Oracle® Cloud

Administering Oracle Visual Builder in Oracle Integration
Contents

Preface

Audience iv
Documentation Accessibility iv
Related Resources iv
Conventions iv

1 Administer Visual Builder Instances

Administer Your Instances 1-1

2 Manage Instance Settings

Manage Applications in the Service Instance 2-1
Access Instance Settings 2-2
Configure Security Options for Applications 2-4
Set Page Messages for Access Denied Errors 2-4
Allow Other Domains Access to Services 2-5
Add a Connection for Fusion Applications Services 2-6
Add a Connection to the Component Exchange 2-6
Manage Self-signed Certificates 2-8
Preface

Describes tasks for administrators of Oracle Visual Builder.

Audience

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

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Resources

For more information, see these Oracle resources:

- Oracle Public Cloud
  http://cloud.oracle.com
- About Oracle Integration in Developing Applications with Oracle Visual Builder in Oracle Integration
- Learn About Oracle Integration in Administering Oracle Integration

Conventions

The following text conventions are used in this document:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface</strong></td>
<td>Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.</td>
</tr>
<tr>
<td><em>italic</em></td>
<td>Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.</td>
</tr>
<tr>
<td>Convention</td>
<td>Meaning</td>
</tr>
<tr>
<td>------------</td>
<td>---------</td>
</tr>
<tr>
<td>monospacer</td>
<td>Monospacer type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.</td>
</tr>
</tbody>
</table>
Administer Visual Builder Instances

You use the My Services console to manage Visual Builder instances provisioned in Oracle Integration, for example, to add or upgrade instances. Each of your instances also has an Administrative Settings page where you can specify global settings that are applied to that instance.

Topics:
• Administer Your Instances

Administer Your Instances

Your Visual Builder instance is provisioned as one of the features in your Oracle Integration subscription. An administrator performs most of the lifecycle management tasks for Visual Builder instances in the My Services Console. Depending on your subscription and environment, some options for administering instances might not be available.

Additional management settings for applications created in an instance are set in the Administrator Settings page that administrators can open from the Home page of each Visual Builder instance. See Manage Instance Settings.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create an instance</td>
<td>You can provision new instances in the My Services Console using Quick Starts or stack templates. The stack template will also provision the Oracle Storage Cloud Service container and Oracle Database Cloud Service instances required by Visual Builder. See Ready, Set Up, and Go in Administering Oracle Integration. In user-managed environments you can also choose to use a provisioning wizard to create an instance. If you want to use the provisioning wizard, you must provision an Oracle Storage Cloud Service container and Oracle Database Cloud Service before using the wizard.</td>
</tr>
<tr>
<td>View overview of your instances</td>
<td>The My Services Console provides details on all of your Visual Builder instances, including the number of Oracle Compute Units (OCPUs) and mount of memory allocated across all instances. See About the User Interfaces of the Oracle Integration My Services Console in Administering Oracle Integration.</td>
</tr>
<tr>
<td>Task</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Add users and assign roles</td>
<td>Visual Builder users need to be added to the identity domain of your Oracle Integration instance and assigned at least one of the pre-defined roles that are permitted to access the Visual Builder instance. See Understanding Oracle Integration Roles and Privileges in <em>Administering Oracle Integration</em>.</td>
</tr>
<tr>
<td>Start and stop instances or stacks</td>
<td>You use the My Services Console to stop instances to free up compute resources used by the instance’s virtual machines. See Starting and Stopping Oracle Integration Instances in <em>Administering Oracle Integration</em>.</td>
</tr>
<tr>
<td>Patch and upgrade instances</td>
<td>New patches that are available for your instance are visible in the My Services Console. In an Oracle Autonomous environment, the patches are visible but are applied for you. In a <strong>user-managed</strong> environment, patches can be applied from the Patching page. See patching and Upgrading Your Environment in <em>Administering Oracle Integration</em>.</td>
</tr>
<tr>
<td>Scale in and scale out instances</td>
<td>In a <strong>user-managed</strong> environment you use the My Services Console to add or remove nodes to your instance on demand in response to changes in load on the instance. You cannot scale in or scale out instances in an Oracle Autonomous environment. See Scaling Out and Scaling In an Oracle Integration Instance in <em>Administering Oracle Integration</em>.</td>
</tr>
<tr>
<td>Back up and restore instances</td>
<td>In a <strong>user-managed</strong> environment you can preserve your instances in a particular state by creating full or incremental backups that you can use later to restore instances. You cannot do this in an Oracle Autonomous environment. See Backing Up and Restoring an Oracle Integration Instance in <em>Administering Oracle Integration</em>.</td>
</tr>
</tbody>
</table>
Manage Instance Settings

After a Visual Builder instance is created, users with the role of Visual Builder Administrator can manage and set global options for applications in the instance and create associations between the instance and other services.

Topics:
- Manage Applications in the Service Instance
- Access Instance Settings
- Configure Security Options for Applications
- Set Page Messages for Access Denied Errors
- Allow Other Domains Access to Services
- Add a Connection for Fusion Applications Services
- Add a Connection to the Component Exchange
- Manage Self-signed Certificates

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.
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.

   **No Visual Builder Access**

   Enter redirect URL

   **"Access Denied" Message**

   ![Access Denied Message](image)

   **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.
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.

Add a Connection to the Component Exchange

The service admin can add a connection to a Component Exchange instance by supplying the location and credentials for accessing it in the Tenant Settings.

Access to the Component Exchange is automatically enabled by supplying the URL and credentials for the Component Exchange. When access is enabled, developers can access Application Templates available in the exchange when creating applications, and components in the exchange can be added as custom components in the Component palette.
Depending on the location of your instance, you can use the following details for adding the connection. If your instance is in the US, use the following details.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td><a href="https://devinstance4wd8us2-wd4devcs8us2.uscom-central-1.oraclecloud.com/profile/devinstance4wd8us2-wd4devcs8us2-s/devinstance4wd8us2-wd4devcs8us2_compcatalog_3461/compcatalog/0.2.0">https://devinstance4wd8us2-wd4devcs8us2.uscom-central-1.oraclecloud.com/profile/devinstance4wd8us2-wd4devcs8us2-s/devinstance4wd8us2-wd4devcs8us2_compcatalog_3461/compcatalog/0.2.0</a></td>
</tr>
<tr>
<td>Username</td>
<td>comp.catalog</td>
</tr>
<tr>
<td>Password</td>
<td>bXwpbh6RMFjn#g</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td><a href="https://devinstance4wd8em2-wd4devcs8em2.eucom-north-1.oraclecloud.com/profile/devinstance4wd8em2-wd4devcs8em2-s/devinstance4wd8em2-wd4devcs8em2_compcatalog_1681/compcatalog/0.2.0">https://devinstance4wd8em2-wd4devcs8em2.eucom-north-1.oraclecloud.com/profile/devinstance4wd8em2-wd4devcs8em2-s/devinstance4wd8em2-wd4devcs8em2_compcatalog_1681/compcatalog/0.2.0</a></td>
</tr>
<tr>
<td>Username</td>
<td>comp.catalog</td>
</tr>
<tr>
<td>Password</td>
<td>!!MWtu4jsQ56wM</td>
</tr>
</tbody>
</table>

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.

```
Component Exchange

Server URL

Enter Component Exchange Service URL

Username

Enter Component Exchange Service Username

Password

Enter Component Exchange Service Password
```

It is recommended that the credentials you provide are for a service admin. The admin also needs to be a member of the DCS project that hosts the Component Exchange.
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.