

Oracle® Cloud

Administering Oracle Content Management



F24099-71
September 2023



Oracle Cloud Administering Oracle Content Management,

F24099-71

Copyright © 2017, 2023, Oracle and/or its affiliates.

Primary Author: Sarah Bernau

Contributors: Chris DeGrace, Marcus Diaz, David Jones, Bob Lies, Mark Paterson, Bruce Silver, Ron van de Crommert, Bonnie Vaughan, Tamanna Wadhwa

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	xii
Documentation Accessibility	xii
Diversity and Inclusion	xii
Related Resources	xii
Conventions	xiii

1 Get Started

Overview of Oracle Content Management	1-1
Access Oracle Content Management	1-2
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
Starter vs. Premium Edition	1-4
Upgrade to the Premium Edition	1-7
Your Role as Administrator	1-8
Administrative Interfaces	1-8
Administrative Tasks	1-16
Roles	1-18
Typical Organization Roles	1-19
Application Roles	1-22
Task and Feature Comparison by Application Role	1-30
Resource Roles (Permissions)	1-35
Asset Types	1-36
Assets	1-37
Audience Attributes	1-37
Collections	1-37
Components and Layouts	1-38
Content Workflows	1-39

Conversations	1-39
Editorial Roles	1-39
Experiences	1-40
Files and Folders	1-40
Localization Policies	1-42
Publishing Channels	1-42
Ranking Policies	1-43
Recommendations	1-43
Rendition Policies	1-43
Repositories	1-44
Sites	1-44
Taxonomies	1-45
Templates	1-45
Themes	1-46
Workflow Roles	1-46
Security	1-46

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
Deploy OCM in a Region with Identity Domains	2-11
Create and Activate an Oracle Cloud Account	2-12
Create an OCM Instance in a Region with Identity Domains	2-13
Create a Compartment for Oracle Content Management	2-13
Delegate Creation of OCM Instances to Other Users	2-14
Create Your Instance in a Secondary Domain	2-16
Create Your Instance in Another Region	2-17
Create a Private Instance Using FastConnect	2-18
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 Non-Federated Users	2-33
Delegate Creation of OCM Instances to SSO Users	2-36
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
Enable Optional Features	2-50
Integrate Microsoft Office Online	2-50
Integrate Microsoft Outlook	2-51
Integrate Kaltura Video Management	2-51

3 Roll Out the Service

Understand the Roll-Out Process	3-1
Provide Sign-In and Get-Started Information to Users	3-2
Deploy the Desktop App	3-2
Run the Executable Installer from the Command Line	3-3
Run the MSI Installer	3-5
Deploy the MSI Installer Through Active Directory's Group Policy	3-7
Set Installation Defaults	3-8

4 Configure System Settings

Configure General Settings	4-1
Restrict File and Asset Types and Sizes	4-1
Apply Custom Branding and URLs	4-3
Enable or Disable Email Notifications	4-3

Set the Default Locale Settings	4-4
Purge Content Delivery Network (CDN) Cache	4-5
Configure Domain Settings	4-5
Configure Security Settings	4-6
Enable Cross-Origin Resource Sharing (CORS)	4-6
Embed Content in Other Domains	4-7
Configure Billing Settings	4-8
Configure Analytics Settings	4-9
Enable or Disable Consumption Analytics	4-9
Use Your Own Infinity Instance	4-9
Enable or Disable Usage Analytics	4-10
Configure Users Settings	4-10
Set the Default Resource Role for New Folder Members	4-11
Enable or Disable External Users	4-12
Search for Users and Groups	4-14
Synchronize User Profile Data	4-15
Display Conversation Membership Messages for a User	4-16
Override Storage Quota for a User	4-16
Transfer File Ownership	4-16
Override Temporary Quota for a User	4-17
Revoke Access to Linked Devices	4-17
Change Settings for Groups	4-18
View and Resynchronize Groups Out of Sync	4-18
Configure Assets Settings	4-19
Configure Sites Settings	4-19
Allow Sites to Be Created	4-20
Enable Governance for Sites	4-20
Set Minimum Security for Online Sites	4-21
Allow Sharing of Sites and Themes	4-21
Limit Site, Template, or Component Creation to Site Administrators	4-22
Add Analytics Tracking Code to Sites	4-22
Set Custom Cache Control Headers for Compiled Sites	4-23
Set a Compilation Endpoint URL	4-23
Automatically Handle Expired Sites	4-24
Install Default Site Templates	4-24
Enable Custom Sign-In	4-24
Configure Vanity Domains	4-27
Configure SEO for Sites Settings	4-28
Enable Prerender	4-28
Configure User Agents	4-28
Configure Experiences Settings	4-29

Configure Documents Settings	4-29
Restrict File and Folder Deletions	4-29
Set User Quotas and Manage Storage Space	4-30
Set Default Link Behavior	4-30
Configure Metadata Settings	4-31

5 Manage Users, Groups, and Access

Does My Region Use IAM Identity Domains?	5-2
External Users	5-3
Set the Default Resource Role for New Folder Members	5-4
Synchronize User Profile Data	5-5
Display Conversation Membership Messages for Users	5-5
Override Storage Quota for a User	5-5
Transfer File Ownership	5-6
View and Resynchronize Groups Out of Sync	5-6
Override Temporary Quota for a User	5-7
Revoke Access to Linked Devices	5-7
Change Settings for Groups	5-8
Manage Users, Groups, and Access in a Region with Identity Domains	5-8
Manage Users with IAM	5-8
Manage Groups with IAM	5-9
Manage Groups with IAM	5-10
Assign Roles to Groups with IAM	5-10
Assign Users to Groups IAM	5-11
Manage Users, Groups, and Access in a Region without Identity Domains	5-11
Enable Single Sign-On (SSO)	5-12
Manage Users with IDCS	5-12
Manage Groups with IDCS	5-14
Manage Groups with IDCS	5-14
Assign Roles to Groups with IDCS	5-15
Assign Users to Groups IDCS	5-15

6 Analyze Service Usage

Understand Analytics	6-1
View the Analytics Dashboard	6-3
View User Statistics	6-4
View Assets and Content Metrics	6-5
Repositories Metrics	6-6
Content Metrics	6-7

Channels Metrics	6-8
Collections Metrics	6-10
View Sites and Channels Analytics	6-11
View Files and Conversations Statistics	6-12
Documents Metrics	6-13
Shared Links Metrics	6-14
Conversations Metrics	6-15
View Capture Metrics	6-16
View Reports and Metrics	6-17

7 Manage the Service

Manage Vanity Domains	7-1
Understand the Different Types of Domains	7-2
Use a Content Delivery Network	7-3
Use Oracle Content Management's Content Delivery Network	7-3
Manage a Domain with a Domain Name System	7-3
Deploy Certificates	7-4
Set Up a Site Vanity Domain	7-4
Configure a Site With a Site Vanity Domain	7-4
Configure the CDN to Route Requests to a Public Site	7-5
Configure the CDN to Route Requests to a Secure Site	7-6
Set Up an Instance Vanity Domain	7-7
Configure Oracle Content Management With Your Instance Vanity Domain	7-7
Configure the CDN When Using Standard Paths	7-7
Configure the CDN When Using Short Paths	7-8
Set Up a Vanity Domain for Oracle Content Management Itself	7-10
Configure Your CDN for Your Friendly Management Domain	7-10
Using a Friendly Management Domain in a Private Instance	7-11
Configure Oracle Content Management with Your Friendly Management Domain	7-13
Edit Your Oracle Content Management Instance	7-14
Monitor Your Instances	7-16
Monitor Billing and Usage	7-17
Report Issues	7-17

A Troubleshoot

I can't access the administration pages	A-1
No one can add files to their accounts	A-2
I need to change the storage quota for a user	A-2
I need to reassign someone's files	A-3

I created a user but can't find the user in the system	A-3
I granted roles to more users than were purchased	A-3
Users can't connect to the service using the sync client	A-4
I need to find out who deleted a file or folder	A-4

B Supported Software, Devices, Languages, and File Formats

Supported Web Browsers	B-1
Supported Software	B-1
Supported Mobile Devices	B-2
Supported Languages	B-2
Supported File Formats	B-3

C Service Limits, Quotas, Policies, and Events

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

D Migrate Oracle Content Management

Migrate an Oracle Content Management Instance	D-2
Prepare for Migration	D-3
Submit a Migration Request	D-3
The Migration Process	D-4
Finalize the Migration	D-4
Communicate the Change to Users	D-5
Migrate an Oracle Content Management Instance from Legacy Cloud Infrastructure	D-5
User Mapping	D-6
Prepare for Migration	D-7
Submit a Migration Service Request	D-7
The Migration Process	D-7
Finalize the Migration	D-8
Migrate Your Sites That Include Assets	D-9
Install the Oracle Content Management Toolkit	D-10
Register the Target Server	D-10

Migrate Your Sites	D-10
Post-Migration Steps	D-11
Make Your Migrated Site Multilingual Site (MLS) Compliant	D-11
Migrate Your Assets	D-15
Register the Source and Target Servers	D-15
Migrate a Collection of Assets	D-16
Communicate the Change to Users	D-17
Migrate Files to Oracle Content Management Assets	D-17
Migration Process	D-18
Migrate Files from Oracle WebCenter Content 12c to Oracle Content Management Assets	D-20
Migrate Files from Oracle WebCenter Content 11g to Oracle Content Management Assets	D-21
Migrate Files from an External Content Management System	D-21
Migrate Files from Oracle WebCenter Content Using Archiver and Content Capture	D-22
Migrate Files from a Documents Folder to an Asset Repository	D-23
File Migration FAQ	D-23
Map Your Source Content to Oracle Content Management Asset Features	D-29
Upload Files to an Object Storage Bucket	D-34
Export Source File Metadata to CSV	D-34
Submit a File Migration Service Request	D-39

E Manage Oracle Content Management in Legacy Environments

Manage Legacy Instances of Oracle Content Management Built on OCI Gen 1	E-2
Understand Active Users per Hour	E-3
Understand Visitor Sessions	E-5
Manage Legacy Instances of Oracle Content Management on OCI Classic	E-8
Understand Active Users per Hour	E-9
Understand Visitor Sessions	E-11
Deploy and Manage Legacy Instances of Oracle Content Management for Government on OCI Classic	E-14
Create an Instance of Oracle Content Management for Government	E-15
Manage Oracle Content Management for Government	E-19
Understand Active Users per Hour	E-19
Understand Visitor Sessions	E-21
Deploy and Manage Legacy Instances of Oracle Content Management for SaaS on OCI Classic	E-24
Create an Instance of Oracle Content Management for SaaS	E-25
Manage and Monitor Oracle Content Management for SaaS	E-27
View Billing Metrics	E-29
Understand Visitor Sessions	E-29

Deploy and Manage Oracle Content Management with a Non-Metered Subscription	E-32
Create an Oracle Content Management Instance with a Non-Metered Subscription	E-33
Set Up Users and Groups (Traditional Cloud Account)	E-34
Application Roles in an Oracle Content Management Instance with a Non-Metered Subscription	E-34
Typical Organization Roles	E-39
Create Groups with a Traditional Cloud Account	E-42
Assign Roles to Groups with a Traditional Cloud Account	E-42
Add Users with a Traditional Cloud Account	E-43
Assign Users to Groups with a Traditional Cloud Account	E-43
Manage Users, Groups, and Access with a Traditional Cloud Account	E-44
Enable Single Sign-On (SSO)	E-44
Manage Users with a Traditional Cloud Account	E-45
Manage Groups (Traditional Cloud Account)	E-45
Set the Default Role for New Folder Members	E-46
Synchronize User Profile Data	E-47
Display Conversation Membership Messages for Users	E-47
Override Storage Quota for a User	E-47
Transfer File Ownership	E-48
Revoke Access to Linked Devices	E-48
Manage and Monitor Oracle Content Management with a Non-Metered Subscription	E-49
View Billing Metrics	E-51
View Business Metrics	E-51
Understand Visitor Sessions	E-54
Migrate Oracle Documents Cloud to Oracle Content Management	E-56
Application Roles in Oracle Documents Cloud	E-58
Troubleshoot Oracle Documents Cloud	E-62
I need to downsize my instance	E-62
Users can't sign in after migration (storage overage)	E-63

Preface

Administering Oracle Content Management describes how to manage the service, including how to add and provision users, monitor the service, and set default behavior for the service. It provides a broad overview of those tasks.

Audience

Administering Oracle Content Management is intended for Oracle Cloud administrators who will set up and configure the service.

Documentation Accessibility

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

Access to Oracle Support

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

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*
- *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*
- *Capturing Content with 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
boldface	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

Get Started

This part provides conceptual information about Oracle Content Management and using it to administer your instance.

- [Overview of Oracle Content Management](#)
- [Starter vs. Premium Edition](#)
- [Your Role as Administrator](#)
- [Administrative Interfaces](#)
- [Administrative Tasks](#)
- [Roles](#)
- [Security](#)



Video

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-party 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.

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	 Only 5 users No limit for SaaS entitlement	 Unlimited
Repositories	 Only one asset repository; no business repositories	 Unlimited business and asset repositories
Digital assets, business documents, and content items (structured content)	 <ul style="list-style-type: none"> • Only 5,000 assets for free (25,000 if bundled with a SaaS service) • Includes out-of-the-box asset types for images, videos, and files • Only 5 custom asset types • No custom renditions (supports automated renditions) 	 Unlimited
Taxonomies	 Only two taxonomies	 Unlimited
Publishing channels	 Only one publishing channel, not including site channel	 Unlimited
Workflows	 Only basic out-of-the-box approve/reject workflow	 Unlimited 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	 Only one site; no site governance	 Unlimited; full access
Experience orchestrations	 Only one experience	 Unlimited
Recommendations	 Only one recommendation	 Unlimited


Feature	Starter Edition	Premium Edition
Developer interface		
Analytics	 Only basic usage metrics (dashboard)	
Documents		
Conversations	 No standalone conversations	 Full access
Integrations	 Only webhooks, proxy service, and APIs	 Full access
Security in repository	 No taxonomy-based granular security	
Smart tags and search		
Smart authoring		
Video Plus		
Content Capture (document capture and processing)	 Only one procedure; no XML	 Unlimited; full access
Content apps		
CDN		
Vanity URLs (vanity domains)	 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	 Doesn't show Recent Items or Quick Links	
Included OCM outbound data	<ul style="list-style-type: none"> OCM Universal Credit Starter Edition (B93411) includes 10GB of OCM outbound data per instance per month OCM SaaS Starter Edition (B93582) includes 100GB OCM outbound data per 5,000-asset pack 	<ul style="list-style-type: none"> OCM Universal Credit Premium Edition (B91210) and OCM for SaaS Premium Edition (B91221) include 10TB of OCM outbound data per instance per month
Included object storage	<ul style="list-style-type: none"> OCM Universal Credit Starter Edition (B93411) uses OCI Object Storage which includes 10GB free object storage per cloud account OCM SaaS Starter Edition (B93582) includes 100GB of OCM for SaaS Object Storage per 5,000-asset pack 	<ul style="list-style-type: none"> OCM Universal Credit Premium Edition (B91210) uses OCI Object Storage which includes 10GB free object storage per cloud account OCM for SaaS Premium Edition (B91221) includes 5TB of OCM Object Storage per 5,000-asset pack


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.

Your Role as Administrator

There are different kinds of administrators and different interfaces in which to perform administrative tasks. As an administrator, you should understand these roles and interfaces, as well as some important terminology, and the tasks you're responsible for.

Before you start, you should understand the following terms, which are used throughout this documentation and other Oracle Cloud documents.

- **Account:** An account corresponds to an Oracle customer who's an individual, an organization, or a company. An account can have more than one service. Each account has one or more identity domains.
- **Service:** A software offering in Oracle Cloud that's managed by a **service administrator**. A service is associated with a particular data center, identity domain, and account.
- **Identity domain:** An identity domain controls the authorization of users. Multiple services can be associated with a single identity domain and share user definitions. Users in an identity domain can have different levels of access to the different services in the domain.
- **Data centers:** A facility housing computer systems. Oracle has data centers in several geographic regions. An identity domain and its services belong to a specific data center.

As an administrator, you need to be familiar with the roles and administrative interfaces that are involved with performing your administrative tasks:

- [Roles](#)
- [Administrative Interfaces](#)
- [Administrative Tasks](#)
- [Security](#)

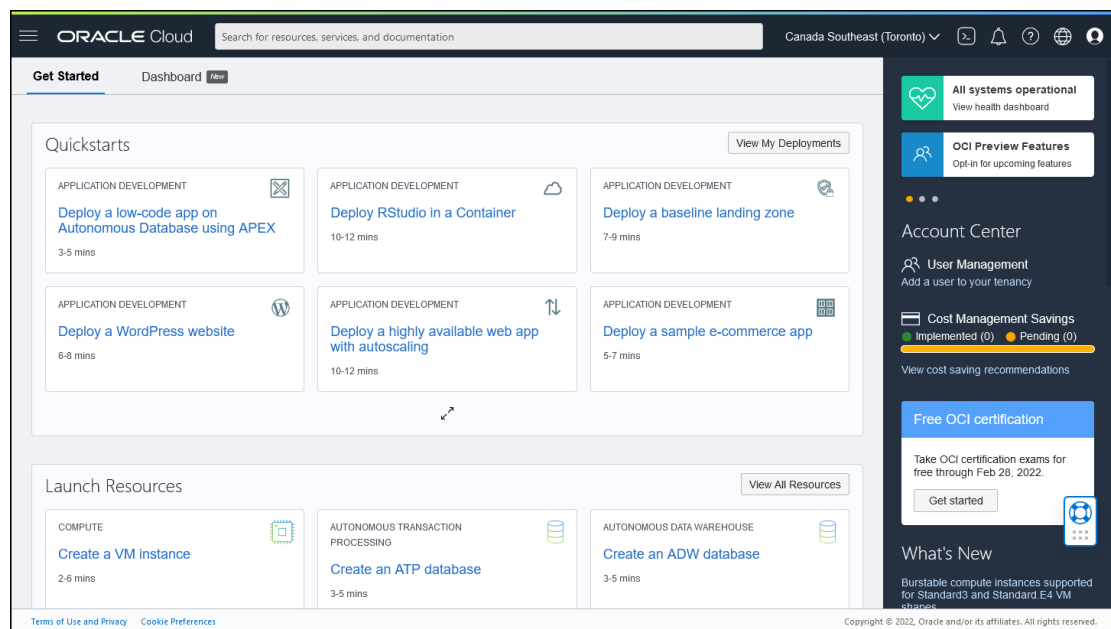
Administrative Interfaces

There are several different interfaces used to manage your services. Depending on the type and date of your subscription, you'll use different interfaces to perform tasks.

- [Oracle Cloud Console](#)—Used to create, manage, and view your Oracle Cloud resources. If [your region uses Identity and Access Management \(IAM\) identity domains](#), this is also where you manage users and groups.

- [Identity Cloud Service \(IDCS\) Console](#)—If your region does not use IAM identity domains, you manage users and groups in IDCS.
- [Oracle Cloud Classic Console](#)—Depending on the type and date of your subscription, you might instead use Oracle Cloud Classic Console to manage your Oracle Cloud services as well as to manage users and groups.
- [Administration: System Interface](#)—Used to enable notifications, manage defaults such as user quotas and time zone settings, add custom branding, and manage custom applications.
- [Administration: Integration Interface](#)—Used to enable integration with other applications, such as third-party content repositories, third-party language service providers (LSP), Oracle Process Cloud Service, or Oracle Visual Builder.
- [Administration: Content Interface](#)—Used to manage asset repositories and all the pieces of the content management structure.
- [Administration: Capture Interface](#)—Used to manage Content Capture to define workflows to scan physical documents and import electronic documents in large batches, process and index them, and upload them to Oracle Content Management for storage and/or further processing.
- [Administration: Applications Interface](#)—Used to manage content apps to develop and deploy web applications that run in the context of Oracle Content Management (using it as the content management system).

Oracle Cloud Console



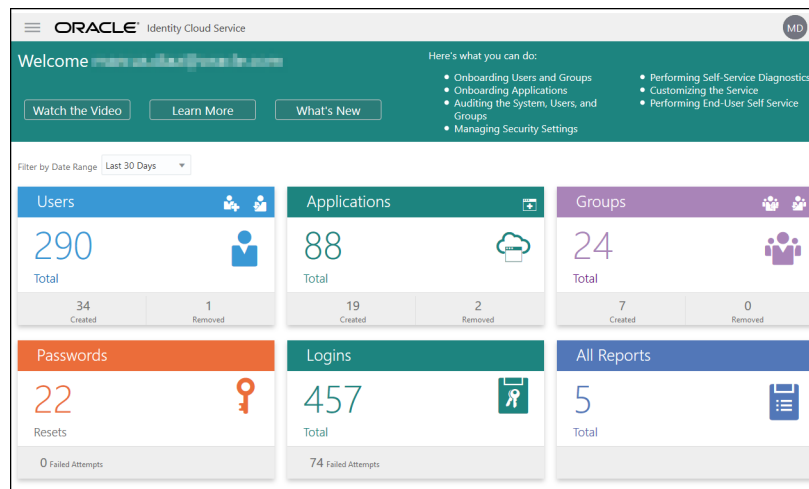
If you have an Oracle Content Management instance running on Oracle Cloud Infrastructure (OCI), you can use the Oracle Cloud Console to create, manage, and view your Oracle Cloud resources, including users and groups.

 **Note:**

If your account hasn't been migrated to IAM yet, you use IDCS to manage users and groups (described below).


To access 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.

Identity Cloud Service (IDCS) Console

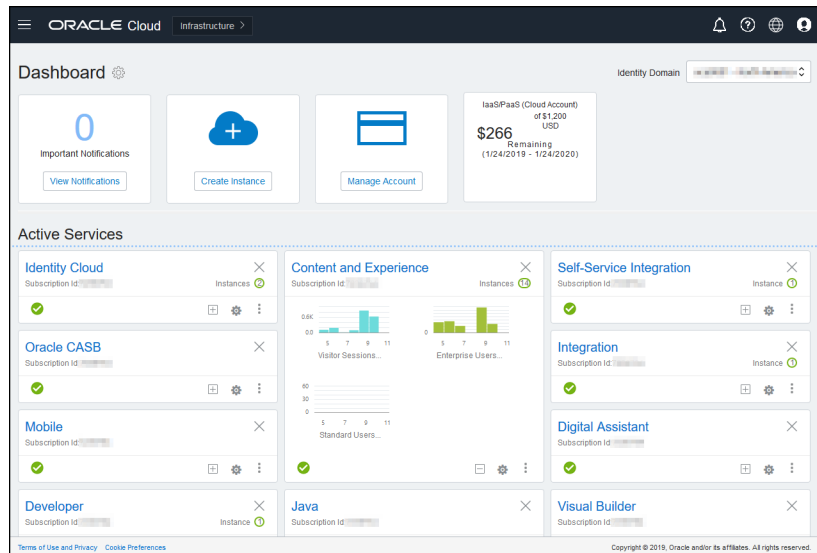


If your account hasn't been migrated to Oracle Cloud Infrastructure Identity and Access Management (IAM) yet, you use Identity Cloud Service (IDCS) to manage users and groups.

To access Identity Cloud Service (IDCS):

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 **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.

Oracle Cloud Classic Console



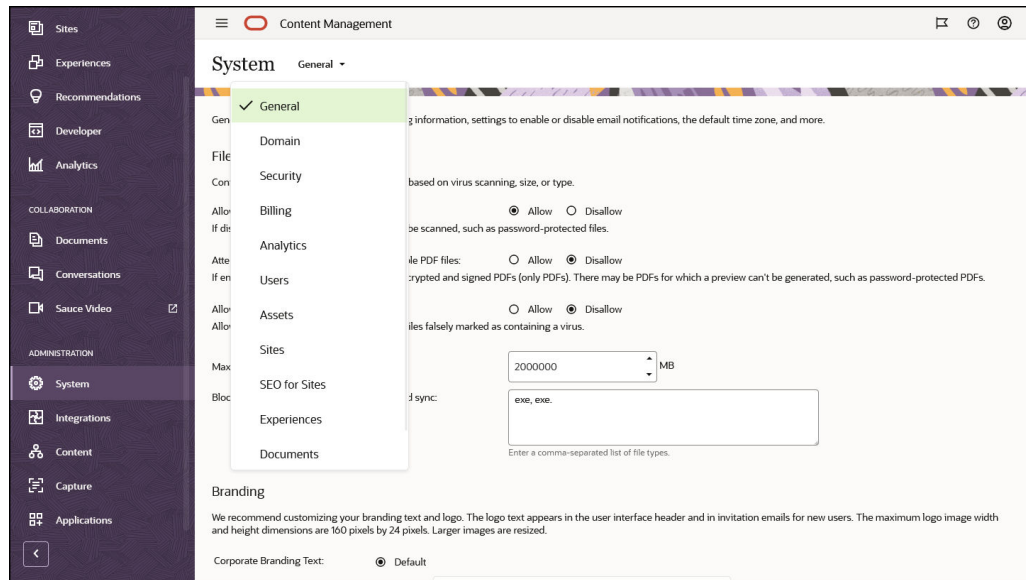
Depending on the type and date of your subscription, you might use Oracle Cloud Classic Console to manage your Oracle Cloud services as well as to manage users and groups. You're automatically brought to the appropriate console for your subscription when you sign in to Oracle Cloud.

The dashboard shows you your existing services and their statuses, enables you create new service instances, and displays your billing and service usage.

To access the Oracle Cloud Classic Console:

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. Click your user avatar on the top right, then click **Service User Console**.
3. Click **Infrastructure Classic Console**.

Oracle Content Management Administration System Interface



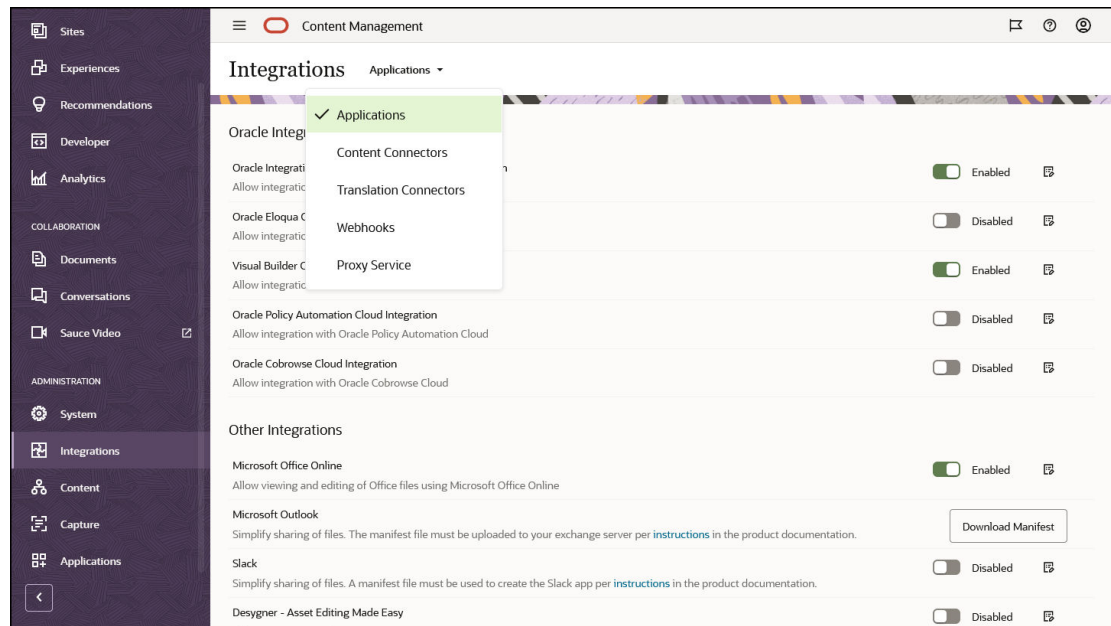
The Oracle Content Management Administration System interface is where you enable notifications, manage defaults such as user quotas and time zone settings, add custom branding, and manage custom applications.

To access the Oracle Content Management Administration System interface:

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** menu, select a page:
 - **General:** Restrict file types and sizes; customize branding; enable or disable notifications; and set default time zone, language, and date/time format.
 - **Domain:** Specify a friendly management domain to make it easier for your users to access your Oracle Content Management web client, the desktop app, the mobile apps, and any sites created with Oracle Content Management.
 - **Security:** Set CORS origins, and enable the display of embedded content from Oracle Content Management within other domains.
 - **Billing:** Specify the limits at which you want to be notified for billing metrics. These settings apply only to Oracle Content Management running on Oracle Cloud Infrastructure (OCI).
 - **Analytics:** Control whether Oracle Content Management collects asset consumption information and anonymous product usage information.
 - **Users:** Manage users; set the default role for new folder members; synchronize user data; set whether to show conversation membership messages by default for a user; override user storage quotas; and transfer ownership of files from deprovisioned users.
 - **Assets:** Manage how many renditions can be saved for each asset and maximum video file size.
 - **Sites:** Enable sites access control options, and install the default site templates.
 - **SEO for Sites:** Enable prerendering for sites and configure additional user agents.

- **Experiences:** Enable experiences so that you can automatically update experiences managed outside of Oracle Content Management based on content changes or published status.
- **Documents:** Set default user storage quota and manage storage space and set default link behavior.
- **Metadata:** Manage metadata (custom properties) so that users can quickly categorize files and folders with additional descriptions.

Oracle Content Management Administration Integrations Interface



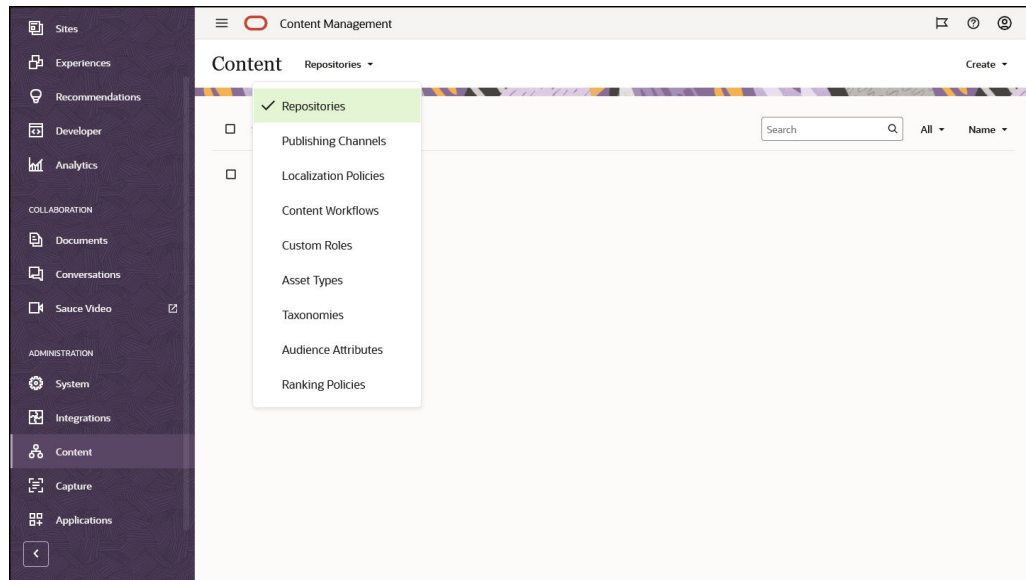
You can enable integration with other applications through the **Administration Integrations** interface.

To access the Oracle Content Management Administration Integrations interface:

1. After you sign in to the Oracle Content Management web application as an administrator, click **Integrations** in the Administration area of the navigation menu.
2. In the **Integrations** menu, you can select **Applications**, **Content Connectors**, **Translation Connectors**, **Webhooks**, or **Proxy Service**.

Depending on your environment, you may be able to integrate with Oracle Process Cloud Service, Oracle Eloqua Cloud Service, Oracle Visual Builder, Oracle Intelligent Advisor, or Oracle Cobrowse Cloud Service. These tasks are described in *Integrating and Extending Oracle Content Management*.

Oracle Content Management Administration Content Interface

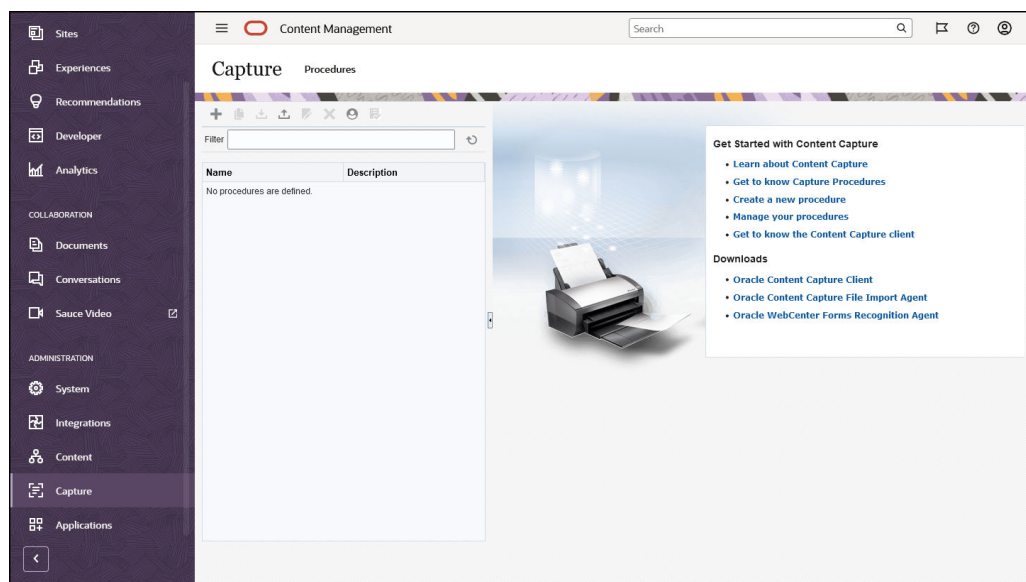


Repository and content administrators can manage asset repositories and all the pieces of the content management structure through the **Administration Content** interface. These tasks are described in *Managing Assets with Oracle Content Management*.

To access the Oracle Content Management Administration Content interface:

1. After you sign in to the Oracle Content Management web application as an administrator, click **Content** in the Administration area of the navigation menu.
2. In the **Content** menu, you can select **Repositories**, **Publishing Channels**, **Localization Policies**, **Content Workflows**, **Custom Roles**, **Asset Types**, **Taxonomies**, **Audience Attributes**, or **Ranking Policies**.

Oracle Content Management Administration Capture Interface

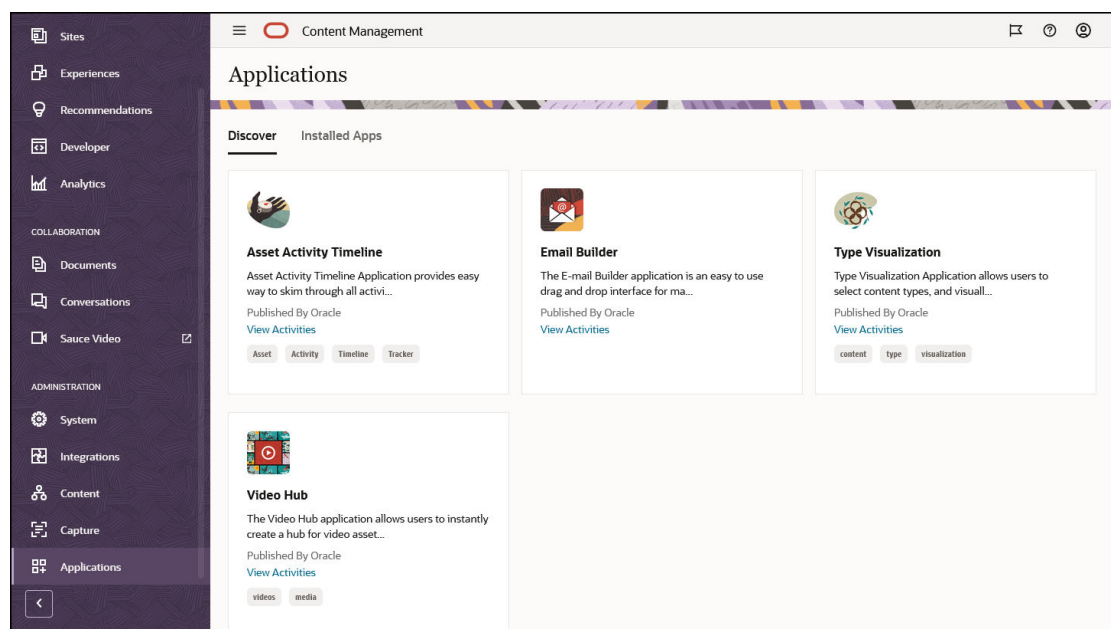


Content Capture administrators can manage procedures to define workflows to scan physical documents and import electronic documents in large batches, process and index them, and upload them to Oracle Content Management for storage and/or further processing. You manage them through the **Administration Capture** interface. These tasks are described in *Capturing Content with Oracle Content Management*.

To access the Oracle Content Management Administration Capture interface:

1. After you sign in to the Oracle Content Management web application as an administrator, click **Capture** in the Administration area of the navigation menu.
2. Use the left side of the page for procedures *management*, to create, edit, delete, import, and export procedures. Use the right side of the page for procedures *configuration*, to customize each procedure for specific content capture environments.

Oracle Content Management Administration Applications Interface



Service administrators with the enterprise user role can manage content apps to discover and deploy web applications that run in the context of Oracle Content Management (using it as the content management system). You manage them through the **Administration Applications** interface. These tasks are described in [Use Oracle Content Management Applications](#).

To access the Oracle Content Management Administration Applications interface:

1. After you sign in to the Oracle Content Management web application as an administrator, click **Applications** in the Administration area of the navigation menu.
2. On the **Applications** page, you can select from the following tabs:
 - **Discover**—This section shows all available apps, both pre-built apps and custom apps. Open any of the app tiles to see app details, install the app, and view app activity.
 - **Installed Apps**—This section shows all apps that are currently installed on your Oracle Content Management instance. Go to this section to run and configure app instances and view app activity.

Administrative Tasks

As an administrator, you'll perform tasks to get Oracle Content Management up and running, as well as tasks to manage it and keep it running smoothly.

 **Note:**

- This topic assumes you've been assigned the necessary role to add users and configure the service. See your Cloud account administrator if you need to have your role changed.
- For information on how to get to the interfaces listed in the table, see [Administrative Interfaces](#).
- 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. If your region has been updated, follow the steps marked **IAM**. If your region hasn't been updated, follow the steps marked **IDCS**.

The following table lists administrative tasks with links to the associated documentation, the interface in which you perform them, and the role you need to complete each task.

Task	Where to Perform Task	Role Needed
Enable single sign-on (SSO)	<ul style="list-style-type: none"> • IAM: Oracle Cloud Console. • IDCS: IDCS Console 	Cloud account administrator
Manage users and groups	<ul style="list-style-type: none"> • IAM: Oracle Cloud Console • IDCS: IDCS Console 	Cloud account administrator
Configure general settings such as file restrictions, custom branding, email notifications, and locale settings	Oracle Content Management Administration — General	Service administrator and standard user/enterprise user
Configure domain settings to specify a friendly management domain to make it easier for your users to access your Oracle Content Management web client, the desktop app, the mobile apps, and any sites created with Oracle Content Management	Oracle Content Management Administration — Domain	Service administrator and standard user/enterprise user

Task	Where to Perform Task	Role Needed
Configure security settings such as cross-origin resource sharing (CORS) and embedding Oracle Content Management in other domains	Oracle Content Management Administration — Security	Service administrator and standard user/enterprise user
Configure analytics settings such as enabling consumption or usage analytics	Oracle Content Management Administration — Analytics	Service administrator and standard user/enterprise user
Configure billing settings to be notified when billing metrics reach specified limits	Oracle Content Management Administration — Billing These settings apply only to Oracle Content Management running on Oracle Cloud Infrastructure (OCI).	Service administrator and standard user/enterprise user
Configure user settings such as enabling external users, managing storage quota, and transferring file ownership	Oracle Content Management Administration — Users	Service administrator and standard user/enterprise user
Configure asset settings for renditions, caching, and video token expiration	Oracle Content Management Administration — Assets	Service administrator and standard user/enterprise user
Configure sites settings and install site templates	Oracle Content Management Administration — Sites	Service administrator and standard user/enterprise user
Enable prerendering of sites and configure additional user agents	Oracle Content Management Administration — SEO for Sites	Service administrator and standard user/enterprise user
Configure experience settings to automatically update experiences managed outside of Oracle Content Management based on content changes or published status	Oracle Content Management Administration — Experiences	Service administrator and standard user/enterprise user
Configure document settings such as restricting file and folder deletion, managing storage, and setting default link behavior	Oracle Content Management Administration — Documents	Service administrator and standard user/enterprise user
Manage metadata (custom properties) so that users can quickly categorize files and folders with additional descriptions	Oracle Content Management Administration — Metadata	Service administrator and standard user/enterprise user
Provide sign-in and get-started information to users	Emails are automatically generated for each user you add to the system	N/A
Deploy the desktop app to users' machines	Use your command line tool to push the desktop app to users' machines	N/A
Analyze service usage	Oracle Content Management Analytics	Service administrator and standard user/enterprise user

Task	Where to Perform Task	Role Needed
Manage vanity domains	Various interfaces: <ul style="list-style-type: none"> Your CDN Your DNS Oracle Content Management Administration — Domain Oracle Content Management Administration — Sites Your site created in Oracle Content Management 	Various roles: <ul style="list-style-type: none"> For CDN: your network administrator For DNS: your network administrator For Oracle Content Management administrative tasks: service administrator and standard user/enterprise user For Oracle Content Management sites: site administrator and standard user/enterprise user
Monitor your service instances	Oracle Cloud Console	Cloud account administrator
Monitor your billing and usage	Oracle Cloud Console	Cloud account administrator
Report any issues you find	Oracle Cloud Console	Cloud account administrator

For information on integration tasks (those found in Administration — Integrations), see *Integrating and Extending Oracle Content Management*.

For information on content administrator tasks (those found in Administration — Assets), see Setting Up Asset Repositories in *Building Sites with Oracle Content Management*.

For information on Content Capture administrator tasks (those found in Administration — Capture), see *Capturing Content with Oracle Content Management*.

For information on content application administrator tasks (those found in Administration — Applications), see [Use Oracle Content Management Applications](#).

Roles

There are different types of roles in Oracle Content Management. Understanding how they work together is essential to giving users the access they need to perform their duties and access appropriate content.

- [Typical Organization Roles](#) — A person's role within your organization determines what tasks they need to perform and how they use features.
- [Application Roles](#) — Application roles control what features a user sees in Oracle Content Management.
- [Task and Feature Comparison by Application Role](#) — Depending on the application roles assigned to a user, the user can perform different tasks and access different features. For example, visitors, standard users, and enterprise users can access files and folders, but only enterprise users can work with digital assets.
- [Resource Roles \(Permissions\)](#) — What users can see and do with a resource, such as a document, content item, site, or template, depends on the role they're assigned when the resource is shared with them.

Typical Organization Roles

When you create users, you'll give them the application roles needed to perform their tasks in Oracle Content Management. These users will typically fall into one of the following organization roles (or user types) and will require the listed application roles.

[Use Oracle Cloud Infrastructure \(OCI\) to create groups](#) for your organization roles and assign the listed application roles to those groups. Then you can add users to those groups to automatically assign them the appropriate application roles.

Organization Role	Application Roles Needed
<p>Anonymous User Anonymous users don't work for your company and don't exist in your Oracle Cloud identity domain or your directory. They are consumers engaging with your company through your public website, mobile site, or other digital experiences to learn about your company offerings, download documents, or make a purchase.</p> <p>They can visit <i>public</i> sites, but can't access <i>secure</i> sites. They can also access content via public links and interact based on the role assigned to the public link.</p> <p>Anonymous users can't access any Oracle Content Management interfaces (web client, desktop client, mobile apps).</p>	<ul style="list-style-type: none"> Anonymous users don't need a user account or any application roles.
<p>Visitor Visitors probably don't work for your company, but they exist in your Oracle Cloud identity domain or your directory. Like anonymous users, they are consumers engaging with your website, mobile site, or other digital experiences to learn about your company offerings, download documents, or make a purchase, but they can also interact with specified secure sites and sign in to services that your company provides.</p> <p>They can visit public sites, and, unlike anonymous users, they can visit any secure sites to which they've been given access. They can also access content via public links and interact based on the role assigned to the public link.</p> <p>Visitors can share and collaborate on files exposed via components on a site they have access to, but they don't have access to any Oracle Content Management interfaces (web client, desktop client, mobile apps), and you can't share folders or conversations with them.</p>	<ul style="list-style-type: none"> Sites Visitor

Organization Role	Application Roles Needed
<p>External User External users may be people outside of your organization that can collaborate on objects to which they're given access, but they can't be assigned the manager role. This safely limits their ability to create and remove content, similar to how visitors can sign in and use specified secure sites. This allows you to work with outside contributors such as translators and partners.</p> <p>External users have limited access to the Oracle Content Management web client, but they can't use the desktop client or mobile apps.</p>	<ul style="list-style-type: none"> Standard External User
<p>Employee Employees obviously work for your company and exist in your Oracle Cloud identity domain or your directory. They share documents with colleagues and view documents shared with them. They collaborate through shared conversations. They can create team sites or partner sites from prebuilt standard templates.</p> <p>Employees can visit public and secure sites to which they have access. They can collaborate on all content types as members and via public links. They can access any Oracle Content Management interfaces (web client, desktop client, mobile apps).</p>	<ul style="list-style-type: none"> Standard User
<p>Content Contributor Content contributors work for your company and exist in your Oracle Cloud identity domain or your directory. They write articles that will be published to your sites, possibly about one of your products or a certain area of your business. These articles (in the form of content items) include images, videos, and other digital assets that make it easy for your customers to understand product features and specs. Content contributors also share and collaborate like an employee. A content contributor is a user with a contributor role within at least one repository.</p>	<ul style="list-style-type: none"> Enterprise User
<p>Content Administrator/Content Translator Content administrators are responsible for the quality of content related to a product. They review submitted content, ensuring it's valid and accurate, and then publish this content. They can also create new content types and taxonomies as needed for your sites.</p> <p>Content translators also administer content. They submit content to the translation vendor, proofread returned content, and sometimes translate articles manually.</p> <p>Content administrators also share and collaborate like an employee.</p>	<ul style="list-style-type: none"> Content Administrator Enterprise User

Organization Role	Application Roles Needed
<p>Repository Administrator Repository administrators organize content authoring and publishing, which requires setting up asset repositories, managing content editors' roles and permissions, viewing content metrics, and configuring content workflows, publishing channels, and localization policies that your company uses to deliver experiences. They interact with back-end developers to define data or content integration requirements. They also share and collaborate like an employee. A repository administrator is a user with a Manager role within at least one repository.</p>	<ul style="list-style-type: none"> • Repository Administrator • Enterprise User
<p>Site Administrator You can limit site, template, and component creation to only site administrators. Site administrators create and manage <i>standard</i> and <i>enterprise</i> sites. They might ask the system administrator to install the default site templates; ask a developer to create custom components, themes, or templates for new sites; or ask a content architect to create new content types for content items that will be used on sites. They also share and collaborate like an employee.</p>	<ul style="list-style-type: none"> • Site Administrator • Enterprise User
<p>Developer Developers develop and configure custom components, corporate themes, and <i>standard</i> templates that colleagues can use for creating team sites or partner sites. They configure integrations between Oracle Content Management and other services. They also share and collaborate like an employee. A developer with the Enterprise User role can also create <i>enterprise</i> templates.</p>	<ul style="list-style-type: none"> • Developer • Enterprise User
<p>Content Capture Administrator Content Capture administrators design and customize content capture workflows, or <i>procedures</i>, which are used to process physical and electronic documents in bulk for various business scenarios. Procedure managers are typically assigned both the manager and application roles, so they can configure procedures and test them in the client.</p>	<ul style="list-style-type: none"> • Capture Administrator • Capture Client User • Standard User
<p>Content Capture Client User Content Capture client users scan or import documents into Oracle Content Management.</p>	<ul style="list-style-type: none"> • Capture Client User
<p>Content Applications Administrator Content applications administrators manage content apps to discover and deploy web applications that run in the context of Oracle Content Management (using it as the content management system).</p>	<ul style="list-style-type: none"> • Service Administrator • Enterprise User <p>Depending on the type of app you're working with, you may also need to have the content administrator and/or site administrator roles; for example, to create repositories, publishing channels, and such.</p>

Organization Role	Application Roles Needed
<p>Service Administrator Service administrators configure and manage your Oracle Content Management service. They can integrate Oracle Content Management with other business services and access operational analytics to monitor key usage metrics for the service.</p>	<ul style="list-style-type: none"> • Service Administrator • Standard or Enterprise User

There are additional users involved in running Oracle Content Management, such as the Integration User, but these are internal users, not actual people. You'll also have a cloud account administrator, but this user is automatically created when you sign up for Oracle Cloud. See [Application Roles](#).

Application Roles

Several predefined application roles define what users can do. Some functionality is available only to users with specific application roles.

People can hold multiple application roles as needed. For example, you might want to designate one person as both a *cloud account administrator* and a *service administrator*. These application roles are assigned by the *identity domain administrator*. See [Assign Roles to Groups](#) and [Assign Users to Groups](#).

Visitors can view certain sites, use public links, and view Oracle Content Management content embedded in apps or websites.

Any users that need to actually *use* Oracle Content Management must be assigned the *standard user* or *enterprise user* role in addition to any other roles they're assigned.



Note:

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. If your region has been updated, follow the steps marked **IAM**. If your region hasn't been updated, follow the steps marked **IDCS**.

Oracle Content Management Roles

The following table describes the application roles involved with Oracle Content Management instances with a Universal Credits subscription, a Government subscription, or a SaaS subscription. For information on how to access the interfaces listed in the table, see [Administrative Interfaces](#).

Application Role (application role name in bold)	Access and Actions	Notes
Cloud account administrator	<p>Cloud account administrators use the Oracle Cloud Console to perform the following actions:</p> <ul style="list-style-type: none">• Monitor and manage services for one or more Cloud accounts.• Upgrade or terminate subscriptions.• Create and manage users and groups.• Provide access to services by assigning roles.• IAM: Cloud account administrators manage users, groups, and roles in the Oracle Cloud Console.• IDCS: Cloud account administrators manage users, groups, and roles in the IDCS Console.	<p>Cloud account administrators are set up when the account is created. They use their Oracle Cloud account to sign in to Oracle Cloud and access the Oracle Cloud Console.</p> <p>If you need account administrator access and don't have it, contact your primary account administrator.</p> <p>If you want cloud account administrators to use Oracle Content Management and modify the service configuration, they must also be assigned the <i>standard user</i> or <i>enterprise user</i> role.</p>

Application Role (application role name in bold)	Access and Actions	Notes
Service administrator (CECServiceAdministrator)	<p data-bbox="646 327 971 411">From the Oracle Content Management Administration: System interface:</p> <ul data-bbox="646 422 1040 1915" style="list-style-type: none"> <li data-bbox="646 422 1040 562">• General: Restrict file types and sizes; customize branding; enable or disable notifications; and set default time zone, language, and date/time format. <li data-bbox="646 573 1040 793">• Domain: Specify a friendly management domain to make it easier for your users to access your Oracle Content Management web client, the desktop app, the mobile apps, and any sites created with Oracle Content Management. <li data-bbox="646 804 1040 940">• Security: Set CORS origins, and enable the display of embedded content from Oracle Content Management within other domains. <li data-bbox="646 951 1040 1119">• Billing: Specify the limits at which you want to be notified for billing metrics. These settings apply only to Oracle Content Management running on Oracle Cloud Infrastructure (OCI). <li data-bbox="646 1129 1040 1266">• Analytics: Control whether Oracle Content Management collects asset consumption information and anonymous product usage information. <li data-bbox="646 1276 1040 1528">• Users: Manage users; set the default role for new folder members; synchronize user data; set whether to show conversation membership messages by default for a user; override user storage quotas; and transfer ownership of files from deprovisioned users. <li data-bbox="646 1539 1040 1644">• Assets: Manage how many renditions can be saved for each asset and maximum video file size. <li data-bbox="646 1654 1040 1738">• Sites: Enable sites access control options, and install the default site templates. <li data-bbox="646 1749 1040 1833">• SEO for Sites: Enable prerendering for sites and configure additional user agents. <li data-bbox="646 1843 1040 1915">• Experiences: Enable experiences so that you can automatically update 	Service administrators must also be assigned the <i>standard user</i> or <i>enterprise user</i> role to be able to use Oracle Content Management.

Application Role (application role name in bold)	Access and Actions	Notes
	<p>experiences managed outside of Oracle Content Management based on content changes or published status.</p> <ul style="list-style-type: none"> • Documents: Set default user storage quota and manage storage space and set default link behavior. • Metadata: Manage metadata (custom properties) so that users can quickly categorize files and folders with additional descriptions. <p>Note: For Custom Properties, you must also have the <i>enterprise user</i> role.</p> <p>From Oracle Content Management Administration: Integrations interface, configure integrations with Oracle Process Cloud Service, Oracle Eloqua Cloud Service, Oracle Visual Builder, Oracle Intelligent Advisor, Oracle Cobrowse Cloud Service, and custom applications.</p> <p>From Oracle Content Management Administration: Applications interface, manage content apps to discover and deploy web applications that run in the context of Oracle Content Management (using it as the content management system).</p> <p>From Oracle Content Management Analytics interface:</p> <ul style="list-style-type: none"> • View service usage statistics, content metrics, and reports to help you analyze system needs or issues. 	
Repository administrator (CECRepositoryAdmin istrator)	<p>From the Oracle Content Management Administration: Content page:</p> <ul style="list-style-type: none"> • Create asset repositories. • Create publishing channels. • Create localization policies. • Create content workflows and workflow roles. • Create editorial roles. <p>From the Oracle Content Management Analytics interface:</p> <ul style="list-style-type: none"> • View assets and content metrics to help you analyze system needs or issues. 	Repository administrators must also be assigned the <i>enterprise user</i> role to be able to use Oracle Content Management and access assets. A repository administrator is a user with a Manager role within at least one repository.

