Oracle® Cloud

Administering Oracle Content and Experience Cloud

F13457-03
March 2019

Oracle Cloud Administering Oracle Content and Experience Cloud,

F13457-03

Copyright © 2017, 2019, Oracle and/or its affiliates. All rights reserved.

Primary Author: Bonnie Vaughan

Contributors: Sarah Bernau, Bob Lies, Bruce Silver, Ron van de Crommert, David Jones, Keith MacDonald, Mark Paterson, Andy Peet, Indira Smith, Sherri Ahern

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 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 installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. 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 and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon 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, Opteron, the AMD logo, and the AMD Opteron 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 ix
Documentation Accessibility ix
Related Resources ix
Conventions x

1 Get Started

What's New 1-1
Your Role as Administrator 1-2
Roles 1-3
- Typical Organization Roles 1-3
- User Roles 1-6
- Task and Feature Comparison by User Role 1-14
- Resource Roles (Permissions) 1-16

Administrative Interfaces 1-24
Administrative Tasks 1-26
Security 1-28
Standard Edition vs. Enterprise Edition 1-33
Understand Active Users per Hour 1-34

2 Roll Out the Service

Understand the Roll-Out Process 2-1
Provide Sign In and Get Started Information to Users 2-2
Deploy the Desktop App 2-2
- Run the Executable Installer from the Command Line 2-2
- Run the MSI Installer 2-5
- Deploy the MSI Installer Through Active Directory's Group Policy 2-6
- Set Installation Defaults 2-7

3 Deploy Oracle Content and Experience Cloud

Subscribe to Oracle Cloud 3-1
Create Your Service Instance 3-2
- Create an Oracle Content and Experience Cloud Instance with a Universal Credits Subscription 3-3
- Create an Oracle Content and Experience Cloud-Classic Instance with a Universal Credits Subscription 3-8
- Create an Oracle Content and Experience Cloud Instance with a Non-Metered Subscription 3-11

Create Groups for Your Organization 3-12
- Create Groups with Oracle Identity Cloud Service 3-13
- Create Groups with a Traditional Cloud Account 3-13

Assign Roles to Groups 3-14
- Assign Roles to Groups with Oracle Identity Cloud Service 3-14
- Assign Roles to Groups with a Traditional Cloud Account 3-15

Add Users 3-16
- Add Users with Oracle Identity Cloud Service 3-16
- Add Users with a Traditional Cloud Account 3-17

Assign Users to Groups 3-17
- Assign Users to Groups with Oracle Identity Cloud Service 3-17
- Assign Users to Groups with a Traditional Cloud Account 3-18

Migrate from Traditional Digital Assets to New Digital Assets 3-19

4 Configure Service Settings

Configure General Settings 4-1
- Apply Custom Branding and URLs 4-1
- Enable or Disable Email Notifications 4-2
- Set the Default Time Zone and Language 4-2

Configure Security Settings 4-3
- Understand Cross-Origin Resource Sharing (CORS) 4-3
- Enable Cross-Origin Resource Sharing (CORS) 4-4
- Embed Content in Other Domains 4-4

Configure User Settings 4-5
- Set the Default Resource Role for New Folder Members 4-6
- Synchronize User Profile Data 4-6
- Display Conversation Membership Messages for Users 4-6
- Override Storage Quota for a User 4-7
- Change Temporary Quota for a User 4-7
- Transfer File Ownership 4-7
- Revoke Access to Linked Devices 4-8

Configure Documents Settings 4-8
Set User Quotas and Manage Storage Space 4-9
Set Default Link Behavior 4-9
Restrict File Types and Sizes 4-10
Set Virus Scanning Options 4-10
Configure Tags and Metadata 4-11
Manage Hashtags 4-11
Configure Custom Properties (Metadata) 4-11
Configure Sites and Assets Settings 4-12

5 Integrate the Service

Understand Integrations 5-2
Use the REST APIs, Sites SDK, and Content Delivery SDK 5-3
Understand Cross-Origin Resource Sharing (CORS) 5-4
Enable Cross-Origin Resource Sharing (CORS) 5-5
Configure Proxy Service Settings 5-6
Debug Proxy Service Endpoints 5-8
Embed the Web Interface 5-9
Manage Custom Applications 5-10
Embed Content in Other Domains 5-11
Configure Sites Settings 5-11
Map a Site URL 5-13
Integrate with Oracle Process Cloud Service 5-14
Integrate with Oracle Eloqua Cloud Service 5-16
Integrate with Oracle Visual Builder Cloud Service 5-19
Integrate with Oracle Policy Automation 5-20
Integrate with Oracle Cobrowse Cloud Service 5-21
Configure Content Connectors to Third-Party Content Repositories 5-21
Enable a Connector 5-22
Provide Configuration Parameter Values for a Connector 5-23
Disable a Connector 5-23
Delete a Connector 5-24
Configure a Google Drive Connector 5-24
Configure a Dropbox Connector 5-26
Configure a OneDrive Connector 5-28
Create and Configure a Custom Connector 5-30
Configure WebCenter Content and OCE for the WCC Connector 5-32
Set Up a Security Policy on WebCenter Content Server 5-32
Sign in to Enterprise Manager 5-33
Open the Oracle UCM Native Web Services 5-33

Open the Web Services Application 5-34
Use the Web Service Endpoint to View and Change Policies 5-34
Detach and Attach Security Policies 5-34
Validate the Security Policy 5-36
Confirm That the Security Policy Is Attached Correctly 5-37
Verify That the wsdl Loads Successfully 5-37
Import the Trusted Certificate from WebCenter Content Server to Content and Experience Cloud 5-37
Configure and Enable the WCC Connector 5-41

6 Manage Users, Groups, and Access

Enable Single Sign-On (SSO) 6-1
Manage Users 6-2
Manage Users with Oracle Identity Cloud Service 6-3
Manage Users with a Traditional Cloud Account 6-3
Manage Groups 6-4
Create Group Standards for Your Organization 6-4
Manage Groups with Oracle Identity Cloud Service 6-6
Manage Groups with a Traditional Cloud Account 6-7
Assign Roles to Groups with Oracle Identity Cloud Service 6-7
Assign Roles to Groups with a Traditional Cloud Account 6-8
Assign Users to Groups with Oracle Identity Cloud Service 6-9
Assign Users to Groups with a Traditional Cloud Account 6-9
Set the Default Role for New Folder Members 6-10
Synchronize User Profile Data 6-10
Display Conversation Membership Messages for Users 6-11
Override Storage Quota for a User 6-11
Transfer File Ownership 6-11
Revoke Access to Linked Devices 6-12

7 Monitor the Service

Monitor Service Activity 7-1
Add Web Analytics Tracking Snippets to Sites and Pages 7-4
Understand Visitor Sessions 7-5
View Billing Metrics 7-8
View Business Metrics 7-10
Report Issues 7-13

8 Analyze Service Usage

About Analytics 8-1
About the Charts, Graphs, and Downloadable Report Files 8-2
View the Dashboard 8-2
View the Sites & Channels Analytics Dashboard 8-3
Content Operations 8-4
- Content Operations: Repositories 8-5
- Content Operations: Collections 8-5
- Content Operations: Channels 8-6

View General Statistics 8-7
- General Statistics: Users 8-8
- General Statistics: Documents 8-8
- General Statistics: Shared Links 8-9
- General Statistics: Conversations 8-9
- General Statistics: One-on-Ones 8-9
- General Statistics: Messages 8-10
- General Statistics: Flags 8-10
- General Statistics: Favorites 8-11
- General Statistics: Likes 8-11
- General Statistics: Hashtags 8-12

View Usage Patterns 8-12
- Usage Patterns: Users 8-13
- Usage Patterns: Documents 8-13
- Usage Patterns: Shared Links 8-14
- Usage Patterns: Conversations 8-14
- Usage Patterns: Messages 8-15
- Usage Patterns: Flags 8-15
- Usage Patterns: Favorites 8-16
- Usage Patterns: Likes 8-17
- Usage Patterns: Hashtags 8-17
- Usage Patterns: One-on-Ones 8-18
- Usage Patterns: Devices 8-18

View Adoption Information 8-18
View Reports and Metrics 8-19
- Run Reports 8-20
- Monitor Service Activity 8-21

A Troubleshoot

I can't access the administration pages A-1
No one can add files to their accounts A-1

I need to change the storage quota for a user A-2
I need to reassign someone's files A-2
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
I need to check the service utilization metrics 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
I need to downsize my instance A-5
Users can't sign in after migration (storage overage) A-5

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 Oracle Documents Cloud

Migrate to Oracle Content and Experience Cloud C-1
Create an Oracle Documents Cloud Service Instance C-3
User Roles in Oracle Documents Cloud C-4

Preface

Administering Oracle Content and Experience Cloud 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 and Experience Cloud 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.

Related Resources

For more information, see these Oracle resources:

- Oracle Public Cloud:

  `http://cloud.oracle.com`
- *Getting Started with Oracle Cloud*
- *Managing Content with Oracle Content and Experience Cloud*
- *Creating Experiences with Oracle Content and Experience Cloud*
- *Developing for Oracle Content and Experience Cloud*
- *Integrating Oracle Content and Experience Cloud*
- *What's New for Oracle Content and Experience Cloud*
- *Known Issues with Oracle Content and Experience Cloud*

Conventions

The following text conventions are used in this document:

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

1
Get Started

Oracle Content and Experience Cloud is an enterprise-level collaboration platform available in Oracle Cloud that connects people and information. It brings everything you and your team need together in one easy-to-use environment: file sync and sharing, conversations, direct communication, notifications, and flags to draw someone's attention. And everything is kept as a running record, so people can easily find out what has happened or get up to speed quickly.

Anything you store or discuss in Oracle Content and Experience Cloud is available wherever you are, using whatever device you have handy: a web browser, your desktop, your mobile device. That means you and your team can work with the tools and applications you're comfortable using without any special training.

Topics

- Your Role as Administrator
- Roles
- Administrative Interfaces
- Administrative Tasks
- Security
- Standard Edition vs. Enterprise Edition
- Understand Active Users per Hour

What's New

Feature	Description	Introduced in
Sites & Channels Analytics Dashboard	You can see usage, utilization, and traffic analytics for your created sites and channels. See View the Sites & Channels Analytics Dashboard.	19.1.5 — March 2019
Temporary storage quota increase	A service administrator can change the temporary quota for a user to allow more storage for uploading large files. See Change Temporary Quota for a User.	19.1.5 — March 2019
Connector tags for assets	A service administrator or developer can assign connector tags to assets pulled from a connector. See Enable a Connector.	19.1.5 — March 2019

Feature	Description	Introduced in
Delete a content connector	A service administrator can use the connector framework to delete a disabled connector. See Delete a Connector.	19.1.5 — March 2019
Custom UI for a content connector	A service administrator or developer can provide additional connector configuration for a custom picker UI. See Create and Configure a Custom Connector.	19.1.5 — March 2019
Site governance	Site governance makes it easy for business users to create sites that conform to company policy and gives site administrators an easy way to control and track sites from a centralized location. See Configure Sites and Assets Settings and Use Site Governance in *Creating Experiences with Oracle Content and Experience Cloud*.	19.1.3 — February 2019
Oracle WebCenter Content asset connector	Browse for assets stored in Oracle WebCenter Content. See Add and Remove Assets in *Creating Experiences with Oracle Content and Experience Cloud* and Configure WebCenter Content and OCE for the WCC Connector.	19.1.3 — February 2019
Custom rendition support	Configure the maximum number of custom renditions per asset through the Administration **Settings Sites and Assets** menu. See Configure Sites and Assets Settings	19.1.3 — February 2019
Custom connector	Create and configure a custom connector to a third-party content repository. See Create and Configure a Custom Connector.	19.1.3 — February 2019
Analytics Content Metrics	Content contributors can view content metrics on the Analytics dashboard for any repositories in which they have the **Contributor** role. If they can contribute to a repository, they can see metrics for all assets, collections, and channels for that repository. See Content Operations.	19.1.3 — February 2019

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 and 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 user roles and administrative interfaces that are involved with performing your administrative tasks:

- Roles
- Administrative Interfaces
- Administrative Tasks
- Security

Roles

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

- **Organization roles** — A person's role within your organization determines what tasks they need to perform and how they use features.

  See Typical Organization Roles.
- **User roles** — User roles control what features a user sees in Oracle Content and Experience Cloud.

  See User Roles and Task and Feature Comparison by User Role.
- **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.

  See Resource Roles (Permissions).

Typical Organization Roles

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

You can create groups for your organization roles and assign the listed user roles to those groups. Then you can add users to those groups to automatically assign them

the appropriate user roles. See Create Groups for Your Organization. For information on assigning user roles, see Add Users.

Organization Role	User Roles Needed
Anonymous User Anonymous users are consumers engaging with your company through your public website, mobile site, or other digital experiences to learn about your company offerings. Anonymous users can interact with your public website, downloading documents or making a purchase.	• Anonymous users don't need a user account or any user roles.
Visitor Visitors are also consumers engaging with your website, mobile site, or other digital experiences to learn about your company offerings. Like anonymous users, visitors can interact with your public website, downloading documents or making a purchase, but they can also interact with specified secure sites and log in to services that your company provides.	• Visitor
Employee Employees 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.	• Standard User
Content Contributor Content contributors 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.	• Enterprise User
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 and create new content types as needed for your sites. Content translators also administer content. They submit content to the translation vendor, proofread returned content, and sometimes translate articles manually. Content administrators also share and collaborate like an employee.	• Content Administrator • Enterprise User

Organization Role	User Roles Needed
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.	• Repository Administrator • Enterprise User
Site Administrator You can limit site, template, and component creation to only site administrators. Site administrators create and manage *standard* and *enterprise* 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.	• Site Administrator • Enterprise User
Standard Developer Standard developers develop custom components, corporate themes, and *standard* templates that colleagues can use for creating team sites or partner sites. They configure integrations between Oracle Content and Experience Cloud and other services. They also share and collaborate like an employee.	• Developer • Standard User
Enterprise Developer Enterprise developers are the same as standard developers, but they can also create *enterprise* templates.	• Developer • Enterprise User
Service Administrator Service administrators configure and manage your Oracle Content and Experience Cloud service. They can integrate Oracle Content and Experience Cloud with other business services and access operational analytics to monitor key usage metrics for the service.	• Service Administrator • Standard or Enterprise User • Identity Domain Administrator • Entitlement Administrator The format of the role name is `service-name_SE service name Based Entitlement Administrator`; for example, **documents_SE Documents Service Based Entitlement Administrator**.

There are additional users involved in running Oracle Content and Experience Cloud, such as the Integration User and the Storage Administrator, 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 User Roles.

User Roles

There are several predefined user roles for Oracle Content and Experience Cloud that define what users can do. Some functionality is available only to users with specific user roles.

People can hold multiple user roles as needed. For example, you might want to designate one person as both an *account administrator* and a *service administrator*. These user roles are assigned by the *identity domain administrator*. See Add Users.

If you have an Oracle Documents Cloud entitlement, see User Roles in Oracle Documents Cloud.

Visitors can view certain sites, use public links, and view Oracle Content and Experience Cloud content embedded in apps or websites. Anonymous users (users that aren't signed in) are counted as visitors. See Change Site Security in *Creating Experiences with Oracle Content and Experience Cloud*.

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 and Experience Cloud must be assigned the *standard user* or *enterprise user* role in addition to any other roles they're assigned.

Each user assigned a user role, whether an administrator or an end user, counts as one user. If you have a universal credits subscription, the user is billed according to the user role they have. If you have a non-metered subscription, each user counts against the total users allowed for your service, except for *visitors*. Visitor usage for non-metered subscriptions is counted as part of daily visitor sessions. See Understand Visitor Sessions.

Each user, no matter how many user roles they are assigned, counts as only one user.

For information on how to access the interfaces listed in the table, see Administrative Interfaces.

User Role (user role name in bold)	Access and Actions	Notes
Cloud account administrator (for universal credits subscriptions) Account administrator (for non-metered subscriptions)	For universal credits subscriptions, Cloud account administrators use the My Services application to perform the following actions: • Monitor and manage services of one or more Cloud accounts. • Create new users. • Provide access to services by assigning roles. • Upgrade or terminate subscriptions. See Overview of Cloud Account Administration Tasks in *Managing and Monitoring Oracle Cloud*. For non-metered subscriptions, account administrator use the My Account application to perform the following actions: • 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. See My Account Administration in *Managing and Monitoring Oracle Cloud*.	Cloud account administrators and account administrators are set up when the account is created. They use their Oracle account to sign in to Oracle Cloud and access My Services or 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 *Getting Started with Oracle Cloud*. If you want account administrators to use Oracle Content and Experience Cloud and modify the service configuration, they must also be assigned the *standard user* or *enterprise user* role.

User Role (user role name in bold)	Access and Actions	Notes
Identity domain administrator (**Identity Domain Administrator**)	From the My Services application: • Create and manage user accounts. • Assign and manage user roles, including creating custom user roles. See Learn About Cloud Account Roles in *Getting Started with Oracle Cloud*.	Assigned at the domain level. Works across multiple services. See Learn About Cloud Account Roles in *Getting Started with Oracle Cloud*. Identity domain administrators perform the same functions that a service administrator can, plus they handle administrative duties related to users. There is only one service per identity domain for Oracle Content and Experience Cloud. One administrator performs the duties of the *service administrator* and the *identity domain administrator*.
Entitlement administrator The format of the role name is *service-name_SE service name Based Entitlement Administrator*; for example, **documents_SE Documents Service Based Entitlement Administrator**.	From the My Services application: • Create, manage, and view details of service instances. Applies when you're subscribed to an entitlement to create multiple instances of Oracle Content and Experience Cloud. • Monitor status of service instances, and export instance metrics data. See Subscribe to Oracle Cloud.	Assigned at the service level. See Oracle Cloud User Roles and Privileges in *Getting Started with Oracle Cloud*.

User Role (user role name in bold)	Access and Actions	Notes
Service administrator • For universal credits subscriptions, **CECServiceAdministrator** • For non-metered subscriptions, **Oracle Content and Experience Cloud Administrator**	From the My Services application: • Assign user roles. • Change user passwords and challenge questions. • Configure, monitor, and manage service instances. From Oracle Content and Experience Cloud **Administration: Settings** interface: • 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 and Experience Cloud Enterprise User** role). • Configure sites settings such as whether sites can be created and installing the default site templates. From Oracle Content and Experience Cloud **Administration: Integrations** interface: • Configure application settings such as those described in Integrate with Oracle Process Cloud Service, Integrate with Oracle Eloqua Cloud Service, and Manage Custom Applications. **Note:** Some of these features are currently unavailable if you have a	Service administrators must also be assigned the *standard user* or *enterprise user* role to be able to use Oracle Content and Experience Cloud.

User Role (user role name in bold)	Access and Actions	Notes
	universal credits subscription. From Oracle Content and Experience Cloud **Analytics** interface: • View service usage statistics and content metrics to help you analyze system needs or issues. • View reports.	
Site administrator • For universal credits subscriptions, **CECSitesAdministrator** • For non-metered subscriptions, **Oracle Content and Experience Cloud Site Administrator**	From Oracle Content and Experience Cloud **Sites** page: • Create sites. From Oracle Content and Experience Cloud **Developer** page: • Create templates, components, and themes. See Configure Sites and Assets Settings.	This role applies if your service administrator configured Oracle Content and Experience Cloud to allow only site administrators to create sites, templates, or components. Site administrators must also be assigned the *standard user* or *enterprise user* role to be able to use Oracle Content and Experience Cloud.

User Role (user role name in bold)	Access and Actions	Notes
Developer (**CECDeveloperUser**)	From Oracle Content and Experience Cloud **Sites** page: • Create, edit, and publish sites as long as this feature hasn't been limited to *site administrators*. From Oracle Content and Experience Cloud **Developer** page: • Create templates, components, and themes as long as these features haven't been limited to *site administrators*. From Oracle Content and Experience Cloud **Administration: Integrations** interface: – Configure application settings such as those described in Integrate with Oracle Process Cloud Service, Integrate with Oracle Eloqua Cloud Service, and Manage Custom Applications. **Note:** Some of these features are currently unavailable if you have a universal credits subscription.	Developers must also be assigned the *standard user* or *enterprise user* role to be able to use Oracle Content and Experience Cloud. Developers with the standard user role can create components, themes, and standard templates. Developers with the enterprise user role can also create layouts and save a site as a standard or enterprise template.
Content administrator • For universal credits subscriptions, **CECContentAdministrator** • For nonmetered subscriptions, **Oracle Content and Experience Cloud Content Administrator**	From Oracle Content and Experience Cloud **Administration: Assets** page: • Create new content types and publish items.	Content administrators must also be assigned the *enterprise user* role to be able to use Oracle Content and Experience Cloud and access assets.

User Role (user role name in bold)	Access and Actions	Notes
Repository administrator (**CECRepositoryAdministrator**)	From Oracle Content and Experience Cloud **Administration: Assets** page: • Create asset repositories. • Create localization policies. • Create publishing channels. From Oracle Content and Experience Cloud **Analytics** interface: • Content Operations to help you analyze system needs or issues.	Repository administrators must also be assigned the *enterprise user* role to be able to use Oracle Content and Experience Cloud and access assets. A repository administrator is a user with a Manager role within at least one repository.
Content Contributor (**Contributor**)	From Oracle Content and Experience Cloud **Analytics** interface: • Content Operations to help you analyze system needs or issues.	
Standard user • For universal credits subscriptions, **CECStandardUser** • For non-metered subscriptions, **Oracle Content and Experience Cloud Standard User**	From Oracle Content and Experience Cloud, *standard users* have access to: • 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 *site administrators*. • View and interact with content items in sites. • Manage and view custom properties and edit values.	Any users that need to actually *use* Oracle Content and Experience Cloud must be assigned the *standard user* or *enterprise user* role. These roles aren't assigned by default to any user. See Task and Feature Comparison by User Role. **WARNING:** If you have an Oracle Content and Experience Cloud Government or Oracle Content and Experience Cloud for SaaS subscription, the *standard user* role isn't supported. If you assign *only* this role to users, they won't be able to access Oracle Content and Experience Cloud. If you're not sure what type of subscription you have, see the Billing Metrics page in My Services. See View Billing Metrics.

User Role (user role name in bold)	Access and Actions	Notes
Enterprise user • For universal credits subscriptions, **CECEnterpriseUser** • For non-metered subscriptions, **Oracle Content and Experience Cloud Enterprise User**	From Oracle Content and Experience Cloud, *enterprise users* have access to all the features that *standard users* have access to, plus: • Create, manage, view, publish, and interact with content items, digital assets, and collections.	For use with an Oracle Content and Experience Cloud subscription. You must have purchased *enterprise users*. Any users that need to actually *use* Oracle Content and Experience Cloud must be assigned the *standard user* or *enterprise user* role. These roles aren't assigned by default to any user. See Task and Feature Comparison by User Role.
Visitor • For universal credits subscriptions, **CECSitesVisitor** • For non-metered subscriptions, **Oracle Content and Experience Cloud Visitor**	Access sites restricted to *visitors*.	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 Change Site Security in *Creating Experiences with Oracle Content and Experience Cloud*. Visitors don't require a license. Visitor usage is counted as part of daily visitor sessions. See Understand Visitor Sessions.
Integration user • For universal credits subscriptions, **CECIntegrationUser** • For non-metered subscriptions, **Social Network Integration User**	Used to impersonate another user while performing operations through the Social REST endpoints of the REST API for Collaboration.	Create a dedicated "Integration User" and assign it the integration user role. **Note:** This role is for an internal user, not an actual person. Users assigned this role can't use the Oracle Content and Experience Cloud user interface. See "Social Resource" in REST API for Collaboration.
Storage administrator (**Storage_Administrator**)	For universal credits subscriptions, this role is used to give Oracle Content and Experience Cloud storage access.	If you have a universal credits subscription, create a dedicated "Storage Administrator" user, then add the dedicated user to the Storage Classic service, and assign the user the **Storage_Administrator** role. **Note:** This role is for an internal user, not an actual person. Users assigned this role can't use the Oracle Content and Experience Cloud user interface.

User Role (user role name in bold)	Access and Actions	Notes
External user (**CECExternalUser**)	Reserved for future use.	Do not use this role. Users assigned this role can't use the Oracle Content and Experience Cloud user interface.

Task and Feature Comparison by User Role

Depending on their user roles, Oracle Content and Experience Cloud users can perform different tasks and access different features.

Visitors can view certain sites, use public links, and view Oracle Content and Experience Cloud content embedded in apps or websites. Anonymous users (users who aren't signed in) are counted as visitors. See Change Site Security in *Creating Experiences with Oracle Content and Experience Cloud*. 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 and Experience Cloud must be assigned the *standard user* or *enterprise user* role. If you purchased enterprise users, you can assign the **Oracle Content and Experience Cloud Enterprise User** role to users to provide them access to more functionality. Your Oracle Content and Experience Cloud instance can have a mixture of standard and enterprise users to fit the needs of your company.

> **Note:**
>
> For more information on roles, see User Roles.

Task	Visitor	Standard User	Enterprise User	Site Admin*	Developer*	Content Admin*	Repository Admin*	Service Admin*
View sites	✓	✓	✓					
Access files and folders through public links	✓	✓	✓					
Manage Your Content (view, upload, and edit documents)	✓ **	✓	✓					
Share Files and Folders	✓ **	✓	✓					

Task	Visitor	Standard User	Enterprise User	Site Admin*	Developer*	Content Admin*	Repository Admin*	Service Admin*
Use Conversations (discuss topics, direct message someone, assign flags to someone, add annotations to documents)	✓ **	✓	✓					
Use Groups and Follow People		✓	✓					
Create and 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.		✓	✓	✓	✓			
View custom properties (metadata) and edit values		✓	✓					
Configure Custom Properties (Metadata) You also need the administrator user role to perform these tasks.		✓	✓					
Work with Digital Assets (images, documents, and videos that you manage independently from your other files and folders; and structured content that is stored separately from its layout so it can be reused in various formats and contexts)			✓					
Create and Share Collections			✓					

Task	Visitor	Standard User	Enterprise User	Site Admin*	Developer*	Content Admin*	Repository Admin*	Service Admin*
Manage content types						✓		
Setting Up Asset Repositories							✓	
Configure service settings								✓
Analyze service usage							✓	✓

* Users with this role must be assigned the *standard user* or *enterprise user* role in addition to the role listed to be able to sign in to Oracle Content and Experience Cloud.

**Visitors can manage and share content through Oracle Content and Experience Cloud components on sites.

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

There are additional user roles, but they are internal users who can't sign in to Oracle Content and Experience Cloud or administrative users who perform their tasks outside of Oracle Content and Experience Cloud. See User Roles.

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 (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.

When you create a resource, you're automatically assigned the Manager role. As the manager, you can share the resource with other users, assigning them roles to determine what they're able to do with that resource.

> **Note:**
>
> - See Set the Default Role for New Folder Members for information on assigning resource roles.
> - Oracle Documents Cloud *service users* are the same as Oracle Content and Experience Cloud *standard users*. Any feature described in the documentation as associated with *enterprise users* isn't available in Oracle Documents Cloud.

The roles below 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, including adding users and assigning them roles for the resource.

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

- Documents
- Conversations
- Sites
- Collections
- Content Items
- Digital Assets
- Components/Layouts
- Templates
- Themes
- Repositories
- Publishing Channels
- Localization Policies
- Content Types

Documents

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

Task	Viewer	Downloader	Contributor	Manager
Create folder • If you create a subfolder, you need these roles for the parent folder.			✓	✓
Upload • You need these roles for the folder into which you're uploading.			✓	✓
View (folder, file, properties)	✓	✓	✓	✓
Download		✓	✓	✓
Edit file/folder (upload new file version, reserve file, rename, move, copy, delete, edit tags)			✓	✓

Task	Viewer	Downloader	Contributor	Manager
Share				✓
Collaborate (add annotations, participate in associated conversation)	✓	✓	✓	✓
Edit custom properties values			✓	✓

Conversations

If you have a standard user or enterprise user role and one of the listed resource roles, you can create conversations. To view and participate in a conversation, you must be a member of the conversation.

