

# Oracle® Cloud

## Deploying Oracle Content Management on Oracle Cloud Infrastructure



F20444-60  
August 2023



Oracle Cloud Deploying Oracle Content Management on Oracle Cloud Infrastructure,

F20444-60

Copyright © 2019, 2023, Oracle and/or its affiliates.

Primary Author: Sarah Bernau

Contributors: Chris DeGrace, Marcus Diaz, Pramondini Gattu, Prabhakar Singh, Ron van de Crommert

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, and MySQL are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

# Contents

## Preface

---

|                             |     |
|-----------------------------|-----|
| Audience                    | vi  |
| Documentation Accessibility | vi  |
| Diversity and Inclusion     | vi  |
| Related Resources           | vi  |
| Conventions                 | vii |

## 1 Overview of Oracle Content Management

---

|  |     |
|--|-----|
| Access Oracle Content Management               | 1-1 |
| Understand Roles                               | 1-2 |
| Manage Assets                                  | 1-2 |
| Collaborate on Documents                       | 1-3 |
| Build Sites                                    | 1-3 |
| Integrate and Extend Oracle Content Management | 1-4 |
| Get Started                                    | 1-4 |
| Migrate to Oracle Cloud Infrastructure         | 1-4 |
| Starter vs. Premium Edition                    | 1-4 |
| Upgrade to the Premium Edition                 | 1-7 |

## 2 Deploy Oracle Content Management

---

|   |     |
|---|-----|
| Understand Your Deployment Architecture Options                           | 2-1 |
| Oracle Content Management Native Disaster Recovery                        | 2-2 |
| Benefits of Oracle Content Management Disaster Recovery                   | 2-3 |
| Disaster Recovery Terminology and Concepts                                | 2-4 |
| Failover Recovery Process   | 2-5 |
| Switchover Testing Process  | 2-5 |
| Implement Disaster Recovery   | 2-5 |
| Data Center Support for Disaster Recovery                                 | 2-6 |
| Beyond High Availability  | 2-7 |
| Set Up a Test to Production (T2P) Deployment                              | 2-8 |
| Install the Oracle Content Management Toolkit on Your VM Compute Instance | 2-9 |

|   |      |
|---|------|
| Register Your Source and Target Servers                     | 2-10 |
| Transfer Your Enterprise Sites                              | 2-11 |
| Does My Region Use IAM Identity Domains?                    | 2-11 |
| Deploy OCM in a Region with Identity Domains                | 2-12 |
| Create and Activate an Oracle Cloud Account                 | 2-13 |
| Create an OCM Instance in a Region with Identity Domains    | 2-14 |
| Create a Compartment for Oracle Content Management          | 2-14 |
| Delegate Creation of OCM Instances to Other Users           | 2-15 |
| Create Your Instance in a Secondary Domain                  | 2-17 |
| Create Your Instance in Another Region                      | 2-18 |
| Create a Private Instance Using FastConnect                 | 2-19 |
| Create Your Oracle Content Management Instance              | 2-23 |
| Set Up Users and Groups Using IAM                           | 2-28 |
| Create Groups for Your Organization                         | 2-29 |
| Assign Roles to Groups                                      | 2-29 |
| Add Users   | 2-30 |
| Assign Users to Groups                                      | 2-30 |
| Deploy OCM in a Region without Identity Domains             | 2-31 |
| Create and Activate an Oracle Cloud Account                 | 2-31 |
| Create an OCM Instance in a Region without Identity Domains | 2-32 |
| Create a Compartment for Oracle Content Management          | 2-33 |
| Delegate Creation of OCM Instances to SSO Users             | 2-33 |
| Delegate Creation of OCM Instances to Non-Federated Users   | 2-34 |
| Create Your Instance in a Secondary IDCS Domain             | 2-37 |
| Create an Instance in Another Region                        | 2-39 |
| Create a Private Instance Using FastConnect                 | 2-39 |
| Create Your Oracle Content Management Instance              | 2-42 |
| Set Up Users and Groups Using IDCS                          | 2-47 |
| Create Groups for Your Organization                         | 2-47 |
| Assign Roles to Groups                                      | 2-48 |
| Add Users   | 2-49 |
| Assign Users to Groups                                      | 2-49 |

### 3 What to Do Next

---

### 4 Manage the Service

---

|  |     |
|--|-----|
| Edit Your Oracle Content Management Instance | 4-1 |
| Monitor Billing and Usage                    | 4-4 |
| Report Issues                                | 4-5 |

|  |      |
|--|------|
| Manage Vanity Domains  | 4-5  |
| Understand the Different Types of Domains                                | 4-6  |
| Use a Content Delivery Network   | 4-7  |
| Use Oracle Content Management's Content Delivery Network                 | 4-7  |
| Manage a Domain with a Domain Name System                                | 4-7  |
| Deploy Certificates  | 4-8  |
| Set Up a Site Vanity Domain  | 4-8  |
| Configure a Site With a Site Vanity Domain                               | 4-8  |
| Configure the CDN to Route Requests to a Public Site                     | 4-9  |
| Configure the CDN to Route Requests to a Secure Site                     | 4-10 |
| Set Up an Instance Vanity Domain   | 4-11 |
| Configure Oracle Content Management With Your Instance Vanity Domain     | 4-11 |
| Configure the CDN When Using Standard Paths                              | 4-11 |
| Configure the CDN When Using Short Paths                                 | 4-12 |
| Set Up a Vanity Domain for Oracle Content Management Itself              | 4-14 |
| Configure Your CDN for Your Friendly Management Domain                   | 4-14 |
| Using a Friendly Management Domain in a Private Instance                 | 4-15 |
| Configure Oracle Content Management with Your Friendly Management Domain | 4-17 |

## 5 Service Limits, Quotas, Policies, and Events

---

|   |     |
|---|-----|
| Service Limits  | 5-1 |
| Service Quotas  | 5-1 |
| Service Policies  | 5-2 |
| Resource Types for Oracle Content Management                            | 5-2 |
| Supported Variables   | 5-2 |
| Details for Verb and Resource-Type Combinations                         | 5-3 |
| Permissions Required for Each API Operation                             | 5-4 |
| Example Policy Statements to Manage Oracle Content Management Instances | 5-5 |
| Service Events  | 5-6 |

# Preface

*Deploying Oracle Content and Experience on Oracle Cloud Infrastructure* describes how to deploy Oracle Content Management running on Oracle Cloud Infrastructure (OCI) and how to monitor service activity.

## Audience

*Deploying Oracle Content and Experience on Oracle Cloud Infrastructure* is intended for Oracle Cloud administrators who will set up and configure the Oracle Content Management 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.

## Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

## Related Resources

For more information, see these Oracle resources:

- *Getting Started with Oracle Cloud*
- *Administering Oracle Content Management*

- *Collaborating on Documents with Oracle Content Management*
- *Managing Assets with Oracle Content Management*
- *Building Sites with Oracle Content Management*
- *Developing with Oracle Content Management As a Headless CMS*
- *Integrating and Extending Oracle Content Management*
- *What's New for Oracle Content Management*
- *Known Issues for Oracle Content Management*

## Conventions

The following text conventions are used in this document:

| Convention      | Meaning  |
|-----------------|--|
| <b>boldface</b> | Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.         |
| <i>italic</i>   | 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

## Overview of Oracle Content Management

Whether you need to manage digital assets, publishing to multiple channels in various languages, or oversee business documents gathered from a variety of sources, Oracle Content Management helps you throughout the entire content lifecycle. Create, capture, organize, review, and protect all your content as it flows through your organization with integrated processes and data. Oracle Content Management is a cloud-based content hub, offering scalability, security, and governance, so you can eliminate the typical inefficiencies in content management—including organizing and tagging new content and locating existing documents—and do more with fewer resources.

Using Oracle Content Management for digital asset management, you can rapidly collaborate internally and externally on any device to approve content and create contextualized experiences. Built-in business-friendly tools make building new web experiences with stunning content a breeze. You can drive digital engagement with all your stakeholders using the same content platform and the same processes. Technical and organizational bottlenecks are gone, so you no longer have barriers to create engaging experiences, improving customer and employee engagement.

Using Oracle Content Management for business document management, you have the same collaboration capabilities internally and externally on any device to manage your content. Integrated tools such as content connectors enable you to upload content from third-part cloud storage, and Content Capture makes it easy to *automate* document discovery and capture.



### Note:

Oracle Content Management Starter Edition has a limited feature set. To take advantage of the full feature set, upgrade to the Premium Edition.

## Access Oracle Content Management

After you've been granted access to Oracle Content Management, you receive a welcome email with details about the instance URL and your user name. You'll need this information to log in to the service, so it's a good idea to keep it for future reference.

There are different ways to interact with Oracle Content Management:

- The web interface provides easy access from your favorite web browser. You can manage your content in the cloud, share files and folders with others, start and participate in conversations, create websites (if allowed), and more.
- The desktop app lets you keep your files and folders synchronized between the cloud and your computer. You can sync your own files and those shared with you, making sure you always have access to the latest versions.
- A Microsoft Office add-on gives you access to Oracle Content Management features directly from Microsoft Word, Excel, PowerPoint, and Outlook.



- Mobile apps for Android and iOS provide easy access on your phone or other mobile devices. The mobile apps are instantly familiar, because they look and act just like the service in your web browser. You can access your cloud content, search and sort your files and folders, share content, and work with conversations.
- REST APIs and SDKs provide developers with powerful tools to programmatically incorporate Oracle Content Management functionality into web applications and mobile apps.

## Understand Roles

The Oracle Content Management features that you can access depend on the role you've been assigned. You'll see different options depending on your application role. Standard users can work with documents, conversations, and sites. Enterprise users can also access assets. Developers see options to build and customize website pieces such as templates, themes, components, and layouts. Administrators see options to configure the service, integrate the service with other business applications, and set up asset repositories.

There are different types of roles in Oracle Content Management:

- **Organization roles** — Your role within your organization determines what tasks you need to perform and how you use features.
- **Application roles** — Application roles control what features you see in Oracle Content Management.
- **Resource roles** (permissions) — What you can see and do with a resource, such as a document, content item, site, or template, depends on the role you're assigned when the resource is shared with you.

Learn more...

## Manage Assets

Oracle Content Management offers enterprise users powerful capabilities to manage all your assets whether you need to manage digital assets, publishing to multiple channels in various languages, or oversee business documents gathered from a variety of sources. It provides a central content hub for all your assets, where you can organize them into repositories and collections, and create rules to define how they can be used and where.

There are also extensive management and workflow features to guide assets through their creation and approval process and to ensure that only authorized versions are available for use.

It's easy to tag and filter assets so you can quickly find the assets you need. And smart content features will tag and suggest assets automatically as you use them!

Create asset types to define what information you need to collect when users create assets. *Digital asset types* define the custom attributes required for your digital assets (files, images, and videos) and business documents. *Content types* group different pieces of content into reusable units. Users can then create digital assets, business documents, and content items based on these asset types for consistent use.

Learn more...

## Collaborate on Documents

With Oracle Content Management, you can manage your content in the cloud, all in one place and accessible from anywhere.

You can group your files in folders and perform common file management operations (copy, move, delete, and so on) in much the same way as on your local computer. And since all your files reside in the cloud, you have access to them wherever you go, also on your mobile devices. If you install the desktop app, all your content can be automatically synchronized to your local computer, so you always have the most recent versions at your fingertips.

After you get all your content in the cloud, it's easy to share your files or folders to collaborate with others inside or outside your organization. Everyone you share your content with has access to the latest information—wherever they are, whenever they need it. You can grant access to entire folders or provide links to specific items. All access to shared items is recorded, so you can monitor how and when each shared item was accessed.

Conversations in Oracle Content Management allow you to collaborate with other people by discussing topics and posting comments in real time. You can start a stand-alone conversation on any topic, adding files as needed. Or you can start a conversation about a specific file, folder, asset, or site for quick and easy feedback.

All messages, files, and annotations associated with a conversation are retained, so it's easy to track and review the discussion. And your conversations live in the cloud, so you can also view them and participate on the go from your mobile devices.

[Learn more...](#)

## Build Sites

With Oracle Content Management, you can rapidly build and publish marketing and community websites—from concept to launch—to provide engaging online experiences. The process is completely integrated: content, collaboration, and creativity are combined in a single authoring and publishing environment.

To get started quickly, use an out-of-the-box template, drag-and-drop components, sample page layouts, and site themes to assemble a site from predefined building blocks. Or developers can create custom templates, custom themes, or custom components to create unique online experiences.

Add YouTube videos, streaming videos, images, headlines, paragraphs, social media links, and other site objects simply by dragging and dropping components into designated slots on a page. Switch themes and rebrand a site at the touch of a button to provide an optimized, consistent look and feel across your organization.

You can work on one or more updates, preview an update in the site, and then, when you're ready, publish the update with a single click.

In addition to creating and publishing sites in Site Builder, Oracle Content Management also supports 'headless' site development using REST APIs, React JS, Node JS, and other web technologies.

[Learn more...](#)

# Integrate and Extend Oracle Content Management

As an Oracle Platform-as-a-Service (PaaS) offering, Oracle Content Management works seamlessly with other Oracle Cloud services.

You can embed the web UI into your web applications so users can interact with content directly. Use the Application Integration Framework (AIF) to integrate third-party services and applications into the Oracle Content Management interface through custom actions. Or develop content connectors to bring content that you have already created elsewhere into Oracle Content Management, manage it centrally, and use it in new experiences across multiple channels.

With a rich set of REST APIs and SDKs for content and site management, delivery, and collaboration, you can incorporate Oracle Content Management functionality into your web applications.

Create client applications that interact with your content SDKs and assets in the cloud. Develop custom integrations with collaboration objects or retrieve assets for use wherever you need them. You can access and deliver all your content and assets optimized for each channel, whether it's through a website, content delivery network (CDN), or mobile apps.

Learn more...

## Get Started

To help you get started with Oracle Content Management, visit the [Oracle Help Center](#), which has lots of resources, including [documentation](#), [videos](#), [guided tours](#), and [developer information](#).

And if you need it, there's [support](#) and a [community](#) to help.

## Migrate to Oracle Cloud Infrastructure

If your Oracle Content Management subscription isn't already running on Oracle Cloud Infrastructure (OCI) with the Infrastructure Console, then Oracle recommends that you migrate to that native OCI environment. This will ensure that you'll enjoy the benefits and advances of Oracle's cloud platform in the future.

Migration is not automatic; you'll need to submit a service request to initiate the process.























Learn more...

## Starter vs. Premium Edition













The Oracle Content Management Starter Edition offers a free content service tier with a limited feature set and limits on the number of users, assets, sites, and other items. However, it's sufficient to work with Oracle Content Management out of the box.

To take advantage of the full feature set and to increase the number of users and other items, [upgrade to the Premium Edition](#).

The following table shows a comparison of the features and limits in the Starter Edition vs. the Premium Edition.

| Feature  | Starter Edition  | Premium Edition  |
|--|--|--|
| Users  | <br>Only 5 users<br>No limit for SaaS entitlement   | <br>Unlimited   |
| Repositories   | <br>Only one asset repository; no business repositories   | <br>Unlimited business and asset repositories   |
| Digital assets, business documents, and content items (structured content) |  <ul style="list-style-type: none"> <li>• Only 5,000 assets for free (25,000 if bundled with a SaaS service)</li> <li>• Includes out-of-the-box asset types for images, videos, and files</li> <li>• Only 5 custom asset types</li> <li>• No custom renditions (supports automated renditions)</li> </ul> | <br>Unlimited   |
| Taxonomies   | <br>Only two taxonomies   | <br>Unlimited   |
| Publishing channels  | <br>Only one publishing channel, not including site channel   | <br>Unlimited   |
| Workflows  | <br>Only basic out-of-the-box approve/reject workflow   | <br>Unlimited<br><br>To use workflows you must create processes in Oracle Integration (sold separately), and integrate Oracle Content Management with Oracle Integration. |
| Batch translation of assets (translation jobs)                             |   |   |
| Ranking policies   |   |   |
| Sites  | <br>Only one site; no site governance   | <br>Unlimited; full access  |
| Experience orchestrations  | <br>Only one experience   | <br>Unlimited   |
| Recommendations  | <br>Only one recommendation   | <br>Unlimited   |


| Feature  | Starter Edition   | Premium Edition   |
|--|---|---|
| Developer interface                                  |    |                              |
| Analytics  | <br>Only basic usage metrics (dashboard)                       |                              |
| Documents  |    |                              |
| Conversations  | <br>No standalone conversations                                | <br>Full access              |
| Integrations   | <br>Only webhooks, proxy service, and APIs                     | <br>Full access              |
| Security in repository                               | <br>No taxonomy-based granular security                        |                              |
| Smart tags and search                                |    |                              |
| Smart authoring                                      |   |                             |
| Video Plus   |    |                            |
| Content Capture<br>(document capture and processing) | <br>Only one procedure; no XML                               | <br>Unlimited; full access |
| <a href="#">Content apps</a>                         |    |                            |
| CDN  |    |                            |
| Vanity URLs (vanity domains)                         | <br>Only one vanity domain for public sites or public assets |                            |
| Mobile apps  |    |                            |
| Desktop app/sync client                              |    |                            |
| Microsoft Office integration                         |    |                            |
| Adobe Creative Cloud extension                       |    |                            |

| Feature                                | Starter Edition   | Premium Edition  |
|--|---|--|
| Oracle Content Management (OCM) groups |    |   |
| Regions in which Gen2 OCI is deployed  | All   | All  |
| Non-primary instances                  |    |   |
| Delayed upgrade                        |    |   |
| Private instances (FastConnect)        |    |   |
| Advanced hosting                       |    |   |
| Home page                              | <br>Doesn't show Recent Items or Quick Links   |   |
| Included OCM outbound data             | <ul style="list-style-type: none"> <li>OCM Universal Credit Starter Edition (B93411) includes 10GB of OCM outbound data per instance per month</li> <li>OCM SaaS Starter Edition (B93582) includes 100GB OCM outbound data per 5,000-asset pack</li> </ul>                                      | <ul style="list-style-type: none"> <li>OCM Universal Credit Premium Edition (B91210) and OCM for SaaS Premium Edition (B91221) include 10TB of OCM outbound data per instance per month</li> </ul>   |
| Included object storage                | <ul style="list-style-type: none"> <li>OCM Universal Credit Starter Edition (B93411) uses OCI Object Storage which includes 10GB free object storage per cloud account</li> <li>OCM SaaS Starter Edition (B93582) includes 100GB of OCM for SaaS Object Storage per 5,000-asset pack</li> </ul> | <ul style="list-style-type: none"> <li>OCM Universal Credit Premium Edition (B91210) uses OCI Object Storage which includes 10GB free object storage per cloud account</li> <li>OCM for SaaS Premium Edition (B91221) includes 5TB of OCM Object Storage per 5,000-asset pack</li> </ul> |


## Upgrade to the Premium Edition

[View the guided tour on upgrading to the Premium Edition.](#)

To take advantage of the full feature set and remove all restrictions, upgrade to the Premium Edition:

1. Navigate to the [Subscription Details](#) page to see what type of Oracle Cloud account you have:
  - a. Sign in to [Oracle Cloud](#) as the cloud account administrator. You can find your account name and login information in your welcome email.
  - b. In the Oracle Cloud Console, click  in the top left to open the navigation menu, click **Billing & Cost Management**, then, under **Billing**, click **Subscriptions**.

If you have a Universal Credit account, continue with the steps to upgrade your instance to the Premium Edition. If you have a SaaS service subscription, talk to your Oracle account representative.

2. In the Oracle Cloud Console, click , click **Developer Services**, then, under **Content Management**, click **Instances**. This opens the Content Management Instances page.
3. Open your instance.
4. Click **Edit Instance**.
5. Change the License Type to **Premium Edition**, and then click **Save Changes**.
6. Sign back in to Oracle Content Management to see all features unlocked and restrictions removed.

# 2

## Deploy Oracle Content Management

Before you deploy Oracle Content Management, you need to [understand your deployment options](#) and decide whether you'll use the [Starter Edition or Premium Edition](#).

Oracle is in the process of updating Oracle Cloud Infrastructure (OCI) regions to switch from Identity Cloud Service (IDCS) to Identity and Access Management (IAM) identity domains. All new Oracle Cloud accounts will automatically use IAM identity domains. [Depending on whether your region uses IAM identity domains or not](#), you'll use different documentation to complete your deployment.

- If your region *has* been updated, follow the steps in [Deploy OCM in a Region with Identity Domains](#)
- If your region *hasn't* been updated, follow the steps in [Deploy OCM in a Region without Identity Domains](#)

After you've deployed your instance, you might want to enable additional features.

