Oracle® Cloud

Administering Oracle Visual Builder

E73612-16
September 2019

Oracle Cloud Administering Oracle Visual Builder,

E73612-16

Primary Author: Oracle Corporation

Contents

1 Preface

Describes tasks for administrators of Oracle Visual Builder.

Audience

Administrator's Guide for Oracle Visual Builder Cloud Service is intended for administrators who will set up and configure the service.

Related Resources

For more information, see these Oracle resources:

- Oracle Public Cloud

  `http://cloud.oracle.com`
- About Oracle Visual Builder in *Developing Applications with Oracle Visual Builder*
- About Oracle Cloud in *Getting Started with Oracle Cloud*

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

2
Getting Started

To set up an Oracle Visual Builder service, tasks such as creating service instances and user accounts need to be performed by Oracle Cloud service administrators with specific roles. If you are a Visual Builder administrator you might not have sufficient privileges to perform the tasks described in this section, but you should be familiar with the steps for setting up the service and the various roles, processes and tools for administering Oracle Cloud services and users.

Topics

Set Up Oracle Visual Builder

Here are the steps for signing up for an Oracle Visual Builder promotion or subscription and creating a service instance:

1. Sign up for a free credit promotion or purchase a subscription. See Requesting and Managing Free Oracle Cloud Promotions or Buying an Oracle Cloud Subscription in *Getting Started with Oracle Cloud*.

   After you sign up for an account you will receive an email message with details about your Oracle Cloud account and how to access your services.

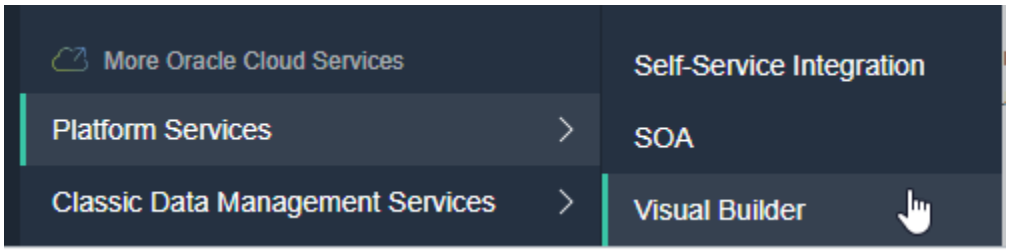
   > **Note:**
   >
   > After signing up, it typically takes approximately 30 minutes before your services are available in the Oracle Cloud Infrastructure Console. You can start creating instances after your services are available.

2. Sign in to Oracle Cloud.

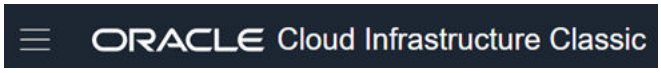
   If you received a welcome email, use it to identify the URL, your user name, and your temporary password. After signing in, you will be prompted to change your password.

3. On most Oracle Cloud accounts, you access the Oracle Visual Builder console from the Oracle Cloud Infrastructure Console. On some older Oracle Cloud accounts, you access the Oracle Visual Builder console from the Oracle Cloud Infrastructure Classic Console.

   - From the Infrastructure Console, click the navigation menu in the top left corner, expand **Platform Services**, and then click **Visual Builder**.



- From the Infrastructure Classic Console, click the navigation menu in the top left corner, and then click **Visual Builder**.



4. When you access the Oracle Visual Builder console the first time, you see the Welcome page. Click **Instances**.
5. From the Instances page, you can create a new Oracle Visual Builder, or you can click an existing instance to view or manage it.
6. Provision your service instance. See Create Your Service Instance.
7. Create accounts for your users and assign them appropriate privileges and roles. See Add Users and Assign Roles.

3

Create Your Service Instance

After subscribing to Oracle Visual Builder, you can provision instances of Oracle Visual Builder using the Quick Start or using the custom template.

Topics:

Create a QuickStart Instance with a Single Click

After you sign up for your Oracle Cloud account and your services are available, you can create a QuickStart instance of Oracle Visual Builder with a single click from the Oracle Visual Builder console. A QuickStart instance does *not* include or support the creation of an Oracle Storage Cloud Service container. Without a container, database backups are not possible.

When your services are available, a link for creating a new instance is provided in the Oracle Visual Builder console. If you have already created some services for your account it might be more convenient for you to access the page for creating instances from the Dashboard in the Oracle Visual Builder console.

This QuickStart template automatically creates an instance with the following features:

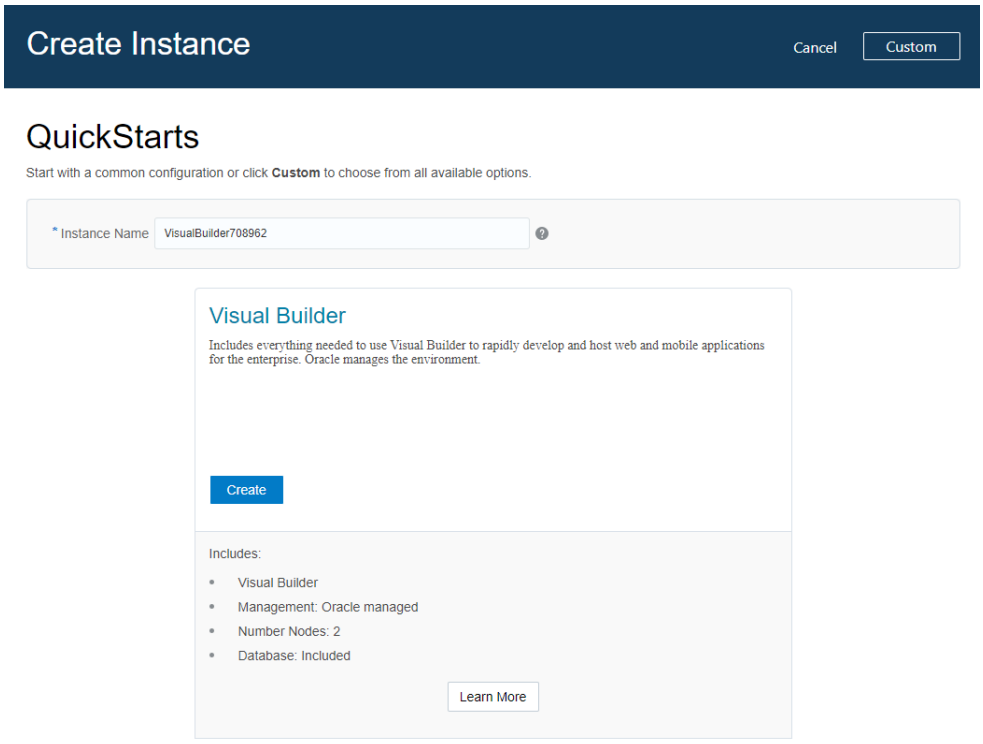
- Oracle Visual Builder.
- Oracle-managed instance.
- Two-node cluster.
- An embedded database.

This instance does *not* include or support the use of an Oracle Storage Cloud Service container. On the overview page for the provisioned instance there is no Backup tab.

To create new instances using QuickStarts:

1. Sign in to Oracle Cloud.
2. From the Infrastructure Console, click the navigation menu in the top left corner, expand **Platform Services**, and then click **Visual Builder**.
3. Click **QuickStarts** at the top of the Instances page.

   The Create Instance page contains a field where you enter the name of the new instance and a description of the features of the QuickStart instance.



4. Type the instance name in the **Instance Name** field. Click **Create**.

   If you do not change the default generated value for the Instance Name, you will encounter an error when you attempt to create the instance.

5. Wait for the instance creation process to finish.

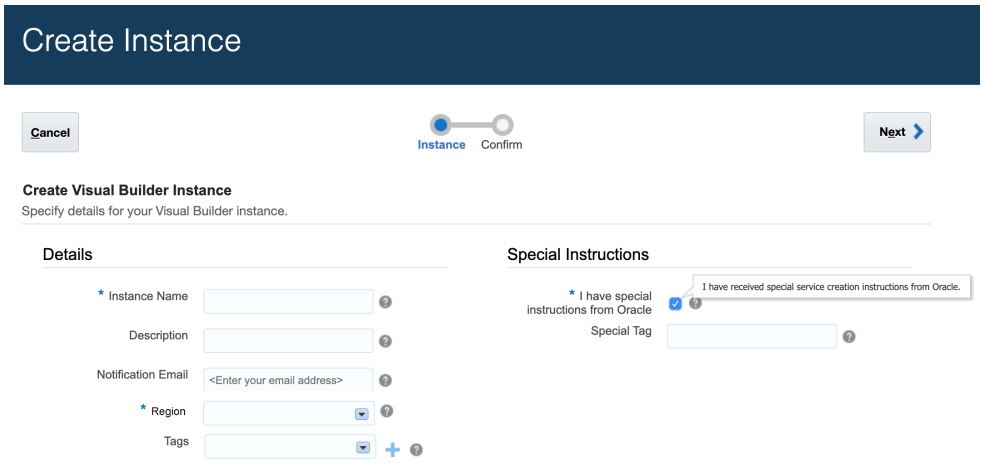
Create a Custom Instance

You can get started quickly by using a brief template that provides you with a pre-provisioned Oracle Visual Builder instance.

