Oracle® Cloud

Using Oracle WebCenter Portal on Marketplace in Oracle Cloud Infrastructure

F92976-05
June 2024

Oracle Cloud Using Oracle WebCenter Portal on Marketplace in Oracle Cloud Infrastructure,

F92976-05

Primary Author: Oracle Corporation

Contents

Preface

This guide describes how to provision and administer Oracle WebCenter Portal 12c (12.2.1.4) on Marketplace in Oracle Cloud Infrastructure.

Audience

This guide is intended for users who want to create, manage, and use WebCenter Portal instances provisioned from Marketplace in Oracle Cloud Infrastructure.

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

The documentation for Oracle WebCenter Portal for 12c (12.2.1.4) is available from the Oracle Help Center.

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.

1

What's New in Oracle WebCenter Portal on Marketplace

Learn about the new and changed features in Oracle WebCenter Portal on Marketplace.

24.6.1— June 2024

Feature	Description
Object Storage for documents is optional	You can choose to store documents in the file system or in Object Storage. See Provision WebCenter Portal Stack.
PDB name	You can now specify the PDB name when configuring the database. See Provision WebCenter Portal Stack.
Database Strategy	You can now specify the Database Strategy (type of database) such as Database System or Autonomous Transaction Processing Database when configuring the database. See Provision WebCenter Portal Stack.
Integration with OCI Logging	You can integrate WebCenter Logs with OCI Logging. See Integrating WebCenter Logs with OCI Logging

24.5.1— May 2024

Feature	Description
Object Storage for documents	Object Storage (a storage provider component) is now available to store documents. See Provision WebCenter Portal Stack.
Configure SAML2 IDCS Single Sign-On in WebCenter Portal	You can configure SAML2 IDCS Single Sign-On in WebCenter Portal on marketplace. See Configure SAML2 IDCS Single Sign-On in WebCenter Portal.

2

Get Started with Oracle WebCenter Portal on Marketplace

Here's information about Oracle WebCenter Portal on Marketplace that will help you get started:

About Oracle WebCenter Portal on Marketplace

Oracle WebCenter Portal on Marketplace is provided as a VM-based solution on Oracle Cloud Infrastructure.

Oracle WebCenter Portal on Marketplace is available in two types of Marketplace offerings: Paid and BYOL. See About the License for Oracle WebCenter Portal on Marketplace.

Oracle WebCenter Portal on Marketplace helps customers to provision/set up the environment in few clicks and enables to deliver Portal solutions on cloud.

About the License for Oracle WebCenter Portal on Marketplace

Oracle WebCenter Portal on Marketplace is based on Oracle WebCenter Portal 12c (12.2.1.4). Oracle WebCenter Portal on Marketplace is available in two types of Marketplace offerings:

- **Paid**: Use the following Oracle WebCenter Portal (Paid) listing to use Universal Credits pricing:
  - Oracle WebCenter Portal 12c (Paid)

  See Oracle Universal Credits.
- **BYOL**: Use the Oracle WebCenter Portal (BYOL) listing to Bring Your Own License using your existing Oracle WebCenter Portal 12c (12.2.1.4) on-premises license, or you can purchase a new license for Oracle WebCenter Portal 12c (12.2.1.4).

  When you activate Oracle WebCenter Portal on Marketplace using the BYOL listing, you are charged only for the Oracle Cloud Infrastructure resources consumed. You must have sufficient supported on-premises licenses as required and specified in the Service Description for Oracle PaaS.

  For the processor conversion ratios and license requirements for the BYOL offering, go to the Cloud Service Descriptions page and go to the Cloud Service Description PDF. In particular, note the following conversion ratios for BYOL:
  - For each supported Processor license, you may activate up to 2 OCPUs of the BYOL Cloud Service.
  - For every 10 supported Named User Plus licenses, you may activate 1 OCPU of the BYOL Cloud Service.

About Roles and User Accounts

Oracle WebCenter Portal on Marketplace uses roles to control access to tasks and resources. A role assigned to a user gives certain privileges to the user.

Access to Oracle WebCenter Portal on Marketplace is based on the roles and users set up for the Oracle Cloud Infrastructure console. You need OCI Administrator role to provision WebCenter Portal.

For information about how to add user accounts in Oracle Cloud, see:

- Add Users to a Cloud Account with Identity Cloud Service in *Getting Started with Oracle Cloud*.
- Managing Oracle Identity Cloud Service Users and Groups in the Oracle Cloud Infrastructure Console in the Oracle Cloud Infrastructure documentation.

3

Create and View Oracle WebCenter Portal on Marketplace Instances

The information in this chapter will help you create and view Oracle WebCenter Portal on Marketplace instances.

Before You Begin

Before you begin, you would need to complete the following tasks and prerequisites.

Sign in to Oracle Cloud Infrastructure Console

Complete the following steps to sign in to the Oracle Cloud Infrastructure console.

1. Go to http://cloud.oracle.com.
2. Enter your cloud account name and click **Next**.
3. Sign in to the Oracle Cloud Infrastructure console:
   - If your cloud account uses identity domains, sign in to the Oracle Cloud Infrastructure console as a user configured in Oracle Cloud Infrastructure Identity and Access Management (IAM).