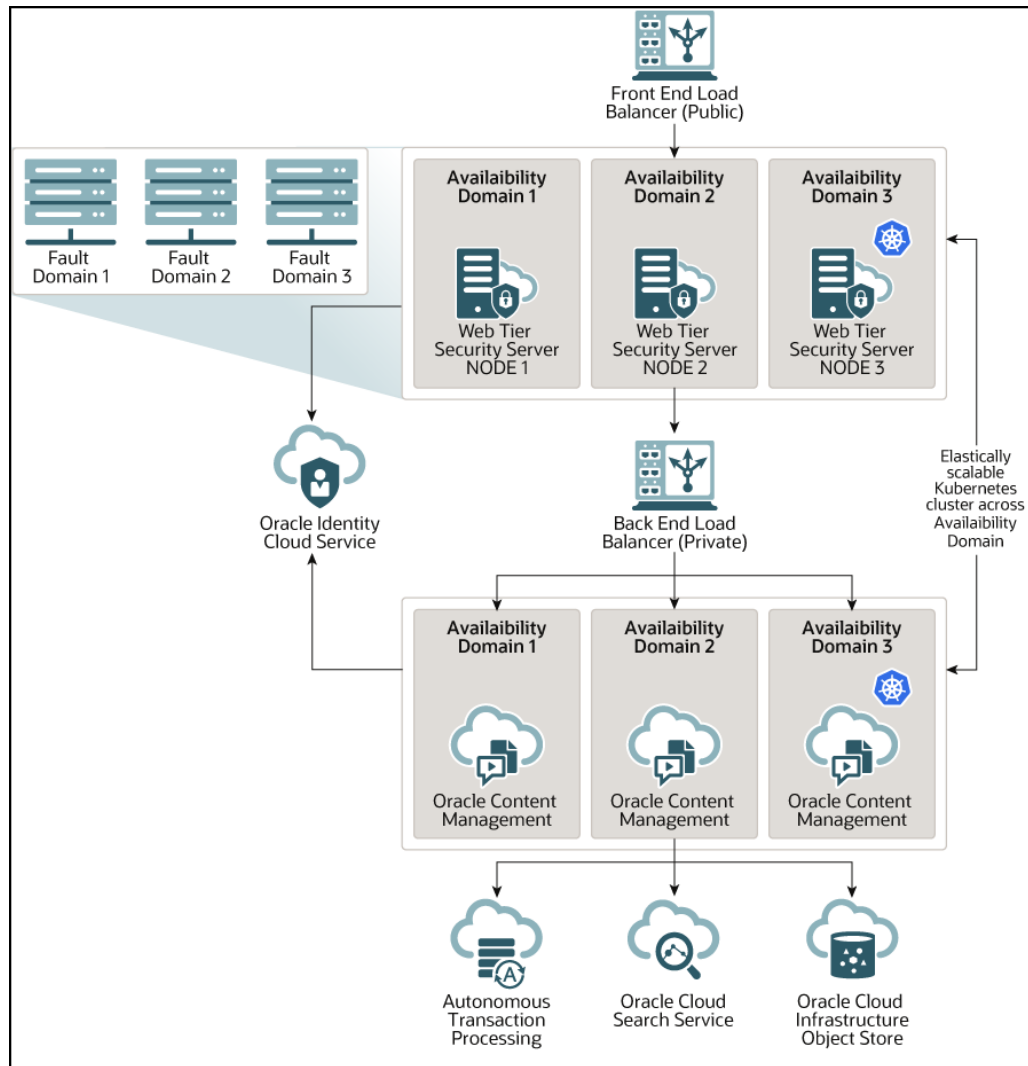
## Understand Your Deployment Architecture Options

When initially provisioned, all instances of Oracle Content Management are deployed on Oracle Cloud Infrastructure. This architecture is a high-availability topology across multiple availability domains within a single geographic region. It uses Oracle Container Engine for Kubernetes (OKE) with its elastically scalable Kubernetes clusters across these availability domains.

- **Availability Domains**—An availability domain is one or more data centers located within a region. Availability domains are isolated from each other, fault tolerant, and unlikely to fail simultaneously. Because availability domains don't share physical infrastructure, such as power or cooling, or the internal availability domain network, a failure that impacts one availability domain is unlikely to impact others. Availability domains in a region are connected to each other by a low-latency, high-bandwidth network. This predictable, encrypted interconnection between availability domains provides the building blocks for both high availability and disaster recovery.
- **Fault Domains**—A fault domain is a grouping of hardware and infrastructure within an availability domain. Each availability domain contains three fault domains. Fault domains let you distribute your instances so that they are not on the same physical hardware within a single availability domain. As a result, hardware failures or maintenance events that affect one fault domain do not affect instances in other fault domains. You can optionally specify the fault domain for a new instance at launch time, or you can let the system select one for you.

In a default deployment, OKE automatically creates multiple clusters (or nodes) across availability domains. All sites and assets are synchronized to each availability domain. If one availability domain goes down, OKE automatically directs all incoming traffic to the operational availability domains. That way end users won't notice a service outage while the failed availability domain is being restored.





We encourage you to use our **Upgrade Schedule** option to control when your instance receives a new release of Oracle Content Management. In most cases your instance that serves production traffic should use the *delayed upgrade* option. Instances that are meant for development and testing purposes should use the *upgrade immediately* option. This combination of settings will provide you a full release cycle to ensure your code is robust and provide you time to address any issues before they might impact your production traffic. The Upgrade Schedule option is set when you [create your Oracle Content Management instance](#).

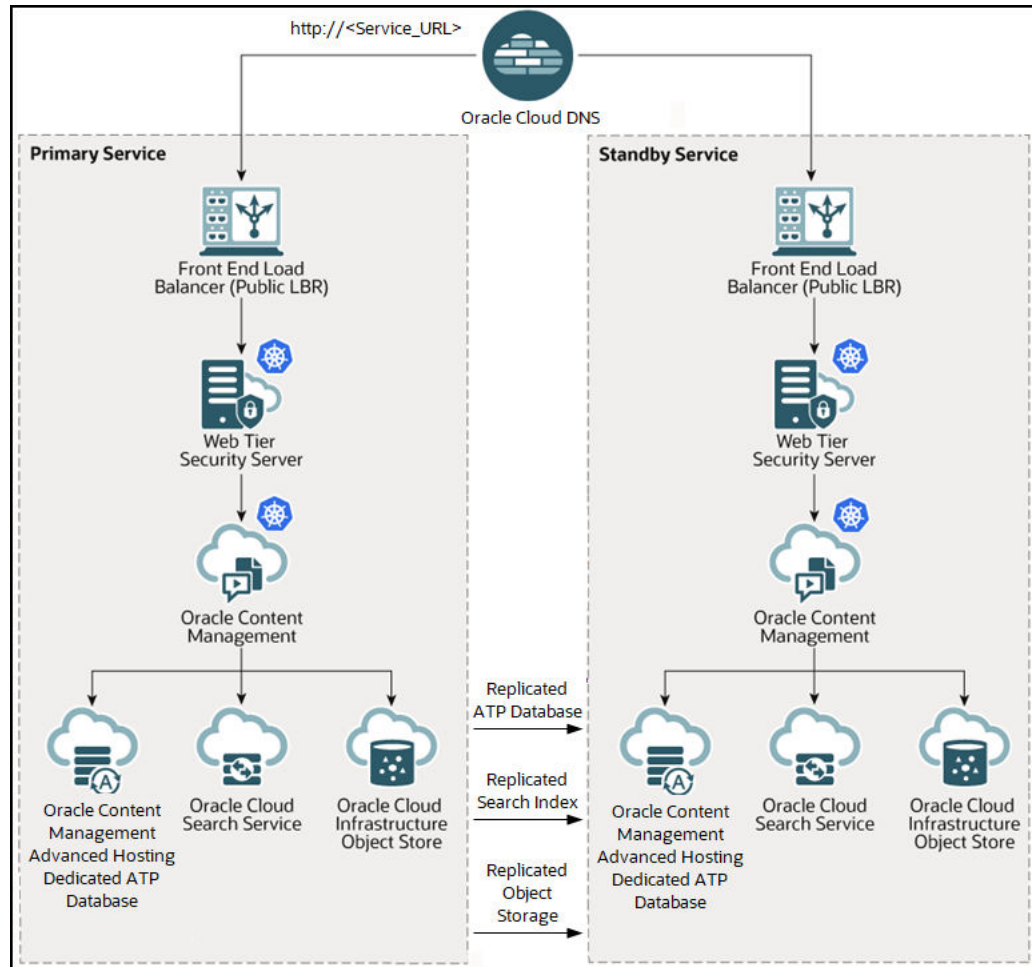
## Oracle Content Management Native Disaster Recovery

Oracle Content Management provides a native disaster recovery product option. The Oracle Content Management disaster recovery product capability essentially provides a full-stack orchestration of the service that includes comprehensive disaster recovery failover capabilities for all layers of the Oracle Content Management application stack including the Oracle Content Management application tiers, database, search index, and object storage.

The terms "Oracle Content Management full-stack disaster recovery", "full-stack disaster recovery", and "disaster recovery" are used interchangeably throughout this documentation. All the terms refer to the same service.

Full-stack disaster recovery assures comprehensive business continuity from a variety of data center outages to ensure that organizations have a minimal impact from region-wide outages.

Oracle Content Management disaster recovery is easily enabled for your Oracle Content Management instance as an add-on product service option. You can actively monitor Oracle Content Management enabled disaster recovery instances via Oracle Cloud Console operations. You can also validate and monitor business continuity readiness and compliance by periodically running disaster recovery switchover tests.



## Benefits of Oracle Content Management Disaster Recovery

Oracle Content Management disaster recovery provides multiple benefits in the area of business continuity.

- **Provides full application recovery:** Oracle Content Management disaster recovery provides recovery for the entire application stack, which includes the components such as database, search indexes, object storage, and the application tier. This full-stack disaster recovery allows for business continuity that depends on recovering the entire application stack instead of a few select components.
- **Minimizes disaster recovery time:** Oracle Content Management disaster recovery eliminates the need to perform manual disaster recovery for individual resources.

- **Eliminates the need for special skills:** The operators and administrators don't require any special skills or domain expertise in areas such as applications and storage replication.
- **Single pane of glass monitoring and management:** Oracle Content Management disaster recovery provides a single pane of glass monitoring and management capability for all Oracle Content Management disaster recovery enabled instances. You can create disaster recovery instances, monitor disaster recovery readiness and check status using the Oracle Cloud Console.

## Disaster Recovery Terminology and Concepts

Before using Oracle Content Management disaster recovery, familiarize yourself with the following key terms and concepts.

- **Disaster Recovery (DR)**—The process of restoring some or all parts of a business system (a service) after an outage. The recovery of this business system occurs across data centers within the same localized geographic area.
- **Full Stack**—A term used to collectively refer to all the functional layers of a business system, application, or software service. An application can be comprised of different functional layers or tiers such as application layer, middleware layer, database layer, and infrastructure layer.
- **Recovery Point Objective (RPO)**—The RPO defines the maximum amount of data loss that can be tolerated as part of the DR restoration. RPO is typically expressed in units of time.
- **Recovery Time Objective (RTO)**—The RTO defines the maximum amount of time that the application or service under DR protection can be unavailable until service is restored. RTO is typically expressed in units of time.
- **Primary**—The production version of an application or service that is currently in use. Disaster recovery refers to the primary version of an application as having a primary role.
- **Standby**—The reserved version of an application or service. Standby is also used to refer to the alternate region in which the application or service will be restored. Disaster recovery refers to the standby version of an application as having a standby role.
- **Warm Standby**—A DR model in which some or all of the components of an application or service are pre-deployed in the standby region to prepare for a future DR transition. This model involves higher operating costs but a lower RTO. Oracle Content Management DR support uses a warm standby implementation.
- **Cold Standby**—A DR model in which very few or none of the components of an application or service need to be pre-deployed in the standby region in preparation for a future DR transition. The application components are deployed as part of the DR transition. This model involves lower operating costs but a higher RTO.
- **Role**—Specifies whether an application and its region is currently the primary (production) version or the standby (reserved) version. An application's role and its region's role changes as a result of a DR transition.
- **Association**—A pair relationship defined between two Oracle Content Management instances. An Oracle Content Management DR enabled instance is associated (paired) in a primary and standby relationship before they can be used to implement DR services.

- **Switchover**—In the case of Oracle Content Management this is a scheduled DR event that performs a planned transition of Oracle Content Management from the primary DR instance to the standby DR instance. Switchover performs an orderly transition by shutting down the application stack in the primary region and then activating the standby service to become active.
- **Failover**—In the case of Oracle Content Management this would be an unscheduled event that requires Oracle to perform a failover transition by activating the Oracle Content Management warm standby instance in the standby region, in the event of a service outage in the primary region.

## Failover Recovery Process

Oracle controls when failover is activated for your Oracle Content Management service. For Oracle Content Management the disaster recovery performance targets are as follows:

- **Recovery Time Objective (RTO) = one hour**—The RTO is the target time that is required to restore your application functionality after a disaster happens. RTO is Oracle's objective for the maximum period of time between Oracle's decision to activate the disaster recovery processes and the point at which you can resume production operations in an alternative site. If the decision to activate disaster recovery processes is made during the period in which an upgrade is in process, the RTO extends to include the time required to complete the upgrade.
- **Recovery Point Objective (RPO) = one hour**—The RPO is Oracle's target timeframe of lost data that your applications can potentially lose during a failover event. Oracle's objective for the maximum period of data loss measured as the time from which the first transaction is lost until Oracle's declaration of the disaster. The RPO does not apply to any data loads that are underway when the disaster occurs.

## Switchover Testing Process

Oracle allows customers to test a switchover of their Oracle Content Management disaster recovery enabled instances. To test switchover, log a service request against your Oracle Content Management instance, and the Oracle support team will work to schedule the test.

## Implement Disaster Recovery

To implement disaster recovery, you must select the following options when you [create an Oracle Content Management instance](#):

- **Advanced Hosting**—You must enable the **Advanced Hosting** license option. Advanced hosting enables a dedicated autonomous transactional processing (ATP) database which is required to support Oracle Content Management's disaster recovery feature. Advanced hosting is an optional feature you can add when creating an Oracle Content Management instance with a Premium Edition or BYOL license. There is an additional billing charge for this option. Refer to your prepaid subscription contract or your Universal Credit contract for additional costs.
- **Disaster Recovery**—Under Advanced Options, you must enable the **Disaster Recovery** option. Disaster recovery is an optional feature you can add when creating an Oracle Content Management instance with a Premium Edition or BYOL license.

**Note:**

**New instances only**—Disaster recovery can be enabled only on new instances, not existing ones.

## Data Center Support for Disaster Recovery

Support for disaster recovery is available in the following Oracle Content Management data center combinations:

| Primary Region     | Standby Region  |
|--------------------|-----------------|
| Ashburn            | Phoenix         |
| Phoenix            | Ashburn         |
| San Jose           | Phoenix         |
| Toronto            | Montreal        |
| Montreal           | Toronto         |
| Tokyo              | Osaka           |
| Osaka              | Tokyo           |
| Mumbai             | Hyderabad       |
| Hyderabad          | Mumbai          |
| Frankfurt          | Amsterdam       |
| Amsterdam          | Frankfurt       |
| Seoul              | Chuncheon       |
| Chuncheon          | Seoul           |
| Dubai              | Abu Dhabi       |
| Abu Dhabi          | Dubai           |
| Sydney             | Melbourne       |
| Melbourne          | Sydney          |
| Sao Paulo          | Vinhedo         |
| Vinhedo            | Sao Paulo       |
| Santiago           | Sao Paulo       |
| Zurich             | Stockholm       |
| Stockholm          | Zurich          |
| Cardiff            | London          |
| London             | Cardiff         |
| Singapore          | Hyderabad       |
| Jeddah             | Abu Dhabi       |
| Johannesburg       | Jerusalem       |
| Jerusalem          | Johannesburg    |
| Milan              | Marseille       |
| Marseille          | Milan           |
| Paris (future)     | Madrid (future) |
| Neom (future)      | Jeddah          |
| Queretaro (future) | Santiago        |
| Chicago (future)   | Ashburn         |

---

| Primary Region  | Standby Region |
|-----------------|----------------|
| Madrid (future) | Paris (future) |

---

## Beyond High Availability

While a high-availability service is designed to deliver a high degree of uptime and accessibility, many customers have additional needs that can be met with different architectures. These additional architectures, while still benefiting from the high availability provided out-of-the-box by Oracle Cloud Infrastructure and OKE, can be built to support development processes, even multi-region failover, or enhanced with private high-performance connections. To find the architecture that's right for your needs, you'll need to determine your organization's development process needs, your acceptable recovery time objectives (RTO), and your recovery point objectives (RPO).

### Private Instance Using Oracle Cloud Infrastructure FastConnect

Some customers may also need additional performance or security that may not be available over the public internet. Oracle Cloud Infrastructure FastConnect can be used to provide a more performant, robust, and secure connection to your Oracle Content Management instance. This type of connection is often used by customers who want to ensure access is limited to internal networks or that end users have the best and most reliable connection possible.

If you want to create such an instance, you need to set up Oracle Cloud Infrastructure FastConnect and perform some additional prerequisite steps. FastConnect provides a dedicated private connection with higher bandwidth and a more reliable and consistent networking experience when compared to internet-based connections.

See [Create a Private Instance Using FastConnect](#).

### Development Process

This refers to the process your organization uses to build and deploy new functionality and content for Oracle Content Management. It can include multiple environments that new functionality and content must go through before being approved for high-level environments and production. A common setup would include environments for development, testing, staging, and, finally, production. Your organization's needs may vary.

Customers who want to utilize multiple instances to support their development processes should provision their additional instances as described in this document but do not need to provision a web application firewall (WAF) in front of them as they will be accessed directly. After you develop content in one of your instances, you can use the command-line interface (CLI) of the Oracle Content Management Toolkit to propagate that content from one Oracle Content Management instance to another.

 **Note:**

When you create an additional instance that won't serve production traffic, you must mark it as *non-primary* so you don't pay for duplicated assets. Primary instances are charged for the total number of assets in the instance. Non-primary instances are charged for a single block of assets per month (for example, 5,000 assets, and, if you have Video Plus, 250 Video Plus assets) regardless of the total number of assets being replicated. For more information, see [Oracle PaaS and IaaS Universal Credits Service Descriptions](#).

To propagate changes, you can use Oracle Content Management Toolkit commands to create sites and manage their life cycles on development, test, and production instances. You can make changes to sites in a development environment and propagate those changes to test and production environments. You can also incorporate this set of command-line utilities into your scripting environments to manage your deployments. With the CLI utilities, you can roll out new items, such as assets and components, as well as updates of existing content.

See [Set Up a Test to Production \(T2P\) Deployment](#).

## Set Up a Test to Production (T2P) Deployment

This model is essential for providing the checks and balances necessary for running a high-availability environment efficiently and to seamlessly manage applications as they move from test to stage to production.

In this deployment you create dedicated instances to keep your development, testing, and production separate.

1. [Create three Oracle Content Management instances](#) with the following settings:
  - **Development**—Instance type: non-primary; Upgrade schedule: immediate upgrade
  - **Testing**—Instance type: non-primary; Upgrade schedule: immediate upgrade
  - **Production**—Instance type: primary; Upgrade schedule: delay upgrade

Setting your development and testing instances to *non-primary* ensures you won't be double-billed for all of your assets in those instances.

Setting your development and testing instances to *upgrade immediately* (as soon as a new release of Oracle Content Management is available) allows you to test the upgrade on those instances, making sure the upgrade doesn't interfere with any sites you've deployed. If you find any issues, you can report them to Oracle Support so they can be fixed before the *delayed upgrade* is applied to your production instance one release later.

2. Create repositories, channels, localization policies, sites, and assets on your *development* instance.
3. Duplicate the repositories, channels, and localization policies on your *testing* and *production* instances.
4. If you haven't already done so, [create a VM Compute instance](#).

5. [Install the Oracle Content Management Toolkit on your VM Compute instance](#) and have it use IDCS authentication.
6. [Register your Oracle Content Management source and target instances.](#)
7. [Transfer your sites and their assets](#) from your source instance to your target instance.
8. Test that your data is being replicated correctly. Make a few changes (less than five) in the source instance, including changes to each object type, then confirm these changes are accurately reflected in the target instance.
9. Sync any users who may need access to the secondary instances. For example, at a minimum, you'll need your administrators and developers synced.

For more information on the Oracle Content Management Toolkit, see Propagate Changes from Test to Production with Oracle Content Management Toolkit in *Building Sites with Oracle Content Management*.

## Install the Oracle Content Management Toolkit on Your VM Compute Instance

To create a Test to Production (T2P) deployment, you need to install the Oracle Content Management Toolkit on your VM Compute instance and have it use IDCS authentication.