Application Role (application role name in bold)	Access and Actions	Notes
Content administrator (CECContentAdministrator)	<p>From the Oracle Content Management Administration: Content page:</p> <ul style="list-style-type: none"> • Create asset types and publish items. • Create and publish taxonomies. • Create audience attributes. • Create ranking policies. <p>From the Oracle Content Management Developer page as long as these features haven't been limited to <i>site administrators</i>:</p> <ul style="list-style-type: none"> • Create components. • Create templates. • Create themes. • Configure the embeddable user interface. 	Content administrators must also be assigned the <i>enterprise user</i> role to be able to use Oracle Content Management and access assets.
Capture administrator (CECCaptureAdministrator)	<p>From the Oracle Content Management Administration: Capture page.</p> <ul style="list-style-type: none"> • Design and customize content capture workflows, or <i>procedures</i>, which are used to process physical and electronic documents in bulk for various business scenarios. <p>From the Oracle Content Management Analytics interface:</p> <ul style="list-style-type: none"> • Capture Administrator users can access the Capture page and the Capture Activities report. 	Procedure managers are typically assigned both the <i>Capture administrator</i> and <i>Capture client user</i> roles, so they can configure procedures and test them in the client.
Capture client user (CECCaptureClient)	<p>From the Oracle Content Capture Client:</p> <ul style="list-style-type: none"> • Scan or import documents into Oracle Content Management. 	
Site administrator (CECSitesAdministrator)	<p>From the Oracle Content Management Sites page:</p> <ul style="list-style-type: none"> • Create sites. <p>From the Oracle Content Management Developer page:</p> <ul style="list-style-type: none"> • Create components. • Create templates. • Create themes. • Configure the embeddable user interface. 	When using site governance, site administrators make approved templates available to users for creating sites, approve site requests, and manage sites. This role also applies if your service administrator configured Oracle Content Management to allow only site administrators to create sites, templates, or components. Site administrators must also be assigned the <i>standard user</i> or <i>enterprise user</i> role to be able to use Oracle Content Management.

Application Role (application role name in bold)	Access and Actions	Notes
Developer (CECDeveloperUser)	<p>From the Oracle Content Management Sites page as long as these features haven't been limited to <i>site administrators</i>:</p> <ul style="list-style-type: none">• Create, edit, and publish sites. <p>From the Oracle Content Management Experiences page:</p> <ul style="list-style-type: none">• Create and manage experience objects. <p>From the Oracle Content Management Developer page as long as these features haven't been limited to <i>site administrators</i>:</p> <ul style="list-style-type: none">• Create components.• Create templates.• Create themes.• Configure the embeddable user interface. <p>From the Oracle Content Management Administration: Integrations interface:</p> <ul style="list-style-type: none">• Configure application settings such as those described in <i>Integrating and Extending Oracle Content Management</i>.	<p>Developers must also be assigned the <i>standard user</i> or <i>enterprise user</i> role to be able to use Oracle Content Management. Developers with the <i>standard user</i> role can create components, themes, and standard templates. Developers with the <i>enterprise user</i> role can also create layouts and save a site as a standard or enterprise template.</p>

Application Role (application role name in bold)	Access and Actions	Notes
Enterprise user (CECEnterpriseUser)	<p>From Oracle Content Management, <i>enterprise users</i> have access to all the Collaboration and Sites features that <i>standard users</i> have access to:</p> <ul style="list-style-type: none"> • Manage content (view, upload, and edit documents). • Share content and sites with others. • Use conversations to collaborate (discuss topics, direct message someone, assign flags to someone, add annotations to documents). • Manage groups. • Create, edit, and publish sites as long as this feature hasn't been limited to <i>site administrators</i>. • View and interact with content items in sites. • Manage and view custom properties and edit values. <p>In addition they have access to Assets:</p> <ul style="list-style-type: none"> • Create and manage content items and digital assets. • Create and manage collections. <p>From the Oracle Content Management Recommendations:</p> <ul style="list-style-type: none"> • Enterprise users with access to contribute to at least one repository can create and manage recommendations. <p>From the Oracle Content Management Analytics interface:</p> <ul style="list-style-type: none"> • Enterprise users with access to at least one repository can access the Assets and Content page. • Enterprise users with access to at least one channel can access the Sites and Channels page. 	<p>Any users that need to actually <i>use</i> Oracle Content Management must be assigned the <i>standard user</i> or <i>enterprise user</i> role. These roles aren't assigned by default to any user.</p> <p>See Task and Feature Comparison by Application Role.</p>

Application Role (application role name in bold)	Access and Actions	Notes
Standard user (CECStandardUser)	<p>From Oracle Content Management, <i>standard users</i> have access to Collaboration and Sites features:</p> <ul style="list-style-type: none"> • Manage content (view, upload, and edit documents). • Share content and sites with others. • Use conversations to collaborate (discuss topics, direct message someone, assign flags to someone, add annotations to documents). • Manage groups. • Create, edit, and publish sites as long as this feature hasn't been limited to <i>site administrators</i>. • View and interact with content items in sites. • Manage and view custom properties and edit values. 	<p>Any users that need to actually <i>use</i> Oracle Content Management must be assigned the <i>standard user</i> or <i>enterprise user</i> role. These roles aren't assigned by default to any user.</p> <p>See Task and Feature Comparison by Application Role.</p>
External user (CECExternalUser)	<p>From Oracle Content Management, <i>external users</i> have access to Collaboration and Sites features for items that are shared with them:</p> <ul style="list-style-type: none"> • Manage content (view, upload, and edit documents). • Use conversations to collaborate (discuss topics, direct message someone, assign flags to someone, add annotations to documents). • Edit sites as long as this feature hasn't been limited to <i>site administrators</i>. 	<p>External users have limited access to Oracle Content Management. See Task and Feature Comparison by Application Role.</p>
Visitor (CECSitesVisitor)	<p>Access sites restricted to <i>visitors</i>.</p>	<p>This role applies if a site is set to be accessed only by visitors. If that restriction is enabled, only users with this role will be able to access the site. Users and groups with this role can't be searched, so you must type the complete user or group name to add them to site security. Visitors don't require a license.</p>
Sauce Video enterprise user (SauceEnterpriseUser)	<p>If you enabled Sauce Video during instance creation, you'll see the <i>SauceEnterpriseUser</i> application role. This role gives users full unlimited access to the Sauce Video application.</p>	<p>If you want Sauce users to be able to use Oracle Content Management, they must also be assigned the <i>standard user</i> or <i>enterprise user</i> role.</p>

Sales Accelerator Roles

If you're an Oracle SaaS customer and you install [Oracle Sales Accelerator](#), you'll see the following [additional application roles](#):

Application Role (application role name in bold)	Assigned Privileges
Viewer (SAUser)	This role allows users to view published content, content properties, and analytics. Viewers access Sales Accelerator in seller view.
Contributor (SACContributor)	This role gives users the same privileges as viewers, plus it allows them to create and manage their own content. Contributors access Sales Accelerator in seller view, but they can turn on contributor view to manage content. To access contributor view, users must also be given the CECEnterpriseUser role.
Content Admin (SACContentAdmin)	This role gives users the same privileges as contributors, plus it allows them to manage content owned by other people, update assets in bulk, and configure home pages. Content admins access Sales Accelerator in seller view, but they can turn on contributor view to manage content. To access contributor view, users must also be given the CECEnterpriseUser role.
Report Admin (SAREports)	This role gives users the same privileges as viewers, plus it allows them to view system-wide analytics and reports. Report admins access Sales Accelerator in seller view.
Application Admin (SAAdmin)	This role gives users the same privileges as viewers, plus it allows them to perform administration tasks in Sales Accelerator and Oracle Content Management. Application admins access Sales Accelerator in seller view.

All Sales Accelerator application roles have viewing privileges. Therefore if someone is assigned the SACContentAdmin role, they don't also need the SAUser role.

Task and Feature Comparison by Application Role

Depending on their application roles, Oracle Content Management users can perform different tasks and access different features.

Visitors can view certain sites, use public links, and view Oracle Content Management content embedded in apps or websites. Anonymous users (users who aren't signed in) are counted as visitors. See *Change Site Security* in *Building Sites with Oracle Content Management*. If you have a Universal Credits subscription, a visitor session is limited to a certain number of API calls and a certain amount of data transfer; see [Understand Active Users per Hour](#). If you have a non-metered subscription, visitor activity counts towards your daily visitor sessions; see [Understand Visitor Sessions](#).

Any users that need to actually *use* Oracle Content Management must be assigned the *standard user* or *enterprise user* role. [External users](#) have limited access to the Oracle Content Management web client. If you purchased enterprise users, you can assign the **Oracle Content Management Enterprise User** role to users to provide them access to more functionality. Your Oracle Content Management instance can have a mixture of standard and enterprise users to fit the needs of your company.




Note:

For more information on roles, see [Application Roles](#).

This following table lists basic tasks and the application roles required to perform them.

Task	A n o n y m o u s U s e r	V i s i t o r	S t a n d a r d E x t e r n a l U s e r	Standard User	Enterprise User
View public sites	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
View secure sites		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Access files and folders through public links	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Access files and folders through member links		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Access Oracle Content Management apps					<input checked="" type="checkbox"/> ¹
Access the Oracle Content Management web client			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Access the Oracle Content Management desktop client and mobile apps				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Manage your documents (view, upload, and edit documents)		<input checked="" type="checkbox"/> ²	<input checked="" type="checkbox"/> ³	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Share files and folders		<input checked="" type="checkbox"/> ²		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Use conversations (discuss topics, direct message someone, assign flags to someone, add annotations to documents)		<input checked="" type="checkbox"/> ²	<input checked="" type="checkbox"/> ⁴	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Task	A n o n y m o u s U s e r	V i s i t o r	S t a n d a r d E x t e r n a l U s e r	S t a n d a r d U s e r	E n t e r p r i s e U s e r
<p>Use groups</p> <p>Create sites This functionality can be restricted to site administrators.</p> <p>Manage sites This functionality can be restricted to site administrators.</p> <p>Use templates and themes in sites This functionality can be restricted to site administrators.</p> <p>Manage custom components and layouts This functionality can be restricted to site administrators.</p> <p>Configure the embeddable user interface This functionality can be restricted to site administrators.</p> <p>View custom properties (metadata) and edit values</p> <p>Work with digital assets (images, documents, and videos that you manage independently from your other files and folders) or business documents</p> <p>Use structured content (structured content, in the form of content items, is stored separately from its layout so it can be reused in various formats and contexts)</p> <p>Use recommendations (provide personalized experiences for website visitors by showing assets based on location or areas of interest)</p>			<p><input checked="" type="checkbox"/> 5</p> <p><input checked="" type="checkbox"/></p> <p><input checked="" type="checkbox"/> 6</p> <p><input checked="" type="checkbox"/></p> <p><input checked="" type="checkbox"/></p> <p><input checked="" type="checkbox"/></p> <p><input checked="" type="checkbox"/></p> <p><input checked="" type="checkbox"/></p> <p><input checked="" type="checkbox"/></p> <p><input checked="" type="checkbox"/></p> <p><input checked="" type="checkbox"/></p> <p><input checked="" type="checkbox"/></p>	<p><input checked="" type="checkbox"/></p> <p><input checked="" type="checkbox"/> 6</p> <p><input checked="" type="checkbox"/> 6</p> <p><input checked="" type="checkbox"/></p> <p><input checked="" type="checkbox"/></p> <p><input checked="" type="checkbox"/></p> <p><input checked="" type="checkbox"/></p> <p><input checked="" type="checkbox"/></p> <p><input checked="" type="checkbox"/></p> <p><input checked="" type="checkbox"/></p> <p><input checked="" type="checkbox"/></p>	

Task	A n o n y m o u s U s e r	V i s i t o r	S t a n d a r d E x t e r n a l U s e r	Standard User	Enterprise User
Analyze service usage					 ⁷

¹ Enterprise users may access any Oracle Content Management app, but additional privileges may be required depending on how they interact with the app.

² Visitors can manage and share content through Oracle Content Management components on sites.

³ Standard external users can create folders only in a folder to which they've been given access.



⁴ Standard external users can't create new conversations, but they can use conversations associated with other objects to which they have Contributor access.

⁵ Standard external users can't be part of public groups, only member groups. They can't create new groups. They can't modify group membership or leave a member group.

⁶ Standard users can create, edit and publish *standard* sites. Enterprise users can create, edit, and publish *standard* or *enterprise* sites.

⁷ Enterprise users with access to at least one repository can access the **Assets and Content** page. Enterprise users with access to at least one channel can access the **Sites and Channels** page.

This following table lists developer and administrative tasks and the application roles required to perform them. Users must be assigned the *enterprise user* role, or sometimes just the *standard user* role, in addition to the role listed to be able to sign in to Oracle Content Management. Any task that involves asset repositories requires the *enterprise user* role.

Task	Site Admin	Developer	Content Admin	Repository Admin	Capture Admin	Service Admin
Create sites This functionality can be restricted to site administrators.						

Task	Site Admin	Developer	Content Admin	Repository Admin	Capture Admin	Service Admin
Manage sites This functionality can be restricted to site administrators.	✓	✓				
Use templates and themes in sites This functionality can be restricted to site administrators.	✓	✓	✓			
Manage custom components and layouts This functionality can be restricted to site administrators.	✓	✓	✓			
Configure the embeddable user interface This functionality can be restricted to site administrators.	✓	✓	✓			
Configure custom properties (metadata)						✓
Create and share collections	✓					
Create and share asset types			✓			
Create localization policies				✓		
Create publishing channels				✓		
Create taxonomies			✓			
Create content workflows and assign workflow roles				✓		
Create editorial roles				✓		
Create asset repositories				✓		
Create audience attributes			✓			
Create ranking policies			✓			
Integrate Oracle Content Management with business applications		✓				✓

Task	Site Admin	Developer	Content Admin	Repository Admin	Capture Admin	Service Admin
Set up Capture procedures						
Manage Oracle Content Management applications Depending on the type of app you're working with, you may also need to have the content administrator and/or site administrator roles; for example, to create repositories, publishing channels, and such.						
Configure service settings						
Manage users, groups, and access						
Analyze service usage						
Manage the service (such as billing and usage)						

* Capture Administrator users can access the **Capture** page and the **Capture Activities** report.

There are additional application roles, but they are internal users who can't sign in to Oracle Content Management or administrative users who perform their tasks outside of Oracle Content Management. See [Application Roles](#).

Resource Roles (Permissions)

What users can see and do with a resource, such as a document, content item, or site, depends on the role (or permission) they're assigned when the resource is shared with them. For example, they might be the manager of one site, a contributor to a folder, or a viewer for another site.

The basic permissions of the roles are described here, but different resources handle permissions slightly differently, as described in the sections in this topic. Also note that, resource roles are cumulative. That is, the Downloader role has all the privileges of the Viewer role with added privileges. The Contributor role has all the privileges of both the Viewer and Downloader roles, and so on.

- **Viewer:** Viewers can view the resource but can't change anything.
- **Downloader:** Downloaders can download the resource or its associated files and save them to their own computer.
- **Contributor:** Contributors can edit the resource. Depending on the type of resource, this might mean they can rename it, edit tags or properties, and other similar tasks.
- **Manager:** Managers have full control of the resource (with the exception of folders, see below), including adding users as members and assigning them roles for the resource.

When you create a resource, you're automatically assigned as the **Owner** of the resource (with the exception of resources created in shared folders). This gives you full control of the resource. It also means that you can't be removed from the resource and your role can't be changed.



As a service administrator, you can also [set a default role](#) to assign to new users that are added to a folder.

To view the roles for a particular resource, click one of the following links:

- [Asset Types](#)
- [Assets](#)
- [Audience Attributes](#)
- [Collections](#)
- [Components and Layouts](#)
- [Content Workflows](#)
- [Conversations](#)
- [Editorial Roles](#)
- [Experiences](#)
- [Files and Folders](#)
- [Localization Policies](#)
- [Publishing Channels](#)
- [Ranking Policies](#)
- [Recommendations](#)
- [Rendition Policies](#)
- [Repositories](#)
- [Sites](#)
- [Taxonomies](#)
- [Templates](#)
- [Themes](#)
- [Workflow Roles](#)

Asset Types

You must have the *enterprise user* role, *content administrator* role, and one of the listed resource roles to perform the following tasks with asset types.

Task	Owner	Manager
View an asset type (in the Administration: Content area) You control users ability to use an asset type through settings in the repository.		
Create an asset type Any user with the <i>enterprise user</i> role and <i>content administrator</i> role can create asset types.	N/A	N/A

Task	Owner	Manager
Edit an asset type		
Share an asset type		
Delete an asset type		

Assets

You must have the *enterprise user* role and one of the listed resource roles to perform the following tasks with assets. Access to assets can be refined based on asset types and taxonomy categories using granular permissions in the parent repository.

Task	Manager	Contributor	Viewer
View an asset You need one of these roles for the repository where the asset is managed.			
Create or upload an asset You need one of these roles for the repository where the asset will be created and the asset type used to create the asset, and the asset type used to create the asset must be associated with the repository.			
Edit an asset (asset, tags, collections, properties, upload new version of digital asset) You need one of these roles for the repository where the asset is managed.			
Publish an asset You need at least Viewer access to the parent repository, plus one of these roles for the publishing channel that will be used to publish the asset.			
Move an asset through workflow You need at least Viewer access, plus any required workflow role.			
Delete an asset You need one of these roles for the repository where the asset is managed.			
Download a digital asset You need one of these roles for the repository where the asset is managed.			

Audience Attributes

If you have the *enterprise user* role and *content administrator* role you can perform any task with audience attributes.

Collections




You must have the *enterprise user* role, at least view access to the parent repository, and one of the listed resource roles to perform the following tasks with collections.

Task	Manag er	Contrib utor	Viewer
View a collection			
Create a collection You need one of these roles for the repository in which you create the collection.			
Add an asset to collection (digital asset, content item, or document) To add an asset to the collection, you one of these roles for the collection. To create a <i>new</i> asset directly in the collection, you need one of these roles for the parent repository (to create the asset), and one of these roles in the collection (to add the asset to the collection).			
Remove an asset from collection Note: Removing an asset from the collection, doesn't delete the asset from the parent repository.			
Edit a collection (rename, properties)			
Share a collection			

Components and Layouts




If you have a *standard user* or *enterprise user* role and one of the listed resource roles, you can perform the following tasks with components and layouts.

Task	Owner	Manag er	Contrib utor	Downl oader	Viewer
View a component or layout (component/layout and properties in the Developer area) To <i>use</i> content layouts, content field editors, and content forms in asset types, users need to be able to create or edit asset types , and the content field editors and content forms must be promoted.					
Create a component or layout Any user with the <i>standard user</i> or <i>enterprise user</i> role can create components or layouts. Note: If your service administrator limited component creation to site administrators, you must be a site administrator.	N/A	N/A	N/A	N/A	N/A
Edit a component or layout (edit or upload component or layout files)					
Copy or export a component or layout					
Delete a component or layout					

Task	Owner	Manager	Contributor	Downloader	Viewer
Share a component or layout					

Content Workflows

You must have the *enterprise user* role, *repository administrator* role, and one of the listed resource roles to perform the following tasks with content workflows.



Task	Manager
View a content workflow Any user with the <i>enterprise user</i> role and <i>repository administrator</i> role can view content workflows.	N/A
Register a content workflow Any user with the <i>enterprise user</i> role and <i>repository administrator</i> role can register content workflows.	N/A
Disable a content workflow	
Unregister a content workflow	
Share a content workflow	

Conversations

If you have a *standard user* or *enterprise user* role, you can create conversations. To view and participate in a conversation, you must be a member of the stand-alone conversation or have access to the resource associated with the conversation.

Editorial Roles

You must have the *enterprise user* role, *repository administrator* role, and one of the listed resource roles to perform the following tasks with editorial roles.

Task	Owner	Manager
View an editorial role Any user with the <i>enterprise user</i> role and <i>repository administrator</i> role can view editorial roles.	N/A	N/A
Create an editorial role Any user with the <i>enterprise user</i> role and <i>repository administrator</i> role can create editorial roles.	N/A	N/A
Edit an editorial role		

Task	Owner	Manager
Copy an editorial role Any user with the <i>enterprise user</i> role and <i>repository administrator</i> role can copy editorial roles.	N/A	N/A
Share an editorial role		
Delete an editorial role		

Experiences

If you have the *enterprise user* role and developer application role you can perform any task with experiences.

Files and Folders

If you have a *standard user* or *enterprise user* role and one of the listed resource roles, you can perform the following tasks with files and folders.

Task	Owner	Manager	Contributor	Downloader	Viewer
Upload a file Any user can upload top-level files. To upload a file to a folder, you need one of these roles on the parent folder.					
Create a folder Any user can create top-level folders. To create a subfolder, you need one of these roles on the parent folder.					
View a file or folder For top-level files, you must be the owner or the owner must share a link with you giving you one of these roles. For other files or folders, you need one of these roles on the folder itself or the parent folder.					
View the properties, tags, and metadata For top-level files, you must be the owner. For other files or folders, you need one of these roles on the folder itself or the parent folder.					
View the file access history and versions For top-level files, you must be the owner. For other files, you need one of these roles on the parent folder.					

Task	Owner	Manager	Contributor	Downloader	Viewer
<p>Edit the properties, tags, and metadata For top-level files, you must be the owner.</p> <p>For other files or folders, you need one of these roles on the folder itself or the parent folder.</p>	✓	✓	✓		
<p>Configure public link settings for a folder</p>	✓	✓			
<p>Edit custom property values</p>	✓	✓	✓		
<p>Collaborate on a file or folder (file annotations and conversation) For top-level files, you must be the owner or the owner must share a link with you giving you one of these roles.</p> <p>For other files or folders, you need one of these roles on the folder itself or the parent folder.</p>	✓	✓	✓	✓	✓
<p>Move a file or folder For top-level files or top-level folders, you must be the owner.</p> <p>For other files or folders, you need one of these roles on the folder itself or the parent folder.</p> <p>Moves must be made to a target folder with the same owner as the source folder.</p>	✓	✓	✓		
<p>Copy a file or folder For top-level files, you must be the owner.</p> <p>For other files or folders, you need one of these roles on the folder itself or the parent folder.</p> <p>Copies must be made to a folder you own or to a folder where you have the Contributor Manager roll (write permissions).</p>	✓	✓	✓	✓	
<p>Rename a file or folder For top-level files, you must be the owner or the owner must share a link with you giving you one of these roles.</p> <p>For other files or folders, you need one of these roles on the folder itself or the parent folder.</p>	✓	✓	✓		
<p>Download a file or folder For top-level files, you must be the owner or the owner must share a link with you giving you one of these roles.</p> <p>For other files or folders, you need one of these roles on the folder itself or the parent folder.</p>	✓	✓	✓	✓	

Task	Owner	Manager	Contributor	Downloader	Viewer
<p>Share members-only links to a file or folder For top-level files, you must be the owner. For other files or folders, you need one of these roles on the folder itself or the parent folder.</p>					
<p>Share public links to a file or folder For top-level files, you must be the owner. For other files or folders, you need one of these roles on the folder itself or the parent folder.</p>					
<p>Upload a new version of a file For top-level files, you must be the owner or the owner must share a link with you giving you one of these roles. For other files, you need one of these roles on the parent folder.</p>					
<p>Lock a file For top-level files, you must be the owner. For other files, you need one of these roles on the parent folder.</p>					
<p>Delete a file or folder For top-level files and top-level folders, you must be the owner. For other files or folders, you need one of these roles on the folder itself or the parent folder.</p>					
<p>Manage members for a folder You need one of these roles on the folder itself or the parent folder.</p>					

Localization Policies

If you have the *enterprise user* role and *repository administrator* role you can perform any task with localization policies.

Publishing Channels

You must have the *enterprise user* role, *repository administrator* role, and one of the listed resource roles to perform the following tasks with publishing channels.

Task	Owner	Manager	Viewer	Contributor
View a publishing channel				
<p>Create a publishing channel Any user with the <i>enterprise user</i> role and <i>repository administrator</i> role can create publishing channels.</p>	N/A	N/A	N/A	N/A

Task	Owner	Manager	Viewer	Contributor
Edit a publishing channel				
Share a publishing channel				
Delete a publishing channel				
Publish assets				

Ranking Policies

If you have the *enterprise user* role and *content administrator* role you can perform any task with ranking policies.

Recommendations

You must have the *enterprise user* role and one of the listed resource roles to perform the following tasks with recommendations.

Task	Manager	Contributor	Viewer
View a recommendation You need one of these roles for the parent repository.			
Create a recommendation You need one of these roles for the repository where the recommendation will be created.			
Edit a recommendation You need one of these roles for the parent repository.			
Move a recommendation through workflow You need at least Viewer access to the parent repository, plus any required workflow role.			
Publish a recommendation You need at least Viewer access to the parent repository, plus one of these roles for the publishing channel that will be used to publish the recommendation.			
Delete a recommendation You need one of these roles for the parent repository.			

Rendition Policies

If you have the *enterprise user* role and *content administrator* role you can perform any task with rendition policies.

Repositories

You must have the *enterprise user* role, *repository administrator* role, and one of the listed resource roles to perform the following tasks with repositories. Access to assets can be refined based on asset types and taxonomy categories using granular permissions in the parent repository.

Task	Manag er	Contrib utor	Viewer
View a repository			
Create a repository You need one of these roles for any asset types and publishing channels you want to assign to the repository.			
Edit a repository			
Share a repository			
Delete a repository			

Sites

If you have a *standard user* or *enterprise user* role and one of the listed resource roles, you can perform the following tasks with sites.

Task	Owner	Manag er	Contrib utor	Downl oader	Viewer
View a site <ul style="list-style-type: none"> Viewers can view site properties and members. Other roles can also preview the site, or open the site to view or add annotations or participate in the associated conversation. 					
Create a site You need one of these roles for the template used to create the site. Note: Your service administrator can disable site creation or limit site creation to site administrators. If you don't see the Create option on the Sites page, contact your service administrator.					
Edit a site (including change status) Only owners and managers can rename a site.					
Copy a site					
Delete a site					

Task	Owner	Manager	Contributor	Downloader	Viewer
Share a site					
Create a template from a site					

Taxonomies

You must have the *enterprise user* role; *content administrator* role or *repository administrator* role; and one of the listed resource roles to perform the following tasks with taxonomies.

Task	Manager	Editor
View a taxonomy		
Create a taxonomy Any user with the <i>enterprise user</i> role and <i>content administrator</i> role can create taxonomies. Repository administrators can't create taxonomies.	N/A	N/A
Import a taxonomy Any user with the <i>enterprise user</i> role and <i>content administrator</i> role can import taxonomies. Repository administrators can't import taxonomies.	N/A	N/A
Edit a taxonomy		
Promote a taxonomy		
Publish a taxonomy		
Share a taxonomy		
Export a taxonomy		
Delete a taxonomy		

Templates

If you have a *standard user* or *enterprise user* role and one of the listed resource roles, you can perform the following tasks with templates.

Task	Manager	Contributor	Downloader	Viewer
View a template				

Task	Manager	Contributor	Downloader	Viewer
Create a template If you're creating a template from an existing site, you need one of these roles for the existing site. Note: If your service administrator limited template creation to site administrators, you must be a site administrator.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Edit a template (edit or upload template files, rename)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Copy or export a template	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Delete a template	<input checked="" type="checkbox"/>			
Share a template	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		

Themes

If you have a *standard user* or *enterprise user* role and one of the listed resource roles, you can perform the following tasks with themes.

Task	Owner	Manager	Contributor	Downloader	Viewer
View a theme	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Publish a theme	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Copy a theme	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Delete a theme	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			
Share a theme	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		

Workflow Roles

If you have the *enterprise user* role and *repository administrator* role you can assign users to workflow roles. All members of a workflow role can perform the action defined for the role.

Security

Oracle Content Management uses a multilayered approach to protect your system and content.

 **Note:**

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. If your region has been updated, follow the steps marked **IAM**. If your region hasn't been updated, follow the steps marked **IDCS**.

Security Feature	Description	Who Manages It and Where
User accounts	You need an account with a user name and password to access Oracle Content Management.	<ul style="list-style-type: none"> • IAM: Cloud account administrators manage user accounts in the Oracle Cloud Console. • IDCS: Cloud account administrators manage user accounts in the IDCS Console.
Application roles	Each user is assigned one or more roles to control what functionality and areas of the web user interface they can access.	<ul style="list-style-type: none"> • IAM: Cloud account administrators assign application roles in the Oracle Cloud Console. • IDCS: Cloud account administrators assign application roles in the IDCS Console.
Groups	Groups make it easy to grant multiple users access to folders, conversations, and content types. By adding someone to a group or removing them from a group, you can quickly update the permissions to all the items that group has access to.	<ul style="list-style-type: none"> • IAM: Cloud account administrators should create high-level organizational groups in the Oracle Cloud Console. • IDCS: Cloud account administrators should create high-level organizational groups in the IDCS Console. <p>Users can create additional groups in Oracle Content Management as necessary.</p>
Mobile device passcodes	When accessing files on a mobile device, you can set a passcode to provide additional security. The passcode is a four-digit number that is set and managed on your device. It's used in addition to your user name and password.	Users manage their passcodes on their mobile devices.
Revoke authorization for a mobile device	If a user loses their device or it's taken, they should remove that device's authorization to access the service. The next time someone tries to activate the app on the device, the account is signed out and all local content stored on the device for that account is deleted.	Users can revoke a device from the web client.

Security Feature	Description	Who Manages It and Where
Single Sign-On (SSO)	If Federated Single Sign-On (SSO) is currently available for your Oracle Content Management environment, you can enable it to customize sign-in procedures. When Single Sign-On (SSO) is enabled, users can sign in to one domain using corporate security credentials and access another domain without signing in again. For example, perhaps you are an administrator for your company which has two Oracle Cloud Services and you must provision these services to your company's organization, roles, and users. Your company may also have on-premise applications and cloud services from other vendors. It's important that communication between these services and applications is done in a secure fashion. With SSO, users can sign in to all of them using the same set of credentials that are managed by using your identity domain system.	Cloud account administrators configure SSO in the Oracle Cloud Console.
File encryption	Files are protected using Transport Layer Security (TLS) technology. Files are encrypted while they're uploaded (in transit) and when they're stored (at rest) in the cloud. Files at rest that are stored using the Oracle Storage Cloud service are encrypted using a 256-bit RSA encryption algorithm. That prevents unauthorized use of the files. Any files downloaded to a mobile device are also encrypted. You can't access those files outside of the Oracle Content Management app unless you specifically download the file for use on the device.	File encryption is handled automatically by Oracle Content Management.
File type and size restrictions	You can specify which types of files can be uploaded and restrict the size of uploaded files. In addition, when you upload files to the cloud, they can be checked by a virus scanner. Any files found to be infected are quarantined in the Trash bin and a special icon marks the file as infected.	Service administrators configure file type and size restrictions through the Oracle Content Management Administration interface.

Security Feature	Description	Who Manages It and Where
File access control	<p>You have total control over who can access your files. You can add co-workers as members of a folder. The added users are granted default access rights, but folder managers can also change those rights.</p> <p>In addition to sharing folders, you can also share files using links. If you send a link to a member of a folder, the member can sign in and use the file in the service. If you send the link to a non-member, that person is restricted from seeing other files in the folder.</p>	<p>Service administrators set the default role for new folder members and set default link behavior.</p> <p>Users control access when they share content.</p>
Conversation encryption	<p>Conversations at rest are stored using the Oracle Storage Cloud service and are encrypted using a 256-bit RSA encryption algorithm. That prevents unauthorized access to conversation content.</p>	<p>Conversation encryption is handled automatically by Oracle Content Management.</p>
Site creation and sharing restrictions	<p>You can specify who can create, share, and use sites functionality, which lets users design, build, publish, and manage websites that are hosted in Oracle Cloud.</p>	<p>Service administrators configure sites settings through the Oracle Content Management Administration interface.</p>
Site security	<p>When you publish a site and make it available online, it's publicly available to anyone. However, you can change the security settings for the site to require users to sign in. You can also require that users have a specific role assigned to them.</p>	<p>Site owners and managers control the security for individual sites.</p>
Site sharing	<p>With site sharing, you specify individual users who can access your unpublished (offline) site and allow them to view, modify, or manage the site based on the permission you give them.</p>	<p>Site owners and managers control the security for individual sites.</p>
Site component sharing	<p>Some components provide access to shared resources such as folders, files, or conversations. Component sharing considers both site security (who can view the published site) and resource sharing (who can view and work with folders, files, and conversations).</p>	<p>Site component sharing is handled automatically by Oracle Content Management based on site and resource security.</p>
Cross-Origin Resource Sharing (CORS)	<p>Cross-Origin Resource Sharing (CORS) allows a web page to make requests such as XMLHttpRequest to another domain. If you have a browser application that integrates with Oracle Content Management but is hosted in a different domain, add the browser application domain to Oracle Content Management's CORS origins list.</p>	<p>Service administrators configure CORS through the Oracle Content Management Administration interface.</p>

Security Feature	Description	Who Manages It and Where
Proxy service	Oracle Content Management includes a proxy service, so that you can use REST services which have Cross-Origin Resource Sharing (CORS) limitations or require service account credentials. The proxy service is a reverse proxy server. It provides a URL to which web browsers connect. The proxy service then acts as an intermediary between the web browser and a remote REST service (or <i>endpoint</i>). The proxy service explicitly adds CORS support to all endpoints and can optionally insert service account credentials to requests coming from web browsers.	Service administrators configure the proxy service through the Oracle Content Management Administration Integrations interface.
Embedded content allowlist	You can display content from Oracle Content Management within other domains. For example, you might embed the Oracle Content Management web user interface into your own web applications to access folder and document management features inside your application. The embedded content appears only if embedded content is enabled and the domain is added to allowed domains allowlist.	Service administrators configure embedded content settings through the Oracle Content Management Administration interface.

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](#).



Note:

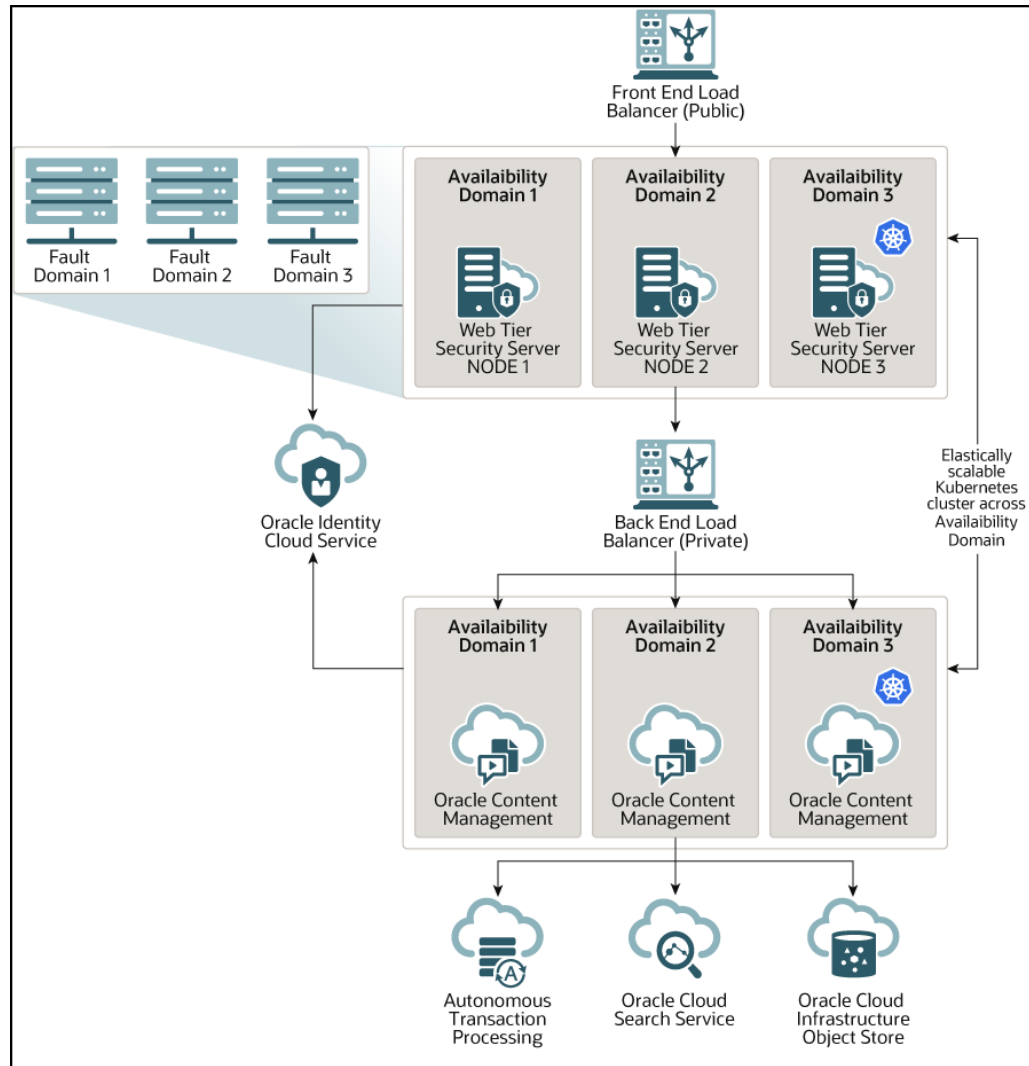
If you purchased your subscription prior to September 2019, your deployment process may vary. See [Manage Oracle Content Management in Legacy Environments](#).

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

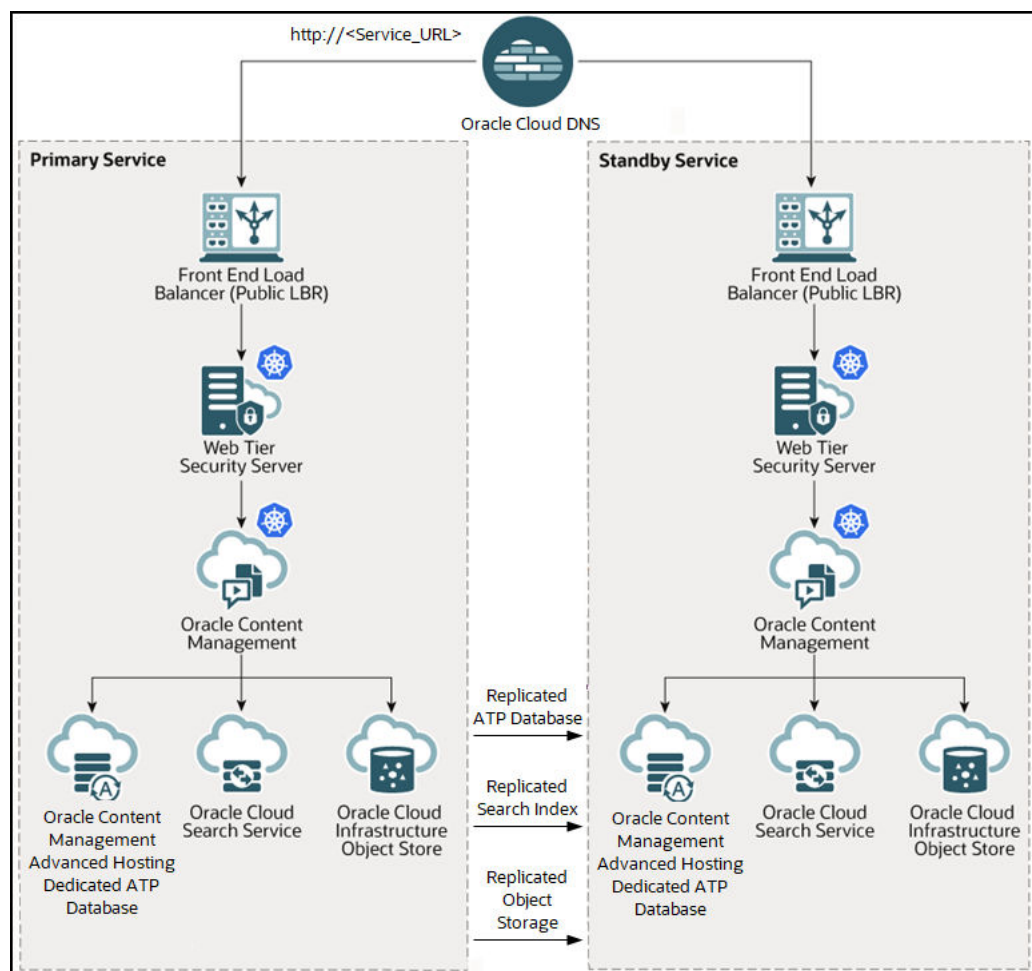
Oracle Content Management provides a native disaster recovery product option. The Oracle Content Management disaster recovery product capability essentially provides a full-stack orchestration of the service that includes comprehensive disaster recovery failover capabilities for all layers of the Oracle 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*.

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 need to perform other tasks to [roll out the service](#).

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.
 - b. 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. Open the administrators group (**Administrators** or **Domain Administrators**).
5. Click the **Users** tab.
6. Click **Assign user to groups**.
7. Select the users you want to delegate to, and then click **Add**.

Users you added to the Administrators group can now create Oracle Content Management instances.

Add Users to a New Administrative Group

To delegate creation of Oracle Content Management instances to users without adding them to the Administrators group, the primary account administrator must create a new group and add users to it, then give the group the proper permissions.

1. Create a group of users you want to delegate to.
 - a. 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:
 - 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 **Domains**.
 - b. Open the identity domain you're using for Oracle Content Management.
 - c. In the navigation menu on the left, click **Groups**.
 - d. To create a group, click **Create group**.
 - e. Enter a name and description for the group that makes clear to others what the group is used for.
 - f. Select the users you want to add to the group.
 - g. Click **Create**.
2. Create a policy to allow the group to manage Oracle Content Management instances.
 - a. In the **Identity & Security** area, under **Identity**, click **Policies**.
 - b. Click **Create Policy**.
 - c. Enter a name and description.
 - d. Next to Policy Builder, click **Show manual editor**.
 - e. In the box, enter the following statement, replacing *IdentityDomainName/GroupName* with the name of your identity domain and the group you created, 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..aaaaaaa4yafecztqbebz nfxpjzwm52wuaeornzgzqrujpbkmeez6zuigv 7a
oc4	ocid1.tenancy.oc4..aaaaaaaamxjaupllkzz2a 2qmvcon7rprzlu4hmyfajsfk3ezzmdstterlbya
oc8	ocid1.tenancy.oc8..aaaaaaaanpm5o3ejwjerj yiwsh4u5rd6mpme5ftq44ue5pkxnnhvf3sw 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 \(VCNs in different tenancies\)](#).

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 (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 (Required for analytics)
- oracle.com
- www.oracle.com
- docs.oracle.com
- apexapps.oracle.com
- cloudcustomerconnect.oracle.com
- community.oracle.com
- youtube.com
- consent.truste.com
- consent.trustarc.com
- prefmgr-cookie.truste-svc.net
- consent-st.trustarc.com
- 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
Instance Name	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.
Description	Optionally, enter a description of the instance.
Compartment	This is the compartment you previously selected. If you need to, you can change it.
Notification Email	Make sure this is the email address to which you want provisioning status updates to be sent.

Field	Description
License Type	<p>Choose the type of license you want to use for this instance:</p> <ul style="list-style-type: none">• Premium Edition: Subscribe to a new full-featured Oracle Content Management license.• BYOL License*: Use your existing Oracle WebCenter Middleware license (BYOL).• Starter Edition: Subscribe to a feature-limited edition of Oracle Content Management. <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 Oracle PaaS and IaaS Universal Credits Service Descriptions for a description of which WebCenter products qualify for BYOL licensing and for the conversion ratios for WebCenter processor licenses.</p>

Field	Description
<p>License Options</p>	<p>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 style="list-style-type: none"> <p>Advanced Hosting (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 Advanced Hosting.</p> <div data-bbox="997 667 1458 842" style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 10px;"> <p> Note:</p> <p>You can't disable this option after the instance has been created.</p> </div> <p>Sales Accelerator—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 purchased an Oracle Sales Accelerator subscription, select Sales Accelerator.</p> <p>Sauce Video—Sauce Video 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 Video Creation Platform.</p> <div data-bbox="997 1318 1458 1671" style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 10px;"> <p> Note:</p> <ul style="list-style-type: none"> – If you're an Oracle SaaS customer, you must have purchased a Sauce Video subscription to see this option. – All Sauce Video Creation Platform data is stored in London, UK. </div>

- 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
Instance Type (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 Non-Primary in the drop-down list. Primary and non-primary instances are billed at different rates.</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>
Upgrade Schedule (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">• Upgrade immediately: Upgrade this instance as soon as a new release of Oracle Content Management is available.• Delay upgrade: Delay the upgrade of this instance, so that it is one release behind the latest release of Oracle Content Management. <p>Once you create this instance, you can't change this setting.</p>

Field	Description
Instance Access Type (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"> • Public: Select this option if you want your instance to be viewed over <i>public internet</i>. • Private: If you want to create a private instance that can be viewed only within your <i>intranet</i>, and you completed the prerequisite steps to set up Oracle Cloud Infrastructure FastConnect, select this option. <p>Once you create this instance, you can't change this setting.</p>
Disaster Recovery (not available for Starter Edition)	<p>You must enable Advanced Hosting before you can select this option. Disaster recovery 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>
Tags	<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 Oracle Content Management, you might want to [enable additional features](#). Then you need to perform other tasks to [roll out the service](#).

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 need to perform other tasks to [roll out the service](#).

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 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](#).

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](#).

Create Your Instance in a Secondary IDCS Domain

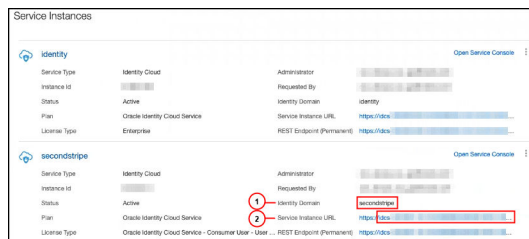
If you want to create multiple Oracle Content Management instances in separate environments, you need to create a secondary IDCS domain before you create those additional Oracle Content Management instances.

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-xxxxxxxxxxxxxx`, 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 nfxpjzwm52wuaeornzgzqrujpbkmeez6zuigv 7a
oc4	ocid1.tenancy.oc4..aaaaaaaamxjaupllkzz2a 2qmvcon7rprzlu4hmyfajsfk3ezzmdstterlbya
oc8	ocid1.tenancy.oc8..aaaaaaaanpm5o3ejwjerj yiwsh4u5rd6mpme5ftq44ue5pkxnnhvfy3sw 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
Instance Name	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.
Description	Optionally, enter a description of the instance.
Compartment	This is the compartment you previously selected. If you need to, you can change it.
Notification Email	Make sure this is the email address to which you want provisioning status updates to be sent.
License Type	<p>Choose the type of license you want to use for this instance:</p> <ul style="list-style-type: none"> • Premium Edition: Subscribe to a new full-featured Oracle Content Management license. • BYOL License: Use your existing Oracle WebCenter Middleware license (BYOL). • Starter Edition: Subscribe to a feature-limited edition of Oracle Content Management. <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 Oracle PaaS and IaaS Universal Credits Service Descriptions for a description of which WebCenter products qualify for BYOL licensing and for the conversion ratios for WebCenter processor licenses.</p>
Access Token (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>Note: 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
License Options	<p data-bbox="943 222 1458 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 1458 1276" style="list-style-type: none"> <li data-bbox="943 375 1458 632"> <p data-bbox="943 375 1458 632">• Advanced Hosting (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 Advanced Hosting.</p> <div data-bbox="997 667 1458 842" style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p data-bbox="1029 709 1154 741"> Note:</p> <p data-bbox="1078 768 1430 821">You can't disable this option after the instance has been created.</p> </div> <li data-bbox="943 848 1458 1104"> <p data-bbox="943 848 1458 1104">• Sales Accelerator—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 purchased an Oracle Sales Accelerator subscription, select Sales Accelerator.</p> <li data-bbox="943 1110 1458 1276"> <p data-bbox="943 1110 1458 1276">• Sauce Video—Sauce Video 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 Video Creation Platform.</p> <div data-bbox="997 1318 1458 1671" style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p data-bbox="1029 1360 1154 1392"> Note:</p> <ul data-bbox="1078 1419 1398 1650" 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 data-bbox="1078 1562 1398 1650">– All Sauce Video Creation Platform data is stored in London, UK. </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
Instance Type (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 Non-Primary in the drop-down list. Primary and non-primary instances are billed at different rates.</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>
Upgrade Schedule (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"> • Upgrade immediately: Upgrade this instance as soon as a new release of Oracle Content Management is available. • Delay upgrade: Delay the upgrade of this instance, so that it is one release behind the latest release of Oracle Content Management. <p>Once you create this instance, you can't change this setting.</p>
Instance Access Type (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"> • Public: Select this option if you want your instance to be viewed over <i>public internet</i>. • Private: If you want to create a private instance that can be viewed only within your <i>intranet</i>, and you completed the prerequisite steps to set up Oracle Cloud Infrastructure FastConnect, select this option. <p>Once you create this instance, you can't change this setting.</p>

Field	Description
Disaster Recovery (not available for Starter Edition)	You must enable Advanced Hosting before you can select this option. Disaster recovery 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.
IDCS Domain Name (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 prerequisite steps .
IDCS Domain ID (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://".
Tags	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 Oracle Content Management, you might want to [enable additional features](#). Then you need to perform other tasks to [roll out the service](#).

Enable Optional Features


Oracle Content Management includes integrations for several third-party applications. You just need to enable them to make use of the features.

1. After you sign in to the Oracle Content Management web application as an administrator, click **Integrations** in the Administration area of the navigation menu.
2. On the **Applications** page, under Other Integrations, enable the features you want to make available in your instance.
 - [Microsoft Office Online](#)—Enable Oracle Content Management web client users to view and edit Office files directly in Microsoft Office Online. For additional Microsoft Office integration features, see [Integrate with Microsoft Office](#).
 - [Microsoft Outlook](#)—Enable users to embed links to their Oracle Content files and folders into email messages or calendar appointments.
 - [Slack](#)—Enable users to post links to files and folders into Slack messages directly, without having to first create the links in the Oracle Content Management web interface and copy them into Slack.
 - [Desygner](#)—Enable designers to create templates that other teams can use to create new assets while following template rules and layouts.
 - [Kaltura video management](#)—Enable Kaltura video features. Kaltura provides a rich video management and delivery experience, including all the standard features, such as upload, manage, preview, and download, plus advanced capabilities for optimized editing, streaming, automatic transcoding and conversion, and more responsive playback options. Videos added as a Video Plus asset type will use the Kaltura video service.

Integrate Microsoft Office Online

Allow Oracle Content Management web client users to view and edit Office files directly in Microsoft Office Online.

1. On the Applications page (in the Integrations area), enable **Microsoft Office Online**.

2. Optionally, you can include additional notification text that will appear in the pop-up window when a user opens an Office file from Oracle Content Management. Click , then enter the additional notification text you want to include. To see what the notification will look like, click **Preview**. When you're satisfied with your text, click **Save**.

Integrate Microsoft Outlook

Deploy Oracle Content Management for Outlook on your Microsoft Exchange server to enable your users to embed links to their Oracle Content files and folders into email messages or calendar appointments.

1. On the Applications page (in the Integrations area), next to **Microsoft Outlook**, click **Download Manifest**.
2. Install the add-in on your Microsoft Exchange server, following [Microsoft's documentation](#).
3. It can take up to 72 hours for a new add-in deployment to reflect for users. After you confirm that the add-in is visible to users:
 - Inform them of the new Oracle Content Management add-in features.
 - If your users previously installed the Oracle Content Add-in for Outlook by installing the Oracle Content Management Desktop app, they should disable that add-in.

Integrate Kaltura Video Management

Enable Kaltura video features. Kaltura provides a rich video management and delivery experience, including all the standard features, such as upload, manage, preview, and download, plus advanced capabilities for optimized editing, streaming, automatic transcoding and conversion, and more responsive playback options. Videos added as a Video Plus asset type will use the Kaltura video service.

On the Applications page (in the Integrations area), enable **Kaltura Video Management - Video Plus**.

3

Roll Out the Service

As a system administrator, you'll need to configure default settings, provide sign in information to users, and, if desired, deploy the desktop app to get your system ready for your users and to get your users up and running.

- [Understand the Roll-Out Process](#)
- [Provide Sign-In and Get-Started Information to Users](#)
- [Deploy the Desktop App](#)

Understand the Roll-Out Process

After deploying Oracle Content Management, you have a few main tasks to perform to get Oracle Content Management up and running:

This topic assumes you've already performed the tasks described in [Deploy Oracle Content Management](#), including creating groups, assigning roles, adding users, and assigning users to groups.

Perform the following tasks, as necessary:

- Set service defaults such as user quotas, link behavior, file type and size restrictions, and virus scan options. See [Configure Documents Settings](#). Another important default to set is the default role given to new folder members. See [Set the Default Resource Role for New Folder Members](#).
- You might want to perform some of the following tasks to get the most out of Oracle Content Management:
 - [Apply Custom Branding and URLs](#)
 - [Enable or Disable Email Notifications](#)
 - [Set the Default Locale Settings](#)
 - [Configure Metadata Settings](#)
- Introduce your users to Oracle Content Management and let them know who to contact if they have questions. See [Provide Sign-In and Get-Started Information to Users](#).
- Optionally, push the desktop app out to your users. See [Deploy the Desktop App](#).

To take your user experience even further, integrate Oracle Content Management with your other business applications. See *Integrating and Extending Oracle Content Management*.

Provide Sign-In and Get-Started Information to Users

To get users started, administrators should provide clear sign-in instructions to users. After you add users to the system, the service sends them welcome emails, giving the user sign-in information. But it's useful for you to also send an email, providing more details.

Automatic Welcome Emails

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](#).

The welcome email for Oracle Content Management users is customized based upon the user's application role, such as administrator, enterprise user, or standard user.

The automatic welcome email includes the web address (URL) for the service and the user's account name and login information.

Service URL

The values used for the URL are created when the service is activated. The URL for the service has this general format:

```
https://<service-name>-<account-name>.<service-  
type>.ocp.oraclecloud.com/documents
```

For example, if `salesdocuments1` was entered as your service name, `myaccount` was entered as your account name, and the service type is `cec`, the service URL is:

```
salesdocuments1-myaccount.cec.ocp.oraclecloud.com/documents
```

Mobile App for Android APK File

If you want to make the .apk file for the Android mobile app available to your users through a link, you can download it from the [Oracle Content Management downloads](#) page, at the bottom of the page.