     Select the **default** domain.
   - If your cloud account does not use identity domains, sign in to the Oracle Cloud Infrastructure console as a user federated through Oracle Identity Cloud Service.

     Under Single Sign-On (SSO) options, note the identity provider selected in the **Identity Provider** field and click **Continue**.
4. Enter the user name and password provided in the welcome email, and click **Sign In**.

The Oracle Cloud Infrastructure console is shown.

Prerequisites

You'll need to complete the following prerequisites before provisioning the WebCenter Portal stack.

- System Requirements
- Generate SSH key pair
- Create a Compartment

- Create a Master Key
- Create Database
- Create the Object Storage Bucket in OCI
- Create a New User API Key
- IDCS
- Create Vault Secrets

After completing the above prerequisites, you can proceed to provision the WebCenter Portal stack.

> **Note:**
>
> WebCenter Content is installed when you provision the WebCenter Portal stack.

System Requirements

You require access to the following services to use Oracle WebCenter Portal on OCI.

- Identity and Access Management (IAM)
- Compute, Network, Block Storage
- Vault, Key, Secret
- Resource Manager
- Database
- Load Balancer
- Tagging

Make sure you have the following minimum limits for the services in your Oracle Cloud Infrastructure tenancy, and if necessary, request for an increase of a service limit.

Service	Minimum Limit
Identity and Access Management (IAM) Policy	1
Compute Shape VM.Standard.E4.Flex or VM.Standard.E5.Flex	4
Virtual Cloud Network	1
Block Storage	1 TB
Vault & Key	1
Secrets	5
Load Balancer	Flexible Load Balancer

In Oracle Cloud Infrastructure Vault (formerly known as Key Management), a standard vault is hosted on a hardware security module (HSM) partition with multiple tenants, and it uses a more cost-efficient, key-based metric for billing purposes. A virtual private vault provides greater isolation and performance by allocating a dedicated partition on HSM. Each type of vault has a separate service limit in your Oracle Cloud Infrastructure tenancy. The limit for secrets spans all the vaults.

See Service Limits in the Oracle Cloud Infrastructure documentation.

Generate SSH key pair

See generate_ssh_key for generating an SSH key pair.

This SSH key pair will be used for connecting to Bastion and Compute instances after stack execution.

> **Note:**
>
> This will be used to create DB and WebCenter Portal nodes.

Create a Compartment

If your tenancy does not already include a compartment for your Oracle WebCenter Portal on Marketplace instances, you can create a new one.

> **Note:**
>
> To create a compartment, your administrator must first add the following policy for your group:
>
> `allow group groupName to manage compartments in tenancy`

To create a compartment in Oracle Cloud Infrastructure:

1. Sign in to the Oracle Cloud Infrastructure Console.
2. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Compartments**. A list of the existing compartments in your tenancy is displayed.
3. Click **Create Compartment**.
4. Enter the following:
   - Name: Specify a name. For example, wcp-compartment. Restrictions for compartment names are: Maximum 100 characters, including letters, numbers, periods, hyphens, and underscores. The name must be unique across all the compartments in your tenancy.
   - Description: A friendly description.
5. Click **Create Compartment**.
6. Once the compartment is created, if you are not an administrator, ask your administrator to grant the following manage and use permissions in the compartment:
   a. Navigate to Identity and Security, Policies, and then Create Policies.
   b. To allow a non-administrator to execute the stack, create an IAM group called **wcp** and then create a policy with the following statements.
      - `allow group wcp` to manage instance-family in compartment `wcp-compartment`
      - `allow group wcp` to manage virtual-network-family in compartment `wcp-compartment`
      - `allow group wcp` to manage volume-family in compartment `wcp-compartment`

- `allow group wcp` to manage load-balancers in compartment `wcp-compartment`
- `allow group wcp` to manage orm-family in compartment `wcp-compartment`

where `wcp` is the group name and `wcp-compartment` is the compartment name.

> **Note:**
>
> You can use any name (**wcp** and **wcp-compartment** are examples).

Create a Master Key

You'll need to create a master key for the vault.

1. Sign in to the Oracle Cloud Infrastructure Console.
2. Open the navigation menu and click **Identity & Security** and then **Vault**.
3. Change the necessary compartment.
4. Click the already created vault name.
5. On the left side, click **Master Encryption keys** and then click **Create Key**.
6. Complete the following:
   - Create In Compartment : Name of the selected compartment
   - Protection Mode: Software
   - Name: Specify a name.
   - For remaining fields, retain the default values.
7. Click **Create Key**.
   Wait for the status to show green.

Create Database

You'd need a new DB system only if you want to provision a new database.

> **Note:**
>
> Otherwise, you can use an existing database too.

> **Note:**
>
> Currently, only the Oracle Base Database Service is supported. Support for other versions will be provided in upcoming releases. For any additional questions, contact the Oracle Support team.