Perform the following the steps on your VM Compute instance:

1. [Sign in as an OPC user.](#)
2. Set up NodeJS:
  - a. Install NodeJS as root:

```
sudo -s
cd /usr/local
wget https://nodejs.org/dist/v12.16.2/node-v12.16.2-linux-x64.tar.xz
tar xf node-v12.16.2-linux-x64.tar.xz
exit
```

- b. Add NodeJS to PATH as opc user and reload profile:

```
vi ~/.bash_profile
--- add :/usr/local/node-v12.16.2-linux-x64/bin to the PATH -- e.g:
PATH=$PATH:$HOME/.local/bin:$HOME/bin:/usr/local/node-v12.16.2-linux-
x64/bin
source ~/.bash_profile
```

- c. Test NPM and NodeJS:

```
[opc@ocivm2pm ~]$ npm --version
6.14.4
[opc@ocivm2pm ~]$ node --version
v12.16.2
```

3. Set up the Oracle Content Management Toolkit:



- a. Oracle Content Management Toolkit supports connection via IDCS app, which removes the need to pop up Chromium to authenticate. Set the flag to skip this download:

```
export PUPPETEER_SKIP_CHROMIUM_DOWNLOAD=true
```

- b. Install the toolkit as opc user:

```
wget https://github.com/oracle/content-and-experience-toolkit/archive/master.zip
unzip master.zip
rm master.zip
cd content-and-experience-toolkit-master/sites/
npm install
```

- c. Test the install:

```
[opc@ocivm2pm sites]$ ./node_modules/.bin/cec --version
20.4.1
```

- d. Add soft link to cec binaries as root:

```
sudo -s
ln -s /home/opc/content-and-experience-toolkit-master/sites/node_modules/.bin/cec /usr/local/bin/cec
exit
```

- e. Test that you can run cec from anywhere as opc user:

```
cd
[opc@ocivm2pm ~]$ cec --version
20.4.1
```

- f. Setup cec source folder, and install cec in the folder. This will create a source tree, with a package.json, and do an npm install to fetch dependencies into the source tree.

```
cd
mkdir cec
cd cec
cec install
```

4. Configure IDCS and register your instances following the directions on the [IDCS app page](#).

## Register Your Source and Target Servers

Register the connection details for your source and target instances using the following command. For example, if you're synchronizing content for a test to

production deployment, you might have development (DEV), staging (TEST), and production (PROD) instances.

```
cec register-server DEV -e http://server:port -u username -p password
cec register-server TEST -e http://server:port -u username -p password
cec register-server PROD -e http://server:port -u username -p password
```

- The first value (for example, *DEV*, *TEST*, *PROD*) is the server name used to identify the instance endpoint. This value can be any name you choose.
- The *-e* value is the server and port that make up the URL you use to access the instance.
- The *-u* value is the username. This user must be the user who can access the sites and assets on the source instance or who will own the sites and assets on the target instance.
- The *-p* value is the password for the user.

 **Note:**

You can pass in `--keyfile` to encrypt the password saved in the file.

## Transfer Your Enterprise Sites

Transfer your enterprise sites using the following command:

```
cec transfer-site SiteName -s DEV -d TEST -r RepositoryName -l
LocalizationPolicyName
```

- The first value (*SiteName*) is the name of the site you want to transfer.
- The *-s* value is the source instance name that you registered in the previous step.
- The *-d* value is the target instance name that you registered in the previous step.
- The *-r* value is the repository in the target instance that you want to transfer the site to. This is only required for transferring new enterprise sites to the target instance.
- The *-l* value is the localization policy in the target instance that you want to apply to the transferred site. This is only required for transferring new enterprise sites to the target instance.

If you are updating a site on the target instance, you don't need to include the repository and localization policy.

For more information, see Propagate Changes from Test to Production with Oracle Content Management Toolkit in *Building Sites with Oracle Content Management*.

## Does My Region Use IAM Identity Domains?

Oracle is in the process of updating Oracle Cloud Infrastructure (OCI) regions to switch from Identity Cloud Service (IDCS) to Identity and Access Management (IAM) identity domains. All new Oracle Cloud accounts will automatically use IAM identity domains.

Depending on whether your region uses IAM identity domains or not, you'll use different documentation to manage users, groups, and access. To see if your region includes IAM

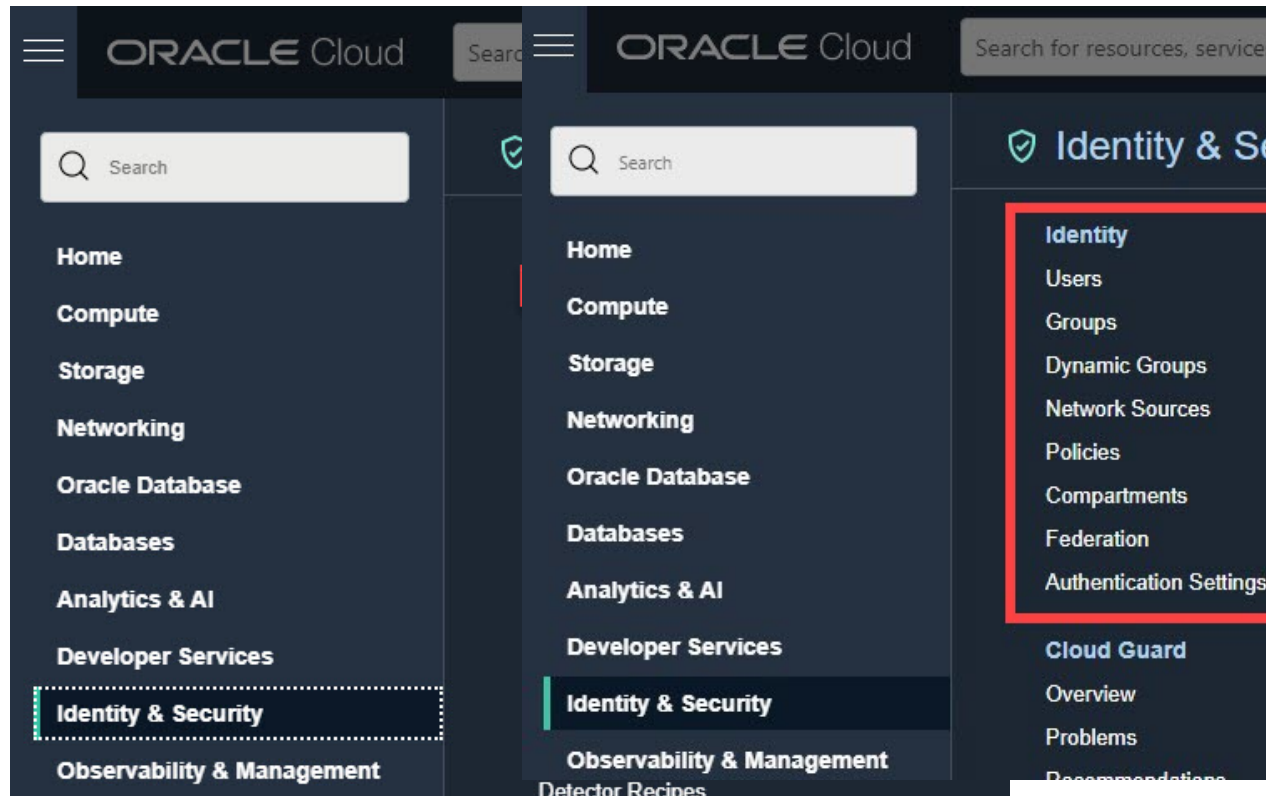
identity domains, sign in to your [Oracle Cloud](#) account as a cloud account administrator. In the navigation menu, click **Identity & Security**. Under **Identity**, check for **Domains**. If you see **Domains**, your cloud account has been updated.

**IAM (updated)**

Region *with* identity domains

**IDCS (not updated)**

Region *without* identity domains



If your region has been updated, use the following documentation:

- [Deploy OCM in a Region with Identity Domains](#)
- In other topics, follow the steps marked **IAM**.

If your region has been updated recently, here's what to expect post update: [OCI IAM Identity Domains: What Oracle IDCS customers need to know](#)

If your region hasn't been updated, use the following documentation:

- [Deploy OCM in a Region without Identity Domains](#)
- In other topics, follow the steps marked **IDCS**.

## Deploy OCM in a Region with Identity Domains

If your Oracle Cloud Infrastructure (OCI) region has been updated and you see **Domains** under **Identity** in the **Identity & Security** section, follow the steps in this section. If you don't see **Domains**, follow the steps in [Deploy OCM in a Region without Identity Domains](#).

To deploy OCM in a region with identity domains:

1. [Create and activate an Oracle Cloud account](#).

2. [Create an Oracle Content Management instance.](#)
3. [Set up users and groups using IAM.](#)

After you've deployed your instance:

- You might want to enable additional features.
- You have a few main tasks to perform in the Oracle Content Management web interface to get Oracle Content Management up and running. See [What to Do Next](#).

The following video shows the basic process of provisioning a new Oracle Content Management instance on Oracle Cloud Infrastructure (OCI) with identity domains.



## Create and Activate an Oracle Cloud Account

There are several ways to create and activate an Oracle Cloud account.

- **Sign yourself up:** Visit <https://signup.oraclecloud.com/> to [sign yourself up](#) and create an account. You'll get a 30-day trial with \$300 of credit; after which, your Universal Credits subscription will begin. Your account will be activated automatically, and you'll receive a welcome email.
- **Contact Oracle Sales:**
  - If you purchase a Universal Credits subscription through Oracle Sales, you need to [create and activate your cloud account through the activation email](#) you receive. After you activate your account, you'll receive a welcome email.
  - If you are a software as a service (SaaS) customer, you must contact your Oracle Sales representative to order Oracle Content Management for SaaS. After you sign the contract for Oracle Content Management, your service will be activated automatically, and you'll receive a welcome email.

### Note:

- You can create multiple Oracle Content Management instances within the same subscription.
- If you switched from a non-metered subscription to a Universal Credits subscription, you'll need to replicate your content to your new service instance. For more information on subscriptions, see [Overview of Oracle Cloud Subscriptions](#).

### What to Do Next

After your account is activated, you need to [create an Oracle Content Management instance](#).

## Create an OCM Instance in a Region with Identity Domains

As the primary account administrator (the person who created the Oracle Cloud subscription), you perform prerequisite steps, and then you or other delegated users can create Oracle Content Management instances from the Oracle Cloud Console.

Creating an Oracle Content Management instance consists of the following steps:


1. [Create a compartment for Oracle Content Management](#).
2. Depending on your specific needs, you may also want to perform some advanced pre-deployment tasks:
  - [Delegate creation of Oracle Content Management instances](#) to other users.
  - [Create your instance in a secondary domain](#) to accommodate different identity and security requirements (for example, one instance for development and one for production).
  - [Create your instance in another region](#) to use services available in other data centers.
  - [Create a private instance](#) to ensure access is limited to internal networks and that end users have the best and most reliable connection possible.
3. [Create your Oracle Content Management instance](#) in the compartment you created.

## Create a Compartment for Oracle Content Management

Compartments are used to organize cloud resources for the purposes of isolation (separating one project or business unit from another), access (through the use of policies), and measuring usage and billing. A common approach is to create a compartment for each major part of your organization (for example, Sales, Human Resources, and so on).

When you create an Oracle Content Management instance, you'll be asked to select a compartment. For security reasons, Oracle strongly recommends creating and using a new storage compartment rather than using the existing root storage compartment.

To create a new compartment for Oracle Content Management:

1. Sign in to [Oracle Cloud](#) as the cloud account administrator. You can find your account name and login information in your welcome email.
2. In the Oracle Cloud Console, click  on the top left to open the navigation menu, click **Identity & Security**, then, under **Identity**, click **Compartments**.
3. On the Compartments page, click **Create Compartment**.
4. Enter a name and description for the compartment. Make clear in your name and description the purpose of the compartment, whether it's specifically for Oracle Content Management, for a project, for a department, or some other purpose.
5. Click **Create Compartment**.  
The newly created compartment may not be available to you immediately. If you don't see it included in selection lists, try again a little later.

You don't need to create a new compartment for every instance. You can use the same compartment for multiple instances.

### What to Do Next

After creating your compartment, perform any necessary advanced pre-deployment tasks or skip right to creating your instance:

- [Delegate creation of Oracle Content Management instances](#) to other users.
- [Create your instance in a secondary domain](#) to accommodate different identity and security requirements (for example, one instance for development and one for production).
- [Create your instance in another region](#) to use services available in other data centers.
- [Create a private instance](#) to ensure access is limited to internal networks and that end users have the best and most reliable connection possible.
- [Create your Oracle Content Management instance](#) in the compartment you created.

## Delegate Creation of OCM Instances to Other Users

To delegate creation of Oracle Content Management instances to users other than the primary account administrator, the primary account administrator must add the users to the Administrators group or add the user to a group with the proper permissions.

Use one of the following methods to delegate users:

- [Add Users to the Administrators Group](#)
- [Add Users to a New Administrative Group](#)

### What to Do Next

After delegating users, perform any other necessary advanced pre-deployment tasks or skip right to creating your instance:

- [Create your instance in a secondary domain](#) to accommodate different identity and security requirements (for example, one instance for development and one for production).
- [Create your instance in another region](#) to use services available in other data centers.
- [Create a private instance](#) to ensure access is limited to internal networks and that end users have the best and most reliable connection possible.
- [Create your Oracle Content Management instance](#) in the compartment you created.

## Add Users to the Administrators Group

To delegate creation of Oracle Content Management instances to users other than the primary account administrator, the primary account administrator can add the users to the Administrators group. The Administrators group is created automatically when you have an Oracle Cloud account running on Oracle Cloud Infrastructure (OCI).

1. Navigate to the Domains page:
  - If you're already in the **Identity & Security** area of the Oracle Cloud Console, in the navigation menu on the left, click **Domains**.
  - If you're not already in the Oracle Cloud Console:
    - a. Sign in to [Oracle Cloud](#) as the cloud account administrator. You can find your account name and login information in your welcome email.



and replacing *CompartmentName* with the name of the compartment you created for Oracle Content Management:

```
Allow group IdentityDomainName/GroupName to manage oce-  
instance-family in CompartmentName
```

- f. Click **Create**.
3. If your delegated users aren't administrators, you must also create the `OCE_Internal_Storage_Policy`, which allows Oracle Content Management to access object storage. Normally this policy is created automatically as part of instance creation, but non-administrators aren't allowed to create policies, so this background process will fail, leaving Oracle Content Management without access to object storage unless you create the policy manually.
    - a. On the Policies page, click **Create Policy**.
    - b. Enter `OCE_Internal_Storage_Policy` as the name, and enter a description.
    - c. Next to Policy Builder, click **Show manual editor**.
    - d. In the box, enter the following statement, replacing *CompartmentName* with the name of the compartment you created for Oracle Content Management:


```
Allow service CEC to manage object-family in compartment  
CompartmentName
```
    - e. Click **Create**.

## Create Your Instance in a Secondary Domain

If you want to create multiple Oracle Content Management instances in separate environments, you need to create a secondary identity domain before you create those additional Oracle Content Management instances.

You might want to create multiple Oracle Content Management instances in separate environments to accommodate different identity and security requirements (for example, one environment for development and one for production). You can accomplish this by creating multiple identity domains. By having separate identity domains, the users who work in one environment won't impact the work of users in another environment. Using multiple instances can also help you maintain the isolation of administrative control over each environment. This is necessary if, for example, your security standards prevent development user IDs from existing in the production environment, or require that different administrators have control over different environments. When multiple instances are utilized, you'll have a *primary* instance, the instance which comes with your Oracle Cloud account, and one or more *secondary* (additional) instances.

To create an Oracle Content Management instance in a secondary identity domain, perform these preliminary steps before you create the Oracle Content Management instance:

1. Navigate to the Domains page:
  - If you're already in the **Identity & Security** area of the Oracle Cloud Console, in the navigation menu on the left, click **Domains**.
  - If you're not already in the Oracle Cloud Console:
    - a. Sign in to [Oracle Cloud](#) as the cloud account administrator. You can find your account name and login information in your welcome email.
    - b. In the Oracle Cloud Console, click , click **Identity & Security**, then, under **Identity**, click **Domains**.



2. Click **Create domain**, and configure the domain. See [Creating Identity Domains](#).
3. Create a policy to allow the Domain\_Administrators group to create and manage Oracle Content Management instances in the new domain.
  - a. On the left, under **Identity**, click **Policies**.
  - b. Click **Create Policy**.
  - c. Enter a name and description. For example, you might name the policy `Tenant_Admin_Policy_for_SecondaryDomain_Domain`, where *SecondaryDomain* is the name of your new domain.
  - d. Next to Policy Builder, click **Show manual editor**.
  - e. In the box, enter the following statement, replacing *SecondaryDomain* with the name of your new domain:

```
Allow group SecondaryDomain/Domain_Administrators to
manage all-resources in tenancy
```
  - f. Click **Create**.
4. You must be signed in to the new domain before you create your Oracle Content Management instance, so sign out of Oracle Cloud, then sign in again, making sure to select the new domain.

#### What to Do Next

After signing in to your new domain, perform any other necessary advanced pre-deployment tasks or skip right to creating your instance in the secondary domain:

- [Delegate creation of Oracle Content Management instances](#) to other users.
- [Create your instance in another region](#) to use services available in other data centers.
- [Create a private instance](#) to ensure access is limited to internal networks and that end users have the best and most reliable connection possible.
- [Create your Oracle Content Management instance](#) in the new domain.

## Create Your Instance in Another Region

If you want to create your Oracle Content Management instance in a region other than your primary region, there are some preliminary steps you need to perform before you create the instance.

Oracle Infrastructure and Platform Cloud Services (Oracle IaaS/PaaS) are enabled in different data centers. These data centers are grouped into data regions based on their geographic locations. When you purchase these services or sign up for a free promotion, you typically choose the data region closest to your location to access them. This becomes your *primary data region*. However, if required, you can extend your subscription to other geographical regions (within the same Oracle Cloud account) and use the services there. For example, if you selected North America as your primary data region during your purchase, you can extend your subscription to the EMEA (Europe, Middle East, and Africa) data region. By doing so, you'll enable your users to use services available in the EMEA data centers.

To create an instance in another region, perform these preliminary steps:

1. [Extend your subscription to another region](#).
2. Switch to the new region by selecting the new region from the **Region** menu.

3. If the new region isn't in the same geographical area as your home region, you must [create a new domain](#) in that region. For example, if your home region is US East (Ashburn), which is in the North America geographical region, and you extend your subscription to Canada Southeast (Toronto), you're not required to create a new domain. However, if you extend your subscription to UK South (London), which is in the EMEA geographical area, you do need to create a new domain in that region. For a list of regions and geographical areas, see [Data Regions for Platform and Infrastructure Services](#).

### What to Do Next

After switching to your new region, perform any other necessary advanced pre-deployment tasks or skip right to creating your instance:

- [Delegate creation of Oracle Content Management instances](#) to other users.
- [Create your instance in a secondary domain](#) to accommodate different identity and security requirements (for example, one instance for development and one for production).
- [Create a private instance](#) to ensure access is limited to internal networks and that end users have the best and most reliable connection possible.
- [Create your Oracle Content Management instance](#) in the new region.

## Create a Private Instance Using FastConnect

You may need additional performance or security that may not be available over the public internet. Oracle Cloud Infrastructure FastConnect can be used to provide a more performant, robust, and secure connection to your Oracle Content Management instance. FastConnect provides a dedicated private connection with higher bandwidth and a more reliable and consistent networking experience when compared to internet-based connections. This type of connection is often used by customers who want to ensure access is limited to internal networks or that end users have the best and most reliable connection possible.



### Note:

If you're using Oracle Content Management Starter Edition, FastConnect isn't supported. To take advantage of the full feature set, upgrade to the [Premium Edition](#).

If you want to create a private instance, you need to review the feature limitations, set up Oracle Cloud Infrastructure FastConnect, and perform some additional prerequisite steps.

Before you can create a private instance, you need to perform the following prerequisite steps:

1. [Review the feature limitations](#).
2. [Set up FastConnect on the tenancy](#).
3. [Get your tenancy OCID and name](#).
4. [Create a local peering gateway](#).
5. [Create a requestor group](#).
6. [Create a requestor policy](#).

7. [Create a support request.](#)
8. [Enable access to safe domains.](#)

## Review the Feature Limitations


Due to the fact that a private instance has, by design, limited networking capabilities, certain features may not work. Features that rely on services outside of Oracle Content Management and outside of your tenancy may not work due to an inability for those services to connect to Oracle Content Management. Features that only reach out, such as outgoing webhooks, email notifications, and other TCP connections on ports 433, 587, 993, 1344, 1521, and 1521 are supported.

The following features are known to be unavailable in private instances:

- External Users
- [Oracle Content Management's built-in Content Delivery Network \(CDN\)](#) for sites and assets
- [Site level vanity domains](#)
- Short paths for [instance level vanity domains](#); only standard paths are supported (for example, `example.com/site/SiteName/`)
- Incoming webhooks
- Public links (users outside of your tenancy won't be able to access these links)
- Microsoft Office Online
- Content connectors:
  - Contentful
  - Dropbox
  - Drupal
  - Google Drive
  - Microsoft OneDrive
  - Microsoft SharePoint Online
  - Oracle WebCenter Content and Oracle WebCenter Content v2.0
  - WordPress.org
  - YouTube
- Translation connectors
- [Sauce Video](#)

## Get Your Tenancy OCID

To get your tenancy's OCID, perform the following steps:



1. If you're not already in the Oracle Cloud Console, sign in to [Oracle Cloud](#) as the cloud account administrator. You can find your account name and login information in your welcome email.
2. In the Oracle Cloud Console, click , click **Governance & Administration**, then, under **Account Management**, click **Tenancy Details**.