To create an instance:

1. Sign in to Oracle Cloud.
2. From the Infrastructure Console, click the navigation menu in the top left corner, expand **Platform Services**, and then click **Visual Builder** to open the Instances page.

   The Instances tab displays a list of your service instances and the resources allocated to the instances. If you do not have any service instances you will see a message with links to information on creating an instance.
3. Click **Create Instance** to open the Create Instance page.



4. In the Details section:
   a. Specify the Instance Name, Description and Notification Email.
   b. Select the compute region from which to perform the installation.
   c. Select or define tags for the service instance.
5. In the Special Instructions section:
   a. Select the **I have special instructions from Oracle** checkbox if you have received a special code from Oracle after filing a Service Request (SR). In some atypical circumstances, Oracle may provide you with a special code to be used during the automated provisioning flow. If you have been issued a special provisioning code, select the checkbox, and enter the code exactly as provided to you.
   b. In the Special Tag field, enter the special code that Oracle communicated to you through the SR that you filed.
6. Click **Next**, confirm your selections, then click **Create**.

   When the instance is ready to use it appears in the Oracle Visual Builder console.

4

Add Users and Assign Roles

User roles define the privileges available to a user and the tasks that the user can perform. You can grant users various roles to enable them to access, administer, and use Oracle Visual Builder.

Topics:

Oracle Visual Builder Roles and Privileges

A role includes privileges that allow users to perform various tasks. All Oracle Cloud services have some predefined roles for performing tasks when setting up, administering, managing, and using a service. There are predefined roles for the PaaS layer, the application layer and Oracle Visual Builder.

The PaaS-layer roles govern access to WebLogic Server. The application-layer predefined roles include ServiceAdministrator, ServiceMonitor, ServiceDeveloper, ServiceDeployer, and ServiceUser, but only some of these roles are used and mapped to the predefined roles used in Oracle Visual Builder. To perform tasks in Oracle Visual Builder, the user must be assigned to one of the Oracle Visual Builder predefined roles. Users can hold multiple roles depending on their responsibilities. For example, a user might be granted both the ServiceAdministrator and ServiceMonitor roles, but any privileges granted by the role of ServiceMonitor are ignored in Oracle Visual Builder.

Predefined Roles in PaaS and Application Layers

The following table describes the predefined roles available in the PaaS layer and the application layer.

Predefined Roles	Description
PaaS-Layer Predefined Roles	Govern access to WebLogic Server
Administrators	A user with the Administrators role can: • View the server configuration, *including* the encrypted value of some encrypted attributes • Modify the entire server configuration • Deploy Enterprise Applications and Web application, EJB, Java EE Connector, and Web Service modules • Start, resume, and stop servers

Predefined Roles	Description
Deployers	A user with the Deployers role can: • View the server configuration, including *some* encrypted attributes related to deployment activities • Change startup and shutdown classes, Web applications, JDBC data pool connections, EJB, Java EE Connector, Web Service, and WebLogic Tuxedo Connector components. If applicable, edit deployment descriptors. • Access deployment operations in the Java EE Deployment Implementation (JSR-88)
Monitors	A user with the Monitors role can: • View the server configuration, *except* for encrypted attributes • Get read-only access to WebLogic Server Administration Console, WLST, and MBean APIs
Operators	A user with the Operators role can: • View the server configuration, *except* for encrypted attributes • Start, resume, and stop servers
Application-Layer Predefined Roles	Govern access to the various Oracle Visual Builder features:
ServiceAdministrator	A user with the ServiceAdministrator role is a super user who can manage and administer the administrator settings of an Oracle Visual Builder instance.
ServiceMonitor	This role is not used in Oracle Visual Builder
ServiceDeveloper	A user with the ServiceDeveloper role can develop applications in an Oracle Visual Builder instance.
ServiceDeployer	This role is not used in Oracle Visual Builder.
ServiceUser	A user with the ServiceDeployer role has privileges to utilize only the basic functionality of a feature such as access to the staged and published applications.

Privileges Available to Roles in Oracle Visual Builder

There are three predefined roles in Oracle Visual Builder, and these roles are mapped to specific application-layer roles. The following table lists Oracle Visual Builder predefined roles and the tasks that users granted those roles can perform.

Oracle Visual Builder Predefined Role	Mapped Role	Tasks Users Can Perform in Oracle Visual Builder
Visual Builder Administrator	ServiceAdministrator	A user with this role can: • Use the visual design tool • Create, manage, and change the owners of applications • Create associations with other services • Configure security options for applications in an instance • Specify error messages for Access Denied pages
Visual Builder Developer	ServiceDeveloper	A user with this role can: • Use the visual design tool • Create, manage, secure, and publish web and mobile applications • Design pages, work with business objects, build and test applications

Oracle Visual Builder Predefined Role	Mapped Role	Tasks Users Can Perform in Oracle Visual Builder
Visual Builder User	ServiceUser	A user with this role can only access staged and published applications. The default permission is enforced only when the service administrator adjusts security settings for the entire service instance to restrict all access to runtime applications to the users granted this role.

Add Users to a Cloud Account with IDCS

If you are using an Oracle Cloud Account with Oracle Identity Cloud Service (IDCS), then you can use Users tab on the Oracle Visual Builder console to access the features of IDCS to manage users and security for your Oracle Cloud services.

Topics:

Add Users

After Oracle Visual Builder is provisioned, you need to create the required user accounts in the identity domain of your Oracle Visual Builder instance.

Only a user with the Identity Domain Administrator role or the User Administrator role through delegated administration can create user accounts. When Oracle Visual Builder is provisioned, the Identity Domain Administrator account gets created in addition to the roles described in Oracle Cloud User Roles and Privileges in *Getting Started with Oracle Cloud*.
To add a user account, you need to know the first name, last name, and email address of the user.

1. Sign in to Oracle Cloud.
2. From the Infrastructure Console, click the navigation menu ☰ in the top left corner, expand **Platform Services**, and then click **Visual Builder** to open the Instances page.
3. In the Oracle Visual Builder console, click **Users**.
4. On the User Management page in the Oracle Visual Builder console, click **Identity Console**.
5. On the User Management page in the Oracle Identity Cloud Service console, click **Add**.
6. In the **First Name** and **Last Name** fields of the Add User dialog, enter the user's first and last name.

   To have the user log in to Oracle Visual Builder with their email address:

   a. Leave the **Use the email address as the user name** check box selected.

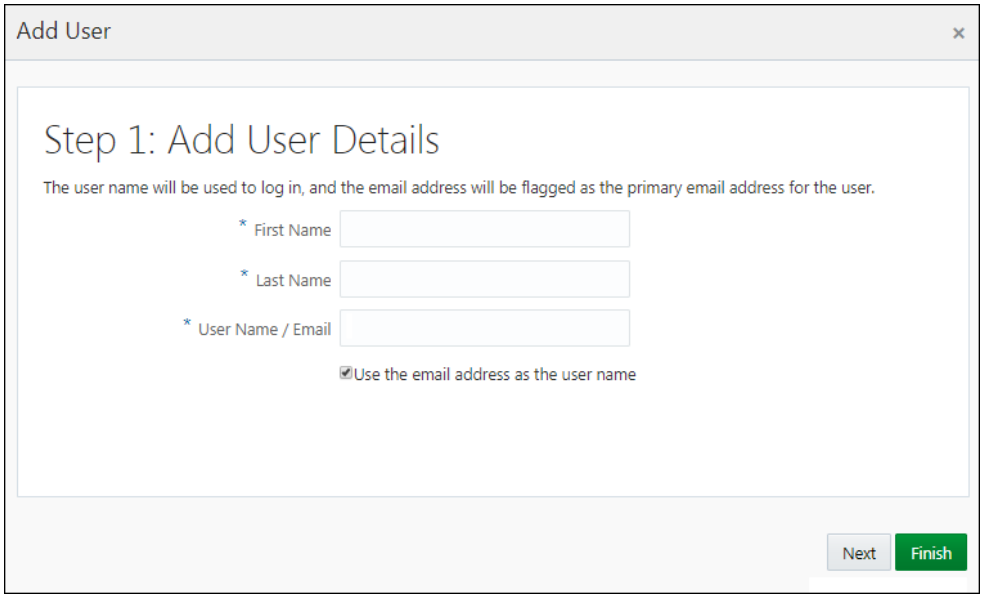
   b. In the **User Name/Email** field, enter the email address for the user account.