Complete the following to create a new DB system:

- Create VCN
- Create a New DB System

Create VCN

1. Log in to OCI Console, navigate to Networking, then to Virtual Cloud Networks.
2. Click **Create VCN via Wizard**.
3. Click **Start VCN Wizard**.
4. **VCN name**: Provide a name.
5. **Compartment**: Specify the compartment in which the VCN needs to be created.
6. **VCN IPv4 CIDR block**: Specify IPv4 CIDR block (for example, 10.0.0.0/16).
7. Select the **Use DNS hostnames in this VCN** check box.
8. In the Configure public subnet and Configure private subnet sections, specify the correct CIDR blocks and click **Next**.
9. Make sure to create the necessary gateways such as Internet gateway, NAT gateway, and Service gateway.
10. Click **Create**.

The VCN is created.

Create a New DB System

1. Create a new DB system in the VCN you created earlier.
2. Make a note of the SSH keys used for the DB system creation. This private SSH key will be added to the vault's secret later.

> **Note:**
>
> Ensure to provide a DB System SSH private key without a passphrase as passphrase is not allowed.

   a. Log in to the console.
   b. Click **Oracle Database**.
   c. Click **Oracle Base Database Service** and then click **Create DB Systems**.
   d. Provide the following parameters:
      - Select a Compartment Name: Choose the appropriate compartment name.
      - Name your DB system: Specify a suitable name.
      - Select an availability domain: Choose AD1. You can choose any AD but make sure that WebCenter Portal and DB are in the same AD.
      - Configure shape: AMD VM Standard E4 Flex
      - Configure storage: 1 TB
      - Configure the DB system: The total node count is 2 and Oracle Database software edition is Enterprise Edition Extreme Performance.
      - Add SSH keys: Upload the public SSH key you created in the first step. You can either reuse the keys generated in the first step or you can generate a new pair of keys too for database instances.

- License: Choose the appropriate license.
- Virtual cloud network: Choose the VCN you created earlier.
- Client subnet: Select (either private or public subnet as needed) from the drop-down list.
- Hostname prefix: Choose an appropriate name.
- Database name: Specify a name for your database. Click **Next**.
- Database image: Oracle Database 19c.
- PDB Name: pdb1
- Create administrator credentials: Specify 'sys' and an appropriate password.
- Backup destination: Object Storage
- For remaining input fields: Select the default values.

e. Click **Create DB System** and wait for the DB provisioning to be completed before you proceed to the next step.

IDCS

1. Create a new IDCS Confidential App for WebCenter Portal provisioning. Log in to your IDCS administration console. For example, `https://<your-idcs-link>.identity.oraclecloud.com/ui/v1/adminconsole`. You can find this URL on the *OracleIdentityCloudService* section by navigating to Identity, Federation, and then Identity Provider Details. The field name that has this URL is **Oracle Identity Cloud Service Console**.
2. Click **Integrated applications**.
3. Click **Add application** on the Integrated Applications page to create a new confidential app.
4. Choose **Confidential Application** in the Add Application pop-up.
5. In the Details section, provide a name and click **Next**.
6. In the Client section, choose **Configure this application as client now** and select the following grant types under Authorization:
   - Client Credentials
   - JWT Assertion
   - SAML2 Assertion
7. Skip all other sections by clicking **Next** till you reach the **Finish** button.
8. Make a note of the Client ID and Client Secret for this app. Client Secret will be added to the vault's secret later.
9. Navigate to the application created and click **Activate** to enable this app for use in WebCenter Portal provisioning.

Create the Object Storage Bucket in OCI

1. Sign in to the Oracle Cloud Infrastructure Console.
2. Click the navigation menu in the upper left corner of the page and click **Storage**.
3. Click **Buckets**.

4. Confirm that you're in the correct compartment and the correct region.
5. Click **Create Bucket** on the "Buckets in <compartment name> Compartment" page.
6. Provide a value for **Bucket Name**.
7. Leave the **Default Storage Tier** set to **Standard**.
8. Leave the **Encryption** set to **Encrypt using Oracle managed keys**.
9. Click **Create**.

See Object Storage Buckets for more information.

Create a New User API Key

1. Sign in to the Oracle Cloud Infrastructure Console.
2. Click on your avatar in the upper-right corner of the page.
3. Click **My profile**.
4. In the **Resources** menu on the left side of the page, click **API Keys**.
5. Click **Add API Key**.
6. Download the private key by clicking **Download private key**. The private key will be added to the vault's secret later.
7. Click **Add**.
8. Click **Copy** to copy the content of the configuration file which has user OCID and fingerprint as this will be required later. Close the dialog.

Create Vault Secrets

1. Log in to the OCI console and search for *Vault*, and then create a vault app.
   a. Click **Create Vault**.
   b. Select the compartment you created earlier
   c. Provide a name and click **Create Vault**.
2. Click the vault app you created earlier. Create a master encryption key by specifying the compartment, protection mode, name, algorithm, length, and so on in the Create Key section.
3. Click **Secrets** on the left side and start adding secrets by specifying the compartment, name, key, secret type template, secret contents, and so on in the Create Secret section.