3. Next to the **OCID**, click **Copy**. Save this tenancy OCID to include with your support request later.

## Create a Local Peering Gateway


For information on peering, see [Local VCN Peering \(Within Region\)](#).

To create a local peering gateway, perform the following steps:

1. In the Oracle Cloud Console, click , click **Networking**, then click **Virtual Cloud Networks**.
2. Open the VCN you created when you set up FastConnect on the tenancy.
3. Click **Local Peering Gateways**.
4. Click **Create Local Peering Gateway**.
5. Enter a name for the gateway (for example, `customer-to-ocm-lpg`).
6. Select the compartment in which you want to store the peering.
7. Click **Create Local Peering Gateway**.
8. In the list of Local Peering Gateways, click , and then click **Copy OCID**. Save this local peering gateway OCID to include with your support request later.

## Create a Requestor Group

To create a requestor group and add the Oracle Cloud Infrastructure tenancy administrator, perform the following steps:

1. In the Oracle Cloud Console, click , click **Identity & Security**, then, under **Identity**, click **Domains**.
2. Open the identity domain you're using for Oracle Content Management.
3. In the navigation menu on the left, click **Groups**.
4. Click **Create Group**.
5. Enter a name for the requestor group (for example, `RequestorGrp`).
6. Click **Create**.
7. Click the group name to open the group details.
8. On the group details page, click **Assign user to groups**.
9. Select a user with Oracle Cloud Infrastructure tenancy administrator privileges, and then click **Add**.
10. On the group details page, copy the **OCID**. Save this requestor group OCID to include with your support request later.

## Create a Requestor Policy

To create a requestor policy, perform the following steps:

1. In the **Identity & Security** area of the Oracle Cloud Console, in the navigation menu on the left, click **Policies**.

2. Click **Create Policy**.
3. Enter the following details:
  - **Policy:** RequestorPolicy
  - **Description:** Requestor policy for peering
  - **Statement:**

```
Define tenancy Acceptor as OCETenancyOCID
Allow group RequestorGroup to manage local-peering-from in
compartment GroupCompartmentName
Endorse group RequestorGroup to manage local-peering-to in
tenancy Acceptor
Endorse group RequestorGroup to associate local-peering-gateways
in compartment PeeringCompartmentName with local-peering-
gateways in tenancy Acceptor
```

Replace the following values:

- *OCETenancyOCID*: Replace with the realm-specific tenancy OCID from the following table.

| Realm | Tenancy OCID   |
|-------|--|
| oc1   | ocid1.tenancy.oc1..aaaaaaaa4yafecztqb<br>ebznfxpjzwm52wuaeornzgzqrujpbkme<br>z6zuigv7a |
| oc4   | ocid1.tenancy.oc4..aaaaaaamxjaupllkz<br>z2a2qmvcon7rprzlu4hmyfajsfk3ezzmdst<br>terlbya |
| oc8   | ocid1.tenancy.oc8..aaaaaaaanpm5o3ej<br>wjerjyiwsh4u5rd6mpme5ftq44ue5pkxnn<br>hvf3swv2q |

- *RequestorGroup*: Replace with the name of the requestor group you created.
- *GroupCompartmentName*: Replace with the name of the compartment in which you created the requestor group.
- *PeeringCompartmentName*: Replace with the name of the compartment in which you created the peering.

For more information, see [Set up the IAM policies \(VCNs in different tenancies\)](#).

4. Click **Create**.

## Create a Support Request

Create a request with Oracle Support stating you want to create a private service instance. Make sure to include the following information that you collected earlier in your request:

- Tenancy OCID
- Local peering gateway OCID
- Requestor group OCID

Oracle Support will reply with a validation URL for you to test.

### What to Do Next

After you've tested the URL, perform any other necessary advanced pre-deployment tasks or skip right to creating your instance:

- [Delegate creation of Oracle Content Management instances](#) to other users.
- [Create your instance in a secondary domain](#) to accommodate different identity and security requirements (for example, one instance for development and one for production).
- [Create your instance in another region](#) to use services available in other data centers.
- [Create your Oracle Content Management instance](#), making sure to set the **Instance Access Type** to **Private**. You can create multiple instances that use FastConnect in this same domain just by setting the instance access type to private.

## Enable Access to Safe Domains


Throughout Oracle Content Management there are links to documentation, videos, and other such resources outside of Oracle Content Management that your end users will need to access. For this reason, you should consider updating your firewall settings to ensure that any clients using this private instance of Oracle Content Management can reach the following domains:

- [static.ocecdn.oraclecloud.com](http://static.ocecdn.oraclecloud.com) (Required)—This domain is used to load common files for the web client, so if users don't have access to this domain, they won't be able to utilize the web client.
- [\\*.oracleinfinity.io](http://*.oracleinfinity.io) (Required for analytics)
- [oracle.com](http://oracle.com)
- [www.oracle.com](http://www.oracle.com)
- [docs.oracle.com](http://docs.oracle.com)
- [apexapps.oracle.com](http://apexapps.oracle.com)
- [cloudcustomerconnect.oracle.com](http://cloudcustomerconnect.oracle.com)
- [community.oracle.com](http://community.oracle.com)
- [youtube.com](http://youtube.com)
- [consent.truste.com](http://consent.truste.com)
- [consent.trustarc.com](http://consent.trustarc.com)
- [prefmgr-cookie.truste-svc.net](http://prefmgr-cookie.truste-svc.net)
- [consent-st.trustarc.com](http://consent-st.trustarc.com)
- [consent-pref.trustarc.com](http://consent-pref.trustarc.com)



## Create Your Oracle Content Management Instance

To create your Oracle Content Management instance you must be the primary account administrator or the account administrator must have set up your user account with the proper permissions.

To create your Oracle Content Management instance:

1. If you're not already in the Oracle Cloud Console, navigate to it by returning to the window or signing in to [Oracle Cloud](#).
2. Make sure that the region that's selected in the menu in the top right of the Oracle Cloud Console is the one in which you want to create your instance.
3. Click , click **Developer Services**, then, under **Content Management**, click **Instances**. This opens the Content Management Instances page.
4. In the **Compartment** menu on the left, make sure you've selected the compartment you're using for Oracle Content Management. The compartment you created may not be available to you immediately. If you don't see it, try again a little later.
5. Click **Create Instance**.
6. Enter the following information:

| Field                     | Description  |
|---------------------------|--|
| <b>Instance Name</b>      | Specify a unique name for your service instance. If you intend to create multiple instances, make sure your instance name makes clear what the instance will be used for. If you specify a name that already exists, the system displays an error and the instance is not created.   |
| <b>Description</b>        | Optionally, enter a description of the instance.   |
| <b>Compartment</b>        | This is the compartment you previously selected. If you need to, you can change it.  |
| <b>Notification Email</b> | Make sure this is the email address to which you want provisioning status updates to be sent.  |
| <b>License Type</b>       | Choose the type of license you want to use for this instance: <ul style="list-style-type: none"> <li>• <b>Premium Edition:</b> Subscribe to a new full-featured Oracle Content Management license.</li> <li>• <b>BYOL License*:</b> Use your existing Oracle WebCenter Middleware license (BYOL).</li> <li>• <b>Starter Edition:</b> Subscribe to a feature-limited edition of Oracle Content Management.</li> </ul> <p>* The BYOL license type bills for assets at a discounted rate compared to a new Oracle Content Management license. To qualify for an Oracle Content Management BYOL license type your company must already own a qualifying on-premise WebCenter product license that is current on support maintenance. For more information please refer to the <a href="#">Oracle PaaS and IaaS Universal Credits Service Descriptions</a> for a description of which WebCenter products qualify for BYOL licensing and for the conversion ratios for WebCenter processor licenses.</p> |

| Field                  | Description   |
|------------------------|---|
| <b>License Options</b> | <p data-bbox="906 226 1370 401">Optionally, enable additional license options. Enabling any of these options will add additional billing charges to your instance. Refer to your prepaid subscription contract or your Universal Credit contract for additional costs.</p> <ul data-bbox="906 401 1370 1451" style="list-style-type: none"> <li data-bbox="906 401 1370 688"> <p data-bbox="906 401 1370 688">• <b>Advanced Hosting</b> (not available for Starter Edition)—Advanced hosting configures an instance to use a dedicated Autonomous Transactional Database. Enabling this feature also allows the instance to support additional instance options such as disaster recovery (described below). To enable advanced hosting, select <b>Advanced Hosting</b>.</p> <div data-bbox="954 726 1370 926" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p data-bbox="987 764 1110 800"> <b>Note:</b></p> <p data-bbox="1036 825 1333 905">You can't disable this option after the instance has been created.</p> </div> </li> <li data-bbox="906 936 1370 1213"> <p data-bbox="906 936 1370 1213">• <b>Sales Accelerator</b>—Oracle Sales Accelerator provides a one-stop shop for sales enablement content. It allows you to readily access a wide variety of information and resources that make selling your products and services easier. If you <a href="#">purchased an Oracle Sales Accelerator subscription</a>, select <b>Sales Accelerator</b>.</p> </li> <li data-bbox="906 1224 1370 1451"> <p data-bbox="906 1224 1370 1451">• <b>Sauce Video</b>—<a href="#">Sauce Video</a> is the video creation platform for teams. It provides a fast, easy, and affordable way to create video together anywhere, anytime. To enable Sauce Video for your instance, select <b>Video Creation Platform</b>.</p> <div data-bbox="954 1493 1370 1841" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p data-bbox="987 1530 1110 1566"> <b>Note:</b></p> <ul data-bbox="1036 1587 1349 1818" style="list-style-type: none"> <li data-bbox="1036 1587 1349 1728">– If you're an Oracle SaaS customer, you must have purchased a Sauce Video subscription to see this option.</li> <li data-bbox="1036 1738 1349 1818">– All Sauce Video Creation Platform data is stored in London, UK.</li> </ul> </div> </li> </ul> |

7. If you need to enter additional details (for example, if you're creating a non-primary instance), click **Show Advanced Options**, and enter the following information:



| Field  | Description   |
|--|---|
| <b>Instance Type</b> (not supported in Starter Edition)    | <p>By default, the instance type is primary (for example, your production instance). You must have at least one primary instance. If this instance is a non-primary instance (for example, for development or testing), select <b>Non-Primary</b> in the drop-down list. Primary and non-primary instances are <a href="#">billed at different rates</a>.</p> <p>If this is a non-primary instance, you might want to include a tag to specify what the instance is used for.</p>   |
| <b>Upgrade Schedule</b> (not supported in Starter Edition) | <p>Control whether your instance is upgraded immediately (as soon as a new release of Oracle Content Management is available) or on a delayed schedule (one release behind the latest release). For example, let's assume you have stage (non-primary) and production (primary) instances. You would set your stage instance to upgrade immediately and your production instance as delayed upgrade. This allows you to test the upgrade on the stage instance, making sure it doesn't interfere with any sites you've deployed. If you find any issues, you can report them to Oracle Support so they can be fixed before the upgrade is applied to your production instance.</p> <p>If you want to use this feature, but you don't see it, contact Oracle Support.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"><li>• <b>Upgrade immediately:</b> Upgrade this instance as soon as a new release of Oracle Content Management is available.</li><li>• <b>Delay upgrade:</b> Delay the upgrade of this instance, so that it is one release behind the latest release of Oracle Content Management.</li></ul> <p>Once you create this instance, you can't change this setting.</p> |

| Field  | Description  |
|--|--|
| <b>Instance Access Type</b> (not supported in Starter Edition) | <p>Control whether your instance is accessible by public internet or through a dedicated private connection using Oracle Cloud Infrastructure FastConnect.</p> <p>If you want to use this feature, but you don't see it, contact Oracle Support.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> <li><b>Public:</b> Select this option if you want your instance to be viewed over <i>public internet</i>.</li> <li><b>Private:</b> If you want to create a private instance that can be viewed only within your <i>intranet</i>, and you completed the <a href="#">prerequisite steps</a> to set up Oracle Cloud Infrastructure FastConnect, select this option.</li> </ul> <p>Once you create this instance, you can't change this setting.</p> |
| <b>Disaster Recovery</b> (not available for Starter Edition)   | <p>You must enable Advanced Hosting before you can select this option. <a href="#">Disaster recovery</a> provides a full-stack orchestration of the service that includes comprehensive disaster recovery failover capabilities for all layers of the Oracle Content Management application stack, including the Oracle Content Management application tiers, database, search index, and object storage.</p>  |
| <b>Tags</b>  | <p>Optionally, add tags to categorize this instance with metadata. You can then filter your list of instances by tag.</p>  |

8. Click **Create Instance**.



**Note:**

If the creation of your service instance is not successful, contact Oracle Support.

After creating your Oracle Content Management instance, you're brought to the **Content Management Instances** page, where you'll see the status of your instance. The instance will take some time to be provisioned, and the page will update automatically to show the current status. The Oracle Content Management instance will be created in the region and compartment you selected, with the tags you entered, and an email will be sent to the notification email address you provided to let you know when the service instance is successfully created. When the instance is successfully created, you can click the instance name to view the details, then click **Open Instance** to open the Oracle Content Management web interface.

If you're an Oracle SaaS customer and you selected the Sales Accelerator license option, the required Sales Accelerator repository, publishing channel, taxonomies, and asset types are created along with your instance.

**Required Compartment and Policies**

During instance creation, there is a compartment and several policies that are automatically created. These are required for your instance to work properly. **Do not delete them.**

- **OCE\_Internal\_Storage\_Policy**—This policy allows Oracle Content Management to access object storage. It's automatically created and added to the root compartment and therefore applies to all compartments in the root compartment, including any new compartment you created for Oracle Content Management.
- **OCMIntegration\_compartment**—This compartment is used for integration with OCI Vision and OCI Speech.
- **speechservice\_auth\_policy**—This policy is used for letting Oracle Content Management make API calls to OCI Speech via service-to-service authentication.
- **aivisionprod\_integration\_policy**—This policy is used for Oracle Content Management integration with OCI Vision and OCI Document Understanding.
- **mediaservices\_integration\_policy**—This policy is used for Oracle Content Management integration with OCI Digital Media Services.
- **speechservice\_integration\_policy**—This policy is used for Oracle Content Management integration with OCI Speech.

#### What to Do Next

After your service instance is successfully created, [set up users and groups using IAM](#), or, if you installed Sales Accelerator, continue with the Sales Accelerator configuration, starting with [customizing content categories](#).

## Set Up Users and Groups Using IAM

After your service instance is successfully created, use IAM to set up your users and groups so they have access to the Oracle Content Management instance that you created earlier.

When your account is created, a default identity domain is created. You can create your users and groups in this domain.

As a best practice, you should create groups based on the roles in your organization, which generally fall into typical organization roles. Then assign the appropriate application roles to those groups to give them access to the Oracle Content Management features they need. Finally, add users to those groups to automatically assign users the appropriate application roles.

#### Note:

If you're using Oracle Content Management Starter Edition, you're limited to only 5 users. To increase the number of users and take advantage of the full feature set, [upgrade to the Premium Edition](#).

If your company uses single sign-on (SSO), you'll want to enable SSO *before* you start adding users.


To set up users and groups:

1. [Create groups for your organization](#)

2. [Assign roles to groups](#)
3. [Add users](#)
4. [Assign users to groups](#)

## Create Groups for Your Organization

To create a group:

1. If you're not already in the Oracle Cloud Console, navigate to it by returning to the window or signing in to [Oracle Cloud](#).
2. In the Oracle Cloud Console, click , click **Identity & Security**, then, under **Identity**, click **Domains**.
3. Open the identity domain you're using for Oracle Content Management.
4. In the navigation menu on the left, click **Groups**.
5. To create a group, click **Create group**.
6. Enter a name and description for the group that makes clear to others what the group is used for.
7. To allow users to request access to this group, click **User can request access**.
8. Click **Create**.


To create another group, click **Groups** in the breadcrumb, then repeat steps 5-8.


## Assign Roles to Groups

After creating groups for your organization roles, assign the appropriate application roles to those groups to give them access to the Oracle Content Management features they need.

Although you can assign roles to users directly, it's easier to manage role assignment when you assign roles to groups and then add users to those groups.

To assign roles to groups:


1. Navigate to your identity domain:
  - If you're viewing the group you just created, click your identity domain in the breadcrumb.
  - If you're not already in the Oracle Cloud Console:
    - a. Sign in to [Oracle Cloud](#) as the cloud account administrator. You can find your account name and login information in your welcome email.
    - b. In the Oracle Cloud Console, click , click **Identity & Security**, then, under **Identity**, click **Domains**.
    - c. Open the identity domain you're using for Oracle Content Management.
2. In the navigation menu on the left, click **Oracle Cloud Services**.
3. On the Oracle Cloud Services page, find the **CECSAUTO\_instanceCECSAUTO** application (where *instance* is the name of the Oracle Content Management instance you created), and open it.
4. On the CECSAUTO\_instanceCECSAUTO application details page, in the navigation menu on the left, click **Application Roles**.

5. Next to the role you want to assign, click , and then select **Assign Groups**.
6. Find and select the group you want, and then click **Assign**.  
For a list of typical organization roles and the application roles they need, see [Typical Organization Roles](#). For a description of the predefined roles in Oracle Content Management, see [Application Roles](#).

## Add Users

Before using your system, you need to add users, either by importing them or creating them individually.

To add users:

1. Navigate to your identity domain:
  - If you're viewing application roles, click your identity domain in the breadcrumb.
  - If you're not already in the Oracle Cloud Console:
    - a. Sign in to [Oracle Cloud](#) as the cloud account administrator. You can find your account name and login information in your welcome email.
    - b. In the Oracle Cloud Console, click , click **Identity & Security**, then, under **Identity**, click **Domains**.
    - c. Open the identity domain you're using for Oracle Content Management.
2. In the navigation menu on the left, click **Users**.
3. Add users using one of the following methods:
  - To import users, you need to create a comma-separated values (CSV) file, and then import the file. See [Importing Users](#).
  - To create a user, click **Create user**. You can assign the user to a group during creation or [assign users to groups](#) at a later time. See "Creating Users" in [Using the Console](#).

### Note:


Make sure to only use printable [ASCII](#) characters (with character codes 32-126) in users' first and last names.

When you add users, they'll receive two emails—one asking them to activate their Oracle Cloud account, and one welcoming them to Oracle Content Management. The Oracle Cloud user account must be activated before the link expires so it can be used. You can send another invitation if necessary. See "Resending Invitations to Users to Activate their Accounts" in [Using the Console](#).

## Assign Users to Groups

Assign users to groups to automatically give them the appropriate roles and permissions for Oracle Content Management.

To assign users to groups:

1. Navigate to the Groups page:
  - If you're viewing users, in the navigation menu on the left, click **Groups**.
  - If you're not already in the Oracle Cloud Console:
    - a. Sign in to [Oracle Cloud](#) as the cloud account administrator. You can find your account name and login information in your welcome email.
    - b. In the Oracle Cloud Console, click , click **Identity & Security**, then, under **Identity**, click **Domains**.
    - c. Open the identity domain you're using for Oracle Content Management.
    - d. In the navigation menu on the left, click **Groups**.
2. Open the group you want to assign users to.
3. Click the **Users** tab.
4. On the Users tab, click **Assign user to groups**.
5. Select the users you want to add, and then click **Add**.

Now that you've deployed your service, created groups, assigned roles, added users, and assigned users to groups, you might want to enable additional features. Then you have a few main tasks to perform in the Oracle Content Management web interface to get Oracle Content Management up and running. See [What to Do Next](#).

## Deploy OCM in a Region without Identity Domains

If your Oracle Cloud Infrastructure (OCI) region hasn't been updated and you don't see **Domains** under **Identity** in the **Identity & Security** section, follow the steps in this section. If you do see **Domains**, follow the steps in [Deploy OCM in a Region with Identity Domains](#).

To deploy OCM in a region with identity domains:

1. [Create and activate an Oracle Cloud account](#).
2. [Create an Oracle Content Management instance](#).
3. [Set up users and groups using IDCS](#).

After you've deployed your instance:

- You might want to enable additional features.
- You have a few main tasks to perform in the Oracle Content Management web interface to get Oracle Content Management up and running. See [What to Do Next](#).

The following video shows the basic process of provisioning a new Oracle Content Management instance on Oracle Cloud Infrastructure (OCI) without identity domains.



## Create and Activate an Oracle Cloud Account

There are several ways to create and activate an Oracle Cloud account.

- **Sign yourself up:** Visit <https://signup.oraclecloud.com/> to [sign yourself up](#) and create an account. You'll get a 30-day trial with \$300 of credit; after which, your Universal Credits subscription will begin. Your account will be activated automatically, and you'll receive a welcome email.

- **Contact Oracle Sales:**
  - If you purchase a Universal Credits subscription through Oracle Sales, you need to [create and activate your cloud account through the activation email](#) you receive. After you activate your account, you'll receive a welcome email.
  - If you are a software as a service (SaaS) customer, you must contact your Oracle Sales representative to order Oracle Content Management for SaaS. After you sign the contract for Oracle Content Management, your service will be activated automatically, and you'll receive a welcome email.