   To have the user log in to Oracle Visual Builder with their user name:

a. Clear the **Use the email address as the user name** check box.

b. In the **User Name** field, enter the user name that the user is to use to log in to the Oracle Identity Cloud Service console.

c. In the **Email** field, enter the email address for the user account.



7. To assign the user account to a group, click **Next**. Otherwise, click **Finish**.

8. In the **Add User** window, select the check box for each group that you want to assign to the user account. Click **Finish**.

After the user account is created, the user receives an email with the sign-in credentials.

You can activate user accounts, import user accounts, and create groups and assign users to various groups, as described in Managing Oracle Identity Cloud Service User Accounts in *Administering Oracle Identity Cloud Service*.

Assign Roles to Users

The Identity Domain Administrator must assign roles to users to specify the tasks they can perform in Oracle Visual Builder. A user can have more than one role.

The role assigned to the user determines the privileges and tasks the user can perform in Oracle Visual Builder. See Oracle Visual Builder Roles and Privileges for a description of the various predefined roles available in Oracle Visual Builder.

1. Sign in to Oracle Cloud.

2. From the Infrastructure Console, click the navigation menu ☰ in the top left corner, expand **Platform Services**, and then click **Visual Builder** to open the Instances page.

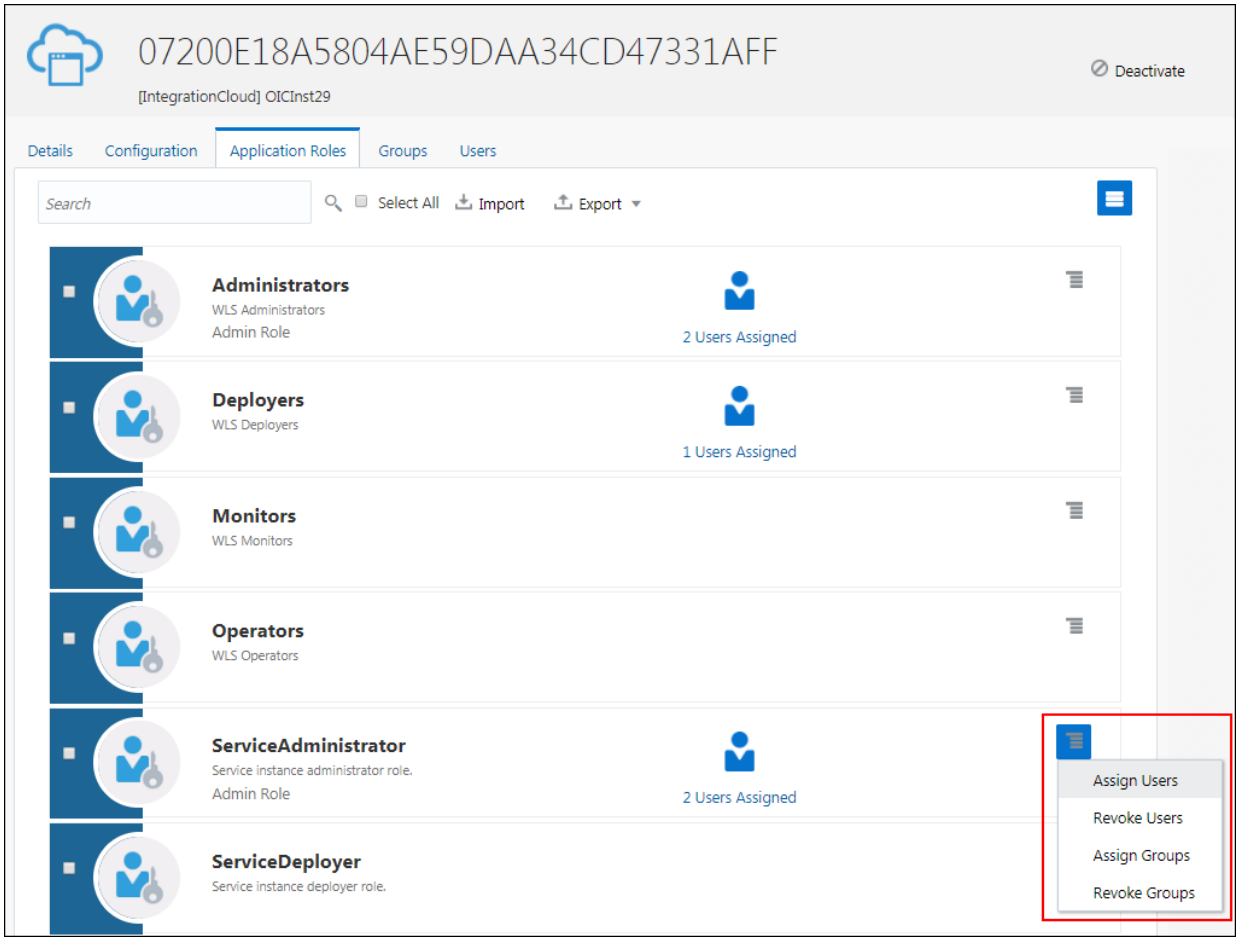
3. From the Oracle Visual Builder console, click **Users** and **Identity Console** to navigate to the Oracle Identity Cloud Service console.

4. From the Oracle Identity Cloud Service console, click the navigation menu ☰ in the top left corner, and then click **Applications**.

5. Click the link for your Oracle Visual Builder instance.

You can use the filter to help you locate your instance. For Oracle Visual Builder instances you might want to search for the name of your instance appended with “vb” (for example, “Testvb”, or “VISUALBUILDERAUTO_Testvb”.

6. Click the **Application Roles** tab.
7. To grant a role to users:
   a. Click the menu options icon shown next the role, and select **Assign Users**. If you want to assign the role to a group, you need to select **Assign Groups**.
   b. Select the check box next to the name of each user that you want to add to the role, and then click **Assign**.



Add Users to a Traditional Cloud Account

Oracle Traditional Cloud Accounts use traditional Identity and Access Management software to manage users and security, as opposed to Cloud Accounts with IDCS, which use Oracle Identity Cloud Service for these tasks.

Oracle Traditional Cloud Accounts use Oracle Shared Identity Manager (SIM) for identity management and authentication to access Oracle Visual Builder and applications developed with Visual Builder. An identity domain administrator can use the options on the Oracle Visual Builder console to manage users and their roles for

Oracle Visual Builder applications and services. Roles assigned to users in SIM are used to determine the following:

- developer access to Oracle Visual Builder
- user access to applications developed in Oracle Visual Builder that implement role-based security
- developer and user access to services exposed in Oracle Visual Builder and visual applications

A developer can set the authentication requirements for an application and create application roles that are mapped to custom roles in SIM. After creating the application roles, the developer can configure role-based security for the pages, components and business objects in the application. Authentication to access a visual application is determined by the roles assigned to users in SIM.

A developer's role in Oracle SaaS determines the content and services in the Oracle SaaS service instance that are available to the Oracle Visual Builder developer. For example, the Oracle Visual Builder services catalog might be empty if the developer is not assigned a role with sufficient privileges. Oracle Visual Builder and other offerings on the Oracle PaaS platform don't use the same identity management stack as Oracle SaaS services, but support for Single Sign-On (SSO) between Oracle PaaS services using Oracle Shared Identity Manager (SIM) and Oracle SaaS services such as Oracle Sales Cloud can be set up when they are in the same data center and identity domain. For SSO to work, Oracle SaaS identities need to be regularly synchronized to the Oracle PaaS SIM user store. Roles and corresponding role assignments can be synchronized in order to support role-based access used in your applications.

The following table briefly describes the steps for adding users, assigning roles, and synchronizing Oracle Sales Cloud and Oracle Visual Builder user accounts and roles.

Task	Description
Add users and assign roles	The **identity domain administrator** creates user accounts and assigns roles to the users in the instance of Oracle Visual Builder that you access from the Oracle Cloud Infrastructure Classic Console. Users that will develop applications with Oracle Visual Builder must be assigned the role of **Visual Builder Developer** or **Visual Builder Administrator**. See Creating a User and Assigning a Role in *Getting Started with Oracle Cloud*. The identity domain administrator also creates the custom roles for authenticating user access to applications and assigns roles to users.