Secret Name	Secret Description	Comment
wcp-admin-password	Secret for WebCenter Portal Admin Password	The **Secret Contents** field should be populated with the Weblogic password value. The password needs to meet the following password policy: The password must be at least 8 alphanumeric characters with at least one number or a special character.
db-system-sys-password	Secret for DB System SYS Password	SYS user password of DB created in the Create a New DB System section should be used in the **Secret Contents** field.

Secret Name	Secret Description	Comment
db-system-ssh-private-key	Secret for DB System SSH private key	The **Secret Contents** field should be populated with the private key value that was used to create DB in the Create a New DB System section.
idcs-client-secret	Secret for IDCS Client secret	The **Secret Contents** field should be populated with the Client Secret value that was noted when the IDCS Confidential App was created in the IDCS section.
wcp-schema-password	Secret for WebCenter Portal schema password.	Example: OCI#db#456789123 The password needs to meet the following password policy: • The password must start with a letter. • The password must contain at least two digits. • The password must contain at least two uppercase letters. • The password must contain at least two lowercase letters. • The password must contain at least two special characters from the set [$#_]. • The password must be at least 15 characters long.
oci-user-private-key	Secret for user API private key	The **Secret Contents** field should be populated with the private key value downloaded earlier in the Create a New User API Key section.

Provision WebCenter Portal Stack

You can provision Oracle WebCenter Portal on a Marketplace instance in a selected compartment in Oracle Cloud Infrastructure.

To provision Oracle WebCenter Portal on a Marketplace instance:

1. Navigate to the WebCenter Portal listing on Marketplace by direct URL or by browsing in Oracle Cloud Infrastructure.
   Using direct URL:
   a. In your browser, enter https://cloudmarketplace.oracle.com/marketplace/en_US/homePage.jspx?tag=WebCenter+Portal.

      The Marketplace listings for WebCenter Portal are displayed.
   b. Click the title of the listing you want to use. The landing page of that listing is displayed.
   c. Click **Get App**.
   d. Select your Oracle Cloud Infrastructure region and click **Sign In**.
   e. Sign in to the Oracle Cloud Infrastructure Console.

   By browsing:
   a. Sign in to the Oracle Cloud Infrastructure Console.
   b. Open the navigation menu and click **Marketplace**. Under **Marketplace**, click **All Applications**.
   c. In the Marketplace search field, enter WebCenter Portal.
      The Marketplace listings for WebCenter Portal are displayed.
   d. Click the title of the listing you want to use and review the information on the **Overview** page.

2. Accept the terms and restrictions, and then click **Launch Stack**.
   The Create Stack wizard is displayed.
3. Provide information about the stack for the instance.
   a. Stack information:
      - Enter name and description.
      - **Create in Compartment**: Select the compartment.
      - **Terraform version**: Specify the Terraform version and click **Next**.
   b. Configure variables:

      Stack Configuration

      - **Resource Name Prefix:** Enter a prefix (for example, WCP). The name of all compute and network resources will begin with this prefix. It must begin with a letter and it can contain only letters or numbers.
      - **SSH Public key**: Provide the SSH public key (created in Generate SSH key pair).
      - **Enable Object Storage as default storage**: Select this check box if you need object storage as the default storage instead of file system for storing documents. If selected, you need to complete the fields in the Object Storage section.

      Virtual Cloud Network

      If you're using an existing VCN, complete the following:

      - **Network Compartment**: Select the compartment you created earlier.
      - **Existing WebCenter Content Virtual Cloud Network**: Select the VCN provisioned with WebCenter Content.

      If you need to use a new VCN, then select the **Create the Virtual Cloud Network** check box and complete the following:

      - **Network Compartment**: Select the compartment you created earlier.
      - **Virtual Cloud Network Name**: Specify a name for the new VCN to be created for this service.
      - **Virtual Cloud Network CIDR**: Specify a CIDR to assign to the new VCN.

      Object Storage

      This section is optional. Complete this section only if you selected the **Enable Object Storage as default storage** check box in the Stack Configuration section.

      - **Object Storage Compartment**: Select the compartment where the bucket was created.
      - **Bucket Name**: Specify the bucket name which you created earlier.
      - **User OCID**: This will be pre-populated with the current user's OCID. If you are using a different user for creating the API key, specify the user OCID of that user.
      - **Public Key Fingerprint**: Specify the fingerprint from the configuration file (that you copied when you created the user API key as part of the prerequisites).
      - **OCI User Private Key Secret Compartment**: Choose the compartment that holds the secret for the user API private key.
      - **Secret for OCI User Private Key**: Select the secret for the user API private key.
   c. Database Configuration:

- **Database Strategy**: Select the type of database to use for provisioning. The supported databases are: Database System and Autonomous Transaction Processing Database.

  If you selected **Autonomous Transaction Processing Database** as the Database Strategy, then complete the following that are displayed:

- Select the value for **Autonomous Database compartment**.
- Select the value for **Autonomous Database**.
- **Autonomous Database Admin Password Secret Compartment**: Choose the compartment that holds the secret for the Autonomous Database Admin Password.
- **Secret for Autonomous Database Admin Password**: Select the secret for Autonomous Database Admin Password.