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	Viewer	Downloader	Contributor	Manager
View (site, properties)	✓	✓	✓	✓
Create • You need these roles for template used to create the site. **Notes:** • Before you can create a site, your service administrator must enable the **Create** option for creating new sites. If you don't see this option on the **Sites** page, contact your service administrator. • If your service administrator limited site creation to site administrators, you must be a site administrator.		✓	✓	✓
Edit (site, rename, change status)			✓	✓
Copy			✓	✓
Delete				✓
Share			✓	✓

Task	Viewer	Downloader	Contributor	Manager
Create template from site			✓	✓

Collections

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

Task	Viewer	Downloader	Contributor	Manager
View (collection, properties)	✓	✓	✓	✓
Create • You need these roles for the repository where the collection will be stored.			✓	✓
Add asset to collection (digital asset, content item, or document) • You need these roles for the collection where the asset will be managed.			✓	✓
Remove asset from collection • You need these roles for the collection where the asset is managed.				✓
Edit (rename, properties)				✓
Share				✓
Submit assets for approval • You need these roles for the repository where the asset is managed.			✓	✓
Approve assets • You need these roles for the collection where the asset is managed, or you must be on the approver list for the collection.				✓
Publish assets • You need these roles for the collection where the asset is managed.				✓

Content Items

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

Task	Viewer	Downloader	Contributor	Manager
View • You need these roles for the collection where the content item is managed.	✓	✓	✓	✓
Create • You need these roles for the content type used to create the content item.	✓	✓	✓	✓
• You need these roles for the collection where the content item will be managed.			✓	✓
Edit (content item, tags) • You also need these roles for the collection where the content item is managed.			✓	✓
Delete **Note:** You must also have the content administrator user role to delete content items.			✓	✓

Digital Assets

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

Task	Viewer	Downloader	Contributor	Manager
Manage folder			✓	✓
Upload • You need these roles for the folder into which you're uploading.			✓	✓
View (asset, properties) • You need these roles for the folder that stores the digital asset.	✓	✓	✓	✓
Edit (add to collection, edit tags, upload new version) • You need these roles for the folder that stores the digital asset.			✓	✓
Download • You need these roles for the folder that stores the digital asset.		✓	✓	✓

Components/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	Viewer	Downloader	Contributor	Manager
View (component, properties)	✓	✓	✓	✓
Create Any user with the standard user or enterprise user 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
Edit (edit/upload component files)			✓	✓
Copy/export			✓	✓
Delete				✓
Share			✓	✓

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	Viewer	Downloader	Contributor	Manager
View (template, details)	✓	✓	✓	✓
Create • If you're creating a template from an existing site, you need these roles for the existing site. **Note:** If your service administrator limited template creation to site administrators, you must be a site administrator.		✓	✓	✓
Edit (edit/upload template files, rename)			✓	✓
Copy/export			✓	✓
Delete				✓
Share			✓	✓

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	Viewer	Downloader	Contributor	Manager
View (theme, properties)	✓	✓	✓	✓
Publish			✓	✓
Copy			✓	✓
Delete				✓
Share			✓	✓

Repositories

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

Task	Viewer	Downloader	Contributor	Manager
View	✓	✓	✓	✓
Create • You need these roles for any content types and publishing channels you want to assign to the repository.	✓	✓	✓	✓
Edit			✓	✓
Share				✓
Delete			✓	✓

Publishing Channels

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

Task	Viewer	Downloader	Contributor	Manager
View	✓	✓	✓	✓
Create Any user with the enterprise user role and content administrator user role can create publishing channels.	N/A	N/A	N/A	N/A
Edit			✓	✓
Share				✓
Delete			✓	✓

Localization Policies

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

Task	Viewer	Downloader	Contributor	Manager
View	✓	✓	✓	✓
Create Any user with the enterprise user role and content administrator user role can create localization policies.	N/A	N/A	N/A	N/A
Edit			✓	✓
Share				✓
Delete			✓	✓

Content Types

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

Task	Viewer	Downloader	Contributor	Manager
View	✓	✓	✓	✓

Task	Viewer	Downloader	Contributor	Manager
Create • You need these roles for any content layouts you want to assign to the content type.	✓	✓	✓	✓
Edit			✓	✓
Share				✓
Delete			✓	✓

Administrative Interfaces

There are several different interfaces used to manage your services. Depending on your administrative role and what you need to do, you perform your task in different areas.

My Account Application

> **Note:**
>
> Many features of the My Account application can now be performed from within the My Services application. In addition, if you have a Universal Credits subscription, then there's no need to use the My Account application, because all your Cloud account management tasks can be performed from My Services.

Use the My Account dashboard page to check the overall health of your *active* services. You can view service status, outages, and availability percentage. See Exploring the My Account Dashboard in *Managing and Monitoring Oracle Cloud*.

To use the My Account application:

1. Go to Oracle Cloud.
2. Select **Traditional Cloud Account** (even if you have a cloud account with Oracle Identity Cloud Service).
3. Under Order Management, click **My Account**.
4. Sign in using your Oracle.com account user name and password.

My Services Application

Use the My Services application to manage your Oracle Cloud services. The dashboard shows you your existing services and their statuses, enables you create new service instances, and displays your billing and service usage. You can also manage users in My Services. See About My Services Dashboard in *Getting Started with Oracle Cloud*.

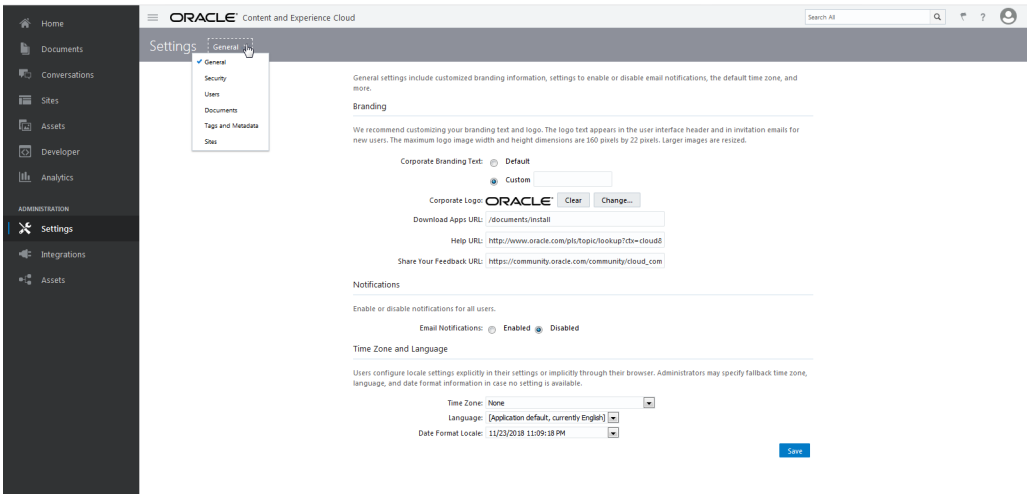
To use the My Services application, use one of the following methods:

- Click the **Access your Cloud Services** link in the email with the subject: “Welcome to Oracle Cloud. Your Oracle Public Cloud Services are ready for use.”, and enter your user name and password.
- Sign in from Oracle Cloud. See Sign In to Your Account From the Oracle Cloud Website in *Getting Started with Oracle Cloud*.

Oracle Content and Experience Cloud Administration Settings Interface

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

> **Note:**
>
> For information on the Administration Assets interface, see Setting Up Asset Repositories in *Creating Experiences with Oracle Content and Experience Cloud*.



To use the Oracle Content and Experience Cloud Administration Settings interface:

1. After you sign in to the Oracle Content and Experience Cloud web application as an administrator, click **Settings** in the Administration area of the navigation menu.
2. In the **Settings** menu, select a page:
   - **General:** Customize branding; enable or disable notifications; and set default time zone, language, and date/time format. See Configure General Settings.
   - **Security:** Set CORS origins, and enable the display of embedded content from Oracle Content and Experience Cloud within other domains. See Configure Security Settings.
   - **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. See Configure User Settings.

- **Documents:** Set default user storage quota and manage storage space; set default link behavior; restrict file types and sizes; and set virus scan options. See Configure Documents Settings.
- **Tags and Metadata:** Manage hashtags, and manage custom properties so that users can quickly categorize files and folders with additional descriptions, known as metadata. See Configure Tags and Metadata.
- **Sites:** Enable sites assets and access control options, and install the default site templates. See Configure Sites and Assets Settings.

Oracle Content and Experience Cloud Administration Integrations Interface

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

To use the Oracle Content and Experience Cloud Administration Integrations interface:

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

Depending on your environment, you might be able to integrate with Oracle Process Cloud Service, Oracle Eloqua Cloud Service, Visual Builder Cloud Service, Oracle Policy Automation Cloud Service, or Oracle Cobrowse Cloud Service. See Integrate the Service.

Administrative Tasks

As an administrator, you'll perform tasks to get Oracle Content and Experience Cloud 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 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.

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

Task	Where to Perform Task	Role Needed
Add corporate brand text and a custom logo to the Oracle Content and Experience Cloud interfaces	Oracle Content and Experience Cloud Administration — General	Identity domain administrator, service administrator, service user or standard user

Task	Where to Perform Task	Role Needed
Enable email notifications	Oracle Content and Experience Cloud Administration — General	Identity domain administrator, service administrator, service user or standard user
Set default time zone and language	Oracle Content and Experience Cloud Administration — General	Identity domain administrator, service administrator, service user or standard user
Enable Cross-Origin Resource Sharing (CORS)	Oracle Content and Experience Cloud Administration — Security	Identity domain administrator, service administrator, service user or standard user
Embed content in other domains	Oracle Content and Experience Cloud Administration — Security	Identity domain administrator, service administrator, service user or standard user
Add service administrator, account administrator, and service users, and assign them roles	My Services application	Identity domain administrator
Create organization groups and group standards	Oracle Content and Experience Cloud — User menu — Groups	Service user or standard user
Set the default role for new folder members	Oracle Content and Experience Cloud Administration — Users	Identity domain administrator, service administrator, service user or standard user
Sync user profile data	Oracle Content and Experience Cloud Administration — Users	Identity domain administrator, service administrator, service user or standard user
Set user quotas and manage storage space	Oracle Content and Experience Cloud Administration — Documents	Identity domain administrator, service administrator, service user or standard user
Set default link behavior	Oracle Content and Experience Cloud Administration — Documents	Identity domain administrator, service administrator, service user or standard user
Restrict file types and sizes	Oracle Content and Experience Cloud Administration — Documents	Identity domain administrator, service administrator, service user or standard user
Set virus scan options	Oracle Content and Experience Cloud Administration — Documents	Identity domain administrator, service administrator, service user or standard user
Manage hashtags	Oracle Content and Experience Cloud Administration — Tags and Metadata	Identity domain administrator, service administrator, service user or standard user
Configure custom properties for files and folders	Oracle Content and Experience Cloud Administration — Tags and Metadata	Identity domain administrator, service administrator, service user or standard user/ enterprise user
Configure sites settings and install site templates	Oracle Content and Experience Cloud Administration — Sites	Identity domain administrator, service administrator, service user or standard user/ enterprise user

Task	Where to Perform Task	Role Needed
Integrate Oracle Content and Experience Cloud with Process Cloud Service, Eloqua Cloud Service, Visual Builder Cloud Service, Oracle Policy Automation, Oracle Cobrowse Cloud Service, and custom applications **Note:** Integrating with Eloqua Cloud Service is currently unavailable if you have a Universal Credits subscription.	Oracle Content and Experience Cloud Administration — Integrations and the applications you're integrating	Identity domain administrator, service administrator, service user or standard user
Configure Proxy Service Settings **Note:** This feature is currently unavailable if you have a Universal Credits subscription.	Oracle Content and Experience Cloud Administration — Integrations	Identity domain administrator, service administrator, service user or standard user
Enable single sign-on (SSO)	My Services application	Identity domain administrator
Let users know how to sign in to Oracle Content and Experience Cloud and who to contact if they have issues	An email is 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
Manage users who join or leave your organization	To manage users, use the My Services application To reassign or delete content owned by users who have left your organization, use Oracle Content and Experience Cloud Administration — Users	Identity domain administrator, service administrator, service user or standard user
Report any issues you find	My Services application	Service instance administrator
Analyze service usage, monitor service activity, and run reports	Oracle Content and Experience Cloud Analytics	Identity domain administrator, service administrator, service user or standard user

For information on content administrator tasks (those found in Administration — Assets), see Setting Up Asset Repositories in *Creating Experiences with Oracle Content and Experience Cloud*.

Security

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

Security Feature	Description	Who Manages It and Where
User accounts	You need an account with a user name and password to access Oracle Content and Experience Cloud.	Identity domain administrators manage accounts in the My Services application. See Add Users.

Security Feature	Description	Who Manages It and Where
User roles	Each user is assigned one or more roles to control what functionality and areas of the user interface they can access.	Identity domain administrators or service administrators assign user roles in the My Services application. See User Roles.
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.	Service administrators should create high-level organizational groups and communicate group standards. See Create Group Standards for Your Organization. Users can create additional groups as necessary. See Using Groups and Following People in *Managing Content with Oracle Content and Experience Cloud*.
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. See How do I set a passcode? in *Managing Content with Oracle Content and Experience Cloud*.
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. See What do I do if my device is lost or stolen? in *Managing Content with Oracle Content and Experience Cloud*.
Single Sign-On (SSO)	If Federated Single Sign-On (SSO) is currently available for your Oracle Content and Experience Cloud 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.	Account administrators configure SSO in the My Services application. See Enable Single Sign-On (SSO).

Security Feature	Description	Who Manages It and Where
File encryption	Files are protected using Secure Sockets Layer (SSL) 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 and Experience Cloud app unless you specifically download the file for use on the device.	File encryption is handled automatically by Oracle Content and Experience Cloud.
File type and size restrictions	You can specify which types of files can be uploaded and restrict the size of uploaded files.	Service administrators configure file type and size restrictions through the Oracle Content and Experience Cloud Administration interface. See Restrict File Types and Sizes.
Virus scanning	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 virus scan settings through the Oracle Content and Experience Cloud Administration interface. See Set Virus Scanning Options.
File access control	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. 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.	Service administrators configure default document security settings. See Set the Default Role for New Folder Members and Set Default Link Behavior. Users control access when they share content. See Sharing Your Content and Sites with Others in *Managing Content with Oracle Content and Experience Cloud*.
Conversation encryption	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.	Conversation encryption is handled automatically by Oracle Content and Experience Cloud.

Security Feature	Description	Who Manages It and Where
Site creation and sharing restrictions	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.	Service administrators configure sites settings through the Oracle Content and Experience Cloud Administration interface. See Configure Sites and Assets Settings.
Site security	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.	Site owners and managers control the security for individual sites. See Understanding Site Security and Changing Site Security in *Creating Experiences with Oracle Content and Experience Cloud*.
Site sharing	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.	Site owners and managers control the security for individual sites. See Understanding Site Security and Changing Site Security in *Creating Experiences with Oracle Content and Experience Cloud*
Site component sharing	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).	Site component sharing is handled automatically by Oracle Content and Experience Cloud based on site and resource security.
Cross-Origin Resource Sharing (CORS)	Cross-Origin Resource Sharing (CORS) allows a web page to make requests such as XMLLHttpRequest to another domain. If you have a browser application that integrates with Oracle Content and Experience Cloud but is hosted in a different domain, add the browser application domain to Oracle Content and Experience Cloud's CORS origins list.	Service administrators configure CORS through the Oracle Content and Experience Cloud Administration interface. See Enable Cross-Origin Resource Sharing (CORS).

Security Feature	Description	Who Manages It and Where
Proxy service **Note:** This feature is currently unavailable if you have a Universal Credits subscription.	Oracle Content and Experience Cloud 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 *endpoint*). 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 and Experience Cloud Administration Integrations interface. See Configure Proxy Service Settings.
Embedded content whitelist	You can display content from Oracle Content and Experience Cloud within other domains. For example, you might embed the Oracle Content and Experience Cloud 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 whitelist.	Service administrators configure embedded content settings through the Oracle Content and Experience Cloud Administration interface. See Embed Content in Other Domains.

Monitoring the Service

Throughout the use of your service, you'll want to monitor the overall system, view reports on your users and documents, and analyze service usage statistics.

- You can view service usage statistics to help you analyze system needs or issues.

  See Analyze Service Usage.

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

  See Run Reports.

- You can check the overall status of your active Oracle Cloud services in the My Services dashboard. You can view the overall service status, outages, and uptime percentages for the past 14 days. You can also see the storage used, and other details. 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.

  See Monitor Service Activity.

Standard Edition vs. Enterprise Edition

Users see the standard edition or enterprise edition of Oracle Content and Experience Cloud depending on which user role they're assigned — *standard user* or *enterprise user*. Your Oracle Content and Experience Cloud instance can have both standard users and enterprise users at the same time; they'll just see different features in the user interface.

> **Note:**
>
> For more information on roles, see User Roles and Task and Feature Comparison by User Role.

Feature	Standard Edition	Enterprise Edition
Documents	✓	✓
Conversations (discuss topics, direct messages, assign flags, add annotations to documents)	✓	✓
Groups	✓	✓
Sites	✓	✓
Assets (images, videos, documents, and content items that you manage independently from your other files and folders, and the collections to keep them organized)		✓
Developer (components, layouts, templates, and themes) This feature can be restricted to only site administrators.	✓	✓
Analytics You also need the Service Administrator user role to access this feature.	✓	✓
Administration: Settings (branding, notifications, default time zone/ language, security settings, users, storage quotas, transferring file ownership, default link behavior, file restrictions, hashtags, custom properties, site creation settings, installing default templates, and integrating with other business applications) You also need the Service Administrator user role to access this feature.	✓	✓

Feature	Standard Edition	Enterprise Edition
Administration: Assets (repositories, publishing channels, localization policies, and content types) You also need the Content Administrator user role to access this feature.		✓

Understand Active Users per Hour

If you have a universal credits subscription, and you create an Oracle Content and Experience Cloud 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 and Experience Cloud 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 credit 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 Credit 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 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 and Experience Cloud 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 and Experience Cloud? Will using the link be counted as an active user session?

Visiting the site created with Oracle Content and Experience Cloud triggers a 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 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 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 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. See Integrating Folder and File Selection and Applinks Resource in *Developing for Oracle Content and Experience Cloud*.

How is a user of the Oracle Content and Experience Cloud desktop client tracked?

A desktop client user is tracked 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 1GB 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).

2
Roll Out the Service

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

Topics

- Understand the Roll-Out Process
- Provide Sign In and Get Started Information to Users
- Deploy the Desktop App

Understand the Roll-Out Process

You have a few main tasks to perform to get Oracle Content and Experience Cloud up and running:

- 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.
- Add users and assign them roles. See Add Users.

  If your company uses single sign-on (SSO), you'll also want to enable SSO. See Enable Single Sign-On (SSO).
- Create groups for your organizational structure. See Create Group Standards for Your Organization.
- You might want to perform some of the following tasks to get the most out of Oracle Content and Experience Cloud:
  - Apply Custom Branding and URLs
  - Enable or Disable Email Notifications
  - Set the Default Time Zone and Language
  - Configure Custom Properties (Metadata)
- Introduce your users to Oracle Content and Experience Cloud 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 and Experience Cloud with your other business applications. See Integrate the Service.

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 a welcome email, giving the user sign-in information. But it's useful for you to also send an email, providing more details.

Automatic Welcome Email

The automatic welcome email includes the web address (URL) for the service and the user's credentials (user name, password, and identity domain).

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-identity_domain_name.documents.dc.cloud.example.com/documents
```

For example, if `salesdocuments1` was entered as your service name, `mydomain` was entered as your identity name, and the data center (*dc*) is `us2`, the service URL is:

```
salesdocuments1-mydomain.documents.us2.cloud.example.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 Documents Cloud Service 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.

- Running the Executable Installer
- Running the MSI Installer
- Deploying the MSI Installer Through Active Directory's Group Policy
- Setting 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

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

- Syntax:

```
{installer path} /d|directory {product directory} /L|
language /g|log {log path} /s|silent /v|custom {options}
```

- Parameters
  - **{installer path}** - The path of an installer executable.
  - **/d** or **/directory {product directory}** (optional) - Specifies the directory into which the product will be placed.
  - **/L** or **/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** or **/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** or **/silent** (optional) - Specifies whether or not the user interface is shown.
  - **/v** or **/custom {options}** (optional) - Specifies options to pass to the Msiexec process. See Running the MSI Installer for details.
- Example

```
oracle_documents_setup.exe /directory "C:\Oracle\Oracle
Documents"
```

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
  - **{installer path}** - The path of an installer MSI file.
  - **/r** or **/repair** - Repairs the product.
  - **/g** or **/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** or **/silent** (optional) - Specifies whether or not the user interface is shown.
  - **/v** or **/custom {options}** (optional) - Specifies options to pass to the Msiexec process. See Running the MSI Installer for details.
- Example

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

To extract the installer MSI and MST

- Syntax

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

- Parameters

  - **{installer path}** - The path of an installer MSI file.
  - **/e** or **/extract {destination directory}** - Extracts the installer MSI and MST into the given directory.
  - **/L** or **/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_documents_setup.exe /extract C:\Users\blair\desktop
  ```

To use the installer without a user interface

- Syntax

  ```
  {installer path} /s|silent
  ```
- Parameters
  - **{installer path}** - The path of an installer executable.
  - **/s** or **/silent** (optional) - Specifies whether or not the user interface is shown.
- Example