Deploy the Desktop App

Individual users can download the desktop app through the web browser and install it on their machines. However, some enterprise environments may not allow users to install their own software. In those cases, you can roll out the desktop app to multiple client machines with the help of the EXE and MSI installer packages.

- [Run the Executable Installer from the Command Line](#)
- [Run the MSI Installer](#)
- [Deploy the MSI Installer Through Active Directory's Group Policy](#)
- [Set Installation Defaults](#)

Run the Executable Installer from the Command Line

You can run the .exe installer from the command line with parameters on a local machine to perform a number of installation tasks. This might be useful when automating some of the installation process.

- [Install or upgrade the software](#)
- [Repair the software](#)
- [Extract the installer MSI and MST](#)
- [Use the installer without a user interface](#)
- [Language codes](#)

Install or upgrade the software

All options following the custom option will be passed to Msiexec.

- **Syntax**

```
{installer path} /user /L|language {language code} /g|log {log path} /s|silent /v|custom {options}
```

- **Parameters**

Parameter	Description
{installer path}	The path of the installer executable.
/user	(optional) Specifies that the product will be installed only for the current user. This type of installation doesn't require administrative privileges. If you don't include this parameter, the product will be installed for <i>all</i> users on the machine, which requires administrative privileges.
/L, /language {language code}	(optional) Specifies the language used in the user interface. See the Language codes section below for a list of supported languages.
/g, /log {log path}	(optional) Specifies that a log should be created detailing the actions undertaken by the installer and written into the given file path.
/s, /silent	(optional) Specifies whether or not the user interface is shown.
/v, /custom {options}	(optional) Specifies options to pass to the Msiexec process. See Running the MSI Installer for details.

- **Example**

```
oracle_content_setup.exe /user /l 1033 /s
```

Repair the software

The language used during repair will be the language used to install the product. All options following the custom option will be passed to Msiexec.

- **Syntax**

```
{installer path} /r|repair /g|log {log path} /s|silent /v|custom {options}
```

- **Parameters**

Parameter	Description
{installer path}	The path of the installer executable.
/r, /repair	Repairs the product.
/g, /log {log path}	(optional) Specifies that a log should be created detailing the actions undertaken by the installer and written into the given file path.
/s, /silent	(optional) Specifies whether or not the user interface is shown.
/v, / custom {options}	(optional) Specifies options to pass to the Msiexec process. See Running the MSI Installer for details.

- **Example**

```
oracle_content_setup.exe /repair /log "C:\logs\oracle
documents.txt"
```

Extract the installer MSI and MST

- **Syntax**

```
{installer path} /e|extract {destination directory} /L|
language {language code}
```

- **Parameters**

Parameter	Description
{installer path}	The path of the installer MSI file.
/e, / extract {destinati on directory}	Extracts the installer MSI and MST into the given directory.
/L, /language {language code}	(optional) - Specifies the language of the strings contained in the extracted MST. See the Language codes section below for a list of supported languages.

- **Example**

```
oracle_content_setup.exe /extract C:\Users\blair\desktop
```

Use the installer without a user interface

- **Syntax**

```
{installer path} /s|silent
```

- **Parameters**

Parameter	Description
{installer path}	The path of the installer executable.
/s, /silent	(optional) Specifies whether or not the user interface is shown.

- **Example**

```
oracle_content_setup.exe /silent
```

Language codes

- Arabic: 1025
- Czech: 1029
- Danish: 1030
- Korean: 1042
- Dutch: 1043
- Norwegian: 1044

- German: 1031
- Greek: 1032
- English: 1033
- Spanish: 1034
- Finnish: 1035
- French (France): 1036
- French (Canada): 3084
- Hebrew: 1037
- Hungarian: 1038
- Italian: 1040
- Japanese: 1041
- Polish: 1045
- Portuguese (Brazil): 1046
- Portuguese (Portugal): 2070
- Romanian: 1048
- Russian: 1049
- Slovak: 1051
- Swedish: 1053
- Thai: 1054
- Turkish: 1055
- Chinese (China): 2052
- Chinese (Taiwan): 1028

Run the MSI Installer

Use this command to extract the MSI package from the .exe installer to a given location:

```
oracle_content_setup.exe /extract c:\directory
```

The following MSI options are supported by the Oracle Content Management MSI package.

- [Install options](#)
- [Upgrade options](#)
- [Uninstall options](#)
- [Repair options](#)
- [User interface options](#)

Install options

Use `/i` to install the product.

- **Syntax**

```
msiexec /i {installer path} ALLUSERS=2 MSIINSTALLPERUSER=1 /
norestart|promptrestart|forcerestart
```

- **Parameters**

Parameter	Description
{installer path}	The path of the installer executable.
ALLUSERS=2 MSIINSTALLPER USER=1	Specifies that the product will be installed only for the current user. This type of installation doesn't require administrative privileges. If you don't include these parameters, the product will be installed for <i>all</i> users on the machine, which requires administrative privileges.
/norestart	Install the product without prompting for a system restart at the end of installation.
/promptrestart	Prompt the user to restart if a restart is required after installation.
/forcerestart	Restart the computer after every installation.

- **Example**

```
msiexec /i oracle_documents_setup.msi ALLUSERS=2
MSIINSTALLPERUSER=1 /norestart
```

Upgrade options

Use `/i` with the path to the latest installer to upgrade the product.

- **Syntax**

```
msiexec /i {path to latest version}
```

- **Parameters**

Parameter	Description
{path to latest version}	The path to the latest version of the installer executable.

- **Example**

```
msiexec /i oracle_documents_setup.msi
```

Uninstall options

Use `/x` to uninstall the product.

- **Syntax**

```
msiexec /x {installer path} /norestart|promptrestart|
forcerestart
```

- **Parameters**

Parameter	Description
{installer path}	The path of the installer executable.
/norestart	Uninstall the product without prompting for a system restart at the end of installation.
/promptrestart	Prompt the user to restart if a restart is required after uninstall.
/forcerestart	Restart the computer after every uninstall.

- **Example**

```
msiexec /x oracle_documents_setup.msi /promptrestart
```

Repair options

Use `/f` to repair the product.

- **Syntax**

```
msiexec /f{p|o|e|d|c|a|u|m|s|v} {installer path}
```

- **Parameters**

Parameter	Description
p	Reinstalls only if file is missing.
o	Reinstalls if file is missing or if an older version is installed.
e	Reinstalls if file is missing or an equal or older version is installed.
d	Reinstalls if file is missing or a different version is installed.
c	Reinstalls if file is missing or the stored checksum doesn't match the calculated value.

Parameter	Description
a	Forces all files to be reinstalled.
u	Rewrites all required user-specific registry entries.
m	Rewrites all required computer-specific registry entries.
s	Overwrites the start menu shortcuts. Doesn't overwrite desktop or favorite shortcuts.
v	Runs the repair from source installer executable and re-caches the local package.
{installer path}	The path of the installer executable.

- **Example**

```
msiexec /fomus oracle_documents_setup.msi
```

User interface options

Set the level of user interface displayed during install, uninstall, or repair by using /q with the options below.

- **Syntax**

```
msiexec /i|x|f {installer path} /q{n|b|r|f}
```

- **Parameters**

Parameter	Description
{installer path}	The path of the installer executable.
n	Displays no user interface.
b	Displays only a progress bar during the process.
r	Displays a reduced user interface with a modal dialog displayed at the end of the process.
f	Displays a full user interface with modal dialog displayed at the end of the process.

- **Example**

```
msiexec /i oracle_documents_setup.msi /qn
```

Deploy the MSI Installer Through Active Directory's Group Policy

You can use Microsoft Active Directory 2008 group policy to distribute the desktop app to computers.

1. From the Start menu, select **Control Panel**, then **Administrative Tools**.
2. Click Active Directory Users and Computers. Create an organization unit that includes all the computers where you want to install Oracle Content Management.
3. From the Start menu, select **Control Panel**, then **Administrative Tools** then **Group Policy Management Console**.
4. In the console tree, right-click **Group Policy Objects** in the forest and domain in which you want to create a group policy object.
5. Click **New**. Specify the name of the new group policy in the dialog box and click **OK**.
6. Select the newly created object and select **Edit** to open the Group Policy Management Editor.
7. Select and expand the Computer Configuration node.

8. Expand the Software Settings folder under the Computer Configuration node.
9. Right-click Software Installation and select **New**.
10. From the Shortcut menu, click **Package**.
11. Enter the path to the extracted MSI package. Ensure that the path is a UNC path and is accessible to all machines that the group policy is targeting.
12. Selected Assigned and click **OK**.
13. In the Properties dialog box, click **OK**.
14. Exit the Active Directory Users and Computers console.

Set Installation Defaults

The following registry entries can be set by an administrator on a machine where the desktop app is installed:

- **Default server URL:** [HKEY_CURRENT_USER\Software\Oracle\Oracle Documents\Account] "DefaultServer"="server_URL". Users can override the default server URL by adding a different server in their preferences.
- **Set the default server URL for users of a particular machine:**
[HKEY_LOCAL_MACHINE\Software\Oracle\Oracle Documents\Account] "DefaultServer"="server_URL"
- **Block upgrade prompts:** [HKEY_CURRENT_USER\Software\Oracle\Oracle Documents\Update] "SuppressDisplay"="true"
- **Block upgrade prompts for all users of a particular machine:**
[HKEY_LOCAL_MACHINE\Software\Oracle\Oracle Documents\Update] "SuppressDisplay"="true"

The HKEY_CURRENT_USER setting takes precedence over the HKEY_LOCAL_MACHINE setting.

4

Configure System Settings

Service administrators can configure settings for Oracle Content Management, including the size of files allowed for uploading, quota values for users, and other aspects of service use.

- [Configure General Settings](#)
- [Configure Domain Settings](#)
- [Configure Security Settings](#)
- [Configure Billing Settings](#) (This option shows only if you have Oracle Content Management running on Oracle Cloud Infrastructure (OCI).)
- [Configure Analytics Settings](#)
- [Configure Users Settings](#)
- [Configure Assets Settings](#)
- [Configure Sites Settings](#)
- [Configure SEO for Sites Settings](#)
- [Configure Documents Settings](#)
- [Configure Metadata Settings](#)

Configure General Settings

General settings include file and asset restrictions, customized branding information, settings to enable or disable email notifications, the default time zone, and more.

From the **General** page, you can perform the following actions:

- [Restrict File and Asset Types and Sizes](#)
- [Apply Custom Branding and URLs](#)
- [Enable or Disable Email Notifications](#)
- [Set the Default Locale Settings](#)
- [Purge Content Delivery Network \(CDN\) Cache](#)

Restrict File and Asset Types and Sizes

You can limit the types of files that can be uploaded, set file scanning options, and limit the size of uploaded files.

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.

On the **General** page, set the **File and Asset Restrictions**.

2. **Allow upload of files that can't be scanned:** If you want users to be able to upload files that can't be scanned to check for viruses, such as password protected or encrypted files,

enable this option. Only the first 4 GB of a file are scanned for viruses, though larger files can still be uploaded. This option is disabled by default.

 **WARNING:**

If you enable this option, it's at your own risk, and you bear all liability for any resulting damages. If you allow unscanned files to be uploaded, it might create risk to you or other users. While the Oracle Content Management interface will mark files that have not been scanned, this visual indicator will not be available in all interfaces, and users might not have any notice that one or more files were not virus scanned. Also, if a file doesn't pass virus scanning, it can't be downloaded through a public link.

Virus scanning can fail in the following cases:

- If a file (such as a zip file) contains folders that have a folder depth exceeding 10 levels.
- If a file that contains other files takes longer than 3 minutes to scan.
- If a single file inside a containing file is larger than 100 MB.

If virus scanning fails, the file will be marked as infected, deleted, and an email will be sent to the user who attempted to upload the file, notifying them.

If you enabled upload of unscanned files, additional options appear:

- **Attempt to create file previews for unscannable PDF files:** Oracle Content Management can attempt to create a file preview for encrypted and signed PDF files. There may still be circumstances where a preview can't be generated, for example, when a PDF is password protected.
- **Allow users to report false positives:** You can allow users to email an administrator if they believe a file has been falsely marked as infected. When you allow this option, you must also enter the email address of the administrator you want to be contacted regarding false positives. When this option is enabled and virus scanning fails, the email sent to the user who attempted to upload the file includes instructions on what to do if they believe the file is safe. The email will contain a link that will create an email, addressed to the specified administrator, with the checksum value of the file in the body of the email.

When the administrator receives the email and determines the file is safe for upload, they enter the checksum value from the email into the **False positive files to ignore** text box, separating each value with a new line. The virus scan results for these files will be ignored. After entering the checksum value, the administrator should ask the user to upload the file again.

3. **Maximum upload and sync file size:** Enter the maximum file size in megabytes.
4. **Block the following file types from upload and sync:** Enter a list of file type extensions, separated by commas, to block them from being uploaded. Enter the extensions excluding the period separator (for example, mp3).

Apply Custom Branding and URLs

You can customize Oracle Content Management by adding your own logo and other branding customizations; and changing the links that are available in the user menu to download apps, access help, and send feedback.

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. On the **General** page, under **Branding**, customize these elements:
 - **Corporate Branding Text:** Controls the text included in the user interface header and in invitation emails for new users.
 - To display “Content Management”, select **Default**.
 - To display custom text, select **Custom** and enter your text.
 - To display no text, select **Custom** and leave the text box blank.
 - **Corporate Icon:** Add an image to use as the favicon in browser tabs where the web client is open. The icon image should be 32 pixels wide by 32 pixels high.
 - **Corporate Logo:** Add an image to use as a logo for your customized service. The logo shows in the user interface header and notification emails to users. The logo image can't be bigger than 160 pixels wide by 24 pixels high. Larger images will be resized.
 - **Download Apps URL:** Enter the path to the location of the Oracle Content Management app installation files. This URL is used for the **Download Apps** link in the user menu.
 - **Help URL:** Enter the URL to the location of your help files. This URL is used for the **Help** link next to the user menu.
To take advantage of context-sensitive help, add `?ctx=cloud&id=cecshelp` to the end of your help URL (for example, `http://www.oracle.com/pls/topic/lookup?ctx=cloud&id=cecshelp`).
 - **Share Your Feedback URL:** Enter the URL to the location you want to send users to provide feedback. This URL is used for the **Share Feedback** link in the user menu.

Enable or Disable Email Notifications

Notifications alert users when certain events occur, like when someone is added to the instance, when a taxonomy changes, when someone flags you, or when someone creates a public link for a file or folder. Notifications are sent via email or a pop-up message in the desktop app. Administrators control whether *email* notifications are available in Oracle Content Management.

Important:

This setting enables or disables *all* email notifications from Oracle Content Management, including welcome emails when a user is added and document link emails when someone shares a file or folder.

To enable or disable email notifications:

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. On the **General** page, under **Notifications**, enable or disable the email notifications you want the server to send to users:
 - **Welcome Email Notifications**—If enabled, users will receive an email notification when they are added to the service. The welcome email is customized based upon the user's application role, such as administrator, enterprise user, or standard user. It includes the web address (URL) for the service and the user's account name and login information.
 - **Taxonomy Email Notifications**—If enabled, taxonomy users will receive an email notification when the taxonomy is promoted, published, removed from the repository, or deleted from Oracle Content Management. Taxonomy users are those that have access to a repository to which the taxonomy is associated. This allows users to take any actions necessitated by the taxonomy change. For example, a user may need to republish assets after a new version of the taxonomy has been promoted to update recategorized assets.
 - **All Other Email Notifications**—If enabled, users will receive an email notification for other events in Oracle Content Management, such as when they are flagged on an item or someone updates a file or folder.
3. Save your changes.

The default setting is to disable email notifications, but after an upgrade users can still receive email notifications when a folder is shared until the administrator changes the setting to **Enabled**, then back to **Disabled**, and re-saves the **General** page.

After email notifications are enabled, users can set email notification preferences. In the web client user menu, users select **Preferences** and choose **Notifications**.

Desktop app pop-up notifications are controlled in the desktop app by the user. In the desktop app, users open **Preferences**, and click **Choose Notifications**.

See Setting Notifications and Preferences in *Collaborating on Documents with Oracle Content Management*.

Set the Default Locale Settings

By default, the web interface time zone, language, and date format is set to match the web browser locale, but users can override this in their user preferences (on the **General** page). If users change their settings, the changes won't take effect until the next time they sign in. See Customizing Your Profile and Settings in *Collaborating on Documents with Oracle Content Management*.

The user interface time zone, language, and date format for the desktop and mobile apps are set automatically based on the user locale set for the operating system. You can't override this language setting. For example, if a user is running the desktop app on a Spanish version of Microsoft Windows, then the desktop app will also be in Spanish.

Service administrators can configure fallback settings to be used if no web browser locale setting is available.

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. On the **General** page, under **Time Zone and Language**, configure the following settings:
 - **Time Zone**—Set the default time zone.
 - **Language**—Set the default language.
 - **Date Format Locale**—Set the default date and time format.
 - **Start Day of the Week**—By default, the week is set to start on Sunday for scheduled publishing. However, you can change the start day as appropriate for your locale.

Purge Content Delivery Network (CDN) Cache

By default, Oracle Content Management sites and assets are delivered using a CDN for improved performance and security. If content isn't refreshed properly on your instance's domain, you can manually purge the CDN's cache to remove files or force an immediate update. This purge only works with the built in domain (.occdn.), not with custom vanity domains or friendly management domains set up through Oracle Support or third party CDNs.

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. On the **General** page, under **Content Delivery Network**, click **Purge**.
While the CDN cache is being refreshed, performance might be temporarily affected.

Additionally, you can configure the amount of time items are cached on the system administration [Assets](#) page.

Configure Domain Settings

You can specify a friendly management domain to make it easier for your users 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.

Before you can make use of the friendly management domain, you must [set up your domain, CDN, and DNS](#). Then you can configure domain settings.

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 you use a [custom sign-in page](#), your friendly management domain must also be configured as an [instance-level site 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.

Configure Security Settings

Security settings include enabling cross-origin resource sharing (CORS) and embedding content into other domains.

From the **Security** page, you can perform the following actions:

- [Enable Cross-Origin Resource Sharing \(CORS\)](#)
- [Embed Content in Other Domains](#)

Enable Cross-Origin Resource Sharing (CORS)

Cross-Origin Resource Sharing (CORS) allows a web page to make requests such as `XMLHttpRequest` to another domain. If you have a browser application that integrates with Oracle Content Management but is hosted in a different domain, add the browser application domain to Oracle Content Management's CORS origins list.

The REST APIs use CORS because they're called from JavaScript code that runs in a browser and the REST APIs and Oracle Content Management are hosted in different domains.

If your browser application needs to use a REST endpoint that doesn't support CORS or that needs service account credentials, you can instead register and use the endpoint via Oracle Content Management's integrated proxy service. See [Configure Proxy Service Settings](#).

In general, inline frames can host content if the protocol, domain, and port of the inline frame are identical to those for the content it displays. For example, by default, an inline frame on the page `http://www.example.com:12345/home.html` can host content only if the content's protocol is also HTTP, the domain is `www.example.com` and the port is `12345`.

However, if the application is in a different domain than Oracle Content Management, you need to add the application's host machine information to the list of front channel CORS origins, back channel CORS origins, or both.

- If the request is a cross-domain request (not originating from Oracle Content Management's domain) that will be served by Oracle Content Management, you need to add a front channel CORS origin. Front channel CORS is typically useful for custom application integration. For example, the REST APIs interact with the front channel.
- If the request is directly from Oracle Content Management to a connected client in another domain, you need to add a back channel CORS origin. For example,

Oracle Content Management can send back-channel messages (real-time updates) to an application.

- If an application gets both front-channel and back-channel communication from Oracle Content Management, you need to add the domain to both the front and back channel CORS origins lists.

The CORS settings apply to all Oracle Content Management calls (documents, social, and content as a service).

To allow resource sharing between a browser application that integrates with Oracle Content Management but is hosted in a different domain, perform the following steps:

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** menu, click **Security**.
3. Under **CORS (Cross-Origin Resource Sharing)**, enter the domains in the appropriate CORS origins text box in the format *http[s]://domainname.com*. Separate entries with a comma. For example, to enable CORS for an app on your server, enter a value similar to the following in both the **Back Channel CORS Origins** and **Front Channel CORS Origins** boxes:

```
https://www.example.com/app
```

If you use a custom domain URL, enter the custom URL as well.

4. When you are done, click **Save**.

Do not use * as an origin value; it allows access from all hosts.

Security measures vary between different browsers and different browser versions. See <http://www.w3.org/TR/UISecurity/>.

The CORS settings apply to all Oracle Content Management calls (documents, social, and content as a service).

Embed Content in Other Domains

You can display content from Oracle Content Management within other domains. For example, you might embed the Oracle Content Management web user interface into your own web applications to access folder and document management features inside your application.

To allow users to embed content, enable embedded content and add domains:

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** menu, click **Security**.
3. Under **Embedded Content**, select **Enabled**.
4. In the **Allowed domains** box, enter a list of permitted domains, separated by commas. Domains must be in the form *www.example.com*.
 - To restrict the domain to a particular port, include the port in the specification. For example, *www.example.com:12345*.
 - If you want to allow a domain that has multiple sub-domains, you can use the * wildcard character. For example, *www.example.** includes the domains *www.example.com*, *www.example.co.uk*, and so on.

To learn about embedding the Oracle Content Management web user interface, see [Embed the Web User Interface in Other Applications](#).

Configure Billing Settings

You can specify the limits at which you want to be notified for billing metrics and several other billing options. You can also see the current counts for billed items. These settings apply only to Oracle Content Management running on Oracle Cloud Infrastructure (OCI).

Note:

Oracle Content Management Starter Edition has a limited feature set, and therefore the billing settings are read-only. To take advantage of the full feature set, [upgrade to the Premium Edition](#).

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 **Billing**.
3. If you want to be notified when you get close to reaching certain billing limits, set the limits, and then enable **Send Administrative Warning**. You'll receive an email if you reach 90% of one of the specified billing limits. You can set the following limits:
 - **Asset Limit:** If you want to be notified when the total number of *standard* assets in your system exceeds a limit, enter that number here. If you don't want to set a limit, enter 0. This setting doesn't apply to archived or business assets.
The current number of *standard* assets and *archived* assets is shown next to the setting.

Archived assets are billed at 1/200th the cost of standard assets. For example, if you have 2,000 archived assets, that would be billed as 10 standard assets.

Business assets (those stored in business repositories) are billed at 1/100th the cost of standard assets. For example, if you have 5,000 business assets, that would be billed as 50 standard assets.
 - **File Limit:** If you want to be notified when the total number of files in your system exceeds a limit, enter that number here. If you don't want to set a limit, enter 0. The current number of files is shown next to the setting. Files are billed at 1/20th the cost of standard assets. For example, if you have 2,000 files in Documents, that would be billed as 100 standard assets.
 - **Storage Limit:** If you want to be notified when the total gigabytes of storage used exceeds a limit, enter that number here. If you don't want to set a limit, enter 0. The current amount of storage used is shown next to the setting.
 - **Enforce Limits:** If you want to restrict users from being able to create new objects (such as assets or files) when your selected billing limits are reached, enable this option. Users will receive an error when they try to create an object type that has reached its billing limit.
4. If you want to be notified when you get close to reaching a specified outbound data transfer limit, set the **Outbound Data Transfer Limit** at which you want to be

notified, and then enable **Send Administrative Warning**. If the total gigabytes of data transferred in an hour reaches 90% of the specified limit, you'll receive an email. If you don't want to set a limit, enter 0. Next to the setting, you see the current amount of data transferred during the current billing period for both origin traffic and content delivery network (CDN) traffic.

Enforce Limits: If you want to restrict users from accessing Oracle Content Management and any sites created in Oracle Content Management when your selected outbound data transfer limit is reached, enable this option. Users will receive an error when they try to access Oracle Content Management or any Oracle Content Management-created sites.

5. Set the **Billing Start Day**, the day of the month that your billing period starts.

Configure Analytics Settings

From the **Analytics** page, you can perform the following actions:

- [Enable or Disable Consumption Analytics](#)
- [Use Your Own Infinity Instance](#)
- [Enable or Disable Usage Analytics](#)

Enable or Disable Consumption Analytics

Oracle can collect information about which published assets are viewed or accessed on sites and portals. These consumption analytics appear in Oracle Content Management in the Analytics sidebar panel when viewing an asset.

To enable or disable collection of usage analytics:

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 **Analytics**.
3. Under **Consumption Analytics**, enable or disable consumption analytics.
4. Click **Save**, then refresh your browser for the saved setting to take effect for your session.

You can also enable site-level consumption analytics.

Use Your Own Infinity Instance

Oracle Content Management provides a default Oracle Infinity instance to collect consumption analytics, but you can use your own instance if you'd prefer.

To use your own Infinity instance:

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 **Analytics**.
3. Under **Consumption Analytics**, enable the setting to use your own Infinity service, and then enter the following information:
 - Infinity service account
 - Infinity service endpoint

- Infinity service token URL
 - Infinity service client ID
 - Infinity service secret
4. Click **Save**.

Enable or Disable Usage Analytics

Oracle Content Management now collects anonymous product usage information by default in order to make the product better. If you'd prefer, you can disable this feature on the instance.

To enable or disable collection of usage analytics:

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 **Analytics**.
3. Under **Usage Analytics**, enable or disable the setting.
4. Click **Save**, then refresh your browser for the saved setting to take effect for your session.

Configure Users Settings

You can configure Oracle Content Management specific user and group settings through the **Users** page of Oracle Content Management Administration: System.

For information on managing users or groups through your identity service, to perform tasks such as creating users or groups or changing users' roles, see [Manage Users, Groups, and Access](#).

From the **Users** page, you can perform the following actions:

- [Set the default resource role for new folder members.](#)
- [Enable or disable external users.](#)

You can perform additional on each of the tabs.

Tab	Actions
Search	<p>Use this tab to search for users and groups. After finding a user, you can perform the following actions:</p> <ul style="list-style-type: none"> • Synchronize the user's profile data. • Set whether conversation membership messages show by default. • Override storage quota for the user. • Transfer the user's file ownership to another user. • Override temporary storage quota (for upload and sync) for the user. • Revoke access to the user's linked devices. <p>After finding a group, you can change settings for the group, including whether the group can be used for sharing, whether they'll be sent notifications. You can also check whether the group is in sync.</p>
Administrators	Use this tab to view a list of users with the service administrator role. You can perform the same user actions that are available on the Search tab.
Deprovisioned Users	Use this tab to view a list of deprovisioned users and manage their files by transferring file ownership or deleting the content .
Group Sync	Use this tab to view and resynchronize groups that are out of sync .

Set the Default Resource Role for New Folder Members

Users in your organization can share folders with other users and assign them a resource role within the shared folder. The following roles are available:

- **Viewer:** Viewers can look at files and folders, but can't change things.
- **Downloader:** Downloaders can also download files and save them to their own computers.
- **Contributor:** Contributors can also modify files, update files, upload new files, and delete files.
- **Manager:** Managers have all the privileges of the other roles and can add or remove other people as members.

To change the default resource role:

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** menu, click **Users**.
3. Under **Members**, in the **Default role for new members added to folders** list, select the resource role users will be assigned by default when added to a folder.

Enable or Disable External Users

You can invite people outside of your organization, [external users](#), to collaborate on objects to which they're given access. After you enable external users with the setting described below, your existing users can invite new external users simply by adding them as members to folders, standard sites, or conversations by entering their email addresses. If there isn't already a user with that email address, Oracle Content Management will automatically provision a new external user.

- [Enable External Users](#)
- [Disable External Users](#) (and customize message users see if they attempt to invite unregistered users)

Enable External Users

To enable external users:

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** menu, click **Users**.
3. Under **Members**, next to **Allow members to invite external users to this service**, click **Enabled**. After enabling external users, new settings become available.
4. If you want to restrict the creation of external users from unwanted domains, enter the domains, separated by commas. Users from these domains can't be added as external users; they must instead be provisioned as internal users. Don't include the @ symbol.
5. Enter the number of days after which you want external user invitations to expire. If the invitation hasn't been accepted by the external user after this time, it will be removed from the system and the user will need to be invited again.
6. If you have a federated identity provider, you can redirect external user invitation requests through your own identity provider. Next to **Use External Identity Provider for new user invites**, click **Enabled**, and enter the required information for the associated outgoing webhook:
 - a. In the **Target URL** box, enter the target URL (endpoint) of the application that will receive user invitation notifications.
 - b. If the endpoint requires authentication, select the type of authentication, and then click **Details** to enter the authentication information. Oracle Content Management webhooks support the following options to configure authentication for the webhook notification receiver:
 - **None**: The receiver does not require authentication.
 - **Basic**: The receiver requires Basic Auth.
 - **Header**: The receiver requires a Secure Header.
 - c. To allow the endpoint to use a self-signed SSL certificate, select **Allow endpoint to use Self-Signed SSL certificate**. This allows the receiver to accept a self-signed SSL certificate. This is recommended only in testing or development.

- d. To authenticate the call between the external service and Oracle Content Management when event notifications are sent to the webhook endpoint, Oracle Content Management signs the event with a signature. The signature is a security token in hash-based message authentication (HMAC) code, using the standard SHA-256 HMAC cryptography. You can use the HMAC token to verify that the notifications are sent by Oracle Content Management.
To enable this option:
 - i. Select **Use Signature Based Security**. The receiver will then require the server and client authentication tokens to be equal.
 - ii. In the **Secret** box, enter a secret key that consists of alphanumeric characters (lowercase letters a-z, digits 0-9) and is 32 characters.
- e. Click **Save**.
- f. Set up a service to receive the webhook payload. When an external user invite event is triggered, Oracle Content Management sends a webhook payload similar to the following:

```
{
  "webhook": {
    "id": 1010,
    "name": "User Invitation webhook"
  },
  "event": {
    "id": "629314f9-593e-4bf5-bf06-519c1ca9b160",
    "name": "USER_INVITED",
    "registeredAt": "2023-03-14T10:04:41.381Z",
    "initiatedBy": "system"
  },
  "entity": {
    "id": "543c29a25d9bb753c4d2fd5e6326bd8e",
    "message": "Welcome to the the demo application!",
    "invites": [
      {
        "userName": "user1",
        "email": "user1.demo@oracle.com",
        "firstName": "user1",
        "lastName": "demo",
        "title": "Associate",
        "country": "IN",
        "additionalAttributes": {
          "key1": "value1",
          "key2": "value2"
        }
      },
      {
        "userName": "user2",
        "email": "user2.demo@oracle.com",
        "firstName": "user2",
        "lastName": "demo",
        "title": "Associate",
        "country": "IN",
        "additionalAttributes": {
          "key1": "value1"
        }
      }
    ]
  }
}
```

```
}  
  }  
} }
```

- g.** Create a new user in your identity provider, based on the webhook payload.
 - h.** Sync the user to IDCS, assigning the user the external user application role (CECEExternalUser). Oracle Content Management then syncs the user, completing the external user invitation process.
- 7.** Click **Save** to save your changes.

Disable External Users

To disable external users:

- 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** menu, click **Users**.
- 3.** Under **Members**, next to **Allow members to invite external users to this service**, click **Disabled**.
- 4.** When a user attempts to invite an unregistered user when external users are disabled, they'll see a message saying they can't invite external users. You can leave the default message or create a custom message. To create a custom message, select **Custom**, and then enter the message you want to display.
- 5.** Click **Save** to save your changes.

Note:

If you want to test your custom message, you must reload the page after saving your changes.

Search for Users and Groups

On the **Search** tab, you can search for users and groups by entering part of the user or group name, display name, or email address in the text box, and then clicking **Search**. Alternatively, you can view a list of all users with the service administrator role on the **Administrators** tab, or a list of all users that have been deleted on the **Devisioned Users** tab.

Users

On the Search and Administrators tabs, each user entry includes the following:

- The user's display name
- Their user name
- Their email address
- Their *verification status*.
User accounts are verified using one of the following methods:

- The user was located in an external account database such as an LDAP (Lightweight Directory Access Protocol) directory service directory.
- An email was sent to the user, the user clicked the link in that email to verify their identity, and then they signed in.

Click the user's display name or the **Edit** button to view or edit the user's properties. From there, you can see additional information and perform additional actions:

- View the user's display name, ID, user name, email, verification status, when they were created and last modified, when they last connected and disconnected.
- [Synchronize the user's profile data.](#)
- View whether the user has the service administrator role.
- [Set whether conversation membership messages show by default.](#)
- [Override storage quota for the user.](#)
- [Transfer the user's file ownership to another user.](#)
- [Override temporary storage quota \(for upload and sync\) for the user.](#)
- [Revoke access to the user's linked devices.](#)

Groups

On the Search tab, each group entry includes the following:

- The group's name
- The group type (PUBLIC_OPEN or PRIVATE_CLOSED)
- The group origin (CEC or IDP), indicating whether the group was created in Oracle Content Management (CEC) or in your identity provider (IDP)

Click the group's name or the **Edit** button to view or edit the group's properties. From there, you can see additional information and perform additional actions:

- View the group's name, ID, group type, and origin type.
- [Change settings for the group](#), including whether the group can be used for sharing, whether they'll be sent notifications. You can also check whether the group information is in sync.

Synchronize User Profile Data

After you add users and assign application roles, you can synchronize those changes with the Oracle Content Management server right away. If you don't synchronize user profile data, it may take up to an hour for the changes to get propagated.

You can replace a user's existing profile information with the information from your identity store:

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** menu, click **Users**.
3. Search for the user whose profile data you want to sync, click **Edit** next to the user's name, and click **Sync Profile Now** on the user details page.

Display Conversation Membership Messages for a User

Configure whether to show the user conversation membership messages (when a person is added to a conversation and who added them) by default. A user can change this display setting for any stand-alone conversation.

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** menu, click **Users**.
3. On the Search tab find the user whose default you want to set. Enter part of the user name, display name, or email address in the text box and click **Search**.
4. Click **Edit** next to the user's name.
5. Select the **Show Conversation Membership Messages by Default** check box and click **Save**.

Override Storage Quota for a User

You can [set a default quota](#) for the amount of storage space that a user is allocated. If you need to override the default for a particular user you can do so using the following steps.

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** menu, click **Users**.
3. Search for the user whose settings you want to override and click **Edit** next to the user's name.
4. In the **User Quota** box, enter the quota amount in gigabytes, and then click **Save**. You can see how much storage the user has used next to **Storage consumed**.

Transfer File Ownership

When people leave your organization or change roles, you might want to assign their files and folders to someone else and add their storage quota back to the total quota you have available for assignments. You can assign a person's entire library of content to someone else. The content appears as a folder in the new user's root folder. All of the sharing actions, such as members and public links, remain intact.

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** menu, click **Users**.
3. Find the user whose files you want to transfer using one of the following methods:
 - To find an active user, on the **Search** tab enter part of the user name, display name, or email address in the text box and click **Search**. Open the user properties by clicking the user name or clicking **Edit** next to the user.
 - To find a deprovisioned user, click the **Deprovisioned Users** tab. You see a list of all users who have been removed from your organization's system, sorted by name. This list is refreshed on a regular basis, but you can also update it manually by clicking **Sync Profile Data**.

To download a CSV file of all deleted users, click **Export Deprovisioned Users**.

4. Click **Transfer Ownership**. For active users, the button is at the bottom of the properties. For deprovisioned users, click the button next to the user you want.
5. Enter part of the user name, display name, or email address of the person who will receive the content and click **Search**.
6. Select the user you want to transfer the content to. A message shows that the content will increase the recipient's quota by the amount of content being transferred. It also shows you how much storage will be released back into the total quota you have available.
7. Click **Transfer**. The content is transferred and the list shows that the deprovisioned account is gone.

Alternatively, for deprovisioned users, you can delete the content. On the **Deprovisioned Users** tab, next to the user whose content you want to delete, click **Delete Content**.

Users can also transfer ownership of their own folders.

Override Temporary Quota for a User

By default the maximum upload and sync file size is 2GB (set on the [Documents](#) page). To ensure more than one 2GB file can be uploaded simultaneously, the default temp storage quota for users is 5GB. If your maximum file size is set higher, the temp storage quota for users is automatically increased to 2.5 times that amount (for example, if the maximum file size is set to 10GB, the temp storage quota for users is set to 25GB).

This temp storage quota setting should suffice for normal circumstances, but if you need a particular user to have a higher Temp Storage quota, you can override the setting.

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** menu, click **Users**.
3. Search for the user whose settings you want to override and click **Edit** next to the user's name.
4. In the **Temp Quota** box, enter the quota amount in gigabytes, and then click **Save**.

Revoke Access to Linked Devices

Users can revoke access to one of their linked devices if they change devices or lose one, but there might be cases where you, as an administrator, need to perform this action. When you revoke access to a linked device, the user's sign-in session is ended. If you or anyone else tries to access Oracle Content Management from the device, the account is signed out and all local content stored on the device for that account is deleted.

Revoking access for the device affects only one account, so if the person has multiple user accounts, you need to revoke access separately for each user account to block all access to Oracle Content Management and delete all local content stored on the device.

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** menu, click **Users**.
3. Search for the user whose device access you want to revoke and click **Edit** next to the user's name.

4. Under **Linked Devices**, click **Revoke** next to the appropriate device.

Change Settings for Groups

You can change the sharing and notification settings for groups and resynchronize groups.

To change settings for groups:

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** menu, click **Users**.
3. Search for the group whose settings you want to change, then click **Edit** next to the group's name.
4. If you don't want the group to be used for sharing, so that users can't add the group to an object (such as a document or a site), select **Cannot be used for sharing**.
5. If you don't want this group to be sent notifications, select **Will not be sent notifications**.
6. To check if the group is in sync, click **Check Synchronization Status**. A message will show the status.
If you need to resynchronize the group information, click **Synchronize**.

View and Resynchronize Groups Out of Sync

If you believe a group in Oracle Content Management is out of sync, you can see a report of the mismatches and manually resynchronize the group. For example, if a user can't access an item to which they should have access through group membership, the group may be out of sync.

To view group sync mismatches:


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** menu, click **Users**.
3. Click the **Group Sync** tab.
4. Search for the group you think is out of sync, then click **Check Synchronization Status**.
5. If the report shows that the group in Oracle Content Management is out of sync, click **Synchronize**.

 **Note:**

Groups that are restricted from sharing and groups that include only site visitors can't be synchronized.

Configure Assets Settings

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** menu, click **Assets**.
3. Configure the **Maximum number of custom renditions per asset**. The default is 20.

 **Note:**

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

4. Configure the **Default asset caching age** to control the amount of time a public asset is cached on the content delivery network (CDN) before a request is made to the server for new content. The default is 15 minutes.
The default cache time balances the need for fresh content with the performance benefits of caching. Decreasing cache time ensures that new content is made available to customers faster, but it minimizes any performance benefits that caching may provide. If you work with largely static content, you can increase the cache time, improving delivery performance.

This setting doesn't impact assets published in secure channels. Those assets won't be cached to avoid private content from being stored on CDNs or client devices.

Alternatively, you can use the "&cb=xxx" URL parameter to make individual assets cacheable. Replace xxx with a random number to create a unique 15-day cache window. Responses to this request parameter include a Cache-Control header with the max-age value of 15 days. If you need to refresh the content before the cache window expires, include a new random number with new requests.

You can [manually purge the CDN cache](#) to remove files or force an immediate update.
5. Configure the **Video token default expiry time**. The default is 8 hours.
6. If [Sauce Video](#) is enabled in your instance, you can select whether everyone or no one can see the Sauce Video link in the navigation.

Configure Sites Settings

You can specify who can create, share, and use sites functionality, which lets users design, build, publish, and manage websites that are hosted in Oracle Cloud.

Sites functionality in Oracle Content Management unites content, collaboration, and creativity in one user interface. You can seamlessly grab and reuse content to build sites, your site content is kept under control, and shared content makes collaboration between and among groups easier than ever.

 **Note:**

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

From the **Sites** page, you can perform the following actions:

- [Allow Sites to Be Created](#)
- [Enable Governance for Sites](#)
- [Set Minimum Security for Online Sites](#)
- [Allow Sharing of Sites and Themes](#)
- [Limit Site, Template, or Component Creation to Site Administrators](#)
- [Add Analytics Tracking Code to Sites](#)
- [Set Custom Cache Control Headers for Compiled Sites](#)
- [Set a Compilation Endpoint URL](#)
- [Automatically Handle Expired Sites](#)
- [Install Default Site Templates](#)
- [Enable Custom Sign-In](#)
- [Configure Vanity Domains](#)

Allow Sites to Be Created

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** menu, click **Sites**.
3. Next to **Allow sites to be created**, select **Enabled** to allow your service users to create sites. When you enable the ability to create sites, you allow all users to create templates and sites.

If you disable site creation, users can still see and work with templates and other folders in the hierarchy. Users can also still work with an existing site if the site is shared with them. They can view, edit, and manage the site, depending on their role.

When you enable sites functionality, users have the ability to publish any content they have access to, including confidential information. You might want to limit your users to creating only secured sites, so that users have to sign in before they can see the site content. For even more security, you can limit site creation to administrators.

See Creating and Managing Sites in *Building Sites with Oracle Content Management*.

Enable Governance for Sites

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** menu, click **Sites**.

3. Next to **Enable governance for sites**, select **Enabled** to simplify and accelerate site delivery for business users, who are not site administrators, while giving site administrators an easy way to control and track sites from a centralized location. With Governance enabled:
 - Developers can populate a template catalog with a set of site templates for the needs of different lines of business. They can apply policies regarding the type of security new sites must adhere to as well as whether new sites require approval.
 - Business users have the ability to rapidly request new sites with required approvals and automated provisioning,
 - Site administrators can manage all sites from one place regardless of who created and deployed the site. They can monitor site status and change status for any deployed site.

See Understand Site Governance in *Building Sites with Oracle Content Management*.

Set Minimum Security for Online Sites

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** menu, click **Sites**.
3. Next to **Minimum security for online sites**, choose one of the following options from the drop-down list:
 - **Specific service users**—Only selected service users (the default setting) Only authenticated users who are explicitly selected as members can access the published site. You can further limit the selected users to only Oracle Content Management users.
 - **Specific cloud users**—Only selected cloud users
 - **Service users**—All service users Only authenticated *service users*, *standard users*, or *enterprise users* can access secure sites. This excludes authenticated *visitors*.
 - **Cloud users**—All cloud users who can sign in to your domain.
 - **Everyone**—Anyone without signing in

For information about specifying who can access public sites, see Changing Site Security in *Building Sites with Oracle Content Management*.

Allow Sharing of Sites and Themes

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** menu, click **Sites**.
3. Next to **Allow sharing of sites and themes from UI**, select **Enabled** to allow users to share sites and themes with other Oracle Content Management users. If you disable sharing, users can still create and publish themes and sites. Users with the manager role for the theme or site (the owner or an administrator) can edit or publish the theme or site.

If you disable sharing, users won't be able to share sites and themes through the user interface. It's still possible to implement sharing of theme and site folders using the Oracle Cloud REST API for Content Management.

Limit Site, Template, or Component Creation to Site Administrators

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** menu, click **Sites**.
3. Next to **Only site administrators can create sites**, select **Enabled** to restrict the ability to create sites to users with the site administrator application role.
4. Next to **Only site administrators can create templates**, select **Enabled** to restrict the ability to create templates to users with the site administrator application role.
5. Next to **Only site administrators can create components**, select **Enabled** to restrict the ability to create components to users with the site administrator application role.

Add Analytics Tracking Code to Sites

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** menu, click **Sites**.
3. Optionally, add JavaScript tracking code to sites for web analytics tracking, making it easier to integrate with external analytics providers like Google, Adobe, or Oracle Infinity. Adding a snippet here will propagate it to all *new* sites and pages. You can also add the snippet to directly to individual sites or pages or customize the propagated snippet as necessary. Click **Edit**, then add a web analytics tracking snippet like the following one for Google Analytics:

```
<!--Global site tag (gtag.js - Google Analytics -->
<script async src="https://www.googletagmanager.com/gtag/js?
id=UA-85172963-3"></script>
<script>
window.dataLayer = window.dataLayer || [];
function gtag(){dataLayer.push(arguments);}
gtag('js', new Date);

gtag('config', 'UA-85172963-3');
</script>
```

Click **Done**, and then click **Save**.

The tracking snippet here will be available in a site's settings, but a site manager must enable the snippet on the site, publish the change, and, if necessary, bring the site online before analytics are collected for that site. Site managers can also customize the snippet in the site settings or page settings.

After the site manager publishes the site and brings it online, you can view the tracked analytics data on the vendor's site, such as Google Analytics. If you used a snippet for Oracle Infinity analytics tracking, go to the Oracle Infinity home page and click **Analytics** to view the data and select or create reports.

Set Custom Cache Control Headers for Compiled Sites

If your company uses compiled sites, you can set custom cache control headers that will be used by default for any compiled sites created on your instance.

By default, compiled sites are cached on a user's browser for 300 seconds (5 minutes). However, you can change this default for your instance through the administrative settings. Site developers can also change the settings for a specific site in the site properties.

To change the default cache settings for compiled sites, perform the following steps:

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** menu, click **Sites**.
3. To change the default cache settings for compiled sites, edit the values shown below in bold. Values are in seconds.

```
Cache-Control: max-age=300  
Edge-Control: !no-store,max-age=1800,downstream-ttl=1800
```

- `Cache-Control` determines how long a page is cached on a user's browser. The default is 300 seconds (5 minutes).
- `Edge-Control` is an Akamai-specific setting. If your instance doesn't use Akamai, this setting has no effect.
 - `!no-store` indicates that this setting should override the corresponding Akamai caching configuration for the property.
 - `max-age` determines how long Akamai should cache this page. The default is 1800 seconds (30 minutes). During that time, Akamai will fulfill requests for the page without requesting the page from Oracle Content Management.
 - `downstream-ttl` tells Akamai to send a "Cache-Control: max-age" header with its response to client browsers, instructing those browsers to cache the page for the allotted time. The default is 1800 seconds (30 minutes).

After changing the settings, click **Save**.

To return to the default values, click **Show defaults**, and then click **Save**.

Set a Compilation Endpoint URL

If you're using a Site Compilation Service, you need to register the compilation endpoint URL with Oracle Content Management so that sites can be compiled when they're published.

For details on setting up the Site Compilation Service, see *Set Up a Site Compilation Service* in *Integrating and Extending Oracle Content Management*.

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** menu, click **Sites**.
3. In the **Compilation Endpoint URL** box, enter the fully-qualified URL you want to be registered with the server, then click **Test** to validate the endpoint.

Automatically Handle Expired Sites

If site governance is enabled, you can have expired sites automatically taken offline and even deleted.

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** menu, click **Sites**.
3. Under **Site Expiration**, if you want sites to be taken offline automatically when they expire, enable **Automatically take expired sites offline**.
4. If you also want expired sites to be deleted, enable **Automatically delete expired sites**, and enter the number of days you want to wait before they're deleted. You can see the list of deleted sites by clicking **Sites** in the navigation menu, then selecting **Trash** from the Sites menu.

See Understand Site Governance in *Building Sites with Oracle Content Management*.

Install Default Site Templates

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** menu, click **Sites**.
3. If you want to install a set of default site templates to help your users get started building their own sites, click **Install default site templates**. This option installs the templates shipped with Oracle Content Management. If this is the first time you have installed the templates, new folders are created for the template, its associated theme, and any custom components included in the template. If these templates were installed previously, installing them again will overwrite the associated template, theme, and custom component files, including any sharing settings you have set. After you install the templates, share the templates with the intended users.

Until you share a template, it can't be used by anyone else. When you share a template with users for the first time, the associated theme and any associated custom components are automatically shared with the identified users, who are given the Downloader role for the theme and components to ensure that they are available if the users create sites from the template. Subsequent changes in the template to the role for one or more users do not update the sharing information for the associated theme or custom components.

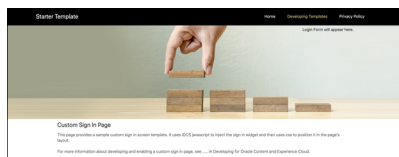
Enable Custom Sign-In

Oracle Content Management provides a custom sign-in feature that enables you to use a site page as a custom sign-in page. Once configured, this will become the sign-in page for Oracle Content Management and all secure sites.

 **Note:**

- The custom sign-in feature is available only in Oracle Content Management instances that are running on Gen 2 Oracle Cloud Infrastructure (OCI) natively (that is, using the Oracle Cloud Console to manage service instances).
- If your instance [uses Oracle Identity Cloud Service \(IDCS\)](#), IDCS comes with an embedded sign-in page. IDCS provides a way of customizing the sign-in page. However, if you need to personalize the look and feel of the sign-in page beyond what the branding feature supports, IDCS provides an [Authentication API](#) that enables you to develop your own customized sign-in page.

The starter template comes with a sample sign-in page with a custom sign-in component to help you get started.



Steps to Use Custom Sign-In

Here's an overview of what you need to do:

1. Create a public site from the starter template.
2. Use Site Builder to edit the site's sign-in page.
3. Publish the custom sign-in site and bring it online.
4. If you've configured a [friendly management domain](#), and you want your custom sign-in site to use the same domain, you must also have this domain set as an [instance-level site vanity domain](#).
5. Enable custom sign-in in the administrative user interface (described below).

 **Note:**

When using a custom sign-in site with a Friendly Management Domain, you may use the original or short-path option with your instance-level site vanity domain. However, if you switch between original and short-paths you must reset the custom sign-in page and then re-enable it. This step is required for the authentication redirection process to use the correct site paths.

Enable Custom Sign-In

After your site is published and online, you need to enable it for custom sign-in.

1. If you're not already signed in as a user that has access to the System administration, sign in to Oracle Content Management as an administrator.
2. Click **System** in the Administration area of the navigation menu.

3. In the **System** menu, click **Sites**.
4. Under Custom Sign In, click **Enabled**, select the site and page you created for custom login, and then click **Save**.

! **Important:**


Make sure you select the correct page. If you sign out or your session ends, you won't be able to sign in directly to Oracle Content Management again. You'll need to sign in to Oracle Cloud, and then navigate to your Oracle Content Management instance. Then you can go back to the Sites and Assets page and correct the issue.

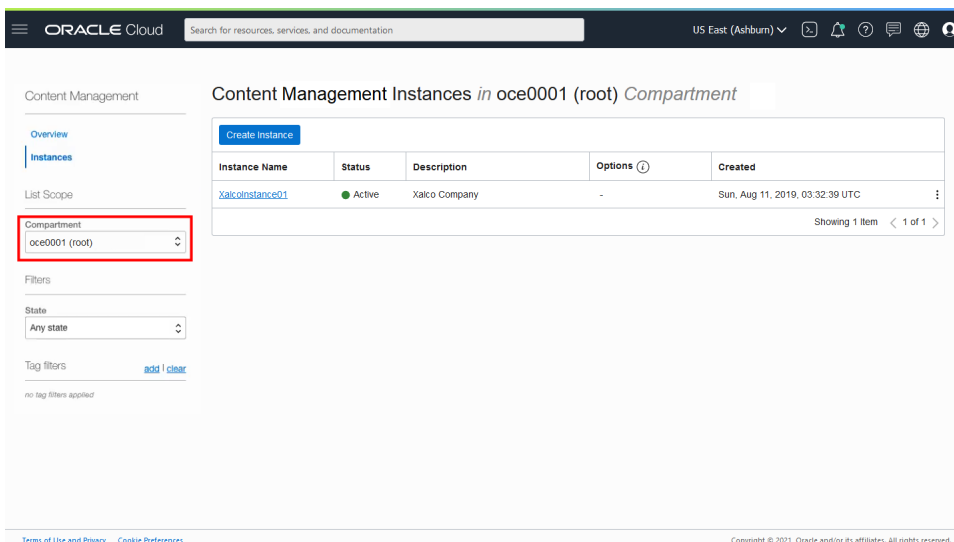
Once you configure the custom sign-in page, the associated site can't be taken offline or unpublished.

You'll probably want to inform your users that they'll see a new sign-in page, so they don't worry that it's a phishing scheme or something similar.

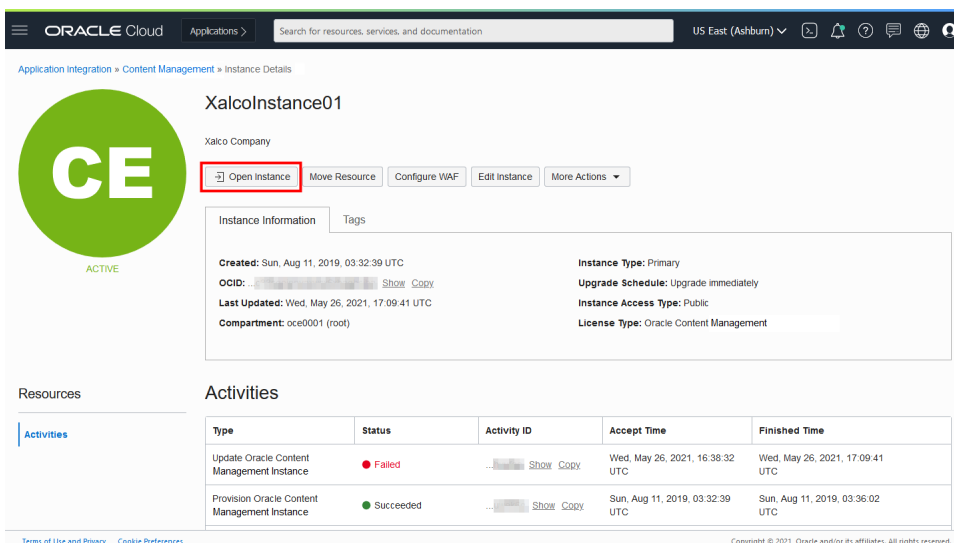
Reset Custom Sign-In

You can reset the sign-in page to the one that comes out-of-the-box in the following ways:

- From Oracle Content Management:
 1. If you're not already signed in as a user that has access to the System administration, sign in to Oracle Content Management as an administrator.
 2. Click **System** in the Administration area of the navigation menu.
 3. In the **System** menu, click **Sites**.
 4. Under Custom Sign-In, click **Disabled**, and then click **Save**.
- If you can't sign in to Oracle Content Management because the sign-in page was configured incorrectly, you can reset the sign-in page in one of two ways:
 - If you sign in to Oracle Cloud Infrastructure (OCI) using single sign-on (SSO), follow these steps to reset the sign-in page:
 1. Sign in to [Oracle Cloud](#) as a Service Administrator user (a user that has access to the System administration in Oracle Content Management).
 2. In the Oracle Cloud Console, click  to open the navigation menu, expand **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 for your Oracle Content Management instance.