  If you selected **Database System** as the Database Strategy, then complete the following that are displayed:

- Select the value for **DB System compartment**.
- Select the value for **DB System OCID**.
- **PDB name**: Provide the PDB name of the DB system.
- Select the value for **DB System Network Compartment**.
- Select the value for **DB System VCN OCID**.
- **DB System PDB User**: Leave the value 'sys' as is. Do not change this user name.
- **DB System Password Secret Compartment**: Choose the compartment that holds the secret for the DB system password.
- **Secret for DB System Password**: Select the secret for DB system password. When defining the secret key, you must have specified a user friendly name for each secret. Use the same name here so that it is easy.
- **DB System SSH Private key Secret Compartment**: Choose the compartment that holds the secret for the DB system SSH private key.
- **Secret for DB System SSH Private key**: Select the secret for DB System SSH private key.

d. Bastion Instance:

- **Bastion Host Subnet CIDR**: Provide the value for Bastion host subnet CIDR. For example, 10.0.2.0/24.
- **Bastion Host Shape**: Select the appropriate Bastion host shape (keep the default value).

e. WebCenter Portal Compute Instance:

- **Compute Shape**: Select the appropriate compute shape.
- **OCPU count**: Select the OCPU count. The default value is 2.
- **WebCenter Portal Subnet CIDR**: Provide the value for WebCenter Portal subnet CIDR. For example, 10.0.3.0/24.
- **Node Count**: Specify the node count. The default value is 2.

f. WebCenter Content Compute Instance:

- **Compute Shape**: Select the appropriate compute shape.
- **OCPU count**: Select the OCPU count. The default value is 2.

- **Node Count**: Specify the node count. The default value is 2.

g. File System:

- **File System Compartment**: Choose the compartment where the WebCenter Content stack will be created.
- **File System Availability Domain**: Select the Availability Domain.
- **Mount Target Subnet CIDR**: This field is shown if you use an existing VCN. Provide the value for Mount Subnet CIDR. For example, 10.0.4.0/24.

h. Load Balancer:

- Provide the value for **Load Balancer Subnet CIDR**. For example, 10.0.5.0/24. This field is shown if you use an existing VCN.
- Provide the value for **Minimum Bandwidth for Flexible Load Balancer**.
- Provide the value for **Maximum Bandwidth for Flexible Load Balancer**.

i. Identity Cloud Service Integration:

- **Identity Domain URL**: Provide the value for IDCS domain URL.
- **Identity Client ID**: Provide the value for IDCS Client ID.
- **Identity Client Secret Compartment**: Choose the compartment that holds the secret for the IDCS client secret.
- **Secret for the Identity Client Secret**: Select the secret for the IDCS client secret.

j. WebCenter Portal WebLogic Domain Configuration:

- **WebCenter Portal Admin User Name**: Leave the value 'weblogic' as is.
- **WebCenter Portal Admin Secret Compartment**: Choose the compartment that holds the secret for the WebCenter Portal Server administrator password.
- **Secret for WebCenter Portal Admin Password**: Select the secret for WebCenter Portal administrator password.
- **WebCenter Portal Schema Password Secret Compartment**: Choose the compartment that holds the secret for the WebCenter Portal schema password.
- **Secret for the WebCenter Portal Schema Password**: Select the secret for the WebCenter Portal schema password.

Click **Next**. Review all the configuration variables and then select the **Run apply** check box under **Run apply on the created stack** section. Click **Create**.

If everything goes as expected, then navigate to the WebCenter Portal stack and click the **Application Information** tab. Under the Output section, you'll see the end points for the services.

- webcenter_portal_x1_weblogic_console_endpoint = "https://<host-IP>:7001/console"
- webcenter_portal_x2_webcenter_portal_endpoint = "https://<host-IP>:8888/webcenter/portal"
- webcenter_portal_x3_webcenter_portal_tools_endpoint = "https://<host-IP>:8889/portalTools"

To navigate to the WebCenter Portal stack:

- In the side menu, select **Developer Services**, **Resource Manager**, and then **Stacks**.
- Select your compartment and click the name of the WebCenter Portal stack you created.

If something goes wrong or if for any reason you want to do a clean-up of all the resources that were provisioned as part of the WebCenter Portal deployment, use **Destroy Job** to do the clean-up.

Additional Steps for Stack Provisioned with a Self-Signed Certificate

If you provisioned the WebCenter Portal stack with a self-signed certificate, then you might encounter issues when trying to upload documents from WebCenter Portal. The upload button might be in a frozen state and will not work, hence the pop-up screen will not be shown. To resolve this issue, complete the following steps.

1. In the browser, open **Developer Tools** using *Ctrl* + *Shift* + *I* (Windows) or *Option* + ⌘ + *I* (Mac) and click the **Network** tab to see the web traffic.

   > **Note:**
   >
   > For Safari browser, navigate to **Settings**, **Advanced** tab, and then to **Show features for web developers** (**Enable**) and then press *Option* + ⌘ + *C* to open Developer Tools and then switch to the Network tab.