#### Note:

- You can create multiple Oracle Content Management instances within the same subscription.
- If you switched from a non-metered subscription to a Universal Credits subscription, you'll need to replicate your content to your new service instance. For more information on subscriptions, see [Overview of Oracle Cloud Subscriptions](#).

#### What to Do Next

After your account is activated, you need to [create an Oracle Content Management instance](#).

## Create an OCM Instance in a Region without Identity Domains

As the primary account administrator (the person who created the Oracle Cloud subscription), you perform prerequisite steps, and then you or other delegated users can create Oracle Content Management instances from the Oracle Cloud Console.

Creating an Oracle Content Management instance consists of the following steps:


1. [Create a compartment for Oracle Content Management](#).
2. Depending on your specific needs, you may also want to perform some advanced pre-deployment tasks:
  - Delegate creation of Oracle Content Management instances to other users:
    - [Delegate to users who sign in with single sign-on \(SSO\)](#).
    - [Delegate to non-federated users](#).
  - [Create your instance in a secondary domain](#) to accommodate different identity and security requirements (for example, one environment for development and one for production).
  - [Create your instance in another region](#) to use services available in other data centers.
  - [Create a private instance](#) to ensure access is limited to internal networks and that end users have the best and most reliable connection possible.
3. [Create your Oracle Content Management instance](#) in the compartment you created.

## Create a Compartment for Oracle Content Management

Compartments are used to organize cloud resources for the purposes of isolation (separating one project or business unit from another), access (through the use of policies), and measuring usage and billing. A common approach is to create a compartment for each major part of your organization (for example, Sales, Human Resources, and so on).

When you create an Oracle Content Management instance, you'll be asked to select a compartment. For security reasons, Oracle strongly recommends creating and using a new storage compartment rather than using the existing root storage compartment.

To create a new compartment for Oracle Content Management:

1. Sign in to [Oracle Cloud](#) as the cloud account administrator. You can find your account name and login information in your welcome email.
2. In the Oracle Cloud Console, click  on the top left to open the navigation menu, click **Identity & Security**, then, under **Identity**, click **Compartments**.
3. On the Compartments page, click **Create Compartment**.
4. Enter a name and description for the compartment. Make clear in your name and description the purpose of the compartment, whether it's specifically for Oracle Content Management, for a project, for a department, or some other purpose.
5. Click **Create Compartment**.  
The newly created compartment may not be available to you immediately. If you don't see it included in selection lists, try again a little later.

You don't need to create a new compartment for every instance. You can use the same compartment for multiple instances.

### What to Do Next



After creating your compartment, perform any necessary advanced pre-deployment tasks or skip right to creating your instance:

- Delegate creation of Oracle Content Management instances to other users:
  - [Delegate to users who sign in with single sign-on \(SSO\)](#).
  - [Delegate to non-federated users](#).
- [Create your instance in a secondary domain](#) to accommodate different identity and security requirements (for example, one environment for development and one for production).
- [Create your instance in another region](#) to use services available in other data centers.
- [Create a private instance](#) to ensure access is limited to internal networks and that end users have the best and most reliable connection possible.
- [Create your Oracle Content Management instance](#) in the compartment you created.

## Delegate Creation of OCM Instances to SSO Users

To delegate creation of Oracle Content Management instances to users who sign in with single sign-on (SSO), the primary account administrator must add the users to the **OCI Administrators** group. The OCI Administrators group is created automatically when you have an Oracle Cloud account running on Oracle Cloud Infrastructure (OCI).



1. If you're not already in the Oracle Cloud Console, sign in to [Oracle Cloud](#) as the primary account administrator.
2. In the Oracle Cloud Console, click  on the top left to open the navigation menu, click **Identity & Security**, then, under **Identity**, click **Federation**.
3. On the Federation page, click **OracleIdentityCloudService**, then, on the identity provider details page, click the link to the **Oracle Identity Cloud Service Console**. The IDCS Console opens in a new window.
4. In the IDCS Console, click , and then click **Groups**.
5. Click **OCI Administrators**.
6. Click the **Users** tab.
7. Click **Assign**.
8. Select the users you want to delegate to, and then click **OK**.

Users you added to the OCI Administrators group can now sign in to Oracle Cloud and create Oracle Content Management instances.

### What to Do Next

After delegating users, perform any other necessary advanced pre-deployment tasks or skip right to creating your instance:

- [Create your instance in a secondary domain](#) to accommodate different identity and security requirements (for example, one environment for development and one for production).
- [Create your instance in another region](#) to use services available in other data centers.
- [Create a private instance](#) to ensure access is limited to internal networks and that end users have the best and most reliable connection possible.
- [Create your Oracle Content Management instance](#).


## Delegate Creation of OCM Instances to Non-Federated Users




To delegate creation of Oracle Content Management instances to non-federated users (users that don't sign in through SSO), the primary account administrator must create a group, add users to the group, create required policies, give the users the application administrator role, and create a confidential application. The users can then generate an access token and create an instance.

### Note:

Even if you are creating an instance in a secondary Oracle Identity Cloud Service (IDCS) domain, you perform the steps described in this topic in the *primary* IDCS domain.

1. Create a group of users you want to delegate to.
  - a. Navigate to the Groups page:

- If you're already in the **Identity & Security** area of the Oracle Cloud Console, in the navigation menu on the left, click **Groups**.
- If you're not already in the Oracle Cloud Console:
  - i. Sign in to [Oracle Cloud](#) as the cloud account administrator. You can find your account name and login information in your welcome email.
  - ii. In the Oracle Cloud Console, click , click **Identity & Security**, then, under **Identity**, click **Groups**.
- b. Click **Create Group**.
- c. Enter a name and description, then click **Create**.
- 2. Add the users you want to delegate to.
  - a. Open the group you created.
  - b. Click **Add User to Group**.
  - c. Start typing the name of the user, then select the user, and click **Add**.
- 3. Create a policy to allow the group to manage Oracle Content Management instances.
  - a. In the navigation menu on the left, click **Policies**.
  - b. Select a compartment. You can apply the policy to all compartments by selecting the root compartment, or you can select a specific compartment.
  - c. Click **Create Policy**.
  - d. Enter a name and description.
  - e. In the Statement box, enter one of the following, replacing *YourGroupName* with the name of the group you created, and, if necessary, replacing *compartment\_id* with the ID of the specific compartment you selected:
    - If you selected the root compartment: `allow group YourGroupName to manage oce-instance-family in tenancy`
    - If you selected a specific compartment: `allow group YourGroupName to manage oce-instance-family in compartment_id`
  - f. Click **Create**.
- 4. If your delegated users aren't administrators, you must also create the `OCE_Internal_Storage_Policy`, which allows Oracle Content Management to access object storage. Normally this policy is created automatically as part of instance creation, but non-administrators aren't allowed to create policies, so this background process will fail, leaving Oracle Content Management without access to object storage unless you create the policy manually.
  - a. On the Policies page, make sure the appropriate compartment is selected. You can apply the policy to all compartments by selecting the root compartment, or you can select a specific compartment.
  - b. Click **Create Policy**.
  - c. Enter `OCE_Internal_Storage_Policy` as the name, and enter a description.
  - d. In the Statement box, enter one of the following, if necessary, replacing *compartment\_id* with the ID of the specific compartment you selected:
    - If you selected the root compartment: `Allow service CEC to manage object-family in tenancy`

- If you selected a specific compartment: Allow service CEC to manage object-family in compartment `compartment_id`
- e. Click **Create**.
5. Give yourself and the delegated users the application administrator role in IDCS so you can all generate your own access tokens.
    - a. Depending on your subscription, you access the IDCS Console in one of the following ways:
      - Through the Federation option in the Oracle Cloud Console:
        - i. In the navigation menu on the left, click **Federation**.
        - ii. On the Federation page, click **OracleIdentityCloudService**, then, on the identity provider details page, click the link to the **Oracle Identity Cloud Service Console**. The IDCS Console opens in a new window.
      - If you don't see the Federation option, use the Oracle Cloud Classic Console, accessed through your welcome email:
        - i. In your "Welcome to Oracle Cloud" email, click the **Get Started** link, then enter your user name and password.
        - ii. In the Oracle Cloud Classic Console, click  on the top left to open the navigation menu, click **Users**, then click **Identity**. The IDCS Console opens in a new window.
    - b. Click , click **Security**, then click **Administrators**.
    - c. Expand the **Application Administrator** section.
    - d. Click **Add**.
    - e. Select yourself and the delegated users, and then click **OK**. These are IDCS users, which aren't the same as Oracle Cloud users, so if you don't see the delegated users you want, create them in IDCS. Stay in the IDCS console to complete the next step.
  6. Create a confidential application.
    - a. In the IDCS Console, click , and then click **Applications**. If you don't see the Applications option, you don't have the Application Administrator role.
    - b. Click **Add**, then select **Confidential Application**.
    - c. On the Details page, enter `OCE Trusted App` as the name, and then click **Next**.
    - d. On the Client page:
      - i. Select **Configure this application as a client now**.
      - ii. For Allowed Grant Types, select **Resource Owner**, **Client Credentials**, and **JWT Assertion**.
      - iii. Under Grant the client access to Identity Cloud Service Admin APIs, click **Add**, select **Application Administrator**, then click **Add**.
      - iv. Click **Next**.
    - e. On the Resources page, select **Skip for later**, and then click **Next**.
    - f. On the Web Tier Policy page, select **Skip for later**, and then click **Next**.

- g. On the Authorization page, click **Finish**.
- h. After the app is created, click **Activate**.  
Stay on this page to complete the next step.

When someone (you or a delegated user) is ready to create an Oracle Content Management instance, they need to generate an IDCS access token and enter the access token when they create the instance.

**Note:**

The token expires after one hour, so you may need to regenerate the token, for example, if you later want to create another instance.

To generate an access token:

1. If you're not already viewing the confidential application you created, in the IDCS Console, open it.
2. On the App Details page, click **Generate Access Token**, select **Customized Scopes**, choose **Application Administrator**, then click **Download Token**.

**What to Do Next**

After delegating users, perform any other necessary advanced pre-deployment tasks or skip right to creating your instance:

- [Create your instance in a secondary domain](#) to accommodate different identity and security requirements (for example, one environment for development and one for production).
- [Create your instance in another region](#) to use services available in other data centers.
- [Create a private instance](#) to ensure access is limited to internal networks and that end users have the best and most reliable connection possible.
- [Create your Oracle Content Management instance](#).

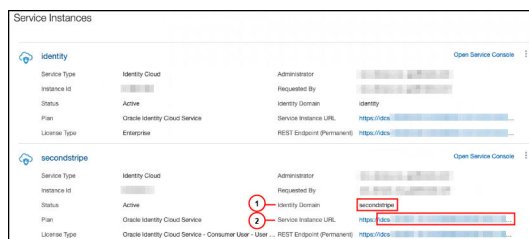
## Create Your Instance in a Secondary IDCS Domain

If you want to create multiple Oracle Content Management instances in separate environments, you need to create a secondary IDCS domain before you create those additional Oracle Content Management instances.

You might want to create multiple Oracle Content Management instances in separate environments to accommodate different identity and security requirements (for example, one environment for development and one for production). You can accomplish this by creating multiple instances of IDCS. By having separate IDCS environments, the users who work in one environment won't impact the work of users in another environment. Using multiple instances can also help you maintain the isolation of administrative control over each environment. This is necessary if, for example, your security standards prevent development user IDs from existing in the production environment, or require that different administrators have control over different environments. When multiple instances are utilized, you'll have a *primary* instance, the instance which comes with your Oracle Cloud account, and one or more *secondary* (additional) instances.

To create an Oracle Content Management instance in a secondary IDCS domain, perform these preliminary steps before you create the Oracle Content Management instance:

1. Create a secondary Oracle Identity Cloud Service (IDCS) domain.
2. Note the identity domain name and the service instance URL of the secondary IDCS instance. You'll use these values when you create your Oracle Content Management instance.
  - a. If you're not already in the Oracle Cloud Classic Console, sign in. If you are using the Oracle Cloud Console, complete the following steps to access the Oracle Cloud Classic Console.
    - i. Open the user menu in the top right in the Oracle Cloud Console. and note the name of the **Tenancy**.
    - ii. Use the following syntax to construct the URL to access the Oracle Cloud Classic Console.  
`https://myservices-mytenancyname.console.oraclecloud.com/mycloud/cloudportal/dashboard`  
 Where, *mytenancyname* is the name that you have noted in the previous step.
  - b. On the dashboard, open the **Identity Cloud** service.
  - c. On the Service Instances page, note the **Identity Domain** (1) and the domain ID (in the format `idcs-xxxxxxxxxxxxx`, after "https://" and before the first ".") in the **Service Instance URL** (2).



**! Important:**

To create your instance in the secondary IDCS domain, you must sign into the *primary* OCI console as the *primary* IDCS administrator. Then, during instance creation, use the advanced options to enter the secondary IDCS domain name and ID.

**What to Do Next**

After creating your new domain, perform any other necessary advanced pre-deployment tasks or skip right to creating your instance:

- [Create your instance in another region](#) to use services available in other data centers.
- [Create a private instance](#) to ensure access is limited to internal networks and that end users have the best and most reliable connection possible.
- [Create your Oracle Content Management instance](#), making sure to enter the secondary IDCS domain name and ID.

## Create an Instance in Another Region

If you want to create an Oracle Content Management instance in a region other than your primary region, there are some preliminary steps you need to perform before you create the instance.

Oracle Infrastructure and Platform Cloud Services (Oracle IaaS/PaaS) are enabled in different data centers. These data centers are grouped into data regions based on their geographic locations. When you purchase these services or sign up for a free promotion, you typically choose the data region closest to your location to access them. This becomes your *primary data region*. However, if required, you can extend your subscription to other geographical regions (within the same cloud account) and use the services there. For example, if you selected North America as your primary data region during your purchase, you can extend your subscription to the EMEA (Europe, Middle East, and Africa) data region. By doing so, you'll enable your users to use services available in the EMEA data centers.

To create an instance in another region, perform these preliminary steps:

1. [Extend your subscription to another region.](#)
2. [Federate Oracle Identity Cloud Service \(IDCS\) from the new region with Oracle Cloud Infrastructure \(OCI\).](#)

### What to Do Next

After extending your subscription and federating the new region, perform any other necessary advanced pre-deployment tasks or skip right to creating your instance:

- [Create your instance in a secondary domain](#) to accommodate different identity and security requirements (for example, one environment for development and one for production).
- [Create a private instance](#) to ensure access is limited to internal networks and that end users have the best and most reliable connection possible.
- [Create your Oracle Content Management instance](#) in the compartment you created.

## Create a Private Instance Using FastConnect

You may need additional performance or security that may not be available over the public internet. Oracle Cloud Infrastructure FastConnect can be used to provide a more performant, robust, and secure connection to your Oracle Content Management instance. This type of connection is often used by customers who want to ensure access is limited to internal networks or that end users have the best and most reliable connection possible.



### Note:

If you're using Oracle Content Management Starter Edition, FastConnect isn't supported. To take advantage of the full feature set, upgrade to the [Premium Edition](#).


If you want to create such an instance, you need to set up Oracle Cloud Infrastructure FastConnect and perform some additional prerequisite steps. FastConnect provides a dedicated private connection with higher bandwidth and a more reliable and consistent networking experience when compared to internet-based connections.

Before you can create a private instance, you need to perform the following prerequisite steps:

1. [Set up FastConnect on the tenancy.](#)
2. [Get your tenancy OCID and name.](#)
3. [Create a local peering gateway.](#)
4. [Create a requestor group.](#)
5. [Create a requestor policy.](#)
6. [Create a support request.](#)

## Get Your Tenancy OCID



To get your tenancy's OCID, perform the following steps:

1. If you're not already in the Oracle Cloud Console, sign in to [Oracle Cloud](#) as the primary account administrator.
2. In the Oracle Cloud Console, click , click **Governance & Administration**, then, under **Account Management**, click **Tenancy Details**.
3. Next to the **OCID**, click **Copy**. Save this tenancy OCID to include with your support request later.

## Create a Local Peering Gateway


For information on peering, see [Local VCN Peering \(Within Region\)](#).

To create a local peering gateway, perform the following steps:

1. In the Oracle Cloud Console, click , click **Networking**, then click **Virtual Cloud Networks**.
2. Open the VCN you created when you set up FastConnect on the tenancy.
3. Click **Local Peering Gateways**.
4. Click **Create Local Peering Gateway**.
5. Enter a name for the gateway (for example, `customer-to-ocelpg`).
6. Select the compartment in which you want to store the peering.
7. Click **Create Local Peering Gateway**.
8. In the list of Local Peering Gateways, click , and then click **Copy OCID**. Save this local peering gateway OCID to include with your support request later.

## Create a Requestor Group


To create a requestor group and add the Oracle Cloud Infrastructure tenancy administrator, perform the following steps:

1. In the Oracle Cloud Console, click  on the top left to open the navigation menu, click **Identity & Security**, then, under **Identity**, click **Groups**.

2. Click **Create Group**.
3. Enter a name for the requestor group (for example, `RequestorGrp`).
4. Click **Create**.
5. Click the group name to open the group details.
6. Click **Add User to Group**.
7. In the Users drop-down list, select a user with Oracle Cloud Infrastructure tenancy administrator privileges, and then click **Add**.
8. On the group details page, copy the **OCID**. Save this requestor group OCID to include with your support request later.

## Create a Requestor Policy

To create a requestor policy, perform the following steps:

1. In the Oracle Cloud Console, click  on the top left to open the navigation menu, click **Identity & Security**, then, under **Identity**, click **Policies**.
2. If necessary, select a different compartment for the policy.
3. Click **Create Policy**.
4. Enter the following details:
  - **Policy:** `RequestorPolicy`
  - **Description:** `Requestor policy for peering`
  - **Statement:**  
 Define tenancy Acceptor as `OCETenancyOCID` Allow group `RequestorGroup` to manage `local-peering-from` in compartment `GroupCompartmentName` Endorse group `RequestorGroup` to manage `local-peering-to` in tenancy Acceptor Endorse group `RequestorGroup` to associate `local-peering-gateways` in compartment `PeeringCompartmentName` with `local-peering-gateways` in tenancy Acceptor

Replace the following values:

- `OCETenancyOCID`: Replace with the realm-specific tenancy OCID from the following table.

| Realm | Tenancy OCID   |
|-------|--|
| oc1   | ocid1.tenancy.oc1..aaaaaaa4yafecztqbebz<br>nfxpjzwm52wuaeornzgzqrujpbkmeez6zuigv<br>7a |
| oc4   | ocid1.tenancy.oc4..aaaaaaaamxjaupllkzz2a<br>2qmvcon7rprzlu4hmyfajsfk3ezzmdstterlbya    |
| oc8   | ocid1.tenancy.oc8..aaaaaaaanpm5o3ejwjerj<br>yiwsh4u5rd6mpme5ftq44ue5pkxnnhvf3sw<br>v2q |

- `RequestorGroup`: Replace with the name of the requestor group you created.
- `GroupCompartmentName`: Replace with the name of the compartment in which you created the requestor group.



- *PeeringCompartmentName*: Replace with the name of the compartment in which you created the peering.

For more information, see [Set up the IAM policies \(VCNs in different tenancies\)](#).

5. Click **Create**.

## Create a Support Request

Create a request with Oracle Support stating you want to create a private service instance. Make sure to include the following information that you collected earlier in your request:

- Tenancy OCID
- Local peering gateway OCID
- Requestor group OCID

Oracle Support will reply with a validation URL for you to test.

### What to Do Next


After you've tested the URL, perform any other necessary advanced pre-deployment tasks or skip right to creating your instance:

- [Create your instance in a secondary domain](#) to accommodate different identity and security requirements (for example, one environment for development and one for production).
- [Create your instance in another region](#) to use services available in other data centers.
- [Create your Oracle Content Management instance](#) in the compartment you created.

## Create Your Oracle Content Management Instance



To create an Oracle Content Management instance you must be the primary account administrator or the account administrator must have set up your user account with the proper permissions.

To create your Oracle Content Management instance:

1. If you're not already in the Oracle Cloud Console, navigate to it by returning to the window or signing in to [Oracle Cloud](#).
2. Click , click **Developer Services**, then, under **Content Management**, click **Instances**. This opens the Content Management Instances page.
3. In the Compartment menu on the left, select the compartment you want to use for Oracle Content Management. You can use the root compartment or another [compartment you created](#) for Oracle Content Management. The compartment you created may not be available to you immediately. If you don't see it, try again a little later.
4. Make sure that the region that's selected in the menu in the top right of the Oracle Cloud Console is the one in which you want to create your instance. If you're selecting a region other than your primary data region or home region, you must have performed the [prerequisite steps](#).