4. Click your service instance to open it.
5. Click **Open Instance**. This opens your Oracle Content Management instance without the need to sign in.



6. Click **System** in the Administration area of the navigation menu.
 7. In the **System** menu, click **Sites**.
 8. Under Custom Sign-In, click **Disabled**, and then click **Save**.
- If you don't sign in to OCI using SSO, open a support ticket with Oracle Support to reset the sign-in page.

Configure Vanity Domains

You can set up vanity domains to access sites created with Oracle Content Management. Before you can configure vanity domains and select a default in Oracle Content Management, you must [perform some preliminary steps](#).

To configure instance-level vanity domains and set a default:

1. If you're not already signed in as a user that has access to the System administration, sign in to Oracle Content Management as an administrator.
2. Click **System** in the Administration area of the navigation menu.
3. In the **System** menu, click **Sites**.
4. Under **Vanity Domain Configuration**, click **Manage Vanity Domains**.
5. In the Manage Vanity Domains dialog, enter the domain (for example, example.com). To register another domain, click **Add Domain**. When you're done, click **Save**.
6. If you want sites created in Oracle Content Management to use a default domain, select it in the drop-down list.
7. If you want short URL paths (for example, www.myexample.com/MySiteName) to be displayed in your sites rather than the full paths (for example, your-instance.cec.oraclecorp.com:8080/site/authsite/MySiteName), select **Enabled**. If you select to use short paths, you'll need to [configure additional CDN settings](#).
8. When you're done, click **Save**.

Site administrators can [override the default vanity domain for a site](#).

Configure SEO for Sites Settings

SEO for sites settings include settings to enable or disable prerendering of sites and for configuring additional user agents.

From the **SEO for Sites** page, you can perform the following actions:

- [Enable Prerender](#)
- [Configure User Agents](#)

Enable Prerender

If you want to prerender pages so they're read correctly by web crawlers or other bots, enable the prerender service.

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** menu, click **SEO for Sites**.
3. Under **Prerender Service**, select **Enabled**.

Configure User Agents

If you need user agents that aren't defined out-of-the-box, you can define them.

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** menu, click **SEO for Sites**.
3. Under **Configure User-Agents**, enter additional user agents, separated by commas.

Configure Experiences Settings

Oracle Content Management provides a way to connect content repositories and publishing channels to experiences developed and managed outside of Oracle Content Management and automatically trigger deployments based on content changes or published status. Content providers can leverage the advantages of repository asset management such as powerful tools to organize, retrieve, translate, collaborate on, approve, and publish content. Experience developers can work with tools they have and configure experiences to automatically build based on changes to content in an associated repository or publishing status of content in an associated publishing channel.

 **Note:**

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

To enable experiences:

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** menu, click **Experiences**.
3. Select **Enable** to allow enterprise users with the developer role to create experiences.

Configure Documents Settings

Documents settings include user quotas and link settings.

 **Note:**

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

From the **Documents** page, you can perform the following actions:

- [Restrict File and Folder Deletions](#)
- [Set User Quotas and Manage Storage Space](#)
- [Set Default Link Behavior](#)

Restrict File and Folder Deletions

You can restrict who is able to delete a file or folder, allowing only the file creator and folder managers to do so.

To restrict file and folder deletions:

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** menu, click **Documents**.
3. Under **File and Folder Restrictions**, select **Enabled** to limit deletion to only the file creator and folder managers.

Set User Quotas and Manage Storage Space

You can set quotas for the amount of storage space that a user is allocated. You can also save storage space by limiting the length of time that items remain in the trash before being permanently deleted and limiting the number of versions to keep before older version are deleted.

To set quotas and storage space:

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** menu, click **Documents**.
3. Under **Quota**, set these defaults:
 - **Default quota per user:** Specify the amount of storage space allotted for each new user in gigabytes. Enter a value between 1 and 999.

Note:

To view the amount of storage used by an existing user and override their storage quota, view the [user's settings](#).

- **Maximum days to keep files and folders in trash:** Specify the number of days that files are kept in the trash before they are permanently deleted. If you set this option to "0", the files will be deleted the next time the purge job runs. The purge job runs once a day.
- **Allow unlimited versions:** If you want to limit the number of versions kept, select **Disabled** and specify the **Maximum number of versions per file**. When the maximum number of versions is exceeded, older versions will be deleted.
- **Permanently delete cleaned up revisions:** By default, the oldest file revisions are immediately deleted when the maximum number of versions is exceeded. If you want to instead move the older versions to the trash, disable this option.

Set Default Link Behavior

Administrators can determine how public links will be handled throughout the entire service. This kind of link lets a person use the files in a folder but limits access to any other folders. If you send a public link to a file, the person can access only that one file.

To set link behavior, complete the following steps:

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** menu, click **Documents**.
3. Under **Links**, configure the following settings:
 - **Allow public links to files and folders:** If you want users to be allowed to create public links and share those links with others, select **Enabled**.
 - **Default Share Link Type:** If you enabled public links, specify what the default is for shared links—members only or public. You might want to leave this setting as **Members Only** so that users don't accidentally create public links.
 - **Access Options:** If you enabled public links, specify whether users can send public links to anyone (**Anyone**) or only to those people who have an Oracle Content Management account (**All Registered Users**).
If you allow public links to be sent to anyone, you reduce security because users could share confidential content with people outside your company. Set this to **Anyone** only if you are certain this is acceptable practice for your company.
 - **Show warning to users when they create public links:** If you want to alert users when they are creating public links, select **Enabled**.
 - **Customize warning message to display when users create public links:** If you enabled the warning message, you can set your own message, cautioning users about the use of public links. Select **Enabled** and enter your custom message.
 - **Maximum role available for public links:** Select the highest role your users can assign when they create a public link. This can help you control who can add or download content from your service.
 - **Default role for new public links:** Select the role that will be assigned by default when your users create a public link. This role can't allow more permissions than the role you set for the **Maximum Role**.
 - **Enforce expiration for all public links:** When a public link is created, the link is given a name and an optional expiration date and access code. If you want to ensure that all public links have an expiration date, select **Enabled** and set a maximum expiration time.
 - **Set maximum expiration time:** If you enforce expiration for public links, enter the maximum number of days those links are valid until they expire. This helps you ensure that the links that are created are ones that are in use, and no links remain valid and unused for a long period of time. If a link does expire, the owner of the link can recreate it and send it again if needed.
 - **Show banner warning that public links or external users have access to an object:** By default, users see a banner warning when they use an object that is available through public links or to external users. To hide this warning, select **Disabled**.

Configure Metadata Settings

You can add metadata to documents so that users can quickly categorize files and folders with additional descriptions. For example, perhaps you need to track the effective date of a policy. You could create a metadata group called "Effective" that lists fields such as start date and end date. You could even add a list of reasons to choose from if the policy is no longer effective.

**Note:**

Metadata is only for documents, not assets.

You, as service administrator, create metadata groups and fields, and enable them to show up in the user interface for files and folders. Then people with the Owner, Manager, or Contributor role apply the metadata to files and folders. People with the Viewer or Downloader role can view any metadata that is set.

To configure metadata:

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** menu, click **Metadata**.
3. Click **New Group** to create a group of fields associated with the metadata.
4. Enter a name for the metadata group.
5. Click **Add** to create a new field. Add fields in the order you want them to appear to users.
6. Select the type of field you want to create (**Text**, **Date**, **Number**, or **Boolean**). The following restrictions apply to the field values users can enter:
 - **Text**: Maximum of 1,000 characters. Can't include # * & | ? < > ^ ; { } () ' = + \
 - **Number**: Maximum of 15 characters. Must be a whole number, no decimals.
7. Enter a label for the field.
8. If you want to set a default value for the field, enter the **Default Value**.
9. For text fields, you can add a **Hint** to the field to clarify what the field is for.
10. If you want to set a value that users can't change, enter the **Default Value**, then set **Read-Only** to **Yes**.
11. When you're done, click **Add**.

To see how your metadata fields will appear to users, click the metadata group to expand it.

To add new fields, edit fields, or delete the metadata group, click **...**.

When you're done configuring metadata, select **Enabled** to make them appear in the user interface for files and folders.

5

Manage Users, Groups, and Access

Securing your system is an ongoing process as people join or leave your company and as needs change and your system grows.



Note:

The groups discussed in this chapter are created in Oracle Cloud Infrastructure (OCI) or imported into OCI from your identity provider. Your users can also create groups in Oracle Content Management that can be used for sharing and collaboration.

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 [Manage Users, Groups, and Access in a Region with Identity Domains](#). In other topics, follow the steps marked **IAM**.
- If your region *hasn't* been updated, follow the steps in [Manage Users, Groups, and Access in a Region without Identity Domains](#). In other topics, follow the steps marked **IDCS**.

All remaining topics apply to both scenarios.

- [External Users](#)
- [Set the Default Resource Role for New Folder Members](#)
- [Synchronize User Profile Data](#)
- [Display Conversation Membership Messages for Users](#)
- [Override Storage Quota for a User](#)
- [Transfer File Ownership](#)
- [View and Resynchronize Groups Out of Sync](#)
- [Override Temporary Quota for a User](#)
- [Revoke Access to Linked Devices](#)
- [Change Settings for Groups](#)

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.

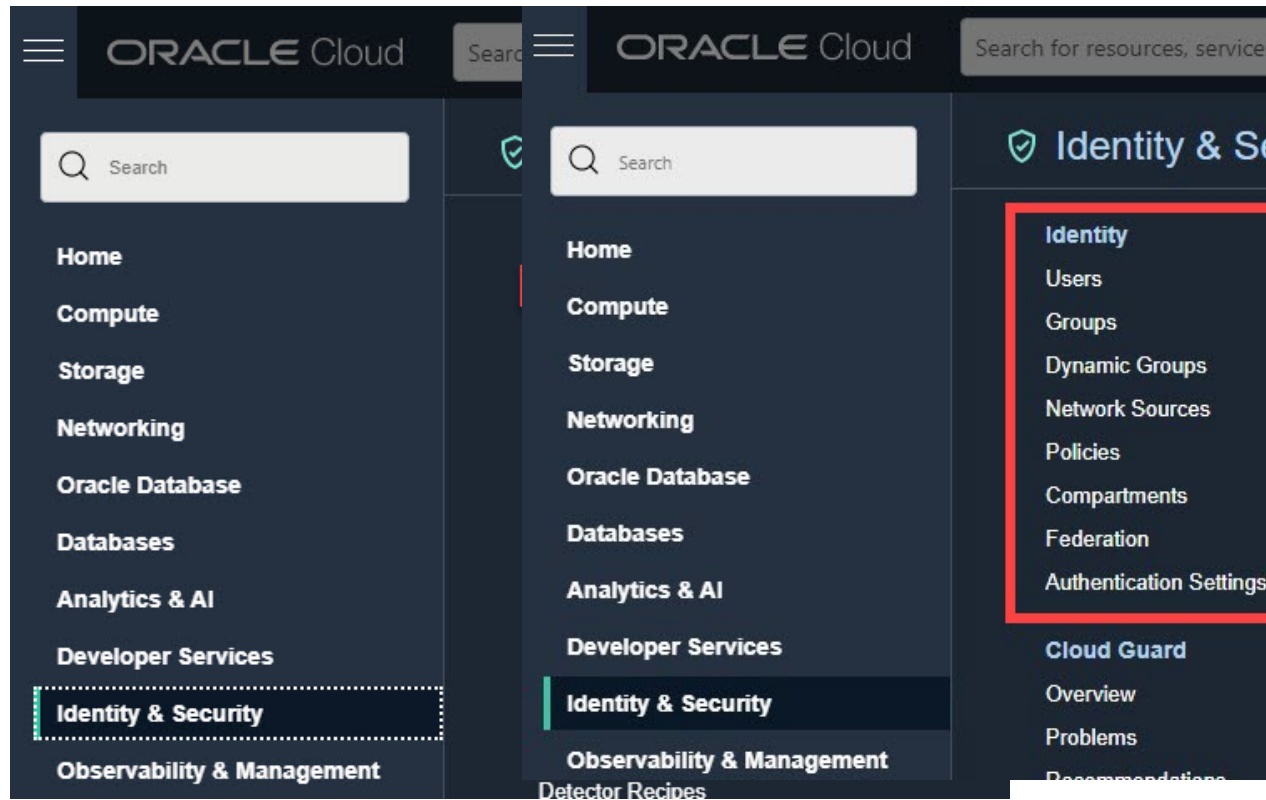
Depending on whether your region uses IAM identity domains or not, you'll use different documentation to manage users, groups, and access. To see if your region includes IAM identity domains, sign in to your [Oracle Cloud](#) account as a cloud account administrator. In the navigation menu, click **Identity & 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



IAM (updated)	IDCS (not updated)
<p>If your region has been updated, use the following documentation:</p> <ul style="list-style-type: none">• Deploy OCM in a Region with Identity Domains• Manage Users, Groups, and Access in a Region with Identity Domains• In other topics, follow the steps marked IAM. <p>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</p>	<p>If your region hasn't been updated, use the following documentation:</p> <ul style="list-style-type: none">• Deploy OCM in a Region without Identity Domains• Manage Users, Groups, and Access in a Region without Identity Domains• In other topics, follow the steps marked IDCS.

External Users

External users may be people outside of your organization that can collaborate on objects to which they're given access, but they can't be assigned the manager role. This safely limits their ability to create and remove content, similar to how visitors can sign in and use specified secure sites. This allows you to work with outside contributors such as translators and partners.



Note:

External users aren't supported in [private instances](#).

There are just a few steps needed to take advantage of external users in your system:

1. [Enable external users](#) in your system.



Note:

Once external users are enabled in your system, they can be added to folders, standard sites, and stand-alone conversations. If you want to prevent external users from being added to a particular folder or standard site, you can disable external user access and membership on the **Members** page for that object. This option isn't available for conversations.

2. Invite new external users simply by adding them as members to folders, standard sites, or conversations by entering their email addresses. If there isn't already a user with that email address, you'll be asked for additional information, such as their name and location, then you can invite them, and Oracle Content Management will automatically provision a new external user.

Alternatively, administrators can add external users just as you would add any other user, and assign them the External User application role.
3. Give them access to the appropriate files, folders, and other objects in Oracle Content Management. When adding an external user as a member of an object, you must enter their full email address.

External users can:

- Access the Oracle Content Management web client.
- Work with files, folders, conversations, and sites to which they've been given access. Just like any other user, an external user must be a Contributor to be able to edit an item.
- Create new files in folders they have Contributor access to and delete files they created.
- Perform the following actions on sites to which they have Contributor access:
 - Delete and restore sites.
 - Copy and export templates.
 - Export components and layouts.
 - View the site's vanity domain.
 - Utilize all Site Builder functionality.
- Be added to membership based groups (not public groups).
- Receive regular sharing and contribution email notifications.
- Work with the Document Manager component, linked to a specific folder.
- Access the APIs with the same privileges they get using the web client.

Varying levels of access can be provided to any user but if a user has *only* the standard *external user* role, they can't:

- Access the desktop client or mobile apps.
- Create new folders (except in a folder they've been given access to), conversations, sites, nor themes.
- Delete other users' files.
- Be assigned Manager role for any object.
- Be on a governance site creation approval list.
- Be part of public groups.
- Create their own groups, modify existing group membership, or remove themselves from member groups.
- Browse translations or localization policies.
- Change a site's vanity domain.

Set the Default Resource Role for New Folder Members

Users in your organization can share folders with other users and assign them a resource role within the shared folder. The following roles are available:

- **Viewer:** Viewers can look at files and folders, but can't change things.
- **Downloader:** Downloaders can also download files and save them to their own computers.
- **Contributor:** Contributors can also modify files, update files, upload new files, and delete files.
- **Manager:** Managers have all the privileges of the other roles and can add or remove other people as members.

To change the default resource role:

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** menu, click **Users**.
3. Under **Members**, in the **Default role for new members added to folders** list, select the resource role users will be assigned by default when added to a folder.

Synchronize User Profile Data

You can replace a user's existing profile information with the information from your identity store:

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** menu, click **Users**.
3. Search for the user whose profile data you want to sync, click **Edit** next to the user's name, and click **Sync Profile Now** on the user details page.

Display Conversation Membership Messages for Users

Configure whether to show the user conversation membership messages (when a person is added to a conversation and who added them) by default. A user can change this display setting for any stand-alone conversation.

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** menu, click **Users**.
3. On the Search tab find the user whose default you want to set. Enter part of the user name, display name, or email address in the text box and click **Search**.
4. Click **Edit** next to the user's name.
5. Select the **Show Conversation Membership Messages by Default** check box and click **Save**.

Override Storage Quota for a User

You can [set a default quota](#) for the amount of storage space that a user is allocated. If you need to override the default for a particular user you can do so using the following steps.

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** menu, click **Users**.
3. Search for the user whose settings you want to override and click **Edit** next to the user's name.
4. In the **User Quota** box, enter the quota amount in gigabytes, and then click **Save**. You can see how much storage the user has used next to **Storage consumed**.

Transfer File Ownership

When people leave your organization or change roles, you might want to assign their files and folders to someone else and add their storage quota back to the total quota you have available for assignments. You can assign a person's entire library of content to someone else. The content appears as a folder in the new user's root folder. All of the sharing actions, such as members and public links, remain intact.

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** menu, click **Users**.
3. Find the user whose files you want to transfer using one of the following methods:
 - To find an active user, on the **Search** tab enter part of the user name, display name, or email address in the text box and click **Search**. Open the user properties by clicking the user name or clicking **Edit** next to the user.
 - To find a deprovisioned user, click the **Deprovisioned Users** tab. You see a list of all users who have been removed from your organization's system, sorted by name. This list is refreshed on a regular basis, but you can also update it manually by clicking **Sync Profile Data**.

To download a CSV file of all deleted users, click **Export Deprovisioned Users**.

4. Click **Transfer Ownership**. For active users, the button is at the bottom of the properties. For deprovisioned users, click the button next to the user you want.
5. Enter part of the user name, display name, or email address of the person who will receive the content and click **Search**.
6. Select the user you want to transfer the content to. A message shows that the content will increase the recipient's quota by the amount of content being transferred. It also shows you how much storage will be released back into the total quota you have available.
7. Click **Transfer**. The content is transferred and the list shows that the deprovisioned account is gone.

Alternatively, for deprovisioned users, you can delete the content. On the **Deprovisioned Users** tab, next to the user whose content you want to delete, click **Delete Content**.

Users can also transfer ownership of their own folders.

View and Resynchronize Groups Out of Sync

If you believe a group in Oracle Content Management is out of sync, you can see a report of the mismatches and manually resynchronize the group. For example, if a user can't access an item to which they should have access through group membership, the group may be out of sync.

To view group sync mismatches:

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** menu, click **Users**.

3. Click the **Group Sync** tab.
4. Search for the group you think is out of sync, then click **Check Synchronization Status**.
5. If the report shows that the group in Oracle Content Management is out of sync, click **Synchronize**.

 **Note:**

Groups that are restricted from sharing and groups that include only site visitors can't be synchronized.

Override Temporary Quota for a User

By default the maximum upload and sync file size is 2GB (set on the [Documents](#) page). To ensure more than one 2GB file can be uploaded simultaneously, the default temp storage quota for users is 5GB. If your maximum file size is set higher, the temp storage quota for users is automatically increased to 2.5 times that amount (for example, if the maximum file size is set to 10GB, the temp storage quota for users is set to 25GB).

This temp storage quota setting should suffice for normal circumstances, but if you need a particular user to have a higher Temp Storage quota, you can override the setting.

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** menu, click **Users**.
3. Search for the user whose settings you want to override and click **Edit** next to the user's name.
4. In the **Temp Quota** box, enter the quota amount in gigabytes, and then click **Save**.

Revoke Access to Linked Devices

Users can revoke access to one of their linked devices if they change devices or lose one, but there might be cases where you, as an administrator, need to perform this action. When you revoke access to a linked device, the user's sign-in session is ended. If you or anyone else tries to access Oracle Content Management from the device, the account is signed out and all local content stored on the device for that account is deleted.

Revoking access for the device affects only one account, so if the person has multiple user accounts, you need to revoke access separately for each user account to block all access to Oracle Content Management and delete all local content stored on the device.

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** menu, click **Users**.
3. Search for the user whose device access you want to revoke and click **Edit** next to the user's name.
4. Under **Linked Devices**, click **Revoke** next to the appropriate device.

Change Settings for Groups

You can change the sharing and notification settings for groups and resynchronize groups.

To change settings for groups:

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** menu, click **Users**.
3. Search for the group whose settings you want to change, then click **Edit** next to the group's name.
4. If you don't want the group to be used for sharing, so that users can't add the group to an object (such as a document or a site), select **Cannot be used for sharing**.
5. If you don't want this group to be sent notifications, select **Will not be sent notifications**.
6. To check if the group is in sync, click **Check Synchronization Status**. A message will show the status.
If you need to resynchronize the group information, click **Synchronize**.

Manage Users, Groups, and Access 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, use the topics in this section. If you don't see **Domains**, follow the steps in [Manage Users, Groups, and Access in a Region without Identity Domains](#).

- [Enable Single Sign-On \(SSO\)](#)
- [Manage Users with IAM](#)
- [Manage Groups with IAM](#)

Manage Users with IAM

Before using your system, you need to add users. As you continue to use your system, you'll need to add and remove users or change some of their settings. For example, if someone changes departments, you might need to change their role, or if someone leaves your organization, you need to remove them from the system.

If you need to manage Oracle Content Management specific user settings, you can do so on the [Users](#) page in System administration.

 **Note:**

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

To manage users:

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 **Identity & Security**, then, under **Identity**, click **Domains**.
3. On the Domains page, open your identity domain.
4. In the navigation menu on the left, click **Users**.
5. Perform any of the following tasks, described in [Managing Users](#).
 - To create a user, click **Create user**.
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](#).

 **Note:**

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

- To import users, you need to create a comma-separated values (CSV) file, and then import the file by clicking **Import users**.
- To export users, click **Export users**.
- To activate a user, select the user, and then click **Activate**.
- To deactivate a user, select the user, and then click **Deactivate**.
- To resend an invitation to a user, select the user, and then click **Resend invitation**.
- To reset a user's password, select the user, and then click **Reset password**.
- To reset all users' passwords, click **Reset all passwords**.
- To deprovision a user, select the user, and then click **Delete**.

Manage Groups with IAM

As a best practice, you should create groups for your organization roles in Identity and Access Management (IAM) and assign the appropriate application roles to those groups.

Then you can add users to those groups to automatically assign them the appropriate application roles.



Note:

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

If you need to manage Oracle Content Management groups, you can do so on the Groups page in your user menu, and you can manage [group settings](#) in System administration.

- [Manage Groups with IAM](#)
- [Assign Roles to Groups with IAM](#)
- [Assign Users to Groups IAM](#)

Manage Groups with IAM

As you use your system, you'll want to add, import, export, or remove groups.

To manage groups:



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 **Identity & Security**, then, under **Identity**, click **Domains**.
3. On the Domains page, open your identity domain.
4. In the navigation menu on the left, click **Groups**.
5. Perform any of the following tasks, described in [Managing Groups](#):
 - To create a group, click **Create group**.
 - To import groups, click **Import groups**.
 - To export groups, click **Export groups**.
 - To remove a group, select it, and then click **Delete**.

Assign Roles to Groups with IAM

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.

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](#).

Assign Users to Groups IAM

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**.

Manage Users, Groups, and Access 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, use the topics in this section. If

you do see **Domains**, follow the steps in [Manage Users, Groups, and Access in a Region with Identity Domains](#).

- [Enable Single Sign-On \(SSO\)](#)
- [Manage Users with IDCS](#)
- [Manage Groups with IDCS](#)

Enable Single Sign-On (SSO)


If you use Federated Single Sign-On (SSO) for your Oracle Content Management environment, you can enable it to customize sign-in procedures. When Single Sign-On (SSO) is enabled, users can sign in to one instance using corporate security credentials and access another instance in the same domain without signing in again. For example, perhaps you are an administrator for your company which has two Oracle Cloud services and you must provision these services to your company's organization, roles, and users. Your company may also have on-premise applications and cloud services from other vendors. It's important that communication between these services and applications is done in a secure fashion. With SSO, users can sign in to all of them using the same set of credentials that are managed by using your identity domain system.

OAuth provides secure access to all services in Oracle Cloud. It provides an access token for communication between services. The token is valid for a limited time and contains the security credentials for a sign-in session. It identifies the user and the user's groups.

Overview of SSO Configuration

Oracle Cloud uses the SAML 2.0 standard to enable secure cross-domain communication between Oracle Cloud and other SAML-enabled sites located on-premise or in a different cloud. The administrator must configure SAML 2.0 SSO between Oracle Cloud and the identity provider. When SSO is enabled, the identity provider performs authentication for Oracle Cloud.

Perform the following steps to configure SSO:

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 **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, add a SAML application, and configure SSO details. See *Add a SAML Application in Administering Oracle Identity Cloud Service*.

Manage Users with IDCS

Before using your system, you need to add users and probably enable single sign-on (SSO). As you continue to use your system, you'll need to add and remove users or change some of their settings. For example, if someone changes departments, you



might need to change their role, or if someone leaves your organization, you need to remove them from the system.

If you need to manage Oracle Content Management specific user settings, you can do so on the [Users](#) page in System administration.

 **Note:**

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

To manage users:

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 **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 **Users**.
5. Perform any of the following tasks:
 - To create a user, click **Add**.
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](#).

 **Note:**

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

- To import users, click **Import**.
- To export users, click **Export**.
- To activate a user, select the user, and then click **Activate**.
- To deactivate a user, select the user, and then click **Deactivate**.
- To resend an invitation to a user, select the user, and then click **Resend Invitation**.
- To reset a user's password, select the user, and then click **Reset Password**.
- To deprovision a user, select the user, and then click **Remove**.

See Managing Oracle Identity Cloud Service Users in *Administering Oracle Identity Cloud Service*.

Manage Groups with IDCS

As a best practice, you should create groups for your organization roles in Oracle Identity Cloud Service (IDCS) and assign the appropriate application roles to those groups. Then you can add users to those groups to automatically assign them the appropriate application roles.

Note:

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



If you need to manage Oracle Content Management groups, you can do so on the Groups page in your user menu, and you can manage [group settings](#) in System administration.

- [Manage Groups with IDCS](#)
- [Assign Roles to Groups with IDCS](#)
- [Assign Users to Groups IDCS](#)

Manage Groups with IDCS

As you use your system, you'll want to add, import, export, or remove groups.

To manage groups:



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 **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. Perform any of the following tasks:
 - To create a group, click **Add**.
 - To import groups, click **Import**.
 - To export groups, click **Export**.
 - To remove a group, select it, and then click **Remove**.

See *Managing Oracle Identity Cloud Service Groups* in *Administering Oracle Identity Cloud Service*.

Assign Roles to Groups with IDCS

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.


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](#).

Assign Users to Groups IDCS

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**.

6

Analyze Service Usage

Throughout the use of your service, you can view service usage statistics to help you analyze system needs or issues.



Note:

If you're using Oracle Content Management Starter Edition, you're limited to only basic usage information (the dashboard). To take advantage of the full feature set, [upgrade to the Premium Edition](#).

The analytics refresh job runs nightly.

- [Understand Analytics](#)
- [View the Analytics Dashboard](#)
- [View User Statistics](#)
- [View Assets and Content Metrics](#)
- [View Sites and Channels Analytics](#)
- [View Files and Conversations Statistics](#)
- [View Capture Metrics](#)
- [View Reports and Metrics](#)

Understand Analytics

The Analytics interface displays statistics about Oracle Content Management usage and content.

To use the Oracle Content Management Analytics interface:

1. After you sign in to the Oracle Content Management web application as an administrator, click **Analytics** in the navigation menu.
2. In the **Analytics** menu, select a page:
 - **Dashboard**: Summarizes the most important usage statistics, including total users, daily active users, total repositories, total channels, total assets, total documents, daily new assets, sign-ins by device type (such as web client or iOS), and assets by type.
 - **User Statistics**: Shows totals and daily statistics for users and system usage.
 - **Assets and Content**: Users with a Manager role within at least one repository can view metrics for repositories, collections, and channels.
 - **Sites and Channels**: Shows analytics for sites and channels, including number of visits, top languages, devices, browsers, most visited, and least visited.

- **Files and Conversations:** Shows data for documents, shared links, and conversations.
- **Capture:** Shows composite data of individual documents and audit history. The metrics show what is being captured and how effectively Content Capture is used by the users.
- **Reports and Metrics:** Use this page to view reports on your users and documents usage to better understand how your system is being used, and monitor service activity. You can search for a report to run or select the User List, User Logins by Device Type, Documents Usage Log, Asset Activities, User Activities, or Capture Activities report.


Understand the Analytics Data

Here are some points to help you understand the analytics data:

- System users, the integration user, and other internal user types that are not actually Oracle Content Management users are not included in the statistics.
- The analytics refresh job runs nightly. The data refresh date is shown at the bottom right of each analytics page.
- For data related to the number of messages (such as in conversations, groups walls, and so on), keep in mind that message counts include membership messages; for example, if a user adds another user to a conversation, the message announcing the addition is counted.
- Some graphs display data for the previous 12 months. If you do not have a complete month of data on your system yet, those graphs will be blank.

Analytics Chart, Graph, and Report Features

The following features are available in charts, graphs, and reports:

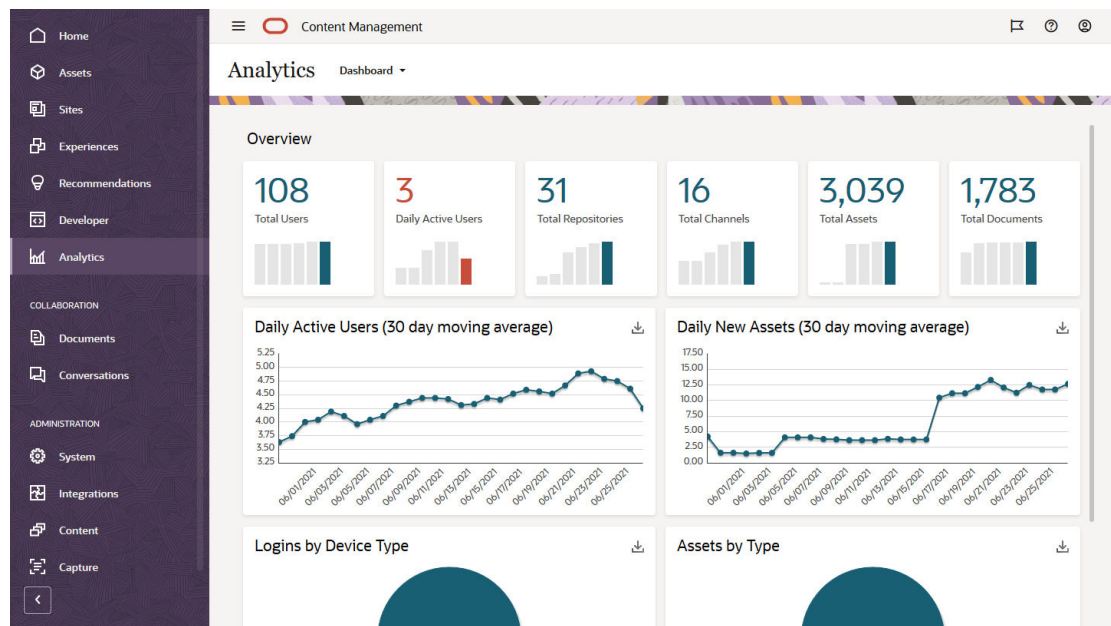
- You can hover over the dots in the graph, or the segments of a bar chart or pie chart, to see the specific number for the time period being displayed.
- For most tables and charts, you can download a CSV file containing the data being displayed by clicking . When reviewing the CSV files, keep these considerations in mind:
 - File names are based on the report name and the most recent update date for the statistics; for example, a Logins by Device Type report with data that was last updated on November 15th, 2018 is named *Logins_by_Device_Type_11-15-2018*.
 - CSV files exported from pie chart graphs show the actual numerical data rather than the percentages portrayed in the pie charts.
 - Certain CSV files may contain more labels (headings) than the chart in the user interface. For example, charts showing smaller moving averages are meant to show trends; including all labels would make the chart difficult to read.

View the Analytics Dashboard

The Analytics dashboard lets you see usage, utilization, and traffic analytics for your users, repositories, channels, assets, and documents.

To view the Analytics dashboard:

1. After you sign in to the Oracle Content Management web application as an administrator, click **Analytics** in the navigation menu.
2. In the **Analytics** menu, choose **Dashboard**.




The **Dashboard** page shows an overview of important usage statistics.

Statistic	Description
Overview	<p>The Overview table shows the following metrics:</p> <ul style="list-style-type: none"> • Total Users: all currently enabled users who have signed in at least once. • Daily Active Users: The average number of users per day who have signed in to Oracle Content Management on any client/device. • Total Repositories: The number of asset repositories created in the system. • Total Channels: The number of channels to which assets have been published or targeted. • Total Assets: The total number of assets in the system. • Total Documents: The total number of documents in the system.
Daily Active Users	<p>The line graph indicates a 30-day moving average of the number of active users on the system. Active users are those who have signed in to Oracle Content Management using any client/device type (such as the browser, the desktop app, or a mobile device).</p>
Daily New Assets	<p>The line graph indicates a 30-day moving average of the number of new assets that were added.</p>

Statistic	Description
Logins by Device Type	The pie chart indicates logins by device type, based on the total number of logins to Oracle Content Management. The Java API "device" represents programmatic logins.
Assets by Type	The pie chart indicates the percentage of assets by type, based on the total number of assets in Oracle Content Management.
Most Used Assets	This table lists the assets used most in your system. Each asset includes the asset name (which you can click to view the asset if you have access to it), the number of channels associated with the asset, the number of channels the asset has been published to, the number of contributors assigned to the asset, the repository that stores the asset, and the asset type used by the asset.

For more information on the analytics data and the features available in the charts, graphs, and reports, see [Understand Analytics](#). For example, you can download a

CSV file containing the data being displayed by clicking  .

View User Statistics


To view user statistics:

1. After you sign in to the Oracle Content Management web application as an administrator, click **Analytics** in the navigation menu.
2. In the **Analytics** menu, click **User Statistics**.
3. By default, the User Statistics page shows data for users in all groups. To display the data for users in a particular group, enter the group name in the search box.

The following table summarizes the statistics for users.

Statistics	Description
Overview Metrics	<ul style="list-style-type: none"> • Total Number of Enabled Users (Total User Population) • Users Enabled Last 30 Days • Deprovisioned Users

Statistics	Description
Charts	<ul style="list-style-type: none"> • Total Number of Enabled Users (Total User Population) by Month: The dark blue line in the chart indicates the number of users that existed in the system during the previous 12 months. The light blue line in the chart shows the number of active users—those who have signed in at least one time. • Number of New Users per Day: The bar chart indicates the trend in new user additions for the period selected in the drop-down list (by default, the last 30 days). • New Users per Month: The line chart indicates the number of new users per month during the previous 12 months. • Unique User Logins per Day: The bar chart indicates the number of users who have logged in per day for the period selected in the drop-down list (by default, the last 30 days). • Users by Login Frequency: The pie chart shows how frequently users sign in to your system based on the previous 12 months. • Logins by Device Type: The pie chart shows the types of devices users use to sign in to your system over the previous 12 months. • Device Type Trend: The line chart shows the types of devices users have used each month to sign in to your system over the previous 12 months. • Active User Base Changes: The bar chart shows a comparison of new, returning, and leaving users per month, and the line shows the net change per month over the previous 12 months. • Monthly Churn Rate: The line chart shows the number of users lost per month over the previous 12 months. • Average Consecutive Months of Use: The line chart shows the average number of consecutive months users have used your system. The data is shown for the previous 12 months.
Report	<ul style="list-style-type: none"> • Top Users by Activity: The list shows the users with the most activity (for example, logins and files submitted) in descending order of activity. This report provides the following usage information for each user: <ul style="list-style-type: none"> – User Name – Logins – Assets Added – Files Submitted – Conversations Created – Conversation Membership – Shared Links • Top Users by Storage: The list shows the users with the highest storage usage in descending order of storage usage. This report provides the following usage information for each user: <ul style="list-style-type: none"> – User Name – Personal Storage (GB) – Shared Storage (GB)

For more information on the analytics data and the features available in the charts, graphs, and reports, see [Understand Analytics](#). For example, you can download a CSV file containing the data being displayed by clicking .


View Assets and Content Metrics

Service administrators can use the **Assets and Content** option on the Analytics menu to view content metrics for any repositories, collections, and channels. Repository administrators can view content metrics for any repositories, collections, and channels in

which they have the Manager role. A content contributor can view content metrics for any repositories, collections, and channels in which they have the Contributor role.

To view asset and content metrics:

1. After you sign in to the Oracle Content Management web application as an administrator, click **Analytics** in the navigation menu.
2. In the **Analytics** menu, click **Assets and Content**.
3. Choose a page in the left pane to show detailed metrics, trends, and reports for one the following content objects:
 - [Repositories](#)
 - [Content](#)
 - [Channels](#)
 - [Collections](#)

For more information on the analytics data and the features available in the charts, graphs, and reports, see [Understand Analytics](#). For example, you can download a CSV file containing the data being displayed by clicking .

Repositories Metrics

Service administrators can view content metrics for all repositories or for a specific repository. Repository administrators can view content metrics for any repository in which they have the Manager role. A content contributor can view content metrics for any repository in which they have the Contributor role.


To view repository metrics:

1. After you sign in to the Oracle Content Management web application as an administrator, click **Analytics** in the navigation menu.
2. In the **Analytics** menu, click **Assets and Content**. The Repositories page is shown by default.
3. By default, you see metrics for all repositories. To display metrics for a specific repository, enter the repository name in the search box at the top of the page. When you select a specific repository, you can click the asset metrics in the overview to view the assets in that repository. For example, if you select a repository, then click the Videos metric, you'll be taken to the Assets page, showing only those videos that are in the selected repository.
4. By default, you see metrics for all content types. To display metrics for a specific content type, select the type from the drop-down list.

The following table describes the content metrics for repositories.

Metric	Description
Repositories	The number of repositories.
Collections	The number of collections in the selected repository.

Metric	Description
Assets	The number of assets in the selected repository. You also see a breakdown of how many standard, business, and archived assets are included in the asset total. If you selected a specific repository, click this metric to go to the Assets page and see the assets in the selected repository.
Videos	The number of videos in the selected repository. If you selected a specific repository, click this metric to go to the Assets page and see the videos in the selected repository.
Channels	The number of channels in the selected repository.
Contributors	The number of contributors in the selected repository.
Storage Used (MB)	The storage used by the selected repository over time, in megabytes, with a bar chart showing the total size of digital assets in blue. Use the drop-down list to select the period for which you want to see data (by default, the last 30 days).
Assets Added	The number of assets added over time, in a bar chart, broken down by asset type, with dark blue for digital assets and light blue for content items. Use the drop-down list to select the period for which you want to see data (by default, the last 30 days).
Assets by Class	The number of assets added over time, in a bar chart, broken down by asset class, with dark blue for standard assets, light blue for business assets, and yellow for archived assets. Use the drop-down list to select the period for which you want to see data (by default, the last 30 days).
Assets by Content Type	The top 10 types by number of assets are shown in a bar chart. The 11th and further ones are bundled together under "Other".
Repositories	A table showing the name of each repository followed by its number of total assets, standard assets, business assets, archived assets, videos, collections, channels, and contributors. If your administrator enabled Video Plus, you also see a breakdown of standard and Video Plus videos.
Top Contributors	The user names of top contributors for the selected period, and the number of assets added by each contributor, broken down by content items and digital assets. If your administrator enabled Video Plus, you also see the number of advanced videos. Use the drop-down list to select the period for which you want to see data (by default, all time).

For more information on the analytics data and the features available in the charts, graphs, and reports, see [Understand Analytics](#). For example, you can download a CSV file containing the data being displayed by clicking .

Content Metrics

Service administrators can view all content metrics. Repository administrators can view content metrics for any repository in which they have the Manager role. A content contributor can view content metrics for any repository in which they have the Contributor role.

To view content metrics:


1. After you sign in to the Oracle Content Management web application as an administrator, click **Analytics** in the navigation menu.
2. In the **Analytics** menu, click **Assets and Content**.

3. Click **Content** in the left pane.

The following table describes the content metrics.

Metric	Description
Published Asset Age - Oldest Assets (in Days)	A bar chart that shows the 20 oldest assets. Hover your cursor over a bar to see the asset name, repository, all associated publishing channels, and the corresponding age in those channels.
Assets by Content Type	The top 10 types by number of assets are shown in a bar chart. The 11th and further ones are bundled together under "Other".
Total Assets by Month	The total number of assets in your system each month are shown in a bar chart. Hover your cursor over a bar to see the date, total number of assets, number of digital assets, and number of content items.
Total Assets by Day	The total number of assets in your system each day are shown in a bar chart. Hover your cursor over a bar to see the date, total number of assets, number of digital assets, and number of content items. Use the drop-down list to select the period for which you want to see data (by default, last 30 days).
Top Contributors	The user names of top contributors for the selected period, and the number of assets added by each contributor, broken down by content items and digital asset types. If your administrator enabled Video Plus, you also see the number of advanced videos. Use the drop-down list to select the period for which you want to see data (by default, all time).
Assets Review Completed But Not Yet Published	The assets that have been reviewed but haven't been published. Each entry includes the asset name, asset creator, the date the asset was reviewed, and how many days have passed since that date.
Orphaned Assets	The assets that haven't been published for more than the selected amount of time. This can help you discover assets that might be able to be deleted to reduce the number of assets you're billed for. Each entry includes the asset name, days untouched, the targeted channels, and whether the asset was reviewed. By default, you see assets untouched for more than 30 days, but you can select a different period from the drop-down list. Initially the table is sorted by days untouched.

For more information on the analytics data and the features available in the charts, graphs, and reports, see [Understand Analytics](#). For example, you can download a

CSV file containing the data being displayed by clicking .

Channels Metrics

Service administrators can view content metrics for all channels or for a specific channel. Repository administrators can view content metrics for any channel in which they have the Manager role. A content contributor can view content metrics for any channel in which they have the Contributor role.


To view channel metrics:

1. After you sign in to the Oracle Content Management web application as an administrator, click **Analytics** in the navigation menu.
2. In the **Analytics** menu, click **Assets and Content**.

3. Click **Channels** in the left pane.
4. By default, you see metrics for all channels. To display metrics for a specific channel or for the channels in a specific repository, enter the channel or repository name in the search boxes at the top of the page.
When you select a specific repository or channel, you can click the asset metrics in the overview to view the assets in that repository or channel. For example, if you select a channel, then click the Published Assets metric, you'll be taken to the Assets page, showing only those published assets that are in the selected channel.
5. By default, you see metrics for all content types. To display metrics for a specific content type, select the type from the drop-down list.

The following table describes the content metrics for channels.

Metric	Description
Channels	The number of channels in the selected repository.
Total Assets	The total number of assets in the selected channel or repository. If you selected a specific repository or channel, click this metric to go to the Assets page and see the assets in the selected repository or channel.
Published Assets	The number of published assets in the selected channel or repository. If you selected a specific repository or channel, click this metric to go to the Assets page and see the published assets in the selected repository or channel.
Pending Assets	The number of pending assets in Draft, In Review, Approved, or In Translation state, which have not yet been published to or rejected from the selected channel or repository. If you selected a specific repository or channel, click this metric to go to the Assets page and see the pending assets in the selected repository or channel.
Rejected Assets	The number of assets rejected and although targeted, have not been published to the selected channel or repository. If you selected a specific repository or channel, click this metric to go to the Assets page and see the rejected assets in the selected repository or channel.
Published Assets by Age	A bar chart that shows how long ago the assets were published, in the selected channel or repository.
Assets Published	A bar chart of assets published over time, in the selected channel or repository. Use the drop-down list to select the period for which you want to see data (by default, the last 30 days).
Assets by Content Type and Status	A bar chart that shows the number of assets for each content type in the selected channel or repository. Blue is for published assets, green is for pending assets, and gold is for rejected assets.
Top Channels	A list of the top channels, with channel names and the number of published, pending, rejected, and total assets in each channel for the selected repository.
Assets by Translation	A list of languages for translations, with the number of published, pending, rejected, and total assets for each language in the selected channel or repository.

For more information on the analytics data and the features available in the charts, graphs, and reports, see [Understand Analytics](#). For example, you can download a CSV file containing the data being displayed by clicking .

Collections Metrics

Service administrators can view content metrics for all collections or for a specific collection. Repository administrators can view content metrics for any collection in which they have the Manager role. A content contributor can view content metrics for any collection in which they have the Contributor role.


To view collection metrics:

1. After you sign in to the Oracle Content Management web application as an administrator, click **Analytix** in the navigation menu.
2. In the **Analytix** menu, click **Assets and Content**.
3. Click **Collections** in the left pane.
4. By default, you see metrics for all collections. To display metrics for a specific collection or for the collections in a specific repository, enter the collection or repository name in the search boxes at the top of the page.
When you select a specific repository or collection, you can click the asset metrics in the overview to view the assets in that repository or collection. For example, if you select a collection, then click the Published Assets metric, you'll be taken to the Assets page, showing only those published assets that are in the selected collection.
5. By default, you see metrics for all content types. To display metrics for a specific content type, select the type from the drop-down list.

The following table describes the content metrics for collections.

Metric	Description
Collections	The number of collections, which can be filtered by repository.
Total Assets	The total number of assets, which can be filtered by repository and collection. If you selected a specific repository or collection, click this metric to go to the Assets page and see the assets in the selected repository or collection.
Published Assets	The number of published assets, which can be filtered by repository and collection. Each translation for a translated asset is counted separately. If you selected a specific repository or collection, click this metric to go to the Assets page and see the published assets in the selected repository or collection.
Pending Assets	The number of pending assets (not yet published), which can be filtered by repository and collection. The assets are in Draft, In Review, Approved, or In Translation states. Each translation for a translated asset is counted separately. If you selected a specific repository or collection, click this metric to go to the Assets page and see the pending assets in the selected repository or collection.
Rejected Assets	The number of rejected assets, which have not been published. These can be filtered by repository and collection. Each translation for a translated asset is counted separately. If you selected a specific repository or collection, click this metric to go to the Assets page and see the rejected assets in the selected repository or collection.

Metric	Description
Average Collection Membership per Asset	The average number of collections an asset belongs to, in all or a specified repository.
Average Assets per Collection	The average number of assets in a collection for all or a specified repository.
Assets by Content Type and Status	A bar chart that shows the number of asset publications for each content type in all or a specified repository.
Assets Added	A bar chart that shows the number of assets added over time. Use the drop-down list to select the period for which you want to see data (by default, the last 30 days).
Assets Published	A bar chart that shows the number of assets published over time. Use the drop-down list to select the period for which you want to see data (by default, the last 30 days).
Top Collections	A list of the top collections, with collection and repository names and the number of published, pending, rejected, and total assets in each collection.

For more information on the analytics data and the features available in the charts, graphs, and reports, see [Understand Analytics](#). For example, you can download a CSV file containing the data being displayed by clicking .

View Sites and Channels Analytics

The Sites and Channels graphs and charts let you see usage, utilization, and traffic analytics for your created sites and channels.

You can also [add JavaScript tracking code to sites and pages](#) for web analytics tracking, making it easier to integrate with external analytics providers like Google, Adobe, or Oracle Infinity.

To view site and channel statistics:


1. After you sign in to the Oracle Content Management web application as an administrator, click **Analytics** in the navigation menu.
2. In the **Analytics** menu, click **Sites and Channels**.
If Video Plus is enabled in your service, you'll see two tabs: **General Usage** and **Video Plus**.
3. By default, the Sites and Channels page (or the General Usage tab) shows data for all sites and channels, in all languages, for the specified period (by default, the last 30 days). To filter the data, enter the site or channel name or a specific language in the search boxes, or select a different period from the drop-down list.
The following table summarizes the general usage statistics for sites and channels.

Statistics	Description
Number of Visits	A line graph indicates the number of visits over a number of days for sites and channels. This counts "unique visits", and these are unique within a 1-hour period. So, if you visit a site 20 times within 1 hour, it still counts as only 1 unique visit. A visit is counted for each channel and at a 60-minute granularity. That is, if a visitor visits the same site in 2 different hours in a day, it's counted as 2 visits.
Top Languages	A bar chart shows the top six languages for site and channel visits.

Statistics	Description
Devices	A pie chart shows devices used to visit sites and channels.
Browsers	A pie charts shows browsers used to visit sites and channels.
Most Visited	A bar chart shows the most visited sites and channels over a number of days.
Least Visited	A bar chart shows the least visited sites and channels over a number of days.

- By default, the Video Plus tab shows data for all sites and channels, in all languages, for the specified period (by default, the last 30 days). To filter the data, enter the site or channel name or a specific language in the search boxes, or select a different period from the drop-down list.
The following table summarizes the Video Plus statistics for sites and channels.

Statistics	Description
Videos	The number of Video Plus assets.
Total Player Loads	The number of times the player has loaded on a page, whether the video was played or not.
Total Plays	The number of times the video was played.
Average Completion Rate	The average percentage of the video that was played.
Play Through	The percentage of plays that completed to the end.
Countries	The number of countries in which the video was played.
Top Platforms	This pie chart shows the top five platforms on which the video was viewed.
Browsers	This pie chart shows the top five browsers on which the video was viewed.
Top Countries	This pie chart shows the top five countries from which the video was viewed.
Top Video Content by Plays	This table shows the top videos by number of plays. Click the video's name to preview it (if you have access to the asset).
Top Video Content by Drop-Off	This table shows the top videos by the percentage of the video that was played. Click the video's name to preview it (if you have access to the asset).
Top Countries	This table shows the countries, ordered by number of plays, from which the video was viewed.
Browsers	This table shows the browsers, ordered by number of plays, from which the video was viewed.
Platforms	This table shows the platform, ordered by number of plays, from which the video was viewed.

For more information on the analytics data and the features available in the charts, graphs, and reports, see [Understand Analytics](#). For example, you can download a CSV file containing the data being displayed by clicking .


View Files and Conversations Statistics

The Files and Conversations Statistics page shows detailed statistics for system objects.

To view file and conversation metrics:

- After you sign in to the Oracle Content Management web application as an administrator, click **Analytics** in the navigation menu.
- In the **Analytics** menu, click **Files and Conversations**.
- Choose a page in the left pane to show detailed metrics, graphs and charts for one the following system objects:

- [Documents](#)
- [Shared Links](#)
- [Conversations](#)

For more information on the analytics data and the features available in the charts, graphs, and reports, see [Understand Analytics](#). For example, you can download a CSV file containing the data being displayed by clicking .

Documents Metrics


To view document metrics:

1. After you sign in to the Oracle Content Management web application as an administrator, click **Analytics** in the navigation menu.
2. In the **Analytics** menu, click **Files and Conversations**. The Documents page is shown by default.
3. By default, you see metrics for all groups. To display metrics for a specific group, enter the group name in the search box at the top of the page.

The following table describes the general statistics for documents, which include files visible through the **Documents** interface. These statistics exclude assets, content items, and files associated with sites.

Statistics	Description
Overview Metrics	<ul style="list-style-type: none"> • Total Number of Documents: Shows the total number of documents currently in the system. • Created in the Last 30 Days: Shows the number of documents created in the last 30 days. • Average Number of Documents Added per Day: Shows the average number of documents added per day based on the last 30 days. • Average Content Size Added per Day (in MB): Shows the average amount of content in MB added per day based on the last 30 days. • Average Documents per User: Shows the average number of documents each user owns based on the last 30 days. <p>When a file is uploaded, the system might create and store more than one file; for example, when an image is uploaded, the system creates and stores several resolutions of that image. All of the files are included in the total number of documents.</p> <p>Document counts go down as the result of deleting files.</p>

Statistics	Description
Charts	<ul style="list-style-type: none"> • Total Number of Documents by Month The bar chart shows the total number of documents in the system during the previous 12 months. • Document Updates vs New Documents The bar chart shows the number of documents updated and the number of new documents added per day during the time period selected in the drop-down list. You can also filter the chart by file type. • Total Document Content Size (MB) The bar chart shows the total amount of content in MB currently in the system. • Amount of Content (MB) per Day The bar chart shows the amount of content in MB in the system per day during the time period selected in the drop-down list. • Document Views by Month The bar chart shows the number times users have viewed documents per month during the previous 12 months. • Document Views by Day The bar chart shows the number times users have viewed documents per day during the time period selected in the drop-down list. • Number of Documents per User The line graph shows the number of documents per user during the previous 12 months. • Number of Untouched Documents by Months Untouched The bar chart shows the number of documents that have no activity (viewed, downloaded, or updated) grouped by the period without activity from three months up to three years.

For more information on the analytics data and the features available in the charts, graphs, and reports, see [Understand Analytics](#). For example, you can download a CSV file containing the data being displayed by clicking .

Shared Links Metrics


To view shared link metrics:

1. After you sign in to the Oracle Content Management web application as an administrator, click **Analytics** in the navigation menu.
2. In the **Analytics** menu, click **Files and Conversations**.
3. Click **Shared Links** in the left pane.
4. By default, you see metrics for all groups. To display metrics for a specific group, enter the group name in the search box at the top of the page.

The following table describes the general statistics for shared links.

Statistics	Description
Overview Metrics	<ul style="list-style-type: none"> • Total Number of Shared Links • Created in the Last 30 Days • Average Shared Links per User • Percentage of Documents Shared

Statistics	Description
Charts	<ul style="list-style-type: none"> • Total Number of Shared Links by Month The line graph indicates the total number of shared links that existed in the system during the previous 12 months. • Number of Shared Links per Day The bar chart indicates the number of links shared by users per day during the time period selected in the drop-down list. • Number of Shared Links per User • Active Users vs. Shared Links Users per Month

For more information on the analytics data and the features available in the charts, graphs, and reports, see [Understand Analytics](#). For example, you can download a CSV file containing the data being displayed by clicking .