Task	Description
Synchronize user identities and roles between associated services	Oracle Visual Builder service instances associated with Fusion Applications services use Fusion Applications user roles for authorizing access to REST services in applications. For Single Sign-On (SSO) between Oracle Visual Builder and Oracle applications such as Sales Cloud, the user accounts must be manually synchronized with the users in Fusion Applications, and the users assigned custom roles that can be used to secure access to applications. An **identity domain administrator** can synchronize user identities and roles from Oracle SaaS services to an Oracle PaaS SIM user store. Oracle Sales Cloud can be configured to sync identities and roles once, or automatically sync on a schedule, using the Oracle Enterprise Scheduler Service (ESS). See Synchronizing Oracle Sales Cloud, Oracle HCM Cloud, and Oracle ERP Cloud User Identities and Roles to SIM in *Oracle Cloud Paas-Saas Integration Online Documentation Library*.
Create custom roles that mirror the names of Oracle SaaS roles	An **identity domain administrator** can create custom roles that are used for authenticating users and securing applications. The custom roles can mirror the names of Oracle SaaS user roles. For example, an administrator can create the custom role Sales Manager, one of the default user roles. See Managing Custom Roles in *Getting Started with Oracle Cloud* .
Assign custom roles to users	After the users and custom roles are created, the **identity domain administrator** can assign custom roles to users in the instance of Oracle Visual Builder that you access from the Oracle Cloud Infrastructure Classic Console according to the user's Oracle SaaS role. For example, the administrator can assign the custom role Sales Manager to all users assigned that role in Oracle SaaS. The administrator can assign an existing role to multiple users by creating and uploading a CSV file. See Assigning One Role to Many Users in *Getting Started with Oracle Cloud*.

5

Administrative Tasks

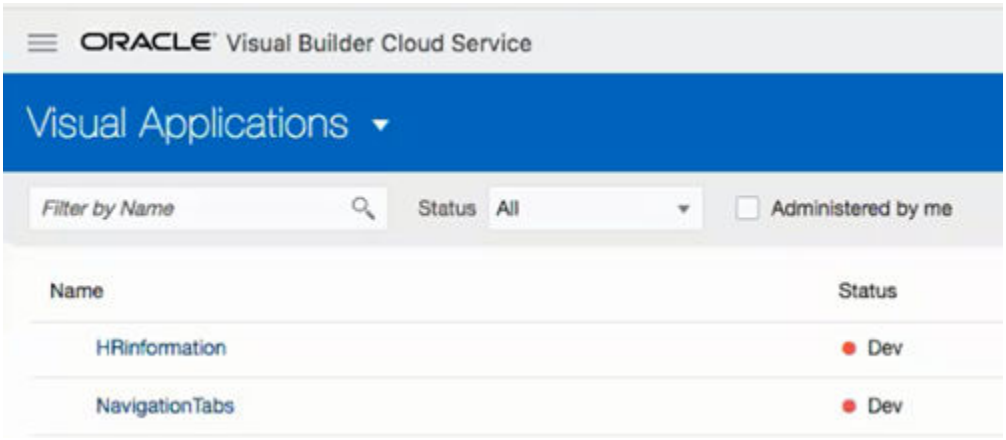
After an Oracle Visual Builder service instance is created, an identity domain administrator assigns one or more users the Visual Builder Administrator role for the service instance. A Visual Builder Administrator can manage and set general options for applications in the service instance.

Topics

Manage Applications in the Service Instance

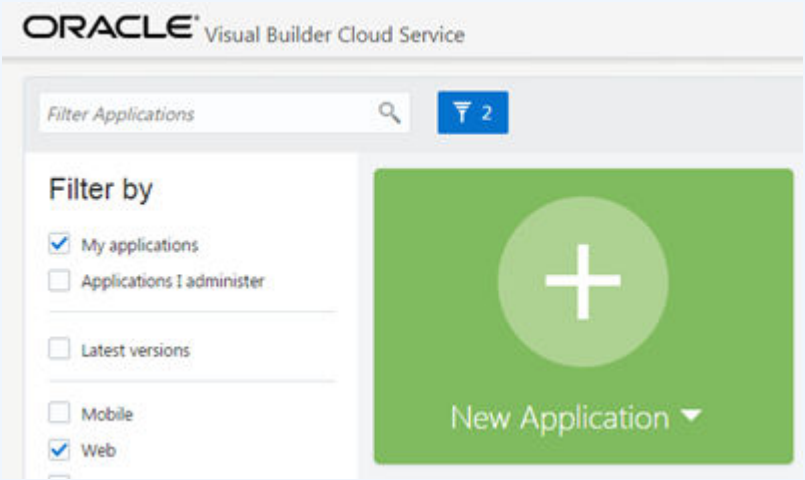
An Oracle Visual Builder administrator can manage any application in the service instance and does not need to be a team member to see an application on the Home page. Administrators can perform all the tasks of a developer, including adding and removing team members, and opening, staging and publishing applications.

The Home page displays a list of the applications in the service instance. Developers can only see and manage an application when they are a member of the application's team. Administrators can select the **Administered by me** checkbox if they want the list of applications to include all the applications in the instance, even the applications where they are not a team member. The checkbox is not visible to developers who do not have the role of administrator.



Note:

On the Home page for classic applications, administrators can select the **Applications I administer** checkbox in the Filter by pane to display the applications where they are not a team member.



Access Instance Settings

Administrators can access a page for managing the instance's global settings. The settings page contains panels for configuring security settings, specifying Access Denied messages and specifying Oracle Process Cloud Service details.

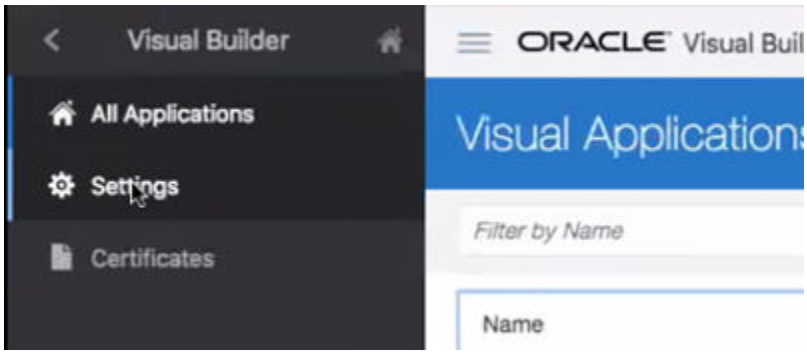
You can access the instance settings page from any Visual Builder page, but the steps for opening the page will depend on if you are developing visual applications or classic applications.

To open an instance's settings page:

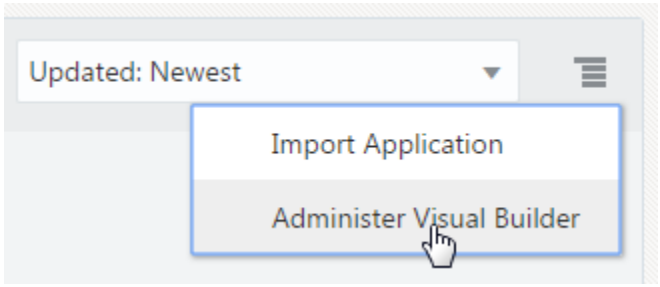
1. Click **Home** in the Visual Builder title bar to open the main menu.

2. Click **Settings** in the main menu.

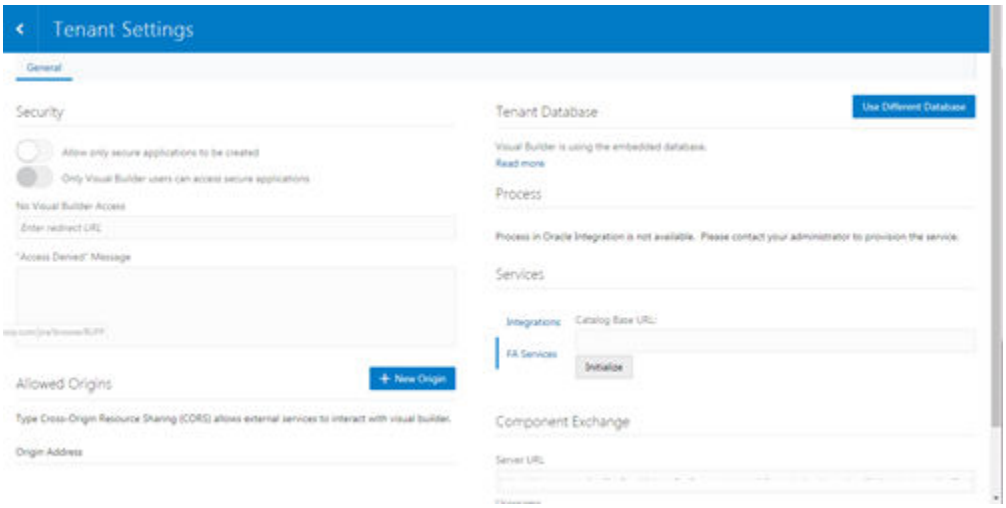
   If you are developing visual applications, open the main navigation pane on the Home page and select **Settings**.