5. Click **Create Instance**.
6. Enter the following information:

| Field  | Description  |
|--|--|
| <b>Instance Name</b>                                 | Specify a unique name for your service instance. If you intend to create multiple instances, make sure your instance name makes clear what the instance will be used for. If you specify a name that already exists, the system displays an error and the instance is not created.   |
| <b>Description</b>                                   | Optionally, enter a description of the instance.   |
| <b>Compartment</b>                                   | This is the compartment you previously selected. If you need to, you can change it.  |
| <b>Notification Email</b>                            | Make sure this is the email address to which you want provisioning status updates to be sent.  |
| <b>License Type</b>                                  | <p>Choose the type of license you want to use for this instance:</p> <ul style="list-style-type: none"> <li>• <b>Premium Edition:</b> Subscribe to a new full-featured Oracle Content Management license.</li> <li>• <b>BYOL License:</b> Use your existing Oracle WebCenter Middleware license (BYOL).</li> <li>• <b>Starter Edition:</b> Subscribe to a feature-limited edition of Oracle Content Management.</li> </ul> <p>The BYOL license type bills for assets at a discounted rate compared to a new Oracle Content Management license. To qualify for an Oracle Content Management BYOL license type your company must already own a qualifying on-premise WebCenter product license that is current on support maintenance. For more information please refer to the <a href="#">Oracle PaaS and IaaS Universal Credits Service Descriptions</a> for a description of which WebCenter products qualify for BYOL licensing and for the conversion ratios for WebCenter processor licenses.</p> |
| <b>Access Token</b> (only appears for non-SSO users) | <p>If you're not the primary account administrator and you signed in with an Oracle Cloud Infrastructure (OCI) user account, not using single sign-on (SSO), enter the IDCS access token you were given. Access tokens expire after one hour.</p> <p><b>Note:</b> If you're creating this Oracle Content Management instance in a secondary Oracle Identity Cloud Service (IDCS) domain, this access token should still be for the <i>primary</i> IDCS domain.</p>   |

| Field                  | Description   |
|------------------------|---|
| <b>License Options</b> | <p data-bbox="943 222 1453 369">Optionally, enable additional license options. Enabling any of these options will add additional billing charges to your instance. Refer to your prepaid subscription contract or your Universal Credit contract for additional costs.</p> <ul data-bbox="943 375 1453 1276" style="list-style-type: none"> <li data-bbox="943 375 1453 632">• <b>Advanced Hosting</b> (not available for Starter Edition)—Advanced hosting configures an instance to use a dedicated Autonomous Transactional Database. Enabling this feature also allows the instance to support additional instance options such as disaster recovery (described below). To enable advanced hosting, select <b>Advanced Hosting</b>.</li> </ul> <div data-bbox="997 667 1453 842" style="border: 1px solid #0070C0; padding: 5px; margin: 10px 0;"> <p data-bbox="1029 709 1154 741"> <b>Note:</b></p> <p data-bbox="1078 768 1430 821">You can't disable this option after the instance has been created.</p> </div> <ul data-bbox="943 848 1453 1276" style="list-style-type: none"> <li data-bbox="943 848 1453 1104">• <b>Sales Accelerator</b>—Oracle Sales Accelerator provides a one-stop shop for sales enablement content. It allows you to readily access a wide variety of information and resources that make selling your products and services easier. If you <a href="#">purchased an Oracle Sales Accelerator subscription</a>, select <b>Sales Accelerator</b>.</li> <li data-bbox="943 1110 1453 1276">• <b>Sauce Video</b>—<a href="#">Sauce Video</a> is the video creation platform for teams. It provides a fast, easy, and affordable way to create video together anywhere, anytime. To enable Sauce Video for your instance, select <b>Video Creation Platform</b>.</li> </ul> <div data-bbox="997 1318 1453 1671" style="border: 1px solid #0070C0; padding: 5px; margin: 10px 0;"> <p data-bbox="1029 1360 1154 1392"> <b>Note:</b></p> <ul data-bbox="1078 1419 1398 1646" style="list-style-type: none"> <li data-bbox="1078 1419 1398 1556">– If you're an Oracle SaaS customer, you must have purchased a Sauce Video subscription to see this option.</li> <li data-bbox="1078 1562 1398 1646">– All Sauce Video Creation Platform data is stored in London, UK.</li> </ul> </div> |

7. If you need to enter additional details (for example, if you're creating your instance in a secondary domain or you're creating a non-primary instance), click **Show Advanced Options**, and enter the following information:

| Field  | Description   |
|--|---|
| <b>Instance Type</b> (not supported in Starter Edition)        | <p>By default, the instance type is primary (for example, your production instance). You must have at least one primary instance. If this instance is a non-primary instance (for example, for development or testing), select <b>Non-Primary</b> in the drop-down list. Primary and non-primary instances are <a href="#">billed at different rates</a>.</p> <p>If this is a non-primary instance, you might want to include a tag to specify what the instance is used for.</p>   |
| <b>Upgrade Schedule</b> (not supported in Starter Edition)     | <p>Control whether your instance is upgraded immediately (as soon as a new release of Oracle Content Management is available) or on a delayed schedule (one release behind the latest release). For example, let's assume you have stage (non-primary) and production (primary) instances. You would set your stage instance to upgrade immediately and your production instance as delayed upgrade. This allows you to test the upgrade on the stage instance, making sure it doesn't interfere with any sites you've deployed. If you find any issues, you can report them to Oracle Support so they can be fixed before the upgrade is applied to your production instance.</p> <p>If you want to use this feature, but you don't see it, contact Oracle Support.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"><li>• <b>Upgrade immediately:</b> Upgrade this instance as soon as a new release of Oracle Content Management is available.</li><li>• <b>Delay upgrade:</b> Delay the upgrade of this instance, so that it is one release behind the latest release of Oracle Content Management.</li></ul> <p>Once you create this instance, you can't change this setting.</p> |
| <b>Instance Access Type</b> (not supported in Starter Edition) | <p>Control whether your instance is accessible by public internet or through a dedicated private connection using Oracle Cloud Infrastructure FastConnect.</p> <p>If you want to use this feature, but you don't see it, contact Oracle Support.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"><li>• <b>Public:</b> Select this option if you want your instance to be viewed over <i>public internet</i>.</li><li>• <b>Private:</b> If you want to create a private instance that can be viewed only within your <i>intranet</i>, and you completed the <a href="#">prerequisite steps</a> to set up Oracle Cloud Infrastructure FastConnect, select this option.</li></ul> <p>Once you create this instance, you can't change this setting.</p>   |

| Field  | Description  |
|--|--|
| <b>Disaster Recovery</b> (not available for Starter Edition) | You must enable Advanced Hosting before you can select this option. <a href="#">Disaster recovery</a> provides a full-stack orchestration of the service that includes comprehensive disaster recovery failover capabilities for all layers of the Oracle Content Management application stack, including the Oracle Content Management application tiers, database, search index, and object storage. |
| <b>IDCS Domain Name</b> (not supported in Starter Edition)   | If you're creating this Oracle Content Management instance in a secondary Oracle Identity Cloud Service (IDCS) domain, enter the identity domain value you noted in the <a href="#">prerequisite steps</a> .   |
| <b>IDCS Domain ID</b> (not supported in Starter Edition)     | Enter the domain ID value of the secondary IDCS domain that you got from the service instance URL and noted in the prerequisite steps. Don't include "https://".   |
| <b>Tags</b>  | Optionally, add tags to categorize this instance with metadata. You can then filter your list of instances by tag.   |

8. Click **Create Instance**.



**Note:**

If the creation of your service instance is not successful, contact Oracle Support.

After creating your Oracle Content Management instance, you're brought to the Content Management Instances page, where you'll see the status of your instance. The instance will take some time to be provisioned, and the page will update automatically to show the current status. The Oracle Content Management instance will be created in the region and compartment you selected, with the tags you entered, and an email will be sent to the notification email address you provided to let you know when the service instance is successfully created. When the instance is successfully created, you can click the instance name to view the details, then click **Open Instance** to open the Oracle Content Management web interface.

If you're an Oracle SaaS customer and you selected the Sales Accelerator license option, the required Sales Accelerator repository, publishing channel, taxonomies, and asset types are created along with your instance.

**Required Compartment and Policies**

During instance creation, there is a compartment and several policies that are automatically created. These are required for your instance to work properly. **Do not delete them.**

- **OCE\_Internal\_Storage\_Policy**—This policy allows Oracle Content Management to access object storage. It's automatically created and added to the root compartment and therefore applies to all compartments in the root compartment, including any new compartment you created for Oracle Content Management.

- **OCMIntegration compartment**—This compartment is used for integration with OCI Vision and OCI Speech.
- **speechservice\_auth\_policy**—This policy is used for letting Oracle Content Management make API calls to OCI Speech via service-to-service authentication.
- **avisionprod\_integration\_policy**—This policy is used for Oracle Content Management integration with OCI Vision and OCI Document Understanding.
- **mediaservices\_integration\_policy**—This policy is used for Oracle Content Management integration with OCI Digital Media Services.
- **speechservice\_integration\_policy**—This policy is used for Oracle Content Management integration with OCI Speech.

### What to Do Next

After your service instance is successfully created, [set up users and groups using IDCS](#), or, if you installed Sales Accelerator, continue with the Sales Accelerator configuration, starting with [customizing content categories](#).

## Set Up Users and Groups Using IDCS

After your service instance is successfully created, use IDCS to set up your users and groups so they have access to the Oracle Content Management instance that you created earlier.

As a best practice, you should create groups based on the roles in your organization, which generally fall into typical organization roles. Then assign the appropriate application roles to those groups to give them access to the Oracle Content Management features they need. Finally, add users to those groups to automatically assign users the appropriate application roles.

### Note:

If you're using Oracle Content Management Starter Edition, you're limited to only 5 users. To increase the number of users and take advantage of the full feature set, [upgrade to the Premium Edition](#).

If your company uses single sign-on (SSO), you'll want to enable SSO *before* you start adding users.



To set up users and groups:

1. [Create groups for your organization](#).
2. [Assign roles to groups](#).
3. [Add users](#).
4. [Assign users to groups](#).

## Create Groups for Your Organization

To create groups:

1. If you're not already in the Oracle Cloud Console, sign in to [Oracle Cloud](#) as the primary account administrator.




2. In the Oracle Cloud Console, click  on the top left to open the navigation menu, click **Identity & Security**, then, under **Identity**, click **Federation**.
3. On the Federation page, click **OracleIdentityCloudService**, then, on the identity provider details page, click the link to the **Oracle Identity Cloud Service Console**. The IDCS Console opens in a new window.
4. In the IDCS Console, click , and then click **Groups**.
5. To create a group, click **Add**.
6. Enter a name and description for the group that makes clear to others what the group is used for.
7. To allow users to request access to this group, click **User can request access**.
8. Click **Finish**.

## Assign Roles to Groups

After creating groups for your organization roles, assign the appropriate application roles to those groups to give them access to the Oracle Content Management features they need.

Although you can assign roles to users directly, it's easier to manage role assignment when you assign roles to groups and then add users to those groups.

To assign roles to groups:



1. If you're not already in the Oracle Identity Cloud Service Console:
  - a. Sign in to [Oracle Cloud](#) as the cloud account administrator. You can find your account name and login information in your welcome email.
  - b. In the Oracle Cloud Console, click  on the top left to open the navigation menu, click **Identity & Security**, then, under **Identity**, click **Federation**.
  - c. On the Federation page, click **OracleIdentityCloudService**, then, on the identity provider details page, click the link to the **Oracle Identity Cloud Service Console**. The IDCS Console opens in a new window.
2. In the IDCS Console, click , and then click **Oracle Cloud Services**.
3. On the Oracle Cloud Services page, find the **CECSAUTO\_instanceCECSAUTO** application (where *instance* is the name of the Oracle Content Management instance you created), and open it.
4. On the CECSAUTO\_instanceCECSAUTO application details page, click **Application Roles**.
5. Next to the role you want to assign, click , and then select **Assign Groups**.
6. Find and select the group you want, and then click **OK**.  
For a list of typical organization roles and the application roles they need, see [Typical Organization Roles](#). For a description of the predefined roles in Oracle Content Management, see [Application Roles](#).

## Add Users

Before using your system, you need to add users, either by importing them or creating them individually.

If your company uses single sign-on (SSO), you'll want to enable SSO *before* you start adding users.

To add users:

1. If you're not already in the Oracle Identity Cloud Service Console:
  - a. Sign in to [Oracle Cloud](#) as the cloud account administrator. You can find your account name and login information in your welcome email.
  - b. In the Oracle Cloud Console, click  on the top left to open the navigation menu, click **Identity & Security**, then, under **Identity**, click **Federation**.
  - c. On the Federation page, click **OracleIdentityCloudService**, then, on the identity provider details page, click the link to the **Oracle Identity Cloud Service Console**. The IDCS Console opens in a new window.
2. In the IDCS Console, click , and then click **Users**.
3. Add users using one of the following methods:
  - To import users, you need to create a comma-separated values (CSV) file, and then click **Import**. See [Importing User Accounts in Administering Oracle Identity Cloud Service](#).
  - To create a user, click **Add**. You can assign the user to a group during creation or [assign users to groups](#) at a later time. See [Creating User Accounts in Administering Oracle Identity Cloud Service](#).

 **Note:**

Make sure to only use printable [ASCII](#) characters (with character codes 32-126) in users' first and last names.

When you add users, they'll receive two emails—one asking them to activate their Oracle Cloud account, and one welcoming them to Oracle Content Management. The Oracle Cloud user account must be activated before the link expires so it can be used. You can send another invitation if necessary.



## Assign Users to Groups

Assign users to groups to automatically give them the appropriate roles and permissions for Oracle Content Management.

To assign users to groups:

1. If you're not already in the Oracle Identity Cloud Service Console:
  - a. Sign in to [Oracle Cloud](#) as the cloud account administrator. You can find your account name and login information in your welcome email.



- b. In the Oracle Cloud Console, click  on the top left to open the navigation menu, click **Identity & Security**, then, under **Identity**, click **Federation**.
  - c. On the Federation page, click **OracleIdentityCloudService**, then, on the identity provider details page, click the link to the **Oracle Identity Cloud Service Console**. The IDCS Console opens in a new window.
2. In the IDCS Console, click , and then click **Groups**.
3. Open the group you want to assign users to.
4. Click the **Users** tab.
5. Click **Assign**.
6. Select the users you want to add, and then click **OK**.

Now that you've deployed your service, created groups, assigned roles, added users, and assigned users to groups, you might want to enable additional features. Then you have a few main tasks to perform in the Oracle Content Management web interface to get Oracle Content Management up and running. See [What to Do Next](#).

# 3

## What to Do Next

After deploying your service and setting up users and groups, you need to complete some additional tasks in the Oracle Content Management web interface to get Oracle Content Management up and running.

Perform the followings tasks, as necessary, as described in *Administering Oracle Content Management*:

- Set service defaults such as user quotas, link behavior, file type and size restrictions, and virus scan options.  
Another important default to set is the default role given to new folder members.
- You might want to perform some of the following tasks to get the most out of Oracle Content Management:
  - Apply branding and URLs to customize Oracle Content Management with your logo and other branding, and change the links that are available in the user menu to download apps, access help, and send feedback..
  - Enable email notifications to alert users when certain events occur, like when someone flags you, or when someone creates a public link for a file or folder.
  - Set the default time zone and language for the Oracle Content Management user interface.
  - Configure custom properties (metadata) so that users can quickly categorize files and folders with additional information.
- Provide sign-in and get-started information to users to introduce your users to Oracle Content Management and let them know who to contact if they have questions.
- Optionally, push the desktop app out to your users.

The desktop app keeps files and folders on your users' computers synchronized with the cloud. They can choose the folders in Oracle Content Management that they want to sync, including folders that are shared with them, so they always have access to the current versions of their content folders and assets. They can also add files and folders into their desktop folder, and they'll automatically be added to Oracle Content Management.

The desktop app also enables users to set notifications, letting them know when there's activity in conversations they participate in, and they can share files and folders, just like they do in the web interface.

To take your user experience even further, integrate Oracle Content Management with your other business applications, such as Oracle Process Cloud Service or custom applications.

# 4

## Manage the Service

Throughout the use of your service, you can manage and monitor your service in the following ways.


- [Manage vanity domains.](#)
- [Edit an instance.](#)
- [View your billing and usage metrics.](#)
- If you added web analytics tracking code to sites and pages, you can view analytics on the vendor's site (Google, Adobe, or Oracle Infinity).
- View service usage statistics.

If you run into problems, you can [report issues](#) to Oracle Customer Support.


## Edit Your Oracle Content Management Instance

As you use your Oracle Content Management instance you may need to change particular options.

To edit your Oracle Content Management instance:

1. Sign in to [Oracle Cloud](#) as the cloud account administrator. You can find your account name and login information in your welcome email.
2. In the Oracle Cloud Console, click  in the top left to open the navigation menu, click **Developer Services**, then click **Instances** under Content Management.
3. In the **Compartment** menu on the left, make sure you've selected the compartment you're using for Oracle Content Management.
4. Click the name of the instance you want to edit.
5. Click **Edit Instance**.
6. You can edit the following options:

| Field        | Description   |
|--------------|---|
| License Type | <p>If you need to change the type of license you use for this instance, select one of the following options:</p> <ul style="list-style-type: none"><li data-bbox="906 317 1377 401">• <b>Premium Edition:</b> Subscribe to a new full-featured Oracle Content Management license.</li><li data-bbox="906 411 1377 495">• <b>BYOL License*:</b> Use your existing Oracle WebCenter Middleware license (BYOL).</li><li data-bbox="906 506 1377 642">• <b>Starter Edition:</b> Subscribe to a feature-limited edition of Oracle Content Management. If you're already using another license type, you can't switch to Starter Edition.</li></ul> <p>* The BYOL license type bills for assets at a discounted rate compared to a new Oracle Content Management license. To qualify for an Oracle Content Management BYOL license type your company must already own a qualifying on-premise WebCenter product license that is current on support maintenance. For more information please refer to the <a href="#">Oracle PaaS and IaaS Universal Credits Service Descriptions</a> for a description of which WebCenter products qualify for BYOL licensing and for the conversion ratios for WebCenter processor licenses.</p> |

| Field  | Description  |
|--|--|
| <p><b>License Options</b></p>                                  | <p>Optionally, enable or disable additional license options. Enabling any of these options will add additional billing charges to your instance. Refer to your prepaid subscription contract or your Universal Credit contract for additional costs.</p> <ul style="list-style-type: none"> <li> <p><b>Sales Accelerator</b>—Oracle Sales Accelerator provides a one-stop shop for sales enablement content. It allows you to readily access a wide variety of information and resources that make selling your products and services easier.</p> <p>If you <a href="#">purchased an Oracle Sales Accelerator subscription</a>, select <b>Sales Accelerator</b>.</p> </li> <li> <p><b>Sauce Video</b>—<a href="#">Sauce Video</a> is the video creation platform for teams. It provides a fast, easy, and affordable way to create video together anywhere, anytime.</p> <p>To enable Sauce Video for your instance, select <b>Video Creation Platform</b>.</p> </li> </ul> <div data-bbox="954 961 1377 1220" style="border: 1px solid #0070C0; padding: 10px; margin-top: 10px;"> <p> <b>Note:</b></p> <p>If you're an Oracle SaaS customer, you must have purchased a Sauce Video subscription to see this option.</p> </div> |
| <p><b>Instance Type</b> (not supported in Starter Edition)</p> | <p>You must have at least one primary instance (for example, your production instance). You can optionally have additional non-primary instances (for example, for development or testing). Primary and non-primary instances are <a href="#">billed at different rates</a>. If you need to change the instance type, select the new type.</p>   |


| Field                     | Description  |
|---------------------------|--|
| <b>Deployment Options</b> | <p>Optionally, enable additional deployment options:</p> <ul style="list-style-type: none"> <li> <b>OCI services content sharing</b>—<br/>           Enable exchange of content between Oracle Content Management (OCM) and Oracle Cloud Infrastructure (OCI) services for advanced processing features. This option is necessary for video transcription and advanced Content Capture features. It's enabled by default in instances created after mid-February 2023.<br/>           If your instance was created before mid-February 2023 and you want to enable content sharing for the instance, select <b>OCI services content sharing</b>.<br/>           Once this option has been enabled, it can't be disabled.         </li> </ul> |

7. Click **Save Changes**.

## Monitor Billing and Usage

The Oracle Cloud Console provides various billing and payment tools that make it easy to monitor your Oracle Content Management billing, service costs, and usage.

To view your billing and usage, perform the following steps:

1. Sign in to [Oracle Cloud](#) as the cloud account administrator. You can find your account name and login information in your welcome email.
2. In the Infrastructure Console, click , then, under Governance and Administration, expand **Account Management**, then click one of the following options:
  - **Cost Analysis:** Provides easy-to-use visualization tools to help you track and optimize your spending.
  - **Upgrade and Manage Payment:** Upgrade your services and manage how you pay for your usage.
  - **Invoices:** View and download invoices for your usage.
  - **Budgets:** set thresholds for your spending. You can set alerts on your budget to let you know when you might exceed your budget, and you can view all of your budgets and spending from one single place. You can also set Oracle Content Management-specific billing limits.
  - **Cost and Usage Reports:** View comma-separated value (CSV) files that can be used to get detailed breakdowns of resources for audit or invoice reconciliation.