Conversations Metrics

To view conversation metrics:

1. After you sign in to the Oracle Content Management web application as an administrator, click **Analytics** in the navigation menu.
2. In the **Analytics** menu, click **Files and Conversations**.
3. Click **Conversations** in the left pane.
4. By default, you see metrics for all groups. To display metrics for a specific group, enter the group name in the search box at the top of the page.

The following table describes the general statistics for conversations.

Statistics	Description
Overview Metrics	<ul style="list-style-type: none"> • Total Number of Conversations • Created in the Last 30 Days • Average Number of Users per Conversation • Average Conversations Created per User
Charts	<ul style="list-style-type: none"> • Total Number of Conversations by Month The line graph indicates the total number of conversations that existed in the system during the previous 12 months. • Number of New Conversations per Day The bar chart indicates the number of new conversations created per day during the time period selected in the drop-down list. • Number of Conversations Created by Users • Number of Conversations of Which Users Are Members • Unique Conversations Entered per Month The bar chart indicates the number of unique conversations entered by users per month. • Unique Conversations Entered per Day The bar chart indicates the number of unique conversations entered by users per day during the time period selected in the drop-down list.

For more information on the analytics data and the features available in the charts, graphs, and reports, see [Understand Analytics](#). For example, you can download a CSV file containing the data being displayed by clicking .

View Capture Metrics

Content Capture metrics show composite data of individual documents and audit history. The metrics show what is being captured and how effectively Content Capture is used by the users.

You can also [view reports](#) on users' Capture activities to help you understand how Content Capture is being used.


To view Capture metrics:

1. After you sign in to the Oracle Content Management web application as an administrator, click **Analytics** in the navigation menu.
2. In the **Analytics** menu, click **Capture**.

The following table summarizes the metrics for Capture.

Statistics	Description
Overview	<p>By default, the overview metrics show data for the life of your system. To display data for a specific period, select Date Range from the drop-down list, enter a start date (no older than one year) and end date, and then click Refresh.</p> <p>The overview metrics show the following data:</p> <ul style="list-style-type: none"> • Total Documents Captured: The total number of documents (not batches) captured across all procedures. • Total Documents Committed: The total number of documents committed to Oracle Content Management. • Total Tiff Conversions: The total number of documents that went through TIFF conversion. • Total Documents Recognized: The total number of documents that went through barcode recognition. • Total Documents OCRred: The total number of documents that went through OCR processing. • Asset Lookups: The total number of documents that went through asset lookup. • Taxonomy Lookups: The total number of documents that went through taxonomy lookup. • XML Transforms: The total number of documents that went through XML transformation. • Conditional Assignments: The total number of documents that went through conditional assignment. • External Processes: The total number of documents that were processed via an external processor. • Total PDF Conversions: The total number of documents that went through PDF conversion. • Total Documents Classified: The total number of documents that went through classification processing. • Users: The total number of users that have used Capture across all procedures. • Sources: Shown only when a date range has been specified, not for All-Time. The total number of import jobs, across all procedures, in which there was at least one batch created. • Types of Documents Captured: The total number of distinct file formats captured.

Statistics	Description
Charts	<p>By default, the charts show data for the last 30 days. To display data for a different period, enter a start date (no older than one year) and end date, and then click Refresh.</p> <p>The following charts are available:</p> <ul style="list-style-type: none"> • Source of Documents: This pie chart shows the distribution of various sources that have used for capturing documents. These sources are scanner, email, list, folder, and WCC (WebCenter Content) archive. • Total Documents Captured (by user): This line graph shows the total documents captured by each user on a daily basis. It's filtered by top ten users to reduce clutter. Overall data is available for download. The date range can't be longer than one month. • Daily Count: This line graph shows the total documents that have undergone the selected activity, broken down by source, on a daily basis. Select an activity, enter a date range, and then click Refresh. The date range can't be longer than one month.
Capture Activities	<p>By default, the Capture activities list shows data for the last 30 days. To display data for a different period, enter a start date (no older than one year) and end date, and then click Refresh.</p> <p>The Capture activities list shows all the jobs that have run for the specified period. Each job entry includes the following information:</p> <ul style="list-style-type: none"> • Import Processor: The name of the import processor, if one was used. • Processor Type: The type of import processor used (email, file folder, or client). • Procedure: The name of the procedure in which the import processor is defined. • Capture: The total number of documents captured in this job. • OCR: The total number of captured documents that went through OCR processing. • TIFF Convert: The total number of captured documents that were converted to TIFF. • PDF Convert: The total number of captured documents that were converted to PDF. • Recognize: The total number of captured documents that went through barcode recognition. • Classify: The total number of captured documents that went through classification processing. • Commit: The total number of captured documents that were committed to Oracle Content Management.

For more information on the analytics data and the features available in the charts, graphs, and reports, see [Understand Analytics](#). For example, you can download a CSV file containing the data being displayed by clicking .

View Reports and Metrics

You can view reports on your users and documents usage to help you understand how your system is being used.

1. After you sign in to the Oracle Content Management web application as an administrator, click **Analytics** in the navigation menu.

2. In the **Analytics** menu, click **Reports and Metrics**.
3. Select a report:

Report	Description
User List	<p>Shows basic system information about each user in the Oracle Content Management instance, sorted by user ID (email address).</p> <ul style="list-style-type: none">• Object ID—The system-assigned numerical ID for the user object.• GUID—The system-assigned numerical ID for the user. This is the user's unique identifier within the system, of the form <i>/ServiceRoot/GUID/</i>. In the user interface these are decoded to the user's name, but the exported report doesn't show the user's name.• User—The user name, typically the email address.• User Name—The user's display name.• Enabled—Indicates whether the user is enabled (True) or disabled (False) on the system.• Service Administrator—Indicates the roles for the user. True means the user is assigned the role. False means the user isn't assigned the role. If all role entries are False, the user is an Employee without any additional roles. <p>The columns aren't sortable on the screen, but you can sort the columns after downloading CSV to Microsoft Excel.</p>
User Logins by Device Type	<p>Shows each user and the number of logins using each client/device, sorted by user name.</p> <p>The columns aren't sortable on the screen, but you can sort the columns after downloading CSV to Microsoft Excel.</p>

Report	Description
Documents Usage Log	<p>Set the report parameters, and then click Run.</p> <p>Shows the following information about the documents in your system, sorted by activity date in descending order (most recent activity at the top):</p> <ul style="list-style-type: none">• Activity—The type of activity performed (upload, view, download, delete).• Date—The date the activity occurred (based on UTC timezone).• User Name—The user that performed the activity.• Asset Type—The target of the activity (file or folder).• Parent—The name of the parent folder.• Name—The name of the file or folder.• GUID—The unique identifier of the file or folder.• File Size—The size of the file, in megabytes. <p>You can filter the report by date range, action, file or folder name, user, file name, and GUID.</p> <p>The columns aren't sortable on the screen, but you can sort the columns after downloading CSV to Microsoft Excel.</p>
Asset Activities	<p>Set the report parameters, and then click Run.</p> <p>Shows the following information about asset events, sorted by date in descending order (most recent activity at the top):</p> <ul style="list-style-type: none">• Name—The name and ID of the asset. Click the name to view the asset.• Content Type—The content type the item is based on, or digital asset.• Activity—The type of activity that occurred.• Activity Detail—The specifics of the activity.• Version—The asset version.• Performed by—The user that performed the activity.• Date—The date and time the activity occurred (based on UTC timezone). <p>You can filter the report by repository, date, activity type, and content type. You can also search for specific assets or events.</p> <p>The columns aren't sortable on the screen, but you can sort the columns after downloading CSV to Microsoft Excel.</p>


Report	Description
User Activities	<p>Set the report parameters, and then click Run.</p> <p>Shows the following information about user activities for the specified period:</p> <ul style="list-style-type: none">• Object—The name and GUID of the object on which the activity was performed.• Object Type—The type of object, for example, digital asset, content item, or repository.• Parent—The repository in which the object is stored.• Activity—The type of activity that occurred.• Activity Detail—The specifics of the activity.• Version—The asset version.• Performed by—The user that performed the activity.• Date—The date and time the activity occurred. <p>You can filter the report by date, user, activity type, or object type. You can also search for a particular user, activity, or object.</p> <p>The columns aren't sortable on the screen, but you can sort the columns after downloading CSV to Microsoft Excel.</p>
Capture Activities	<p>Set the report parameters, and then click Run.</p> <p>Shows the following information about user activities for the specified period, sorted by date in descending order (most recent activity at the top):</p> <ul style="list-style-type: none">• Name or Document—The name and ID of the asset or document.• Content Type—The content type the item or document is based on, or digital asset.• Activity—The type of activity that occurred.• Activity Detail—The specifics of the activity.• Version—The asset version.• Performed by—The user that performed the activity.• Date—The date and time the activity occurred (based on UTC timezone). <p>You can filter by repository, date, item type, and activity type; or search for specific activities. If you selected Business Asset, you can also filter by content type.</p> <p>The columns aren't sortable on the screen, but you can sort the columns after downloading CSV to Microsoft Excel.</p>

Report	Description
Asset Details	<p data-bbox="906 233 1341 285">Set the report parameters, and then click Run.</p> <p data-bbox="906 289 1377 373">Shows the following information about all the assets in the specified repository for the specified period:</p> <ul data-bbox="906 384 1377 1608" style="list-style-type: none"><li data-bbox="906 384 1377 436">• Name—The name of the asset. Click the name to view the asset.<li data-bbox="906 447 1377 520">• Created Date—The date and time the asset was created (based on UTC timezone).<li data-bbox="906 531 1377 604">• Modified Date—The date and time the asset was last modified (based on UTC timezone).<li data-bbox="906 615 1377 667">• Repository—The repository in which the asset is stored.<li data-bbox="906 678 1377 730">• Status—The approval status of the asset.<li data-bbox="906 741 1377 793">• Targeted Channels—Any channels the asset is targeted to.<li data-bbox="906 804 1377 856">• Published Channels—Any channels the asset has been published to.<li data-bbox="906 867 1377 940">• Published Date—The date and time the asset was last published (based on UTC timezone).<li data-bbox="906 951 1377 1003">• Collection—Any collections the asset belongs to.<li data-bbox="906 1014 1377 1066">• Created By—The user that created the asset.<li data-bbox="906 1077 1377 1129">• Modified By—The user that last modified the asset.<li data-bbox="906 1140 1377 1192">• Language—The language assigned to the asset.<li data-bbox="906 1203 1377 1234">• Age—The age of the asset (in days).<li data-bbox="906 1245 1377 1266">• Version—The asset version.<li data-bbox="906 1276 1377 1329">• Total Size—The size of the asset (in MBs).<li data-bbox="906 1339 1377 1392">• Asset Type—The asset type the item is based on.<li data-bbox="906 1402 1377 1455">• Category Name—Any categories applied to the asset.<li data-bbox="906 1465 1377 1518">• Category Path—The taxonomy paths for any categories applied to the asset.<li data-bbox="906 1528 1377 1581">• Category API Name—The API IDs for any categories applied to the asset.<li data-bbox="906 1591 1377 1608">• Asset ID—The ID of the asset. <p data-bbox="906 1619 1377 1692">The remaining columns show all other custom attributes included in your asset types.</p> <p data-bbox="906 1703 1377 1755">You can filter the report by repository, created date, updated date, or asset type.</p> <p data-bbox="906 1766 1377 1881">You can sort the columns on the screen by name, created date, or modified date. You can sort all the columns after downloading CSV to Microsoft Excel.</p>

Report	Description
Untouched Documents	<p>Set the report parameters, and then click Run.</p> <p>Shows the following information about the documents that haven't been touched for the specified period, sorted by days untouched in descending order (longest untouched at the top):</p> <ul style="list-style-type: none"> • Name—The name of the document. • Version—The document version. • Date of Last Activity—The date the document was last touched. • Days Untouched—The number of days since the document was last touched. • Parent—The name of the parent folder. • GUID—The unique identifier of the document. • Creator—The user who created the document. • Created Date—The date the document was created. • File Size—The size of the document, in megabytes. <p>You can sort all the columns on the screen or after downloading CSV to Microsoft Excel.</p>

The User List and User Logins by Device Type reports are based on the entire history of your Oracle Content Management instance. The Documents Usage Log, Asset Activities, User Activities, and Capture Activities reports are based on the last three months of activity.

For more information on the analytics data and the features available in the charts, graphs, and reports, see [Understand Analytics](#). For example, you can download a

CSV file containing the data being displayed by clicking .

You can view additional metrics in the Oracle Cloud Console or the Infrastructure Classic Console, depending on the type of your Oracle Content Management subscription:

- [Oracle Content Management *running* on Oracle Cloud Infrastructure \(OCI\) managed with the *Oracle Cloud Console*](#)
- [Oracle Content Management *built* on Oracle Cloud Infrastructure \(OCI\) managed with the *Infrastructure Classic Console*](#)
- [Oracle Content Management on Oracle Cloud Infrastructure Classic](#)
- [Oracle Content Management for Government](#)
- [Oracle Content Management for SaaS](#)
- [Non-metered subscription with an Oracle Content Management entitlement](#)

7

Manage the Service

You can manage and monitor your service in the following ways:

- [Manage vanity domains.](#)
- [Edit an instance.](#)
- [Monitor your instances.](#)
- [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.

Note:

If you purchased your subscription prior to September 2019, the way you monitor your service may vary. See [Manage Oracle Content Management in Legacy Environments](#).

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 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"> Select an available Virtual Cloud Network (VCN) or have the system create one for you. Select a regional subnet that has network access to the private load balancer IP through LPG peering.
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"> Protocol : TCP Port: 443 Interval in ms: 30000 Timeout in ms: 10000 Number of retries: 3
Use SSL	Select this option to apply SSL. <ul style="list-style-type: none"> SSL Certificate: Paste the full certificate chain for your friendly management domain certificate in PEM format. Specify CA Certificate: Paste the root CA certificate in PEM format. Specify Private Key: Paste the private key in PEM format.
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"> • SSL Certificate: Paste the full certificate chain for your friendly management domain certificate in PEM format. • Specify CA Certificate: Paste the root CA certificate in PEM format. • Specify Private Key: Paste the private key in PEM format.
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.

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
<p>License Type</p>	<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"> • Premium Edition: Subscribe to a new full-featured Oracle Content Management license. • BYOL License*: Use your existing Oracle WebCenter Middleware license (BYOL). • Starter Edition: 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. <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 Oracle PaaS and IaaS Universal Credits Service Descriptions for a description of which WebCenter products qualify for BYOL licensing and for the conversion ratios for WebCenter processor licenses.</p>
<p>License Options</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"> • Sales Accelerator—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 purchased an Oracle Sales Accelerator subscription, select Sales Accelerator. • Sauce Video—Sauce Video 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 Video Creation Platform. <div data-bbox="997 1591 1458 1814" style="border: 1px solid #0070C0; padding: 10px; margin-top: 10px;"> <p> Note:</p> <p>If you're an Oracle SaaS customer, you must have purchased a Sauce Video subscription to see this option.</p> </div>

Field	Description
Instance Type (not supported in Starter Edition)	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 billed at different rates . If you need to change the instance type, select the new type.
Deployment Options	<p>Optionally, enable additional deployment options:</p> <ul style="list-style-type: none"> • OCI services content sharing—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. If your instance was created before mid-February 2023 and you want to enable content sharing for the instance, select OCI services content sharing. Once this option has been enabled, it can't be disabled.

7. Click **Save Changes**.

Monitor Your Instances

You can monitor your Oracle Content Management instances in the Oracle Cloud Console.

To see an overview of your Oracle Content Management instances, in the Oracle Cloud Console, click  in the top left to open the navigation menu, click **Developer Services**, then click **Content Management**. Alternatively, you can click **Overview** under Content Management.


You can perform the following tasks on the Overview page.

- To [create a new Oracle Content Management instance](#), click **Create Instance**.
- To view a summary of your Oracle Content Management instances, expand the **Instances** section. When expanded, you see how many of each instance type (Premium, Starter, or BYOL) you have. To view existing instances, click the link under the instance type or click **Instances** in the left navigation, and you'll be brought to the Instances page. To create a new instance of a particular type, click **Create Instance** under that instance type.
- You can also see a quick picture of the status of your instances in the **Service Health** tile, which shows the number of instances that are active, that have failed, and that have been deleted. Click the service health icon to view more details on the Instances page.
- To view documentation and other user assistance, click the links under **What's New** and **Help**.

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 Oracle Cloud Console, click , click **Billing & Cost Management**, then click one of the following options:
 - **Subscriptions:** View subscriptions detail, usage information, billing schedule, and rate card information.
 - **Invoices:** View and download invoices for your usage.
 - **Payment History:** track and monitor your Oracle Cloud paid invoice history. Only *paid* invoices are shown on this page, in contrast to the Invoices page, which shows all invoices.
 - **Upgrade and Manage Payment:** Upgrade your services and manage how you pay for your usage.
 - **Cost Analysis:** Provides easy-to-use visualization tools to help you track and optimize your spending.
 - **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.

- **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](#).

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**.

A

Troubleshoot

This section helps you troubleshoot administrative functions for Oracle Content Management.

- [I can't access the administration pages](#)
- [No one can add files to their accounts](#)
- [I need to change the storage quota for a user](#)
- [I need to reassign someone's files](#)
- [I created a user but can't find the user in the system](#)
- [I granted roles to more users than were purchased](#)
- [Users can't connect to the service using the sync client](#)
- [I need to find out who deleted a file or folder](#)

I can't access the administration pages

Make sure you have been granted the Oracle Content Management Administrative role for the service instance.

Note:



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. If your region has been updated, follow the steps marked [IAM](#). If your region hasn't been updated, follow the steps marked [IDCS](#).

IAM

1. Sign in to [Oracle Cloud](#). You can find your account name and login information in your welcome email.
2. In the Oracle Cloud Console, click **Identity & Security**, then, under **Identity**, click **Domains**.
3. On the Domains page, open your identity domain.
4. In the navigation menu on the left, click **Oracle Cloud Services**.
5. 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.
6. On the CECSAUTO_instanceCECSAUTO application details page, in the navigation menu on the left, click **Application Roles**.

7. Find the [application role](#) you're looking for, click the link under **User assignments**, and look for your user name. The following roles include varying access to the administration pages:
 - CECServicesAdministrator
 - CECDeveloperUser
 - CECContentAdministrator
 - CECRepositoryAdministrator

IDCS

1. Sign in to [Oracle Cloud](#). 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 **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 **Applications**.
5. Click the name of the service you want check.
6. Find your user name, and hover over the roles to all the [application roles](#) you've been assigned. The following roles include varying access to the administration pages:
 - CECServicesAdministrator
 - CECDeveloperUser
 - CECContentAdministrator
 - CECRepositoryAdministrator

No one can add files to their accounts

When you purchase a subscription, you can specify a number of users and an amount of storage space. After the storage space limit is reached, you can't add any more files. You must have users delete files, or you must purchase more storage space.

I need to change the storage quota for a user

If you need to change the storage quota for a user, you can do so in the System Settings.

You can [set a default quota](#) for the amount of storage space that a user is allocated. If you need to override the default for a particular user you can do so using the following steps.

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** menu, click **Users**.

3. Search for the user whose settings you want to override and click **Edit** next to the user's name.
4. In the **User Quota** box, enter the quota amount in gigabytes, and then click **Save**. You can see how much storage the user has used next to **Storage consumed**.

I need to reassign someone's files

When people leave your organization or change roles, you might want to assign their files and folders to someone else and add their storage quota back to the total quota you have available for assignments. You can assign a person's entire library of content to someone else. The content appears as a folder in the new user's root folder. All of the sharing actions, such as members and public links, remain intact.

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** menu, click **Users**.
3. Find the user whose files you want to transfer using one of the following methods:
 - To find an active user, on the **Search** tab enter part of the user name, display name, or email address in the text box and click **Search**. Open the user properties by clicking the user name or clicking **Edit** next to the user.
 - To find a deprovisioned user, click the **Deprovisioned Users** tab. You see a list of all users who have been removed from your organization's system, sorted by name. This list is refreshed on a regular basis, but you can also update it manually by clicking **Sync Profile Data**. To download a CSV file of all deleted users, click **Export Deprovisioned Users**.
4. Click **Transfer Ownership**. For active users, the button is at the bottom of the properties. For deprovisioned users, click the button next to the user you want.
5. Enter part of the user name, display name, or email address of the person who will receive the content and click **Search**.
6. Select the user you want to transfer the content to. A message shows that the content will increase the recipient's quota by the amount of content being transferred. It also shows you how much storage will be released back into the total quota you have available.
7. Click **Transfer**. The content is transferred and the list shows that the deprovisioned account is gone.

Alternatively, for deprovisioned users, you can delete the content. On the **Deprovisioned Users** tab, next to the user whose content you want to delete, click **Delete Content**.

Users can also transfer ownership of their own folders.

I created a user but can't find the user in the system

Users are provisioned when they sign in to the system. After the user signs in, the user name appears on administration pages.

I granted roles to more users than were purchased

The identity domain doesn't restrict the number of users you can assign roles, but when the service reaches the purchased limit, additional users can't sign in unless you either deprovision some users or purchase additional users.

Users are provisioned on their first sign in, so this is handled on a first-come, first-serve basis.


Users can't connect to the service using the sync client

If you use Man In The Middle (MITM) proxies, you need to copy the self-signed MITM proxy into the Java key store. Contact Oracle Support for help with this issue.

I need to find out who deleted a file or folder

If a file or folder was deleted within the last three months, and you need to find out who deleted it, you can view the Documents Usage Log.

1. After you sign in to the Oracle Content Management web application as an administrator, click **Analytics** in the navigation menu.
2. In the **Analytics** menu, select **Reports and Metrics**.
3. Select **Documents Usage Log**.
4. Set the date range (within the last three months). The Documents Usage Log reports only the last three months of activity.
5. In the Action list, select **Move to Trash** or **Move Revision to Trash**, and then click **Refresh**.

Click  to export the data as a CSV file.

B

Supported Software, Devices, Languages, and File Formats

Oracle Content Management supports various web browsers, software, devices, languages, and file formats.

- [Supported Web Browsers](#)
- [Supported Software](#)
- [Supported Mobile Devices](#)
- [Supported Languages](#)
- [Supported File Formats](#)

Supported Web Browsers

Oracle Content Management supports the latest version at the time of release of each of the following four major browsers:

- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Apple Safari

For more detail, see [Oracle Software Web Browser Support Policy](#).

When sharing a link to a document or folder, users of Microsoft Edge need to use the **Show Link** button, and copy the link shown in the dialog.

Supported Software

Oracle Content Management supports the following software:

- Microsoft Windows 10 Version 2004 (OS Build 19041) or later, and Microsoft Windows 11 (64-bit only)
Notice: Microsoft Windows 32-bit versions aren't supported.
- Microsoft Office 2016, 2019, and 2021
- Microsoft Outlook 2016, 2019, and 2021
- Microsoft 365 (aka Office 365)
- Apple macOS Big Sur (11), Monterey (12), Ventura (13)

The Content Capture Client is available only for Microsoft Windows.

Supported Mobile Devices

Oracle Content Management mobile apps can run on the following devices:

- Apple iPhones running iOS 15.7 or higher
- Apple iPads running iPadOS 15.7 or higher
- Android phones and tablets running Android 11 or higher

Supported Languages

Oracle Content Management offers localized user experiences for its web interface and desktop and mobile apps. The following languages are available:

- Arabic (ar)—web interface only
- Czech (cs)
- Danish (da)
- German (de)
- Greek (el)
- English (en)
- Spanish (es)
- Finnish (fi)
- French (fr)
- French - Canada (fr_CA)
- Hungarian (hu)
- Italian (it)
- Japanese (ja)
- Korean (ko)
- Dutch (nl)
- Norwegian - Bokmål (no, nb_NO)
- Polish (pl)
- Portuguese (pt)
- Portuguese - Brazil (pt_BR)
- Romanian (ro)
- Russian (ru)
- Slovak (sk)
- Swedish (sv)
- Thai (th)
- Turkish (tr)
- Chinese - Simplified (zh_CN)
- Chinese - Traditional (zh_TW)

The languages in the table refer to the user interface and help content only. Oracle Content Management can handle document content, file names, conversation messages, etc. in many additional languages, including multibyte characters. For sites and content items you create in Oracle Content Management, you can provide translations in any languages you choose.

Web Interface

By default, the web interface language is set to match the web browser locale, but users can override this in their user preferences (on the General page). If users change their language setting, the change won't take effect until the next time they sign in. See *Customize Your Profile and Settings in Collaborating on Documents with Oracle Content Management*.

Service administrators can configure a fallback language to be used if no web browser locale setting is available. See [Set the Default Locale Settings](#).

Arabic and right-to-left language support has some limitations, described in *Known Issues for Oracle Content Management*.

Desktop and Mobile Apps

The user interface language for the desktop and mobile apps is set automatically based on the user locale set for the operating system. You can't override this language setting. For example, if a user is running the desktop app on a Spanish version of Microsoft Windows, then the desktop app will also be in Spanish.

The Thai language is not supported for the desktop app on Mac computers.

Supported File Formats

Oracle Content Management can display or play the content of a wide variety of files directly in the web client or mobile apps.

Here are a few best practices:

- It's best to use MP4 formats.
- Files over 10 MB aren't full-text indexed.
- Maximum upload size is controlled by a setting on the [General settings page](#) in the system administration area.
- File names are limited to the characters and length supported by Windows and Macintosh.

Supported Audio and Video File Formats

Web client: When viewing the web client in a browser that supports the HTML5 <video> element, the supported video formats play directly in the Oracle Content Management interface. When viewing the web client in other browsers and viewing unsupported video formats, you must download the file and view it outside the Oracle Content Management interface.

The following formats are supported for viewing directly:

- Chrome—MP4, WEBM, and OGG
- Firefox—MP4, WEBM, and OGG
- Safari—MP4










iPhone/iPad app:





- Videos formats—MP4, M4V, MOV
- Audio formats—MP3, AAC, WAV (for iPhone voice memos), MOV
Some MOV formats might not be viewable.

Android app:

- Videos formats—3GP, MP4, WEBM, MKV
- Audio formats—MKV, OGG, IMY, OTA, RTTTL, RTX, MP3, 3GP, FLAC, MID, XMF, MXMF, AAC, M4A, WAV

Supported Image and Business File Formats

Extension	Description	Full-Text Indexed
PSD	Adobe Photoshop	
DWG	AUTOCAD	
BMP	bitmap images	
VCAL	Calendar	
CSV	comma-separated values	
VCARD	Contacts (electronic business cards)	
CDR	CorelDRAW	
WPD	Corel WordPerfect	
SHW	Corel WordPerfect presentations	
QPW	Corel WP Quattro	
MSG, EML	Email (various)	
EPS	Encapsulated Postscript	
GIF	GIF images	
WEBP	WebP images	
URL	Internet Shortcut File	
JP2, JPG, JPEG	JPEG images	
123	Lotus 1–2–3	
LWP	Lotus WordPro	
WEBLOC	Mac Internet Shortcut File	
HTM, HTML	Hypertext Markup Language (HTML) files	
XML	eXtensible Markup Language (XML) files	
XLT, XLTX	Microsoft Excel templates	
XLS, XLSX	Microsoft Excel workbooks	
PPT, PPTX	Microsoft PowerPoint presentations	
SLDX	Microsoft PowerPoint slides	
POT, POTX	Microsoft PowerPoint templates	
VSD, VST, VSS, VSW	Microsoft Visio	
DOC, DOCX	Microsoft Word documents	
DOT, DOTX	Microsoft Word templates	
WRI	Microsoft Write	

Extension	Description	Full-Text Indexed
ODS, ODP, ODT, OTT, OTS, OTG, OTP	OpenOffice/LibreOffice documents	
PNG	PNG images	
PDF	Portable Document Format (Adobe Acrobat)	
PS	Postscript	
RTF	Rich Text Format	
SVG	Scalable Vector Graphics	
TXT*, TEXT*, LIST, LOG, C, CPP, H, JAVA, JSON, KEY, BAT, SH, M, MD, MM, PLIST	Plain-text files (various)	 (formats marked with *)
TIF, TIFF	TIFF images	

C

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. 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"> oce-instance oce-instances oce-workrequest oce-workrequests oce-instance-family 	<ul style="list-style-type: none"> OCE_INSTANCE_INSPECT OCE_INSTANCE_WORKREQUEST_INSPECT OCE_INSTANCE_INSPECT OCE_INSTANCE_WORKREQUEST_INSPECT

READ

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

USE

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

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

MANAGE

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

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

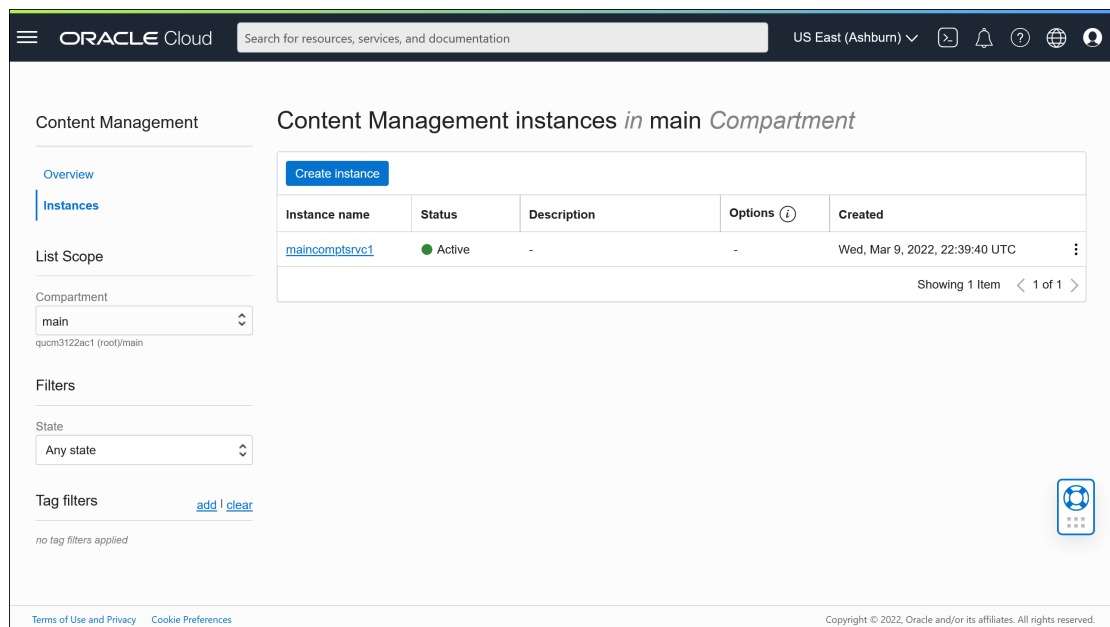
This example shows information associated with the event **CreateOceInstance (begin)**:

```
{
  "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": "ocid1.coreservicesworkrequest.oc1..<unique_ID>",
    "eventName": "CreateOceInstance",
    "compartmentId": "ocid1.compartment.oc1..<unique_ID>",
    "compartmentName": "my_compartment",
    "resourceName": "my_oce",
    "resourceId": "ocid1.contentexperiencecloudservice.oc1..<unique_ID>",
    "availabilityDomain": "<availability_domain>",
    "freeformTags": null,
    "definedTags": null,
    "identity": {
      "principalName": "admin",
      "principalId": "ocid1.user.oc1..<unique_ID>",
      "authType": "natv",
      "callerName": null,
      "callerId": null,
      "tenantId": "ocid1.tenancy.oc1..<unique_ID>",
      "ipAddress": "<ip_address>",
      "credentials": "ocid1.tenancy.oc1..<unique_ID>/
ocid1.user.oc1..<unique_ID>",
      "userAgent": null,
      "consoleSessionId": null
    },
    ...
  }
}
```

D

Migrate Oracle Content Management

At some point, you might need to migrate an Oracle Content Management instance. For example, if you have Oracle Content Management instances that aren't running on Gen 2 Oracle Cloud Infrastructure (OCI) natively (that is, using the Oracle Cloud Console to manage service instances), Oracle recommends that you migrate those instances to this new *native* OCI environment. This will ensure that you'll enjoy the benefits and advances of Oracle's cloud platform in the future. Or you might want to move an instance running on Gen 2 OCI to a different region.



To initiate migration, you'll need to perform a few premigration steps and work with Oracle Support to schedule the migration.

The only automated migration paths currently supported are from these environments:

- [Oracle Content Management on OCI Gen 2, OCI Gen 1, or OCI Classic](#)
- [Oracle Content Management on legacy Cloud Infrastructure using a non-metered subscription](#)

Automated migration from other deployment environments will be supported at a later date. For instances with limited data and files, a manual migration may be an option. Sign in to your Oracle Support account, and see [Migrating Legacy Oracle Content & Experience Cloud to Oracle Cloud Infrastructure \(OCI\)](#).

You can also migrate files into Oracle Content Management as assets.

Migrate an Oracle Content Management Instance

If you have an Oracle Content Management instance running on Oracle Cloud Infrastructure (OCI) Gen 1 or OCI Classic, Oracle recommends that you migrate the instance to the new *native* OCI environment—Gen 2 OCI (that is, using the Oracle Cloud Console to manage service instances). This will ensure that you'll enjoy the benefits and advances of Oracle's cloud platform in the future. Or you might want to move an instance running on Gen 2 OCI to a different region.



Note:

If your instance is running on legacy Cloud Infrastructure using a non-metered subscription, follow the steps in [Migrate an Oracle Content Management Instance from Legacy Cloud Infrastructure](#) instead.

To initiate migration, you'll need to perform a few steps prior to migration and work with Oracle Support to schedule the migration.

1. [Create a new instance](#) of Oracle Content Management on OCI with the Oracle Cloud Console. This will be the target instance your data will be migrated to. Do NOT use this instance until migration has been completed.
2. Migrate your users and groups using the appropriate methods. If you're migrating from OCI Classic, you don't need to migrate your groups. 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 old instance (the *source*) and your new instance (the *target*) [use IAM identity domains or not](#), you'll use different methods to migrate your users.

Exporting Users and Groups from Your Old Source Instance

- If your source instance uses IDCS, use the IDCS user export and group export features to export your users and groups.
- If your source instance uses IAM, use the IAM [import users](#) and [import groups](#) features to export your users and groups.

Make sure to preserve the user names so that roles and permissions can be migrated appropriately as part of the migration process. In the exported CSV file, it's the "User Name" entry.

Importing Users and Groups to Your New Target Instance

- If your target instance uses IDCS, use the IDCS user import and group import features to import your users and groups.
 - If your target instance uses IAM, use the IAM [import users](#) and [import groups](#) features to import your users and groups.
3. [Prepare for migration](#) by collecting information you'll need for your service request and creating a list of any integrations you have for steps you'll need to take after migration.
 4. [Submit a migration service request](#), and confirm the date and time of your migration.

5. [Watch the progress of the migration](#). Your service request will be updated as your migration progresses, and when it's done, you'll be asked to verify that your new instance is working as expected.
6. [Finalize the migration](#) by completing any steps necessary to migrate any integrations that your instance has with other services or applications.
7. [Communicate the change to your users](#).

Prepare for Migration

You need to gather some information to prepare for migration:

- Make a note of the URL of the new instance (the *target*) you created, to include it in your migration request.
- Make a note the URL of your old instance (the *source*), to include it in your migration request.
- Make an inventory of all integrations that your old instance has with any other services or applications, either directly or through REST API calls. If there are any such integrations, then you'll need to take some actions after the migration.

Submit a Migration Request

When you're ready for your migration, you must submit a migration request to get the process started:

1. Sign in to Oracle Cloud Support.
2. Create a new service request.
3. For the **Problem Type**, select **Service Instance Migration**, then select the option appropriate for your migration:
 - **From OCI-Gen1 to OCI-Gen2**
 - **From OCI-Gen2 to OCI-Gen2**
 - **From OCI-Classic to OCI-Gen2**
4. Provide the following information in your service request:
 - The URL of your source instance (the instance you're migrating from)
 - The URL of your target instance (the instance you're migrating to)
 - If you use Akamai delivered by Oracle, mention that so we can update the URLs in your Akamai configuration after migration
5. Provide the preferred date you would like migration to start. We recommend that you give two weeks advanced notice.

 **Note:**

We'll attempt to schedule your migration based on your requested date, but this may not always be possible given competing ongoing activities.

6. Submit your service request.

After Oracle Support receives your migration service request, they'll work with you to finalize a date that works for you and Oracle, and the service request will be updated with the date and time your migration will start.

7. Confirm in the service request that you approve the migration start date and time.

Updates will be made to the service request to show how the migration is progressing. The data migration will be done at the back end; no action is required at your end other than to keep up with any service request updates, and to validate the migration after it's done.

The Migration Process

Here's what happens during the migration:

1. Oracle Support updates the service request when migration begins.

Important:

At this point, you must not make any changes to your old (source) instance. Any changes made after migration starts won't be migrated to your new instance.

2. Your content and configuration data is exported from your old instance (the *source*), and imported into your new instance (the *target*).
3. When the migration is complete, Oracle Support updates the service request, and you're asked to validate your new instance to make sure everything is working as expected.
4. If you find any problems, note them in the service request. Oracle Support will work to resolve the issues, and will let you know through the service request when the instance is ready for validation.
5. When everything is working as expected, note in the service request that you accept the migrated instance.
6. Delete the old instance so you won't continue to be charged for it.

Finalize the Migration

If your old instance integrated or communicated with other services or applications, either directly or through REST API calls, you might need to perform post-migration tasks.

The following items apply service-wide:

- Credentials aren't migrated, so you'll need to reconfigure user credentials for all integrations that use them.
- The Oracle Content Management URL pattern is different, so you'll need to update the URLs in your integrations that use them.

The old URLs used the following pattern:

`https://<service-name>-<account-name>.<region>.oraclecloud.com/documents`

The new URLs used the following pattern:

<https://<service-name>-<account-name>.<service-type>.ocp.oraclecloud.com/documents>

Integration	Things to Do After Migration
Oracle Integration	<ul style="list-style-type: none"> Reconfigure credentials. Update Oracle Content Management URLs in Oracle Integration Cloud.
Oracle Commerce Cloud	<ul style="list-style-type: none"> Reconfigure credentials. Update Oracle Content Management URLs in Oracle Commerce Cloud.
Oracle Content Capture	<ul style="list-style-type: none"> Reconfigure credentials.
Oracle Process Cloud Service	<ul style="list-style-type: none"> Reconfigure credentials.
Oracle Eloqua Cloud Service	<ul style="list-style-type: none"> Reconfigure credentials.
Oracle Intelligent Advisor	<ul style="list-style-type: none"> Reconfigure credentials.
Oracle Cobrowse Cloud Service	<ul style="list-style-type: none"> Reconfigure credentials.
Responsys	<ul style="list-style-type: none"> Reconfigure credentials.
Visual Builder Cloud Service (VBCS)	<ul style="list-style-type: none"> Reconfigure credentials. Update Oracle Content Management URLs in VBCS components.
CDN/Akamai	<ul style="list-style-type: none"> If you use Akamai delivered by Oracle, we'll update the Oracle Content Management URLs in your Akamai configuration after you verify your migration. Otherwise, you must update the URLs in your CDN configuration yourself.
REST API calls	<ul style="list-style-type: none"> Update Oracle Content Management URLs in any REST API calls.
Client SDK/CLI usage	<ul style="list-style-type: none"> If the URL is persisted/cached locally on the client side, then update Oracle Content Management URLs in the configuration.
Connectors	<ul style="list-style-type: none"> Reconfigure credentials.



Note:

Any bookmarks to content on your old instance will no longer work because the URL of your new instance has changed.

Communicate the Change to Users

Communicate the new service URL to your users. Desktop and mobile users will need to configure their devices with a new account and resynchronize all content.

Migrate an Oracle Content Management Instance from Legacy Cloud Infrastructure

If you have Oracle Content Management instances running on legacy Cloud infrastructure using a non-metered subscription, Oracle recommends that you migrate those instances to the new *native* Oracle Cloud Infrastructure (OCI) environment—Gen 2 OCI (that is, using the Oracle Cloud Console to manage service instances). This will ensure that you'll enjoy the benefits and advances of Oracle's cloud platform in the future.

To initiate migration, you'll need to perform a few steps prior to migration and work with Oracle Support to schedule the migration.

1. Migrate your subscription to a universal credits subscription. Contact your Oracle Sales representative to assist you with this.
2. [Create a new instance](#) of Oracle Content Management on OCI with the Oracle Cloud Console. This will be the target instance your data will be migrated to. Do NOT use this instance until migration has been completed.
3. Migrate your users from traditional cloud accounts to Oracle Identity Cloud Service (IDCS) accounts. Make sure to preserve user names so that roles and permissions can be assigned appropriately as part of the migration process. In the exported CSV file, the user name entry is called "User Login". The application roles will be assigned according to the [user mapping](#).
4. [Prepare for migration](#) by collecting information you'll need for your service request and creating a list of any integrations you have for steps you'll need to take after migration.
5. [Submit a migration service request](#), and confirm the date and time of your migration.
6. [Watch the progress of the migration](#). Your service request will be updated as your migration progresses, and when it's done, you'll be asked to verify that your new instance is working as expected.
7. [Finalize the migration](#) by completing any steps necessary to migrate any integrations that your instance has with other services or applications.
8. [Migrate your sites that include assets](#) and make them multilingual compliant.
9. [Migrate your assets](#) that were excluded from migration.
10. [Communicate the change to your users](#).

User Mapping

This table describes the mapping of Oracle Content Management permission groups to OCI application roles.

Oracle Content Management Permission Group	OCI Application Role
DocumentsServiceUser	CECStandardUser
DocumentsServiceAdmin	CECServiceAdministrator
SitesServiceVisitor	CECSitesVisitor
SitesServiceAdmin	CECSitesAdministrator
ContentAdministratorRole	CECContentAdministrator
CECSStandardUser	CECStandardUser
CECSEnterpriseUser	CECEnterpriseUser



Note:

If the target IDCS domain already contains a user with the same user name, the user will be assigned the OCI application roles corresponding to the user's Oracle Content Management permission groups.

Prepare for Migration

- Make a note of the URL of the new instance (the *target*) you created, to include it in your migration request.
- Make a note the URL of your old instance (the *source*), to include it in your migration request.
- Make an inventory of all integrations that your old instance has with any other services or applications, either directly or through REST API calls. If there are any such integrations, then you'll need to take some actions after the migration.

Submit a Migration Service Request

When you're ready for your migration, you must submit a migration request to get the process started:

1. Sign in to Oracle Cloud Support.
2. Create a new service request.
3. For the **Problem Type**, select **Service Instance Migration**, then choose **From Non-Metered Subscription to OCI-Gen2**.
4. Provide the following information in your service request:
 - The URL of your source instance (the instance you're migrating from)
 - The URL of your target instance (the instance you're migrating to)
 - If you use Akamai delivered by Oracle, mention that so we can coordinate a time to update the URLs in your Akamai configuration after migration
5. Provide the preferred date you would like migration to start. We recommend that you give two weeks advanced notice.

 **Note:**

We'll attempt to schedule your migration based on your requested date, but this may not always be possible given competing ongoing activities.

6. Submit your service request.
After Oracle Support receives your migration service request, they'll work with you to finalize a date that works for you and Oracle, and the service request will be updated with the date and time your migration will start.
7. Confirm in the service request that you approve the migration start date and time.

Updates will be made to the service request to show how the migration is progressing. The data migration will be done at the back end; no action is required at your end other than to keep up with any service request updates, and to validate the migration after it's done.

The Migration Process

Here's what happens during the migration:

1. Oracle Support updates the service request when migration begins.

! Important:

At this point, you must not make any changes to your old (source) instance. Any changes made after migration starts won't be migrated to your new instance.

2. Your content and configuration data is exported from your old instance (the *source*), and imported into your new instance (the *target*).
3. When the migration is complete, Oracle Support updates the service request, and you're asked to validate your new instance to make sure everything is working as expected.
4. If you find any problems, note them in the service request. Oracle Support will work to resolve the issues, and will let you know through the service request when the instance is ready for validation.
5. When everything is working as expected, note in the service request that you accept the migrated instance.

**Note:**

The old instance will remain up so that you can refer back to it for validation. You'll also need it to [migrate any sites that use assets](#), and to [migrate any other assets](#) that were excluded during migration.

Finalize the Migration

If your old instance integrated or communicated with other services or applications, either directly or through REST API calls, you might need to perform post-migration tasks.

The following items apply service-wide:

- Review the OCI application roles, and assign roles that didn't exist in your source instance, such as the CECRepositoryAdministrator application role.
- Reconfigure user credentials for all integrations that use them. Credentials aren't migrated.
- The Oracle Content Management URL pattern is different, so you'll need to update the URLs in your integrations that use them.
The old URLs used the following pattern:
`https://<service-name>-<account-name>.<region>.oraclecloud.com/documents`
The new URLs used the following pattern:
`https://<service-name>-<account-name>.<service-type>.ocp.oraclecloud.com/documents`
- Reconfigure [CORS](#) and [embedded content](#) settings. Target service settings aren't migrated.
- Standard sites will be migrated, but enterprise sites won't. Manually migrate enterprise sites and any digital assets and content items that are associated with

the sites by creating a template for each enterprise site, exporting the template from the source instance, and importing it into the target instance.

- Remove or update any custom controllers used in migrated sites.

Integration	Things to Do After Migration
Oracle Integration	<ul style="list-style-type: none"> • Reconfigure credentials. • Update Oracle Content Management URLs in Oracle Integration Cloud.
Oracle Commerce Cloud	<ul style="list-style-type: none"> • Reconfigure credentials. • Update Oracle Content Management URLs in Oracle Commerce Cloud.
Oracle Process Cloud Service	<ul style="list-style-type: none"> • Reconfigure credentials.
Oracle Eloqua Cloud Service	<ul style="list-style-type: none"> • Reconfigure credentials.
Oracle Intelligent Advisor	<ul style="list-style-type: none"> • Reconfigure credentials.
Oracle Cobrowse Cloud Service	<ul style="list-style-type: none"> • Reconfigure credentials.
Responsys	<ul style="list-style-type: none"> • Reconfigure credentials.
Visual Builder Cloud Service (VBCS)	<ul style="list-style-type: none"> • Reconfigure credentials. • Update Oracle Content Management URLs in VBCS components.
CDN/Akamai	<ul style="list-style-type: none"> • If you use Akamai delivered by Oracle, coordinate a time with Oracle Support to update the Oracle Content Management URLs in your Akamai configuration. Otherwise, you must update the URLs in your CDN configuration yourself.
REST API calls	<ul style="list-style-type: none"> • Update Oracle Content Management URLs in any REST API calls.
Client SDK/CLI usage	<ul style="list-style-type: none"> • If the URL is persisted/cached locally on the client side, then update Oracle Content Management URLs in the configuration.
Connectors	<ul style="list-style-type: none"> • Reconfigure credentials.



Note:

Any bookmarks to content on your old instance will no longer work because the URL of your new instance has changed.

Migrate Your Sites That Include Assets

Sites that *don't* include assets will be migrated automatically, but sites that *do* include assets require some additional steps to make them work in your new Oracle Content Management instance.

1. [Install the Oracle Content Management Toolkit.](#)
2. [Register the target server.](#)
3. [Migrate a site.](#)
4. [Perform post-migration steps.](#)
5. [Make your migrated site multilingual site \(MLS\) compliant.](#)

Install the Oracle Content Management Toolkit

The "cec migrate-site" command is new, so you'll need to install the Oracle Content Management Toolkit from webclient git repository even if you've downloaded and installed it previously.

Follow the directions on [sites toolkit page](#) to download and install the Oracle Content Management Toolkit.

Register the Target Server

Register the connection details for the target server (the server you're migrating your sites to):

```
> cec register-server <target_server_name>
    -e http://<target_server>:<target_port>
    -u <target_username> -p <target_password>
    -t pod_ec
```

- The <target_server_name> is used to identify the target endpoint and can be any name you choose.
- The <target_server> and <target_port> make up the URL you use to access the target server.
- The <target_username> and <target_password> must be the user name and password for the person who will export the site templates from the source server so that there won't be permission problems when the templates are imported during migration.
- The value "pod_ec" is the target server type, used to identify what type of server the instance is built on.

Migrate Your Sites

To migrate your sites, perform the following steps:

1. On the source server, create templates from each site that includes assets.
2. On the source server, export each template. Make sure you perform this step as the user you referenced when you registered the target server.
3. On the target server, sign in as a repository administrator (a user with the CECRepositoryAdministrator role). Then, create a repository for the assets that will be imported with the template.
4. For each downloaded template, run the following command, replacing <site_name> with the name you want the site to have on the target server:

```
> cec migrate-site <site_name>
    --template <template_path_and_name>
    --destination <registered_target_server_name>
    --repository <repository_name>
```

5. On the target server, share the migrated sites and assets appropriately.

Post-Migration Steps

After you've migrated your site, it will run using Content REST v1.1 calls. This may cause some issues that need to be resolved before the site runs correctly. Take a look at the following to determine what you need to do:

- If you're using the ContentSDK, your calls will be automatically updated to use v1.1 Content REST calls.
- If your content layouts do not say they support v1.1, the ContentSDK will also add in the "data" entry (v1.0) in the response which will simply point to the "fields" entry (v1.1) so your templates may continue to work without change.
- If you are using the "fields.type.equals=" v1.0 Content REST syntax in your additional query string, we do try to parse and modify this to be v1.1 syntax but you should validate this.
- If you are making any direct (rather than via the ContentSDK) Content REST v1.0 calls these will fail. You will need to fix your custom code and upgrade these calls.
- Likewise you need any custom content queries that make "fields.type.equals=" v1.0 syntax to be 'q=(type eq "..")' syntax.
- "updateddate" vs. "updatedDate": This is supposedly being fixed by CaaS but until we get an EC build where the Content REST v1.1 API supports both values, you need to change any "updateddate" values to be the camelCase: "updatedDate" value.

Make Your Migrated Site Multilingual Site (MLS) Compliant

Once you have your site running correctly, you then need to make your site MLS compliant. If you were to create an Enterprise site in an External Compute server, it would require a default language and localization policy. As your site was copied across, it is a non-MLS site so you need to upgrade it to an MLS site to ensure you can support future functionality.

The following table shows the differences between MLS and non-MLS sites.

Site Object	MLS Site	Non-MLS Site
Content Items	The content item language variant will be displayed, not the content item dropped onto the page. The language can change depending on what language was requested when the site is rendered.	The content item that was dropped onto the page will be displayed always.
Content Layouts	Content Layouts must support v1.1 APIs. If they don't the content item won't appear, instead a warning will be shown. This is because all v1.1 API calls will have a "locale" added that isn't supported in the v1.0 API.	Content layouts can be either v1.0 or v1.1. If the content layout only supports v1.0, the ContentSDK will add a "data" entry in the response to match the "fields" entry. There may be still other issues so this should not be considered a "supported feature" for not upgrading the content layout.

Site Object	MLS Site	Non-MLS Site
Content Lists	Only content items available in the requested language variant will be displayed.	All content items regardless of language will be displayed. The user has the option within the content list to pin the results to a specific language so you can have two content lists on the page showing results in different languages. This settings panel option to choose a language is not available for MLS sites.
defaultLocale	MLS sites have a default site locale. This means that all content queries will only return content items that are in that locale (or non-translatable).	There is no default locale in an non-MLS site so, the content query used returns all content items regardless of language.
Localization Policy	Defines the list of languages available to the site. There will be a drop-down of these in the builder. Also, in the management UI, there will be a drop-down of languages to allow you to open/preview in the requested language.	Since there is no localization policy, the drop-down to switch languages is removed from the builder. In the management UI, there is no language listed, including no "default" language. This is how you recognize non-MLS vs. MLS sites in the management UI.
Translation/Translatable	The context menu in the management UI has "Translate" as an option. This allows you to create a translation job to translate the site.	The context menu in the management UI will have a "Translatable" option. Effectively a non-MLS is non-translatable, so you need to make it a translatable (MLS) site first before you can translate it. This is also how you "upgrade" a site from non-MLS to MLS. Note: This is one-way only. You can't downgrade to non-translatable.

Before you can turn your site into an MLS site, you need to do the following:

- Upgrade all of your content layout components to support Content REST APIs v1.1
- Upgrade any "additional query strings" in your content lists in the site to be Content REST API v1.1 compatible

Then, if you happen to have any custom component code that makes Content REST calls you also need to upgrade these to make v1.1 calls. This is uncommon since most content calls are made from content layouts.

Upgrading Content Layouts

Specifying Supported Content REST API Versions

Content layouts need to specify which version of the Content REST API they support. This is to ensure that the appropriate Content REST call is made to return the expected response data to the layout.

If you do not specify any version support it is assumed the content layout only supports v1.0.

The console will list the content layouts that are still on v1.0.

To allow your content layout to support other versions, add in the "contentVersion" property to your content layout object.

In this example, it says it supports all version between v1.0 and less than 2.0 (Note: 2.0 doesn't exist, but major version changes may introduce breaking changes)

```
// Content Layout
definition.ContentLayout.prototype = {
  // Specify the versions of the Content REST API that are supported
  // by the this Content Layout.
  // The value for contentVersion follows Semantic Versioning syntax.
  // This allows applications that use the content layout to pass
  // the data through in the expected format.
  contentVersion: ">=1.0.0 <2.0.0",
  // Main rendering function:
  // - Updates the data to handle any required additional requests
  // and support both v1.0 and v1.1 Content REST APIs
  // - Expands the Mustache template with the updated data
  // - Appends the expanded template HTML to the parentObj DOM
  // element
  render: function (parentObj)
  {
```

Handling v1.1 Response Changes

The minimum you will need to do is to handle the Content REST API response change from: "data" to "fields". The simplest way to do this is to add back in the "data" property and point to the new "fields" property

```
render: function (parentObj)
{
  ...
  if(!content.data)
  {
    content.data = content.fields;
  }
}
```

A better option is to change to use the v1.1 "fields" value throughout your content layouts. This will involve updating both your JavaScript and template code.