2. Refresh the browser tab in which WebCenter Portal was accessed. Navigate to **Home Portal** and click the **Documents** page.
3. Press *Ctrl* + *Shift* + *R (Windows) or* ⌘ *+Shift* + *R (Mac)* to do a hard refresh. In the web traffic, look for a URL that is similar to

   ```
   https://<WebCenter Content host>:16200/cs/idcplg?IdcService=GET_COAO_JS
   ```

   For Safari browser, *Option* + ⌘ + *R can be used to do a hard refresh.*
4. Copy the URL for **GET_COAO_JS** IdcService and open it in a new browser tab. Accept the certificate risk to get the response.
5. Refresh the browser tab in which WebCenter Portal was accessed. Navigate to **Home Portal**, click the **Documents** page and click the **Upload** button to see a pop-up screen for Document Upload in the browser.

> **Note:**
>
> **The above steps need to be completed by all users (for each new browser one time) if users need to resolve the specified issue and upload files using WebCenter Portal Documents Upload UI.**

> **Note:**
>
> **The specified issue with the upload button is not encountered when a CA signed certificate is used.**

4

Configure Elastic Search in Oracle WebCenter Portal

Learn how you can configure Elastic Search to index and search objects in the Marketplace WebCenter Portal instance.

Create a crawl user

1. Log in to the Oracle WebLogic Server administration console.
2. Click **Security Realm** in the **Domain Structure** pane.
3. On the Summary of Security Realms page, select the name of the realm (for example, **myrealm**). Click **myrealm**.
4. Click **Users and Groups** and then the **User** tab.
5. Click the **New** button and add a user by providing a name (for example, **wccrawladmin**) and a password. Note down the name and password for future use.

Install Elasticsearch and Plug-ins

Elasticsearch can be installed as either a single server set-up or a cluster set-up (with a minimum of three servers).

To install a single server set-up, complete the following steps:

1. Log in to the WebCenter Portal machine as an Oracle user and run the following commands:

```
sudo su - oracle

export JAVA_HOME=/u01/jdk/

export PATH=$JAVA_HOME/bin:$PATH

export ORACLE_HOME=/u01/app/oracle/middleware

unset -f $(env | grep -oP "^BASH_FUNC_\K([^%]*)")
```

2. Download the Elasticsearch binary file.

```
cd $ORACLE_HOME/wcportal/es/
wget https://artifacts.elastic.co/downloads/elasticsearch/
elasticsearch-7.17.17-linux-x86_64.tar.gz
```

3. Edit `installES.properties` and update the following properties:

```
ORACLE_HOME=/u01/app/oracle/middleware
ADMIN_SERVER_HOST_NAME=<VM's private IP address>
ADMIN_SERVER_PORT=7001
WLS_ADMIN_USER=<user name for Weblogic server administration console>
```

```
SEARCH_APP_USER=<user name you noted down before in previous steps>
WCP_FMW_CONFIG_LOCATION=/u01/data/domains/wcp_domain/config/fmwconfig
ELASTIC_SEARCH_INSTALLER_LOCATION=elasticsearch-7.17.17-linux-x86_64.tar.gz
ELASTIC_SEARCH_VERSION=7.17.17
```

4. Install the elastic search server using the following command:

```
$ORACLE_HOME/oracle_common/common/bin/wlst.sh
$ORACLE_HOME/wcportal/es/installES.py
$ORACLE_HOME/wcportal/es/installES.properties <weblogic server password>
<search app password you noted down before> <es certificate password you
noted down before>
```

Configure WebCenter Portal for Elasticsearch

To configure WebCenter Portal for search, you need to configure the connection between WebCenter Portal and Elasticsearch, and you need to configure the WebCenter Content crawl user and WebCenter Content administrator in Elasticsearch.

1. Navigate to your Oracle home directory and invoke the WLST script.
2. Connect to the Oracle WebCenter Portal domain (**WC_Portal**) server.
3. At the WLST command prompt, run the `createCred` WLST command to configure the WebCenter Content crawl user in Elasticsearch.

```
$ORACLE_HOME/oracle_common/common/bin/wlst.sh
connect('weblogic server user name', '<weblogic server password>', 't3://
<VM's private IP>:7001')
createCred(map="oracle.es.security", key="content.crawl.credentials",
user='<wcc-crawl-user>', password='<wcc-crawl-password>', desc="UCM Crawl
User")
```

   where,

   - *wcc-crawl-user* is the WebCenter Content crawl user. See Creating a Crawl User in WebCenter Content.
   - *wcc-crawl-password* is the password of the WebCenter Content crawl user.
   - *desc* is the description of the WebCenter Content crawl user.

4. At the WLST command prompt, run the `createCred` WLST command to configure the WebCenter Content administrator in Elasticsearch.

```
createCred(map="oracle.es.security", key="content.admin.credentials",
user='<wcc-admin-user>', password='<wcc-admin-password>', desc="WebCenter
Content administrator")
```

5. At the WLST command prompt, run the `createCred` WLST command to configure the WebCenter Content crawl user in Elasticsearch.

```
$ORACLE_HOME/oracle_common/common/bin/wlst.sh
connect('weblogic server user name', '<weblogic server password>', 't3://
<VM's private IP>:7001')
createCred(map="oracle.es.security", key="content.crawl.credentials",
```

```
user='<wcc-crawl-user>', password='<wcc-crawl-password>', desc="UCM Crawl
User")
```

where,

- *wcc-admin-user* is the WebCenter Content Administrator.
- *wcc-admin-password* is the password of the WebCenter Content Administrator.
- *desc* is the description of the WebCenter Content Administrator.