   If you are developing classic applications, select **Administer Visual Builder** in the Administration Options menu and then click **Global Settings**.



The settings available for the instance are grouped on the page.



Configure Security Options for Applications

Administrators can use the Security panel in the settings page to require authentication for all applications in the instance.

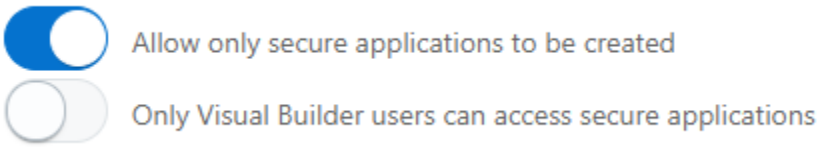
When an administrator enables the **Allow only secure applications to be created** option, all published and staged applications in the instance will require user authentication. When the option is enabled, users must be assigned a role by the identity domain administrator and log in to access an application. When the option is not enabled, applications can be created that allow access to anonymous users.

When an application has the default security settings, any user with a valid login can access the pages in an application. A developer can modify the default security settings to define the roles that can access applications, pages and components. When the secure application option is enabled, an administrator can enable an option that users must be assigned the role of Visual Builder User in addition to any other roles used to secure access to staged and published applications. For example, security can be configured so that users assigned the role Visual Builder Developer can access the designer but can't access the published application and data because they are not assigned the role Visual Builder User.

To block access by anonymous users to all applications in the instance:

1. Open the instance's settings page.
2. In the **Security** panel, enable **Allow only secure applications to be created**.

   Anonymous users can't access the applications when this option is enabled.



   When the secure applications option is enabled, administrators can enable the **Only Visual Builder Users can access secure applications** option.

Set Page Messages for Access Denied Errors

Administrators can use the instance's settings page to specify a URL that users are navigated to when they are denied access to an application or page.

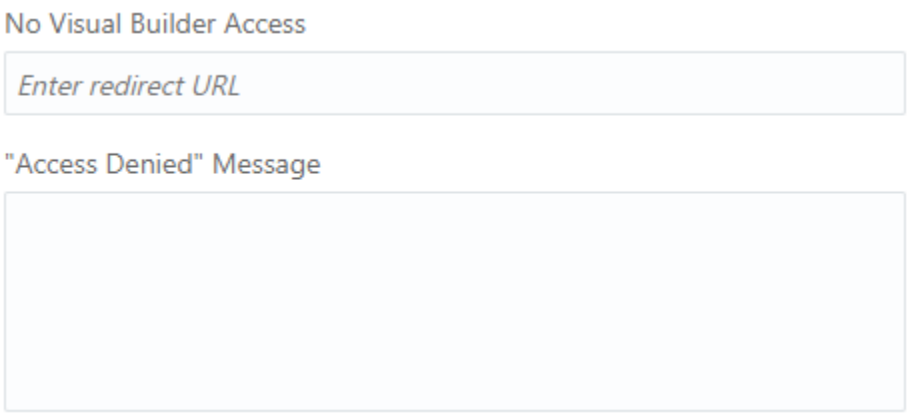
Authenticated users might see an Access Denied page or message when they attempt to access an application or page in an application that their user role is not permitted to access. Administrators can set the default page or message that users see when they are denied access to an application or page. Access Denied messages that are set at the application level in the General Settings of an application will override messages set in the instance's settings page. The default Access Denied page and message is used if the message options in this panel are not set.

To specify an Access Denied page or message for applications in the instance:

1. Open the instance's settings page.

2. In the **Security** panel, type a URL that users are directed to when denied access to an application.

   The URL that you specify is used as the Access Denied page for all applications in the instance and should be accessible to users who are not logged in.



> **Note:**
>
> If you are configuring settings for classic applications, the Access Denied settings are set in the **Messages** panel.

3. Type the message that you want users to see when they are denied access to a page.

   The message that you enter will be displayed in the Access Denied page for all applications in the instance except for those where a message was set at the application level in the application's General Settings page.

Allow Other Domains Access to Services

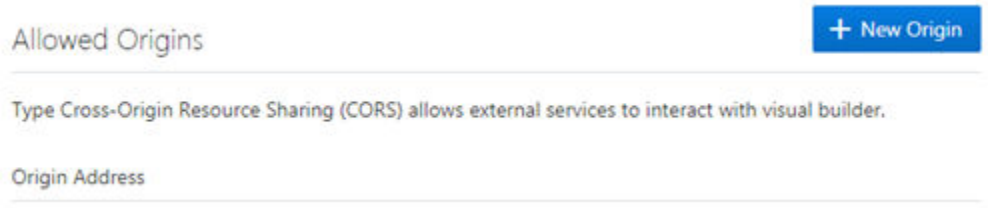
Use the Global Settings page to specify the domains that are permitted to interact with services in your instance.

Cross-Origin Resource Sharing (CORS) is a mechanism that enables you to specify the domains that are allowed to exchange data with applications in your instance. By default, incoming requests from domains not on your instance's list of allowed origins are blocked from accessing application resources.

To add a domain to the list of allowed origins:

1. Open the instance's settings page.
2. In the **Allowed Origins** panel, click **New Origin** and type the URL of the domain that you want to allow. Click **Submit**.

   The Allowed Origins panel lists all origins that are permitted to retrieve information from the instance.



Switch to Your Own Oracle DB Instance

If the 5GB limit of the database provisioned with your Visual Builder instance is insufficient for your tenant schema, you can configure your instance to use an Oracle DB instance that has more space instead of the default database.

To use a different Oracle DB instance, you use a wizard in the Tenant Settings to create a connection to the database instance and export the applications stored in tenant's current database. You can connect to an Oracle DBaaS or Autonomous Transaction Processing Database (ATP) instance.

If you decide to use JDBC to connect to your DBaaS instance, you must include the privileges required to enable the ADMIN user to create a tenant schema. The following SQL shows the grants that are needed:

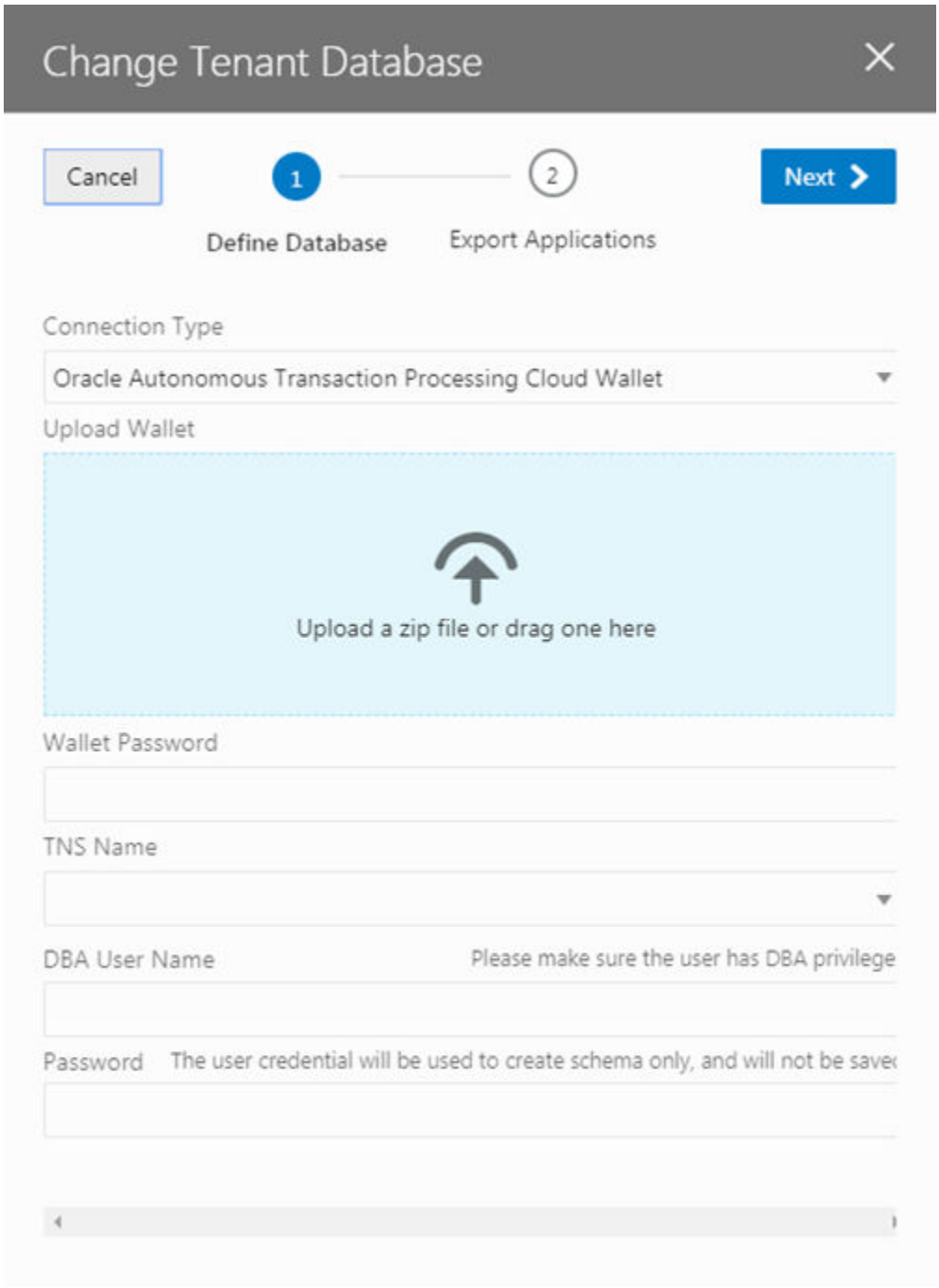
```
CREATE USER [adminuser] IDENTIFIED BY [password];
GRANT CONNECT, RESOURCE, DBA TO [adminuser];

GRANT SELECT ON SYS.DBA_PROFILES TO [adminuser] WITH GRANT OPTION;
GRANT SELECT ON SYS.DBA_USERS TO [adminuser] WITH GRANT OPTION;
GRANT SELECT ON SYS.DBA_DATA_FILES TO [adminuser] WITH GRANT OPTION;
GRANT SELECT ON SYS.DBA_SEGMENTS TO [adminuser] WITH GRANT OPTION;
```