To fully support v1.1, you will need to handle the following Content REST API changes between v1.0 and v1.1:

Content REST API Change	v1.1	v1.0
"fields" vs. "data"	<pre>"items": [{ "type": "Starter- Blog-Author", "name": "Alex Read", "id": "COREB62DBAB5CEDA4915A 9C9F6050E554F63", "fields": { "starter-blog- author_bio": "Alex's bio", "starter-blog- author_name": "Alex Read" } },</pre>	<pre>"items": [{ "type": "Starter- Blog-Author", "name": "Alex Read", "id": "COREB62DBAB5CEDA4915A 9C9F6050E554F63", "data": { "starter-blog- author_bio": "Alex's bio", "starter-blog- author_name": "Alex Read" } },</pre>
camelCase property names	"updatedDate"	"updateddate"
query format	/items?q=(type eq "Starter-Blog-Author")	/items?fields.type.equals="Starter-Blog-Author"
API version	/content/management/api/v1.1/items	/content/management/api/v1/items
language specific queries	/content/management/api/v1.1/items?q=((type eq "Promo") and (language eq "en-US" or translatable eq "false"))	Not supported. You need to migrate all custom v1 calls to include the "language" option. This ensures the results are consistent with those returned for the MLS site when viewed in a specific language.

Upgrading Content Query String

You may be making Content API calls in any custom code so you need to validate all the custom code used by your site that is making Content REST API calls.

- **Custom Components:** Check the following components:
 - Content Layouts
 - Local Components
 - Section Layouts
 - Remote Components
- **Themes: JavaScript:** Though less likely, you may have JavaScript in your theme that is making custom Content REST API calls so those should also be validated.
- **Site Properties: Additional Query String:** Once you've validated that you have upgrade all your custom code making Content REST API calls you should also

upgrade the "Additional Query String" in any "Content List" components on any pages in your site. While we do try to parse and convert these at runtime, they should be upgraded to be compatible v1.1 Content REST calls for continued support.

Converting a Non-MLS Site to MLS

Once you've converted your site to fully support v1.1 Content REST APIs, you can add support for languages by changing into an MLS site.

If you select your site in the site management UI, you will see a "translatable" content menu option. Selecting this option will bring up a dialog asking you to choose a localization policy and a default language for the site from the list of required languages in the localization policy. If no localization policies exist, you will not be able to complete this step and you will first have to go to the content admin screens and create a localization policy with at least one required language.

After completing this step, your site will now render in the default locale. It will also allow you to switch to other locales specified in your localization policy.

You will need to validate that your site renders as expected in your default locale.

Migrate Your Assets

Assets that are associated with sites will be migrated when you migrate your sites, but any assets that aren't associated with sites need to be migrated separately.

Before you begin migration, take into account the following points:

- Only assets associated with a collection can be migrated. If you want to migrate assets that aren't associated with a collection, you must add them to a collection before you can migrate them.
- Non-metered instances don't support languages on assets, so when you migrate your assets, the default language will be inherited from the default language of the repository. Make sure your repository's default language is set to the desired default language *before* you migrate your assets.
- Only published items will be migrated. If, after migration, you're missing items, confirm that the items have been published in the source instance.
- If any of your published items have draft versions, the draft versions will become the published versions on the target instance, and the original published versions from the source instance will be lost.
- In the non-metered version of Oracle Content Management, when viewing a content item, users could choose "Content Layout" view or "Content" view. "Content" view was replaced by **Content Form View** in the current version of Oracle Content Management, and "Content Layout" view was removed.

To migrate your assets, perform the following steps:

1. If you haven't already done so, [install the Oracle Content Management Toolkit](#).
2. [Register the source and target servers](#).
3. [Migrate a collection of assets](#).

Register the Source and Target Servers

Register the connection details for the source and target servers.

Register the source server (the server you're migrating your assets from):

```
> cec register-server <source_server_name>
    -e http://<source_server>:<source_port>
    -u <source_username> -p <source_password>
    -t pod_ic
```

- The <source_server_name> is used to identify the source endpoint and can be any name you choose.
- The <source_server> and <source_port> make up the URL you use to access the source server.
- The <source_username> and <source_password> must be the user name and password for the person who can access the assets on the source server.
- The value "pod_ic" is the source server type, used to identify what type of server the instance is built on.

Register the target server (the server you're migrating your assets to):

```
> cec-install % cec register-server <target_server_name>
    -e http://<source_server>:<source_port>
    -u <target_username> -p <target_password>
    -t pod_ec
```

- The <target_server_name> is used to identify the target endpoint and can be any name you choose.
- The <target_server> and <target_port> make up the URL you use to access the target server.
- The <target_username> and <target_password> must be the user name and password for the person who will own the assets on the target server.
- The value "pod_ec" is the target server type, used to identify what type of server the instance is built on.

Migrate a Collection of Assets

Migrate a collection of assets by running the following command:

```
> cec migrate-content <source_collection_name>
    --server <source_server_name>
    --destination <target_server_name>
    --repository <target_repository_name>
    --collection <target_collection_name>
    --channel <target_channel_name>
```

The assets will be created on the target server in the specified repository and will be associated with the collection and channel. If necessary, the collection and channel will be created automatically. The default language for all migrated assets will be the default language that is set in specified repository.

Communicate the Change to Users

Communicate the new service URL to your users. Desktop and mobile users will need to configure their devices with a new account and resynchronize all content.

Migrate Files to Oracle Content Management Assets

If you currently manage your files in Oracle WebCenter Content or an external repository, there are many reasons to migrate to Oracle Content Management assets. This topic answers some of the questions you may have about migrating to help you decide how to proceed. For additional answers, refer to [File Migration FAQ](#).

Why should I migrate my content to Oracle Content Management assets?

Moving your content to Oracle Cloud and Oracle Content Management provides the following benefits:

- Bring your own license (BYOL), simplifying cloud purchasing and consumption
- Autoscale your environment based on resource usage and user traffic
- Automated zero-downtime patching and upgrading
- [Continuous monitoring](#)
- Create a [private Oracle Content Management instance](#) accessible only through FastConnect
- Built-in [high availability and disaster recovery](#)
- [Always encrypted content](#)

Converting your files to Oracle Content Management assets provides additional benefits:

- Secure REST APIs for content [management](#) and [delivery](#)
- Full-text multilingual search
- Role-based search results
- Smart tagging powered by artificial intelligence (AI)
- Video lifecycle management from creation to streaming with CDN
- Site, portal, and microsite creation capabilities
- State-of-the-art digital asset management (DAM)
- Headless experiences
- Marketing collaboration
- Secure document management with granular permissions

What are my migration options?

Depending on the source and volume of files you're migrating, you use different methods to migrate your content.

Source Repository	Migration Method
Oracle WebCenter Content	<p>For high-volume migrations (more than 500,000 files):</p> <ul style="list-style-type: none"> Oracle WebCenter Content 12c—Use the Object Storage Migration Tool to export your source files to OCI object storage, export your source file metadata to CSV, then work with Oracle Support to finish the migration. Oracle WebCenter Content 11g—Oracle recommends using the following approach to migrate files from Oracle WebCenter Content 11g to Oracle Content Management assets. Upgrade your on-premise Oracle WebCenter Content 11g instance to 12c, and then follow the method above. <p>For moderate-volume migrations (fewer than 500,000 files):</p> <ul style="list-style-type: none"> Use Archiver to export your files to HDA format, and then use Content Capture to import the content and metadata into Oracle Content Management.
External repository	<p>For high-volume migrations (more than 500,000 files):</p> <ul style="list-style-type: none"> Export your files to a common file system, upload them to Oracle Cloud Infrastructure object storage using the Object Storage command line tool or offline data transfer, export your source file metadata to CSV, then work with Oracle Support to finish the migration. <p>For moderate-volume migrations (fewer than 500,000 files):</p> <ul style="list-style-type: none"> Use Content Capture to import content and metadata from external repositories into Oracle Content Management.
Oracle Content Management Documents	<p>For migrations of any volume:</p> <ul style="list-style-type: none"> Work with Oracle Support to perform the migration directly from Documents to assets.

What are the prerequisites for migration?

- Define the target environment and provide the mapping from the source data to the target Oracle Content Management environment.
- Redefine your solution leveraging the features of Oracle Content Management, such as repositories, asset types, taxonomies, and such. This includes configuring the asset type to accept all of the file types (based on file extension) that will be migrated.
- Reimplement security using the Oracle Content Management features of groups, roles, repository security, and granular taxonomy security.
- Define the mapping between source (Oracle WebCenter Content, external repository, or Oracle Content Management Documents) and target (Oracle Content Management).

Migration Process

Migrations follow these basic steps:

- If a migration needs to follow a very specific schedule, submit a service request specifically to facilitate scheduling in advance. Otherwise you'll submit your service request in a later step. We recommend that you give two weeks advanced notice.

 **Note:**

You don't need to submit a service request if you're migrating fewer than 500,000 files from Oracle WebCenter Content (you can [use Archiver and Content Capture](#) to migrate a moderate number of files from Oracle WebCenter Content).

2. [Map your source data structure and security](#) to Oracle Content Management asset features.
3. [Create an Oracle Content Management instance](#).

 **Note:**

This step isn't necessary if you already have an Oracle Content Management instance, for example, if you're migrating files from a Documents folder.

For large deployments you may want to:

- Set up the appropriate primary and non-primary environments for Oracle Content Management (for example, development, staging, and production) within the Oracle Cloud Infrastructure compartment.
 - Enable Identity and Access Management (IAM) to support SSO and user/group synchronization between Active Directory and IAM for the staging identity stripe.
4. Create the Oracle Content Management structure based on your planning. The repositories you create will be the targets your data will be migrated to. The target repositories and all associated taxonomies must remain empty until migration has been completed.
 5. Migrate your files and metadata to Oracle Content Management.

A "migration" targets a single asset type in a single repository. Thus, it's likely that you'll require multiple "migrations" to complete the transfer of your data. For example, the Accounts Payable department of a company may have multiple document types that will be represented by multiple new asset types: Invoice, Purchase Order, Shipping, and such. Each of these is a separate migration.

The migration can be divided into multiple migration passes.

- a. The primary pass is expected to migrate the bulk of the content and thus be the largest pass. While this migration proceeds the source system is assumed to still be in production.
- b. After the primary migration is complete, a "delta" migration can be performed which migrates only the changes that have occurred since the data export for the primary migration was produced.
- c. Multiple deltas are supported until a final delta is small enough to be completed in an acceptable downtime window.
- d. Prior to the final delta, the source system is shutdown for the last time. The delta migration is performed, after which you'll transition production to the new asset-based implementation.

Depending on the source and volume of files you're migrating, you'll perform different steps.

Source Repository	Migration Scenarios
Oracle WebCenter Content	<p>For high-volume migrations (more than 500,000 files):</p> <ul style="list-style-type: none"> • Migrate Files from Oracle WebCenter Content 12c to Oracle Content Management Assets • Migrate Files from Oracle WebCenter Content 11g to Oracle Content Management Assets <p>For moderate-volume migrations (fewer than 500,000 files):</p> <ul style="list-style-type: none"> • Migrate Files from Oracle WebCenter Content Using Archiver and Content Capture
External repository	<p>For high-volume migrations (more than 500,000 files):</p> <ul style="list-style-type: none"> • Migrate Files from an External Content Management System <p>For moderate-volume migrations (fewer than 500,000 files):</p> <ul style="list-style-type: none"> • Use Content Capture to import content and metadata from external repositories into Oracle Content Management.
Oracle Content Management Documents	<p>For migrations of any volume:</p> <ul style="list-style-type: none"> • Migrate Files from a Documents Folder to an Asset Repository

6. Continue with the next migration (the next target repository and asset type) until all your files and metadata have been migrated.
7. Communicate the change to your users.

[File Migration FAQ](#)

Migrate Files from Oracle WebCenter Content 12c to Oracle Content Management Assets

The May 2022 bundle patch for Oracle WebCenter Content 12.2.1.4.0 introduced Object Storage Migration Tool to migrate content from either a file or database storage location to Oracle Cloud Infrastructure object storage. This object storage migration tool leverages a given search criteria to identify documents, and then moves the corresponding files to the new storage provider. Leveraging searches allows for migrating content from different departments (or document types) at different times. It can also provide an “oldest first” approach or an “only the newest” approach. This migration can be performed while the system continues to operate in production.

The following procedure assumes you've already started a service request, mapped your source data structure and security to Oracle Content Management asset features, created your Oracle Content Management instance, and created the asset structure in Oracle Content Management.

To migrate files from Oracle WebCenter Content 12c, perform the following steps:

1. Create an Oracle Cloud Infrastructure object storage bucket for Oracle WebCenter Content.

Although you can create your object storage bucket in any compartment, using the compartment you created for Oracle Content Management during Oracle Content Management instance creation is the most efficient. Consider the following:

- The easiest and fastest migration occurs when the bucket for the source content is created within the Oracle Content Management compartment.
- If the files are uploaded to a compartment in a distant physical location, copying the content to Oracle Content Management will take longer.

- In order for the migration tool to reach the content in a separate compartment, a security grant is required to allow access to the content.


```
Allow service CEC to manage object-family in tenancy

Allow service objectstorage-us-ashburn-1 to manage object-family in tenancy
```
- 2. Use the [Object Storage Migration Tool](#) to export your source files from WebCenter Content to Oracle Cloud Infrastructure object storage.
 - a. The Object Storage Migration Tool is in a new WebCenter Content component (OCIObjectStorage). If necessary, enable the component via the Advanced Component Manager.
 - b. Configure the Oracle WebCenter Content instance to point to the object storage bucket.
 - c. The migration tool works with the My Saved Queries feature of the Content Server. Define a search query for the files you want to migrate using the Search Builder form.
 - d. Run a **Direct Transfer** migration to migrate the files from Oracle WebCenter Content to Oracle Cloud Infrastructure object storage.
 - e. If you want the migration utility to clean up the Oracle WebCenter Content system, run the clean-up process.
 - f. The migration utility runs a verification process to ensure that all the documents selected using the saved search were picked up during the migration job run.
- 3. [Export source file metadata to CSV](#). You'll send this metadata file with your migration service request so that the source content can be properly mapped to the target environment.
- 4. [Submit a file migration service request](#), keeping up with any updates to the service request, and providing information to Oracle Support and the migration team as necessary. Oracle Support will work with you and the migration team to gather additional required details, finalize a migration date, and execute the migration.

Migrate Files from Oracle WebCenter Content 11g to Oracle Content Management Assets

Oracle recommends using the following approach to migrate files from Oracle WebCenter Content 11g to Oracle Content Management assets. Upgrade your on-premise Oracle WebCenter Content 11g instance to 12c (May 2022 bundle patch for Oracle WebCenter Content 12.2.1.4.0), and then follow the procedure for [migrating files from 12c](#).

Migrate Files from an External Content Management System

Content can be migrated from any external content management system to Oracle Content Management using the CSV-based migration approach. Content needs to be exported and made available in a file system along with the relevant metadata in CSV format.

The following procedure assumes you've already mapped your source data structure and security to Oracle Content Management asset features, created your Oracle Content Management instance, and created the asset structure in Oracle Content Management.

To migrate files from an external content management system, perform the following steps:

1. Export the source content to a common file system using an export tool or bulk download. Oracle Consulting or a partner can help with this.
2. [Upload the source files to an Oracle Cloud Infrastructure object storage bucket.](#)
3. [Export source file metadata to CSV.](#) You'll send this metadata file with your migration service request so that the source content can be properly mapped to the target environment.
4. [Submit a file migration service request,](#) keeping up with any updates to the service request, and providing information to Oracle Support and the migration team as necessary. Oracle Support will work with you and the migration team to gather additional required details, finalize a migration date, and execute the migration.

Migrate Files from Oracle WebCenter Content Using Archiver and Content Capture

You can migrate Oracle WebCenter Content environments of moderate volume (less than 500,000 files) using Archiver and Content Capture. The Archiver tool, provided with Oracle WebCenter Content, can export document metadata and the corresponding files based on a provided search criteria. Content Capture, part of Oracle Content Management, can import files in bulk and process them automatically before uploading them to Oracle Content Management. Content Capture implicitly understands the Archiver output file format, simplifying the process of migrating documents from Oracle WebCenter Content to Oracle Content Management.

The following procedure assumes you've already mapped your source data structure and security to Oracle Content Management asset features, created your Oracle Content Management instance, and created the asset structure in Oracle Content Management.

To migrate files from Oracle WebCenter Content using Archiver and Content Capture, perform the following steps:

1. [Use Archiver to manually export your source files](#) from Oracle WebCenter Content into HDA format.

For traditional Oracle WebCenter Content systems, the file content is stored either on the file system or in the database. The Archiver tool, provided by Oracle WebCenter Content, can be used to export file metadata and the corresponding files. Archiver exports content based on a provided search criteria. You can build conditions referencing system or custom metadata fields.

For each Archiver export definition, Archiver creates a folder on the Oracle WebCenter Content server in the shared file space under the Weblogic domain. Within the export folder, Archiver creates subfolders for each performed export by date. The date folders store the metadata and files.

More details about how the Archiver works, can be found at the following links:

- [Managing Archives, Collections, and Batch Files](#)
- [Archive and Migration Strategies](#)

2. Use Content Capture's file import agent to import the content and metadata from the exported HDA files into Oracle Content Management. You configure Content Capture to target the asset repository you created in Oracle Content Management, map the metadata fields from the HDA files to the fields in the Oracle Content Management asset types, and specify how you want your content files and attachments to be processed. Content Capture then uploads the

contents of the archive folder to your repository in Oracle Content Management, and copies the corresponding metadata into the new assets.

Migrate Files from a Documents Folder to an Asset Repository

You migrate files from a single Documents folder to a single asset type in a single repository. All files in the Documents folder and its subfolders will be migrated.

The following procedure assumes you've already mapped your source data structure and security to Oracle Content Management asset features and created the asset structure in Oracle Content Management.

To migrate files from a Documents folder to an asset repository, submit a service request:

1. Sign in to Oracle Cloud Support.
2. Create a new service request.
3. For the **Product**, select **Oracle Content Management**.
4. For the **Problem Type**, select **Service Instance Migration**.
5. Submit your service request. Then make sure to keep up with any service request updates so you can provide additional information when necessary.
6. Oracle Support will work with you to gather additional required details about your migration, including your source and target information, field mappings, and taxonomy definitions.
7. After the details are gathered, Oracle Support will coordinate with the migration team to finalize a migration date that works for you and Oracle. The service request will be updated with the date and time your migration will start.
8. After you confirm in the service request that you approve the migration start date and time, Oracle Support and the migration team will execute your migration request. Updates will be made to the service request to show how the migration is progressing. The data migration will be done at the back end; no action is required at your end other than to keep up with any service request updates, and to validate the migration after it's done.

Your files are managed in the following way during migration:

- The migration process leaves the original files in the source Documents folders.
- For each new asset created during migration, a secondary reference to the original file is made. The files are not copied.
- You're responsible for validating that the migration was successful. Once satisfied, you delete the files and folders from Documents.
- After you delete the files from Documents, the references from Documents are removed.

File Migration FAQ

These questions are grouped into the following categories:

- [General Questions](#)
- [Oracle WebCenter Content Questions](#)

General Questions

1. What are the benefits of migrating my content to Oracle Content Management assets?

Moving your content to Oracle Cloud and Oracle Content Management provides the following benefits:

- Bring your own license (BYOL), simplifying cloud purchasing and consumption
- Autoscale your environment based on resource usage and user traffic
- Automated zero-downtime patching and upgrading
- [Continuous monitoring](#)
- Create a [private Oracle Content Management instance](#) accessible only through FastConnect
- Built-in [high availability and disaster recovery](#)
- [Always encrypted content](#)

Converting your files to Oracle Content Management assets provides additional benefits:

- Secure REST APIs for content [management](#) and [delivery](#)
- Full-text multilingual search
- Role-based search results
- Smart tagging powered by artificial intelligence (AI)
- Video lifecycle management from creation to streaming with CDN
- Site, portal, and microsite creation capabilities
- State-of-the-art digital asset management (DAM)
- Headless experiences
- Marketing collaboration
- Secure document management with granular permissions

2. What are the available migration options?

Depending on the source and volume of files you're migrating, you use different methods to migrate your content.

Source Repository	Migration Method
Oracle WebCenter Content	<p>For high-volume migrations (more than 500,000 files):</p> <ul style="list-style-type: none"> Oracle WebCenter Content 12c—Use the Object Storage Migration Tool to export your source files to OCI object storage, export your source file metadata to CSV, then work with Oracle Support to finish the migration. Oracle WebCenter Content 11g—Oracle recommends using the following approach to migrate files from Oracle WebCenter Content 11g to Oracle Content Management assets. Upgrade your on-premise Oracle WebCenter Content 11g instance to 12c, and then follow the method above. <p>For moderate-volume migrations (fewer than 500,000 files):</p> <ul style="list-style-type: none"> Use Archiver to export your files to HDA format, and then use Content Capture to import the content and metadata into Oracle Content Management.
External repository	<p>For high-volume migrations (more than 500,000 files):</p> <ul style="list-style-type: none"> Export your files to a common file system, upload them to Oracle Cloud Infrastructure object storage using the Object Storage command line tool or offline data transfer, export your source file metadata to CSV, then work with Oracle Support to finish the migration. <p>For moderate-volume migrations (fewer than 500,000 files):</p> <ul style="list-style-type: none"> Use Content Capture to import content and metadata from external repositories into Oracle Content Management.
Oracle Content Management Documents	<p>For migrations of any volume:</p> <ul style="list-style-type: none"> Work with Oracle Support to perform the migration directly from Documents to assets.

3. What are the prerequisites for migration?

- Define the target environment and provide the mapping from the source data to the target Oracle Content Management environment.
- Redefine your solution leveraging the features of Oracle Content Management, such as repositories, asset types, taxonomies, and such. This includes configuring the asset type to accept all of the file types (based on file extension) that will be migrated.
- Reimplement security using the Oracle Content Management features of groups, roles, repository security, and granular taxonomy security.
- Define the mapping between source (Oracle WebCenter Content, external repository, or Oracle Content Management Documents) and target (Oracle Content Management).

4. How long does migration take?

That depends on how much content you're migrating, but we recommend that you give Oracle Support two weeks advanced notice. If a migration needs to follow a very specific schedule, submit a service request specifically to facilitate scheduling in advance.

5. With large volume migrations taking significant time, can we use the production system in the meanwhile?

Yes. No matter what method you use, you can continue using your source system.

A "migration" targets a single asset type in a single repository. Thus, it's likely that you'll require multiple "migrations" to complete the transfer of your data. For example, the Accounts Payable department of a company may have multiple document types that will be represented by multiple new asset types: Invoice, Purchase Order, Shipping, and such. Each of these is a separate migration.

After the primary migration is complete, a “delta” migration can be performed which migrates only the changes that have occurred since the data export for the primary migration was produced. Multiple deltas are supported until a final delta is small enough to be completed in an acceptable downtime window. Prior to the final delta, the source system is shutdown for the last time. The delta migration is performed, after which you'll transition production to the new asset-based implementation.

6. How will we get the delta? We have approximately one million new documents ingested every month.

When you're ready to perform a delta migration, you'll export only those source files that have changed since your last export, and you'll generate a metadata CSV file with the corresponding entries for those new and updated source files.

7. What are the tools to upload content and metadata to OCI object storage?

You can upload content to OCI object storage using the following methods:

- For Oracle WebCenter Content, we recommend you use the [Object Storage Migration Tool](#) in Oracle WebCenter Content 12c (May 2022 bundle patch for Oracle WebCenter Content 12.2.1.4.0). However, it's also possible to [lift and shift your existing content](#) to Oracle Cloud Infrastructure.
- For external content management systems:
 - Use the [Object Storage command line tool](#) to upload the exported documents to the target object storage bucket.
 - [Use offline data transfer](#). Save the content on an external hard drive, send it to Oracle's Object Storage team, and they will upload it to the target object storage bucket.

8. What is the format of the CSV file that supports migration from an external repository to Oracle Content Management? What are the mandatory fields/metadata that need to be included?

The [CSV file](#) should contain all the metadata that needs to be migrated to Oracle Content Management. There are a set of mandatory fields that should be present in the CSV file. Additionally some optional columns and custom metadata can also be included depending on the business requirements.

9. Could I create/upload/migrate a file with a back-dated file creation date?

Yes, we can migrate files with creation date values mapped to creation dates in past (original date in Oracle WebCenter Content or external repository).

If the details are provided, the values will be assigned to the system level asset attributes. An asset will appear to have been created or modified at the given point in the past by the given user.

10. How does the Oracle migration team assist and get involved in bulk migration?

High-volume migrations require the involvement of the Oracle Content Management migration team. Migrations are scheduled by opening a service request with Oracle Support. Oracle Support will work with you and the migration team to gather required migration details, finalize a migration date, and execute the migration.

11. What is the questionnaire that needs to be provided to the migration team to enable migration?

The questionnaire, supplied by Oracle Support, contains details about the target deployment environment, the taxonomy configuration, and the mapping information required to successfully migrate the content and metadata from your

existing source repository to Oracle Content Management. You need to fill out the questionnaire with details for your specific migration, open a service request to schedule the migration, and attach the questionnaire and the corresponding CSV file to the service request.

12. How will we reconcile the objectIDs back into the CSV?

The upload request would include "name" of the object, and the same name would be provided in the CSV file.

13. How does the system maintain a link between the source file (Oracle WebCenter Content or external repository) and target file (Oracle Content Management asset)?

The migration process will produce an output file that provides a mapping from the original unique identifier of the file to the identifier of the newly created asset. Make sure you request to receive this file after migration by answering "yes" to the appropriate question in the questionnaire supplied by Oracle Support.

Oracle WebCenter Content Questions

1. How do I enable the object storage rule in Oracle WebCenter Content?

Refer to [Adding or Editing a Storage Rule](#).

2. What is the impact of network bandwidth speed on the migration tool/job?

The Oracle WebCenter Object Storage Migration Tool runs in both online and offline mode. In online mode content can be transferred to OCI object storage over network. As a benchmarking exercise we could migrate approximately 90,000 files to object storage in about 40 minutes via online method (network transfer) and 20 minutes via offline method (media transfer) using ~10 threads.

3. If I'm using FileStore in Oracle WebCenter Content on-premise, how can I move my content to OCI object storage without impacting business as usual?

Content can be migrated from file storage or object storage without bringing down the Oracle WebCenter Content instance. The migration job can run in background while the Oracle WebCenter Content instance is being used to upload content to file storage.

Typically the active storage rule will define where the content gets uploaded. Migration can be planned in such a way that after the cut-off date any uploaded content will automatically go to object storage.

4. Does the migration tool ensure zero downtime in production?

Yes, migration to OCI object storage can be scheduled in parallel to on-premise usage. The migration tool picks up files for migration based on a saved search that can be defined by the migration administrator/end user. Multiple migration jobs can be configured to run at the backend while the Oracle WebCenter Content instance is being used

5. Does the migration tool move the security model/settings from Oracle WebCenter Content to Oracle Content Management?

No, the migration tool doesn't move the security configuration during migration of the files. However while defining the target repository structure and configuration, access groups and roles can be defined, and users can be mapped to these groups and roles. Additionally, the security settings can be mapped by defining taxonomies in Oracle Content Management, which can then be used to restrict users' access to content at different levels, based on different metadata.

6. How can we replicate the security settings from Oracle WebCenter Content to Oracle Content Management?

The Oracle WebCenter Content security model can be replicated to Oracle Content Management using asset repository membership roles. More granular security can be implemented using taxonomies. You can also create custom roles.

7. Could I use the object storage migration tool on version 11g of Oracle WebCenter Content?

The migration tool is currently supported only in version 12c.

8. How does the Archiver work?

For traditional Oracle WebCenter Content systems, the file content is stored either on the file system or in the database. The Archiver tool, provided by Oracle WebCenter Content, can be used to export file metadata and the corresponding files. Archiver exports content based on a provided search criteria. You can build conditions referencing system or custom metadata fields.

For each Archiver export definition, Archiver creates a folder on the Oracle WebCenter Content server in the shared file space under the Weblogic domain. Within the export folder, Archiver creates subfolders for each performed export by date. The date folders store the metadata and files.

More details about how the Archiver works, can be found at the following links:

- [Managing Archives, Collections, and Batch Files](#)
- [Archive and Migration Strategies](#)

9. Can I use 11g Archiver output to import content into Oracle Content Management?

Yes, 11g Archiver output can be used to import content into Oracle Content Management.

The exported metadata file is in a Oracle WebCenter Content format known as HDA. The HDA file format is text based and has a straightforward structure. Helper Java classes are provided in the Oracle WebCenter Content client RIDC jar for deciphering files of this type.

- The RIDC jar is provided in the Oracle WebCenter Content shiphome at **Oracle-Home/oracle_common/ucm/Distribution/RIDC/oracle.ucm.ridc.jar**.
- In this jar is the `oracle.stellent.ridc.model.serialize.HdaBinderSerializer` class which can read an HDA file, creating an in-memory representation via the `oracle.stellent.ridc.model.DataBinder` class.
- For more details on APIs used, refer to [Class HdaBinderSerializer](#).

10. What is a sample query that can be used to extract the metadata related to the content and generate a CSV file?

For CSV creation you can use a simple SQL query to extract the required metadata from your Oracle WebCenter Content database. You can customize the following sample query depending on your business requirements, and export the result output to a CSV file.

Sample Query:

```
SELECT REVISIONS.DDOCNAME AS FILEID, (ROW_NUMBER() OVER
(PARTITION BY REVISIONS.DDOCNAME ORDER BY REVISIONS.DREVRANK
desc)) AS FILEVERSION, DOCMETA.DID || '.' ||
DOCUMENTS.DEXTENSION AS OCIOFILE, DOCUMENTS.DFORMAT AS
FILEMIMETYPE, DOCUMENTS.DEXTENSION AS FILEEXTENSION,
DOCUMENTS.DORIGINALNAME AS ORIGINALFILENAME,
REVISIONS.DCREATEDATE AS CREATEDATE FROM
REVISIONS, DOCUMENTS, DOCMETA WHERE REVISIONS.DID =
DOCUMENTS.DID AND REVISIONS.DID = DOCMETA.DID AND
```

```
DOCUMENTS.DISPRIMARY = 1 AND REVISIONS.DSECURITYGROUP = 'Public'
ORDER BY REVISIONS.DDOCNAME
```

11. How can content be exported from file storage and database storage for migration to OCI object storage?

- We strongly recommend you use the [Object Storage Migration Tool](#) in Oracle WebCenter Content 12c (May 2022 bundle patch for Oracle WebCenter Content 12.2.1.4.0).
- Alternatively, to export content out of Oracle WebCenter Content file system to a common file system, you can use the Archiver in Oracle WebCenter Content.
- Alternatively, to export content out of Oracle WebCenter Content database storage to a common file system, you can use the following SQL query to extract content from the database secure file system:

```
SELECT bfiledata FROM filestorage where DID IN (select
Revisions.DID FROM REVISIONS, DOCUMENTS, DOCMETA WHERE
REVISIONS.DID = DOCUMENTS.DID AND REVISIONS.DID = DOCMETA.DID
AND DOCUMENTS.DISPRIMARY = 1

AND REVISIONS.DSECURITYGROUP = 'Public');
```

The above query returns the set of BLOBs. A script would be required to loop through this set and store it in filesystem so that they can be exported. The following article may help in building out the script: <https://oracle-base.com/articles/9i/export-lob-9i>.

12. How long does it take for end-to-end migration (for moving content from on-premise Oracle WebCenter Content to Oracle Content Management)?

To migrate large volumes like a few terabytes of content, we suggest that you use the object storage provider to move content from on-premise to an OCI object storage bucket and then from that bucket to the Oracle Content Management asset repository.

As a benchmarking exercise 90,000 files (175 KB) were migrated in 40 minutes with 10 threads (suggested configuration) from Oracle WebCenter Content on-premise to OCI Object storage. Then, moving the content from OCI object storage to Oracle Content Management can be scheduled using a service request, providing the relevant CSV file and mapping questionnaire.

Large migrations such as this will be split across multiple asset types. Each asset type is considered as a separate migration, so the time it takes to move the content from the OCI object storage bucket to the Oracle Content Management repository will vary depending on how we structure and organize the multiple migration batches based on asset types. We recommend that if you know the eventual goal is to migrate to Oracle Content Management, that the bucket for the Oracle WebCenter Content system should be included within the same compartment as the Oracle Content Management instance. This improves the migration performance.

13. How will you support us if we do our own object store migration from Oracle WebCenter Content 11g?

Oracle WebCenter Content 11g customers can migrate to Oracle Content Management using the suggested approach in [Migrate Files from Oracle WebCenter Content 11g to Oracle Content Management Assets](#). An Oracle certified partner or our consulting team can assist and support in the migration process and provide additional guidance where needed.

Map Your Source Content to Oracle Content Management Asset Features

Depending on your data source, you have different data structure to map to Oracle Content Management asset features:

- [Oracle WebCenter Content](#)
- [External Content Management System](#)
- [Documents Folders](#)

Oracle WebCenter Content

Map your Oracle WebCenter Content data structure and security to Oracle Content Management asset structure:

Oracle WebCenter Content Data Structure	Oracle Content Management Asset Structure
Security groups and accounts	<p>Repositories and granular permissions Create repositories with granular permissions that map to the security groups and accounts.</p> <p>You can grant users permissions to assets by assigning roles in the repository, but you can further refine access through granular permissions based on asset type and taxonomy category. You can apply granular permissions consistently by saving them as editorial roles.</p> <p>After creating your asset types and taxonomies, create editorial roles corresponding to the accounts and permissions. Then create corresponding groups for each editorial role, and add the appropriate users to the groups.</p>
Document types	<p>Asset types Create asset types corresponding to document types for each department. Each asset type must include:</p> <ul style="list-style-type: none"> • All file extensions of the files you want to migrate • Fields for any metadata you want to migrate from the source files <p>When you complete the questionnaire supplied by Oracle Support, you'll map the source metadata fields from Oracle WebCenter Content to the fields in the asset type. The source field name in the mapping must include the metadata group name, followed by a dot ("."), and then the metadata field name (for example, <code>Contract_Provider.Email_Address</code>).</p> <p>You can also use the following system values for the field mappings in the questionnaire:</p> <ul style="list-style-type: none"> • FILEID—The original unique identifier of the document. • FOLDERNAME—The name of the folder in which the document resides; this is a single folder name, not the full path. • CREATEDATE—The original creation date of the document.

Oracle WebCenter Content Data Structure	Oracle Content Management Asset Structure
Hierarchical accounts and folders	<p>Taxonomies Create taxonomies corresponding to the hierarchical accounts based on department, country and security levels. Create additional taxonomies corresponding to the hierarchical folder structure of your source content.</p> <p>Each asset can be a member of multiple taxonomies. Taxonomies are built out during migration based on custom metadata fields, system values, folder paths, or static values. They can have hierarchical levels based on fields such as "State", "County", and "City". The folder path can also be used to build hierarchical levels in a taxonomy.</p> <p>There are two special functions that can be used in the taxonomies. The "year()" function will extract the year portion of date so it can be used as a category value. The "month()" function similarly will provide the month of a date field. These functions can only be used on date type fields (whether custom or system fields).</p> <p>For example, you could specify a taxonomy sequence like this:</p> <ul style="list-style-type: none"> • Taxonomy Name: Months • Level 1: year(CREATEDATE) • Level 2: month (CREATEDATE)

External Content Management System

Map your source data structure and security to Oracle Content Management asset structure:

Source Data Structure	Oracle Content Management Asset Structure
Folders and file structure	Repositories to store the content and taxonomies to structure the categorical hierarchies
Categorization and hierarchies	<p>Taxonomies to categorize your content. Each asset can be a member of multiple taxonomies. Taxonomies are built out during migration based on static values, custom metadata fields, system values, or folder paths. They can have hierarchical levels such as "State", "County", and "City". There are two special functions that can be used in the taxonomies. The "year()" function will extract the year portion of date so it can be used as a category value. The "month()" function similarly will provide the month of a date field. These functions can only be used on date type fields (whether custom or system fields).</p> <p>For example, you could specify a taxonomy sequence like this:</p> <ul style="list-style-type: none"> • Taxonomy Name: Months • Level 1: year(CREATEDATE) • Level 2: month (CREATEDATE)

Source Data Structure	Oracle Content Management Asset Structure
File types	Asset types, which must include: <ul style="list-style-type: none"> • All file extensions of the files you want to migrate • Fields for any metadata you want to include from the documents. This can include custom metadata or the following system values: <ul style="list-style-type: none"> – FILEID—The original unique identifier of the document. – FOLDERNAME—The name of the folder in which the document resides; this is a single folder name, not the full path. – CREATEDATE—The original creation date of the document.
Groups	Groups
Roles	Application roles, repository roles, and granular security

Documents Folders

Map your source Documents folder structure and security to Oracle Content Management asset features:

Source Documents Folder Structure	Oracle Content Management Asset Structure
Folder	Repository You must create a repository to store all the files from the source Documents folder.
File types (extensions)	Extensions associated with the asset type You can use the out-of-the-box <i>File</i> asset type, which accepts all file types, or you can create a custom asset type. If you create a custom asset type, it must include all file extensions of the files you want to migrate. Any files of a type not explicitly listed in the asset type will be rejected by the migration.

Source Documents Folder Structure	Oracle Content Management Asset Structure
File metadata (for field values)	<p>Fields in the asset type</p> <p>You can use the out-of-the-box <i>File</i> asset type, or you can create a custom asset type if you want to store custom metadata.</p> <p>If you create a custom asset type, it must include fields for any custom metadata you want to migrate from the source files. The custom metadata comes from the metadata groups you applied to the Documents folder.</p> <p>When you complete the questionnaire supplied by Oracle Support, you'll map the source metadata fields from Documents to the fields in the asset type. The source field name in the mapping must include the metadata group name, followed by a dot ("."), and then the metadata field name (for example, <code>Contract_Provider.Email_Address</code>).</p> <p>You can also use the following system values for the field mappings in the questionnaire:</p> <ul style="list-style-type: none"> • FILEID—The original unique identifier of the document. • FOLDERNAME—The name of the folder in which the document resides; this is a single folder name, not the full path. • CREATEDATE—The original creation date of the document.
File metadata and folder path (for categorization)	<p>Taxonomies</p> <p>Each asset can be a member of multiple taxonomies. Taxonomies are built out during migration based on custom metadata fields, system values, folder paths, or static values. They can have hierarchical levels based on fields such as "State", "County", and "City". The folder path can also be used to build hierarchical levels in a taxonomy.</p> <p>You create the taxonomy but don't add any categories to it. The categories will be created during migration.</p> <p>There are two special functions that can be used in the taxonomies. The "year()" function will extract the year portion of date so it can be used as a category value. The "month()" function similarly will provide the month of a date field. These functions can only be used on date type fields (whether custom or system fields).</p> <p>For example, you could specify a taxonomy sequence like this:</p> <ul style="list-style-type: none"> • Taxonomy Name: Months • Level 1: year(CREATEDATE) • Level 2: month(CREATEDATE)

Source Documents Folder Structure	Oracle Content Management Asset Structure
Folder role	Repository role <ul style="list-style-type: none"> • Users with the Manager role for the Documents folder will be given the Manager role for the repository. • Users with the Contributor role for the Documents folder will be given the Contributor role for the repository. • Users with the Downloader or Viewer role for the Documents folder will be given the Viewer role for the repository.

Upload Files to an Object Storage Bucket

1. Create an Oracle Cloud Infrastructure object storage bucket for uploading your files.
 Although you can create your object storage bucket in any compartment, using the compartment you created for Oracle Content Management during Oracle Content Management instance creation is the most efficient. Consider the following:
 - The easiest and fastest migration occurs when the bucket for the source content is created within the Oracle Content Management compartment.
 - If the files are uploaded to a compartment in a distant physical location, copying the content to Oracle Content Management will take longer.
 - In order for the migration tool to reach the content in a separate compartment, a security grant is required to allow access to the content.


```
Allow service CEC to manage object-family in tenancy
```

```
Allow service objectstorage-us-ashburn-1 to manage object-family in tenancy
```
2. Upload the files to the object storage bucket you created using one of the following options:
 - Use the [Object Storage command line tool](#) to upload the exported documents to the target object storage bucket.
 - [Use offline data transfer](#). Save the content on an external hard drive, send it to Oracle's Object Storage team, and they will upload it to the target object storage bucket.

Export Source File Metadata to CSV

Export the file metadata from your source repository. Databases generally provide this ability as the output of a query. The exported metadata is formatted into a CSV file. The CSV file can include:

- [Required Columns](#)
- [Optional Columns](#)
- [Custom Columns](#)

Required Columns

The CSV file must include the following required columns with these exact names.

Column Name	Data Type	Details
FILEID	STRING	The unique identifier of the file as it appeared in the source system (the unique document identifier). This identifier needs to be unique across the entire migration. If the migration is gathering data from different repositories that might have overlapping unique identifiers, the values need to be made unique at the scope of the whole migration. For example, this could be accomplished by prepending an "A" to the unique identifiers of the first system, and a "B" to the unique identifiers of the second system. This would ensure the two sets of unique identifiers never overlapped.
FILEVERSION	INTEGER	Indicates the version of the file. Version numbers should be in ascending order (the most recent revision would have the highest revision value). There can be gaps in the version number sequence (some versions may have been deleted). There can be a file with version 1 and version 3 but not version 2. If the source content file system doesn't support versioning, use "1" as the version value in this column.
FILEEXTENSION	STRING	The extension of the file, such as pdf, doc, docx, xlsx.
OCIOSFILE	STRING	The object name of the file as stored in Oracle Cloud Infrastructure object storage. The object name is simply a string value, so it can include slashes that make it appear to be an entire folder path. If the content is uploaded from a directory structure those directory names will be part of the object names.
ORIGINALFILENAME	STRING	The original name of the file when it was uploaded into the original source system. This is the same name that will be given to this file if it is subsequently downloaded from Oracle Content Management.

Optional Columns

Your CSV can also include the following optional columns. If these details are provided, the values will be assigned to the system-level asset attributes, and the asset will appear to have been created or modified at the given point in the past by the given user.

Column Name	Data Type	Details
CREATOR	STRING	The user identifier to be assigned as the creator of the document. If there are multiple versions, data from oldest revision will be used. The user identifiers must exist in the Oracle Content Management instance, those defined in the associated identity server. You're responsible for translating these user identifiers from the source system to the equivalent user identifiers available in Oracle Content Management. You can also specify a default user in the questionnaire to be assigned if a given user identity isn't found.
CREATEDATE	DATE	The date to be assigned to the new asset as its creation date. If there are multiple versions, data from oldest revision will be used.

Column Name	Data Type	Details
LASTMODIFIER	STRING	The user identifier to be assigned as the last modifier of the document. If there are multiple versions, data from newest revision will be used. The user identifiers must exist in the Oracle Content Management instance, those defined in the associated identity server. You're responsible for translating these user identifiers from the source system to the equivalent user identifiers available in Oracle Content Management. You can also specify a default user in the questionnaire to be assigned if a given user identity isn't found.
LASTMODIFIEDDATE	DATE	The date to be assigned to the new asset as its last modification date. If there are multiple versions, data from newest revision will be used.

Custom Columns

You can also include custom columns. Make sure to include all metadata you want to see in the target assets (for example, an invoice number or customer name) and any metadata that will be used to assign taxonomy categories to assets (for example, supplier state or sales territory).

Column names must be valid Oracle database column names. Generally, they must not:

- Contain spaces
- Contain special characters: &*\$|~@%?()
- Start with OCM_

Custom columns can specify the data type of the column following the name, in this format "ColumnName (DATATYPE)".

Datatype	Example	Notes
INTEGER	• "InvoiceNumber (INTEGER)"	
DECIMAL	• "InvoiceAmount (DECIMAL)"	

Datatype	Example	Notes
VARCHAR / STRING	<ul style="list-style-type: none"> • "Cu sto me rE mai l (VA RC HA R)" • "Cu sto me rE mai l (ST RI NG)" • "Cu sto me rE mai l" 	<p>If no type is specified it is assumed to be STRING.</p>
TIMESTAMP	<ul style="list-style-type: none"> • "Inv oic eD ate (TI ME ST AM P)" • "Inv oic eD ate (TI ME ST AM P:d d- MM M- yy)" 	<p>Date types can also include the format of the date. The timestamp mask format is whatever is acceptable by the Java DateTimeFormatter class. The default format if none is given is "yyyy-MM-dd'T'HH:mm:ss.SSSXXX" an example of which is "2022-07-12T01:35:45.868+05:30".</p>

Sample SQL Query for WebCenter Content Migrations

The following sample SQL statement illustrates how to produce a result set from WebCenter Content, which can be exported to a CSV file. It can be adjusted based on your needs.

For other external systems we recommend working with a partner to generate CSV files.

```

SELECT
    REVISIONS.DDOCNAME      AS FILEID,
    (ROW_NUMBER() OVER (PARTITION BY REVISIONS.DDOCNAME ORDER BY
REVISIONS.DREVRANK desc))  AS FILEVERSION,
    OCIDOCHASHES.HASH || '-' || OCIDOCHASHES.DCHECKINID      AS
OCIOSFILE,
    DOCUMENTS.DFORMAT      AS FILEMIMETYPE,
    DOCUMENTS.DEXTENSION   AS FILEEXTENSION,
    DOCUMENTS.DORIGINALNAME AS ORIGINALFILENAME,
    REVISIONS.DCREATEDATE  AS CREATEDATE,
    DOCMETA.XMKTCAMPAIGNHOSTCOUNTRY AS XMKTCAMPAIGNHOSTCOUNTRY,
    DOCMETA.XLGLEVENTDATE  AS XLGLEVENTDATE
FROM REVISIONS,
    DOCUMENTS,
    OCIDOCHASHES,
    DOCMETA
WHERE REVISIONS.DID = DOCUMENTS.DID
    AND REVISIONS.DSECURITYGROUP = 'LEGAL-APPROVAL'
    AND REVISIONS.DID = OCIDOCHASHES.DID
    AND REVISIONS.DID = DOCMETA.DID
    AND OCIDOCHASHES.DRENDITIONID = 'primaryFile'
    AND DOCUMENTS.DISPRIMARY = 1
    AND DOCMETA.XSTORAGERULE = 'OCIObjectStorageRule'
ORDER BY REVISIONS.DDOCNAME

```

Here's a description of the SQL:

- In the SELECT statement, the REVISIONS and DOCUMENTS clauses specify the required and optional CSV columns. The text after "AS" is what the column will be called in the CSV file.
- In the SELECT statement, the OCIDOCHASHES clause assumes the files have been migrated from Oracle WebCenter Content to object storage. This clause produces the name of the object in object storage as the value of the OCIOSFILE column of the CSV file.
- In the SELECT statement, the DOCMETA clauses specify custom data fields.
- In the WHERE statement, the REVISIONS.DSECURITYGROUP clause limits the set of documents to a particular Oracle WebCenter Content security group. Additional WHERE clauses can be added to partition the data into smaller units to be migrated separately. This is necessary since each migration is limited to a single target repository and asset type.
- In the WHERE statement, the OCIDOCHASHES.DRENDITIONID = 'primaryFile' and DOCUMENTS.DISPRIMARY = 1 clauses limit the set of files to only the primary (original) documents ignoring web renderings.
- In the WHERE statement, the DOCMETA.XSTORAGERULE = 'OCIObjectStorageRule' clause limits the set of files to only those that have been migrated to the object storage provider.

Submit a File Migration Service Request

When your Oracle Content Management instance and target repositories are set up, and you're ready for your migration, you must submit a migration request. We recommend that you give two weeks advanced notice. Oracle will attempt to schedule your migration based on your requested date. If a migration needs to follow a very specific schedule, submit a service request specifically to facilitate scheduling in advance.

 **Note:**

You don't need to submit a service request if you're migrating fewer than 500,000 files from Oracle WebCenter Content (you can [use Archiver and Content Capture](#) to migrate a moderate number of files from Oracle WebCenter Content).

To submit your migration service request:

1. Sign in to Oracle Cloud Support.
2. Create a new service request.
3. For the **Product**, select **Oracle Content Management**.
4. For the **Problem Type**, select **Service Instance Migration**.
5. Attach the CSV file to your request.
6. Submit your service request. Then make sure to keep up with any service request updates so you can provide additional information when necessary.
7. Oracle Support will work with you to gather additional required details about your migration, including your source and target information, field mappings, and taxonomy definitions.
8. After the details are gathered, Oracle Support will coordinate with the migration team to finalize a migration date that works for you and Oracle. The service request will be updated with the date and time your migration will start.
9. After you confirm in the service request that you approve the migration start date and time, Oracle Support and the migration team will execute your migration request. Updates will be made to the service request to show how the migration is progressing. The data migration will be done at the back end; no action is required at your end other than to keep up with any service request updates, and to validate the migration after it's done.

E

Manage Oracle Content Management in Legacy Environments

The way you manage and deploy Oracle Content Management may vary depending on the type, start date, and status of your subscription. This topic covers the tasks that differ in legacy environments.

Deployment scenario	SKU	Date you purchased Oracle Content Management	Deployment and management tasks
Oracle Content Management <i>built</i> on Oracle Cloud Infrastructure (OCI) (Universal Credits subscription)	B89969, B89970, and B89971	October 2018 through September 2019	Manage Legacy Instances of Oracle Content Management Built on OCI Gen 1 <ul style="list-style-type: none"> Manage instances created in the Infrastructure Classic Console Monitor the service
Oracle Content Management on OCI Classic (Universal Credits subscription)	B87494, B87496, and B87498	March 2018 through September 2018*	Manage Legacy Instances of Oracle Content Management on OCI Classic <ul style="list-style-type: none"> Manage instances created in the Infrastructure Classic Console Monitor the service
Oracle Content Management for Government on OCI Classic (Universal Credits subscription)	B88834, B88835, B90265, and B90266	November 2019 or earlier	Deploy and Manage Legacy Instances of Oracle Content Management for Government on OCI Classic <ul style="list-style-type: none"> Create an instance Manage instances Monitor the service
Oracle Content Management for SaaS on OCI Classic (Universal Credits subscription)	B89710 and B89711	October 2019 or earlier	Deploy and Manage Legacy Instances of Oracle Content Management for SaaS on OCI Classic <ul style="list-style-type: none"> Create an instance Manage instances Monitor the service

Deployment scenario	SKU	Date you purchased Oracle Content Management	Deployment and management tasks
Oracle Content Management entitlement (non-metered subscription)	B87425, B87426 , and B87427	February 2017 through February 2018	Deploy and Manage Oracle Content Management with a Non-Metered Subscription <ul style="list-style-type: none"> • Create an instance • Set up users and groups • Manage users, groups, and access • Manage instances • Monitor the service
Oracle Documents Cloud entitlement (non-metered subscription)	B76606	January 2017 or earlier	Migrate Oracle Documents Cloud to Oracle Content Management <ul style="list-style-type: none"> • Migrate to Oracle Content Management

* Oracle Content Management on OCI Classic can be [migrated](#) to run on 2nd generation OCI.

Manage Legacy Instances of Oracle Content Management Built on OCI Gen 1

If you have legacy instances of Oracle Content Management built on Oracle Cloud Infrastructure (OCI) Gen 1, there are some differences in how you manage those instances.

You should always [create new instances](#) in the Oracle Cloud Console to take advantage of the benefits and advances of Gen 2 OCI and Oracle's cloud platform in the future. You'll then manage and monitor those instances through the Oracle Cloud Console.

For legacy instances that you created in the Infrastructure Classic Console (previously called My Services), you can manage them as described in this topic. However, Oracle recommends that you [migrate those instances](#) to the new *native* OCI environment—Gen 2 OCI (that is, using the Oracle Cloud Console to manage service instances), so that those instances will also take advantage of future benefits and advances in Oracle's cloud platform.


! Important:

- If you created a legacy instance, a user named CEC_INTERNAL_APPID_USER was automatically created. It's an internal user that can't be used to sign in. This user enables communication between Oracle Content Management components. *Do not delete this user* or some functionality in Oracle Content Management will no longer work.
- If you have a legacy universal credits subscription, you'll be billed based on [active users per hour](#) and [visitor sessions](#).




All other tasks are performed as described in previous chapters:

- [Configure service settings](#)
- [Manage users, groups, and access](#)
- [Manage the Service](#)
- [Analyze service usage](#)
- You might also want to integrate Oracle Content Management with other business applications as described in *Integrating and Extending Oracle Content Management*.

To view your legacy instances:

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 , under More Oracle Cloud Services, expand **Platform Services**, then click **Content and Experience**. You might need to use the scroll bar on the left to scroll down to see the menu option.

From the list of instances you can perform the following actions:

- You can perform some management tasks from the list of instances. Next to the instance you want to manage, click . You can access the Oracle Content Management web client for the instance, add tags, or delete the instance.
- To view general information about an instance, click its name. You see information such as storage OCIDs, version, and account name. To view additional information, click .
- To manage an instance, click its name, then click . You can access the Oracle Content Management web client for the instance, add an association, update instance credentials, add tags, or view activity.

Understand Active Users per Hour

If you have an Oracle Content Management instance built on Oracle Cloud Infrastructure (OCI) and managed with the Infrastructure Classic Console, you'll be billed based on active users per hour.

An *active user per hour* is defined as a unique user that interacts with the service during a one-hour session. Active users are tracked through a cookie, user ID, token, device ID, IP, or session ID. Authenticated users and visitors are tracked based on the role given to the user

(standard, enterprise, or visitor) in that service instance. Anonymous users are tracked as visitors.

Visitors and anonymous users that access the service from multiple channels (website, mobile app, desktop client, custom app via APIs, email, etc.) count as multiple active users sessions. An *authenticated user* that accesses the service from multiple channels counts as one active user session. For example, if one *visitor* in a one-hour period accesses the same Oracle Content Management instance from a Firefox desktop web browser, a Chrome desktop web browser, and a mobile web browser, that would count as a total of *three* active user sessions. Whereas, if one *authenticated user* performs the same actions, that would count as *one* active user session.