 **Note:**

The first time you access usage reports, you must create a policy in your root compartment. Follow the instructions on the Usage Report page to create the policy, copying the statements as directed.

For more information on the billing and payment tools, see [Billing, Cost Management, and Payments Overview](#).

## Report Issues

If you run into problems, you can access user assistance, get help from the Oracle Cloud Community, contact support, or start a live online chat with an Oracle Support representative.

In the Oracle Cloud Console, click  to perform the following actions:

- To access documentation or the Oracle Cloud Community, click one of the links under Help.
- To view the various ways you can contact Oracle Support, click **Contact Support**.
- To start a live online chat with an Oracle Support representative, click **Live Chat**.

## Manage Vanity Domains

You can set up vanity domains to make it easier for users to access sites created with Oracle Content Management or Oracle Content Management itself.

For example, the URL for your Oracle Content Management instance might be `http://instanceName-accountName.cec.ocp.oraclecloud.com` and the URL for one of your sites might be `http://instanceName-accountName.cec.ocp.oraclecloud.com/site/MyCustomerSite/`. However, a friendlier URL such as `http://www.example.com` is easier to remember, potentially better for branding, and generally simpler to use. Depending on what is required, a site created with Oracle Content Management can also be hosted with a custom path, such as `http://www.example.com/store/` or a site vanity domain, such as `https://www.mycustomer.com`.

To make use of vanity domains, several steps are required.

1. [Use a Content Delivery Network \(CDN\)](#). You can [use Oracle Content Management's CDN](#).
2. [Manage a vanity domain with a domain name system \(DNS\)](#) so the domain Canonical Name (CNAME) record is mapped to the CDN.
3. [Deploy a valid certificate on the CDN](#) protecting the vanity domain.
4. Set up the vanity domains you want.

 **Note:**

If you're using Oracle Content Management Starter Edition, you're limited to only one vanity domain for public sites or public assets, so this step doesn't apply to your instance. To take advantage of the full feature set, [upgrade to the Premium Edition](#).

- [Set up a site level vanity domain](#).
- [Set up an instance level vanity domain](#).
- [Set up a vanity domain for Oracle Content Management itself](#) (a friendly management domain).

## Understand the Different Types of Domains

There are several types of domains used to construct URLs for sites created with Oracle Content Management:

- **Site level vanity domains:** These domains can be used to access specific sites. They're individually configured in the sites themselves.
- **Instance level vanity domains for sites:** These domains can be used to access any sites in the instance. For example, if you register `example.com`, users can access your sites through `example.com/site/SiteOne` and `example.com/site/SiteTwo`. You configure these domains on the Sites page of the administrative interface. You can select one of these domains as the default for your instance, and it will be used by default to build site URLs in the Oracle Content Management user interface. With an instance level vanity domain you can also use the **Display Short Paths** option which removes the `/site/` or `/site/authsite/` portion of URLs displayed for sites in the production. This requires additional CDN configuration described below.
- **Friendly management domain:** This can be used to access your Oracle Content Management web client, the desktop app, the mobile apps, and any sites created with Oracle Content Management. You set the friendly management domain on the Domain page of the administrative interface.
- **Content delivery network (CDN) domain:** This points to your CDN. It's displayed in sites and assets when requesting their delivery URLs, and takes the form of `instanceName.ocecdn.oracelcloud.com`.
- **Origin domain:** This points to the Oracle Content Management origin and takes the form of `instanceName-accountName.cec.ocp.oraclecloud.com`.

The list above also represents the priority in which the domains are used to construct a site URL.

- If there's a site level vanity domain, that will be used as the site URL.
- If there's no site level vanity domain, the default instance level domain will be used to construct the site URL (for example, `http://www.exampleInstance.com/site/SiteOne/`).
- If there's no default instance level vanity domain, the CDN domain will be used (for example, `http://instanceName.ocecdn.oracelcloud.com/site/SiteOne/`).



- And finally, if there is no CDN, the origin domain will be used (for example, `https://instanceName-accountName.cec.ocp.oraclecloud.com:8080/site/SiteOne/`).

## Use a Content Delivery Network

Both site and instance vanity domains require the use of a Content Delivery Network (CDN). A CDN is a platform of globally distributed servers meant to improve the performance and security of web sites. A CDN minimizes the distance between users and servers while optimizing the end-to-end performance of requests for content. While the primary goal of a CDN is to improve user experience, a CDN can also be used to alter requests in transit so that what the visitor sees is clean even if the process behind the scenes is not.

To support the hosting of an Oracle Content Management site on a vanity domain you will need to work with the CDN to configure it to handle all requests from the configured vanity domain, route them back to Oracle Content Management properly, and make alterations to the requests so they are handled properly and securely by Oracle Content Management.

## Use Oracle Content Management's Content Delivery Network

Oracle Content Management provides CDN services to enable several vanity domain setups. By using Oracle Content Management's CDN services you can host site level vanity domains, including bare domains and custom paths, as well as instance level vanity domains, both standard and short paths, and friendly management URLs.



### Note:

Oracle Content Management's built-in Content Delivery Network isn't supported in private instances.

To set these up, sign in to your Oracle Support account and see knowledge base article [How to Use a Custom Hostname with Oracle Content Management](#). Work with the support teams to complete the process.

Oracle Content Management controls the CDN and associated security policies so access to full CDN capabilities and customizations are not possible. If you require additional control over the CDN delivery layer you must acquire your own CDN services and configure them to your needs.

## Manage a Domain with a Domain Name System

Any domain can be used as a vanity domain for an Oracle Content Management site. You must control any domain used as the vanity domain before configuring it for use with an Oracle Content Management site.

Due to the limitations of domain name systems (DNS), using a root domain, such as `example.com`, without a `www` or another subdomain, such as `store.example.com`, may not be possible. Check with your DNS and CDN providers to determine if using a canonical name (CNAME) record for your root domain is possible.

Because DNS functions at the domain level and not the path level, for Oracle Content Management to host some paths of your domain and another service host other paths,

routing will need to be handled by the CDN. DNS can only be used to segregate traffic at the domain and subdomain level.

## Deploy Certificates

A certificate protecting a vanity domain needs to be created and hosted by the CDN. A certificate may protect a single domain, multiple domains, subdomains, and wildcarded subdomains such as \*.example.com. Any combination is acceptable for a vanity domain. All protected domains will be visible in the certificate details, so if sharing these details publicly is unintended, separate certificates should be used.



### Note:

The process for creating and hosting certificates is often specific to the CDN and they will need to specify how best to do this.

## Set Up a Site Vanity Domain

The following steps must be completed to configure a site vanity domain. This process may be repeated for additional sites on the same domain, at different paths, or on different domains.

- [Configure a Site With a Site Vanity Domain](#)
- [Configure the CDN to Route Requests to a Public Site](#)
- [Configure the CDN to Route Requests to a Secure Site](#)

## Configure a Site With a Site Vanity Domain

For an Oracle Content Management site to load properly when using a vanity domain, you must configure the site to do so. This is done in the site's properties.

1. In Oracle Content Management, click **Sites** in the side navigation.
2. Select the site you want to use a vanity domain with and choose **Properties** from the right-click menu or in the actions bar.
3. Enter the vanity domain in the vanity domain field and click **Save**.

It can take up to an hour for Oracle Content Management to be ready to accept requests on the vanity domain. During this time, you can access the site on the original domain. You can monitor progress at any time in the site properties panel.



### Note:

If you are using the [Oracle Content Management CDN](#) you do not need to perform any additional actions. If you are using a different 3rd-party CDN, review [Configure the CDN to Route Requests to a Public Site](#) and [Configure the CDN to Route Requests to a Secure Site](#). If necessary, consult your CDN for specific instructions.

## Configure the CDN to Route Requests to a Public Site

Once Oracle Content Management is properly configured and ready to accept them, requests made using the vanity domain will be routed according to the DNS entries to the CDN and the CDN will forward the requests to Oracle Content Management. This routing is usually done with a CNAME entry in your DNS records. Consult your CDN for specific instructions.

For example, if an Oracle Content Management site with a site URL of `https://myinstance.cec.ocp.oraclecloud.com/site/MyCustomerSite/` is configured with a vanity domain of `https://www.example.com/store/`, then the CDN must be configured to:

- recognize the vanity domain and custom path: `https://www.example.com/store/`
- specify the origin Oracle Content Management instance using the vanity domain: `https://myinstance.cec.ocp.oraclecloud.com/`
- append the site path for the specific site, in this case: `/site/MyCustomerSite/`
- send the full site URL to the origin Oracle Content Management instance: `https://myinstance.cec.ocp.oraclecloud.com/site/MyCustomerSite/`

Oracle Content Management will then receive the request and respond to the CDN, which satisfies the request to the visitor's browser, showing only the vanity domain and custom path to the visitor: `https://www.example.com/store/`

CDN configuration steps are often specific to the CDN, so work with your CDN provider to properly configure the desired behaviors.

### Note:

The CDN configuration altering the path must not apply to any requests containing the following strings. The trailing wildcard is required for proper matching.

- `/documents*`
- `/system*`
- `/content/published*`
- `/osn*`
- `/pxysvc*`
- `/_compdelivery/*`
- `/_themes/*`
- `/site*`
- `/_sitesclouddelivery/*`
- `/favicon.ico*`

Requests to these paths are not meant to include the site path and so should be excluded from the path modification behavior. They should resolve to the root of the Oracle Content Management instance to be handled properly.

Routing requests from a single vanity domain to multiple Oracle Content Management instances is not supported. Many required requests have shared paths that do not include a

site identifier so it is not possible to properly route requests to the correct instance. It is recommended that you use different domains or subdomains if you are working with multiple Oracle Content Management instances.

## Configure the CDN to Route Requests to a Secure Site

A secure site requires visitors to authenticate so Oracle Content Management can confirm they are authorized to view the site before accessing it. This authentication is handled by routing the visitor to an Oracle identity manager such as Oracle Cloud Infrastructure (OCI) Identity and Access Manager (IAM), and then back to the site once a proper session has been established. This means the CDN configuration for a secure site requires a few more behaviors than for a public site. Consult your CDN for specific instructions.

For example, if a secure Oracle Content Management site with a site URL of `https://myinstance.cec.ocp.oraclecloud.com/site/authsite/MySecureSite/` is configured with a vanity domain of `https://www.example.com/secure/` then the CDN must be configured to:

- recognize the vanity domain and custom path: `https://www.example.com/secure/`
- specify the origin Oracle Content Management instance using the vanity domain: `https://myinstance.cec.ocp.oraclecloud.com/`
- append the site path for this specific site: `/site/authsite/MySecureSite/`
- send the full site URL to the origin Oracle Content Management instance: `https://myinstance.cec.ocp.oraclecloud.com/site/authsite/MySecureSite/`
- ensure the Forward Host Header matches the vanity domain using a Custom Value or Incoming Host Header option.
- ensure all calls to the server function by enabling the HTTP DELETE, POST, PUT, and PATCH methods, which are often not enabled by default in CDN configurations.
- create a separate rule that will update the location header of the `/cloudgate/v1/oauth2/callback` response. This will ensure the visitor ends up at the correct domain and path.

By default, the authenticated user will be returned to a combination of the vanity domain and original site path, such as `https://www.example.com/site/authsite/MySecureSite/`. You want the visitor returned to `https://www.example.com/secure/`. To do this, this rule must execute on the `/cloudgate/v1/oauth2/callback` request when the response's location header includes the name of your site. In this case, *MySecureSite*.

This rule should then execute a find and replace of the location header's value, replacing `/site/authsite/MySecureSite/` with `/secure/`. A find and replace operation will allow all pages of the site to also redirect properly, where as a simple path replacement would always return the user to the home page.

When implemented correctly, Oracle Content Management will receive the request and respond to the CDN, which satisfies the request to the visitor's browser, showing only the vanity domain and path to the visitor. In this example: `https://www.example.com/secure/`

CDN configuration steps are often specific to the CDN, so work with your CDN provider to properly configure the described behaviors.

## Set Up an Instance Vanity Domain

The following steps must be completed to configure an instance vanity domain. While multiple instance vanity domains can be configured, only a single instance vanity domain will be used by the user interface to display site URLs.

- [Configure Oracle Content Management With Your Instance Vanity Domain](#)
- [Configure the CDN When Using Standard Paths](#)
- [Configure the CDN When Using Short Paths](#)

## Configure Oracle Content Management With Your Instance Vanity Domain

For Oracle Content Management sites to load properly on an instance vanity domain, you must configure Oracle Content Management properly.

1. Sign in as a service administrator and click **System** under **Administration** in the side navigation panel.
2. Select **Sites** from the banner menu.
3. Click **Manage Vanity Domains** under the **Vanity Domain Configuration** section and enter your instance level vanity domain and click **Save**. Multiple domains can be added and managed.
4. Select a vanity domain as the default.
5. Enable or disable **Display Short Paths** to toggle on or off the display of `/site/` or `/site/authsite/` in the user interface. This is helpful when most or all of your sites are either public or secure, and your CDN is configured properly.

 **Note:**

Short paths aren't supported in private instances.

It can take up to an hour for Oracle Content Management to be ready to accept requests on the vanity domain. During this time, you can access your sites on the original domain.

 **Note:**

If you are using the [Oracle Content Management CDN](#) you do not need to perform any additional actions. If you are using a different 3rd-party CDN, review [Configure the CDN When Using Standard Paths](#) and [Configure the CDN When Using Short Paths](#). If necessary, consult your CDN for specific instructions.

## Configure the CDN When Using Standard Paths

If **Display Short Paths** is disabled, all site URLs shown in the product will include the full instance vanity domain and site path. Your CDN needs to be configured to route those requests back to the Oracle Content Management origin unaltered.

Once Oracle Content Management is properly configured and ready to accept them, requests made using the instance vanity domain will be routed according to the DNS entries to the

CDN and the CDN will forward the requests to Oracle Content Management properly. This is usually done using a CNAME entry in your DNS records. Consult your CDN for specific instructions.

For example, if an Oracle Content Management site has the URL of `https://myinstance.cec.ocp.oraclecloud.com/site/MyFirstProjectSite/` and you want to access that site at `https://www.example.com/site/MyFirstProjectSite/` the CDN must be configured to:

- recognize the vanity domain: `https://www.example.com/`
- identify the origin Oracle Content Management instance using the vanity domain: `https://myinstance.cec.ocp.oraclecloud.com/`
- passthrough the request path: `/site/MyFirstProjectSite/`
- and send the full request path to the origin Oracle Content Management instance: `https://myinstance.cec.ocp.oraclecloud.com/site/MyFirstProjectSite/`
- Oracle Content Management receives the request and responds to the CDN, which satisfies the request to the visitor's browser, showing only the vanity domain and standard path to the visitor: `https://www.example.com/site/MyFirstProjectSite/`

These same steps would apply to all requests made for a secure site. The only difference is those paths include `/site/authsite/` rather than just `/site/`.

CDN configuration steps are often specific to the CDN, so work with your CDN provider to properly configure the desired behaviors.

## Configure the CDN When Using Short Paths

If **Display Short Paths** is enabled, site URLs shown in the product will only include the site name rather than including the `/site/` or `/site/authsite/` portion of the path.

For example, if you enable **Display Short Paths** and want to reach your Acme-Store site and you know it's a public site, you could make a request to `https://www.acme.com/Acme-Store/` and the CDN would inject `/site/` when going back to the Oracle Content Management instance with the full path of `https://acmeInstance.cec.ocp.oraclecloud.com/site/Acme-Store/`.

A limitation of this feature is that the CDN must know to inject `/site/` or `/site/authsite/`. This is because the Oracle Content Management instance must receive the full path, including `/site/` or `/site/authsite/`, depending on if the site is a public site or a secure site. This means this option is most useful when the majority of your sites are of the same type, either public or secure.

If you have a large mix of public and secure sites, then short paths may not be worth the effort required to maintain your CDN configuration. Preferably most of your sites would be of one type and each of the few remainders could then be handled with exception rules.

For example, let's say you have 10 sites, 9 of which are public and one is secure called *MyAccountSite*. Your CDN should be configured such that the public site requests coming to your domain, for a path other than `/MyAccountSite/` or one of the excluded paths listed below, have `/site/` injected into the path before going back to the Oracle Content Management instance to load the site resources. But if the request is for the secure site `/MyAccountSite/`, then an exception rule for that site will instead

inject `/site/authsite/` into the path and the additional behaviors needed to authenticate users are done. If most of your sites are secure, then the CDN configuration should be reversed so that each public site would need an exception rule.

If you do not set up exception rules for each site not covered by the default path injection behavior in your CDN configuration, those sites will fail to load as your Oracle Content Management instance will not know where to find the site.

 **Note:**

The CDN configuration altering the path must not apply to any requests containing the following strings. The trailing wildcard is required for proper matching.

- `/documents*`
- `/system*`
- `/content*`
- `/osn*`
- `/pxysvc*`
- `/_compdelivery/*`
- `/_themes/*`
- `/site*`
- `/_sitesclouddelivery/*`
- `/favicon.ico*`

Once Oracle Content Management is properly configured and ready to accept them, requests made using the instance vanity domain will be routed according to the DNS entries to the CDN and the CDN will forward the requests to Oracle Content Management properly.

For example, if an Oracle Content Management has been configured to use short paths, your sites are public, and a request is made to `https://www.example.com/MySecondProjectSite/` the CDN must be configured to:

- recognize the vanity domain: `https://www.example.com/`
- specify the origin Oracle Content Management instance using the vanity domain: `https://myinstance.cec.ocp.oraclecloud.com/`
- prepend `/site/` to the path
- send the full site URL to the origin Oracle Content Management instance: `https://myinstance.cec.ocp.oraclecloud.com/site/MySecondProjectSite/`
- Oracle Content Management receives the request and responds to the CDN, which satisfies the request to the visitor's browser, showing only the vanity domain and site name: `https://www.example.com/MySecondProjectSite/`

If most of your sites are secure sites the same rules apply. Instead of prepending `/site/` you need to prepend `/site/authsite/`.

Exception rules must be defined for all sites that are not the default type. Configure that exception rule to match on the specific site names so those requests can have the proper path appended rather than the default.

CDN configuration steps are often specific to the CDN, so work with your CDN provider to properly configure the desired behaviors.

## Set Up a Vanity Domain for Oracle Content Management Itself

You can configure a *friendly management domain*, a vanity domain to be used to access your Oracle Content Management web client, the desktop app, and the mobile apps. When you define a friendly management domain, users will still be able to access the web client using the original URL, but will be redirected to your friendly management domain automatically.

Complete the following steps to configure a friendly management domain:

1. Depending on whether you use a CDN or a private instance, you'll configure your tenancy in different ways:
  - [Configure Your CDN for Your Friendly Management Domain](#)
  - [Using a Friendly Management Domain in a Private Instance](#)
2. [Configure Oracle Content Management with Your Friendly Management Domain](#)
3. If you use a custom sign-in page, your friendly management domain must also be configured as an [instance-level vanity domain](#).
4. If you want to use your friendly management domain to access Oracle Content Management sites, your friendly management domain must also be configured as an [instance-level vanity domain](#) or a [site-level vanity domain](#).

## Configure Your CDN for Your Friendly Management Domain

Before your Oracle Content Management instance can function using your friendly management domain, your CDN needs to be configured to route those requests back to the Oracle Content Management origin unaltered.

Once Oracle Content Management is properly configured and ready to accept them, requests made using the friendly management domain will be routed according to the DNS entries to the CDN, and the CDN will forward the requests to Oracle Content Management properly. This is usually done using a CNAME entry in your DNS records. Consult your CDN for specific instructions.

For example, if your Oracle Content Management instance is accessed at a URL like `https://myinstance.cec.ocp.oraclecloud.com/documents/home` and you want to access that site at `https://www.example.com/documents/home`, the CDN must be configured to:

- Recognize the vanity domain: `https://www.example.com/`
- Specify the origin Oracle Content Management instance using the vanity domain: `https://myinstance.cec.ocp.oraclecloud.com/`
- Ensure the Forward Host Header matches the friendly management domain (details below)
- Ensure all calls to the server function by enabling the HTTP DELETE (with Body enabled), POST, PUT, and PATCH methods, which are often not enabled by default in CDN configurations
- Send the full request path to the origin Oracle Content Management instance: `https://myinstance.cec.ocp.oraclecloud.com/documents/home`



After the CDN is configured properly, Oracle Content Management receives the request and responds to the CDN, which satisfies the request to the visitor's browser, showing only the friendly management domain and path: `https://www.example.com/documents/home`.

The Forward Host Header is included on all requests made by your client. By default, it contains your instance's original host name (the origin domain). When you configure a friendly management domain, you must change the Forward Host Header so that your CDN knows to route requests to the friendly management domain back to the origin domain.

Depending on which CDN you use, this process will be done differently. Generally, you alter the rules that define your origin or you apply a behavior to requests passing through the CDN. Consult your CDN's documentation for additional details.