In the wizard you need to select and export all the applications in your instance that you want to keep. After confirming that your instance is using the new database instance, you must import the exported applications into Visual Builder to save them in the new database instance.

To switch to a different Oracle DB instance:

1. Open the instance's Tenant Settings page.
2. Click **Use Different Database** in the Tenant Database panel to open the Change Tenant Database wizard.

   In the Change Tenant Database wizard you supply the details for the connection to your Oracle DB instance.



3. Select a Connection Type in the drop-down list.

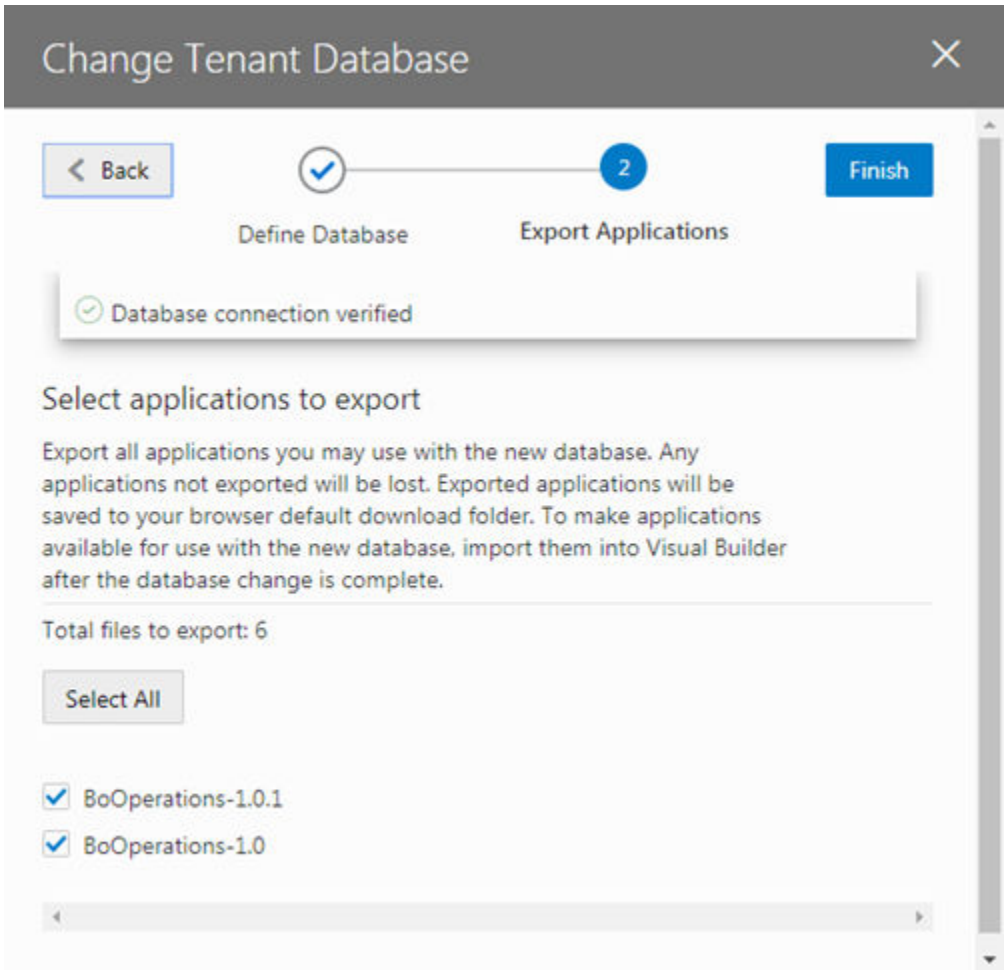
   You can connect to your Oracle DB instance using either JDBC or an ATP Cloud Wallet.

4. Provide the details for connecting to your database. Click **Next**.

   The details you need to provide will depend upon the type of connection you selected.

5. Select all the applications that you want to export. Click **Finish**.

You must select and export all the applications that you want to keep. Any applications that are not exported will be lost.



When you click Finish, the applications that you selected are downloaded to your local file system.

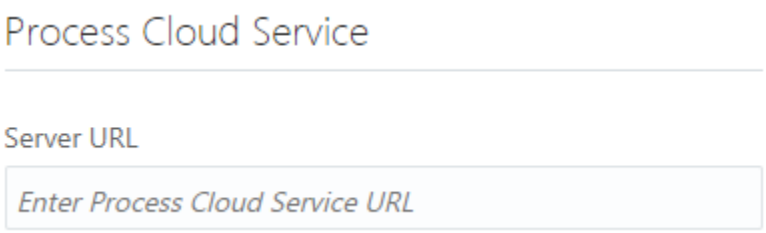
Add a Connection to Process Cloud Service

Administrators can use the instance's settings page to add a connection to an Oracle Process Cloud Service instance.

If you are using multiple Visual Builder instances, for example, development and production instances, you might need to add connections to Oracle Process Cloud Service in more than one instance.

To add a connection to an Oracle Process Cloud Service instance:

1. Open the instance's settings page.
2. In the **Process Cloud Service** panel, type the Server URL of the service.



3. In the **Allowed Origins** panel, click **New Origin** and type the URL of the Process Cloud Service instance.

   The Allowed Origins tab lists all origins that are permitted to retrieve information from the service instance.

Add a Connection for Fusion Applications Services

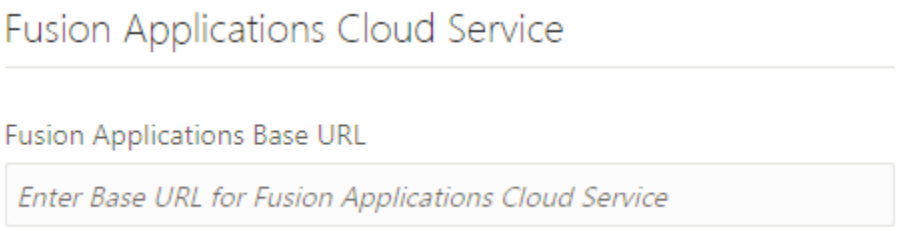
The list of REST services in the service catalog of visual applications is retrieved from a Fusion Applications service. The URL of the Fusion Applications service can be specified in the Tenant Settings dialog box or in the Settings dialog box of a visual application.

All visual applications in the tenant space will use the Fusion Applications base URL specified in Tenant Settings, but a visual application can be configured to use a different Fusion Applications service by specifying its URL in the application's Settings dialog box. The URL in Tenant Settings is ignored if a URL is specified in a visual application's Settings dialog box.

To specify a Fusion Applications service for the tenant:

1. Open the instance's settings page.
2. Enter the base URL of the Fusion Applications service.

   When specifying the URL in the Tenant Settings, the administrator only needs to provide the base URL of the Fusion Applications service to retrieve the list of services. The URL in the Settings dialog box for a visual application requires the full path to the `interfaceCatalogs` endpoint for retrieving the list of services. For example, if the URL for a Fusion Applications instance is *<my-fa-instance>*, the URL for the `interfaceCatalogs` endpoint would be `https://<my-fa-instance>/helpPortalApi/otherResources/latest/interfaceCatalogs`.