Depending on whether the user is a standard user, an enterprise user, or a visitor, the user is allowed a certain number of API calls, a certain amount of outbound data transfer, and, for enterprise users, a certain number of new published content assets. Therefore, for billing purposes, the following metrics are also tracked during each one-hour active user session:

- Number of API calls made to the service by custom third-party applications (non-Oracle) — If the number of API calls exceeds the API calls that are entitled per active user in a one-hour period, a new active user is added to the hourly count.
- Outbound data transfer — This includes the data a user downloads from the Oracle Cloud Service *and* any transfer of data from the Oracle Cloud Service over the internet, including responses to client requests. If the outbound data transfer exceeds the data transfer that is entitled per active user in a one-hour period, a new active user is added to the hourly count.
- Number of newly published assets (enterprise users only) — A published asset is either a file based asset (for example, a document, an image, or a video) or a content item that has been published. A content item is a block of information created using a content type. If the number of newly published assets exceeds the published assets that are entitled per active user in a one-hour period, a new active user is added to the hourly count. This count doesn't include previously published assets, only assets published during the one hour active user session.

 **Note:**

For information on Universal Credits pricing and usage limits (for example, the number of API calls, amount of outbound data transfer, and number published assets allowed per user), see [Oracle Universal Credits Pricing](#) and [Oracle Cloud Services](#) (view “Oracle PaaS and IaaS Universal Credits - Service Descriptions” near the bottom of the list).

Frequently Asked Questions

Does a user visiting a second site count as a second active user session?

Only a *visitor or anonymous user* accessing a different resource (such as a different site) will be counted as a separate active user session. An *authenticated user* accessing the service from multiple channels will be counted as one active user session. For example, the same *visitor* accessing two different sites within the one-hour session window will be counted as two active user sessions. Essentially the count is per visitor or anonymous user, per resource, per channel, per one-hour session window for a given service instance.

Will visits to a site by bots or crawlers count as active user sessions?

Repeated visits from bots or crawlers will not be counted as active user sessions.

Will a user accessing a public download link be counted as an active user session?

A user accessing a public download link to download a document will not be counted as an active user session. Even if the user is brought to the Oracle Content Management user interface, showing the **Download** button, it won't count as an active user session. However, the outbound data transfer per hour will be tracked.

What if the public download link is accessed via a site created with Oracle Content Management? Will using the link be counted as an active user session?

Visiting the site created with Oracle Content Management triggers an active user session, so it will count as an active user for that hour, but not due to using the public download link. Again, the outbound data transfer will be tracked.

For a browser session, how are active user sessions tracked?

The active user sessions for a browser are tracked by placing a cookie that expires after the one-hour session window ends in the browser session.

What happens if a user clears cookies in the browser or closes an incognito browser session?

If the user clears the cookie (by clearing in browser or closing an incognito window), the next request will be treated as a new user and count as a new active user session.

Are AppLinks and API calls tracked for billing purposes?

AppLinks and API calls from third-party applications and from other Oracle Cloud applications are charged according to the user identity (Standard or Enterprise) used to establish the API connection. Every 100 API calls in a given hour count as an additional active user for that hour.

How are AppLink calls tracked as visitor sessions?

The `assignedUser` parameter in the [AppLink](#) request body is used to track the client-side invocations associated to unique users.

How is a user of the Oracle Content Management desktop client tracked?

A desktop client user is tracked as an active user (either as a standard or enterprise user as appropriate) if they create, edit, or update files or folders from their desktop. Downward syncing actions from the cloud server caused by other user updates to files or folders are not counted as active user sessions. However, syncing does count toward the outbound data transfer metric. For example, if a user syncs more than 1 GB of data per hour, each additional GB synced will count as an additional active user session for that hour (either standard or enterprise as appropriate).

Understand Visitor Sessions

A *visitor session* is metric used by Oracle Content Management to track usage during a specified *session window* (one hour for hourly visitor sessions and 24 hours for daily visitor sessions). A visitor session is triggered when a unique unauthenticated user or an authenticated user who has the *site visitor* role accesses the service using a specific channel (for example, via a browser, mobile browser or applink, etc.). Access from multiple channels counts as multiple visitor sessions. For example, if one user in a 24 hour period accesses the same Oracle Content Management instance from a Firefox desktop web browser, a Chrome

desktop web browser, and a mobile web browser, that would count as a total of three *daily* visitor sessions.

Unauthenticated users can access certain sites, use public links, and view Oracle Content Management content embedded in apps or websites. See [Task and Feature Comparison by Application Role](#).

Frequently Asked Questions

If a user accesses multiple pages within the same Oracle Content Management instance, does that count as multiple visitor sessions?

No. Visitor sessions are only counted at the instance (site) level.

When is a visitor session triggered?

A visitor session is initiated by any user (anonymous or authenticated *guest*) who accesses an Oracle Content Management resource such as an Oracle Content Management instance, a site created with Oracle Content Management, or via an API (for example, using applinks) at least once during the session window.

How long does a visitor session last?

The duration of an hourly visitor session is one hour; a daily visitor session is 24 hours. It starts the first time the user accesses a specific Oracle Content Management resource via a unique channel. After one hour, subsequent visits by the same user to the same resource triggers another *hourly* visitor session. After 24 hours, subsequent visits by the same user to the same resource triggers another *daily* visitor session.

Will an Oracle Content Management standard or enterprise user be counted in visitor session counts?

No. An authenticated (signed-in) standard or enterprise user that visits an Oracle Content Management resource isn't included in visitor session counts.

Does the visitor session apply to authenticated (signed-in) users visiting an Oracle Content Management resource?

As stated above an authenticated Oracle Content Management standard or enterprise user that visits an Oracle Content Management resource will not be counted in visitor session counts. However, an authenticated user with the *site visitor* role *will* be counted in the visitor session counts. See [Application Roles](#).

How often is the visitor session calculated?

The visitor might access the same resource (site, API or applink) multiple times in the visitor session window (one hour for hourly visitor sessions and 24 hours for daily visitor sessions), but will be counted as one/single visit. If the user accesses the same resource again after the visitor session window, it will be counted as new visit.

Does a user visiting a second site count as a second visitor session?

The same user accessing a different resource (such as a different site) will be counted as a separate visitor session visit. For example, the same user accessing two different sites within the session window will be counted as two visits. Essentially the count is per user, per resource, per channel, per visitor session window for a given service instance.

Will visits to a site by bots or crawlers count as visitor sessions?

Repeated visits from bots or crawlers will not be counted as visitor sessions.

Will a user accessing a public download link be counted as visitor session?

A user accessing a public download link to download a document will not be counted as a visitor session. Even if the user is brought to the Oracle Content Management user interface, showing the **Download** button, it won't count as a visitor session.

What if the public download link is accessed via a site created with Oracle Content Management? Will using the link be counted as visitor session?

Visiting the site created with Oracle Content Management triggers a visitor session, so it will count as a visitor session, but not due to using the public download link.

For a browser session, how are the visitor sessions tracked?

The visitor sessions for a browser are tracked by placing a cookie that expires after the session window ends in the browser session.

What happens if a user clears his cookies in his browser or closes an incognito browser session?

If the user clears the cookie (by clearing in browser or closing an incognito window), the next request will be treated as a new user and count as a new visitor session.

What metrics are reported to administrators?

Oracle Content Management Analytics provides the following metrics:

- Break down of visitor session counts on hourly basis
- Aggregation of visitor session counts per month
- Ability to drill down on each day of the month (to get to visitor counts)

What metrics are not currently supported or captured?

- Cookie disabling: Some customers can disable cookie tracking on the browser side as an end user policy. In such cases, Oracle Content Management can't track the visitor based cookies since they are turned off, meaning the count will be lower than the actual number of visitors.
- Tracking visitors via the Oracle Content Management desktop application (the desktop application currently supports counting only named users).
- Tracking visits via the Oracle Content Management mobile applications (the mobile applications currently support counting only named users).

What about opt-out or privacy support with regards to cookie tracking?

Oracle Content Management sites will provide a standard option of letting the user know that a Oracle Content Management resource (site) is using cookies and users can opt-out by disabling the cookie. To support this, the following two items are added consistently across all the Oracle Content Management site resources:

- Opt-out summary message: This message appears on each site to indicate that a cookie is being used for tracking. It includes a link to the privacy page.
- Privacy site page: A standard sites page explaining the usage of a cookie as well the steps to disable the cookie. You can customize this page like any other sites page.

Are AppLinks and API calls tracked as visitor sessions?

AppLinks and REST API calls from third-party applications are included in the visitor sessions counts.

How are AppLink calls tracked as visitor sessions?

The `assignedUser` parameter in the `AppLink` request body is used to track the client-side invocations associated to unique users.

Examples

Here are some examples of visitor session counts. Let's assume ACME Corporation has an Oracle Content Management service instance and has created three sites: SiteA, SiteB, and SiteC. Following are examples of how the visitor sessions would be counted during a session window.

Visitor	Resource (Site)	Daily Visitor Session Counts
User1	https://docs-acme.sites.us2.oracelcloud/authsite/SiteA	Count increases to 1 (cookie1, user visits a site—SiteA, using Firefox)
User1	https://docs-acme.sites.us2.oracelcloud/authsite/SiteB	Count increases to 2 (cookie2, same user but different site—SiteB, using Firefox)
User2	https://mysite.acme.example.com (vanity URL for SiteC)	Count increases to 3 (cookie3, different user, different site—SiteC, using Firefox)
User3	https://mysite.acme.example.com (vanity URL for SiteC)	Count increases to 4 (cookie4, different user, same site—SiteC, using Firefox)
User2	https://mysite.acme.example.com (vanity URL for SiteC)	Count stays at 4 (no change, cookie3, same user—User2, same site—SiteC, using Firefox, same session window)
User2	https://mysite.acme.example.com (vanity URL for SiteC)	Count increases to 5 (cookie5, same user—User2, same site—SiteC, same session window, but using Chrome)

Manage Legacy Instances of Oracle Content Management on OCI Classic

If you have legacy instances of Oracle Content Management on Oracle Cloud Infrastructure (OCI) Classic, there are some differences in how you manage those instances.

You should always [create new instances](#) in the Oracle Cloud Console to take advantage of the benefits and advances of Gen 2 OCI and Oracle's cloud platform in the future. You'll then manage and monitor those instances through the Oracle Cloud Console.

For legacy instances that you created in the Infrastructure Classic Console (previously called My Services), you can manage them as described in this topic. However, Oracle recommends that you [migrate those instances](#) to the new *native* OCI environment—Gen 2 OCI (that is, using the Oracle Cloud Console to manage service instances), so that those instances will also take advantage of future benefits and advances in Oracle's cloud platform.


! Important:

- If you created a legacy instance, a user named CEC_INTERNAL_APPID_USER was automatically created. It's an internal user that can't be used to sign in. This user enables communication between Oracle Content Management components. *Do not delete this user* or some functionality in Oracle Content Management will no longer work.
- If you have a legacy universal credits subscription, you'll be billed based on [active users per hour](#) and [visitor sessions](#).




All other tasks are performed as described in previous chapters:

- [Configure service settings](#)
- [Manage users, groups, and access](#)
- [Manage the Service](#)
- [Analyze service usage](#)
- You might also want to integrate Oracle Content Management with other business applications as described in *Integrating and Extending Oracle Content Management*.

To view your legacy instances:

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 , under More Oracle Cloud Services, expand **Platform Services**, then click **Content and Experience**. You might need to use the scroll bar on the left to scroll down to see the menu option.

From the list of instances you can perform the following actions:

- You can perform some management tasks from the list of instances. Next to the instance you want to manage, click . You can access the Oracle Content Management web client for the instance, add tags, or delete the instance.
- To view general information about an instance, click its name. You see information such as storage OCIDs, version, and account name. To view additional information, click .
- To manage an instance, click its name, then click . You can access the Oracle Content Management web client for the instance, add an association, update instance credentials, add tags, or view activity.

Understand Active Users per Hour

If you have an Oracle Content Management-Classic instance, you'll be billed based on active users per hour.

An *active user per hour* is defined as a unique user that interacts with the service during a one-hour session. Active users are tracked through a cookie, user ID, token, device ID, IP, or session ID. Authenticated users and visitors are tracked based on the role given to the user (standard, enterprise, or visitor) in that service instance. Anonymous users are tracked as visitors.

Visitors and anonymous users that access the service from multiple channels (website, mobile app, desktop client, custom app via APIs, email, etc.) count as multiple active users sessions. An *authenticated user* that accesses the service from multiple channels counts as one active user session. For example, if one *visitor* in a one-hour period accesses the same Oracle Content Management instance from a Firefox desktop web browser, a Chrome desktop web browser, and a mobile web browser, that would count as a total of *three* active user sessions. Whereas, if one *authenticated user* performs the same actions, that would count as *one* active user session.

Depending on whether the user is a standard user, an enterprise user, or a visitor, the user is allowed a certain number of API calls, a certain amount of outbound data transfer, and, for enterprise users, a certain number of new published content assets. Therefore, for billing purposes, the following metrics are also tracked during each one-hour active user session:

- Number of API calls made to the service by custom third-party applications (non-Oracle) — If the number of API calls exceeds the API calls that are entitled per active user in a one-hour period, a new active user is added to the hourly count.
- Outbound data transfer — This includes the data a user downloads from the Oracle Cloud Service *and* any transfer of data from the Oracle Cloud Service over the internet, including responses to client requests. If the outbound data transfer exceeds the data transfer that is entitled per active user in a one-hour period, a new active user is added to the hourly count.
- Number of newly published assets (enterprise users only) — A published asset is either a file based asset (for example, a document, an image, or a video) or a content item that has been published. A content item is a block of information created using a content type. If the number of newly published assets exceeds the published assets that are entitled per active user in a one-hour period, a new active user is added to the hourly count. This count doesn't include previously published assets, only assets published during the one hour active user session.

 **Note:**

For information on Universal Credits pricing and usage limits (for example, the number of API calls, amount of outbound data transfer, and number published assets allowed per user), see [Oracle Universal Credits Pricing](#) and [Oracle Cloud Services](#) (view “Oracle PaaS and IaaS Universal Credits - Service Descriptions” near the bottom of the list).

Frequently Asked Questions

Does a user visiting a second site count as a second active user session?

Only a *visitor or anonymous user* accessing a different resource (such as a different site) will be counted as a separate active user session. An *authenticated user* accessing the service from multiple channels will be counted as one active user session. For example, the same *visitor* accessing two different sites within the one-hour session window will be counted as two active user sessions. Essentially the count is per visitor or anonymous user, per resource, per channel, per one-hour session window for a given service instance.

Will visits to a site by bots or crawlers count as active user sessions?

Repeated visits from bots or crawlers will not be counted as active user sessions.

Will a user accessing a public download link be counted as an active user session?

A user accessing a public download link to download a document will not be counted as an active user session. Even if the user is brought to the Oracle Content Management user interface, showing the **Download** button, it won't count as an active user session. However, the outbound data transfer per hour will be tracked.

What if the public download link is accessed via a site created with Oracle Content Management? Will using the link be counted as an active user session?

Visiting the site created with Oracle Content Management triggers an active user session, so it will count as an active user for that hour, but not due to using the public download link. Again, the outbound data transfer will be tracked.

For a browser session, how are active user sessions tracked?

The active user sessions for a browser are tracked by placing a cookie that expires after the one-hour session window ends in the browser session.

What happens if a user clears cookies in the browser or closes an incognito browser session?

If the user clears the cookie (by clearing in browser or closing an incognito window), the next request will be treated as a new user and count as a new active user session.

Are AppLinks and API calls tracked for billing purposes?

AppLinks and API calls from third-party applications and from other Oracle Cloud applications are charged according to the user identity (Standard or Enterprise) used to establish the API connection. Every 100 API calls in a given hour count as an additional active user for that hour.

How are AppLink calls tracked as visitor sessions?

The `assignedUser` parameter in the [AppLink](#) request body is used to track the client-side invocations associated to unique users.

How is a user of the Oracle Content Management desktop client tracked?

A desktop client user is tracked as an active user (either as a standard or enterprise user as appropriate) if they create, edit, or update files or folders from their desktop. Downward syncing actions from the cloud server caused by other user updates to files or folders are not counted as active user sessions. However, syncing does count toward the outbound data transfer metric. For example, if a user syncs more than 1 GB of data per hour, each additional GB synced will count as an additional active user session for that hour (either standard or enterprise as appropriate).

Understand Visitor Sessions

A *visitor session* is metric used by Oracle Content Management to track usage during a specified *session window* (one hour for hourly visitor sessions and 24 hours for daily visitor sessions). A visitor session is triggered when a unique unauthenticated user or an authenticated user who has the *site visitor* role accesses the service using a specific channel (for example, via a browser, mobile browser or applink, etc.). Access from multiple channels counts as multiple visitor sessions. For example, if one user in a 24 hour period accesses the same Oracle Content Management instance from a Firefox desktop web browser, a Chrome

desktop web browser, and a mobile web browser, that would count as a total of three *daily* visitor sessions.

Unauthenticated users can access certain sites, use public links, and view Oracle Content Management content embedded in apps or websites.

Frequently Asked Questions

If a user accesses multiple pages within the same Oracle Content Management instance, does that count as multiple visitor sessions?

No. Visitor sessions are only counted at the instance (site) level.

When is a visitor session triggered?

A visitor session is initiated by any user (anonymous or authenticated *guest*) who accesses an Oracle Content Management resource such as an Oracle Content Management instance, a site created with Oracle Content Management, or via an API (for example, using applinks) at least once during the session window.

How long does a visitor session last?

The duration of an hourly visitor session is one hour; a daily visitor session is 24 hours. It starts the first time the user accesses a specific Oracle Content Management resource via a unique channel. After one hour, subsequent visits by the same user to the same resource triggers another *hourly* visitor session. After 24 hours, subsequent visits by the same user to the same resource triggers another *daily* visitor session.

Will an Oracle Content Management standard or enterprise user be counted in visitor session counts?

No. An authenticated (signed-in) standard or enterprise user that visits an Oracle Content Management resource isn't included in visitor session counts.

Does the visitor session apply to authenticated (signed-in) users visiting an Oracle Content Management resource?

As stated above an authenticated Oracle Content Management standard or enterprise user that visits an Oracle Content Management resource will not be counted in visitor session counts. However, an authenticated user with the *site visitor* role *will* be counted in the visitor session counts.

How often is the visitor session calculated?

The visitor might access the same resource (site, API or applink) multiple times in the visitor session window (one hour for hourly visitor sessions and 24 hours for daily visitor sessions), but will be counted as one/single visit. If the user accesses the same resource again after the visitor session window, it will be counted as new visit.

Does a user visiting a second site count as a second visitor session?

The same user accessing a different resource (such as a different site) will be counted as a separate visitor session visit. For example, the same user accessing two different sites within the session window will be counted as two visits. Essentially the count is per user, per resource, per channel, per visitor session window for a given service instance.

Will visits to a site by bots or crawlers count as visitor sessions?

Repeated visits from bots or crawlers will not be counted as visitor sessions.

Will a user accessing a public download link be counted as visitor session?

A user accessing a public download link to download a document will not be counted as a visitor session. Even if the user is brought to the Oracle Content Management user interface, showing the **Download** button, it won't count as a visitor session.

What if the public download link is accessed via a site created with Oracle Content Management? Will using the link be counted as visitor session?

Visiting the site created with Oracle Content Management triggers a visitor session, so it will count as a visitor session, but not due to using the public download link.

For a browser session, how are the visitor sessions tracked?

The visitor sessions for a browser are tracked by placing a cookie that expires after the session window ends in the browser session.

What happens if a user clears his cookies in his browser or closes an incognito browser session?

If the user clears the cookie (by clearing in browser or closing an incognito window), the next request will be treated as a new user and count as a new visitor session.

What metrics are reported to administrators?

Oracle Content Management Analytics provides the following metrics:

- Break down of visitor session counts on hourly basis
- Aggregation of visitor session counts per month
- Ability to drill down on each day of the month (to get to visitor counts)

What metrics are not currently supported or captured?

- Cookie disabling: Some customers can disable cookie tracking on the browser side as an end user policy. In such cases, Oracle Content Management can't track the visitor based cookies since they are turned off, meaning the count will be lower than the actual number of visitors.
- Tracking visitors via the Oracle Content Management desktop application (the desktop application currently supports counting only named users).
- Tracking visits via the Oracle Content Management mobile applications (the mobile applications currently support counting only named users).

What about opt-out or privacy support with regards to cookie tracking?

Oracle Content Management sites will provide a standard option of letting the user know that a Oracle Content Management resource (site) is using cookies and users can opt-out by disabling the cookie. To support this, the following two items are added consistently across all the Oracle Content Management site resources:

- Opt-out summary message: This message appears on each site to indicate that a cookie is being used for tracking. It includes a link to the privacy page.
- Privacy site page: A standard sites page explaining the usage of a cookie as well the steps to disable the cookie. You can customize this page like any other sites page.

Are AppLinks and API calls tracked as visitor sessions?

AppLinks and REST API calls from third-party applications are included in the visitor sessions counts.

How are AppLink calls tracked as visitor sessions?

The `assignedUser` parameter in the `AppLink` request body is used to track the client-side invocations associated to unique users.

Examples

Here are some examples of visitor session counts. Let's assume ACME Corporation has an Oracle Content Management service instance and has created three sites: SiteA, SiteB, and SiteC. Following are examples of how the visitor sessions would be counted during a session window.

Visitor	Resource (Site)	Daily Visitor Session Counts
User1	<code>https://docs-acme.sites.us2.oraclecloud/authsite/SiteA</code>	Count increases to 1 (cookie1, user visits a site—SiteA, using Firefox)
User1	<code>https://docs-acme.sites.us2.oraclecloud/authsite/SiteB</code>	Count increases to 2 (cookie2, same user but different site—SiteB, using Firefox)
User2	<code>https://mysite.acme.example.com</code> (vanity URL for SiteC)	Count increases to 3 (cookie3, different user, different site—SiteC, using Firefox)
User3	<code>https://mysite.acme.example.com</code> (vanity URL for SiteC)	Count increases to 4 (cookie4, different user, same site—SiteC, using Firefox)
User2	<code>https://mysite.acme.example.com</code> (vanity URL for SiteC)	Count stays at 4 (no change, cookie3, same user—User2, same site—SiteC, using Firefox, same session window)
User2	<code>https://mysite.acme.example.com</code> (vanity URL for SiteC)	Count increases to 5 (cookie5, same user—User2, same site—SiteC, same session window, but using Chrome)

Deploy and Manage Legacy Instances of Oracle Content Management for Government on OCI Classic

If you have Oracle Content Management for Government on Oracle Cloud Infrastructure Classic (OCI Classic), there are some differences in how you deploy and manage Oracle Content Management.

If you have Oracle Content Management Cloud Service for Oracle CX, you *must* [create new instances](#), as well as manage and monitor those instances, in the Oracle Cloud Console. Don't follow the instructions below.

If you have Oracle Content Management for Government on Oracle Cloud Infrastructure Classic (OCI Classic), you perform the following tasks differently:

- [Create new instances](#)
- [Manage existing instances](#)

All other tasks are performed as described in previous chapters:

- [Configure service settings](#)

- [Manage users, groups, and access](#)
- [Manage the Service](#)
- [Analyze service usage](#)
- You might also want to integrate Oracle Content Management with other business applications as described in *Integrating and Extending Oracle Content Management*.



Create an Instance of Oracle Content Management for Government

To create an Oracle Content Management for Government instance, follow these steps.

1. [Verify that the cloud account Administrator is part of the OCI_Administrators Group](#)
2. [Get region, user, and tenancy values](#)
3. [Create a compartment for OCI object storage](#)
4. [Generate a private key](#)
5. [Generate a public key, and add it to OCI](#)
6. [Create your Oracle Content Management instance](#)

Verify That the Cloud Account Administrator Is Part of the OCI_Administrators Group

To create an instance, you must be part of the **OCI_Administrators** group. This group is created automatically when you have an Oracle Cloud account with Oracle Cloud Infrastructure (OCI). If you are the primary account administrator, you're automatically part of this group and can skip this step. If you're not the primary account administrator, follow these steps to confirm you're in the group.




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 **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 **Users** to list the group members.
7. Verify that the cloud account administrator user is listed.

If you're not a member of **OCI_Administrators**, you need to add yourself to the group. See [Assign Users to Groups](#).


Get Region, User, and Tenancy Values

When you create your Oracle Content Management instance, you'll be asked for values from Oracle Cloud Infrastructure for setting up object storage. To get these values, perform the following steps:


1. Return to the Oracle Cloud Console window.

2. In the data center drop-down list in the top right, select the data center that's closest to the region in which your company is based. Note the name of the region. This will be your Region and your Storage Infrastructure Region Name.
3. Click , expand **Identity**, and click **Users**.
4. Under Users, look for the cloud account administrator user and note the **OCID** value. You can use this value as your Storage User OCID. Several users might be listed here, so be sure to use the OCID of a user who has administrator privileges. Or you can create another user for storage service, assign that user to the **Administrators** group, and use the OCID of the user you created. To create a user in the Oracle Cloud Console:
 - a. Click , expand **Identity**, click **Users**, and then click **Create User**.
 - b. Enter a user name, and then click **Create**.
 - c. Click , expand **Identity**, and click **Groups**.
 - d. Click the **Administrators** link.
 - e. Click **Add User to Group**, select the new user in the drop-down list, and then click **Add**.
 - f. Get the User OCID of the new user from Group Members. You can use this value as your Storage User OCID.

Creating a user in the Oracle Cloud Console is not going to add or create the user account in IDCS. The cloud account administrator should use the IDCS Admin Console to create the user and assign the application roles for the user to sign into and access the Oracle Content Management service.

5. Click , click **Administration**, and then click **Tenancy Details**. Under Tenancy Information, note the **OCID** value. You can use this value as your tenancy OCID.

Create a Compartment for OCI Object Storage

1. In the Oracle Cloud Console, click , under Governance and Administration, expand **Identity**, and click **Compartments**.
Two compartments are created by default, the root compartment of the Tenancy (RC) and the ManagedCompartmentforPaaS (C). Do not use these default compartments. You need to create a new compartment for object storage.
2. On the Compartments page, click **Create Compartment**.
3. Enter a name and description for the compartment.
4. Click **Create Compartment**.
5. After the compartment is created, next to **OCID**, click **Show**, and note the value. This will be your Storage Compartment ID.
You need to create a new compartment the first time you create an Oracle Content Management instance, but you do not need to create a new compartment for every instance,. You can use the same compartment for multiple instances.

Generate a Private Key

Use the following OpenSSL commands to generate an API signing key/key pair in the required PEM format.

 **Note:**

- If you're using Windows, you need to run the commands with Git for Windows. If you don't have Git for Windows, you can download it from <https://git-scm.com/download/win>.
- If you're using Linux, OpenSSL is installed by default.

1. If you haven't already, create an `.oci` directory to store the credentials:

```
mkdir ~/.oci
```

2. Generate the private key with no passphrase:

```
openssl genrsa -out ~/.oci/oci_api_key.pem 2048
```

3. Ensure that only you can read the private key file:

```
chmod go-rwx ~/.oci/oci_api_key.pem
```

You'll upload this private key file when you create your Oracle Content Management instance.

Generate a Public Key and Add it to OCI

1. Generate a public key:

```
openssl rsa -pubout -in ~/.oci/oci_api_key.pem -out ~/.oci/oci_api_key_public.pem
```

2. Show the public key:


```
cat ~/.oci/oci_api_key_public.pem
```

3. Copy the full text of the public key.

4. Add the public key to the Oracle Cloud Console:

- a. From the menu, click **Identity** and then **Users**.
- b. Select the user.
- c. Click **Add Public Key**.
- d. In the dialog, paste the public key, and then click **Add**.
- e. After you add the public key, note the **Fingerprint** value. If you've added more than one public key, make sure to note the correct fingerprint value based on the time stamp. This will be your Storage Public Key Fingerprint.

Create Your Oracle Content Management Instance

1. Return to the Oracle Cloud Console, click  on the top left to open the navigation menu, expand **Platform Services**, then click **Content and Experience**.
2. Click **Create Instance**.


 **Note:**

For successful creation of the instance, be sure to follow the instructions on the Create Instance page exactly as indicated in the **Description** column for every field. Do not leave any default values prior to committing your information.

3. Enter the following information, and then click **Next**.

Field	Description
Instance Name	Specify a unique name for your service instance. If you specify a name that already exists, the system displays an error and the instance is not created.
Description	Optionally, enter a description of the instance.
Notification Email	Enter the email address to which you want provisioning status updates to be sent.
Region	Select the region name you noted when getting region, user, and tenancy values.
Tags	Leave this field blank.
Storage User OCID	Enter the storage user OCID you noted when getting region, user, and tenancy values.
Storage Tenancy OCID	Enter the tenancy OCID you noted when getting region, user, and tenancy values.
Storage Infrastructure Region Name	Enter the region name you noted when getting region, user, and tenancy values.
Storage Compartment ID	Enter the compartment OCID you noted after creating a compartment for OCI object storage.
Storage Public Key Fingerprint	Enter the public key fingerprint you noted after adding the public key to Oracle Cloud Infrastructure.
Storage Private Key	Upload the private key file you generated.

What to Do Next

After your service instance is successfully created, you get an email to confirm it. The email includes a link to your instance. To access the Oracle Content Management web client, click  next to your Oracle Content Management service instance, and select **Access Content Cloud Service Instance**.

Next, [set up users and groups](#).


Important:

- When you create your instance, a user named CEC_INTERNAL_APPID_USER is automatically created. It's an internal user that can't be used to sign in. This user enables communication between Oracle Content Management components. *Do not delete this user* or some functionality in Oracle Content Management will no longer work.
- After your instance is created, you'll be billed based on [active users per hour](#) and [visitor sessions](#).




Manage Oracle Content Management for Government

If you have Oracle Content Management for Government, there are some differences in how manage your instances.

To view your instances:

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 , under More Oracle Cloud Services, expand **Platform Services**, then click **Content and Experience**. You might need to use the scroll bar on the left to scroll down to see the menu option.

From the list of instances you can perform the following actions:

- You can perform some management tasks from the list of instances. Next to the instance you want to manage, click . You can access the Oracle Content Management web client for the instance, add tags, or delete the instance.
- To view general information about an instance, click its name. You see information such as storage OCIDs, version, and account name. To view additional information, click .
- To manage an instance, click its name, then click . You can access the Oracle Content Management web client for the instance, add an association, update instance credentials, add tags, or view activity.

Understand Active Users per Hour

If you have an Oracle Content Management instance built on Oracle Cloud Infrastructure (OCI) and managed with the Infrastructure Classic Console, you'll be billed based on active users per hour.

An *active user per hour* is defined as a unique user that interacts with the service during a one-hour session. Active users are tracked through a cookie, user ID, token, device ID, IP, or session ID. Authenticated users and visitors are tracked based on the role given to the user (standard, enterprise, or visitor) in that service instance. Anonymous users are tracked as visitors.

Visitors and anonymous users that access the service from multiple channels (website, mobile app, desktop client, custom app via APIs, email, etc.) count as multiple active user sessions. An *authenticated user* that accesses the service from multiple channels counts as one active user session. For example, if one *visitor* in a one-hour period accesses the same Oracle Content Management instance from a Firefox desktop web browser, a Chrome desktop web browser, and a mobile web browser, that would count as a total of *three* active user sessions. Whereas, if one *authenticated user* performs the same actions, that would count as *one* active user session.

Depending on whether the user is a standard user, an enterprise user, or a visitor, the user is allowed a certain number of API calls, a certain amount of outbound data transfer, and, for enterprise users, a certain number of new published content assets. Therefore, for billing purposes, the following metrics are also tracked during each one-hour active user session:

- Number of API calls made to the service by custom third-party applications (non-Oracle) — If the number of API calls exceeds the API calls that are entitled per active user in a one-hour period, a new active user is added to the hourly count.
- Outbound data transfer — This includes the data a user downloads from the Oracle Cloud Service *and* any transfer of data from the Oracle Cloud Service over the internet, including responses to client requests. If the outbound data transfer exceeds the data transfer that is entitled per active user in a one-hour period, a new active user is added to the hourly count.
- Number of newly published assets (enterprise users only) — A published asset is either a file based asset (for example, a document, an image, or a video) or a content item that has been published. A content item is a block of information created using a content type. If the number of newly published assets exceeds the published assets that are entitled per active user in a one-hour period, a new active user is added to the hourly count. This count doesn't include previously published assets, only assets published during the one hour active user session.

**Note:**

For information on Universal Credits pricing and usage limits (for example, the number of API calls, amount of outbound data transfer, and number published assets allowed per user), see [Oracle Universal Credits Pricing](#) and [Oracle Cloud Services](#) (view “Oracle PaaS and IaaS Universal Credits - Service Descriptions” near the bottom of the list).

Frequently Asked Questions

Does a user visiting a second site count as a second active user session?

Only a *visitor or anonymous user* accessing a different resource (such as a different site) will be counted as a separate active user session. An *authenticated user* accessing the service from multiple channels will be counted as one active user session. For example, the same *visitor* accessing two different sites within the one-hour session window will be counted as two active user sessions. Essentially the count is per visitor or anonymous user, per resource, per channel, per one-hour session window for a given service instance.

Will visits to a site by bots or crawlers count as active user sessions?

Repeated visits from bots or crawlers will not be counted as active user sessions.

Will a user accessing a public download link be counted as an active user session?

A user accessing a public download link to download a document will not be counted as an active user session. Even if the user is brought to the Oracle Content Management user interface, showing the **Download** button, it won't count as an active user session. However, the outbound data transfer per hour will be tracked.

What if the public download link is accessed via a site created with Oracle Content Management? Will using the link be counted as an active user session?

Visiting the site created with Oracle Content Management triggers an active user session, so it will count as an active user for that hour, but not due to using the public download link. Again, the outbound data transfer will be tracked.

For a browser session, how are active user sessions tracked?

The active user sessions for a browser are tracked by placing a cookie that expires after the one-hour session window ends in the browser session.

What happens if a user clears cookies in the browser or closes an incognito browser session?

If the user clears the cookie (by clearing in browser or closing an incognito window), the next request will be treated as a new user and count as a new active user session.

Are AppLinks and API calls tracked for billing purposes?

AppLinks and API calls from third-party applications and from other Oracle Cloud applications are charged according to the user identity (Standard or Enterprise) used to establish the API connection. Every 100 API calls in a given hour count as an additional active user for that hour.

How are AppLink calls tracked as visitor sessions?

The `assignedUser` parameter in the [AppLink](#) request body is used to track the client-side invocations associated to unique users.

How is a user of the Oracle Content Management desktop client tracked?

A desktop client user is tracked as an active user (either as a standard or enterprise user as appropriate) if they create, edit, or update files or folders from their desktop. Downward syncing actions from the cloud server caused by other user updates to files or folders are not counted as active user sessions. However, syncing does count toward the outbound data transfer metric. For example, if a user syncs more than 1 GB of data per hour, each additional GB synced will count as an additional active user session for that hour (either standard or enterprise as appropriate).

Understand Visitor Sessions

A *visitor session* is metric used by Oracle Content Management to track usage during a specified *session window* (one hour for hourly visitor sessions and 24 hours for daily visitor sessions). A visitor session is triggered when a unique unauthenticated user or an authenticated user who has the *site visitor* role accesses the service using a specific channel (for example, via a browser, mobile browser or applink, etc.). Access from multiple channels counts as multiple visitor sessions. For example, if one user in a 24 hour period accesses the same Oracle Content Management instance from a Firefox desktop web browser, a Chrome desktop web browser, and a mobile web browser, that would count as a total of three *daily* visitor sessions.

Unauthenticated users can access certain sites, use public links, and view Oracle Content Management content embedded in apps or websites.

Frequently Asked Questions

If a user accesses multiple pages within the same Oracle Content Management instance, does that count as multiple visitor sessions?

No. Visitor sessions are only counted at the instance (site) level.

When is a visitor session triggered?

A visitor session is initiated by any user (anonymous or authenticated *guest*) who accesses an Oracle Content Management resource such an Oracle Content Management instance, a

site created with Oracle Content Management, or via an API (for example, using applinks) at least once during the session window.

How long does a visitor session last?

The duration of an hourly visitor session is one hour; a daily visitor session is 24 hours. It starts the first time the user accesses a specific Oracle Content Management resource via a unique channel. After one hour, subsequent visits by the same user to the same resource triggers another *hourly* visitor session. After 24 hours, subsequent visits by the same user to the same resource triggers another *daily* visitor session.

Will an Oracle Content Management standard or enterprise user be counted in visitor session counts?

No. An authenticated (signed-in) standard or enterprise user that visits an Oracle Content Management resource isn't included in visitor session counts.

Does the visitor session apply to authenticated (signed-in) users visiting an Oracle Content Management resource?

As stated above an authenticated Oracle Content Management standard or enterprise user that visits an Oracle Content Management resource will not be counted in visitor session counts. However, an authenticated user with the *site visitor* role *will* be counted in the visitor session counts.

How often is the visitor session calculated?

The visitor might access the same resource (site, API or applink) multiple times in the visitor session window (one hour for hourly visitor sessions and 24 hours for daily visitor sessions), but will be counted as one/single visit. If the user accesses the same resource again after the visitor session window, it will be counted as new visit.

Does a user visiting a second site count as a second visitor session?

The same user accessing a different resource (such as a different site) will be counted as a separate visitor session visit. For example, the same user accessing two different sites within the session window will be counted as two visits. Essentially the count is per user, per resource, per channel, per visitor session window for a given service instance.

Will visits to a site by bots or crawlers count as visitor sessions?

Repeated visits from bots or crawlers will not be counted as visitor sessions.

Will a user accessing a public download link be counted as visitor session?

A user accessing a public download link to download a document will not be counted as a visitor session. Even if the user is brought to the Oracle Content Management user interface, showing the **Download** button, it won't count as a visitor session.

What if the public download link is accessed via a site created with Oracle Content Management? Will using the link be counted as visitor session?

Visiting the site created with Oracle Content Management triggers a visitor session, so it will count as a visitor session, but not due to using the public download link.

For a browser session, how are the visitor sessions tracked?

The visitor sessions for a browser are tracked by placing a cookie that expires after the session window ends in the browser session.

What happens if a user clears his cookies in his browser or closes an incognito browser session?

If the user clears the cookie (by clearing in browser or closing an incognito window), the next request will be treated as a new user and count as a new visitor session.

What metrics are reported to administrators?

Oracle Content Management Analytics provides the following metrics:

- Break down of visitor session counts on hourly basis
- Aggregation of visitor session counts per month
- Ability to drill down on each day of the month (to get to visitor counts)

What metrics are not currently supported or captured?

- Cookie disabling: Some customers can disable cookie tracking on the browser side as an end user policy. In such cases, Oracle Content Management can't track the visitor based cookies since they are turned off, meaning the count will be lower than the actual number of visitors.
- Tracking visitors via the Oracle Content Management desktop application (the desktop application currently supports counting only named users).
- Tracking visits via the Oracle Content Management mobile applications (the mobile applications currently support counting only named users).

What about opt-out or privacy support with regards to cookie tracking?

Oracle Content Management sites will provide a standard option of letting the user know that a Oracle Content Management resource (site) is using cookies and users can opt-out by disabling the cookie. To support this, the following two items are added consistently across all the Oracle Content Management site resources:

- Opt-out summary message: This message appears on each site to indicate that a cookie is being used for tracking. It includes a link to the privacy page.
- Privacy site page: A standard sites page explaining the usage of a cookie as well the steps to disable the cookie. You can customize this page like any other sites page.

Are AppLinks and API calls tracked as visitor sessions?

AppLinks and REST API calls from third-party applications are included in the visitor sessions counts.

How are AppLink calls tracked as visitor sessions?

The `assignedUser` parameter in the [AppLink](#) request body is used to track the client-side invocations associated to unique users.

Examples

Here are some examples of visitor session counts. Let's assume ACME Corporation has an Oracle Content Management service instance and has created three sites: SiteA, SiteB, and SiteC. Following are examples of how the visitor sessions would be counted during a session window.

Visitor	Resource (Site)	Daily Visitor Session Counts
User1	https://docs-acme.sites.us2.oraclecloud/authsite/SiteA	Count increases to 1 (cookie1, user visits a site—SiteA, using Firefox)
User1	https://docs-acme.sites.us2.oraclecloud/authsite/SiteB	Count increases to 2 (cookie2, same user but different site—SiteB, using Firefox)
User2	https://mysite.acme.example.com (vanity URL for SiteC)	Count increases to 3 (cookie3, different user, different site—SiteC, using Firefox)
User3	https://mysite.acme.example.com (vanity URL for SiteC)	Count increases to 4 (cookie4, different user, same site—SiteC, using Firefox)
User2	https://mysite.acme.example.com (vanity URL for SiteC)	Count stays at 4 (no change, cookie3, same user—User2, same site—SiteC, using Firefox, same session window)
User2	https://mysite.acme.example.com (vanity URL for SiteC)	Count increases to 5 (cookie5, same user—User2, same site—SiteC, same session window, but using Chrome)

Deploy and Manage Legacy Instances of Oracle Content Management for SaaS on OCI Classic

If you have Oracle Content Management for SaaS on Oracle Cloud Infrastructure Classic (OCI Classic), there are some differences in how you deploy and manage Oracle Content Management.

If you have Oracle Content Management Cloud Service for Oracle CX, you *must* [create new instances](#), as well as manage and monitor those instances, in the Oracle Cloud Console. Don't follow the instructions below.

If you have Oracle Content Management for SaaS on Oracle Cloud Infrastructure Classic (OCI Classic), you perform the following tasks differently:

- [Create new instances](#)
- [Manage and monitor](#)

All other tasks are performed as described in previous chapters:


- [Configure service settings](#)
- [Manage users, groups, and access](#)
- [Analyze service usage](#)
- You might also want to integrate Oracle Content Management with other business applications as described in *Integrating and Extending Oracle Content Management*.

Create an Instance of Oracle Content Management for SaaS


If you have Oracle Content Management for SaaS, you need to set up your storage service and create the storage user, and then create your service instance.

To create an Oracle Content Management for SaaS instance, use the following procedure:

1. Set up your storage service:
 - 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 Infrastructure Classic Console, next to Storage Classic, click , and select **Open Service Console**.


Note:


If you don't see Storage Classic in the dashboard, click , and set Storage Classic to **Show**.

- c. The first time you access the Storage Classic service, you'll be prompted to set the georeplication policy. Select a region close to where the service will primarily be used.
After the storage service is configured, you'll be asked to create a new container, indicating that the configuration finished. You can continue to the next step without creating a new container.
 - d. Click the **Account** tab, and make note of **REST Endpoint**. This is the Storage URL you'll enter when you create your Oracle Content Management for SaaS instance.
2. Create the storage user:
Create a dedicated user for storage access so that you have an independent user, separate from the root user, to avoid conflicts with password resets, and so on.

Note:


This user won't be used to access Oracle Content Management.

- a. In the Infrastructure Classic Console, click , then, under Account Management, click **Users**. You might need to use the scroll bars on the right to scroll down to see the menu option.
 - b. On the User Management page, in the banner, click **Identity Console**. This opens the Oracle Identity Cloud Service Users page.
 - c. Click **Add**.
 - d. Enter `Storage` as the first name and `Admin` as the last name.
 - e. Enter `storageadmin` as the user name.
 - f. Clear the **Use the email address as the user name** box.

- g. Enter an email that *won't* be used to sign in to Oracle Content Management, but that you have access to, so you can set the password.
- h. After you receive the welcome email for the storageadmin user, set the storageadmin password.
- i. Click **Finish**.
- j. Expand the navigation drawer, and then click **Applications**.
- k. Find and open your Storage Classic application.
- l. Click the **Application Roles** tab.
- m. Next to the **Storage_Administrator** role, click , and then select **Assign Users**.
- n. Find and select the **Storage User**, and then click **Assign**.

 **Important:**

Make sure no one deletes this user or Oracle Content Management will no longer be able to communicate with the storage service.

3. Create your Oracle Content Management for SaaS instance:
 - a. To return to the Infrastructure Classic Console, click , then click **My Services**.
 - b. Click **Create Instance**.
 - c. Click the **All Services** tab.
 - d. Scroll down to the **Content and Experience** section.
 - e. Next to **Content Cloud**, click **Create**.
 - f. On the **Instances** tab of the Oracle Content Management Service page, click **Create Instance**.
 - g. Enter the following information, and then click **Next**.

Field	Description
Instance Name	Specify a unique name for your service instance. If you specify a name that already exists, the system displays an error and the instance is not created.
Description	Optionally, enter a description of the instance.
Notification Email	Enter the email address to which you want provisioning status updates to be sent.
Region	Select the data center that is closest to the region in which your company is based.
Tags	Leave this field blank..
Storage URL	Enter the URL to your storage service.
Storage Username	Enter the user name of the dedicated user you created for your storage service (this should be <code>storageadmin</code>).

Field	Description
Storage Password	Enter the password for the storage service user.

h. Click Create.

After your service instance request is approved, you receive an email saying the instance was successfully created and a second email welcoming you to Oracle Content Management. The first email includes a link to your instance (in the Infrastructure Classic Console). The second email includes a link to the Oracle Content Management web client.

! Important:

- When you create your instance, a user named `CEC_INTERNAL_APPID_USER` is automatically created. It's an internal user that can't be used to sign in. This user enables communication between Oracle Content Management components. *Do not delete this user* or some functionality in Oracle Content Management will no longer work.
- If you purchased visitor licenses, you'll be billed based on [visitor sessions](#).

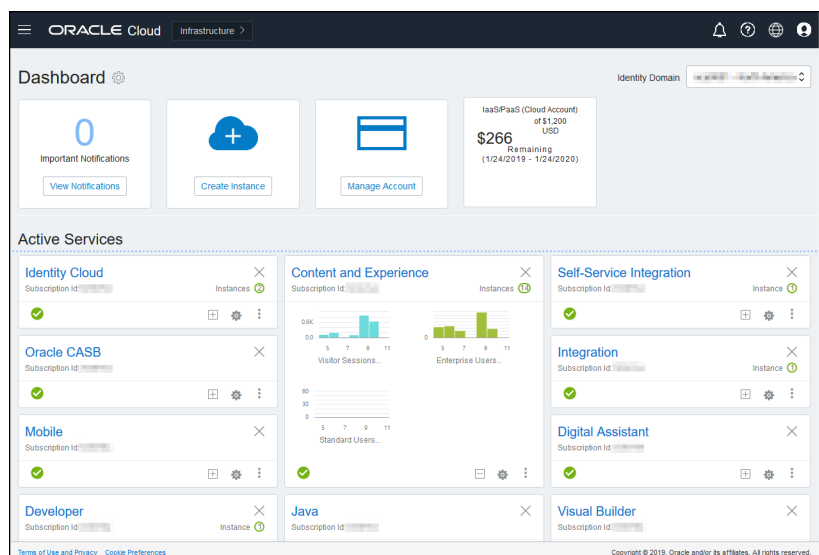
What to Do Next

After your service instance request is approved, you receive an email saying the instance was successfully created and a second email welcoming you to Oracle Content Management. The first email includes a link to the Infrastructure Classic Console (click the link to your instance). The second email includes a link to the web client.

Next, [set up users and groups](#).


Manage and Monitor Oracle Content Management for SaaS




If you have Oracle Content Management for SaaS, you manage and monitor your service through the Infrastructure Classic Console.



Expand the Content and Experience panel to see the following metrics:

Metric	Description
Visitor Sessions	Displays the number of daily visitor sessions allocated to this service instance. This metric appears only if you've purchased daily visitor sessions. To view additional usage metrics, click Visitor Sessions . See Understand Visitor Sessions .
Enterprise Users	Displays the number of enterprise users registered on this service instance. This metric appears only if you've purchased enterprise users. To view additional usage metrics, click Enterprise Users .
Standard Users	Displays the number of standard users registered on this service instance. To view additional usage metrics, click Standard Users .


To see details about your service, in the Content and Experience panel, click , then select one of the following actions:

- **View Details:** You see the following tabs:
 - **Overview:** Displays information on your service and any service instances. From this page you can create a new service instance or change the settings for an existing instance.
 - **Billing Metrics:** Displays detailed usage information about your service.
 - **Billing Alerts:** Configure rules to limit usage and alert administrators when usage exceeds the configured limits.
 - **Documents:** Download reports pertaining to your subscriptions. Different categories of reports, such as usage metrics, billing, or incidents, can be downloaded if they are available. You can download daily, weekly, monthly, or yearly reports as required. Reports are available in PDF, MS Word, or Open XML.
- **Open Service Console:** View a list of all your service instances. From the list of instances you can perform the following actions:
 - You can perform some management tasks from the list of instances. Next to the instance you want to manage, click . You can access the Oracle Content Management web client for the instance, add tags, or delete the instance.
 - To view general information about an instance, click its name. You see information such as storage OCIDs, version, and account name. To view additional information, click .
 - To manage an instance, click its name, then click . You can access the Oracle Content Management web client for the instance, add an association, update instance credentials, add tags, or view activity.
- **View Account Usage Details:** You see the following tabs:

- **Usage:** Displays the aggregated usage charges for individual services along with resource utilization and overages, if any.
- **Account Management:** Displays your subscription details.
- **Activate:** Activate and complete set up for pending orders.
- **My Admin Accounts:** View admin login credentials, manage passwords, and access your service consoles for all your Oracle Cloud admin accounts in one place.

View Billing Metrics

The Billing Metrics page in the Infrastructure Classic Console displays detailed usage information about your service.

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 dashboard, next to your service, click , and select **View Details**.
3. Click **Billing Metrics**. Use the metrics to better understand how much your service is being used and whether you need to change storage allocations. Which metrics you see depend on the service subscription that you have.

You see the following metrics:

Metric	Description
Visitor Sessions	Displays the number of daily visitor sessions allocated to this service instance. This metric appears only if you've purchased daily visitor sessions. To view additional usage metrics, click Visitor Sessions . See Understand Visitor Sessions .
Enterprise Users	Displays the number of enterprise users registered on this service instance. This metric appears only if you've purchased enterprise users. To view additional usage metrics, click Enterprise Users .
Standard Users	Displays the number of standard users registered on this service instance. To view additional usage metrics, click Standard Users .

Understand Visitor Sessions

A *visitor session* is metric used by Oracle Content Management to track usage during a specified *session window* (one hour for hourly visitor sessions and 24 hours for daily visitor sessions). A visitor session is triggered when a unique unauthenticated user or an authenticated user who has the *site visitor* role accesses the service using a specific channel (for example, via a browser, mobile browser or applink, etc.). Access from multiple channels counts as multiple visitor sessions. For example, if one user in a 24 hour period accesses the same Oracle Content Management instance from a Firefox desktop web browser, a Chrome desktop web browser, and a mobile web browser, that would count as a total of three *daily* visitor sessions.

Unauthenticated users can access certain sites, use public links, and view Oracle Content Management content embedded in apps or websites.

Frequently Asked Questions

If a user accesses multiple pages within the same Oracle Content Management instance, does that count as multiple visitor sessions?

No. Visitor sessions are only counted at the instance (site) level.

When is a visitor session triggered?

A visitor session is initiated by any user (anonymous or authenticated *guest*) who accesses an Oracle Content Management resource such as an Oracle Content Management instance, a site created with Oracle Content Management, or via an API (for example, using applinks) at least once during the session window.

How long does a visitor session last?

The duration of an hourly visitor session is one hour; a daily visitor session is 24 hours. It starts the first time the user accesses a specific Oracle Content Management resource via a unique channel. After one hour, subsequent visits by the same user to the same resource triggers another *hourly* visitor session. After 24 hours, subsequent visits by the same user to the same resource triggers another *daily* visitor session.

Will an Oracle Content Management standard or enterprise user be counted in visitor session counts?

No. An authenticated (signed-in) standard or enterprise user that visits an Oracle Content Management resource isn't included in visitor session counts.

Does the visitor session apply to authenticated (signed-in) users visiting an Oracle Content Management resource?

As stated above an authenticated Oracle Content Management standard or enterprise user that visits an Oracle Content Management resource will not be counted in visitor session counts. However, an authenticated user with the *site visitor* role will be counted in the visitor session counts.

How often is the visitor session calculated?

The visitor might access the same resource (site, API or applink) multiple times in the visitor session window (one hour for hourly visitor sessions and 24 hours for daily visitor sessions), but will be counted as one/single visit. If the user accesses the same resource again after the visitor session window, it will be counted as new visit.

Does a user visiting a second site count as a second visitor session?

The same user accessing a different resource (such as a different site) will be counted as a separate visitor session visit. For example, the same user accessing two different sites within the session window will be counted as two visits. Essentially the count is per user, per resource, per channel, per visitor session window for a given service instance.

Will visits to a site by bots or crawlers count as visitor sessions?

Repeated visits from bots or crawlers will not be counted as visitor sessions.

Will a user accessing a public download link be counted as visitor session?

A user accessing a public download link to download a document will not be counted as a visitor session. Even if the user is brought to the Oracle Content Management user interface, showing the **Download** button, it won't count as a visitor session.

What if the public download link is accessed via a site created with Oracle Content Management? Will using the link be counted as visitor session?

Visiting the site created with Oracle Content Management triggers a visitor session, so it will count as a visitor session, but not due to using the public download link.

For a browser session, how are the visitor sessions tracked?

The visitor sessions for a browser are tracked by placing a cookie that expires after the session window ends in the browser session.

What happens if a user clears his cookies in his browser or closes an incognito browser session?

If the user clears the cookie (by clearing in browser or closing an incognito window), the next request will be treated as a new user and count as a new visitor session.

What metrics are reported to administrators?

Oracle Content Management Analytics provides the following metrics:

- Break down of visitor session counts on hourly basis
- Aggregation of visitor session counts per month
- Ability to drill down on each day of the month (to get to visitor counts)

What metrics are not currently supported or captured?

- Cookie disabling: Some customers can disable cookie tracking on the browser side as an end user policy. In such cases, Oracle Content Management can't track the visitor based cookies since they are turned off, meaning the count will be lower than the actual number of visitors.
- Tracking visitors via the Oracle Content Management desktop application (the desktop application currently supports counting only named users).
- Tracking visits via the Oracle Content Management mobile applications (the mobile applications currently support counting only named users).

What about opt-out or privacy support with regards to cookie tracking?

Oracle Content Management sites will provide a standard option of letting the user know that a Oracle Content Management resource (site) is using cookies and users can opt-out by disabling the cookie. To support this, the following two items are added consistently across all the Oracle Content Management site resources:

- Opt-out summary message: This message appears on each site to indicate that a cookie is being used for tracking. It includes a link to the privacy page.
- Privacy site page: A standard sites page explaining the usage of a cookie as well the steps to disable the cookie. You can customize this page like any other sites page.