  ```
  oracle_documents_setup.exe /silent
  ```

Language Codes

- 1025: Arabic
- 1029: Czech
- 1030: Danish
- 1031: German
- 1032: Greek
- 1033: English
- 1034: Spanish
- 1035: Finnish
- 1036: French (France)
- 3084: French (Canada)
- 1037: Hebrew
- 1038: Hungarian
- 1040: Italian
- 1041: Japanese
- 1042: Korean
- 1043: Dutch
- 1044: Norwegian
- 1045: Polish
- 1046: Portuguese (Brazil)
- 2070: Portuguese (Portugal)
- 1048: Romanian

- 1049: Russian
- 1051: Slovak
- 1053: Swedish
- 1054: Thai
- 1055: Turkish
- 2052: Chinese (China)
- 1028: Chinese (Taiwan)

Run the MSI Installer

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

`oracle_documents_setup.exe /extract c:\`*directory*

The following MSI options are supported by the Oracle Content and Experience Cloud MSI package.

Option	Parameter	Meaning	Example

`/i`		Install the product.
		• Use the `/norestart` parameter to install the product without prompting for a system restart at the end of installation.
		• Use the `/promptrestart` parameter to prompt the user to restart if a restart is required.
		• Use the `/forcerestart` parameter to restart the computer after every installation.
			`msiexec /i oracle_documents_setup.msi`
			`msiexec /i oracle_documents_setup.msi /norestart`
			`msiexec /i oracle_documents_setup.msi /promptrestart`
			`msiexec /i oracle_documents_setup.msi /forcerestart`

`/i`	*{path to latest version}*	Upgrade the product to the latest version.	`msiexec /i oracle_documents_setup.msi`
`/i`	`CUSTOM_INSTALLDIR` =*{path to custom directory}*	Install the product in a non-default (custom) location.	`msiexec oracle_documents_setup.msi CUSTOM_INSTALLDIR="c:\example"`

`/x`		Uninstall the product.
		• Use the `/norestart` parameter to uninstall the product without prompting for a system restart at the end of removal.
		• Use the `/promptrestart` parameter to prompt the user to restart if a restart is required.
		• Use the `/forcerestart` parameter to restart the computer.
			`msiexec /x oracle_documents_setup.msi`
			`msiexec /x oracle_documents_setup.msi /norestart`
			`msiexec /x oracle_documents_setup.msi /promptrestart`
			`msiexec /x oracle_documents_setup.msi /forcerestart`

Option	Parameter	Meaning	Example
`/f {p|o|e|d|c|a|u|m|s|v}`		Repair the product. • `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`: installs if file is missing or the stored checksum does not match the calculated value • `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. Does not overwrite desktop or favorite shortcuts.	`msiexec /fomus oracle_documents_setup.msi` `msiexec /fpecms oracle_documents_setup.msi`
`/i|x|f /q{n|b|r|f}`		Set the level of user interface displayed on installation, uninstallation or repairing the product by using `/q` with one of these options: • `n`: Displays no user interface. • `b`: Displays only a progress bar during install. • `r`: Displays a reduced user interface with a modal dialog displayed at the end of the installation • `f`: Displays a full user interface with modal dialog displayed at the end	`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 and Experience Cloud.
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.

3

Deploy Oracle Content and Experience Cloud

There are several tasks involved in deploying Oracle Content and Experience Cloud.

- Subscribe to Oracle Cloud
- Create Your Service Instance
- Create Groups for Your Organization
- Assign Roles to Groups
- Add Users
- Assign Users to Groups
- Migrate from Traditional Digital Assets to New Digital Assets

Subscribe to Oracle Cloud

Before you can begin using Oracle Content and Experience Cloud, your organization must purchase a subscription, create a cloud account, and then activate the service.

Depending on what type of subscription you purchase and how you order it, you perform different tasks as described in *Getting Started with Oracle Cloud*:

- Universal Credits subscriptions through the Oracle Cloud website — If you use Universal Credits to purchase a subscription through the Oracle Cloud website self-service tools, your service will be activated automatically and you'll create your Cloud account as part of your subscription sign-up. See Buying an Oracle Cloud Subscription.
- Universal Credits subscriptions through Oracle Sales — If you use Universal Credits to purchase a subscription through Oracle Sales, you need to create your cloud account and activate your service through the welcome email you received. See Activating Your Order from Your Welcome Email.
- Non-metered subscriptions through Oracle Sales— If you purchased a non-metered subscription through Oracle Sales, you need to activate your account to access your services. See Activating Your Order.

Note:

- If you weren't able to create a cloud account when you purchased your subscription or when you activated your service, see Signing Up for a Cloud Account in *Getting Started with Oracle Cloud*.
- In March 2018, Oracle Content and Experience Cloud moved to the Universal Credits model. If you purchased your subscription after March 2018, you have a Universal Credits subscription, and you have a cloud account with Oracle Identity Cloud Service (IDCS). See About Universal Credits in *Getting Started with Oracle Cloud*. If you purchased your subscription prior to March 2018, you have a non-metered subscription, and you have a traditional cloud account.
- If you switch from a non-metered subscription to a Universal Credits subscription, you'll need to replicate your content to your new service instance.
- If you have a non-metered subscription, you also need an entitlement. If you purchased your subscription between February 2017 and March 2018, you have an entitlement to Oracle Content and Experience Cloud. If you purchased your subscription prior to February 2017, you might have an entitlement to Oracle Documents Cloud.
- For more information on subscriptions, see Overview of Oracle Cloud Subscriptions in *Getting Started with Oracle Cloud*.

What to Do Next

After your service is activated, you need to create a service instance. See Create Your Service Instance.

Note:

If you have a Universal Credits subscription, and you create an Oracle Content and Experience Cloud instance, you'll be billed based on active users per hour. See Understand Active Users per Hour.

Create Your Service Instance

After subscribing to Oracle Cloud and activating your service, you need to create a service instance.

> **Note:**
>
> - If you haven't subscribed to Oracle Cloud, activated your service, or set up your cloud account, or you're not sure what type of subscription you have, see Subscribe to Oracle Cloud.
> - If you have a Universal Credits subscription, and you create an Oracle Content and Experience Cloud-Classic instance, you'll be billed based on active users per hour. See Understand Active Users per Hour.
>
> Depending on the type of subscription and service you have, you'll be asked for different information when creating your service instance:

- If you have a Universal Credits subscription with Oracle Content and Experience Cloud, see Create an Oracle Content and Experience Cloud Instance with a Universal Credits Subscription.
- If you have a Universal Credits subscription with Oracle Content and Experience Cloud-Classic, see Create an Oracle Content and Experience Cloud-Classic Instance with a Universal Credits Subscription.
- If you have a non-metered subscription with Oracle Content and Experience Cloud, see Create an Oracle Content and Experience Cloud Instance with a Non-Metered Subscription.
- If you have a non-metered subscription with Oracle Documents Cloud, see Create an Oracle Documents Cloud Service Instance.

Create an Oracle Content and Experience Cloud Instance with a Universal Credits Subscription

If you have a Universal Credits subscription with Oracle Content and Experience Cloud, you can follow the steps in this section to create your service instance.

Creating an instance of Oracle Content and Experience Cloud involves the followings 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 and Experience Cloud Instance

Verify That the Cloud Account Administrator Is Part of the OCI_Administrators Group

The administrator who creates the instance must be part of the **OCI_Administrators** group. You can check My Services to confirm that the administrator is a member of this group.

1. On the My Services dashboard, click **Users** in the top menu.
2. Click **Groups** under User Management.
3. Verify that the OCI_Administrators group is listed.
4. Click **OCI_Administrators**.
5. Click **Users** to list the group members.
6. Verify that the Cloud Account Administrator user is listed.

If the administrator is not a member of **OCI_Administrators**, you need to add the administrator to the group. See Assign Users to Groups with Oracle Identity Cloud Service.

Get Region, User, and Tenancy Values

When you create your Oracle Content and Experience Cloud 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. Open the email with the subject: "Welcome to Oracle Cloud. Your Oracle Public Cloud Services are ready for use."
2. Click the **Access your Cloud Services** link in the email, and enter the My Services user name and password from your email. If you're prompted to do so, reset your password.
3. On the My Services dashboard, next to Compute, click , and select **Open Service Console**. This opens the Oracle Cloud Infrastructure Console.

   > **Note:**
   >
   > If you don't see Compute in the dashboard, click **Customize Dashboard**, and set Compute to **Show**.

4. In the data center drop-down list in the top right (next to , 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.
5. In the Oracle Cloud Infrastructure console, from the menu on the top left, click **Identity** and then **Users**.
6. 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 OCI Console:

   a. On the navigation menu, click **Identity**, then **Users**, and then **Create User**.
   b. Enter a user name in the **NAME** field and then click **Create**.
   c. On the navigation menu, click **Identity** and then **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.

> **Important:**
>
> Creating a user in the OCI 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 CECS service.

7. From the menu on the top left, click **Administration** and then **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 Infrastructure navigation menu, under Governance and Administration, click **Identity**, and then 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 such as `OCIStorageCompartment`.
4. Enter a description such as `Compartment for OCI object storage`.
5. Click **Create Compartment**.
6. 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 a Content and Experience Cloud 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 and Experience Cloud 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 Infrastructure 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 and Experience Cloud Instance

1. Return to My Services.
2. On the My Services dashboard, click **Oracle Content and Experience Cloud**.
3. 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.

4. 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.

Note:

For more information, see Creating a Service Instance in *Getting Started with Oracle Cloud*.

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 and Experience Cloud web client, click next to your Oracle Content and Experience Cloud service instance, and select **Access Content Cloud Service Instance**.

Important:

When your service instance is created, 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 and Experience Cloud components. *Do not delete this user* or some functionality in Oracle Content and Experience Cloud will no longer work.

Next, create groups for the roles in your organization. See Create Groups for Your Organization.

Create an Oracle Content and Experience Cloud-Classic Instance with a Universal Credits Subscription

If you have a Universal Credits subscription with Oracle Content and Experience Cloud-Classic, you need to set up your storage service and create the storage user, and then create your service instance.

Creating a Oracle Content and Experience Cloud-Classic instance involves the followings steps:

1. Set Up Your Storage Service
2. Create the Storage User
3. Create Your Oracle Content and Experience Cloud-Classic Instance

Set Up Your Storage Service

Before you create an Oracle Content and Experience Cloud-Classic instance, complete the following steps to set up your storage service:

1. Sign in to My Services using one of the following methods:
   - Click the **Access your Cloud Services** link in the email with the subject: “Welcome to Oracle Cloud. Your Oracle Public Cloud Services are ready for use.”, and enter your user name and password.
   - Sign in from Oracle Cloud:
     a. Go to http://cloud.oracle.com.
     b. Click **Sign In**.
     c. From the **Cloud Account** menu, select **Cloud Account with Identity Cloud Service**.
     d. In the **Cloud Account Name** field, enter the name of your cloud account.
     e. Click **My Services**.
     f. Enter the user name and password for your cloud account.
2. On the My Services dashboard, next to Storage Classic, click , and select **Open Service Console**.

   > **Note:**
   >
   > If you don’t see Storage Classic in the dashboard, click **Customize Dashboard**, and set Storage Classic to **Show**.

3. 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.

4. Click the **Account** tab, and make note of **REST Endpoint**. This is the Storage URL you'll enter when you create your Oracle Content and Experience Cloud instance.

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 and Experience Cloud.

1. In My Services, click the **Users** tab.
2. On the User Management page, in the banner, click **Identity Console**.

   You'll be redirected to the Oracle Identity Cloud Service Users page.
3. Click **Add**.
4. Enter `Storage` as the first name and `Admin` as the last name.
5. Enter `storageadmin` as the user name.
6. Clear the **Use the email address as the user name** box.
7. Enter an email that *won't* be used to log in to Oracle Content and Experience Cloud, but that you have access to, so you can set the password.
8. After you receive the welcome email for the storageadmin user, set the storageadmin password.
9. Click **Finish**.
10. Expand the navigation drawer, and then click **Applications**.
11. Find and open your Storage Classic application.
12. Click the **Application Roles** tab.
13. Next to the **Storage_Administrator** role, click , and then select **Assign Users**.
14. Find and select the **Storage User**, and then click **Assign**.

Create Your Oracle Content and Experience Cloud-Classic Instance

To create an Oracle Content and Experience Cloud-Classic instance with a Universal Credits subscription:

1. On the My Services dashboard, click **Create Instance**.
2. Click the **All Services** tab.
3. Scroll down to the **Content and Experience** section.
4. Next to **Content Cloud**, click **Create**.
5. On the **Instances** tab of the Content and Experience Cloud Service page, click **Create Instance**.

6. 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. See Set Up Your Storage Service.
Storage Username	Enter the user name of the dedicated user you created for your storage service (this should be storageadmin). See Set Up Your Storage Service.
Storage Password	Enter the password for the storage service user. See Set Up Your Storage Service.

7. Click **Create**.

> **Note:**
>
> For more information, see Creating a Service Instance in *Getting Started with Oracle Cloud*.

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 and Experience Cloud. The first email includes a link to your instance (in My Services). The second email includes a link to the Oracle Content and Experience Cloud web client.

> **Important:**
>
> When your service instance is created, 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 and Experience Cloud components. *Do not delete this user* or some functionality in Oracle Content and Experience Cloud will no longer work.

Next, create groups for the roles in your organization. See Create Groups for Your Organization.

Create an Oracle Content and Experience Cloud Instance with a Non-Metered Subscription

If you have a non-metered subscription with Oracle Content and Experience Cloud, follow the instructions in this topic to create a service instance.

> **Note:**
>
> If you haven't subscribed to Oracle Cloud, activated your service, set up your cloud account, or you're not sure what type of subscription you have, see Subscribe to Oracle Cloud.

To create an Oracle Content and Experience Cloud instance with a non-metered subscription:

1. Sign in to My Services using one of the following methods:
   - Click the **Access your Cloud Services** link in the email with the subject: "Welcome to Oracle Cloud. Your Oracle Public Cloud Services are ready for use.", and enter your user name and password.
   - Sign in from Oracle Cloud:
     a. Go to http://cloud.oracle.com.
     b. Click **Sign In**.
     c. From the **Cloud Account** menu, select **Traditional Cloud Account**.
     d. Select your data center.
     e. Click **My Services**.
     f. Enter your identity domain, and click **Go**.
     g. Enter the user name and password for your cloud account.
2. Next to Content Cloud, click **Create**.
3. On the Create New Oracle Content and Experience Cloud 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 and Experience Cloud** from the list.
Product	Select **Content and Experience Cloud** from the list.

Field	Description
Number of Standard Users	Enter the number of *standard users* 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 a Content and Experience Cloud entitlement.
Number of Enterprise Users	Enter the number of *enterprise users* 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.

> **Note:**
>
> For more information, see Creating a Service Instance in *Getting Started with Oracle Cloud*.

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 and Experience Cloud. The first email includes a link to My Services (click the link to your instance). The second email includes a link to the Oracle Content and Experience Cloud web client.

Next, create groups for the roles in your organization. See Create Groups for Your Organization.

Create Groups for Your Organization

As a best practice, you should create groups for your organization roles and assign the appropriate user roles to those groups. Then you can add users to those groups to automatically assign them the appropriate user roles.

For a list of typical organization roles and the user roles they need, see Typical Organization Roles.

How you create groups depends on what type of subscription you have.

- For Universal Credits subscriptions, see Create Groups with Oracle Identity Cloud Service.

- For non-metered subscriptions, see Create Groups with a Traditional Cloud Account.

Create Groups with Oracle Identity Cloud Service

If you have a Universal Credits subscription, you create groups in Oracle Identity Cloud Service.

To create groups:

1. Sign in to My Services using one of the following methods:
   - Click the **Access your Cloud Services** link in the email with the subject: “Welcome to Oracle Cloud. Your Oracle Public Cloud Services are ready for use.”, and enter your user name and password.
   - Sign in from Oracle Cloud:
     a. Go to http://cloud.oracle.com.
     b. Click **Sign In**.
     c. From the **Cloud Account** menu, select **Cloud Account with Identity Cloud Service**.
     d. In the **Cloud Account Name** field, enter the name of your cloud account.
     e. Click **My Services**.
     f. Enter the user name and password for your cloud account.
2. In the dashboard, click **Users**.
3. On the User Management page, in the banner, click **Identity Console**.

   You’ll be redirected to the Oracle Identity Cloud Service Users page.
4. Display the navigation drawer, and then click the **Groups** tab.
5. To create a group, click **Add**. See Creating Groups in *Administering Oracle Identity Cloud Service*.

Next, assign roles to your group. See Assign Roles to Groups.

Create Groups with a Traditional Cloud Account

If you have a non-metered subscription, you create groups in My Services.

To create a group:

1. Sign in to My Services using one of the following methods:
   - Click the **Access your Cloud Services** link in the email with the subject: “Welcome to Oracle Cloud. Your Oracle Public Cloud Services are ready for use.”, and enter your user name and password.
   - Sign in from Oracle Cloud:
     a. Go to http://cloud.oracle.com.
     b. Click **Sign In**.
     c. From the **Cloud Account** menu, select **Traditional Cloud Account**.
     d. Select your data center.

   e. Click **My Services**.
   f. Enter your identity domain, and click **Go**.
   g. Enter the user name and password for your cloud account.
2. In the dashboard, click **Users**.
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 group. See Assign Roles to Groups.

Assign Roles to Groups

As a best practice, you should create groups for your organization roles and assign the appropriate user roles to those groups. Then you can add users to those groups to automatically assign them the appropriate user roles.

For a list of typical organization roles and the user roles they need, see Typical Organization Roles.

How you assign roles to groups depends on what type of subscription you have.

- For Universal Credits subscriptions, see Assign Roles to Groups with Oracle Identity Cloud Service.
- For non-metered subscriptions, see Assign Roles to Groups with a Traditional Cloud Account.

Assign Roles to Groups with Oracle Identity Cloud Service

If you have a Universal Credits subscription, you assign roles to groups through the **Applications** tab of Oracle Identity Cloud Service.

To assign roles to groups:

1. Sign in to My Services using one of the following methods:
   - Click the **Access your Cloud Services** link in the email with the subject: “Welcome to Oracle Cloud. Your Oracle Public Cloud Services are ready for use.”, and enter your user name and password.
   - Sign in from Oracle Cloud:
     a. Go to http://cloud.oracle.com.
     b. Click **Sign In**.
     c. From the **Cloud Account** menu, select **Cloud Account with Identity Cloud Service**.
     d. In the **Cloud Account Name** field, enter the name of your cloud account.
     e. Click **My Services**.
     f. Enter the user name and password for your cloud account.
2. In the dashboard, click **Users**.
3. On the User Management page, in the banner, click **Identity Console**.

You'll be redirected to the Oracle Identity Cloud Service Users page.

4. Expand the navigation drawer, and then click **Applications**.
5. Open your Oracle Identity Cloud Service application.
6. Click the **Application Roles** tab.
7. Next to the role you want to assign to the group, click , and then select **Assign Groups**.
8. Find and select the group you want, and then click **Assign**.

   For a list of typical organization roles and the user roles they need, see Typical Organization Roles. For a description of the predefined roles in Oracle Content and Experience Cloud, see User Roles.

Next, assign your users to groups to give them the appropriate roles and permissions. See Assign Users to Groups.

Assign Roles to Groups with a Traditional Cloud Account

If you have a non-metered subscription, you assign roles to groups in My Services.

To assign roles to groups:

1. Sign in to My Services using one of the following methods:
   - Click the **Access your Cloud Services** link in the email with the subject: "Welcome to Oracle Cloud. Your Oracle Public Cloud Services are ready for use.", and enter your user name and password.
   - Sign in from Oracle Cloud:
     a. Go to http://cloud.oracle.com.
     b. Click **Sign In**.
     c. From the **Cloud Account** menu, select **Traditional Cloud Account**.
     d. Select your data center.
     e. Click **My Services**.
     f. Enter your identity domain, and click **Go**.
     g. Enter the user name and password for your cloud account.
2. In the dashboard, click **Users**.
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 user roles they need, see Typical Organization Roles. For a description of the predefined roles in Oracle Content and Experience Cloud, see User Roles.

Next, assign your users to groups to give them the appropriate roles and permissions. See Assign Users to Groups.

Add Users

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

How you add users depends on what type of subscription you have.

- For Universal Credits subscriptions, see Add Users with Oracle Identity Cloud Service.
- For non-metered subscriptions, see Add Users with a Traditional Cloud Account.

Add Users with Oracle Identity Cloud Service

If you have a Universal Credits subscription, you add users in Oracle Identity Cloud Service.

To add users:

1. Sign in to My Services using one of the following methods:
   - Click the **Access your Cloud Services** link in the email with the subject: “Welcome to Oracle Cloud. Your Oracle Public Cloud Services are ready for use.”, and enter your user name and password.
   - Sign in from Oracle Cloud:
     a. Go to http://cloud.oracle.com.
     b. Click **Sign In**.
     c. From the **Cloud Account** menu, select **Cloud Account with Identity Cloud Service**.
     d. In the **Cloud Account Name** field, enter the name of your cloud account.
     e. Click **My Services**.
     f. Enter the user name and password for your cloud account.
2. In the dashboard, click **Users**.
3. On the User Management page, in the banner, click **Identity Console**.

   You’ll be redirected to the Oracle Identity Cloud Service Users page.
4. Add users using one of the following methods:
   - To import users, you need to a create 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**. See Creating User Accounts in *Administering Oracle Identity Cloud Service*.

Next, assign your users to groups to give them the appropriate roles and permissions. See Assign Users to Groups. For other user management tasks, see Manage Users, Groups, and Access.

Add Users with a Traditional Cloud Account

If you have a non-metered subscription, you manage users in My Services.

To add users:

1. Sign in to My Services using one of the following methods:
   - Click the **Access your Cloud Services** link in the email with the subject: “Welcome to Oracle Cloud. Your Oracle Public Cloud Services are ready for use.”, and enter your user name and password.
   - Sign in from Oracle Cloud:
     a. Go to http://cloud.oracle.com.
     b. Click **Sign In**.
     c. From the **Cloud Account** menu, select **Traditional Cloud Account**.
     d. Select your data center.
     e. Click **My Services**.
     f. Enter your identity domain, and click **Go**.
     g. Enter the user name and password for your cloud account.
2. In the dashboard, click **Users**.
3. To create users individually or in a batch, and to assign user roles, see Adding Users to a Traditional Cloud Account in *Getting Started with Oracle Cloud*.

Next, assign your users to groups to give them the appropriate roles and permissions. See Assign Users to Groups. For other user management tasks, see Manage Users, Groups, and Access.

Assign Users to Groups

Assign users to groups to automatically give them the appropriate roles and permissions.

How you assign users to groups depends on what type of subscription you have.

- For Universal Credits subscriptions, see Assign Users to Groups with Oracle Identity Cloud Service.
- For non-metered subscriptions, see Assign Users to Groups with a Traditional Cloud Account.

Assign Users to Groups with Oracle Identity Cloud Service

If you have a Universal Credits subscription, you assign users to groups inOracle Identity Cloud Service.

To assign users to groups:

1. Sign in to My Services using one of the following methods:

- Click the **Access your Cloud Services** link in the email with the subject: “Welcome to Oracle Cloud. Your Oracle Public Cloud Services are ready for use.”, and enter your user name and password.
- Sign in from Oracle Cloud:
  a. Go to http://cloud.oracle.com.
  b. Click **Sign In**.
  c. From the **Cloud Account** menu, select **Cloud Account with Identity Cloud Service**.
  d. In the **Cloud Account Name** field, enter the name of your cloud account.
  e. Click **My Services**.
  f. Enter the user name and password for your cloud account.

2. In the dashboard, click **Users**.
3. On the User Management page, in the banner, click **Identity Console**.

   You’ll be redirected to the Oracle Identity Cloud Service Users page.
4. Expand the navigation drawer, and then click **Groups**.
5. Open the group you want to assign users to.
6. Click **Assign**.
7. Select the users you want to add, and then click **OK**.

Assign Users to Groups with a Traditional Cloud Account

If you have a non-metered subscription, you assign users to groups in My Services.

To assign users to groups:

1. Sign in to My Services using one of the following methods:
   - Click the **Access your Cloud Services** link in the email with the subject: “Welcome to Oracle Cloud. Your Oracle Public Cloud Services are ready for use.”, and enter your user name and password.
   - Sign in from Oracle Cloud:
     a. Go to http://cloud.oracle.com.
     b. Click **Sign In**.
     c. From the **Cloud Account** menu, select **Traditional Cloud Account**.
     d. Select your data center.
     e. Click **My Services**.
     f. Enter your identity domain, and click **Go**.
     g. Enter the user name and password for your cloud account.
2. In the dashboard, click **Users**.
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**.

Migrate from Traditional Digital Assets to New Digital Assets

If you created assets with a Universal Credits subscription to Oracle Content and Experience Cloud prior to August 2018, you need to migrate those assets to the new asset repository structure. The new asset repository structure includes support for publishing channels and localization.

Perform the following steps to migrate your digital assets:

1. Repository Administrator Creates a Repository for Migration
2. Site Administrator Configures Repository for Migration
3. Collection Owners Migrate Their Collections

If you run into any problems, see Troubleshooting.

Repository Administrator Creates a Repository for Migration

The repository administrator needs to create a repository to store the migrated assets and give your site administrator and collection owners access to the new repository. A repository administrator is a user with a Manager role within at least one repository.

1. Sign in to Oracle Content and Experience Cloud as a repository administrator.
2. Create a repository to store your migrated assets, and assign your site administrator the contributor resource role to the repository. See Creating and Sharing Asset Repositories in *Creating Experiences with Oracle Content and Experience Cloud*.

   Collection owners will automatically be granted the manager resource role to the repository when they migrate their collections.
3. Let your site administrator know that he or she can configure the repository for migration.

> **WARNING:**
>
> After you configure a repository for migration, you won't be able to delete it until all collections have been successfully migrated. You can leave the repository in place indefinitely and delete it later if needed.

Site Administrator Configures Repository for Migration

The site administrator needs to configure the repository for the migrated content.

1. Sign in to Oracle Content and Experience Cloud as the site administrator.
2. Open the Asset Migration tool by navigating to `https://service_name-identity_domain_name.documents.dc.cloud.oracle.com/documents/assets/migration`.

   For example, if `salesdocuments1` is your service name, `mydomain` is your identity name, and the data center (*dc*) is `us2`, you would access the migration tool by

navigating to `https://salesdocuments1-mydomain.documents.us2.cloud.oracle.com/documents/assets/migration`.

3. On the Asset Migration page, click **Setup**.
4. In the Migration Setup dialog, select the repository you want to configure to store migrated content.
5. Let the collection owners know that they can start migrating their collections.

Collection Owners Migrate Their Collections

Each collection owner migrates their collections and the associated assets to the new repository so the assets are ready for use.

When you migrate digital assets, the published version is migrated. If it was never published, the latest version is migrated. Prior revisions aren't migrated.

Before migrating a site collection, bring the site offline.

1. Sign in to Oracle Content and Experience Cloud.
2. Open the Asset Migration tool by navigating to `https://service_name-identity_domain_name.documents.dc.cloud.oracle.com/documents/assets/migration`.

   For example, if `salesdocuments1` is your service name, `mydomain` is your identity name, and the data center (*dc*) is `us2`, you would access the migration tool by navigating to `https://salesdocuments1-mydomain.documents.us2.cloud.oracle.com/documents/assets/migration`.
3. By default, you see all the collections you own. Filter the list of collections to those that are ready for migration. In the menu, select **Ready**.
4. Select the collection you want to migrate, and then click **Migrate**. You can migrate only one collection at a time.
5. Confirm that you want to migrate the collection.

   If there's already a collection with that name, the newly migrated collection will be renamed to avoid conflict. For example, "Collection A" becomes "Collection A(1)". The collections will not be merged in the new repository.

   The collection will show that migration is in progress. Oracle Content and Experience Cloud migrates the collection, its content types, its content items, and its digital assets to the new repository. If the collection is associated with a site, Oracle Content and Experience Cloud creates a new publishing channel, assigns it to the repository, associates it with the site, and targets all associated assets to the publishing channel.
6. When migration has completed successfully, you need to republish all the migrated assets and sites.

If there are collections that you no longer use or don't want to migrate, you can "skip" them. Skipping a collection means that the assets won't be migrated and won't be able to be used going forward.

> **WARNING:**
>
> If you mark a collection as skipped, it will be lost forever the next time the cleanup service runs. There is no way to retrieve the collection after it's been skipped. You can instead just leave a collection as "ready" for migration if you aren't absolutely sure you want to get rid of the collection permanently.

To skip a collection:

1. Select one or more collections, and then click **Skip Migration**.
2. Confirm that you want to skip migration for the selected collections.

   The collection will show that migration has been marked as skipped.

To view the status of your collections, you can look at the status messages displayed when viewing all your collections, or you can filter your collections by status:

- **Ready** — the collections that are ready to be migrated and haven't previously been attempted to migrate.
- **Skipped** — the collections that have been marked skipped (that won't be migrated and therefore won't be able to be used going forward).
- **Complete** — the collections that have been successfully migrated.
- **In Progress** — the collections that are in the process of being migrated.
- **Error** — the collections that had errors during migration.

For migrations that completed successfully or migrations that had errors, you can view detailed information about the migration. Select the collection, and then click **Show Result**.

The following information is displayed:

- Collection Name
- Collection ID (if you experience any problems and contact Oracle Support, you'll be asked for this number)
- Site Name (if the collection belongs to a site)
- Migration Status
- Start Time
- End Time
- Migrated Collection (if the collection was migrated with or without errors)
- Error (if there is an error in migration)
- Details (if there is an error in migration)
- Failures (if the collection was migrated with errors)

Troubleshooting

If a collection migration fails (status shows "Error in Migration"):

- You can try to migrate again.

- You can skip the migration. Again, the collection will be permanently deleted, so choose this option only when you are positive the collection content will never be needed.
- You can show the result, and, if necessary, contact Oracle Support. Copy the information in the Migration Result dialog, and save it to share with Oracle Support.

4
Configure Service Settings

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

- Configure General Settings
- Configure Security Settings
- Configure User Settings
- Configure Documents Settings
- Configure Tags and Metadata
- Configure Sites and Assets Settings

Configure General Settings

General settings include 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:

- Apply Custom Branding and URLs
- Enable or Disable Email Notifications
- Set the Default Time Zone and Language

Apply Custom Branding and URLs

You can customize Oracle Content and Experience Cloud by adding your own logo and other branding customizations, as well as 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 and Experience Cloud web application as an administrator, click **Settings** 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 and Experience Cloud”, 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 Logo:** Add an image to use as a logo for your customized service. The logo image can’t be bigger than 160 pixels wide by 22 pixels high. Larger images will be resized.

- **Download Apps URL:** Enter the path to the location of the Oracle Content and Experience Cloud 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 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 and Experience Cloud.

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

To enable email notifications:

1. After you sign in to the Oracle Content and Experience Cloud web application as an administrator, click **Settings** in the Administration area of the navigation menu.
2. On the **General** page, under **Notifications**, click **Enabled** if you want the system to send email notifications to users.
3. Save the **General** page.

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 resaves 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 *Managing Content with Oracle Content and Experience Cloud*.

Set the Default Time Zone and Language

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 *Managing Content with Oracle Content and Experience Cloud*.

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

1. After you sign in to the Oracle Content and Experience Cloud web application as an administrator, click **Settings** in the Administration area of the navigation menu.
2. On the **General** page, under **Time Zone and Language**, select a default time zone, language, and date/time format.

   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.

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:

- Understand Cross-Origin Resource Sharing (CORS)
- Enable Cross-Origin Resource Sharing (CORS)
- Embed Content in Other Domains

Understand Cross-Origin Resource Sharing (CORS)

Cross-Origin Resource Sharing (CORS) allows a web page to make requests such as `XMLLHttpRequest` to another domain. If you have a browser application that integrates with Oracle Content and Experience Cloud but is hosted in a different domain, add the browser application domain to Oracle Content and Experience Cloud'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 and Experience Cloud 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 and Experience Cloud'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 and Experience Cloud, you need to 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 and Experience Cloud's domain) that will be served by Oracle Content and Experience Cloud, 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 and Experience Cloud to a connected client in another domain, you need to add a back channel CORS origin. For example, Oracle Content and Experience Cloud 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 and Experience Cloud, you need to add the domain to both the front and back channel CORS origins lists.

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

Enable Cross-Origin Resource Sharing (CORS)

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

1. After you sign in to the Oracle Content and Experience Cloud web application as an administrator, click **Settings** in the Administration area of the navigation menu.
2. In the **Settings** 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 and Experience Cloud calls (documents, social, and content as a service).

Embed Content in Other Domains

You can display content from Oracle Content and Experience Cloud within other domains. For example, you might embed the Oracle Content and Experience Cloud 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 and Experience Cloud web application as an administrator, click **Settings** in the Administration area of the navigation menu.

2. In the **Settings** 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 and Experience Cloud web user interface, see Embed the Web User Interface in *Developing for Oracle Content and Experience Cloud*.

Configure User Settings

You can configure default resource roles, synchronize user profile data, and manage Oracle Content and Experience Cloud settings on individual users through the **Users** page of Oracle Content and Experience Cloud Administration: Settings.

For information on creating or importing users, changing users' roles, modifying users' information, resetting users' passwords, unlocking accounts, and removing users, see Add Users.

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

- 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
- Change Temporary Quota for a User
- Transfer File Ownership
- Revoke Access to Linked Devices

Finding a User

You must find the user that you're interested in before you can edit the user's properties.

You can view a list of administrators by selecting the **Administrators** tab, or you can search for an individual user on the **Search** tab.

To find an individual user, enter part of the user name, display name, or email address in the text box and click **Search**. All matching user accounts are listed.

The user list shows some basic information about the users, including the name, email address, user type, and verification status.

Verified user accounts have been verified using one of these 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, and the user clicked the link in that email to verify their identity and signed in.

You can also see a list of users that have been deleted by selecting the **Deprovisioned Users** tab. To download a CSV file of all deleted users, click **Export Deprovisioned Users**.

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 and Experience Cloud web application as an administrator, click **Settings** in the Administration area of the navigation menu.
2. In the **Settings** 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 users' existing profile information with the information from your identity store. You can update all users' profile data or just the data for one user:

1. After you sign in to the Oracle Content and Experience Cloud web application as an administrator, click **Settings** in the Administration area of the navigation menu.
2. In the **Settings** menu, click **Users**.
   - To update all users' profile data, click **Sync Profile Data**.
   - To update a specific user's profile data, 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

You can set the default display setting for conversation membership messages for users .

1. After you sign in to the Oracle Content and Experience Cloud web application as an administrator, click **Settings** in the Administration area of the navigation menu.
2. In the **Settings** 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

1. After you sign in to the Oracle Content and Experience Cloud web application as an administrator, click **Settings** in the Administration area of the navigation menu.
2. In the **Settings** 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**.

Change Temporary Quota for a User

For large file uploads, a service administrator can change the temporary quota for a user.

1. After you sign in to the Oracle Content and Experience Cloud web application as an administrator, click **Settings** in the Administration area of the navigation menu.
2. In the **Settings** 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**.

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 and Experience Cloud web application as an administrator, click **Settings** in the Administration area of the navigation menu.
2. In the **Settings** 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 and Experience Cloud 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 and Experience Cloud and delete all local content stored on the device.

1. After you sign in to the Oracle Content and Experience Cloud web application as an administrator, click **Settings** in the Administration area of the navigation menu.
2. In the **Settings** 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.

Configure Documents Settings

Documents settings include user quotas, link settings, file restrictions, and more.

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

- Set User Quotas and Manage Storage Space
- Set Default Link Behavior
- Restrict File Types and Sizes
- Set Virus Scanning Options

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 and Experience Cloud web application as an administrator, click **Settings** in the Administration area of the navigation menu.
2. In the **Settings** menu, click **Documents**.
3. Under **Quota**, set these defaults:
   - **Default quota per user:** Specify the amount of storage space per user in gigabytes. Enter a value between 1 and 999.
   - **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.

To view the amount of storage used and override the storage quota for a particular user, see Override Storage Quota for a User.

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 and Experience Cloud web application as an administrator, click **Settings** in the Administration area of the navigation menu.
2. In the **Settings** 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**.
   - **Access Options**: If you enabled public links, you can specify whether users can send public links to anyone (**Anyone**) or only to those people who have an Oracle Content and Experience Cloud 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 that 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.

Restrict File Types and Sizes

You can limit the types of files that can be uploaded and the size of those files.

1. After you sign in to the Oracle Content and Experience Cloud web application as an administrator, click **Settings** in the Administration area of the navigation menu.
2. In the **Settings** menu, click **Documents**.
3. Under **File Restrictions**, set these defaults:
   - **Maximum upload and sync file size:** Enter the maximum file size in megabytes.
   - **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`).

Set Virus Scanning Options

You can choose what kind of virus scanning will be performed on the content uploaded to your service.

1. After you sign in to the Oracle Content and Experience Cloud web application as an administrator, click **Settings** in the Administration area of the navigation menu.
2. In the **Settings** menu, click **Documents**.
3. To run a virus scan on files during upload, under **File Restrictions**, enable **Scan all files upon upload**. Infected files are rejected.
4. If you enabled virus scanning, and you don't want users to be able to upload files that can't be checked for viruses, such as password-protected PDF files, enable **Reject file types that can't be scanned**.

Virus scanning can fail in the following cases, and files will be marked as infected:

- 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 you want to allow these kinds of files to upload, you must disable rejecting files that can't be scanned.

> **Note:**
>
> If a file doesn't pass virus scanning, it can't be downloaded through a public link.

If you disable or limit the virus scan, 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 and Experience Cloud 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.

Configure Tags and Metadata

Tags and metadata help users find the content they're looking for.

From the **Tags and Metadata** page, you can perform the following actions:

- Manage Hashtags
- Configure Custom Properties (Metadata)

Manage Hashtags

You can prevent specific words from being managed as hashtags. For example, if a user types a censored hashtag, it does not display as a link and is not included in hashtag search results.

1. After you sign in to the Oracle Content and Experience Cloud web application as an administrator, click **Settings** in the Administration area of the navigation menu.
2. In the **Settings** menu, click **Tags and Metadata**.
3. Under **Manage Hashtags**, enter a comma-separated list of hashtags, without the # symbol. For example:

   ```
   banthistag, banthisothertag
   ```

Configure Custom Properties (Metadata)

You can add metadata through custom properties so that users can quickly categorize files and folders with additional descriptions, known as metadata. For example, perhaps you need to track the effective date of a policy. You could create a custom

property 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.

You, as service administrator, create the custom properties 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 custom properties to files and folders. People with the Viewer or Downloader role can view any properties that are set.

To create custom properties:

1. After you sign in to the Oracle Content and Experience Cloud web application as an administrator, click **Settings** in the Administration area of the navigation menu.
2. In the **Settings** menu, click **Tags and Metadata**.
3. Next to **Custom Properties**, click **New Group** to create a group of fields associated with the property.
4. Enter a name for the property.
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**).
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 custom property fields will appear to users, click the property.

To add new fields, edit fields, or delete the property, click ⋯.

When you’re done creating properties, select **Enabled** to make them appear in the user interface for files and folders.

Configure Sites and Assets 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 and Experience Cloud 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.

1. After you sign in to the Oracle Content and Experience Cloud web application as an administrator, click **Settings** in the Administration area of the navigation menu.
2. In the **Settings** drop-down menu, choose **Sites and Assets**.
3. You can select settings for the following options:
   - **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.

- **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 *Creating Experiences with Oracle Content and Experience Cloud*.

- **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 and Experience Cloud 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*. See User Roles.

  - **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 *Creating Experiences with Oracle Content and Experience Cloud*.

- **Allow sharing of sites and themes from UI**: Select **Enabled** to allow users to share sites and themes with other Oracle Content and Experience Cloud 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.

  This option disables sharing 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. See *Developing for Oracle Content and Experience Cloud*.

- **Only site administrators can create sites**: Select **Enabled** to restrict the ability to create sites to users with the site administrator user role.
- **Only site administrators can create templates**: Select **Enabled** to restrict the ability to create templates to users with the site administrator user role.
- **Only site administrators can create components**: Select **Enabled** to restrict the ability to create components to users with the site administrator user role.

4. 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 and Experience Cloud. 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.

5. Under **Assets**, configure the **Maximum number of custom renditions per asset**. The default is 20.

See Use Site Governance and Creating and Managing Sites in *Creating Experiences with Oracle Content and Experience Cloud*.

5
Integrate the Service

You can integrate Oracle Content and Experience Cloud with your business applications. Integrations include Process Cloud Service, Eloqua Cloud Service, Visual Builder Cloud Service, embedded content, custom applications, and an integrated proxy service.

From the **Integrations** page, you can select an application for integration with Oracle Content and Experience Cloud, configure content connectors to third-party content repositories, and configure proxy service settings. You can also add custom actions created with the Application Integration Framework (AIF) to change the menu options for your users, add pop-up dialogs, and evaluate data entered into forms.

> **Note:**
>
> Some of these features are currently unavailable if you have a Universal Credits subscription.

Topics

- Understand Integrations
- Use the REST APIs, Sites SDK, and Content Delivery SDK
- Understand Cross-Origin Resource Sharing (CORS)
- Enable Cross-Origin Resource Sharing (CORS)
- Configure Proxy Service Settings
- Debug Proxy Service Endpoints
- Embed the Web Interface
- Manage Custom Applications
- Embed Content in Other Domains
- Configure Sites Settings
- Map a Site URL
- Integrate with Oracle Process Cloud Service
- Integrate with Oracle Eloqua Cloud Service
- Integrate with Oracle Visual Builder Cloud Service
- Integrate with Oracle Policy Automation
- Integrate with Oracle Cobrowse Cloud Service
- Configure Content Connectors to Third-Party Content Repositories

Understand Integrations

Oracle Content and Experience Cloud can be integrated multiple ways with applications that your organization relies on to be successful in day-to-day operations.

> **Note:**
>
> Some of these features are currently unavailable if you have a Universal Credits subscription.

For example, your sales portal could associate each sales opportunity with its own shared folder and conversations in Oracle Content and Experience Cloud to give your sales team quick, easy, and contextual access to the latest content and discussions. No more outdated or missing information when you need it.

- As an Oracle Platform as a Service (PaaS) offering, Oracle Content and Experience Cloud works seamlessly with other Oracle Cloud services. And the developer platform lets you integrate your custom applications through REST APIs and embeddable user interfaces. See Use the REST APIs, Sites SDK, and Content Delivery SDK and Embed the Web Interface.
- Cross-Origin Resource Sharing (CORS) allows a web page to make requests such as XMLLHttpRequest to another domain. If you have a browser application that integrates with Oracle Content and Experience Cloud but is hosted in a different domain, add the browser application domain to Oracle Content and Experience Cloud's CORS origins list. See Enable Cross-Origin Resource Sharing (CORS).
- Oracle Content and Experience Cloud includes a proxy service, so that you can use REST services which have Cross-Origin Resource Sharing (CORS) limitations or require service account credentials. See Configure Proxy Service Settings.

  > **Note:**
  >
  > This feature is currently unavailable if you have a Universal Credits subscription.

- You can use Application Integration Framework (AIF) to create your own custom applications to change the menu options your users see, add pop-up dialogs as needed, and evaluate data being entered into forms. See Manage Custom Applications.
- If you just want to display *content* from Oracle Content and Experience Cloud in another web application, you can specify a list of domains where the content is allowed to be embedded. See Embed Content in Other Domains.
- With sites integration, your users can easily create and publish websites. All site assets stay secure in Oracle Content and Experience Cloud, always current and timely. See Configure Sites and Assets Settings.
- When integrating with Oracle Process Cloud Service, you can automate business-driven, company-specific processes, such as employee on-boarding or IT service requests, and incorporate those processes into Oracle Content and Experience Cloud. See Integrate with Oracle Process Cloud Service.

- You can integrate with Oracle Eloqua Cloud Service to plan and execute automated marketing campaigns while delivering a personalized customer experience for your prospects. See Integrate with Oracle Eloqua Cloud Service.

> **Note:**
>
> This feature is currently unavailable if you have a Universal Credits subscription.

- Integrate Oracle Visual Builder Cloud Service (VBCS) to rapidly create web and mobile applications with minimal to no coding. See Integrate with Oracle Visual Builder Cloud Service.
- You can integrate Oracle Policy Automation (OPA) to implement online ‘interview” scenarios, such as feedback for troubleshooting or eligibility assessments for services. See Integrate with Oracle Policy Automation.
- Integrate with Oracle Cobrowse Cloud Service to enable users to share screens or initiate a cobrowsing session with another person. See Integrate with Oracle Cobrowse Cloud Service.
- When Oracle Content and Experience Cloud is used with Oracle WebCenter Content, you have a truly comprehensive hybrid enterprise content management solution, with a unified ECM infrastructure and security from a single vendor.

Use the REST APIs, Sites SDK, and Content Delivery SDK

REST Application Programming Interfaces (APIs) let you access Oracle Content and Experience Cloud functionality to create your own integrations within the service or across services. The Sites Software Development Kit (SDK) includes JavaScript calls that let applications interact with the underlying site architecture. The Content Delivery SDK lets applications interact with the Content Delivery REST API to retrieve structured content, digital assets, and content layouts.

Because the REST APIs are called from JavaScript code that runs in a browser, they rely on Cross-Origin Resource Sharing (CORS) to make HTTP calls to the Oracle Content and Experience Cloud server. An administrator must register the REST API domain in the Oracle Content and Experience Cloud CORS origins list. See Enable Cross-Origin Resource Sharing (CORS).

REST API for Content Delivery

With the REST API for Content Delivery, you can interact with the content stored in Content and Experience Cloud sites. See Overview of the REST API for Content Delivery in *Developing for Oracle Content and Experience Cloud*. For API reference information and examples, see REST API for Content Delivery.

REST API for Conversations

With the REST API for Conversations, you can create and manage conversations in your cloud resources that enable real-time collaboration between individuals and teams and connect your business processes, enterprise applications, and content. See Overview of the REST API for Conversations in *Developing for Oracle Content and Experience Cloud*. For API reference information and examples, see REST API for Conversations.

REST API for Documents

With the REST API for Documents, you can manage folders, files, shares, public links, application links, and metadata collections. You can also get user information, access items in a user's home folder, and get version and resource information about the API. See Overview of the REST API for Documents in *Developing for Oracle Content and Experience Cloud*. For API reference information and examples, see REST API for Documents.

REST API for Users and Groups

With the REST API for Users and Groups, you can enable collaboration among users through conversations, manage users and one-on-one conversations, configure resources and services, and manage connections and access. For an overview, see Overview of the REST API for Users and Groups in *Developing for Oracle Content and Experience Cloud*. For API reference information and examples, see REST API for Users and Groups.

REST API for Content Management

With the REST API for Content Management, you can manage assets in Oracle Content and Experience Cloud. Assets include content items as well as digital assets and their renditions. For an overview, see Overview of the REST API for Content Management. For API descriptions, examples, and information about getting started, see *REST API for Content Management*.

Content Delivery SDK

The Content Delivery SDK for Oracle Content and Experience Cloud is a light-weight JavaScript wrapper that interacts with the Content Delivery REST API. This is a read-only SDK for retrieving structured content, digital assets, and content layouts that are managed in Oracle Content and Experience Cloud.

The Content Delivery SDK consists of two main modules:

- **ContentSDK**: the main entry-point object. The ContentSDK object lets you create *client* objects to access content based on your requirements.
- **ContentDeliveryClient** : a *client* object that is set up to access *published* content items and digital assets.

See Content Delivery SDK.

Sites SDK

The Sites SDK helps application developers communicate across inline frame and domain boundaries, get and set properties, and handle site events. See Oracle Content and Experience Sites SDK Reference in *Developing for Oracle Content and Experience Cloud* .

Understand Cross-Origin Resource Sharing (CORS)

Cross-Origin Resource Sharing (CORS) allows a web page to make requests such as `XMLLHttpRequest` to another domain. If you have a browser application that integrates with Oracle Content and Experience Cloud but is hosted in a different domain, add the

browser application domain to Oracle Content and Experience Cloud'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 and Experience Cloud 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 and Experience Cloud'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 and Experience Cloud, you need to 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 and Experience Cloud's domain) that will be served by Oracle Content and Experience Cloud, 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 and Experience Cloud to a connected client in another domain, you need to add a back channel CORS origin. For example, Oracle Content and Experience Cloud 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 and Experience Cloud, you need to add the domain to both the front and back channel CORS origins lists.

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

Enable Cross-Origin Resource Sharing (CORS)

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

1. After you sign in to the Oracle Content and Experience Cloud web application as an administrator, click **Settings** in the Administration area of the navigation menu.
2. In the **Settings** 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 and Experience Cloud calls (documents, social, and content as a service).

Configure Proxy Service Settings

Oracle Content and Experience Cloud includes a proxy service, so that you can use REST services that have Cross-Origin Resource Sharing (CORS) limitations or require service account credentials.

Oracle Content and Experience Cloud 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 endpoint). The proxy service explicitly adds CORS support to all endpoints and can optionally insert service account credentials to requests coming from web browsers.

> **Note:**
>
> - This feature is currently unavailable if you have a Universal Credits subscription.
> -

If you are using a REST server (or endpoint) which already supports CORS and doesn't require the use of service account credentials, you don't need to register it with the proxy service. You can instead register it directly with the Oracle Cloud REST API for Content Management. See Use the REST APIs, Sites SDK, and Content Delivery SDK.

1. After you sign in to the Oracle Content and Experience Cloud web application as an administrator, click **Integrations** in the Administration area of the navigation menu.
2. Under **Proxy Service**, select **Enable**.
3. Using the following steps, define any credentials needed by your endpoints, and define the endpoints you want to use the proxy service.

Credentials

When an endpoint uses a credential, the proxy service adds basic access authentication (via the HTTP Authorization header) to requests made by web browsers. If the browser request already includes the Authorization header, the browser request Authorization header will be used instead of the one in the credential.

This gives you the flexibility to provide a read-only credential for most requests, but allow individual requests to provide their own write-capable authentication as needed.

Providing a credential to an endpoint gives all users of the endpoint the same effective permissions granted to the user defined in that credential. To ensure you don't inadvertently create a security risk, take the following precautions:

- Don't provide a credential for an endpoint unless absolutely necessary. If possible, let the browser requests provide their own Authorization header instead.
- If you must provide a credential, try to use one which has read-only access on the target endpoint.
- Limit the allowed methods on the endpoint to what is actually required. Unless absolutely necessary, always disable the PUT, POST, and DELETE methods on an endpoint.
- When possible, limit the Target URI for the endpoint to a specific area of functionality. For example, rather than providing the base URI to the full API such as `http://example.api/`, you might be able to limit it to a specific area such as `http://example.api/weather/` (for weather-related requests) or `http://example.api/date/` (for date-related requests).

If an endpoint requires credentials, define a credential and select it in the endpoint definition:

1. Click **Create new Credential**, and complete the following information.
2. In the **Credential Name** box, enter a name for the credential that will make clear to other users what the credential is for (for example, `DocsAPIUser`).
3. In the **Username** box, enter the user that should be used to authenticate all requests with the endpoint.
4. In the **Password** box, enter the password for the user you entered.
5. In the **Keywords** box, optionally provide space-delimited keywords for the credential. Keywords are purely informational for your own needs and do not alter the functionality of the credential. Keywords can include alphanumeric characters, periods, hyphens, and underscores.

   The **Keywords** field is exposed by the proxy service API and can be viewed by non-administrator users. Never include user names, passwords, API keys, or other sensitive information in the **Keywords** field.
6. Click **Save**.

The new credential is available to use with one or more endpoints. It appears in the **Credential** drop-down list when you create or edit an endpoint.

Endpoints

1. Define the remote API endpoint you want to use the proxy service. Click **Create new Endpoint**, and complete the following information:
   a. In the Endpoint Name box, enter a name for the endpoint that will make clear to other users what this endpoint is (for example, `Content Management API 1.1`).
   b. Under **Enable Endpoint**, select **Enabled**.

      You can disable individual endpoints as necessary, rather than disabling the whole proxy service.

c. In the **Path Name** box, enter a path name for the endpoint (for example, `docs`). This will become part of the URL path to access the endpoint (for example, `/pxysvc/proxy/docs`).

   The name must be unique, URL-safe, and lowercase, and it must start with a letter. It can include alphanumeric characters, hyphens, and underscores.

d. In the **Target URI** box, enter the URI for the endpoint (for example, `http://service.example.com/documents/api/1.1`).

e. Under **Credential**, if necessary, select the credentials to use for this endpoint. This list is populated by the credentials you created using the steps above.

f. Under **HTTP Methods**, select the HTTP methods you want to enable for this endpoint.

   GET and OPTIONS methods are always enabled.

g. In the **Keywords** box, optionally provide space-delimited keywords for the endpoint. Keywords are purely informational for your own needs and do not alter the functionality of the endpoint. Keywords can include alphanumeric characters, periods, hyphens, and underscores.

   The **Keywords** field is exposed by the proxy service API and can be viewed by non-administrator users. Never include user names, passwords, API keys, or other sensitive information in the **Keywords** field.

h. In the **Connection Timeout** box, enter the maximum number of seconds to wait when trying to make a connection with the target URI.

i. In the **Socket Timeout** box, enter the maximum number of seconds to wait for a pooled connection in the proxy service.

j. In the **Connection Request Timeout** box, enter the maximum number of seconds to wait when trying to make a connection with the proxy service.

k. Test your endpoint, by clicking **Save** and **Debug**. See Debug Proxy Service Endpoints.

l. When you're satisfied with the result, click **Save** and **Close**.

Debug Proxy Service Endpoints

You can quickly test a proxy service endpoint without writing any test code. This can be a valuable tool to see how requests and responses are handled between your web browser, the proxy service, and the target URI of the endpoint.

1. After defining the endpoint, test it by clicking **Save and Debug**.

   Alternatively, in the list of endpoints, click next to the endpoint you want to debug.

   At the top of the **Debug Endpoint** section, you see the **URI mapping**, which shows how the endpoint's local path name is mapped to the target URI of the endpoint. Both the local path and the target URI are links so you can make sure they are pointing to the correct locations.

2. Optionally, enter a user name and password and additional headers to use for the test request. These credentials will be used in lieu of any credential already set on the endpoint. This enables you to test or verify the use of credentials without making them available to all users of the endpoint.

3. Optionally, enter additional headers to use for the test request. Enter one header per line, using the standard format *Name: Value*. For example: `Content-Type: application/json`.
4. Select an HTTP method, then provide a complete path for the request.

   If you select **POST** or **PUT**, in the **Data** box, enter the content which should be sent in the POST or PUT request body.
5. Click **Submit Request**.
6. In the **Debug Result** section, expand the panels to see the detailed results:
   - **Browser Request to Proxy:** Displays the HTTP request headers and body sent by the web browser to the proxy service.
   - **Proxy Request to Endpoint:** Displays the HTTP request headers and body sent by the proxy service to the target URI of the endpoint. If the endpoint uses a credential, an authorization header is inserted in the request, but the header value isn't shown in the debug results.
   - **Endpoint Response to Proxy:** Displays the HTTP response headers and body sent by the target URI of the endpoint back to the proxy service.
   - **Proxy Response to the Browser:** Displays the HTTP response headers sent by the proxy service back to the web browser. If the target URI of the endpoint doesn't return CORS headers, the proxy service inserts them in its response to the browser.
7. If necessary, change the debug request and submit the request again.

   > **Note:**
   >
   > The old debug results are overwritten with the new results.

8. When you're satisfied with the result, click **Close**.

Embed the Web Interface

Embed the web user interface for Oracle Content and Experience Cloud into your own web applications to get access to the folder and document management features of the service.

These topics in *Developing for Oracle Content and Experience Cloud* describe how to embed the interface and use it to display content from other domains and access folders and files on Oracle Content and Experience Cloud from your applications:

- Embedding the Web User Interface
- Displaying Content from Other Domains
- Integrating Folder and File Selection

Manage Custom Applications

You can create custom applications using the Application Integration Framework (AIF).

With custom applications, you can change the menu options your users will see, add pop-up dialogs as needed, call third-party services, and specify how the results are presented to the user.

For details about creating applications using AIF, see Application Integration Framework Overview in *Developing for Oracle Content and Experience Cloud*.

After creating an application, you can add it to Oracle Content and Experience Cloud and manage it from the Administration interface.

1. After you sign in to the Oracle Content and Experience Cloud web application as an administrator, click **Integrations** in the Administration area of the navigation menu.
2. On the **Integrations** page, choose **Applications**.
3. To add an application, click **Add** next to **Custom Actions**, navigate to the configuration file that contains the application information, and select it.
4. After adding the application, you can enable or disable it by selecting or clearing the check box.

For details about creating applications using AIF, see Application Integration Framework Overview in *Developing for Oracle Content and Experience Cloud*.

After you add your application and enable it, you can manage it by clicking the appropriate icon for any of the following actions:

- View information about the application. What is shown is set by the application's `info` application property (for example, a popup window).
- Set the preferences for the application. What is shown is set by the application's `tenantPrefs` property.
- Edit the application. You can alter the application's code and click **Load** to test the application, save the application, or cancel your edit. Syntax errors will be identified, as well as some information about basic issues, such as allowed actions.
- Download the application. You can save the application or open it using an editor of your choice.
- Remove the application. When you delete an application, it is not moved to your trash. You will need to add the application file again if you want to use it.

When an application is disabled, you can only edit the application, download it, or delete it.

To view the preferences for all enabled applications, open your user menu, click **Preferences**, and then, in the **Preferences** menu, choose **Applications**. The preferences information is defined in the application itself, so it may launch a dialog or get information, but only as defined. You can view the information for the application and the preferences. The **Applications** option is not shown in the **Preferences** menu unless at least one application is enabled.

Embed Content in Other Domains

You can display content from Oracle Content and Experience Cloud within other domains. For example, you might embed the Oracle Content and Experience Cloud 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 and Experience Cloud web application as an administrator, click **Settings** in the Administration area of the navigation menu.
2. In the **Settings** 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 and Experience Cloud web user interface, see Embed the Web User Interface in *Developing for Oracle Content and Experience Cloud*.

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 and Experience Cloud 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.

1. After you sign in to the Oracle Content and Experience Cloud web application as an administrator, click **Settings** in the Administration area of the navigation menu.
2. In the **Settings** drop-down menu, choose **Sites and Assets**.
3. You can select settings for the following options:
   - **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.

- **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 *Creating Experiences with Oracle Content and Experience Cloud*.

- **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 and Experience Cloud 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*. See User Roles.

  – **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 *Creating Experiences with Oracle Content and Experience Cloud*.

- **Allow sharing of sites and themes from UI**: Select **Enabled** to allow users to share sites and themes with other Oracle Content and Experience Cloud 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.

This option disables sharing 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. See *Developing for Oracle Content and Experience Cloud*.

- **Only site administrators can create sites**: Select **Enabled** to restrict the ability to create sites to users with the site administrator user role.
- **Only site administrators can create templates**: Select **Enabled** to restrict the ability to create templates to users with the site administrator user role.
- **Only site administrators can create components**: Select **Enabled** to restrict the ability to create components to users with the site administrator user role.

4. 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 and Experience Cloud. 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.

5. Under **Assets**, configure the **Maximum number of custom renditions per asset**. The default is 20.

See Use Site Governance and Creating and Managing Sites in *Creating Experiences with Oracle Content and Experience Cloud*.

Map a Site URL

Once a site is created and published using Oracle Content and Experience Cloud, you can configure the Domain Name System (DNS) so that this site is accessible with a registered domain name, such as www.mysite.com

A Domain Name System (DNS) specifies where someone can find your web pages by mapping your domain name to your site's location, or canonical name (CNAME).

To map your domain name, you'll need the following:

- The URL of your Oracle Content and Experience Cloud instance. It's typically of the form:

  `service-tenant.documents.datacenter.oraclecloud.com`

- The domain name as registered by your domain name registrar.

  For example, www.mysite.com. It could also be a sub-domain such as www.mysite.com/subdomain

- An account with a content delivery network (CDN) provider, such as Akamai.

Different Domain Name System providers have different interfaces and different steps for updating a CNAME record. The steps below provide the information you'll need and the general steps to follow.

To map the site URL to a domain name:

1. Request a secure sockets layer (SSL) certificate from your content delivery network provider for the domain. For example, https://www.mysite.com.
2. Configure the content delivery network so that:
   a. The content delivery network accepts all incoming requests to the domain and forwards them using secure protocol (https).
   b. The origin points to the domain from Oracle Content and Experience Cloud:

      `service-tenant.documents.datacenter.oraclecloud.com`
3. Change the DNS server zone file to map the domain name to the edge server provided by the content delivery network provider:

   domain CNAME *CDN Server*
4. Wait for the update to propagate. Depending on your DNS service, this can take anywhere from 2 to 48 hours.

   After the change is propagated, you can access the site using your domain name. For example:

   `https://www.mysite.com/site_name`

By default, the endpoint for the Oracle Cloud REST API for Content Management is available if you use the standard URL provided for the site. Folder and file list components, for example, use the REST API to perform folder and file operations. If you use a custom URL, verify that you have access to the endpoint with your domain name. For example:

`https://www.mysite.com/documents`

Integrate with Oracle Process Cloud Service

You can allow your users to access Oracle Process Cloud Service functionality, which lets users manage business processes in the cloud, such as document routing for approval or review.

> **Note:**
>
> Integration between these services requires SSO sign-ons, so both services must be in the same identity domain.

Integrating Oracle Content and Experience Cloud with Oracle Process Cloud Service benefits document-intensive processes by organizing, managing, and restricting access to documents that must be submitted, reviewed, and approved or rejected by different roles and organizations during the business process. Conversations enable users to easily discuss things that come up during the process.

Oracle Content and Experience Cloud integrates documents and conversations with your process applications.

- Documents: Oracle Process Cloud Service provides simple file attachment functionality, but if you need something more robust to handle document-intensive processes, you can integrate Oracle Content and Experience Cloud. This service enables you to organize files into folders, manage access to each folder, and even start a process when you upload a document. For example, if you're processing a home loan, you need to manage documents such as loan applications, employment histories, and house appraisals, making sure that the right users see the documents they need to submit, review, or approve, but they don't get access to restricted information.
- Conversations: When you integrate conversations, users can easily discuss things that come up during the process. This provides a record of what happened, enabling you to quickly bring new stakeholders up to speed or refer back to things as necessary. Plus, the conversation tools work like the social media tools users regularly use, but with enterprise-wide security and controls. For example, if you're working on a contract you might need to discuss some of the terms, while still making sure your discussion is confidential.
- Document- and Folder-Initiated Processes: You can automatically start a process when someone uploads a document (or folder of documents) to a chosen document folder.

You must configure settings in both Oracle Process Cloud Service and Oracle Content and Experience Cloud before users can take advantage of the integrated functionality. For an overview, see the video Integrate Oracle Documents with Oracle Process Cloud Service.

To configure Oracle Content and Experience Cloud to integrate with Oracle Process Cloud Service:

1. Enable the integration and enter connection information.
   a. After you sign in to the Oracle Content and Experience Cloud web application as an administrator, click **Integrations** in the Administration area of the navigation menu.
   b. Under **Oracle Integrations**, select **Process Cloud Service Integration** to enable the service, and then set these values:
      - **Service URL:** The URL of the service that users can access for their applications:
        - If you have Universal Credits subscription, your Service URL should look something like this: `https://servicename/ic/api/process/v1/processes`.
        - If you have a non-metered subscription, your Service URL should look something like this: `https://servicename/bpm/api/3.0/processes`.
      - **Service User:** Enter the email address of the user who owns the process to be used in Oracle Content and Experience Cloud. This must be the same user you entered in Oracle Process Cloud Service.
      - **Service Password:** Enter the user password. This must be the same password you entered in Oracle Process Cloud Service.

2. In Oracle Content and Experience Cloud, enable Oracle Process Cloud Service use for the desired folders.
   a. In Oracle Content and Experience Cloud, open the properties for the folder.
   b. Enable Oracle Process Cloud Service use.
   c. Select a process from the list.

   If the process list is blank, it's caused by one of the following issues:

   - The Oracle Process Cloud Service user you specified in step 2 doesn't have rights to see the processes.
   - The Oracle Process Cloud Service URL you specified in step 2 isn't correct.
   - The Oracle Process Cloud Service user/password combination you specified in step 2 isn't correct.
   - The Oracle Process Cloud Service doesn't have a process that uses a Documents Start Event. To create a process with a Document Start Event, see Creating a Document- or Folder-Initiated Process in *Using Processes in Oracle Integration Cloud*.

After both services have been configured for integration, Oracle Process Cloud Service users can take actions (such as approvals) on the files directly in Oracle Process Cloud Service. Oracle Content and Experience Cloud users can upload files into folders to initiate a workflow associated with the folder. Oracle Content and Experience Cloud site designers can create web pages with ready-to-use components that provide folder and file access, process selection and initiation, associated conversation display and interaction and much more.

Integrate with Oracle Eloqua Cloud Service

Oracle Eloqua Cloud Service enables you to plan and execute automated marketing campaigns while delivering a personalized customer experience for your prospects.

You can let Oracle Eloqua Cloud Service users select content from Oracle Content and Experience Cloud to include in their marketing campaigns. After you enable integration in both Oracle Content and Experience Cloud and Oracle Eloqua Cloud Service, Eloqua users see Oracle Content and Experience Cloud in the **Apps** menu, allowing them to select any content they have access to.

Create the Oracle Content and Experience Cloud App in Eloqua

To create the Oracle Content and Experience Cloud app and menu service, perform the following steps in Oracle Eloqua Cloud Service:

1. Create the app:
   a. Click , and then select **AppCloud Developer**.
   b. Click **Create App**.
   c. Set the following values:
      i. **Name:** Enter a name for the app (for example, `Oracle Content and Experience Cloud`).
      ii. **Description:** Enter a description for the app so that users know what the app does.

iii. **Icon:** Enter the URL to the icon image:

```
https://<OracleContentAndExperienceCloud_Host>/
documents/static/img/docs-app-icon.png
```

Replace `<OracleContentAndExperienceCloud_Host>` with your company's Oracle Content and Experience Cloud host. For example:

```
https://documents.xyzcompany.com/documents/static/img/
docs-app-icon.png
```

iv. Click **Save**.

2. Create the menu service:
   a. Under **Services**, click **Add Services**.
   b. Click **Add Menu Service**.
   c. Enter the same **Name**, **Description**, and **Icon** values you entered when creating the app.
3. Configure the visibility settings and style:
   a. **User Access:** Select where in Eloqua (for example, in Email or My Eloqua) you want the app to be visible in the **Apps** menu.
   b. **Default View:** Select whether the app should always be visible, or only when users are editing assets (**Only visible for a selected asset**).
   c. **Action URL:** Enter the following URL:

```
https://<OracleContentAndExperienceCloud_Host>/documents/
embed/folder/home/deloqua/nameasc/lyt=list/cfg=nvw,hbr,sdo
```

Replace `<OracleContentAndExperienceCloud_Host>` with your company's Oracle Content and Experience Cloud host. For example:

```
https://documents.xyzcompany.com/documents/embed/folder/
home/deloqua/nameasc/lyt=list/cfg=nvw,hbr,sdo
```

   d. **Content Display Layout:** Select **Drawer (430x796px)**, otherwise the menu service page launches in a new web browser tab.
   e. Click **Save**.

The app is installed in AppCloud developer.

Install the Eloqua Menu Service App

1. In the breadcrumb, navigate up one level. This corresponds to the name of your new app.
2. Under **Lifecycle Setup**, click **Start App**.
3. Under **Install URL**, click the URL to start the installer for your app.
4. Click **Accept and Install**.
5. Sign out of Oracle Eloqua Cloud Service for the changes to take effect.

   The Oracle Content and Experience Cloud app is now visible in **Apps** menu.

Create an Eloqua User for Oracle Content and Experience Cloud

You must create an Eloqua user for Oracle Content and Experience Cloud actions. You'll enter this user name when configuring Eloqua in Oracle Content and Experience

Cloud, and all content copied from Oracle Content and Experience Cloud to Eloqua will be added by this user.

Configure Eloqua in Oracle Content and Experience Cloud

1. After you sign in to theOracle Content and Experience Cloud web application as an administrator, click **Integrations** in the Administration area of the navigation menu.
2. Under **Oracle Integrations**, select **Eloqua Cloud Service Integration** to enable the service.
3. Set the following values in the dialog box, and then click **Save**:
   - **Service User:** Enter the name of the Eloqua user you created for Oracle Content and Experience Cloud. Use the following format:

     `<Company_Name>\<User_Name>`

     For example:

     `XYZCompany\Cathy.Woods`

     Service Password: Enter the password for the Eloqua user.
4. In the **Administration** menu, click **Security**.
5. In the **Embedded Content** section, select **Enabled**.
6. In the **Allowed domains** box, enter `*.eloqua.com`, and then click **Save**.

Use the Oracle Content and Experience Cloud App in Eloqua

1. While editing a marketing asset, such as an email template, click to open the **Apps** menu.
2. Click the Oracle Content and Experience Cloud app.

   Your administrator might have named the app something else. If you can't find the app, contact your administrator.
3. Click **Select Assets**. You might be prompted for your Oracle login information.
4. In the Documents file picker, select one or more files you want to use in Eloqua, and then click **Copy to Eloqua**. Content that is classified as images is copied to the Images Components Library into a directory called **Documents-Images**. Content that is not classified as images is copied to the File Storage Components Library into a directory called **Documents-Files**.

   If the file you select has a file name with more than 100 characters, copying to Eloqua will fail. You must edit the file name in Oracle Content and Experience Cloud before you can copy the file to Eloqua.

   When you copy files from Oracle Content and Experience Cloud to Oracle Eloqua Cloud Service, they aren't synchronized, so any changes made in Oracle Content and Experience Cloud won't be copied to Oracle Eloqua Cloud Service.

   If you want to upload a file to Oracle Content and Experience Cloud, click **Upload**, and then select a file from your computer. After uploading the file Oracle Content and Experience Cloud, you must copy it to Eloqua as described above.
5. When you're done, click **Close**.

For information on additional Oracle Content and Experience Cloud features available in the file picker, see ManageYour Files and Folders in *Managing Content with Oracle Content and Experience Cloud*.

Integrate with Oracle Visual Builder Cloud Service

You can let your users access Oracle Visual Builder Cloud Service functionality. Oracle Visual Builder Cloud Service (VBCS) is a hosted environment for your application development infrastructure. It provides an open-source standards-based integration to develop, collaborate on, and deploy applications within Oracle Cloud. This enables users to rapidly create web and mobile applications with minimal to no coding.

> **Note:**
>
> This feature is currently unavailable if you have a Universal Credits subscription.

Integration between these services requires SSO, so both services must be in the same identity domain.

Only administrators with the *enterprise user* role can enable integration with VBCS. If you aren't an enterprise user, the **Visual Builder Cloud Service Integration** option is grayed out.

On the VBCS side, the following must be done before this feature can be used with Oracle Content and Experience Cloud:

- Cross-Origin Resource Sharing (CORS) must be enabled on the VBCS site. See Allow Other Domains Access to Services in *Administering Visual Builder in Oracle Integration Cloud*.
- Apps must be created and made available for embedding. See Creating a New Web Application in *Using Visual Builder in Oracle Integration Cloud*.
- The apps must be configured for use with Oracle Content and Experience Cloud. See Embedding the Application in *Using Visual Builder in Oracle Integration Cloud*.
- Web applications must be created and made available for embedding in an iframe.
- The Sites SDK must be imported.
- The Sites SDK must be referenced in the web applications.
- A page URL parameter called "id" must be added to the web applications.

On the Oracle Content and Experience Cloud side, you need to configure integration with VBCS:

1. After you sign in to theOracle Content and Experience Cloud web application as an administrator, click **Integrations** in the Administration area of the navigation menu.
2. Under **Oracle Integrations**, select **Visual Builder Cloud Service Integration** to enable the service.

3. Enter the **Service URL** of the Oracle Visual Builder Cloud Service.

> **Note:**
>
> If you have Universal Credits subscription, you must include `ic/builder` in your Service URL. For example, `https://vbcsserver.example.com/ic/builder`.

After both services have been configured for integration, Oracle Content and Experience Cloud users can create components for your VBCS apps and add them to site pages. See Oracle Visual Builder Cloud Service in *Creating Experiences with Oracle Content and Experience Cloud*.

Integrate with Oracle Policy Automation

You can let your users access Oracle Policy Automation functionality. Oracle Policy Automation (OPA) is used to implement online "interview" scenarios, such as feedback for troubleshooting or eligibility assessments for services. It delivers advice across channels by capturing rules in natural-language Microsoft Word and Excel documents, then building interactive customer service experiences called interviews around those rules.

Only administrators with the *enterprise user* role can enable integration with OPA. If you aren't an enterprise user, the **Oracle Policy Automation Cloud Service Integration** option is grayed out.

> **Note:**

On the OPA side, interviews must be created and stored on the host site. In addition, the OPA administrator must add the Oracle Content and Experience Cloud domains (*.documents.* and *.sites.*) to the list of hosts authorized to embed interviews. See the Oracle Policy Automation documentation.

On the Oracle Content and Experience Cloud side, you need to configure integration with OPA:

1. After you sign in to the Oracle Content and Experience Cloud web application as an administrator, click **Integrations** in the Administration area of the navigation menu.
2. Under **Oracle Integrations**, select **Oracle Policy Automation Cloud Service Integration** to enable the service, and then set these values:
   - **Service URL:** Enter the URL of the Oracle Policy Automation Cloud Service.
   - **Service User:** Enter the name of the OPA user. This user must be an Integration user and must have the *Deploy Admin* role for the OPA collections.
   - **Service Password:** Enter the user password.

After both services have been configured for integration, Oracle Content and Experience Cloud users can add an OPA component to site pages. See Oracle Policy Automation in *Creating Experiences with Oracle Content and Experience Cloud*.

Integrate with Oracle Cobrowse Cloud Service

You can let your users access Oracle Cobrowse Cloud Service functionality, which lets users share screens or initiate a cobrowsing session with another person. For example, you might want to use cobrowse on a sales site so that a sales representative can help a customer select appropriate products or services on the site.

Only administrators with the *enterprise user* role can enable integration with Oracle Cobrowse Cloud Service. If you aren't an enterprise user, the **Oracle Cobrowse Cloud Service Integration** option is grayed out.

To integrate with Oracle Cobrowse Cloud Service:

1. After you sign in to the Oracle Content and Experience Cloud web application as an administrator, click **Integrations** in the Administration area of the navigation menu.
2. Under **Oracle Integrations**, select **Oracle Cobrowse Cloud Service Integration** to enable the service, and then set these values:
   - **Service URL:** Enter the URL for the Cobrowse service. See Log in to the Agent Console in the *Standalone Cobrowse User Guide* for the link (for example, `https://www.livelook.com`).
   - **Service User:** Enter the Oracle Cobrowse Cloud Service administrator user name.
   - **Service Password:** Enter the user's password.

After you've configured the integration, Oracle Content and Experience Cloud users can enable cobrowse to work with a site and add the Cobrowse Launcher component to a site page. See Enabling Cobrowse Integration and Using Cobrowse on a Page in *Creating Experiences with Oracle Content and Experience Cloud*.

If you later decide to disable cobrowse, you must disable the option on the **Integrations** page and in the site settings for any sites that use cobrowse. If you disable only the option on the **Integrations** page, any sites that use cobrowse will continue to do so, but users won't be able to add new cobrowse functionality.

Configure Content Connectors to Third-Party Content Repositories

A developer or service administrator can configure content connectors so Oracle Content and Experience Cloud users can retrieve content from storage providers, including Google Drive, Microsoft OneDrive, Dropbox, and WebCenter Content (WCC).

Your Oracle Content and Experience Cloud instance provides preconfigured Google Drive, OneDrive, Dropbox, and WCC connectors. You can configure Custom content connectors to other storage providers.

The following sections describe how a developer or service administrator can use the connector framework to configure content connectors:

- Enable a Connector
- Create and Configure a Custom Connector

- Provide Configuration Parameter Values for a Connector
- Disable a Connector
- Delete a Connector
- Configure a Google Drive Connector
- Configure a Dropbox Connector
- Configure a OneDrive Connector
- Configure WebCenter Content and OCE for the WCC Connector
- Create and Configure a Custom Connector

Enable a Connector

Content and Experience Cloud provides preconfigured content connectors for Google Drive, Microsoft OneDrive, and Dropbox. A service administrator can enable any or all of these through the Administration Integrations interface.

To enable a connector:

1. Click **Integrations** in the Administration area of the navigation menu.
2. On the **Integrations** page, go to the **Applications** drop-down menu and choose **Connectors**.
3. On the **Connectors** tab, click the **Configure** button next to a content connector: **Google Drive**, **Microsoft OneDrive**, **Dropbox**, or **WebCenter Content**.
4. On the **Connector Settings** page, you can change the following default information:
   - A user-friendly name, instead of `Google Drive`.
   - A description, instead of `Allow integration with Google Drive file storage service`.
   - An **Enabled For End Users** check box, which you can select to enable the connector or deselect to disable it.
   - A **Connector Service URL** a read-only field that becomes editable if the URL can't connect to the service. Once the URL can connect, it displays as read only again. Make note of the **Redirect URL** beneath the **Connector Service URL**.
   - A **Connector Tags** field, where you can assign connector tags so that assets pulled from a connector can be tagged with the connector name or with some tag that connector configures. This lets you search for all items from that connector in an asset repository.
5. Enter custom fields on the **Connector Settings** page.

   For information about the values for custom fields, see Configure a Google Drive Connector, Configure a Dropbox Connector, or Configure a OneDrive Connector.
6. Click the **Save** button to finish configuring the connector.

After a connector is configured, you can enable it by clicking the **Enable** button on the **Connectors** tab.

Provide Configuration Parameter Values for a Connector

A service administrator can register a connector on the cloud storage provider's website to get configuration parameter values to enter for the connector in Content and Experience Cloud (OCE).

Only one set of user credentials is stored for a logged in OCE user. If you need to use a separate user to fetch data, use Manage Sources and revoke the authorization for the existing user. Then you can use credentials for a second user.

1. Click **Integrations** in the Administration area of the navigation menu.
2. On the **Integrations** page, go to the **Applications** drop-down menu and choose **Connectors**.
3. On the **Connectors** tab, click the **Configure** button next to a content connector.
4. To get custom field information, go to the third-party content repository's website, like Google Developers, and register the connector as an application that you want to integrate.
5. Get custom field values for the connector from the third-party content repository and enter the values under **Custom Fields** on the **Connectors** tab in Content and Experience Cloud. For example, for the Google Drive connector, you need to enter values for the following fields:
   - **Client ID**
   - **Client Secret**
   - **Developer Key**
   - **App Id**

   Google Drive has more custom fields. The Microsoft OneDrive, Dropbox, and WebCenter Content connectors have different custom fields.
6. Click the **Save** button to save the configuration parameter values.

After a content connector is configured and enabled, it is available in the asset repository for Content and Experience Cloud users to download content, through the **Add From** drop-down menu on the **Assets** page.

Disable a Connector

A service administrator can use the connector framework to disable a connector in a Content and Experience Cloud instance at any time.

To disable a connector:

1. Click **Integrations** in the Administration area of the navigation menu.
2. On the **Integrations** page, go to the **Applications** drop-down menu and choose **Connectors**.
3. On the **Connectors** tab, click the **Disable** button next to a content connector: **Google Drive**, **Microsoft OneDrive**, **Dropbox**, or **WebCenter Content**.
4. Click the **Save** button to finish disabling the connector.

After a content connector is disabled, it is no longer available on the **Add From** drop-down menu on the Assets page, until it is enabled again. You can now click the **Enable** button to enable the content connector again.

You can also disable or enable a connector when you drill down to the **Connector Settings** page.

Delete a Connector

A service administrator can use the connector framework to delete a disabled connector in a Content and Experience Cloud instance at any time.

You cannot delete a delivered connector. You can only delete newly added connectors (custom connectors).

To delete a connector:

1. Click **Integrations** in the Administration area of the navigation menu.
2. On the **Integrations** page, go to the **Applications** drop-down menu and choose **Connectors**.
3. If the connector is enabled, click the **Disable** button on the **Connectors** tab next to the custom connector you want to delete.

   Or from the page that lists the connectors, you can click a connector and deselect the **Enabled For End Users** check box. On this page you need to click **Save** to finish disabling the connector.

   After a content connector is disabled, it is no longer available on the **Add From** drop-down menu on the **Assets** page.
4. Click the **Delete** button next to the custom connector, on the **Connectors** tab.

Configure a Google Drive Connector

After you configure and enable a Google Drive Connector, you can connect to Google Drive and pull required content from it into Oracle Content and Experience Cloud.

To configure a Google Drive connector:

1. Get the Oracle Content and Experience Cloud host name and authorization URL details.
   a. Sign in to Oracle Content and Experience Cloud.
   b. Click **Integrations** in the **Administration** area of the navigation menu on the left.
   c. On the **Integrations** page, go to the **Applications** drop-down menu and choose **Connectors**.
   d. On the **Connectors** tab, click the **Configure** button next to the Google Drive content connector.
   e. Note down the Redirect URL, which will be in this format:

   ```
   https://<hostname>.<domainname>.com:<port>/documents/web/
   AR_COMPLETE_AUTHORIZATION
   ```

The **Redirect URL** field is truncated. Double-click the field to copy the value to your clipboard.

f. You can override the default connector settings, as described in Enable a Connector.

   In the **Connector Tags** field, you can assign tags for assets that the connector pulls into Oracle Content and Experience Cloud.

2. Create a Google Drive app:

   a. Go to `https://console.developers.google.com/project` in a browser window.

   b. Sign in with a Google user name and password .

      If you have already created projects in the Google Developers Console, you will see the list of created projects. If not, the **Manage resources** screen will appear.

   c. Click the **Create Project** button.

      You will be redirected to a page where you can enter **Project Name** and **Project ID** values to help you recognize your project in the console.

   d. Click the **Create** button.

      Your project will be created, and you will be redirected to your projects list in the console.

   e. Go to the Dashboard through menu navigation, **APIs & Services** > **Dashboard**, from the left corner icon.

   f. Click the name of the project you recently created to go to your Project Dashboard.

   g. Select a library. Go to Library page through menu navigation, **APIs & Services** > **Library**, from the left corner icon.

   h. Search for the "Google Drive API" library, then select and enable it.

   i. Search for the "Google Picker API" library, then select and enable it.

   j. From the left corner icon, navigate to **APIs & Services** > **Credentials** > **OAuth Consent Screen** tab. Check your email address and enter your product name, **GDrivePickerApp**, and save it.

   k. Click the **Credentials** tab to open a popup in which you can select an OAuth client ID option under the **Create credentials** select box.

   l. Select your application type, **Web application**.

   m. Name the client and add the Authorized redirect URIs.

      i. Get the redirect URL from Oracle Content and Experience Cloud and paste it in **Authorized redirect URI**.

         A redirect URI must be the same as your application installation URL.

      ii. For Oracle Content and Experience Cloud, you will get it from **Administration**> **Integration** > **Connectors** > **Google Drive** > **Configure** and copy the value from the **Redirect URL**

      iii. In **Authorized Javascript Origins**, add the part until before documents from the redirect URL.

If you get the message as Invalid Origin, click the authorized domains list and add your domain.

iv. Repeat steps i through iii for each redirect URI.

v. Click **ENTER** on your keyboard, and then click the **Save** button in the UI.

Once you have added to the authorized domains, you should be able to create an OAuth ID. In the result, you'll get the Client ID and Client Secret. Note down the values of **Client ID** and **Client Secret**.

3. Create credentials to get the API key (Developer Key). Click **Create Credentials** and then **API key** in the drop-down menu. Note down value of **API Key**. This is the **Developer Key** in the Oracle Content and Experience Cloud **Google Drive Configure** page.

4. Get the App ID.

   a. From the left corner icon, navigate to **IAM & admin** > **Settings**.

   b. From that page note down the value of **Project Number**.

   This is the App Id in the Oracle Content and Experience Cloud **Google Drive Configure** page.

5. Provide Configuration Parameter values for the connector.

   a. Sign in to Oracle Content and Experience Cloud.

   b. Click **Integrations** in the **Administration** area of the navigation menu on the left.

   c. On the **Integrations** page, go to the **Applications** drop-down menu and choose **Connectors**.

   d. On the **Connectors** tab, click the **Configure** button next to the Google Drive content connector.

   e. Enter values under **Custom Fields** under **Connector Settings** in Oracle Content and Experience Cloud. For Google Drive, enter values for the following fields:

      - **Client ID**
      - **Client Secret**
      - **Developer Key**
      - **App Id**

   f. Make sure the **Enabled For End Users** check box is selected.

   g. Click the **Save** button to save the configuration parameter values.

After a Google Drive content connector is enabled and configured, it is available in the asset repository for Content and Experience Cloud users to download content, through the **Add From** drop-down menu on the **Assets** page.

Configure a Dropbox Connector

After you configure and enable a Dropbox connector, you can connect to Dropbox and pull required content from it into Oracle Content and Experience Cloud.

To configure a Dropbox connector:

1. Get the Oracle Content and Experience Cloud host name and authorization URL details.
   a. Sign in to Oracle Content and Experience Cloud.
   b. Click **Integrations** in the **Administration** area of the navigation menu on the left.
   c. On the **Integrations** page, go to the **Applications** drop-down menu and choose **Connectors**.
   d. On the **Connectors** tab, click the **Configure** button next to the Dropbox content connector.
   e. Note down the Redirect URL, which will be in this format:

      ```
      https://<hostname>.<domainname>.com:<port>/documents/web/
      AR_COMPLETE_AUTHORIZATION
      ```

      The **Redirect URL** field is truncated. Double-click the field to copy the value to your clipboard.
   f. You can override the default connector settings, as described in Enable a Connector.

      In the **Connector Tags** field, you can assign tags for assets that the connector pulls into Oracle Content and Experience Cloud.
2. Create a Dropbox app:
   a. Go to `https://www.dropbox.com/developers/apps` in a Browser window
   b. Sign in with a Dropbox user name and password.
   c. Go to **My apps**.
   d. Click the **Create App** button, and on next screen, in Step 1, choose a Dropbox API.
   e. Choose an access type and name for your application, and click **Create App**.

      For production deployment of the Dropbox app, refer to Dropbox documentation for the approval required: `https://www.dropbox.com/developers/reference/developer-guide#production-approval`.
   f. After the app is created, you can add or configure additional values on the next screen.
   g. Note down the values of **App key** and **App secret**.
3. In the **OAuth 2 - Redirect URIs** section, add the URL you captured earlier from the Oracle Content and Experience Cloud Dropbox configuration screen to the list.
4. On the **Dropbox App** page, navigate to the lower section, **Chooser/Saver domains**, and add the host name used to access Oracle Content and Experience Cloud to this section.
5. Provide Configuration Parameter values for a Connector in Oracle Content and Experience Cloud.
   a. Sign in to Oracle Content and Experience Cloud.
   b. Click **Integrations** in the **Administration** area of the navigation menu on the left.

c. On the **Integrations** page, go to the **Applications** drop-down menu and choose **Connectors**.

d. On the **Connectors** tab, click the **Configure** button next to the OneDrive content connector.

e. Enter values under **Custom Fields** under **Connector Settings** in Oracle Content and Experience Cloud. For Dropbox, enter values for the following fields:

- **App key**
- **App secret**

f. Make sure the **Enabled For End Users** check box is selected.

g. Click the **Save** button to save the configuration parameter values.

After a Dropbox content connector is enabled and configured, it is available in the asset repository for Content and Experience Cloud users to download content, through the **Add From** drop-down menu on the **Assets** page.

Configure a OneDrive Connector

After you configure and enable a Microsoft OneDrive Connector as a content repository, you can connect to OneDrive and pull required content from it into Oracle Content and Experience Cloud.

To configure a OneDrive connector:

1. Get the Oracle Content and Experience Cloud host name and authorization URL details.

   a. Sign in to Oracle Content and Experience Cloud.

   b. Click **Integrations** in the **Administration** area of the navigation menu on the left.

   c. On the **Integrations** page, go to the **Applications** drop-down menu and choose **Connectors**.

   d. On the **Connectors** tab, click the **Configure** button next to the OneDrive content connector.

   e. Note down the Redirect URL, which will be in this format:

   ```
   https://<hostname>.<domainname>.com:<port>/documents/web/
   AR_COMPLETE_AUTHORIZATION
   ```

   The **Redirect URL** field is truncated. Double-click the field to copy the value to your clipboard.

   f. You can override the default connector settings, as described in Enable a Connector.

   In the **Connector Tags** field, you can assign tags for assets that the connector pulls into Oracle Content and Experience Cloud.

2. Create a OneDrive app:

   a. Sign in to the Microsoft developer console at `https://apps.dev.microsoft.com` using a Microsoft user name and password:

b. Click the **Add an app** button.

c. Enter an application name, and click **Create**.

   The sampleApp Registration screen is displayed.

d. Under **Properties**, type a name for your application.

e. Note down the **Application id** value.

3. Generate a password.

   a. Under **Application Secrets**, click the **Generate a New Password** button.

   b. Note down the password, which will not be displayed again.

   c. Click **Ok**.

   More than one password can be generated for an app. All passwords will work.

4. Add a web platform.

   a. Under **Platforms**, click the **Add Platform** button.

   b. In the **Add Platform** popup, click **Web**.

   c. In the **Add Platforms** dialog box under **Platforms**, click **Add URL**, and add one or more URLs in the following format:

   ```
   https://<host>:<port>/documents/static/gemini/html/
   onedrive_redirect.html
   ```

   User the redirect URL you noted down earlier in Oracle Content and Experience Cloud.

   d. Click **Save**.

   e. **Under Microsoft Graph Permissions**, you can add **Delegated Permissions** and **Application Permissions**.

   The default permission is User.Read. There is no need to change that for OneDrive connector integration with Oracle Content and Experience Cloud.

5. Provide configuration parameter values for the connector in Oracle Content and Experience Cloud.

   a. Sign in to Oracle Content and Experience Cloud.

   b. Click **Integrations** in the **Administration** area of the navigation menu on the left.

   c. On the **Integrations** page, go to the **Applications** drop-down menu and choose **Connectors**.

   d. On the **Connectors** tab, click the **Configure** button next to the OneDrive content connector.

   e. Enter values under **Custom Fields** under **Connector Settings** in Oracle Content and Experience Cloud. For OneDrive, enter values for the following fields:

      - **Client ID** (the value of **Application id** that you noted down earlier)
      - **Client Secret** (the value of the generated password)

   f. Make sure the **Enabled For End Users** check box is selected.

g. Click the **Save** button to save the configuration parameter values.

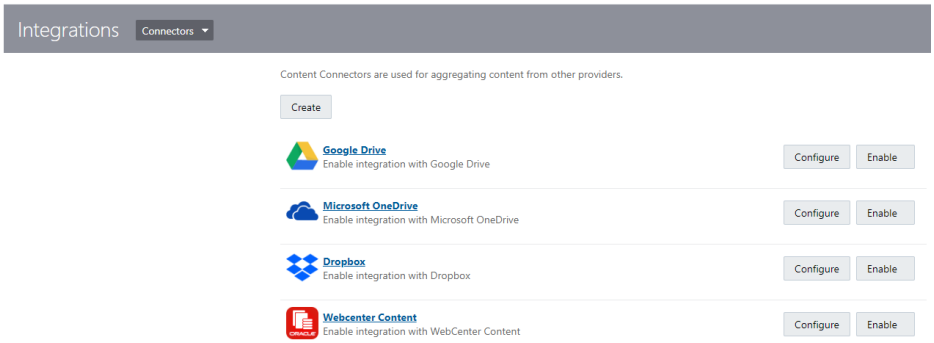
After a OneDrive content connector is enabled and configured, it is available in the asset repository for Content and Experience Cloud users to download content, through the **Add From** drop-down menu on the **Assets** page.

Create and Configure a Custom Connector

After you create, configure, and enable a custom connector, you can connect to a third-party content repository and pull required content from it into Oracle Content and Experience Cloud.

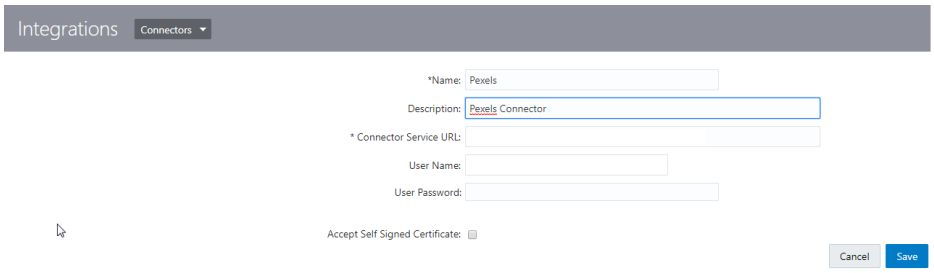
To create and configure a custom connector:

1. Create an app for a Custom connector. See Develop Content Connectors in *Developing for Oracle Content and Experience Cloud*.
2. Get the Oracle Content and Experience Cloud host name and authorization URL details.
   a. Sign in to Oracle Content and Experience Cloud.
   b. Click **Integrations** in the **Administration** area of the navigation menu on the left.
   c. On the **Integrations** page, go to the **Applications** drop-down menu and choose **Connectors**.
   d. On the **Connectors** tab, click the **Create** button to create a connector of type `CUSTOM`.

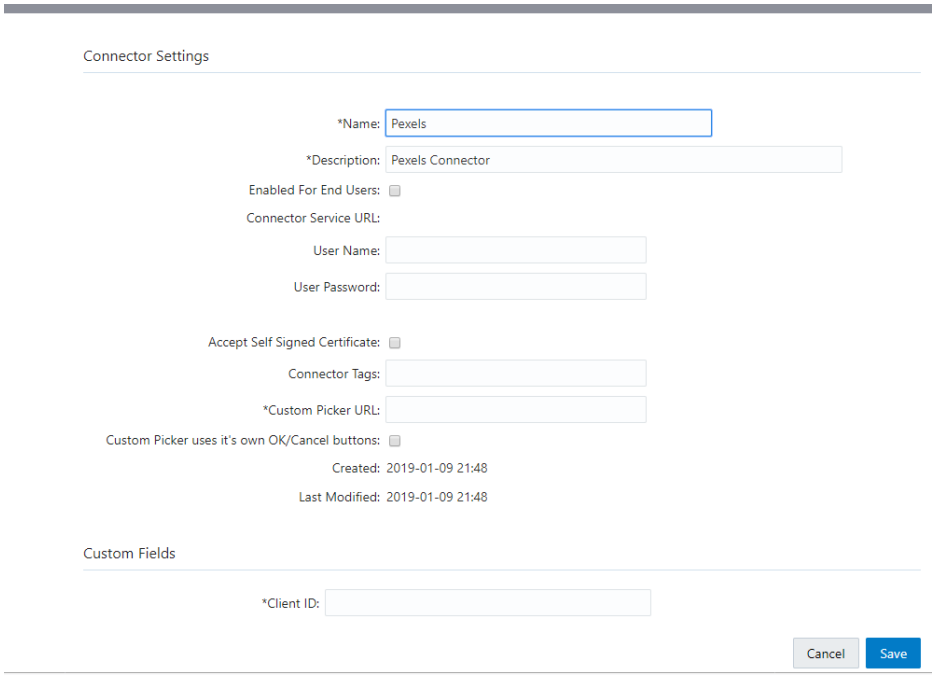


   e. You can override the default connector settings, as described in Enable a Connector.

      On the next screen, enter a name and description for your Custom connector, check **Accept Self-Signed Certificate** if required, and click **Save**. After you enter and save the field values, a spinner appears until the connector is created and the page is filled with the custom fields and other returned fields.



f. On the **Connector Settings** screen, enter configuration information for the Custom connector.



In the **Connector Tags** field, you can assign tags for assets that the connector pulls into Oracle Content and Experience Cloud. This field is available on the edit page, after you have entered the initial information on the create page and clicked **Save**.

A connector of type `CUSTOM` has two additional configuration fields: **Custom Picker URL** and **Custom Picker uses it's own OK/Cancel buttons**.

g. Note down the Redirect URL, which will be in this format:

```
https://<hostname>.<domainname>.com:<port>/documents/web/
AR_COMPLETE_AUTHORIZATION
```

The **Redirect URL** field is truncated. Double-click the field to copy the value to your clipboard.

h. Click **Save**.

3. Enable the Custom connector. See Enable a Connector.

Configure WebCenter Content and OCE for the WCC Connector

An administrator can configure WebCenter Content (WCC) and Oracle Content and Experience Cloud (OCE) for the WCC connector so site users can pull content from the WebCenter Content Server into their sites.

To configure WebCenter Content and OCE for the WCC Connector:

1. Set Up a Security Policy on WebCenter Content Server
2. Import the Trusted Certificate from WebCenter Content Server to Content and Experience Cloud
3. Configure and Enable the WCC Connector

Set Up a Security Policy on WebCenter Content Server

Oracle Content and Experience Cloud communicates with WebCenter Content Server using the JAX-WS communication channel. Use the OWSM policies to secure the JAX-WS endpoints.

Use the `oracle/wss_username_token_over_ssl_service_policy` server-side policy. For client communication with the WebCenter Content Server instance, the user needs to enter both a user name and password. If these values are incorrect, then the handshake with the WebCenter Content Server will not be established.

Check the prerequisites before setting up the security policy:

- First check if any OWSM policy is attached to JAX-WS.

  Access your Oracle Content and Experience Cloud wsdl at *`ucm-instance/ /`* `idcnativews/IdcWebLoginPort?WSDL`. You should see the policy *`wsp:PolicyReference`* field in the wsdl.

```
  - <operation name="contentServerLogin">
      <input message="tns:contentServerLoginInput" ns1:Action=""/>
      <output message="tns:contentServerLoginOutput" ns1:Action=""/>
    </operation>
  - <operation name="contentServerLogout">
      <input message="tns:contentServerLogoutInput" ns1:Action=""/>
      <output message="tns:contentServerLogoutOutput" ns1:Action=""/>
    </operation>
  </portType>
- <binding name="IdcWebLoginSoapHttp" type="tns:IdcWebLogin">
    <soap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsp:PolicyReference URI="#wss_username_token_service_policy" wsdl:required="false"/>
  - <operation name="contentServerLogin">
      <soap:operation soapAction=""/>
```

- If the attached policy is `oracle/wss_username_token_over_ssl_service_policy`, then you can ignore the following configurations.
- If the attached policy is a different one, you need to detach that policy and then attach the policy `oracle/wss_username_token_over_ssl_service_policy`.

- If no policy is attached, then you to attach the policy `oracle/wss_username_token_over_ssl_service_policy`.

Take the following steps to configure the server-side policy:

1. Sign in to Enterprise Manager
2. Open the Oracle UCM Native Web Services
3. Open the Web Services Application
4. Use the Web Service Endpoint to View and Change Policies
5. Detach and Attach Security Policies
6. Validate the Security Policy
7. Confirm That the Security Policy Is Attached Correctly
8. Verify That the wsdl Loads Successfully

Sign in to Enterprise Manager

Sign in to Enterprise Manager on the Oracle WebCenter Content instance.

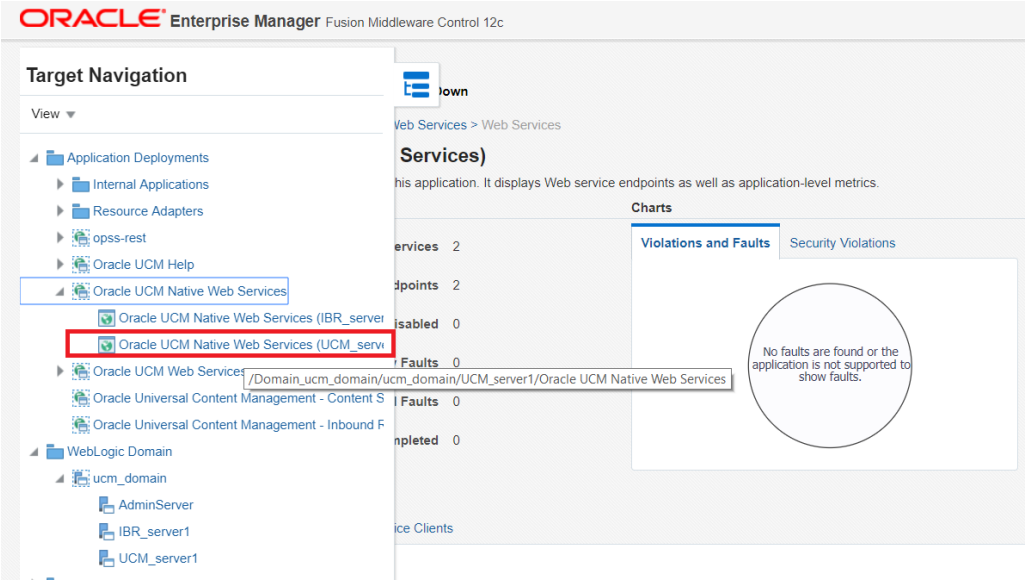
Go to *wcc-instance*:7001/em.

Sign in as the `weblogic` user with your password.

Open the Oracle UCM Native Web Services

In Enterprise Manager, you can open the Oracle UCM Native Web Services.

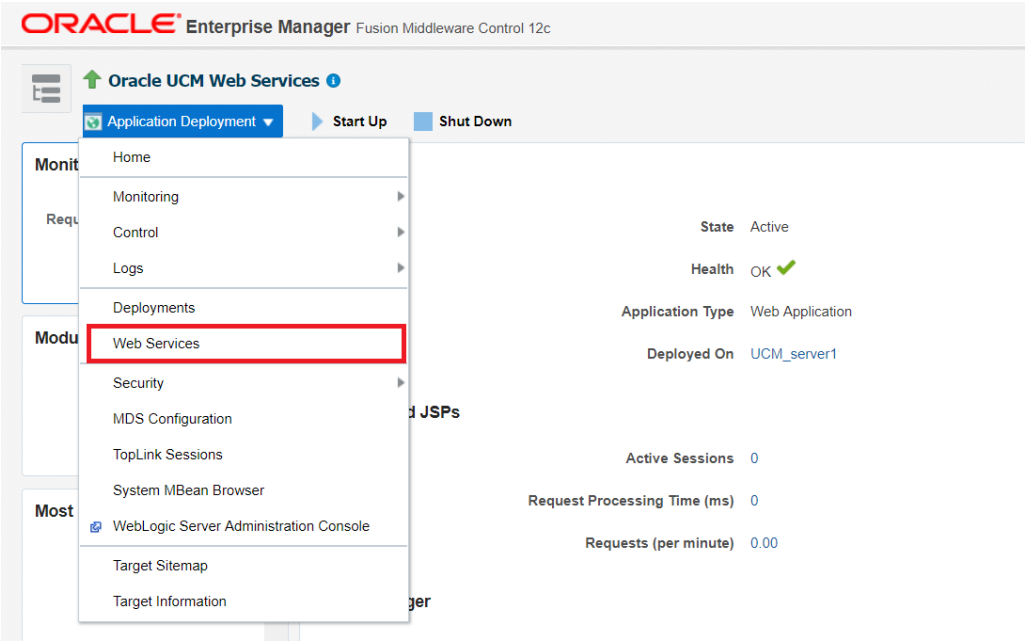
1. Go to **Target Navigation > Application Deployments > Oracle UCM Native Web Services**.
2. Click **Oracle UCM Native Web Services (UCM_server1)**.



Open the Web Services Application

In Entprise Manager Fusion Middleware Control, you can open the Oracle UCM Web Services application.

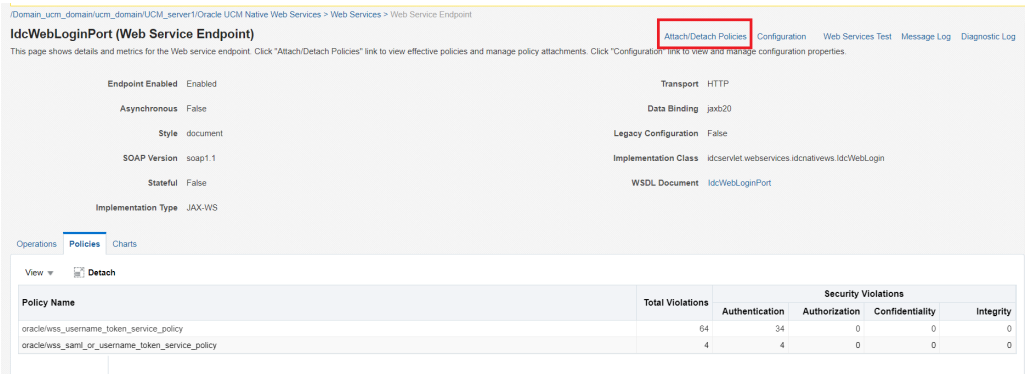
On the **Application Deployment** drop-down menu, click **Web Services**.



Use the Web Service Endpoint to View and Change Policies

From the Web Service endpoint, you can list directly attached policies.

Click **IdcWebLoginPort**. Then click **Attach/Detach Policies**.



Detach and Attach Security Policies

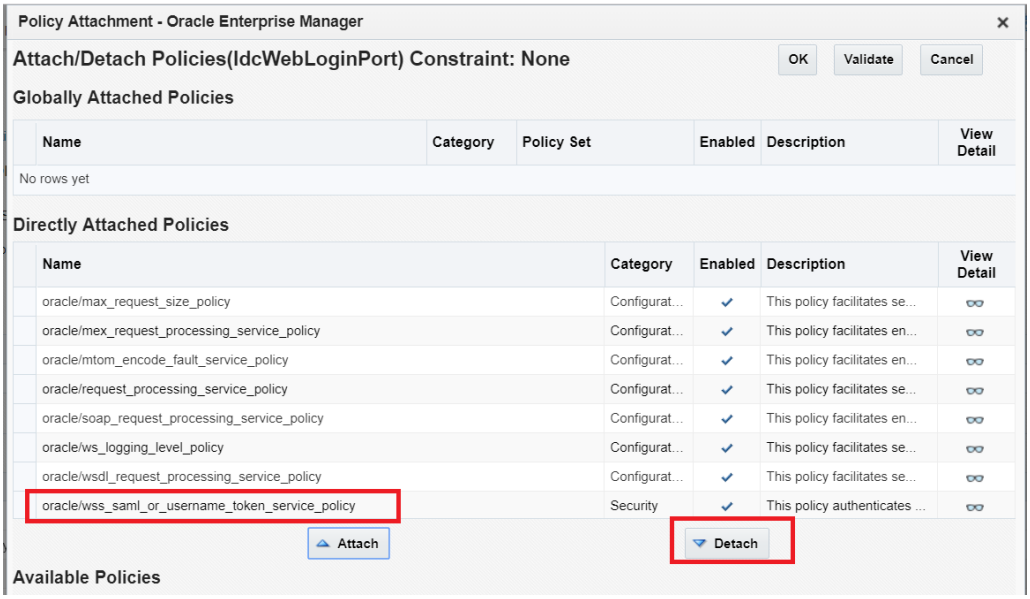
Under the directly attached policies section, you can detach or attach security policies.

If there is any security policy other than **oracle/wss_username_token_over_ssl_service_policy** attached, first detach the other policy. Then attach **oracle/wss_username_token_over_ssl_service_policy**.

To detach a security policy:

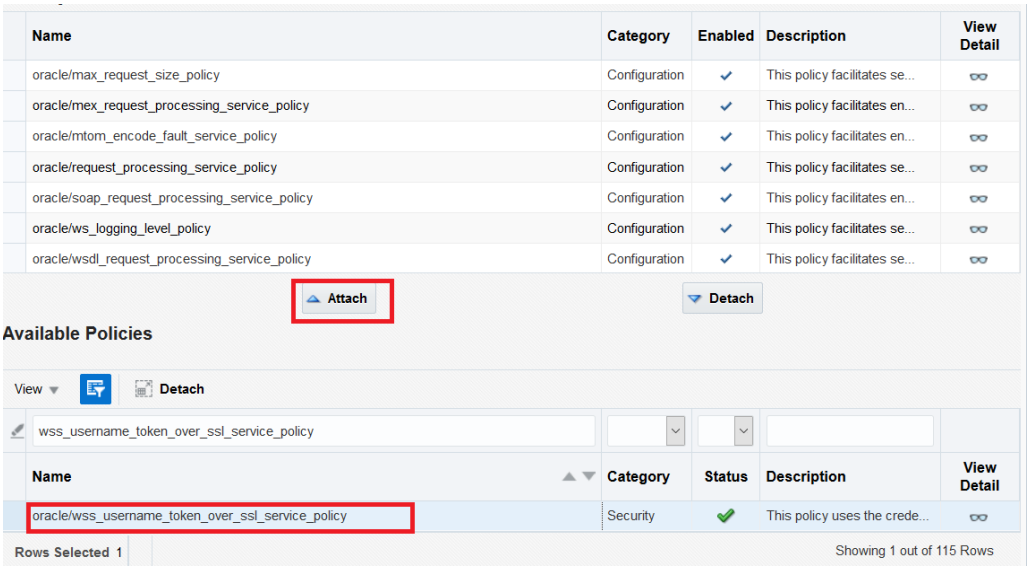
1. Select the policy whose category is **Security**, and then click the **Detach** button.
2. Click the **Detach** button.

   This policy is removed from the **Directly Attached Policies** list.



To attach the **oracle/wss_username_token_over_ssl_service_policy** security policy:

1. In the **Available Policies** section, search for **wss_username_token_over_ssl_service_policy**.
2. In the result section, select **oracle/wss_username_token_over_ssl_service_policy**.
3. Click the **Attach** button.



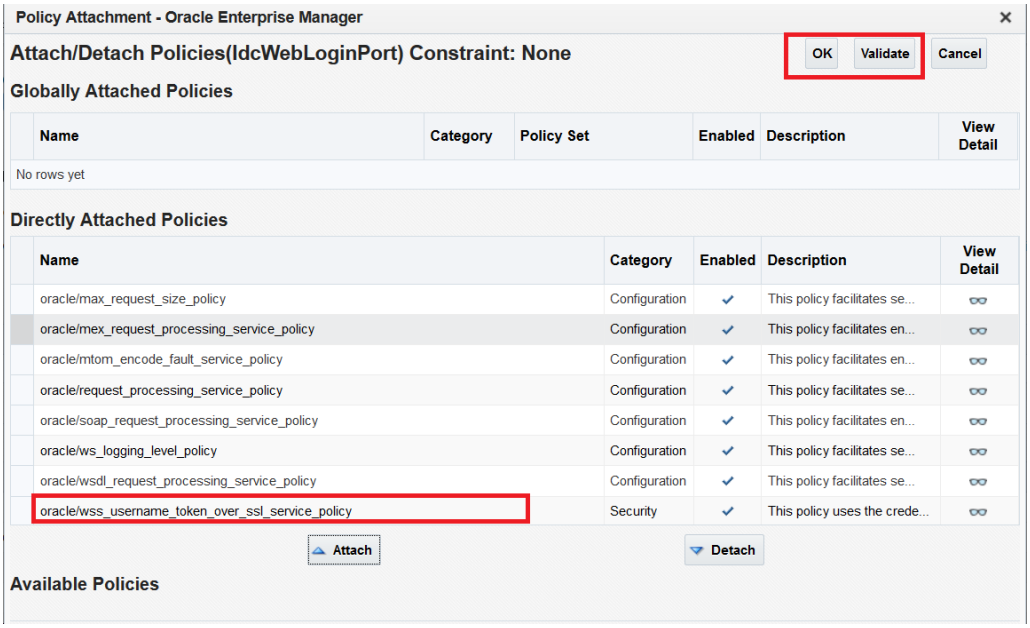
Validate the Security Policy

You can see `oracle/wss_username_token_over_ssl_service_policy` under the Directly Attached Policies.

To validate the security policy:

1. Click **Validate**, and then click **OK**.
2. After the popup closes, click the **Return** button.

   No restart is required.



Confirm That the Security Policy Is Attached Correctly

You can access the `IdcWebLoginPort wsdl` to confirm that the security policy is attached correctly.

You should see the policy `oracle/wss_username_token_over_ssl_service_policy` being attached to the `IdcWebLoginPort wsdl`,