6. Restart the elastic search server using the following commands:

```
/u01/app/oracle/esHome/stopElasticsearch.sh
/u01/app/oracle/esHome/startElasticsearch.sh
```

7. Navigate to your Oracle home directory and invoke the WLST script to run the following command for creating a search connection.

```
$ORACLE_HOME/oracle_common/common/bin/wlst.sh
connect('weblogic server user', '<weblogic server password>', 't3://<VM's
private IP>:7001')
createSearchConnection(appName='webcenter',name='webcenter-es',
url='http://<wcp-es-machine-ip>:9200', indexAliasName='webcenter_portal',
appUser='<search app user you noted down before>, appPassword='<password
of search app user you noted down before>', server='WC_Portal_server1')
```

where *wcp-es-machine-ip* is the IP address of the host where elastic search server is installed.

8. Restart all the Webcenter Portal managed servers.

Create a Portal Crawl Source

To create a crawl source to crawl objects such as lists, page metadata, page content (contents of HTML, text, and styled text components), portals, and profiles:

1. On the Settings page in WebCenter Portal, click **Tools and Services** or enter the following URL in your browser to navigate directly to the Tools and Services pages:
`http://host:port/webcenter/portal/admin/settings/tools`
2. Click the icon for Search to open the Search Settings page.
3. On the **Scheduler** tab, select the Portal crawl source and click **Edit**.
4. On the Edit Portal Crawl Source page, modify the following source parameters as needed:
   - Maximum number of connection attempts: Maximum number of connection attempts to access the configuration URL. Choose a number from 2 to 10.
   - Configuration URL: URL of the RSS crawl servlet. For example: `http://<WebCenter Portal host>:<port>/rsscrawl` or `http://<WebCenter Portal-VM-IP>:<port>/rsscrawl`.

> **Note:**
>
> In case of HTTPS-based URL for WebCenter Portal, it should be a valid domain host with updated DNS entry and CA-signed certificate.

5. Enter the credentials for the WebCenter Portal crawl administrator.
6. Click **Test** to test the connection.
7. Click **Save and Close** to save the changes.

5

Configure SAML2 IDCS Single Sign-On in WebCenter Portal

Learn to configure SAML2 IDCS Single Sign-On in WebCenter Portal.

Prerequisites

Complete the following before running the configuration script.

Create a WebCenter Portal Stack

A WebCenter Portal stack should have been created from OCI Marketplace on which SAML2 IDCS SSO configuration needs to be configured.

Create an OAuth Client for IDCS
Follow the below instructions based on whether OCI Tenancy IAM is with Identity Domains or not.

- For OCI accounts where IAM is with Identity Domains (tenancy with IAM domains), complete the following:
  1. Log in to OCI console.
  2. Navigate to **Identity** and then **Domains**.
  3. Select the domain which needs to be used for SSO log-in.
  4. Go to **Integrated Applications** and click **Add application**.
  5. Choose **Confidential Application** and launch the workflow.
  6. On the Add Application Details page, fill the **Name** and **Description** fields, and then click **Next**.
  7. On the Configure OAuth page, select the **Configure this application as a client now** option under Client configuration section.
  8. In the Authorization section, select the **Client credentials** check box for the **Allowed Grant Types** field.
  9. Scroll down and select the **Add app roles** check box. In the App roles section, add the **Identity Domain Administrator** role.
  10. Click **Next**. Leave the default settings for the next page as is and click **Finish**.
  11. Make a note of the client ID and client secret. These values will be needed when you run the script.
  12. Activate the application.
- For OCI accounts where IDCS is not yet migrated to IAM Domains (tenancy without IAM domains), complete the following:
  1. Log in to the IDCS administration console of the federated IDCS.
     For example, `https://idcs-abcde.identity.oraclecloud.com/ui/v1/adminconsole`.
  2. Navigate to **Applications**. Click **+** to add an application. Choose **Confidential Application** in the wizard:

a. Add a name and a description on the App details page.

b. Click **Next**. Select the **Configure this application as a client now** option.

c. In the Authorization section, select the **Client credentials** check box for the **Allowed Grant Types** field.

d. In the Grant the client access to Identity Cloud Service Admin APIs section, click **Add** to add the application roles. You need to add the **Identity Domain Administrator** role.

e. Click **Next**. Leave the default settings for the next pages as is and click **Finish**.

f. Make a note of the client ID and client secret. These values will be needed when you run the script.

g. Activate the application.

Configuration in Stack

A configuration helper script will be available in every stack VM. It can be executed from Admin compute VM or VM-1 (*-wls-1) for WebCenter Portal and WebCenter Content domains.

The script expects the following inputs.