Are AppLinks and API calls tracked as visitor sessions?

AppLinks and REST API calls from third-party applications are included in the visitor sessions counts.

How are AppLink calls tracked as visitor sessions?

The `assignedUser` parameter in the [AppLink](#) request body is used to track the client-side invocations associated to unique users.

Examples

Here are some examples of visitor session counts. Let's assume ACME Corporation has an Oracle Content Management service instance and has created three sites: SiteA, SiteB, and

SiteC. Following are examples of how the visitor sessions would be counted during a session window.

Visitor	Resource (Site)	Daily Visitor Session Counts
User1	https://docs-acme.sites.us2.oraclecloud/authsite/SiteA	Count increases to 1 (cookie1, user visits a site—SiteA, using Firefox)
User1	https://docs-acme.sites.us2.oraclecloud/authsite/SiteB	Count increases to 2 (cookie2, same user but different site—SiteB, using Firefox)
User2	https://mysite.acme.example.com (vanity URL for SiteC)	Count increases to 3 (cookie3, different user, different site—SiteC, using Firefox)
User3	https://mysite.acme.example.com (vanity URL for SiteC)	Count increases to 4 (cookie4, different user, same site—SiteC, using Firefox)
User2	https://mysite.acme.example.com (vanity URL for SiteC)	Count stays at 4 (no change, cookie3, same user—User2, same site—SiteC, using Firefox, same session window)
User2	https://mysite.acme.example.com (vanity URL for SiteC)	Count increases to 5 (cookie5, same user—User2, same site—SiteC, same session window, but using Chrome)

Deploy and Manage Oracle Content Management with a Non-Metered Subscription

If you have a non-metered subscription with an Oracle Content Management entitlement, there are some differences in how you deploy and manage Oracle Content Management.

For legacy instances that you created in the Infrastructure Classic Console (previously called My Services), you can manage them as described in this topic. However, Oracle recommends that you [migrate those instances](#) to the native OCI environment (that is, using the Oracle Cloud Console to manage service instances). This will ensure that you'll enjoy the benefits and advances of Oracle's cloud platform in the future.

When managing legacy instances, you perform the following tasks differently:

- [Create new instances](#)
- [Set up users and groups](#)
- [Manage users, groups, and access](#)
- [Manage and monitor existing instances](#)

All other tasks are performed as described in previous chapters:

- [Configure service settings](#)
- [Analyze service usage](#)

- You might also want to integrate Oracle Content Management with other business applications as described in *Integrating and Extending Oracle Content Management*.

Create an Oracle Content Management Instance with a Non-Metered Subscription

If you have a non-metered subscription with Oracle Content Management, follow the instructions in this topic to create a service instance.

To create an Oracle Content Management instance with a non-metered subscription:

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. Click **Create Instance**.
3. Click the **All Services** tab.
4. Scroll down to the **Content Cloud** section.
5. On the Create New Oracle Content Management Instance page, enter the following information, and then click **Next**.

Field	Description
Name	Specify a unique name for your service instance. If you specify a name that already exists, the system displays an error and the instance is not created.
Plan	Select Oracle Content Management from the list.
Product	Select Content and Experience Cloud from the list.
Number of Standard Users	Enter the number of <i>standard users</i> you expect to use this instance. Each instance must include a minimum of 10 users. Under this box you see the number of users you have available. Note: If you don't see this option, you don't have an Oracle Content Management entitlement.
Number of Enterprise Users	Enter the number of <i>enterprise users</i> you expect to use this instance. Each instance must include a minimum of 10 users. Under this box you see the number of users you have available.
Daily Visitor Session Packs	Enter the number of Additional Daily Visitor Session Packs you expect to use with this instance each month. One daily visitor session pack equals 1,000 additional daily visitor sessions per month. Under this box you see the number of daily visitor session packs you have available.
Administrator Details	Enter the administrator's email, user name, first name, and last name.

What to Do Next

After your service instance request is approved, you receive an email saying the instance was successfully created and a second email welcoming you to Oracle Content

Management. The first email includes a link to the Infrastructure Classic Console (click the link to your instance). The second email includes a link to the web client.

Next, [set up users and groups](#).

Set Up Users and Groups (Traditional Cloud Account)

After your service instance is successfully created, set up your users and groups.

The [application roles](#) in Oracle Content Management are different when you have a non-metered subscription with an Oracle Content Management entitlement. 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.

If your company uses single sign-on (SSO), you'll want to enable SSO before adding users. See [Enable Single Sign-On \(SSO\)](#).

These are the main steps:

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

Application Roles in an Oracle Content Management Instance with a Non-Metered Subscription

The application roles in an Oracle Content Management instance with a non-metered subscription are slightly different than in an Oracle Content Management instance with a Universal Credits subscription.

The roles for a Universal Credits subscription are described in [Application Roles](#). The following table describes the application roles for an Oracle Content Management instance with a non-metered subscription.

Application Role (application role name in bold)	Access and Actions	Notes
Account administrator	<p>Account administrators use the My Account application to perform the following actions:</p> <ul style="list-style-type: none"> • Activate and create identity domains. • Activate a service. • Monitor and manage services across all identity domains and data centers. • Create identity domain administrators and other account administrators. <p>See Manage Your Oracle Cloud Service in <i>Getting Started with Oracle Cloud</i>.</p>	<p>Account administrators are set up when the account is created. They use their Oracle account to sign in to Oracle Cloud and access My Account. If you need account administrator access and don't have it, contact your primary account administrator. See Learn About Cloud Account Roles in <i>Getting Started with Oracle Cloud</i>.</p> <p>If you want account administrators to use Oracle Content Management and modify the service configuration, they must also be assigned the <i>standard user</i> or <i>enterprise user</i> role.</p>
Identity domain administrator (Identity Domain Administrator)	<p>From the Infrastructure Classic Console:</p> <ul style="list-style-type: none"> • Create and manage user accounts. • Assign and manage application roles, including creating custom application roles. <p>See Learn About Cloud Account Roles in <i>Getting Started with Oracle Cloud</i>.</p>	<p>Assigned at the domain level. Works across multiple services. Identity domain administrators perform the same functions that a service administrator can, plus they handle administrative duties related to users.</p> <p>There is only one service per identity domain for Oracle Content Management. One administrator performs the duties of the <i>service administrator</i> and the <i>identity domain administrator</i>.</p>
Entitlement administrator The format of the role name is <i>service-name_SE service name Based Entitlement Administrator</i> , for example, documents_SE Documents Service Based Entitlement Administrator .	<p>From the Infrastructure Classic Console:</p> <ul style="list-style-type: none"> • Create, manage, and view details of service instances. Applies when you're subscribed to an entitlement to create multiple instances of Oracle Content Management. • Monitor the status of service instances, and export instance metrics data. <p>See Create and Activate an Oracle Cloud Account.</p>	<p>Assigned at the service level. See Oracle Cloud User Roles and Privileges in <i>Getting Started with Oracle Cloud</i>.</p>

Application Role (application role name in bold)	Access and Actions	Notes
Service administrator (Oracle Content Management Administrator)	<p>From the Infrastructure Classic Console:</p> <ul style="list-style-type: none"> • Assign application roles. • Change user passwords and challenge questions. • Configure, monitor, and manage service instances. <p>From the Oracle Content Management Administration: System interface:</p> <ul style="list-style-type: none"> • Configure general settings such as branding, enabling notifications, and default time zone and language. • Configure user settings such as syncing profile data, setting the default role for new members added to folders, and transferring content ownership. • Configure documents settings such as storage quotas, enabling public links, and setting restrictions on the size and types of files that can be uploaded. • Configure custom properties (must also have Oracle Content Management <i>enterprise user</i> role). • Configure sites settings such as whether sites can be created and installing the default site templates. <p>From the Oracle Content Management Administration: Integrations interface:</p> <ul style="list-style-type: none"> • Integrate other business applications as described in <i>Integrating and Extending Oracle Content Management</i>. <p>From the Oracle Content Management Analytics interface:</p> <ul style="list-style-type: none"> • View service usage statistics and content metrics to help you analyze system needs or issues. • View reports. 	Service administrators must also be assigned the <i>standard user</i> or <i>enterprise user</i> role to be able to use Oracle Content Management.

Application Role (application role name in bold)	Access and Actions	Notes
Site administrator (Oracle Content Management Site Administrator)	<p>From the Oracle Content Management Sites page:</p> <ul style="list-style-type: none"> • Create sites. <p>From the Oracle Content Management Developer page:</p> <ul style="list-style-type: none"> • Create templates, components, and themes. <p>See Configure Sites Settings.</p>	<p>This role applies if your service administrator configured Oracle Content Management to allow only site administrators to create sites, templates, or components. Site administrators must also be assigned the <i>standard user</i> or <i>enterprise user</i> role to be able to use Oracle Content Management.</p>
Developer (CECDeveloperUser)	<p>From Oracle Content Management Sites page:</p> <ul style="list-style-type: none"> • Create, edit, and publish sites as long as this feature hasn't been limited to <i>site administrators</i>. <p>From Oracle Content Management Developer page:</p> <ul style="list-style-type: none"> • Create templates, components, and themes as long as these features haven't been limited to <i>site administrators</i>. <p>From Oracle Content Management Administration: Integrations interface:</p> <ul style="list-style-type: none"> – Integrate other business applications as described in <i>Integrating and Extending Oracle Content Management</i>. 	<p>Developers must also be assigned the <i>standard user</i> or <i>enterprise user</i> role to be able to use Oracle Content Management. Developers with the <i>standard user</i> role can create components, themes, and standard templates. Developers with the <i>enterprise user</i> role can also create layouts and save a site as a standard or enterprise template.</p>
Content administrator (Oracle Content Management Content Administrator)	<p>From the Oracle Content Management Administration: Assets page:</p> <ul style="list-style-type: none"> • Create new content types and taxonomies and publish items. 	<p>Content administrators must also be assigned the <i>enterprise user</i> role to be able to use Oracle Content Management and access assets.</p>
Repository administrator (CECRepositoryAdministrator)	<p>From the Oracle Content Management Administration: Assets page:</p> <ul style="list-style-type: none"> • Create asset repositories. • Create localization policies. • Create publishing channels. <p>From the Oracle Content Management Analytics interface:</p> <ul style="list-style-type: none"> • View Assets and Content Metrics to help you analyze system needs or issues. 	<p>Repository administrators must also be assigned the <i>enterprise user</i> role to be able to use Oracle Content Management and access assets. A repository administrator is a user with a Manager role within at least one repository.</p>

Application Role (application role name in bold)	Access and Actions	Notes
Standard user (Oracle Content Management Standard User)	From Oracle Content Management, <i>standard users</i> have access to: <ul style="list-style-type: none"> • Manage content (view, upload, and edit documents). • Share content and sites with others. • Use conversations to collaborate (discuss topics, direct message someone, assign flags to someone, add annotations to documents). • Manage groups. • Create, edit, and publish sites as long as this feature hasn't been limited to <i>site administrators</i>. • View and interact with content items in sites. • Manage and view custom properties and edit values. 	Any users that need to actually <i>use</i> Oracle Content Management must be assigned the <i>standard user</i> or <i>enterprise user</i> role. These roles aren't assigned by default to any user. See Task and Feature Comparison by Application Role .
Enterprise user (Oracle Content Management Enterprise User)	From Oracle Content Management, <i>enterprise users</i> have access to all the features that <i>standard users</i> have access to, plus: <ul style="list-style-type: none"> • Create, manage, view, publish, and interact with content items, digital assets, and collections. 	For use with an Oracle Content Management subscription. You must have purchased <i>enterprise users</i> . Any users that need to actually <i>use</i> Oracle Content Management must be assigned the <i>standard user</i> or <i>enterprise user</i> role. These roles aren't assigned by default to any user. See Task and Feature Comparison by Application Role .
Visitor (Oracle Content Management Visitor)	Access sites restricted to <i>visitors</i> .	This role applies if a site is set to be accessed only by visitors. If that restriction is enabled, only users with this role will be able to access the site. See <i>Change Site Security in Building Sites with Oracle Content Management</i> . Each user counts against the total users allowed for your service, except for visitors, which don't require a license. Visitor activity counts towards your daily visitor sessions. See Understand Visitor Sessions .
External user (CECEXternalUser)	Reserved for future use.	Do not use this role. Users assigned this role can't use the Oracle Content Management user interface.

Typical Organization Roles

When you create users, you'll give them the application roles needed to perform their tasks in Oracle Content Management. These users will typically fall into one of the following organization roles (or user types) and will require the listed application roles.

You can create groups for your organization roles and assign the listed application roles to those groups. Then you can add users to those groups to automatically assign them the appropriate application roles.

Organization Role	Application Roles Needed
<p>Anonymous User Anonymous users don't work for your company and don't exist in your Oracle Cloud identity domain or your directory. They are consumers engaging with your company through your public website, mobile site, or other digital experiences to learn about your company offerings, download documents, or make a purchase.</p> <p>They can visit <i>public</i> sites, but can't access <i>secure</i> sites. They can also access content via public links and interact based on the role assigned to the public link.</p> <p>Anonymous users can't access any Oracle Content Management interfaces (web client, desktop client, mobile apps).</p>	<ul style="list-style-type: none"> Anonymous users don't need a user account or any application roles.
<p>Visitor Visitors probably don't work for your company, but they exist in your Oracle Cloud identity domain or your directory. Like anonymous users, they are consumers engaging with your website, mobile site, or other digital experiences to learn about your company offerings, download documents, or make a purchase, but they can also interact with specified secure sites and sign in to services that your company provides.</p> <p>They can visit public sites, and, unlike anonymous users, they can visit any secure sites to which they've been given access. They can also access content via public links and interact based on the role assigned to the public link.</p> <p>Visitors can share and collaborate on files exposed via components on a site they have access to, but they don't have access to any Oracle Content Management interfaces (web client, desktop client, mobile apps), and you can't share folders or conversations with them.</p>	<ul style="list-style-type: none"> Sites Visitor

Organization Role	Application Roles Needed
<p>External User External users may be people outside of your organization that can collaborate on objects to which they're given access, but they can't be assigned the manager role. This safely limits their ability to create and remove content, similar to how visitors can sign in and use specified secure sites. This allows you to work with outside contributors such as translators and partners.</p> <p>External users have limited access to the Oracle Content Management web client, but they can't use the desktop client or mobile apps.</p>	<ul style="list-style-type: none"> • Standard External User
<p>Employee Employees obviously work for your company and exist in your Oracle Cloud identity domain or your directory. They share documents with colleagues and view documents shared with them. They collaborate through shared conversations. They can create team sites or partner sites from prebuilt standard templates.</p> <p>Employees can visit public and secure sites to which they have access. They can collaborate on all content types as members and via public links. They can access any Oracle Content Management interfaces (web client, desktop client, mobile apps).</p>	<ul style="list-style-type: none"> • Standard User
<p>Content Contributor Content contributors work for your company and exist in your Oracle Cloud identity domain or your directory. They write articles that will be published to your sites, possibly about one of your products or a certain area of your business. These articles (in the form of content items) include images, videos, and other digital assets that make it easy for your customers to understand product features and specs. Content contributors also share and collaborate like an employee. A content contributor is a user with a contributor role within at least one repository.</p>	<ul style="list-style-type: none"> • Enterprise User
<p>Content Administrator/Content Translator Content administrators are responsible for the quality of content related to a product. They review submitted content, ensuring it's valid and accurate, and then publish this content. They can also create new content types and taxonomies as needed for your sites.</p> <p>Content translators also administer content. They submit content to the translation vendor, proofread returned content, and sometimes translate articles manually.</p> <p>Content administrators also share and collaborate like an employee.</p>	<ul style="list-style-type: none"> • Content Administrator • Enterprise User

Organization Role	Application Roles Needed
<p>Repository Administrator Repository administrators organize content authoring and publishing, which requires setting up asset repositories, managing content editors' roles and permissions, viewing content metrics, and configuring content workflows, publishing channels, and localization policies that your company uses to deliver experiences. They interact with back-end developers to define data or content integration requirements. They also share and collaborate like an employee. A repository administrator is a user with a Manager role within at least one repository.</p>	<ul style="list-style-type: none"> • Repository Administrator • Enterprise User
<p>Site Administrator You can limit site, template, and component creation to only site administrators. Site administrators create and manage <i>standard</i> and <i>enterprise</i> sites. They might ask the system administrator to install the default site templates; ask a developer to create custom components, themes, or templates for new sites; or ask a content architect to create new content types for content items that will be used on sites. They also share and collaborate like an employee.</p>	<ul style="list-style-type: none"> • Site Administrator • Enterprise User
<p>Developer Developers develop and configure custom components, corporate themes, and <i>standard</i> templates that colleagues can use for creating team sites or partner sites. They configure integrations between Oracle Content Management and other services. They also share and collaborate like an employee. A developer with the Enterprise User role can also create <i>enterprise</i> templates.</p>	<ul style="list-style-type: none"> • Developer • Enterprise User
<p>Content Capture Administrator Content Capture administrators design and customize content capture workflows, or <i>procedures</i>, which are used to process physical and electronic documents in bulk for various business scenarios. Procedure managers are typically assigned both the manager and application roles, so they can configure procedures and test them in the client.</p>	<ul style="list-style-type: none"> • Capture Administrator • Capture Client User • Standard User
<p>Content Capture Client User Content Capture client users scan or import documents into Oracle Content Management.</p>	<ul style="list-style-type: none"> • Capture Client User
<p>Content Applications Administrator Content applications administrators manage content apps to discover and deploy web applications that run in the context of Oracle Content Management (using it as the content management system).</p>	<ul style="list-style-type: none"> • Service Administrator • Enterprise User <p>Depending on the type of app you're working with, you may also need to have the content administrator and/or site administrator roles; for example, to create repositories, publishing channels, and such.</p>

Organization Role	Application Roles Needed
<p>Service Administrator Service administrators configure and manage your Oracle Content Management service. They can integrate Oracle Content Management with other business services and access operational analytics to monitor key usage metrics for the service.</p>	<ul style="list-style-type: none"> • Service Administrator • Standard or Enterprise User


There are additional users involved in running Oracle Content Management, such as the Integration User, but that is an internal user, not an actual person. You'll also have a cloud account administrator, but this user is automatically created when you sign up for Oracle Cloud. See [Application Roles in an Oracle Content Management Instance with a Non-Metered Subscription](#).

Create Groups with a Traditional Cloud Account

As a best practice, you should create groups based on the roles in your organization, then assign the appropriate application roles to those groups to give them access to the features they need. Then add users to those groups to automatically assign users the appropriate application roles.

For a list of typical organization roles and the application roles they need, see [Typical Organization Roles](#).

To create a group:


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 Classic Console, click , then, under Account Management, click **Users**. You might need to use the scroll bars on the right to scroll down to see the menu option.
3. Click the **Groups** tab.
4. Click **Add**.
5. Provide a name and description to your group, and then click **Add**.

Next, [assign roles to your groups](#).

Assign Roles to Groups with a Traditional Cloud Account

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

To assign roles to groups:

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 Classic Console, click , then, under Account Management, click **Users**. You might need to use the scroll bars on the right to scroll down to see the menu option.
3. Click the **Groups** tab.

4. Open the group you want to assign roles to.
5. Click the **Roles** tab.
6. Find your service.
7. Click the roles box, and select the roles you want to assign to the group.

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 in an Oracle Content Management Instance with a Non-Metered Subscription](#).


Next, [add users](#).

Add Users with a Traditional Cloud Account

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 adding users. See [Enable Single Sign-On \(SSO\)](#).

To add users:


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 Classic Console, click , then, under Account Management, click **Users**. You might need to use the scroll bars on the right to scroll down to see the menu option.
3. To create users individually or in a batch, and to assign application roles, see Adding Users to a Traditional Cloud Account in *Getting Started with Oracle Cloud*. 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.

Next, [assign your users to groups to give them the appropriate roles and permissions](#).

Assign Users to Groups with a Traditional Cloud Account

Assign users to groups to automatically give them the appropriate roles and permissions.

To assign users to groups:

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 Classic Console, click , then, under Account Management, click **Users**. You might need to use the scroll bars on the right to scroll down to see the menu option.
3. Click the **Groups** tab.
4. Open the group you want to assign users to.
5. Click the **Users** tab.
6. Click **Add To Group**
7. Select the users you want to assign to the group, and then click **Add**.

Now that you've deployed Oracle Content Management, you might want to [enable additional features](#). Then you need to perform other tasks to [roll out the service](#).

Manage Users, Groups, and Access with a Traditional Cloud Account

Securing your system is an ongoing process as people join or leave your company and as needs change as your system grows.

- [Enable Single Sign-On \(SSO\)](#)
- [Manage Users with a Traditional Cloud Account](#)
- [Manage Groups \(Traditional Cloud Account\)](#)
- [Set the Default Role for New Folder Members](#)
- [Synchronize User Profile Data](#)
- [Display Conversation Membership Messages for Users](#)
- [Override Storage Quota for a User](#)
- [Transfer File Ownership](#)
- [Revoke Access to Linked Devices](#)

Enable Single Sign-On (SSO)

If you use Federated Single Sign-On (SSO) for your Oracle Content Management environment, you can enable it to customize sign-in procedures. When Single Sign-On (SSO) is enabled, users can sign in to one instance using corporate security credentials and access another instance in the same domain without signing in again. For example, perhaps you are an administrator for your company which has two Oracle Cloud services and you must provision these services to your company's organization, roles, and users. Your company may also have on-premise applications and cloud services from other vendors. It's important that communication between these services and applications is done in a secure fashion. With SSO, users can sign in to all of them using the same set of credentials that are managed by using your identity domain system.

OAuth provides secure access to all services in Oracle Cloud. It provides an access token for communication between services. The token is valid for a limited time and contains the security credentials for a sign-in session. It identifies the user and the user's groups.

Overview of SSO Configuration

Oracle Cloud uses the SAML 2.0 standard to enable secure cross-domain communication between Oracle Cloud and other SAML-enabled sites located on-premise or in a different cloud. The administrator must configure SAML 2.0 SSO between Oracle Cloud and the identity provider. When SSO is enabled, the identity provider performs authentication for Oracle Cloud.



Perform the following steps to configure SSO:

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. Configure SSO. See [Managing Oracle Single Sign-On in *Administering Oracle Cloud Identity Management*](#).

Manage Users with a Traditional Cloud Account

Before using your system, you need to add users and probably enable single sign-on (SSO). As you continue to use your system, you'll need to add and remove users or change some of their settings. For example, if someone changes departments, you might need to change their role, or if someone leaves your organization, you need to remove them from the system.

To manage users:

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 Classic Console, click , then, under Account Management, click **Users**. You might need to use the scroll bars on the right to scroll down to see the menu option.
3. Perform any of the following tasks:
 - To create a user, click **Add**.
 - To edit a user, open it.
 - To remove a user, next to the user you want to remove, click , and then select **Remove**.

See Add Users to a Traditional Cloud Account in *Getting Started with Oracle Cloud*.

Manage Groups (Traditional Cloud Account)


As a best practice, you should create groups for your organization roles and assign the appropriate application roles to those groups. Then you can add users to those groups to automatically assign them the appropriate application roles.


- [Manage Groups with a Traditional Cloud Account](#)
- [Assign Roles to Groups with a Traditional Cloud Account](#)
- [Assign Users to Groups with a Traditional Cloud Account](#)

Manage Groups with a Traditional Cloud Account

As you use your system, you'll want to add, edit, or remove groups.

To manage groups:

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 Classic Console, click , then, under Account Management, click **Users**. You might need to use the scroll bars on the right to scroll down to see the menu option.
3. Click the **Groups** tab.
4. Perform any of the following tasks:
 - To create a group, click **Add**.
 - To edit a group, open it.


- To remove a group, next to the group you want to remove, click , and then select **Remove**.

See About User Groups in *Managing and Monitoring Oracle Cloud*.

Assign Roles to Groups with a Traditional Cloud Account

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


To assign roles to groups:

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 Classic Console, click , then, under Account Management, click **Users**. You might need to use the scroll bars on the right to scroll down to see the menu option.
3. Click the **Groups** tab.
4. Open the group you want to assign roles to.
5. Click the **Roles** tab.
6. Find your service.
7. Click the roles box, and select the roles you want to assign to the group.

Assign Users to Groups with a Traditional Cloud Account

Assign users to groups to automatically give them the appropriate roles and permissions.

To assign users to groups:

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 Classic Console, click , then, under Account Management, click **Users**. You might need to use the scroll bars on the right to scroll down to see the menu option.
3. Click the **Groups** tab.
4. Open the group you want to assign users to.
5. Click the **Users** tab.
6. Click **Add To Group**
7. Select the users you want to assign to the group, and then click **Add**.

Set the Default Role for New Folder Members

Users in your organization can share folders with other users and assign them a resource role within the shared folder. The following roles are available:

- **Viewer**: Viewers can look at files and folders, but can't change things.
- **Downloader**: Downloaders can also download files and save them to their own computers.

- **Contributor:** Contributors can also modify files, update files, upload new files, and delete files.
- **Manager:** Managers have all the privileges of the other roles and can add or remove other people as members.

To change the default resource role:

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** menu, click **Users**.
3. Under **Members**, in the **Default role for new members added to folders** list, select the resource role users will be assigned by default when added to a folder.

Synchronize User Profile Data

You can replace a user's existing profile information with the information from your identity store:

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** menu, click **Users**.
3. Search for the user whose profile data you want to sync, click **Edit** next to the user's name, and click **Sync Profile Now** on the user details page.

Display Conversation Membership Messages for Users

Configure whether to show the user conversation membership messages (when a person is added to a conversation and who added them) by default. A user can change this display setting for any stand-alone conversation.

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** menu, click **Users**.
3. On the Search tab find the user whose default you want to set. Enter part of the user name, display name, or email address in the text box and click **Search**.
4. Click **Edit** next to the user's name.
5. Select the **Show Conversation Membership Messages by Default** check box and click **Save**.

Override Storage Quota for a User

You can [set a default quota](#) for the amount of storage space that a user is allocated. If you need to override the default for a particular user you can do so using the following steps.

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** menu, click **Users**.
3. Search for the user whose settings you want to override and click **Edit** next to the user's name.
4. In the **User Quota** box, enter the quota amount in gigabytes, and then click **Save**.

You can see how much storage the user has used next to **Storage consumed**.

Transfer File Ownership

When people leave your organization or change roles, you might want to assign their files and folders to someone else and add their storage quota back to the total quota you have available for assignments. You can assign a person's entire library of content to someone else. The content appears as a folder in the new user's root folder. All of the sharing actions, such as members and public links, remain intact.

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** menu, click **Users**.
3. Find the user whose files you want to transfer using one of the following methods:
 - To find an active user, on the **Search** tab enter part of the user name, display name, or email address in the text box and click **Search**. Open the user properties by clicking the user name or clicking **Edit** next to the user.
 - To find a deprovisioned user, click the **Deprovisioned Users** tab. You see a list of all users who have been removed from your organization's system, sorted by name. This list is refreshed on a regular basis, but you can also update it manually by clicking **Sync Profile Data**.

To download a CSV file of all deleted users, click **Export Deprovisioned Users**.

4. Click **Transfer Ownership**. For active users, the button is at the bottom of the properties. For deprovisioned users, click the button next to the user you want.
5. Enter part of the user name, display name, or email address of the person who will receive the content and click **Search**.
6. Select the user you want to transfer the content to. A message shows that the content will increase the recipient's quota by the amount of content being transferred. It also shows you how much storage will be released back into the total quota you have available.
7. Click **Transfer**. The content is transferred and the list shows that the deprovisioned account is gone.

Alternatively, for deprovisioned users, you can delete the content. On the **Deprovisioned Users** tab, next to the user whose content you want to delete, click **Delete Content**.

Users can also transfer ownership of their own folders.

Revoke Access to Linked Devices

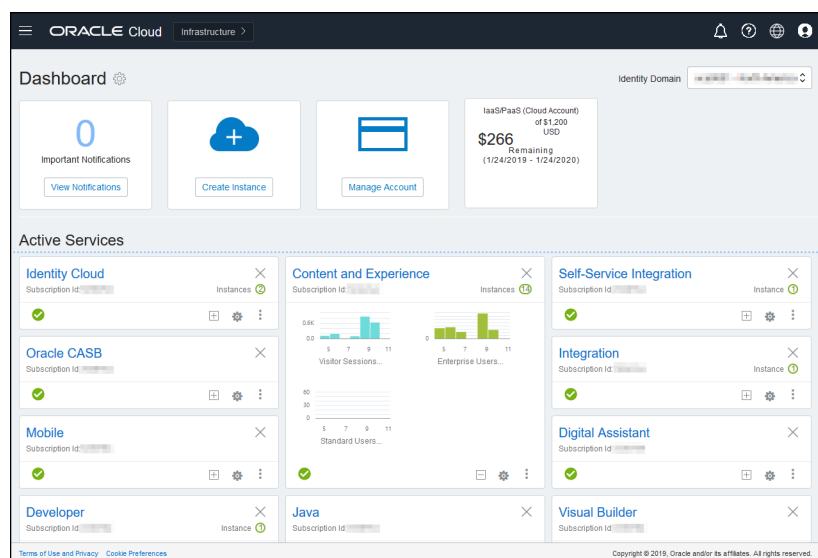
Users can revoke access to one of their linked devices if they change devices or lose one, but there might be cases where you, as an administrator, need to perform this action. When you revoke access to a linked device, the user's sign-in session is ended. If you or anyone else tries to access Oracle Content Management from the device, the account is signed out and all local content stored on the device for that account is deleted.

Revoking access for the device affects only one account, so if the person has multiple user accounts, you need to revoke access separately for each user account to block all access to Oracle Content Management and delete all local content stored on the device.

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** menu, click **Users**.
3. Search for the user whose device access you want to revoke and click **Edit** next to the user's name.
4. Under **Linked Devices**, click **Revoke** next to the appropriate device.

Manage and Monitor Oracle Content Management with a Non-Metered Subscription

If you have a non-metered subscription with an Oracle Content Management entitlement, you manage and monitor your service through the Infrastructure Classic Console.







To open the Infrastructure Classic Console, sign in to [Oracle Cloud](#) as the cloud account administrator. You can find your account name and login information in your welcome email.

Expand the Content and Experience panel to see the following metrics:

Metric	Description
Visitor Sessions	Displays the number of daily visitor sessions allocated to this service instance. This metric appears only if you've purchased daily visitor sessions. To view additional usage metrics, click Visitor Sessions . See Understand Visitor Sessions .
Enterprise Users	Displays the number of enterprise users registered on this service instance. This metric appears only if you've purchased enterprise users. To view additional usage metrics, click Enterprise Users .


Metric	Description
Standard Users	Displays the number of standard users registered on this service instance. To view additional usage metrics, click Standard Users .

To see details about your service, in the Content and Experience panel, click , then select one of the following actions:

- **View Details:** You see the following tabs:
 - **Overview:** Displays information on your service and any service instances. From this page you can create a new service instance or change the settings for an existing instance.
 - **Billing Metrics:** Displays detailed usage information about your service.
 - **Billing Alerts:** Configure rules to limit usage and alert administrators when usage exceeds the configured limits.
 - **Business Metrics:** Displays the usage data collected for each service instance. You must select an instance from the list below the graph to view individual metrics. You can also create alert rules to monitor the resource usage from this page.
 - **Documents:** Download reports pertaining to your subscriptions. Different categories of reports, such as usage metrics, billing, or incidents, can be downloaded if they are available. You can download daily, weekly, monthly, or yearly reports as required. Reports are available in PDF, MS Word, or Open XML.
- **Open Service Console:** View a list of all your service instances. From the list of instances you can perform the following actions:
 - You can perform some management tasks from the list of instances. Next to the instance you want to manage, click . You can access the Oracle Content Management web client for the instance, add tags, or delete the instance.
 - To view general information about an instance, click its name. You see information such as storage OCIDs, version, and account name. To view additional information, click .
 - To manage an instance, click its name, then click . You can access the Oracle Content Management web client for the instance, add an association, update instance credentials, add tags, or view activity.
- **View Account Usage Details:** You see the following tabs:
 - **Usage:** Displays the aggregated usage charges for individual services along with resource utilization and overages, if any.
 - **Account Management:** Displays your subscription details.
 - **Activate:** Activate and complete set up for pending orders.
 - **My Admin Accounts:** View admin login credentials, manage passwords, and access your service consoles for all your Oracle Cloud admin accounts in one place.

View Billing Metrics

The Billing Metrics page in the Infrastructure Classic Console displays detailed usage information about your service.

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 dashboard, next to your service, click , and select **View Details**.
3. Click **Billing Metrics**. Use the metrics to better understand how much your service is being used and whether you need to change storage allocations. Which metrics you see depend on the service subscription that you have.

Expand the Content and Experience panel to see the following metrics:

Metric	Description
Visitor Sessions	Displays the number of daily visitor sessions allocated to this service instance. This metric appears only if you've purchased daily visitor sessions. To view additional usage metrics, click Visitor Sessions . See Understand Visitor Sessions .
Enterprise Users	Displays the number of enterprise users registered on this service instance. This metric appears only if you've purchased enterprise users. To view additional usage metrics, click Enterprise Users .
Standard Users	Displays the number of standard users registered on this service instance. To view additional usage metrics, click Standard Users .


View Business Metrics



Note:

This page is currently unavailable if you have a Universal Credits subscription.

The **Business Metrics** page in the Infrastructure Classic Console displays detailed information about your service. Use the metrics to better understand how much your service is being used and whether you need to change storage allocations.

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 dashboard, next to your service, click , and select **View Details**.
3. Click **Business Metrics**. The **Business Metrics** page includes two sections: **Business Metrics** and **Latest Business Metrics**.

Business Metrics

Under **Business Metrics**, select the instance for which you want to see metrics, and select the metric you want to see.

Metric	Description
Total Documents Uploaded (last day)	Displays the number of documents uploaded in the last 24 hour period.
Total Documents Downloaded (last day)	Displays the number of documents download in the last 24 hour period.
Total Documents (All Revisions)	Displays the total number of documents, including all revisions, that are stored in this instance. For example, if you have 100 documents, each with 3 revisions, the Total Documents (All Revisions) value would be 300.
Total Documents (Latest Revisions)	Displays the total number of documents (regardless of revisions) that are stored in this instance. Using the same example as above, if you have 100 documents, each with 3 revisions, the Total Documents (Latest Revisions) value would be 100.
User Requests (last day)	Displays the number of user requests made to Oracle Content Management in the last 24 hour period, typically through the web client. Browsing Oracle Content Management counts as a user request even if the user doesn't download anything.

You can perform the following additional actions:

- To add another metric to the table, click **Add Metric**, then select the instance and metric you want to add.
- To limit the data to a specific period by entering dates in the **FROM** and **TO** boxes.
- To see the data in a table format, click **Show Table**.
- To save a copy of the data as a .csv file, click **Export**.

Latest Business Metrics

Under **Latest Business Metrics**, select the instance for which you want to see metrics.

Metric	Description
Used Sites Interactions	Displays the number of interactions users have had with this instance. An interaction is defined as a unique user visiting the instance through a unique method (Firefox web browser, Chrome web browser, mobile web browser, etc.) in a 24 hour period. This metric applies only if you have an Oracle Documents Cloud subscription.
Allocated Content and Experience Daily Visitor Sessions	Displays the number of daily visitor sessions allocated to this instance. See Understand Visitor Sessions . This metric applies only if you have an Oracle Content Management subscription.

Metric	Description
Used Content and Experience Daily Visitor Sessions	<p>Displays the number of daily visitor sessions used in this instance. See Understand Visitor Sessions.</p> <p>This metric applies only if you have an Oracle Content Management subscription.</p>
Sites Created	<p>Displays the number of sites created in this instance.</p>
Sites Active	<p>Displays the number of sites that are online and served by this instance.</p>
Bandwidth Consumed (MB)	<p>Displays the network bandwidth (in MB) used to serve sites pages.</p>
Allocated Storage (GB)	<p>Displays the amount of storage (in GB) that has been allocated to this instance.</p>
Used Storage (GB)	<p>Displays the amount of storage (in GB) that have been used in this instance.</p>
Provisioned Documents Users	<p>Displays the number of users that have been provisioned in this instance.</p> <p>This metric applies only if you have an Oracle Documents Cloud subscription.</p>
Provisioned Content and Experience Standard Users	<p>Displays the number of <i>standard</i> users that have been provisioned in this instance.</p> <p>This metric applies only if you have an Oracle Content Management subscription.</p>
Provisioned Content and Experience Enterprise Users	<p>Displays the number of <i>enterprise</i> users that have been provisioned in this instance.</p> <p>This metric applies only if you have an Oracle Content Management subscription.</p>
Documents Users in Use	<p>Displays the total days that all users have been signed in to this instance. For example, if you had 110 users that signed in for 2 hours each day, the Purchased Documents Users value for the day would be 9.166; for the month it would be 275.</p> <p>This metric applies only if you have an Oracle Documents Cloud subscription.</p>
Content and Experience Standard Users in Use	<p>Displays the total days that all <i>standard</i> users have been signed in to this instance. For example, if you had 75 standard users that signed in for 5 hours each day, the Purchased Content and Experience Standard Users value for the day would be 15.625; for the month it would be 468.75.</p> <p>This metric applies only if you have an Oracle Content Management subscription.</p>
Content and Experience Enterprise Users in Use	<p>Displays the total days that all <i>enterprise</i> users have been signed in to this instance. For example, if you had 25 enterprise users that signed in for 3 hours each day, the Purchased Content and Experience Enterprise Users value for the day would be 3.125; for the month it would be 93.75.</p> <p>This metric applies only if you have an Oracle Content Management subscription.</p>

Understand Visitor Sessions

A *visitor session* is metric used by Oracle Content Management to track usage during a specified *session window* (one hour for hourly visitor sessions and 24 hours for daily visitor sessions). A visitor session is triggered when a unique unauthenticated user or an authenticated user who has the *site visitor* role accesses the service using a specific channel (for example, via a browser, mobile browser or applink, etc.). Access from multiple channels counts as multiple visitor sessions. For example, if one user in a 24 hour period accesses the same Oracle Content Management instance from a Firefox desktop web browser, a Chrome desktop web browser, and a mobile web browser, that would count as a total of three *daily* visitor sessions.

Unauthenticated users can access certain sites, use public links, and view Oracle Content Management content embedded in apps or websites.

Frequently Asked Questions

If a user accesses multiple pages within the same Oracle Content Management instance, does that count as multiple visitor sessions?

No. Visitor sessions are only counted at the instance (site) level.

When is a visitor session triggered?

A visitor session is initiated by any user (anonymous or authenticated *guest*) who accesses an Oracle Content Management resource such an Oracle Content Management instance, a site created with Oracle Content Management, or via an API (for example, using applinks) at least once during the session window.

How long does a visitor session last?

The duration of an hourly visitor session is one hour; a daily visitor session is 24 hours. It starts the first time the user accesses a specific Oracle Content Management resource via a unique channel. After one hour, subsequent visits by the same user to the same resource triggers another *hourly* visitor session. After 24 hours, subsequent visits by the same user to the same resource triggers another *daily* visitor session.

Will an Oracle Content Management standard or enterprise user be counted in visitor session counts?

No. An authenticated (signed-in) standard or enterprise user that visits an Oracle Content Management resource isn't included in visitor session counts.

Does the visitor session apply to authenticated (signed-in) users visiting an Oracle Content Management resource?

As stated above an authenticated Oracle Content Management standard or enterprise user that visits an Oracle Content Management resource will not be counted in visitor session counts. However, an authenticated user with the *site visitor* role *will* be counted in the visitor session counts.

How often is the visitor session calculated?

The visitor might access the same resource (site, API or applink) multiple times in the visitor session window (one hour for hourly visitor sessions and 24 hours for daily visitor sessions), but will be counted as one/single visit. If the user accesses the same resource again after the visitor session window, it will be counted as new visit.

Does a user visiting a second site count as a second visitor session?

The same user accessing a different resource (such as a different site) will be counted as a separate visitor session visit. For example, the same user accessing two different sites within the session window will be counted as two visits. Essentially the count is per user, per resource, per channel, per visitor session window for a given service instance.

Will visits to a site by bots or crawlers count as visitor sessions?

Repeated visits from bots or crawlers will not be counted as visitor sessions.

Will a user accessing a public download link be counted as visitor session?

A user accessing a public download link to download a document will not be counted as a visitor session. Even if the user is brought to the Oracle Content Management user interface, showing the **Download** button, it won't count as a visitor session.

What if the public download link is accessed via a site created with Oracle Content Management? Will using the link be counted as visitor session?

Visiting the site created with Oracle Content Management triggers a visitor session, so it will count as a visitor session, but not due to using the public download link.

For a browser session, how are the visitor sessions tracked?

The visitor sessions for a browser are tracked by placing a cookie that expires after the session window ends in the browser session.

What happens if a user clears his cookies in his browser or closes an incognito browser session?

If the user clears the cookie (by clearing in browser or closing an incognito window), the next request will be treated as a new user and count as a new visitor session.

What metrics are reported to administrators?

Oracle Content Management Analytics provides the following metrics:

- Break down of visitor session counts on hourly basis
- Aggregation of visitor session counts per month
- Ability to drill down on each day of the month (to get to visitor counts)

What metrics are not currently supported or captured?

- Cookie disabling: Some customers can disable cookie tracking on the browser side as an end user policy. In such cases, Oracle Content Management can't track the visitor based cookies since they are turned off, meaning the count will be lower than the actual number of visitors.
- Tracking visitors via the Oracle Content Management desktop application (the desktop application currently supports counting only named users).
- Tracking visits via the Oracle Content Management mobile applications (the mobile applications currently support counting only named users).

What about opt-out or privacy support with regards to cookie tracking?

Oracle Content Management sites will provide a standard option of letting the user know that a Oracle Content Management resource (site) is using cookies and users can opt-out by disabling the cookie. To support this, the following two items are added consistently across all the Oracle Content Management site resources:

- Opt-out summary message: This message appears on each site to indicate that a cookie is being used for tracking. It includes a link to the privacy page.
- Privacy site page: A standard sites page explaining the usage of a cookie as well the steps to disable the cookie. You can customize this page like any other sites page.

Are AppLinks and API calls tracked as visitor sessions?

AppLinks and REST API calls from third-party applications are included in the visitor sessions counts.

How are AppLink calls tracked as visitor sessions?

The `assignedUser` parameter in the [AppLink](#) request body is used to track the client-side invocations associated to unique users.

Examples

Here are some examples of visitor session counts. Let's assume ACME Corporation has an Oracle Content Management service instance and has created three sites: SiteA, SiteB, and SiteC. Following are examples of how the visitor sessions would be counted during a session window.

Visitor	Resource (Site)	Daily Visitor Session Counts
User1	https://docs-acme.sites.us2.oracecloud/authsite/SiteA	Count increases to 1 (cookie1, user visits a site—SiteA, using Firefox)
User1	https://docs-acme.sites.us2.oracecloud/authsite/SiteB	Count increases to 2 (cookie2, same user but different site—SiteB, using Firefox)
User2	https://mysite.acme.example.com (vanity URL for SiteC)	Count increases to 3 (cookie3, different user, different site—SiteC, using Firefox)
User3	https://mysite.acme.example.com (vanity URL for SiteC)	Count increases to 4 (cookie4, different user, same site—SiteC, using Firefox)
User2	https://mysite.acme.example.com (vanity URL for SiteC)	Count stays at 4 (no change, cookie3, same user—User2, same site—SiteC, using Firefox, same session window)
User2	https://mysite.acme.example.com (vanity URL for SiteC)	Count increases to 5 (cookie5, same user—User2, same site—SiteC, same session window, but using Chrome)

Migrate Oracle Documents Cloud to Oracle Content Management


If you previously used Oracle Documents Cloud Service, you need to migrate to Oracle Content Management after you renew your subscription.

Things to know before you renew your subscription and migrate to Oracle Content Management:

- Each user gets 100 GB storage. You add storage by purchasing more users. To ensure you have enough storage, you should purchase enough users to cover the 500 GB of storage you got with your Oracle Documents Cloud Service, plus any additional storage packs you purchased. For example, if you had 5 storage packs in Oracle Documents Cloud Service, that means you had a total of 1,000 GB storage, so you'd want to purchase 10 standard and/or enterprise users in Oracle Content Management.
- Although users should not lose access during migration, perform the migration during off hours to avoid users running into problems.
- After your renewal order goes through, you might receive an email saying your subscription is in a suspended state. Users will still be able to use the instance while it's suspended. It will remain suspended until you complete the migration steps.

After submitting your renewal order with Oracle Services, you'll receive an email saying that your subscription has been processed. After you receive that email, continue with 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. Click the documents service instance you want to migrate. Each instance must be migrated separately.
3. Click the menu icon:
 - If you *don't* see the **Modify** option, your migration was done automatically, and you can skip the remaining steps.
 - If you *do* see the **Modify** option, continue with the migration steps.
4. Click **Modify**.
The Modify Oracle Content Management page should show Oracle Content Management options now (for example, Additional Number of Standard Users, Additional Number of Enterprise Users). If you don't see these options, your renewal order has not completed. Contact Oracle Customer Support.
5. If your subscription is in a suspended state, you need to flush the system to clear the suspended state. Set all entitlements to "0". Enter 0 for **Additional Number of Standard Users**, **Additional Number of Enterprise Users**, and **Additional Number of Daily Visitor Session Packs**.

 **Note:**

You don't need to perform this step if your subscription isn't in a suspended state.

Wait to receive an email saying that your subscription is no longer suspended before you proceed with the next step.

6. Click the menu icon, and then select **Modify**.
7. Enter the number of standard users, enterprise users, and visitors that will use this instance. See [Task and Feature Comparison by Application Role](#).
All [Oracle Documents Cloud Service users](#) are automatically modified to be standard users. They'll be able to access all content and features they did before the migration.

8. Assign the *enterprise user* role to any users you want to be able to access enterprise user features. See [Assign Roles to Groups with a Traditional Cloud Account](#) and [Assign Users to Groups with a Traditional Cloud Account](#).

For troubleshooting, see [Users can't sign in after migration \(storage overage\)](#).

After migrating, you [manage users, groups, and access](#) and [monitor the service](#) just like any other non-metered Oracle Content Management instance.

Application Roles in Oracle Documents Cloud

There are several predefined application roles for Oracle Documents Cloud which define what users can do. Some functionality is available only to users with specific application roles. People can hold multiple application roles as needed. For example, you might want to designate one person as both an *account administrator* and a *service administrator*. These application roles are assigned by the *identity domain administrator*. See [Assign Roles to Groups with a Traditional Cloud Account](#) and [Assign Users to Groups with a Traditional Cloud Account](#) for information on assigning application roles.

Visitors can view certain sites, use public links, and view Oracle Content Management content embedded in apps or websites. Anonymous users (users that aren't signed in) are counted as visitors. See [Change Site Security in Building Sites with Oracle Content Management](#).

Any users that need to actually *use* Oracle Content Management must be assigned the *service user* role in addition to any other roles they're assigned.

Oracle Documents Cloud *service users* are the same as Oracle Content Management *standard users*. Any feature described in the documentation as associated with *enterprise users* isn't available in Oracle Documents Cloud.

Each user assigned an application role, whether an administrator or an end user, counts as one user. Each user counts against the total users allowed for your service, except for *visitors*. Visitor usage is counted as part of daily visitor sessions. See [Understand Visitor Sessions](#).

Each user, no matter how many application roles they are assigned, counts as only one user.

For information on how to get to the interfaces listed in the table, see [Administrative Interfaces](#).

Application Role (application role name in bold)	Access and Actions	Notes
Account administrator	<p>Account administrators use the My Account application to perform the following actions:</p> <ul style="list-style-type: none"> • Activate and create identity domains. • Activate a service. • Monitor and manage services across all identity domains and data centers. • Create identity domain administrators and other account administrators. <p>See Manage Your Oracle Cloud Service in <i>Getting Started with Oracle Cloud</i>.</p>	<p>Account administrators are set up when the account is created. They use their Oracle account to sign in to Oracle Cloud. If you need account administrator access and don't have it, contact your primary account administrator..</p> <p>If you want account administrators to use Oracle Content Management and modify the service configuration, they must also be assigned the <i>service user</i> role.</p>
Identity domain administrator (Identity Domain Administrator)	<p>From the Infrastructure Classic Console:</p> <ul style="list-style-type: none"> • Create and manage user accounts. • Assign and manage application roles, including creating custom application roles. 	<p>Assigned at the domain level. Works across multiple services. Identity domain administrators perform the same functions that a service administrator can, plus they handle administrative duties related to users.</p> <p>There is only one service per identity domain for Oracle Content Management. One administrator performs the duties of the <i>service administrator</i> and the <i>identity domain administrator</i>.</p>
Entitlement administrator The format of the role name is <i>service-name_SE service name Based Entitlement Administrator</i> , for example, documents_SE Documents Service Based Entitlement Administrator .	<p>From the Infrastructure Classic Console:</p> <ul style="list-style-type: none"> • Create, manage, and view details of service instances. Applies when you're subscribed to an entitlement to create multiple instances of Oracle Content Management. • Monitor status of service instances, and export instance metrics data. <p>See Create and Activate an Oracle Cloud Account.</p>	<p>Assigned at the service level.</p>

Application Role (application role name in bold)	Access and Actions	Notes
Service administrator (Oracle Documents Cloud Administrator)	<p>From the Infrastructure Classic Console:</p> <ul style="list-style-type: none"> • Assign application roles. • Change user passwords and challenge questions. • Configure, monitor, and manage service instances. <p>From Oracle Content Management Administration: System interface:</p> <ul style="list-style-type: none"> • Configure general settings such as branding, enabling notifications, and default time zone and language. • Configure user settings such as syncing profile data, setting the default role for new members added to folders, and transferring content ownership. • Configure documents settings such as storage quotas, enabling public links, and setting restrictions on the size and types of files that can be uploaded. • Configure custom properties (must also have Enterprise User role). • Configure sites settings such as whether sites can be created and installing the default site templates. <p>From the Oracle Content Management Administration: Integrations interface:</p> <ul style="list-style-type: none"> • Integrate other business applications as described in <i>Integrating and Extending Oracle Content Management</i>. <p>From the Oracle Content Management Analytics interface:</p> <ul style="list-style-type: none"> • View service usage statistics and content metrics to help you analyze system needs or issues. • View reports. 	Service administrators must also be assigned the <i>service user</i> role to be able to use Oracle Content Management.

Application Role (application role name in bold)	Access and Actions	Notes
Site administrator (Oracle Content and Experience Site Administrator)	From Oracle Content Management Sites page: <ul style="list-style-type: none"> • Create sites. From Oracle Content Management Developer page: <ul style="list-style-type: none"> • Create templates, components, and themes. See Configure Sites Settings	This role applies if your service administrator configured Oracle Content Management to allow only site administrators to create sites, templates, or components. Site administrators must also be assigned the <i>service user</i> role to be able to use Oracle Content Management.
Developer (CECDeveloperUser)	From Oracle Content Management Sites page: <ul style="list-style-type: none"> • Create, edit, and publish sites as long as this feature hasn't been limited to <i>site administrators</i>. From Oracle Content Management Developer page: <ul style="list-style-type: none"> • Create templates, components, and themes as long as these features haven't been limited to <i>site administrators</i>. 	Developers must also be assigned the <i>service user</i> role to be able to use Oracle Content Management.
Service user (Oracle Documents Cloud Service User)	From Oracle Content Management, <i>service users</i> have access to: <ul style="list-style-type: none"> • Manage content (view, upload, and edit documents). • Share content and sites with others. • Use conversations to collaborate (discuss topics, direct message someone, assign flags to someone, add annotations to documents). • Follow people. • Create, edit, and publish sites as long as this feature hasn't been limited to <i>site administrators</i>. • Create templates, components, and themes as long as these features haven't been limited to <i>site administrators</i>. • Manage and view custom properties and edit values. 	For use with an Oracle Documents Cloud Service subscription. Any users that need to actually use Oracle Content Management must be assigned the <i>service user</i> role. This role isn't assigned by default to any user.

Application Role (application role name in bold)	Access and Actions	Notes
Visitor (Oracle Content and Experience Visitor)	Access sites restricted to <i>visitors</i> .	This role applies if a site is set to be accessed only by visitors. If that restriction is enabled, only users with this role will be able to access the site. See <i>Change Site Security in Building Sites with Oracle Content Management</i> . Visitors don't require a license. Visitor usage is counted as part of daily visitor sessions. See Understand Visitor Sessions .
External user (CECEExternalUser)	Reserved for future use.	Do not use this role. Users assigned this role can't use the Oracle Content Management user interface.

Troubleshoot Oracle Documents Cloud

This section helps you troubleshoot Oracle Documents Cloud.

- [I need to downsize my instance](#)
- [Users can't sign in after migration \(storage overage\)](#)

I need to downsize my instance



Note:

You can downsize only if you are an Oracle Documents Cloud Service customer. If you purchased or migrated to Oracle Content Management, you can't use this procedure; you must contact Oracle Support.

If you are using fewer users or storage in an instance than you thought you would, you can downsize it.

1. If you are reducing the number of users and need to delete existing users, reassign their content and remove the users. See [Manage Users with a Traditional Cloud Account](#) and [Transfer File Ownership](#).
2. Modify the service:
 - 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. Click the service instance you want to downsize.
If you are downsizing more than one instance, each instance must be downsized separately.
 - c. Click the menu icon, and then select **Modify**.
 - d. Downsize the number of users or storage packs by entering negative numbers. For example, if you want to decrease your users by 10, you would enter -10 .

Users can't sign in after migration (storage overage)

If some users can't sign in after you migrated from Oracle Documents Cloud Service to Oracle Content Management or if you received an email saying that there is a storage breach, it's because not enough users were provisioned to accommodate the storage needs for the instance. No data will be lost. You just need to provision more users.

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. Click the service instance you need to add more storage to.
3. Click the menu icon, and then select **Modify**.
The Modify Oracle Content Management page should show Oracle Content Management options now (for example, Additional Number of Standard Users, Additional Number of Enterprise Users). If you don't see these options, your renewal order has not completed. Contact Oracle Customer Support.
4. On the Modify Oracle Content Management page, update the number of users to accommodate the storage needs for the instance. Each user gets 100 GB storage. So, if the email said you were exceeding your storage by 500 GB, you'd need to add 5 users.