.

   The **Create Application** dialog appears.
3. In the **Application template** section, click **Change template**.
4. Click the newest reference implementation tile which will match the Fusion Service version you're using.

   This template creates an application with basic service functionality, including the ability to create and update SRs, search knowledge, and chat with an agent.
5. Click **Select**.
6. Specify the **Application Name**.
7. Specify the **Application ID**.

   The **Application ID** is automatically derived from the specified Application Name, but you can change it, if desired. The Application ID can't be changed once the application is created: it appears in the application URL.
8. Click **Finish**.

   Once the Digital Customer Service application has been created, you're now ready to configure the application to meet your business needs.

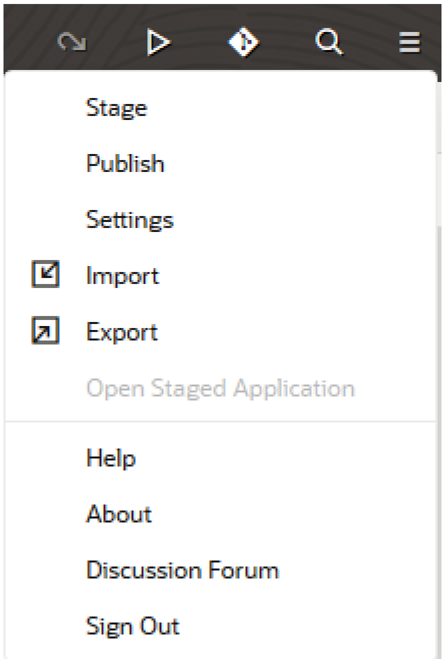
> **Note:** When Oracle Fusion Service is deployed with multiple business units, more configuration is required.

> **CAUTION:** For your Digital Customer Service Reference Implementation template to work properly, access to Knowledge and Chat must be allowed anonymously. Your Oracle Visual Builder settings must to be configured to allow publicly accessible applications to be created. To verify the settings, do the following:
> 1. Open the application artifact and select the Settings editor in the Designer.
> 2. Open the Security tab and then, in the Access pane, select **Allow anonymous access**.

Stage and Publish the Digital Customer Service application

You can preview your changes as you develop them by clicking the **Preview** button.

Test that your changes perform as expected by staging the application. Access the **Stage** option by clicking the **Menu** button from the Visual Builder home page as shown in the following example:



Staging your application enables you to test each update you make to confirm that it acts as you expect and that no problems have been introduced, for example, when you add new features or change your data model.

When you publish a version of your application, it becomes read-only and can no longer be changed. To make changes or updates to your application, you need to create a new version. When you publish a staged version of your application, it becomes the active version.

> **Note:** After staging and publishing the application you must use the Self-Service user. The Developer user is only applicable when the application is in Preview mode.

If you're updating an earlier version of your application, the previous active version is archived and locked. Only one version of an application can be active at a time, but multiple versions of an application can be staged simultaneously.

User Registration

User personas

You can create Digital Customer Service users in IDCS, and grant different roles to them. You can then map these users to records in Fusion Service to assign Data Privileges to them. Here are the user personas used in Digital Customer Service:

Customer Self-Service User: This role grants the following privileges:

- View and edit service requests created by the user.
- Create service requests.
- View and update work orders on which the user is the contact.
- View interactions on which the user is the primary contact.

Customer Self-Service Account Manager: This role grants the following privileges:

- View and edit all service requests.
- View and edit all work orders for a specific customer account.
- Create service requests.

Customer Self-Service Account Administrator: This role grants the following privileges:

- View and approve registration requests in the customer account for which they're the Account Administrator.
- Assign and remove the Account Administrator and Account Manager roles.

Roles	Functional Privileges	Data Privileges
User	• Edit service requests created by the user. • Create service requests. • Update work orders on which the user is the contact.	• View service requests created by the user. • View work orders on which the user is the contact. • View interactions on which the user is the primary contact.
Account Manager	• Edit all service requests. • Edit all work orders for a specific customer account. • Create service requests	• View all service requests. • View all work orders for a specific customer account.
Account Administrator	• Approve registration requests in the customer account for which they're the Account Administrator. • Assign and remove the Account Administrator and Account Manager roles.	• View registration requests in the customer account for which they're the Account Administrator.

Security Model

Security model

Contact records created in Fusion Service and users created in IDCS, map to a few proxy users that are created during initial setup.

The proxy users define the functional privileges that are accessible to the users.