Argument	Description
idcs_tenant	IDCS tenant name For example, if IDCS URL is `idcs-abcde.identity.example.com`, then IDCS tenant name would be `idcs-abcde`.
idcs_domain	IDCS domain For example, if IDCS URL is `idcs-abcde.identity.example.com`, then IDCS domain would be `identity.example.com`.
idcs_client	Client ID of the OAuth client created in prerequisites
idcs_client_secret	Client secret of the OAuth client created in prerequisites
service_host	Service host with DNS record mapped to load balancer IP For example, wcpstack1.xyz.com, wccstack1.xyz.com. If service host is not available, a load-balancer IP can be provided here for testing.
idcs_user_name	IDCS user who is configured as WebCenter product administrator user

For WebCenter Portal Domain

Complete the following steps to execute the script:

Run the configure sso script for WebCenter Portal domain from VM having a name like `<*>-wcp-wls-1` with service host value for WebCenter Portal load balancer DNS host or IP.

```
ssh -o ProxyCommand="ssh -W %h:%p -i <key> opc@<bastion-ip>" -i <key>
opc@<wcp-vm-1-ip>

sudo su - oracle
cd /u01/scripts/sh

nohup sh configure_sso.sh --idcs_tenant <idcs-tenant> --idcs_domain
identity.oraclecloud.com --idcs_client <idcs_client> --idcs_client_secret
<idcs_client> --idcs_username <idcs_username> --service_host
<wcp_service_host> &
```

The script execution progress can be monitored from `/u01/logs/provisioning.log`. Once the execution completes without any error, the configuration is completed in the stack environment.

> **Note:**
>
> If the configuration was done with load-balancer IP, then the above script needs to be executed again with the service host once the DNS mapping to WebCenter Portal load-balancer IP is created.

For WebCenter Content Domain

Run the configure sso script for WebCenter Content domain from VM having a name like `<*>-wcc-wls-1` **with service host value for WebCenter Content load balancer DNS host or IP**.

```
ssh -o ProxyCommand="ssh -W %h:%p -i <key> opc@<bastion-ip>" -i <key>
opc@<wcc-vm-1-ip>

sudo su - oracle
cd /u01/scripts/sh

nohup sh configure_sso.sh --idcs_tenant <idcs-tenant> --idcs_domain
identity.oraclecloud.com --idcs_client <idcs_client> --idcs_client_secret
<idcs_client> --idcs_username <idcs_username> --service_host
<wcc_service_host> &
```

The script execution progress can be monitored from `/u01/logs/provisioning.log`. Once the execution completes without any error, the configuration is completed in the stack environment.

> **Note:**
>
> If the configuration was done with load-balancer IP, then the above script needs to be executed again with the service host once the DNS mapping to WebCenter Content load-balancer IP is created.

Configuration in your IDCS Tenant

Once the SAML configuration is completed on WebCenter Portal, SAML applications will be created under Integrated Applications in the IDCS domain. The WebCenter Portal/WebCenter Content role mapping groups (as described in the tables below) are also created.

WebCenter Portal Group	Description
WebcenterGroup	The admin role is assigned to the system administrator. By default, this role has Admin permission to all security groups and all accounts, and has rights to all the administration tools.

WebCenter Content Groups	Description
admin	The admin role is assigned to the system administrator. By default, this role has Admin permission to all security groups and all accounts, and has rights to all the administration tools.

WebCenter Content Groups	Description
contributor	The contributor role has Read and Write permissions to the Public security group, which enables users to search for, view, check in, and check out content.
guest	The guest role has Read permission to the Public security group, which enables users to search for and view content.
sysmanager	The sysmanager role has privileges to access the Admin Server links from the **Administration** menu in the user interface.

The Admin user is granted membership to the WebcenterGroup/admin group and can be used to access the service.

The SAML applications will be prefixed with the stack service name. Examples: wcp12_wcp_saml, wcp12_wcc_saml.

Add Users to Groups

To add a new user other than the administrator, you would need to add the user to the IDCS WebCenter Portal/WebCenter Content groups based on the permissions required for their usage.

Verification

After the configuration of SAML, verify the WebCenter Portal application URLs and validate that the IDCS SSO log-in is working.

Portal Server: `https://<WebCenter Portal service_host|lb_ip>:8888/webcenter/portal`

Content Server: `https://<WebCenter Content service_host|lb_ip>:16200/cs`

Web UI: `https://<WebCenter Content service_host|lb_ip>:16225/wcp`

Capture: `https://<WebCenter Content service_host|lb_ip>:16400/dc-console`

Imaging: `https://<WebCenter Content service_host|lb_ip>:16000/imaging`

6
Troubleshoot

This chapter describes common problems that you might encounter and also provides information that can be helpful with the troubleshooting process.

Issue	Description
Provisioning failed	If you encountered a failure when trying to provision WebCenter Portal, do the following to see the logs which might help in troubleshooting: 1. Log in to bastion host. 2. From bastion host perform ssh to wls-1 VM. For example: `ssh -I <private key> opc@<IP Address of wls-1 VM>` 3. `sudo su - oracle` 4. `cd /u01/data/domains/logs` 5. `vi provisioning.log`