Manage Self-signed Certificates

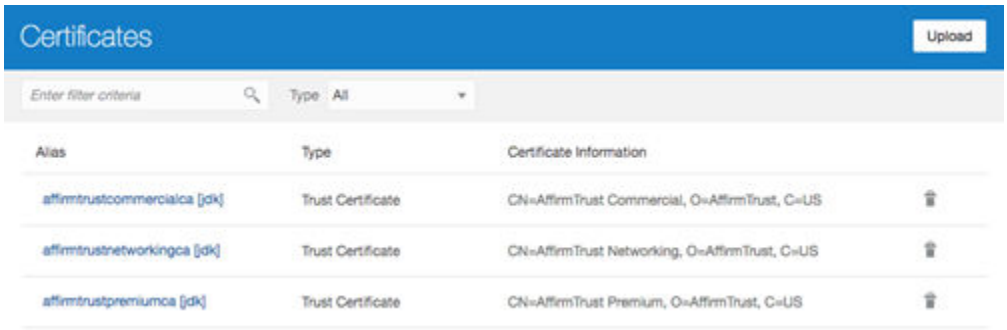
Administrators can use the Certificates page to upload and manage the self-signed certificates used by the instance to enable inbound and outbound SSL communications to a service's REST APIs

When creating connections to REST services that use self-signed certificates, you might need to add an API's certificate to your Visual Builder instance to validate SSL connections to that service. You can use the Certificates page to upload and remove certificate files (`.pem`) for services. Uploading a service's certificate file to the keystore will allow all applications in the instance to communicate with that service. The Certificates page displays a list of certificates that have been added. You can click the Delete button in a row to remove the certificate.

To upload a self-signed certificate:

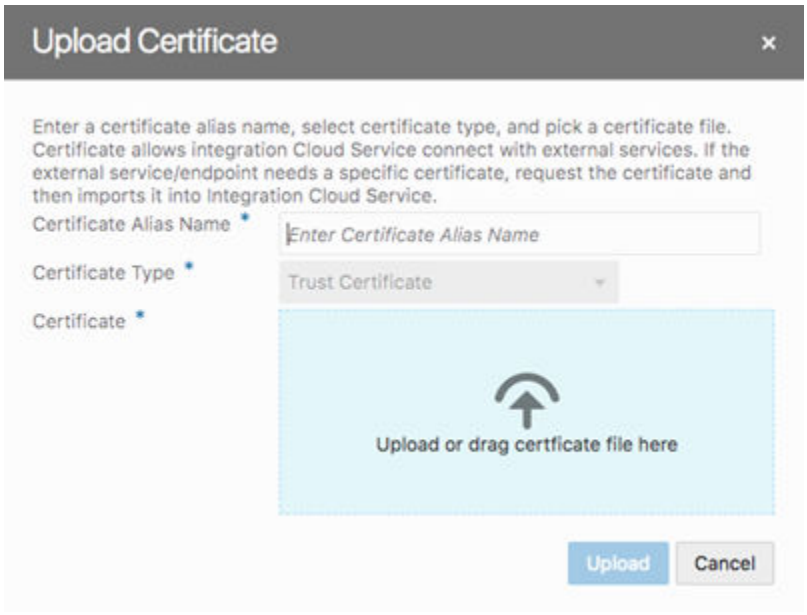
1. Open the Visual Builder main menu and click **Certificates**.

   The Certificates page displays a list of the certificates already uploaded to the instance.



2. Click **Upload** to open the Upload Certificate dialog box.

   You use the Upload Certificate dialog box to create an alias for the certificate and upload the service's certificate file from your local system.



3. Type the alias in the Certificate Alias Name field.

   The alias is used to identify the certificate in the table in the Certificates page. The Certificate Type dropdown list is read-only because only Trust Certificates are supported.

4. Drag the certificate file from your local system into the upload target area, or click the upload target area to browse your local system.

5. Click **Upload** to add the certificate to the service keystore.

Manage Your Component Exchange

When you add a component exchange in the Tenant Settings, users can use it to get additional components that they can then use in their applications.

Topics:

About Component Exchanges

A component exchange is hosted by an Oracle Developer project and is used to store components that can be used in visual applications, for example, web components and application templates. Many of the components provided by Oracle can be installed from a component exchange.

To integrate a component exchange with a Visual Builder instance, an administrator needs to provide the exchange's URL and credentials in the Tenant Settings. The exchange can be a private exchange in a Developer project or one of the exchanges maintained by Oracle.

If your organization develops or uses proprietary components, these components can be published to a private exchange hosted by a Developer project. For example, if you have a web component designed to be used in applications in your tenant, you can set up your own exchange and use it to distribute the component to developers in the tenant. Additionally, components provided by Oracle are automatically available from all private component exchanges.

Oracle maintains two component exchanges containing components validated by Oracle that are publicly available to all developers. If you don't have a private exchange but you want to give developers access to these Oracle components, you can add one of the following exchanges maintained by Oracle. If your instance is in the US, use the following details.

Field	Value
URL	https://devinstance4wd8us2-wd4devcs8us2.uscom-central-1.oraclecloud.com/profile/devinstance4wd8us2-wd4devcs8us2/s/devinstance4wd8us2-wd4devcs8us2_compcatalog_3461/compcatalog/0.2.0
Username	comp.catalog
Password	bXwphh6RMFjn#g

If your instance is in Europe, use the following details.

Field	Value
URL	https://devinstance4wd8em2-wd4devcs8em2.eucom-north-1.oraclecloud.com/profile/devinstance4wd8em2-wd4devcs8em2/s/devinstance4wd8em2-wd4devcs8em2_compcatalog_1681/compcatalog/0.2.0
Username	comp.catalog
Password	!!MWtu4jsQ56wM

About Component Exchanges Hosted in Developer Projects

An Oracle Developer project can host a secure component exchange to store and distribute components only available to developers in the instance.

Each Oracle Developer project includes the component exchange 'compcatalog', which is the service used to access components stored in the project. The compcatalog service is provisioned by default with each project. Any project can be used to host an exchange if storage is enabled for the Developer instance. Component developers can use the service's APIs to publish components to the exchange.

To integrate a private exchange in a Developer project with a Visual Builder instance, an administrator specifies the URL for the project's compcatalog service and the credentials for a user that can access the project. The credentials used to connect to the exchange must be an owner or member of the Developer project hosting the exchange. All developers in the tenant use these credentials to connect to the exchange to get the components and application templates they want to use in their projects.

The URL for the project's compcatalog service has the following form: `https://<hostname>/<org_id>/s/<project_id>/compcatalog/0.2.0/`

In the URL, "compcatalog" is the exchange service and "0.2.0" is the API version of the service.

To determine the URL for the compcatalog service, you need to know the following details about the Developer project:

- <*hostname*>. This is the Developer server where the project is hosted.
- <*org_id*>. This is the organization (tenant) name.
- <*project_id*>. This is a project identifier unique to the tenant. This is not the same as the project display name entered by the project owner and is not displayed in the Developer UI.

If you do not know the <*project_id*> for the project hosting the exchange, you can get it from the Git or Maven configuration, or by using the Oracle Developer Projects API. The following table describes how to get the <*project_id*>.

Method	Steps
From a Git or Maven configuration	1. In Oracle Developer, open the project and locate the Repositories tab on the project's Home Page. 2. Expand the the Git or Maven section and copy the repository URL. The Git repository URL will be similar to the following: `https://{user_id}@{hostname}/{org_id}/s/my-org_testproject_5/scm/my-repo.git` The Maven repository URL will be similar to the following: `http://{hostname}/{org_id}/s/my-org_testproject_5/maven/` In these examples, "my-org_testproject_5" is the project identifier. In this case, the URL for the 'compcatalog' service will be similar to `https://{hostname}/my-org/s/my-org_testproject_5/compcatalog/0.2.0/`

Method	Steps

Using Developer Projects API	If you know the name of the project sharing your exchange instance, you can get the project metadata using a REST call to the Developer Projects API.
	For example, you can use cURL to send a REST call similar to the following:
	`curl -X GET -u '{username}:{password}'https://{hostname}/{org_id}/api/v2/projects/info/name:TestProject`
	The return should be similar to the following:
	`[ { "organization":"my-org", "identifier":"my-org_testproject_5", "name":"TestProject", "urlId":"testproject", "description":null, "accessibility":"PRIVATE", "template":false, "state":"READY", "locked":false, "relation": {"membership":"OWNER","favorite":false} } ]`
	In this example, the identifier property in the return is the project identifier that is needed for the "compcatalog" service URL.