 **Note:**

Your CDN may provide you the option to hard code a custom Forward Host Header or simply pass through the Incoming Host Header that was sent by the client. Best practice is to hard code the custom Forward Host Header to the vanity domain you have selected. Although the pass through option will work, it may trigger warnings if you run a vulnerability test. Such a test may see this as an opportunity for a malicious user to alter the Forward Host Header and facilitate an attack. Oracle Content Management protects itself from this type of attack, but it's best to avoid the confusion such a finding may cause.

Next, [configure Oracle Content Management with your friendly management domain](#).

## Using a Friendly Management Domain in a Private Instance

 **Note:**

This method works for a friendly management domain or an instance level vanity domain using standard paths. It doesn't work for an instance level vanity domain using short paths or for site level vanity domains, as both of those situations require a CDN to modify paths, and this method doesn't use a CDN.

You must complete the following prerequisites before you can set up a friendly management domain in your private instance:

- [Create your private instance](#).
- Obtain an SSL certificate for your friendly management domain. For more information, see [SSL Certificate for Load Balancers](#).
- [Create a front-end public load balancer](#) in your tenancy.

To set up a friendly management domain in your private instance:

1. [Create a private load balancer](#) in your tenancy. This load balancer will be added as a backend to handle traffic for your friendly management domain.
  - a. In the Create Load Balancer dialog, use the following settings for the **Add Details** section:

| Field  | Setting   |
|--|---|
| Load Balancer Name                             | Specify a friendly name.  |
| Choose Visibility Type                         | Private   |
| Choose IP Address Type                         | Leave the default—Ephemeral IP Address.   |
| Bandwidth                                      | Flexible Shapes<br>Set the minimum and maximum bandwidths. The Oracle Content Management back-end private load balancer supports up to 400Mbps bandwidth.   |
| Choose Networking                              | <ul style="list-style-type: none"> <li>Select an available Virtual Cloud Network (VCN) or have the system create one for you.</li> <li>Select a regional subnet that has network access to the private load balancer IP through LPG peering.</li> </ul> |
| Use Network Security Groups to Control Traffic | Leave unchecked.  |
| Show Advanced Options                          | Skip the advanced options.  |

- b. Use the following settings for the **Choose Backends** section:

| Field                           | Setting  |
|---------------------------------|--|
| Specify a Load Balancing Policy | Weighted Round Robin   |
| Select Backend Servers          | Skip this setting.   |
| Specify Health Check Policy     | <ul style="list-style-type: none"> <li>Protocol : TCP</li> <li>Port: 443</li> <li>Interval in ms: 30000</li> <li>Timeout in ms: 10000</li> <li>Number of retries: 3</li> </ul>   |
| Use SSL                         | Select this option to apply SSL. <ul style="list-style-type: none"> <li>SSL Certificate: Paste the full certificate chain for your friendly management domain certificate in PEM format.</li> <li>Specify CA Certificate: Paste the root CA certificate in PEM format.</li> <li>Specify Private Key: Paste the private key in PEM format.</li> </ul> |
| Show Advanced Options           | Skip the advanced options.   |

- c. Use the following settings for the **Configure Listener** section:

| Field   | Setting                 |
|---|-------------------------|
| Listener Name   | Specify a friendly name |
| Specify the type of traffic your listener handles           | TCP                     |
| Specify the port your listener monitors for ingress traffic | 443                     |

| Field                 | Setting   |
|-----------------------|---|
| Use SSL               | Select this option to apply SSL. <ul style="list-style-type: none"> <li>• <b>SSL Certificate:</b> Paste the full certificate chain for your friendly management domain certificate in PEM format.</li> <li>• <b>Specify CA Certificate:</b> Paste the root CA certificate in PEM format.</li> <li>• <b>Specify Private Key:</b> Paste the private key in PEM format.</li> </ul> |
| Show Advanced Options | Skip the advanced options.  |

- d. Submit the settings to create the load balancer.
- e. After the private load balancer is created, note its IP address for the next step.
2. [Add the private load balancer as a backend server](#) to your front-end public load balancer.
  - a. In the Add Backends dialog, choose **IP Addresses**, and enter the following settings:

| Field      | Setting  |
|------------|--|
| IP Address | The IP address of the private load balancer you just created |
| Port       | 443  |
| Weight     | 100  |

- b. Add the backend.
3. [Check the health](#) of the front-end public load balancer and the back-end private load balancer, making sure both are good.
4. [Add a DNS record](#) for the friendly management domain.
  - a. In the Add Record dialog, select type **A**.
  - b. Enter the IP address of the private load balancer you just created.
  - c. Submit and publish your changes.
5. Update your firewall settings to ensure that any clients using this private instance of Oracle Content Management can reach `static.ocecdn.oraclecloud.com`. This domain is used to load common files for the web client, so if users don't have access to this domain, they won't be able to utilize the web client.

Next, [configure Oracle Content Management with your friendly management domain](#).

## Configure Oracle Content Management with Your Friendly Management Domain

After you've configured your tenancy, you're ready to configure Oracle Content Management with your friendly management domain.

1. After you sign in to the Oracle Content Management web application as a service administrator, click **System** in the Administration area of the navigation menu.
2. In the **System Settings** drop-down menu, choose **Domain**.
3. In the **Friendly Management Domain** box, enter the URL (for example, `content.example.com`) you want users to use to access Oracle Content Management.

4. It can take up to 30 minutes for Oracle Content Management to make the necessary back-end changes. During this time you won't be able to edit the setting, but users can continue to access your instance on the original domain. You must complete the next step before your friendly management domain will be available to users.
5. When the process has completed, you'll receive an email notification with the status of the change.  
If the change was successful, the email will include a link to confirm that the redirect to the friendly management domain works as expected. You must validate the domain within 60 minutes or the change will be reverted. Once you validate the domain, Oracle Content Management will send an email to all users informing them that they can access your instance through the new friendly management domain.

If the change wasn't successful or doesn't work as expected, you can revert the change through the notification email or on the Domain page.

If necessary, perform these additional steps:

- If you use a custom sign-in page, your friendly management domain must also be configured as an [instance-level vanity domain](#).
- If you want to use your friendly management domain to access Oracle Content Management sites, your friendly management domain must also be configured as an [instance-level vanity domain](#) or a [site-level vanity domain](#).

To delete the friendly management domain, click **Remove**. Oracle Content Management will send an email to all users informing them that they should now access your instance through the original domain.

# 5

## Service Limits, Quotas, Policies, and Events

This section describes Oracle Content Management service limits, quotas, policies, and events.

- [Service Limits](#)
- [Service Quotas](#)
- [Service Policies](#)
- [Service Events](#)

### Service Limits

Oracle Content Management has various default limits. Whenever you create an Oracle Content Management instance, the system ensures that your request is within the bounds of your limit.

If necessary, you can submit a request to increase your limits in the Oracle Cloud Console from the **Limits, Quotas, and Usage** page. See [About Service Limits and Usage](#).

This table lists the default service limits for Oracle Content Management.

| Resource Limit                        | Limit Short Names             | Default Value | Description  |
|---------------------------------------|-------------------------------|---------------|--|
| Oracle Content Management Service Max | max-services-count-per-tenant | 100           | Maximum number of Oracle Content Management instances you can create per tenant. |

### Service Quotas

You can use quotas to determine how other users allocate Oracle Content Management resources across compartments in Oracle Cloud Infrastructure. Whenever you create an Oracle Content Management instance, the system ensures that your request is within the bounds of the quota for that compartment.

You can manage the service quotas in the Oracle Cloud Console from the compartment detail page. See [About Compartment Quotas](#).

This table lists the service quotas for Oracle Content Management.

| Quota Name         | Scope    | Description                                   |
|--------------------|----------|---|
| oce-instance-count | Regional | Number of Oracle Content Management instances |

#### Example Quota Statements for Oracle Content Management

- Limit the number of Oracle Content Management instances that users can create in MyCompartment to 10.

```
Set oce_quota oce-instance-count to 10 in compartment MyCompartment
```

## Service Policies

You use authorization policies to control access to resources in your tenancy. For example, you can create a policy that authorizes users to create and manage Oracle Content Management instances.

You create policies using the Oracle Cloud Console. See [Managing Policies](#).

The following information pertains to service policies for Oracle Content Management:

- [Resource Types for Oracle Content Management](#)
- [Supported Variables](#)
- [Details for Verb and Resource-Type Combinations](#)
- [Permissions Required for Each API Operation](#)
- [Example Policy Statements to Manage Oracle Content Management Instances](#)

## Resource Types for Oracle Content Management

This table lists the resource types for Oracle Content Management.

| Resource Type    | Description  |
|------------------|--|
| oce-instance     | A single Oracle Content Management instance.   |
| oce-instances    | One or more Oracle Content Management instances.   |
| oce-workrequest  | A single work request for Oracle Content Management.<br>Each operation you perform on an Oracle Content Management instance, creates a work request. For example, operations such as create, update, terminate, and so on. |
| oce-workrequests | One or more work requests for Oracle Content Management.   |

## Supported Variables

The values of these variables are supplied by Oracle Content Management. In addition, other general variables are supported. See [General Variables for All Requests](#).

This table lists the supported variables for Oracle Content Management.

| Variable              | Type   | Description   | Sample Value  |
|-----------------------|--------|---|---|
| target.compartment.id | entity | The OCID of the primary resource for the request.               | target.compartment.id = 'ocid1.compartment.oc1.<unique_ID>'                 |
| request.operation     | string | The operation id (for example, 'GetUser') for the request.      | request.operation = 'ocid1.compartment.oc1.<unique_ID>'                     |
| target.resource.kind  | string | The resource kind name of the primary resource for the request. | target.resource.kind = 'ocid1.contentexperienceloudservice.oc1.<unique_ID>' |

## Details for Verb and Resource-Type Combinations

Oracle Cloud Infrastructure offers a standard set of verbs to define permissions across Oracle Cloud Infrastructure resources (**Inspect**, **Read**, **Use**, **Manage**). These tables list the Oracle Content Management permissions associated with each verb. The level of access is cumulative as you go from **Inspect** to **Read** to **Use** to **Manage**.

### INSPECT

| Resource Type   | INSPECT Permissions  |
|---|--|
| <ul style="list-style-type: none"> <li>oce-instance</li> <li>oce-instances</li> <li>oce-workrequest</li> <li>oce-workrequests</li> <li>oce-instance-family</li> </ul> | <ul style="list-style-type: none"> <li>OCE_INSTANCE_INSPECT</li> <li>OCE_INSTANCE_WORKREQUEST_INSPECT</li> <li>OCE_INSTANCE_INSPECT</li> <li>OCE_INSTANCE_WORKREQUEST_INSPECT</li> </ul> |

### READ

| Resource Type   | READ Permissions   |
|---|--|
| <ul style="list-style-type: none"> <li>oce-instance</li> <li>oce-instances</li> <li>oce-workrequest</li> <li>oce-workrequests</li> <li>oce-instance-family</li> </ul> | <ul style="list-style-type: none"> <li>OCE_INSTANCE_INSPECT</li> <li>OCE_INSTANCE_READ</li> <li>OCE_INSTANCE_WORKREQUEST_INSPECT</li> <li>OCE_INSTANCE_WORKREQUEST_READ</li> <li>OCE_INSTANCE_INSPECT</li> <li>OCE_INSTANCE_READ</li> <li>OCE_INSTANCE_WORKREQUEST_INSPECT</li> <li>OCE_INSTANCE_WORKREQUEST_READ</li> </ul> |

### USE

| Resource Type   | USE Permissions  |
|---|--|
| <ul style="list-style-type: none"> <li>oce-instance</li> <li>oce-instances</li> </ul> | <ul style="list-style-type: none"> <li>OCE_INSTANCE_INSPECT</li> <li>OCE_INSTANCE_READ</li> <li>OCE_INSTANCE_UPDATE</li> </ul> |

| Resource Type   | USE Permissions   |
|---|---|
| <ul style="list-style-type: none"> <li>oce-workrequest</li> <li>oce-workrequests</li> </ul> | <ul style="list-style-type: none"> <li>OCE_INSTANCE_WORKREQUEST_INSPECT</li> <li>OCE_INSTANCE_WORKREQUEST_READ</li> </ul>   |
| <ul style="list-style-type: none"> <li>oce-instance-family</li> </ul>                       | <ul style="list-style-type: none"> <li>OCE_INSTANCE_INSPECT</li> <li>OCE_INSTANCE_READ</li> <li>OCE_INSTANCE_UPDATE</li> <li>OCE_INSTANCE_WORKREQUEST_INSPECT</li> <li>OCE_INSTANCE_WORKREQUEST_READ</li> </ul> |

## MANAGE

| Resource Type   | MANAGE Permissions  |
|---|---|
| <ul style="list-style-type: none"> <li>oce-instance</li> <li>oce-instances</li> </ul>       | <ul style="list-style-type: none"> <li>OCE_INSTANCE_INSPECT</li> <li>OCE_INSTANCE_READ</li> <li>OCE_INSTANCE_CREATE</li> <li>OCE_INSTANCE_UPDATE</li> <li>OCE_INSTANCE_DELETE</li> </ul>  |
| <ul style="list-style-type: none"> <li>oce-workrequest</li> <li>oce-workrequests</li> </ul> | <ul style="list-style-type: none"> <li>OCE_INSTANCE_WORKREQUEST_INSPECT</li> <li>OCE_INSTANCE_WORKREQUEST_READ</li> </ul>   |
| <ul style="list-style-type: none"> <li>oce-instance-family</li> </ul>                       | <ul style="list-style-type: none"> <li>OCE_INSTANCE_INSPECT</li> <li>OCE_INSTANCE_READ</li> <li>OCE_INSTANCE_CREATE</li> <li>OCE_INSTANCE_UPDATE</li> <li>OCE_INSTANCE_DELETE</li> <li>OCE_INSTANCE_WORKREQUEST_INSPECT</li> <li>OCE_INSTANCE_WORKREQUEST_READ</li> </ul> |

## Permissions Required for Each API Operation

This table shows the API operations available for Oracle Content Management, grouped by resource type.

| REST API Operation            | CLI Command Operation           | Permission Required to Use the Operation |
|-------------------------------|---------------------------------|--|
| ListOcelInstances             | oce-instance list               | OCE_INSTANCE_INSPECT                     |
| GetOcelInstance               | oce-instance get                | OCE_INSTANCE_READ                        |
| CreateOcelInstance            | oce-instance create             | OCE_INSTANCE_CREATE                      |
| DeleteOcelInstance            | oce-instance delete             | OCE_INSTANCE_DELETE                      |
| UpdateOcelInstance            | oce-instance update             | OCE_INSTANCE_UPDATE                      |
| ChangeOcelInstanceCompartment | oce-instance change-compartment | OCE_INSTANCE_UPDATE                      |
| ListWorkRequests              | work-request list               | OCE_INSTANCE_WORKREQUEST_INSPECT         |



| REST API Operation    | CLI Command Operation   | Permission Required to Use the Operation |
|-----------------------|-------------------------|--|
| GetWorkRequest        | work-request get        | OCE_INSTANCE_WORKREQUEST_READ            |
| ListWorkRequestErrors | work-request-error list | OCE_INSTANCE_WORKREQUEST_INSPECT         |
| ListWorkRequestLogs   | work-request-log list   | OCE_INSTANCE_WORKREQUEST_INSPECT         |

## Example Policy Statements to Manage Oracle Content Management Instances

Here are typical policy statements that you might use to authorize access to Oracle Content Management instances.

When you create a policy for your tenancy, you grant users access to all compartments by way of [policy inheritance](#). Alternatively, you can restrict access to individual Oracle Content Management instances or compartments.

### Let users in the Administrators group fully manage any Oracle Content Management instance

```
# Full admin permissions (CRUD)
allow group Administrators to manage oce-instances in tenancy
allow group Administrators to manage oce-workrequests in tenancy
```

```
# Full admin permissions (CRUD) using family
allow group Administrators to manage oce-instance-family in tenancy
```

### Let users in the group1 group inspect any Oracle Content Management instance and their associated work requests

```
# Inspect permissions (list oce instances and work requests) using metaverbs:
allow group group1 to inspect oce-instances in tenancy
allow group group1 to inspect oce-workrequests in tenancy
```

```
# Inspect permissions (list oce instances and work requests) using
permission names:
allow group group1 to {OCE_INSTANCE_INSPECT} in tenancy
allow group group1 to {OCE_INSTANCE_WORKREQUEST_INSPECT} in tenancy
```

### Let users in the group2 group read details about any Oracle Content Management instance and their associated work requests

```
# Read permissions (read complete oce instance and work request metadata)
using metaverbs:
```

```
allow group group2 to read oce-instances in tenancy
allow group group2 to read oce-workrequests in tenancy
```

```
# Read permissions (read complete oce instance and work request
metadata) using permission names:
allow group group2 to {OCE_INSTANCE_INSPECT, OCE_INSTANCE_READ} in
tenancy
allow group group2 to {OCE_INSTANCE_WORKREQUEST_INSPECT,
OCE_INSTANCE_WORKREQUEST_READ} in tenancy
```

### **Let users in the group3 group read all Oracle Content Management instances and read their associated work requests**

```
# Use permissions (read on oce instance, read on work request) using
metaverbs:
allow group group3 to use oce-instances in tenancy
allow group group3 to read oce-workrequests in tenancy
```

```
# Use permissions (read on oce instance, read on work request) using
permission names:
allow group group3 to {OCE_INSTANCE_INSPECT, OCE_INSTANCE_READ,
OCE_INSTANCE_UPDATE} in tenancy
allow group group3 to {OCE_INSTANCE_WORKREQUEST_INSPECT,
OCE_INSTANCE_WORKREQUEST_READ} in tenancy
```

### **Let users in the group4 group manage any Oracle Content Management instance and their associated work requests**

```
# Manage permissions (use/delete on oce instance, read/cancel on work
request) using metaverbs:
allow group group4 to manage oce-instances in tenancy
allow group group4 to manage oce-workrequests in tenancy
```

```
# Manage permissions (use/delete on oce instance, read/cancel on work
request) using permission names:
allow group group4 to {OCE_INSTANCE_INSPECT, OCE_INSTANCE_READ,
OCE_INSTANCE_UPDATE,OCE_INSTANCE_CREATE, OCE_INSTANCE_DELETE} in
tenancy
allow group group4 to {OCE_INSTANCE_WORKREQUEST_INSPECT,
OCE_INSTANCE_WORKREQUEST_READ} in tenancy
```

## Service Events

Actions that you perform on Oracle Content Management instances emit events. You can use the Oracle Cloud Console to define rules that trigger a specific action when an event occurs. For example, you might define a rule that sends a notification to administrators when someone deletes an instance. See [Overview of Events](#) and [Get Started with Events](#).

This table lists the Oracle Content Management events that you can reference.

| Event Name                           | Event Type   |
|--------------------------------------|--|
| GetOceInstance                       | com.oraclecloud.oce.GetOceInstance                     |
| ListOceInstances                     | com.oraclecloud.oce.ListOceInstances                   |
| ChangeOceInstanceCompartment (begin) | com.oraclecloud.oce.ChangeOceInstanceCompartment.begin |
| ChangeOceInstanceCompartment (end)   | com.oraclecloud.oce.ChangeOceInstanceCompartment.end   |
| CreateOceInstance (begin)            | com.oraclecloud.oce.CreateOceInstance.begin            |
| CreateOceInstance (end)              | com.oraclecloud.oce.CreateOceInstance.end              |
| DeleteOceInstance (begin)            | com.oraclecloud.oce.DeleteOceInstance.begin            |
| DeleteOceInstance (end)              | com.oraclecloud.oce.DeleteOceInstance.end              |
| UpdateOceInstance (begin)            | com.oraclecloud.oce.UpdateOceInstance.begin            |
| UpdateOceInstance (end)              | com.oraclecloud.oce.UpdateOceInstance.end              |

### Example

This example shows information associated with the event **CreateOceInstance (begin)**:

```
{
  "eventType": "com.oraclecloud.oce.CreateOceInstance.begin",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "oce",
  "eventId": "<unique_ID>",
  "eventTime": "2019-10-10T04:33:06.133Z",
  "contentType": "application/json",
  "data": {
    "eventGroupingId": "ocidl.coreservicesworkrequest.oc1.<unique_ID>",
    "eventName": "CreateOceInstance",
    "compartmentId": "ocidl.compartment.oc1.<unique_ID>",
    "compartmentName": "my_compartment",
    "resourceName": "my_oce",
    "resourceId": "ocidl.contentexperiencecloudservice.oc1.<unique_ID>",
    "availabilityDomain": "<availability_domain>",
    "freeformTags": null,
    "definedTags": null,
    "identity": {
      "principalName": "admin",
      "principalId": "ocidl.user.oc1.<unique_ID>",
      "authType": "natv",
      "callerName": null,
      "callerId": null,
      "tenantId": "ocidl.tenancy.oc1.<unique_ID>",
      "ipAddress": "<ip_address>",
      "credentials": "ocidl.tenancy.oc1.<unique_ID>/
ocidl.user.oc1.<unique_ID>",
      "userAgent": null,
      "consoleSessionId": null
    }
  },
  ...
}
```