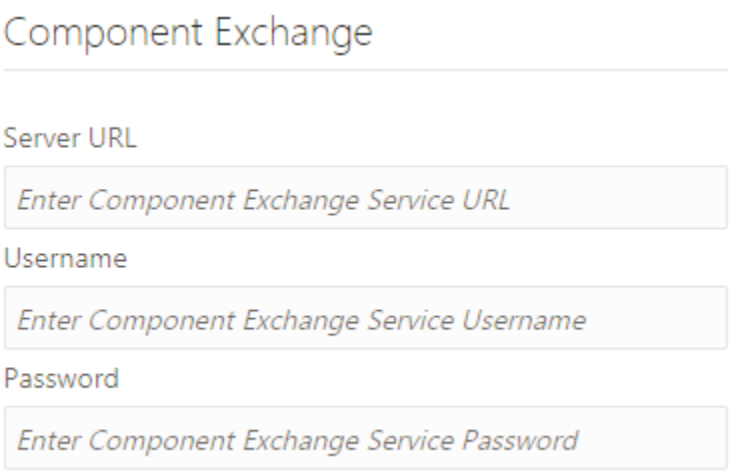
Add a Connection to a Component Exchange

When an instance is integrated with a component exchange, all developers using the instance can access and install components stored there.

After an exchange is added to the instance, all developers can use the Components tab in the Navigator to install and mange the components from the exchange that they want to use in their applications. When creating an application in the Create Application wizard, developers can also select any of the application templates that have been published to the exchange.

To add a connection to the Component Exchange:

1. Open the instance’s Tenant Settings page.
2. In the Component Exchange panel, enter the URL and credentials for the component exchange.



If you are adding a connection to a private component exchange, it is recommended that the credentials you provide are for an administrator who is a member of the Developer project hosting the exchange or the project owner.

Configure Support for a Custom Domain

When a custom domain (for example, `foo.example.org`) is mapped to your instance, customers can use it to access a web application instead of using the default URL generated by Visual Builder.

A custom domain is created by editing your domain to add a subdomain. After configuring your instance to use a custom domain, customers accessing the app using the custom domain will not see the typical Oracle domain (for example, `myvbinstance-accountname.builder.ocp.oraclecloud.com`) in the URL. The application is loaded from the custom domain root, and no additional path information or query parameters are required in the URL. The custom domain can also be used to access the APIs of the application's business objects.

Only one custom domain can be mapped to a visual application, and it can only be used to access one web application in the visual application. It is recommended that your visual application only contain one web application if you are going to use a custom domain to ensure that the correct web application is loaded. You specify the custom domain in the visual application's Settings editor.

You can configure multiple custom domains for your instance, but each must be mapped to a different visual application. For example, if the visual application `myvisualapp1` is mapped to the subdomain `mysubdomain1`, if you want to map `mysubdomain2` to an application it must be mapped to a different visual application (`myvisualapp2`).

To configure a custom domain for your instance, you must be the registered owner of the domain and have access to its SSL certificate bundle information. To use a custom domain you need to perform the following tasks:

- Edit the DNS record of your domain to create a subdomain.
- Log a Service Request through your Oracle Support Representative to configure the server backend to handle requests for the subdomain.
- Edit the Web Tier Policy for your service's IDCS application

- Set the custom domain in the visual application's Settings editor.

Create and Configure a Subdomain

To use a custom URL for your app you'll first need to use your domain provider's tools to create a subdomain that points to your instance. You will then need to log a Service Request to configure the instance backend, including the SSL certificate for the subdomain.

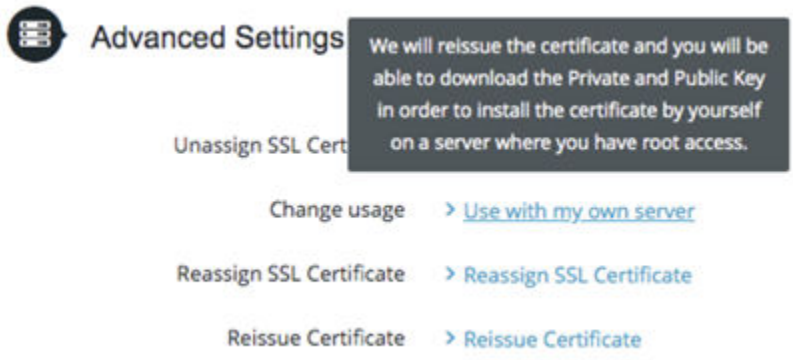
Using the tools for administering your domain, you will need to create or identify the subdomain and map it to your Visual Builder instance URL. edit the DNS record of your domain to register the CNAME for the subdomain.

To create and configure a subdomain for your instance:

1. Open the tool of your domain provider for creating a subdomain.
2. Create the subdomain and edit it's CNAME record to point to your Visual Builder instance URL.
3. Confirm there is a valid SSL certificate that applies to the subdomain.

   Oracle will need to maintain the certificate bundle on Oracle servers, so you might want to consider an SSL certificate specifically for the subdomain rather than a wildcard SSL cert (`*.example.com`). The certificate might be provided by your domain provider or through a valid certifying authority (for example, Comodo, DigiCert).
4. Extract or export the bundle containing the certificate and private key.

Depending on your domain provider, you may need to indicate that you want to use the certificate on your own server in order to download the bundle.



5. Log a Service Request through your Oracle Support representative to request that your Visual Builder instance be configured to handle requests for your custom subdomain.

   When you file the service request you will need to provide the following information:

   - The URL of your instance.
   - The details of the CNAME record showing the subdomain and the Visual Builder instance it points to.
   - Certificate and Private key files (`.cer` and `.key`)

Once setup is complete you can map your visual application to the custom domain.

Edit the Web Tier Policy of the Application

To allow the service instance to handle requests at the root URL, you need to configure the Web Tier Policy for the service IDCS . An application developer can then set the custom domain for the visual application.

To configure the Web Tier Policy for the application:

1. Login to the IDCS identity console and locate the IDCS application for your Visual Builder or Integration instance.

   To log in you must have Application Administration privileges in IDCS.

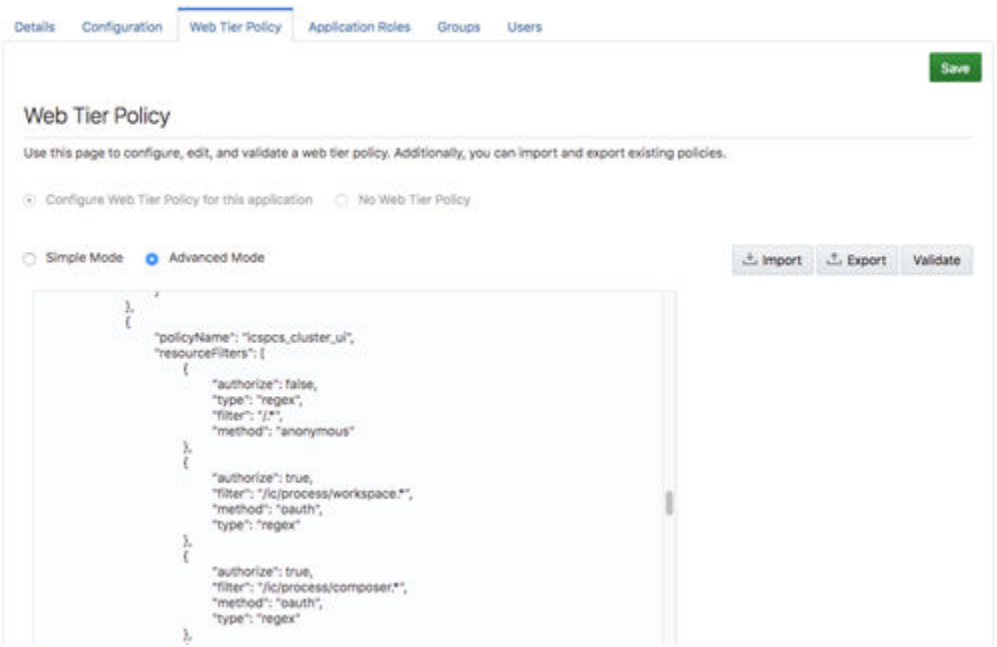
2. In the **Web Tier Policy** tab for the IDCS app, export the current web tier policy.

   Keep a copy of the file in case you want to reset to the policy factory settings.

3. In the web tier policy, add the following element into the code section called `icspcs_cluster_ui` and save your changes.

```
{
  "authorize": false,
  "type": "regex",
  "filter": "/.*",
  "method": "anonymous"
},
```

4. Import the saved file.
5. Open **Advanced Mode** and verify the changes. Click **Save**.



After configuring the Web Tier Policy, an application developer can specify which visual application in the instance is mapped to the custom domain. The developer will need to enter the full custom domain (for example, `https://foo.example.org`) in the Vanity URL field of the visual application's Settings editor: After the visual application is staged and published, the web application and the business object APIs can be accessed directly using the custom domain.