```
- <definitions name="IdcWebLoginService" targetNamespace="http://idcnativews.webservices.idcservlet/">
  - <wsp:Policy wsu:Id="wss_username_token_over_ssl_service_policy">
    - <sp:TransportBinding>
      - <wsp:Policy>
        - <sp:AlgorithmSuite>
          - <wsp:Policy>
              <sp:Basic128/>
            </wsp:Policy>
          </sp:AlgorithmSuite>
        - <sp:TransportToken>
          - <wsp:Policy>
            - <sp:HttpsToken RequireClientCertificate="false">
                <wsp:Policy/>
              </sp:HttpsToken>
            </wsp:Policy>
          </sp:TransportToken>
        - <sp:Layout>
          - <wsp:Policy>
              <sp:Lax/>
            </wsp:Policy>
          </sp:Layout>
          <sp:IncludeTimestamp/>
        </wsp:Policy>
      </sp:TransportBinding>
    - <sp:SupportingTokens>
```

Verify That the wsdl Loads Successfully

To finish the seurity policy setup on WebCenter Content Server, verify that the wsdl loads successfully.

Verify that `https://<host>:<port>/idcws/GenericSoapPort?WSDL` loads successfully.

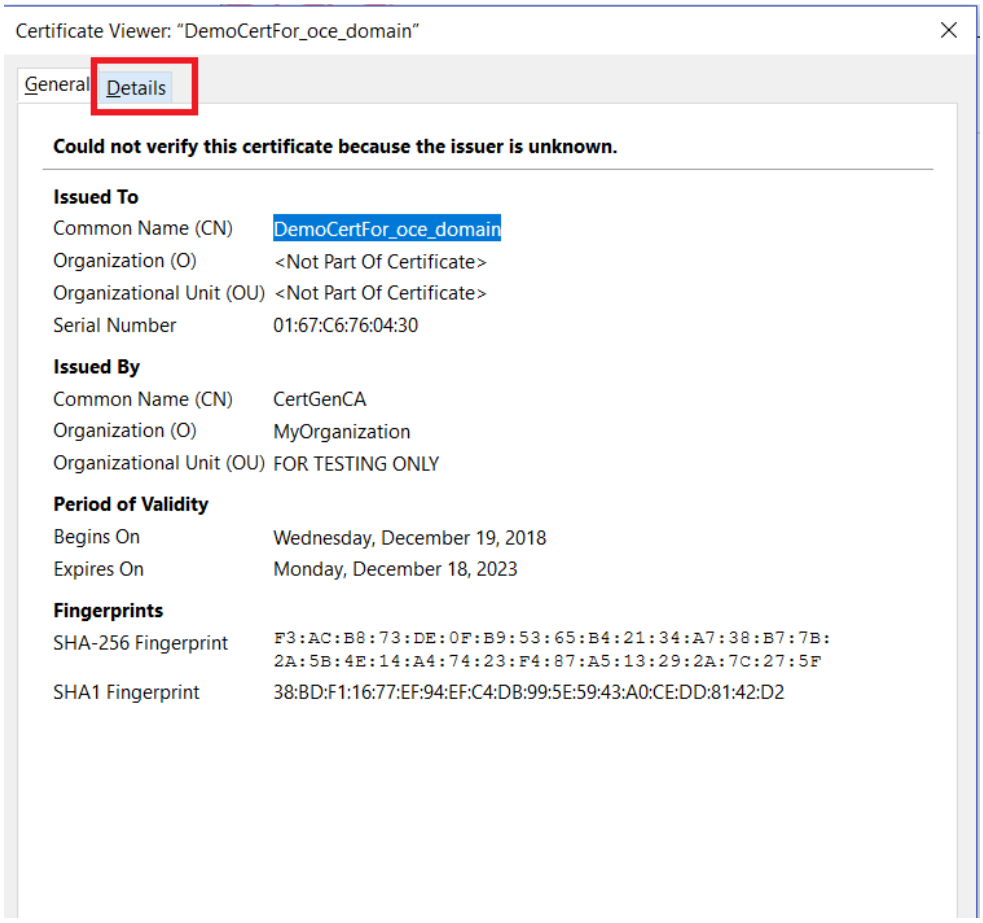
Import the Trusted Certificate from WebCenter Content Server to Content and Experience Cloud

Since SSL is enabled on UCM, import the trusted certificate of the UCM server to Content and Experience Cloud, for the successful handshake between it and UCM.

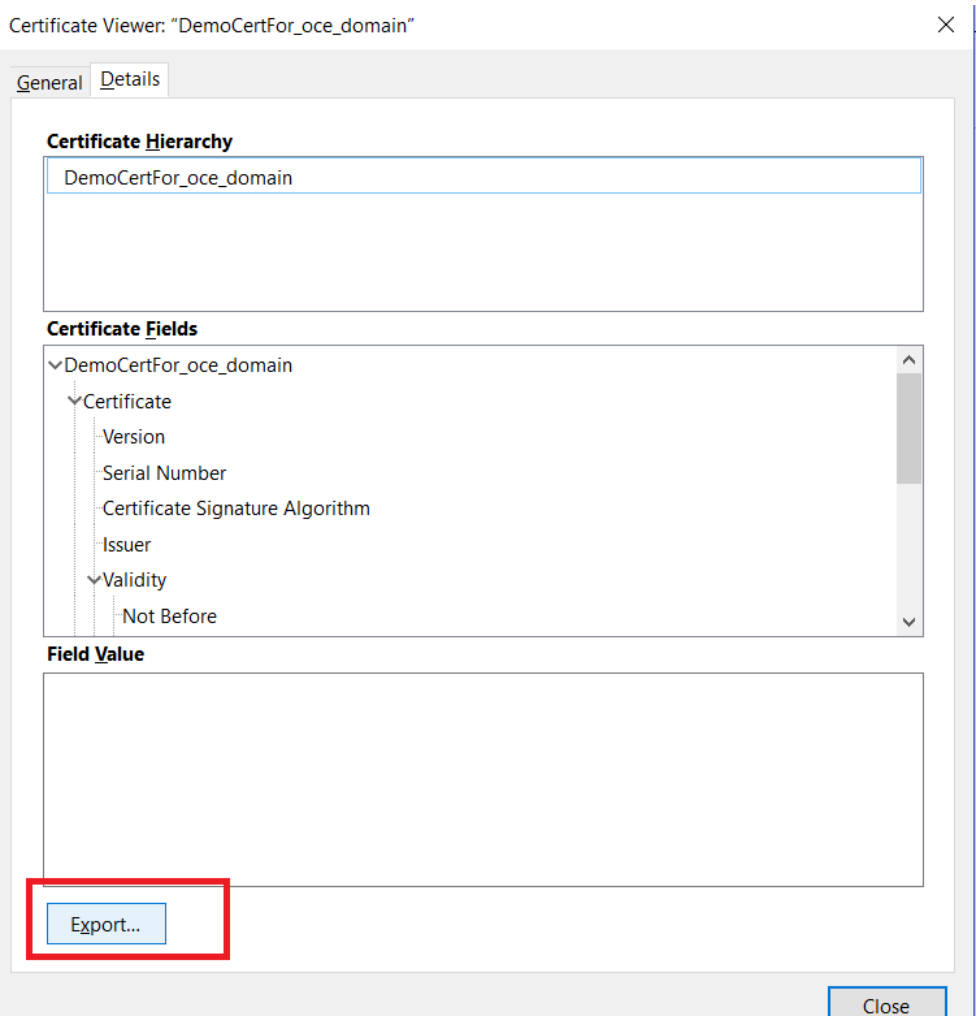
Take the following steps to import the trusted certificate;

1. Access the UCM server in a Firefox browser. Click the warning icon before the address bar.
2. Click the right arrow.
3. Click **More Information**.

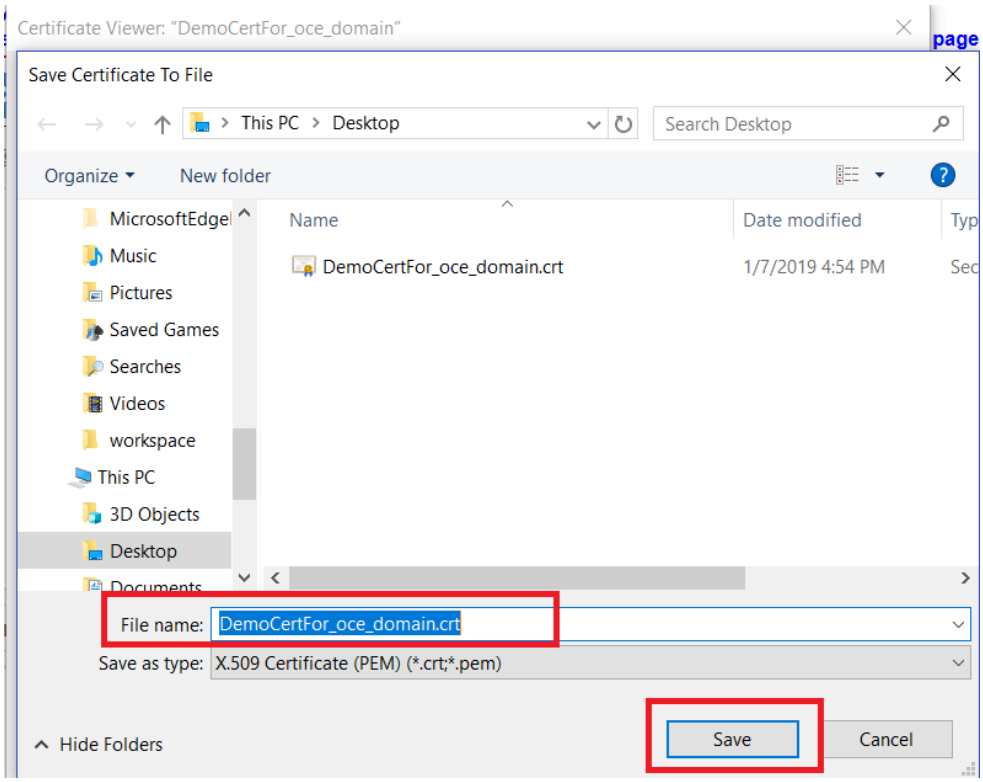
4. Click on **View Certificate**.
5. Click the **Details** tab.



6. Click the **Export** button.

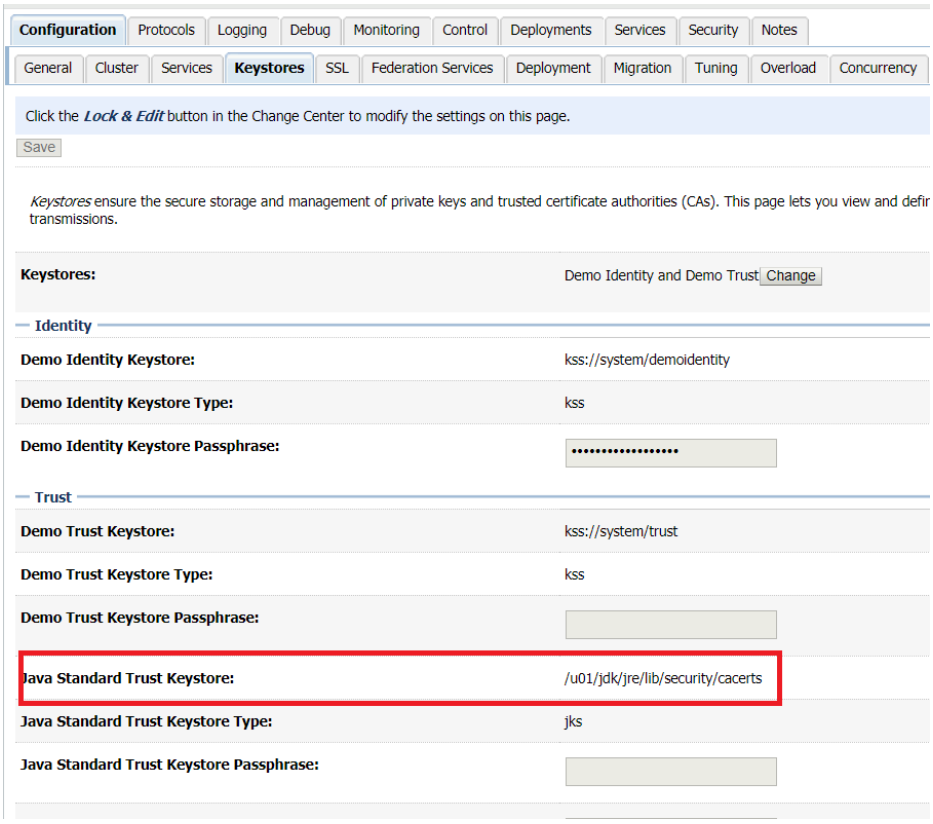


7. Download the certificate to a Windows machine.



8. To import the certificates into the Content and Experience server's castore, follow these steps:

   a.



b. In a Putty terminal, SSH to the VM1. Then copy the certificate previously downloaded on the Windows machine to this VM1.

c. Import the certificate using the following command:

```
keytool -import-trustcacerts -alias adcucmpod -keystore
          /u01/jdk/jre/lib/security/cacerts -storepass <password> -
file
          /u01/app/oracle/tools/home/oracle/
DemoCertFor_oce_domain.crt This command imports the UCM certificate
to CEC truststore. Following
          are the parameters used in thiscommandkeytool - This is
a  java command used forimporting the  certificates to keystores.
Also before running
          thiscommand, check ifkeytool command works fine in the
terminal. Type keytool, it will
          show options available, this   means that you can run the
keytool command. If it does not give
          options, then set the JAVA_HOME correctly, keytool will
start working
         import- This command is used when we importthe
certificates  trustcacerts - This
          argument tells keytool that you want to importthisas a
trusted certificate. alias - This is unique name. The certificates
will be mapped to
          thisalias name. Here we have given the name as
adcucompod, we gave any
          meaningful name as alias name keystore - In
          thiscontext, the Java Standard Trust Keystore location
noted down in
          the earlier step from console has to be given ie
        /u01/jdk/jre/lib/security/cacerts storepass - We
          have to give the password of keystore. In our casewe have
to give the password of cacerts which is
        <password>. file - The location where the
          certificate had been copied from the Windows machine. In
this case the certificate was copied to following location on the VM
          /u01/app/oracle/tools/home/oracle/
DemoCertFor_oce_domain.crt
```

d. When you run this command, you will be asked if this certificate can be trusted. Type `Yes`.

e. Repeat the same steps for VM2 as well. First get the location of the `cacerts` from the console, then copy the certificate to VM2, and then import the certificate to the cacerts truststore.

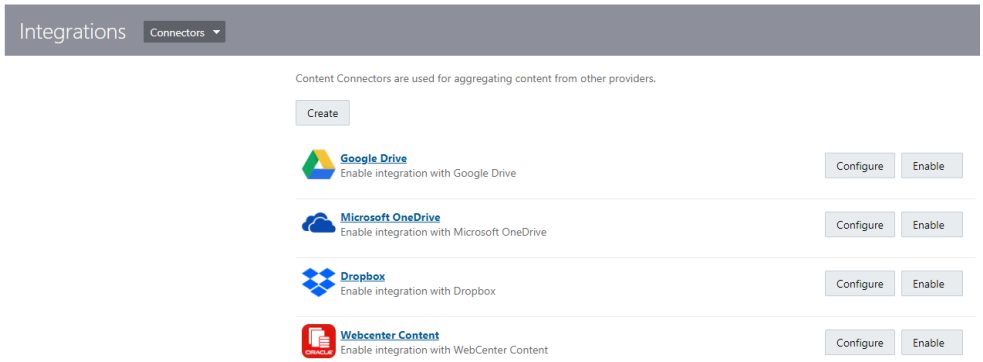
f. Restart all the servers.

Configure and Enable the WCC Connector

After you configure and enable a WebCenter Content (WCC) connector for an Oracle Content and Experience Cloud instance, site users can import content from WebCenter Content Server.

To configure and enable a WCC connector:

1. Sign in to your Oracle Content and Experience Cloud instance.
2. On the **Integrations** page, go to the **Applications** drop-down menu and choose **Connectors**.



3. On the **Connectors** tab, click the **Configure** button next to **WebCenter Content** .
4. In the **Custom Field** section, provide the following values:
   a. The URI of the WebCenter Content JAX-WS Server Connection; for example, `ucm_host:port/idcnativews`
   b. The WebCenter Content Server JAX-WS Client Policy: for example, `oracle/wss_username_token_over_ssl_client_policy`
5. On the **Connectors** tab, click the **Enable** button next to **WebCenter Content** .

6

Manage Users, Groups, and Access

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

Topics

- Enable Single Sign-On (SSO)
- Manage Users
- Manage Groups
- 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 Federated Single Sign-On (SSO) is currently available for your Oracle Content and Experience Cloud 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.

Shared Identity Management (SIM) is part of the Oracle Cloud security infrastructure. It is designed to let Oracle Cloud services set up user authentication, web single sign-on (SSO), outbound identity federation, and web services authorization. SIM brings users, services, and applications in the cloud together in a secure manner. It's accomplished using Oracle Identity Platform Service and OAuth as an authorizing mechanism.

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 login session. It identifies the user and the user's groups.

See Role of the Identity Domain in *Understanding Identity Concepts* to learn about how the identity domain is used to manage many features of Oracle Cloud.

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.

The following steps must be followed to configure SSO:

1. Sign in to My Services using one of the following methods:
   - Click the **Access your Cloud Services** link in the email with the subject: “Welcome to Oracle Cloud. Your Oracle Public Cloud Services are ready for use.”, and enter your user name and password.
   - Sign in from Oracle Cloud. See Signing In From the Oracle Cloud Website in *Getting Started with Oracle Cloud*.
2. Configure Oracle Cloud as the service provider by using the **SSO Configuration** page in My Services. You must have the necessary metadata from the identity provider to configure Oracle Cloud.
3. Configure the identity provider that users sign in to. You can download metadata or copy URLs using the **SSO Configuration** page in My Services. You can then use that data to configure the identity provider. You must configure your identity provider using the identity provider’s interface.
4. Test the configuration to verify it works. You can use a test application built into the **SSO Configuration** page in My Services. This application provides information to help you diagnose problems. Make sure to test the feature before you enable it.
5. Enable SSO for your users from the **SSO Configuration** page in My Services.
6. Update any metadata if necessary.

See Managing Oracle Single Sign-On in *Administering Oracle Cloud Identity Management* for complete details about setting up SSO.

For more information and tutorials that demonstrate the configuration process, see *Secure Platform Services* in the Oracle Help Center.

Manage Users

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.

How you manage users depends on what type of subscription you have.

- For Universal Credits subscriptions, see Manage Users with Oracle Identity Cloud Service.
- For non-metered subscriptions, see Manage Users with a Traditional Cloud Account.

Manage Users with Oracle Identity Cloud Service

If you have a Universal Credits subscription, you manage users in Oracle Identity Cloud Service.

To manage users:

1. Sign in to My Services using one of the following methods:
   - Click the **Access your Cloud Services** link in the email with the subject: “Welcome to Oracle Cloud. Your Oracle Public Cloud Services are ready for use.”, and enter your user name and password.
   - Sign in from Oracle Cloud:
     a. Go to http://cloud.oracle.com.
     b. Click **Sign In**.
     c. From the **Cloud Account** menu, select **Cloud Account with Identity Cloud Service**.
     d. In the **Cloud Account Name** field, enter the name of your cloud account.
     e. Click **My Services**.
     f. Enter the user name and password for your cloud account.
2. In the dashboard, click **Users**.
3. On the **User Management** page, in the banner, click **Identity Console**.

   You’ll be redirected to the Oracle Identity Cloud Service **Users** page.
4. Perform any of the following tasks:
   - To create a user, click **Add**.
   - 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 Users with a Traditional Cloud Account

If you have a non-metered subscription, you manage users in My Services.

To manage users:

1. Sign in to My Services using one of the following methods:

- Click the **Access your Cloud Services** link in the email with the subject: “Welcome to Oracle Cloud. Your Oracle Public Cloud Services are ready for use.”, and enter your user name and password.
- Sign in from Oracle Cloud:
  a. Go to http://cloud.oracle.com.
  b. Click **Sign In**.
  c. From the **Cloud Account** menu, select **Traditional Cloud Account**.
  d. Select your data center.
  e. Click **My Services**.
  f. Enter your identity domain, and click **Go**.
  g. Enter the user name and password for your cloud account.

2. In the dashboard, click **Users**.
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 Managing Users with Traditional Cloud Accounts in *Managing and Monitoring Oracle Cloud*.

Manage Groups

As a best practice, you should create groups for your organization roles and assign the appropriate user roles to those groups. Then you can add users to those groups to automatically assign them the appropriate user roles.

Topics

- Create Group Standards for Your Organization
- Manage Groups with Oracle Identity Cloud Service
- Manage Groups with a Traditional Cloud Account
- Assign Roles to Groups with Oracle Identity Cloud Service
- Assign Roles to Groups with a Traditional Cloud Account
- Assign Users to Groups with Oracle Identity Cloud Service
- Assign Users to Groups with a Traditional Cloud Account

Create Group Standards for Your Organization

Using groups makes it easy to ensure that you include the right people when sharing documents, starting conversations, or creating content types. However, to avoid

duplication and overuse of groups, you should create high-level groups for your organization and establish group standards that you communicate to your users.

Benefits of Using Groups

A group is a set of users that have a common position, goal, or concern. The great thing about using groups when adding members to documents, conversations, or content types is that you can make sure no one is accidentally left out. And, if someone new needs to be included, you can add them to the group rather than tediously adding them to each folder, conversation, or content type that they need to know about.

Best Practices for Creating Groups

Here are some best practices for creating groups:

- **Don't duplicate groups**. Use the **Find Public Groups** option on the Group menu to see if a group already exists that might be useful for your purpose.
- **Use a meaningful name**. Don't use acronyms or abbreviations for your group name. Make it meaningful so people will understand its purpose.
- **Choose the right privacy control for your group**. You can control who can see or use the group, and you can control if someone can add themselves to a group. There are three kinds of groups:
  - **Public group**. A public group is visible to anyone and anyone can add themselves to the group. You should use this kind of group sparingly. For example, you may have a rollout of a project and you'd like to gather feedback from anyone who used the project. You can open up a group to everyone and let people add themselves so they can add feedback about that specific project.
  - **Closed group**. A closed group is one that can be seen by everyone but people can't add themselves to the group. This can be useful when you want to limit a group to a subset of people. People could discover the group exists and use the group to share information with those people. For example, you can create a group for the Engineering department. Anyone who needs to collaborate or share with that department can add that group as a member to a conversation or folder.
  - **Private group**. This type of group gives you the tightest control on membership. No one will be able to see the group unless they're already a member and no one can add themselves to the group. For example, perhaps a small set of people need to discuss an upcoming acquisition or project. No one else in the organization needs to know about this, so by creating a group for restricted members, you control who can see the information.

Those best practices as well as other tips are included in Groups Overview in *Managing Content with Oracle Content and Experience Cloud*.

Develop Group Naming Standards

To ensure users can find the groups they need, establish group naming standards for your company. You'll probably want to create separate naming standards for more permanent groups such as department groups and for shorter-term groups such as project groups. For example, you might want to format project group names as *Department - Project*, such as "Marketing - Spring 2017 Campaign."

Create High-Level Groups for Your Organization

Before you roll out your service to users, you should create groups for each department, project team, or other business unit.

You can use the REST APIs to create groups. See People and Groups Resource in *Developing for Oracle Content and Experience Cloud*.

You can also create groups manually. If you create groups manually, you'll want to have an organizational chart so you know what groups to create and which users to add to each group. Remember to use meaningful names and to choose the right privacy control for your groups. See Creating or Deleting a Group in *Managing Content with Oracle Content and Experience Cloud*.

Communicate Your Group Structure and Best Practices

You need to let your users know that they are already part of the high-level groups you created, tell them about your group naming standards, and point them to the best practices. You can include this information in your additional welcome email when you roll out your service. See Provide Sign In and Get Started Information to Users.

Manage Groups with Oracle Identity Cloud Service

If you have a Universal Credits subscription, you manage groups in Oracle Identity Cloud Service.

To manage groups:

1. Sign in to My Services using one of the following methods:
   - Click the **Access your Cloud Services** link in the email with the subject: “Welcome to Oracle Cloud. Your Oracle Public Cloud Services are ready for use.”, and enter your user name and password.
   - Sign in from Oracle Cloud:
     a. Go to http://cloud.oracle.com.
     b. Click **Sign In**.
     c. From the **Cloud Account** menu, select **Cloud Account with Identity Cloud Service**.
     d. In the **Cloud Account Name** field, enter the name of your cloud account.
     e. Click **My Services**.
     f. Enter the user name and password for your cloud account.
2. In the dashboard, click **Users**.
3. On the User Management page, in the banner, click **Identity Console**.

   You’ll be redirected to the Oracle Identity Cloud Service Users page.
4. Display the navigation drawer, and then click the **Groups** tab.
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*.

Manage Groups with a Traditional Cloud Account

If you have a non-metered subscription, you manage groups in My Services.

To manage groups:

1. Sign in to My Services using one of the following methods:
   - Click the **Access your Cloud Services** link in the email with the subject: “Welcome to Oracle Cloud. Your Oracle Public Cloud Services are ready for use.”, and enter your user name and password.
   - Sign in from Oracle Cloud:
     a. Go to http://cloud.oracle.com.
     b. Click **Sign In**.
     c. From the **Cloud Account** menu, select **Traditional Cloud Account**.
     d. Select your data center.
     e. Click **My Services**.
     f. Enter your identity domain, and click **Go**.
     g. Enter the user name and password for your cloud account.
2. In the dashboard, click **Users**.
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 Oracle Identity Cloud Service

If you have a Universal Credits subscription, you assign roles to groups through the **Applications** tab of Oracle Identity Cloud Service.

To assign roles to groups:

1. Sign in to My Services using one of the following methods:
   - Click the **Access your Cloud Services** link in the email with the subject: “Welcome to Oracle Cloud. Your Oracle Public Cloud Services are ready for use.”, and enter your user name and password.
   - Sign in from Oracle Cloud:
     a. Go to http://cloud.oracle.com.
     b. Click **Sign In**.

   c. From the **Cloud Account** menu, select **Cloud Account with Identity Cloud Service**.
   d. In the **Cloud Account Name** field, enter the name of your cloud account.
   e. Click **My Services**.
   f. Enter the user name and password for your cloud account.
2. In the dashboard, click **Users**.
3. On the User Management page, in the banner, click **Identity Console**.

   You'll be redirected to the Oracle Identity Cloud Service Users page.
4. Expand the navigation drawer, and then click **Applications**.
5. Open your Oracle Identity Cloud Service application.
6. Click the **Application Roles** tab.
7. Next to the role you want to assign to the group, click , and then select **Assign Groups**.
8. Find and select the group you want, and then click **Assign**.

   For a list of typical organization roles and the user roles they need, see Typical Organization Roles. For a description of the predefined roles in Oracle Content and Experience Cloud, see User Roles.

Assign Roles to Groups with a Traditional Cloud Account

If you have a non-metered subscription, you assign roles to groups in My Services.

To assign roles to groups:

1. Sign in to My Services using one of the following methods:
   - Click the **Access your Cloud Services** link in the email with the subject: "Welcome to Oracle Cloud. Your Oracle Public Cloud Services are ready for use.", and enter your user name and password.
   - Sign in from Oracle Cloud:
     a. Go to http://cloud.oracle.com.
     b. Click **Sign In**.
     c. From the **Cloud Account** menu, select **Traditional Cloud Account**.
     d. Select your data center.
     e. Click **My Services**.
     f. Enter your identity domain, and click **Go**.
     g. Enter the user name and password for your cloud account.
2. In the dashboard, click **Users**.
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 user roles they need, see Typical Organization Roles. For a description of the predefined roles in Oracle Content and Experience Cloud, see User Roles.

Assign Users to Groups with Oracle Identity Cloud Service

If you have a Universal Credits subscription, you assign users to groups inOracle Identity Cloud Service.

To assign users to groups:

1. Sign in to My Services using one of the following methods:
   - Click the **Access your Cloud Services** link in the email with the subject: “Welcome to Oracle Cloud. Your Oracle Public Cloud Services are ready for use.”, and enter your user name and password.
   - Sign in from Oracle Cloud:
     a. Go to http://cloud.oracle.com.
     b. Click **Sign In**.
     c. From the **Cloud Account** menu, select **Cloud Account with Identity Cloud Service**.
     d. In the **Cloud Account Name** field, enter the name of your cloud account.
     e. Click **My Services**.
     f. Enter the user name and password for your cloud account.
2. In the dashboard, click **Users**.
3. On the User Management page, in the banner, click **Identity Console**.

   You’ll be redirected to the Oracle Identity Cloud Service Users page.
4. Expand the navigation drawer, and then click **Groups**.
5. Open the group you want to assign users to.
6. Click **Assign**.
7. Select the users you want to add, and then click **OK**.

Assign Users to Groups with a Traditional Cloud Account

If you have a non-metered subscription, you assign users to groups in My Services.

To assign users to groups:

1. Sign in to My Services using one of the following methods:
   - Click the **Access your Cloud Services** link in the email with the subject: “Welcome to Oracle Cloud. Your Oracle Public Cloud Services are ready for use.”, and enter your user name and password.
   - Sign in from Oracle Cloud:
     a. Go to http://cloud.oracle.com.
     b. Click **Sign In**.

   c. From the **Cloud Account** menu, select **Traditional Cloud Account**.
   d. Select your data center.
   e. Click **My Services**.
   f. Enter your identity domain, and click **Go**.
   g. Enter the user name and password for your cloud account.
2. In the dashboard, click **Users**.
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 and Experience Cloud web application as an administrator, click **Settings** in the Administration area of the navigation menu.
2. In the **Settings** 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 users' existing profile information with the information from your identity store. You can update all users' profile data or just the data for one user:

1. After you sign in to the Oracle Content and Experience Cloud web application as an administrator, click **Settings** in the Administration area of the navigation menu.
2. In the **Settings** menu, click **Users**.
   - To update all users' profile data, click **Sync Profile Data**.
   - To update a specific user's profile data, 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

You can set the default display setting for conversation membership messages for users .

1. After you sign in to the Oracle Content and Experience Cloud web application as an administrator, click **Settings** in the Administration area of the navigation menu.
2. In the **Settings** 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

1. After you sign in to the Oracle Content and Experience Cloud web application as an administrator, click **Settings** in the Administration area of the navigation menu.
2. In the **Settings** 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 and Experience Cloud web application as an administrator, click **Settings** in the Administration area of the navigation menu.
2. In the **Settings** 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 and Experience Cloud 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 and Experience Cloud and delete all local content stored on the device.

1. After you sign in to the Oracle Content and Experience Cloud web application as an administrator, click **Settings** in the Administration area of the navigation menu.
2. In the **Settings** 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.

7

Monitor the Service

Throughout the use of your service, you'll want to monitor the overall system, view reports on your users and documents, and report any issues that occur.

Topics

- Monitor Service Activity
- Add Web Analytics Tracking Snippets to Sites and Pages
- Understand Visitor Sessions
- View Billing Metrics
- View Business Metrics
- Report Issues

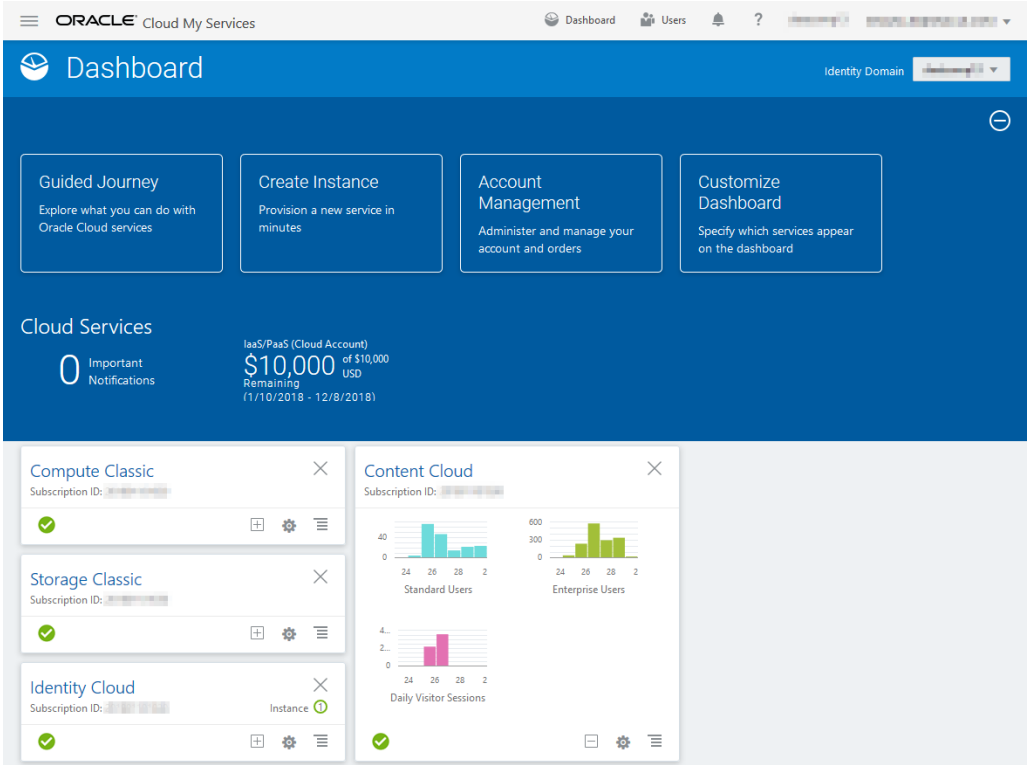
Monitor Service Activity

You can check the overall status of your active Oracle Cloud services in the My Services dashboard. You can view the overall service status, outages, and uptime percentages for the past 14 days. You can also see the storage used, and other details. 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.

To sign in to My Services, use one of the following methods:

- Click the **Access your Cloud Services** link in the email with the subject: "Welcome to Oracle Cloud. Your Oracle Public Cloud Services are ready for use.", and enter your user name and password.
- Sign in from Oracle Cloud. See Sign In to Your Account From the Oracle Cloud Website in *Getting Started with Oracle Cloud*.

Only four metrics show on the dashboard. To change the metrics you see on the dashboard, click



Metrics for Universal Credits Subscriptions to Oracle Content and Experience Cloud

The following metrics apply to Universal Credits subscriptions to Oracle Content and Experience Cloud:

Metric	Description
Standard Users	Displays the number of standard users registered on this service instance. To view additional usage metrics, click **Standard Users**.
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**.
Daily Visitor Sessions	Displays the number of daily visitor sessions recorded on this service instance. To view additional usage metrics, click **Daily Visitor Sessions**. See Understand Visitor Sessions.

Metrics for Non-Metered Subscriptions to Oracle Content and Experience Cloud

The following metrics apply to non-metered subscriptions to Oracle Content and Experience Cloud:

Metric	Description
Purchased Content and Experience Standard Users	Displays the number of standard users registered on this service instance. To view additional usage metrics, click **Purchased Content and Experience Standard Users**.
Purchased Content and Experience 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 **Purchased Content and Experience Enterprise Users**.
Purchased Content and Experience Daily 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 **Purchased Content and Experience Daily Visitor Sessions**. See Understand Visitor Sessions.

Metrics for Non-Metered Subscriptions to Oracle Documents Cloud Service

The following metrics apply to Oracle Documents Cloud Service subscriptions:

Metric	Description
Purchased Documents Storage	Displays the amount of storage space in GB allocated to this service instance. To view additional usage metrics, click **Purchased Documents Storage**.
Purchased Documents Users	Displays the number of users registered on this service instance. To view additional usage metrics, click **Purchased Documents Users**.
Purchased Documents Interactions	Displays the number of interactions allocated to this service instance. To view additional usage metrics, click **Purchased Documents Interactions**.

Viewing Service Details

Click and select **View Details** to see details about your service:

- **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. See View Billing Metrics.
- **Resource Quotas:** Displays information about the purchased resources, including purchased amounts, remaining balances, and start and end dates for purchase. You can also configure alert rules to monitor the resource usage.
- **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. See View Business Metrics.

- **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.
- **Status:** Displays the service status of each active instance.

> **Note:**
>
> Some of these details are currently unavailable if you have a Universal Credits subscription.

See also Exploring the My Account Dashboard in *Managing and Monitoring Oracle Cloud*.

Add Web Analytics Tracking Snippets to Sites and Pages

A service administrator can add a snippet of JavaScript tracking code that gets added to sites for web analytics tracking, making it easier to integrate with external analytics providers like Google, Adobe, or Oracle Infinity. This snippet can also be added to individual sites and pages, and it can be customized for all sites or for individual sites and pages.

A service administrator can configure a script that will ripple down into all the sites and pages. At the site level, a service administrator can customize the script; for example, with a different web property ID for the site. At the page level, a service administrator can customize the snippet further, like marking the page as part of a campaign.

Add a Web Analytics Tracking Snippet for Sites

To add a web analytics tracking snippet for all sites in a Content and Experience Cloud instance:

1. Under **Administration** in the left navigation menu, choose **Settings**.
2. On the **Settings** page, from the **General** drop-down menu, choose **Sites**. Near the bottom of the site-specific settings is a Web Analytics Tracking Snippet area, where a service administrator can 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 || O:
function gtag0{dataLayer.push(arguments);}
gtag('js', new Date0;

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

   To revise the tracking snippet, click the **Edit** button at the bottom.

After the tracking snippet is added to the **Settings** page, whenever you create a new site, the snippet is added to the site's settings after you edit the site and turn it on.

Modify a Web Analytics Tracking Snippet for a Site

A service administrator can modify the snippet for a site:

1. In the left navigation menu, choose **Sites**.
2. Open the site.
3. In the top menu, select **View** and then provide a name and description for the update in the New Update dialog box.
4. In the **Settings** menu on the left, click **Analytics**.
5. In the JavaScript Tracking Snippet area, you can customize the script for site-specific tags, identifiers, or other tracking metrics.
6. At the top of the **Analytics** page, select **Enable tracking snippet for the site**.

   After you edit the snippet, a message says that the script has been modified. There is also a button you can click to revert your changes:**Restore to Latest Tenant Script**.
7. When you finish revising the tracking snippet, save the site.

To revert your changes in the tracking snippet for the site, click **Restore to Latest Tenant Script** at the bottom of the page and then save the site.

Modify a Web Analytics Tracking Snippet for a Page

A service administrator can modify a web analytics tracking snippet for a page in a site:

1. Open the **Settings** page for one of your site's pages.
2. Scroll down to the JavaScript Tracking Snippet area.
3. Customize the script for site-specific tags, identifiers, or other tracking metrics.
4. Under Analytics Options, select **Override tracking snippet on this page**.
5. After you edit the snippet, a message says that the script has been modified from the site script. There is also a button you can click to revert your changes: **Restore to Latest Site Script**.
6. When you finish revising the tracking snippet, save the page.

Viewing Site and Page Analytics Data

After you publish a site that includes a web analytics tracking snippet and bring the site 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.

Understand Visitor Sessions

A *visitor session* is metric used by Oracle Content and Experience Cloud 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 and Experience Cloud 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 and Experience Cloud content embedded in apps or websites. See Task and Feature Comparison by User Role.

Frequently Asked Questions

If a user accesses multiple pages within the same Oracle Content and Experience Cloud 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 and Experience Cloud resource such an Oracle Content and Experience Cloud instance, a site created with Oracle Content and Experience Cloud, 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 and Experience Cloud 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 and Experience Cloud standard or enterprise user be counted in visitor session counts?

No. An authenticated (signed-in) standard or enterprise user that visits an Oracle Content and Experience Cloud resource isn't included in visitor session counts.

Does the visitor session apply to authenticated (signed-in) users visiting an Oracle Content and Experience Cloud resource?

As stated above an authenticated Oracle Content and Experience Cloud standard or enterprise user that visits an Oracle Content and Experience Cloud 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 User 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 and Experience Cloud 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 and Experience Cloud? Will using the link be counted as visitor session?

Visiting the site created with Oracle Content and Experience Cloud 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 and Experience Cloud 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 and Experience Cloud 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 and Experience Cloud desktop application (the desktop application currently supports counting only named users).
- Tracking visits via the Oracle Content and Experience Cloud 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 and Experience Cloud sites will provide a standard option of letting the user know that a Oracle Content and Experience Cloud 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 and Experience Cloud 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. See Integrating Folder and File Selection and Applinks Resource in *Developing for Oracle Content and Experience Cloud*.

Examples

Here are some examples of visitor session counts. Let's assume ACME Corporation has an Oracle Content and Experience Cloud 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)

View Billing Metrics

The **Billing Metrics** page in the My Services application displays detailed usage information about your service.

1. Sign in to My Services using one of the following methods:

- Click the **Access your Cloud Services** link in the email with the subject: “Welcome to Oracle Cloud. Your Oracle Public Cloud Services are ready for use.”, and enter your user name and password.
- Sign in from Oracle Cloud. See Signing In From the Oracle Cloud Website in *Getting Started with Oracle Cloud*.

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.

Metrics for Universal Credits Subscriptions to Oracle Content and Experience Cloud

The following metrics apply to Universal Credits subscriptions to Oracle Content and Experience Cloud:

Metric	Description
Standard Users	Displays the number of standard users registered on this service instance. To view additional usage metrics, click **Standard Users**.
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**.
Daily Visitor Sessions	Displays the number of daily visitor sessions recorded on this service instance. To view additional usage metrics, click **Daily Visitor Sessions**. See Understand Visitor Sessions.

Metrics for Non-Metered Subscriptions to Oracle Content and Experience Cloud

The following metrics apply to non-metered subscriptions to Oracle Content and Experience Cloud:

Metric	Description
Purchased Content and Experience Standard Users	Displays the number of standard users registered on this service instance. To view additional usage metrics, click **Purchased Content and Experience Standard Users**.
Purchased Content and Experience 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 **Purchased Content and Experience Enterprise Users**.

Metric	Description
Purchased Content and Experience Daily 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 **Purchased Content and Experience Daily Visitor Sessions**. See Understand Visitor Sessions.

Metrics for Non-Metered Subscriptions to Oracle Documents Cloud Service

The following metrics apply to Oracle Documents Cloud Service subscriptions:

Metric	Description
Purchased Documents Storage	Displays the amount of storage space in GB allocated to this service instance. To view additional usage metrics, click **Purchased Documents Storage**.
Purchased Documents Users	Displays the number of users registered on this service instance. To view additional usage metrics, click **Purchased Documents Users**.
Purchased Documents Interactions	Displays the number of interactions allocated to this service instance. To view additional usage metrics, click **Purchased Documents Interactions**.

View Business Metrics

> **Note:**
>
> This page is currently unavailable if you have a Universal Credits subscription.

The **Business Metrics** page in the My Services application 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. After you sign in to the Oracle Content and Experience Cloud web application as an administrator, click **Settings** in the Administration area of the navigation menu.
2. In the **Settings** menu, click **Documents**.
3. Under **Service Metrics**, click **View Metrics**.
4. In the dashboard, click and select **View Details**.
5. 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 and Experience Cloud in the last 24 hour period, typically through the web client. Browsing Oracle Content and Experience Cloud 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.

Metric	Description
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 and Experience Cloud.
Used Content and Experience Daily Visitor Sessions	Displays the number of daily visitor sessions used in this instance. See Understand Visitor Sessions. This metric applies only if you have an Oracle Content and Experience Cloud.
Sites Created	Displays the number of sites created in this instance.
Sites Active	Displays the number of sites that are online and served by this instance.
Bandwidth Consumed (MB)	Displays the network bandwidth (in MB) used to serve sites pages.
Allocated Storage (GB)	Displays the amount of storage (in GB) that has been allocated to this instance.
Used Storage (GB)	Displays the amount of storage (in GB) that have been used in this instance.
Provisioned Documents Users	Displays the number of users that have been provisioned in this instance. This metric applies only if you have an Oracle Documents Cloud subscription.
Provisioned Content and Experience Standard Users	Displays the number of *standard* users that have been provisioned in this instance. This metric applies only if you have an Oracle Content and Experience Cloud subscription.
Provisioned Content and Experience Enterprise Users	Displays the number of *enterprise* users that have been provisioned in this instance. This metric applies only if you have an Oracle Content and Experience Cloud.
Documents Users in Use	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. This metric applies only if you have an Oracle Documents Cloud subscription.
Content and Experience Standard Users in Use	Displays the total days that all *standard* 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. This metric applies only if you have an Oracle Content and Experience Cloud.

Metric	Description
Content and Experience Enterprise Users in Use	Displays the total days that all *enterprise* 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. This metric applies only if you have an Oracle Content and Experience Cloud.

Report Issues

You can use My Services to report issues, access Oracle Support, get help, or create a service request.

To sign in to My Services, use one of the following methods:

- Click the **Access your Cloud Services** link in the email with the subject: “Welcome to Oracle Cloud. Your Oracle Public Cloud Services are ready for use.”, and enter your user name and password.
- Sign in from Oracle Cloud. See Signing In From the Oracle Cloud Website in *Getting Started with Oracle Cloud*.

You can perform the following support actions from My Services:

- To start a live online chat with an Oracle Support representative, click at the right edge of the My Services application.
- To view Oracle contact information, click at the right edge of the My Services application.
- To access My Oracle Support to search for solutions, use the My Oracle Support Community, or to create a service request, click the Create Service Request in the Quick Links section of the My Services dashboard.

8

Analyze Service Usage

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

The analytics refresh job runs once a week, during the weekend. With non-metered subscriptions, there's also a sync job that runs nightly.

Topics

- About Analytics
- About the Charts, Graphs, and Downloadable Report Files
- View the Dashboard
- View the Sites & Channels Analytics Dashboard
- Content Operations
- View General Statistics
- View Usage Patterns
- View Adoption Information
- View Reports and Metrics

About Analytics

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

The **Analytics** option is displayed only if it is available in your environment.

System users, the integration user, and the storage administrator (internal user types that are not actually Oracle Content and Experience Cloud users) are not included in the statistics.

The analytics refresh job runs once a week, during the weekend. With non-metered subscriptions, there's also a sync job that runs nightly.

To use the Oracle Content and Experience Cloud Analytics interface:

1. After you sign in to the Oracle Content and Experience Cloud 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, such as the total user population, total number of conversations, total size of the content being stored, daily active users, logins by device type (web client or iOS, for example), and so on. See View the Dashboard.
   - **Sites & Channels:** Displays the Sites & Channels Analytics Dashboard, which lets you see usage, utilization, and traffic analytics for your created sites and channels. See View the Sites & Channels Analytics Dashboard.

-
- **Content:** Users with a Manager role within at least one repository can use the **Content** option on the Analytics Dashboard to view metrics for repositories, collections, and channels.
- **General Statistics:** Shows totals and daily statistics for system objects, including users, conversations, messages, files, flags, and so on. See View General Statistics.
- **Usage Patterns:** Helps you identify trends by showing changes over time, such as conversation traffic, user login frequency, the number of messages of each type that are being created, the average number of flags assigned per user, and so on. See View Usage Patterns.
- **Adoption:** Helps you identify the user churn rate by showing statistics for new user participation, leaving users, and users who leave and then return. See View Adoption Information.
- **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. See View Reports and Metrics.

About the Charts, Graphs, and Downloadable Report Files

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 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.

For most tables and charts, you can download a CSV file containing the data being displayed. 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 Dashboard

The **Dashboard** page shows a summary of important usage statistics.

Statistic	Description
Overview	The **Overview** table shows the following metrics: • **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 and Experience Cloud 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 created.
Daily Active Users	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 and Experience Cloud using any client/device type (such as the browser, the desktop app, or a mobile device).
Daily New Assets	The line graph indicates a 30-day moving average of the number of new assets that were added.
Logins by Device Type	The pie chart indicates logins by device type, based on the total number of logins to Oracle Content and Experience Cloud. 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 and Experience Cloud.

See About the Charts, Graphs, and Downloadable Report Files for graph and chart features.

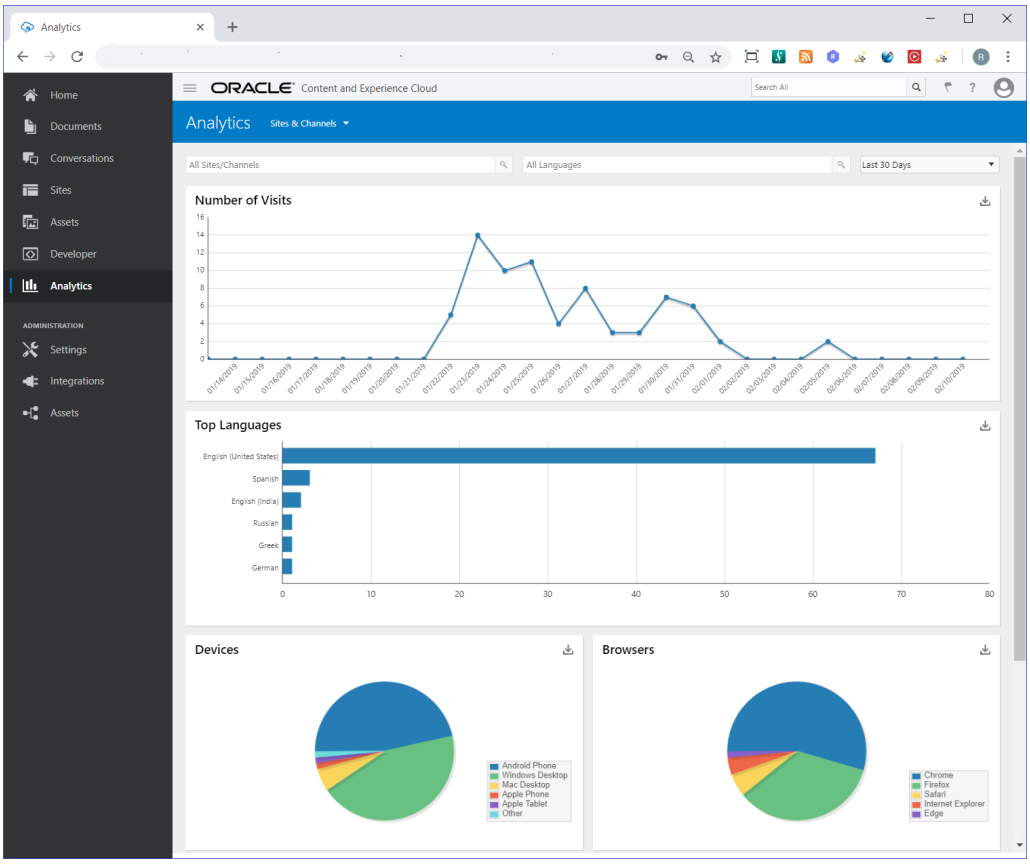
View the Sites & Channels Analytics Dashboard

The Sites & Channels Analytics Dashboard lets you see usage, utilization, and traffic analytics for your created sites and channels.

To view the Sites & Channels Analytics Dashboard:

1. After you sign in to the Oracle Content and Experience Cloud web application as an administrator, click **Analytics** in the navigation menu.
2. In the **Analytics** menu, choose **Sites & Channels**.

On this dashboard, a service administrator can view analytics for all of their sites and channels in all languages over a period of time. Or you can view analytics for specified sites, channels, and languages.



The Analytics for Sites & Channels dashboard include the following graphs and charts:

- A line graph indicates the number of visits over a number of days for sites and channels.

  This counts visits that 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.

  You can specify how many days your Number of Visits graph covers, like the last 30 days.
- A bar chart shows the six top languages for site and channel visits.
- Pie charts show devices and browsers used to visit sites and channels.
- Bar charts show the most visited and least visited sites and channels over a number of days.

You can download a graph or chart in a CSV file that contains the data being displayed. See About the Charts, Graphs, and Downloadable Report Files for graph and chart features.

Content Operations

Service administrators can use the **Content** option on the Analytics Dashboard 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.

The **Content** page shows analytics data for content items in repositories, collections, and channels.

When you choose an object in the **Content** menu, the **Content** page shows detailed metrics, trends, and reports. See About the Charts, Graphs, and Downloadable Report Files for graph and chart features.

You can choose from the following content objects:

- Repositories
- Collections
- Channels

Content Operations: Repositories

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 display metrics for a specific repository, enter the repository name in the search box at the top of the **Content Operations** page.

The following table describes the content metrics for repositories.

Metric	Description
Repositories	The number of repositories.
Collections	The number of collections in all or a specified repository.
Assets	The number of assets in all or a specified repository.
Channels	The number of channels in all or a specified repository.
Contributors	The number of contributors in all or a specified repository.
Total Repository Size (MB)	The size of all repositories or the selected repository over time, in megabytes, with a bar chart showing the total size of digital assets in blue and the total size of content items in green.
Assets Added	The number of assets added over time (default 30 days), in a line chart, with blue for digital assets and green for content items.
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 list	The name of each repository followed by its number of assets, number of collections, number of channels, and number of contributors.
Top Contributors	The user names of top contributors, and the number of assets added by each contributor for all time, the last 30 days, the current year, or a specified month.

Content Operations: Collections

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 display metrics for a specific collection, enter the collection name in the search box at the top of the **Content Operations** page.

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.
Published Assets	The number of published assets, which can be filtered by repository and collection. Each translation for a translated asset is counted separately.
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.
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.
Avg Collection Membership per Asset	The average number of collections an asset belongs to, in all or a specified repository.
Avg 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.
Assets Published	A bar chart that shows the number of assets published over time.
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.

Content Operations: Channels

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 display metrics for a specific channel, enter the channel name in the search box at the top of the **Content** page.

The following table describes the content metrics for channels.

Metric	Description
Channels	The number of channels, which can be filtered by repository and channel.
Published Assets	The number of published assets in all or a specified channel, which can be filtered by repository.
Pending Assets	The number of pending assets in Draft, In Review, Approved, or In Translation state, which have not yet been published to the specified channel(s) or rejected. This can be filtered by repository.

Metric	Description
Rejected Assets	The number of assets rejected and although targeted, have not been published to the specified channel(s). This can be filtered by repository.
Total Assets	The total number of assets in all or a specified channel, which can be filtered by repository.
Published Assets by Age	A bar chart that shows how long ago the assets were published, in all or a specified channel, which can be filtered by repository.
Assets Published	A bar chart of assets published over time, in all or a specified channel, which can be filtered by repository.
Assets by Content Type and Status	A bar chart that shows the number of assets for each content type in all or a specified channel, which can be filtered by repository. Blue is for published assets, green is for pending assets, and gold is for rejected assets. This can be filtered by repository.
Top Channels	A list of the top channels, with channel names and the number of published, pending, rejected, and total assets in each channel. This can be filtered by repository.
Assets by Translation	A list of languages for translations, with the number of published, pending, rejected, and total assets for each language in all or a specified channel. This can be filtered by repository.

View General Statistics

The General Statistics page shows detailed statistics for system objects.

When you click a system object in the left pane, the graphs and charts in the right pane show detailed statistics. The overview area at the top of the right pane shows averages for that system object. See About the Charts, Graphs, and Downloadable Report Files for graph and chart features.

Some graphs on this page 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.

You can choose from the following system objects:

- Users
- Documents
- Shared Links
- Conversations
- One-on-Ones
- Messages
- Flags
- Favorites
- Likes
- Hashtags

General Statistics: Users

To display the data for a particular group, enter the group name in the **Filter by Group** box. To return to the default search, All Groups, remove the group name from the search box and click the button next to it.

The following table describes the general statistics for users:

Statistic	Description
Overview	The overview shows the following information: • Total Number of Enabled Users (Total User Population) • Users Created Last 30 Days • Deprovisioned Users
Total Number of Enabled Users by Month	The blue line in the graph indicates the number of users that existed in the system during the previous 12 months; this is the same data shown in the Usage Statistics page. The green line in the graph 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 previous 12 months.

See About the Charts, Graphs, and Downloadable Report Files for graph and chart features.

General Statistics: Documents

To display the data for a particular group, enter the group name in the **Filter by Group** box. To return to the default search, All Groups, remove the group name from the search box and click the button next to it.

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.

Statistic	Description
Overview	The overview shows the following information: • Total Number of Files • Created in the Last 30 Days 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. Document counts go down as the result of deleting files.
Total Number of Files by Month	The line graph indicates the total number of files in the system during the previous 12 months.
Number of New Files per Day	The bar chart indicates the number of files added per day during the time period selected in the drop-down list.

See About the Charts, Graphs, and Downloadable Report Files for graph and chart features.

General Statistics: Shared Links

To display the data for a particular group, enter the group name in the **Filter by Group** box. To return to the default search, All Groups, remove the group name from the search box and click the button next to it.

The following table describes the general statistics for shared links:

Statistic	Description
Overview	The overview shows the following information: • Total Number of Shared Links • Created in the Last 30 Days
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.

See About the Charts, Graphs, and Downloadable Report Files for graph and chart features.

General Statistics: Conversations

To display the data for a particular group, enter the group name in the **Filter by Group** box. To return to the default search, All Groups, remove the group name from the search box and click the button next to it.

The following table describes the general statistics for conversations:

Statistic	Description
Overview	The overview shows the following information: • Total Number of Conversations • Created in the Last 30 Days
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.

See About the Charts, Graphs, and Downloadable Report Files for graph and chart features.

General Statistics: One-on-Ones

To display the data for a particular group, enter the group name in the **Filter by Group** box. To return to the default search, All Groups, remove the group name from the search box and click the button next to it.

The following table describes the general statistics for one-on-one conversations:

Statistic	Description
Overview	The overview shows the following information: • Total Number of One-on-Ones • Created in the Last 30 Days
Total Number of One-on-Ones by Month	The line graph indicates the total number of one-on-one conversations that existed in the system during the previous 12 months.
Number of New One-on-Ones per Day	The bar chart indicates the number of new one-on-one conversations created per day during the time period selected in the drop-down list.

See About the Charts, Graphs, and Downloadable Report Files for graph and chart features.

General Statistics: Messages

To display the data for a particular group, enter the group name in the **Filter by Group** box. To return to the default search, All Groups, remove the group name from the search box and click the button next to it.

Keep in mind that message totals include membership messages; for example, if a user adds another user to a conversation, the message announcing the addition is counted as part of the message total.

The following table describes the general statistics for messages:

Statistic	Description
Overview	The overview shows the following information: • Total Number of Messages • Created in the Last 30 Days Message totals include membership messages; for example, if a user adds another user to a conversation, the message announcing the addition is counted as part of the message total.
Total Number of Messages by Month	The line graph indicates the total number of messages that existed in the system during the previous 12 months.
Number of New Messages per Day	The bar chart indicates the number of new messages created per day during the time period selected in the drop-down list.

See About the Charts, Graphs, and Downloadable Report Files for graph and chart features.

General Statistics: Flags

To display the data for a particular group, enter the group name in the **Filter by Group** box. To return to the default search, All Groups, remove the group name from the search box and click the button next to it.

The following table describes the general statistics for flags:

Statistic	Description
Overview	The overview shows the following information: • Total Number of Flags • Created in the Last 30 Days
Total Number of Flags by Month	The line graph indicates the total number of flags that existed in the system during the previous 12 months.
Number of New Flags per Day	The bar chart indicates the number of new flags created per day during the time period selected in the drop-down list.

See About the Charts, Graphs, and Downloadable Report Files for graph and chart features.

General Statistics: Favorites

To display the data for a particular group, enter the group name in the **Filter by Group** box. To return to the default search, All Groups, remove the group name from the search box and click the button next to it.

The following table describes the general statistics for favorites:

Statistic	Description
Overview	The overview shows the following information: • Total Number of Favorites • Created in the Last 30 Days Favorite counts don't go down when items are removed as favorites.
Total Number of Favorites by Month	The line graph indicates the total number of items marked as favorites that existed in the system during the previous 12 months.
Number of New Favorites per Day	The bar chart indicates the number of new items marked as favorites per day during the time period selected in the drop-down list.

See About the Charts, Graphs, and Downloadable Report Files for graph and chart features.

General Statistics: Likes

To display the data for a particular group, enter the group name in the **Filter by Group** box. To return to the default search, All Groups, remove the group name from the search box and click the button next to it.

The following table describes the general statistics for likes:

Statistic	Description
Overview	The overview shows the following information: • Total Number of Likes • Created in the Last 30 Days
Total Number of Likes by Month	The line graph indicates the total number of items marked as liked that existed in the system during the previous 12 months.
Number of New Likes per Day	The bar chart indicates the number of new items marked as liked per day during the time period selected in the drop-down list.

See About the Charts, Graphs, and Downloadable Report Files for graph and chart features.

General Statistics: Hashtags

To display the data for a particular group, enter the group name in the **Filter by Group** box. To return to the default search, All Groups, remove the group name from the search box and click the button next to it.

Unless otherwise specified, hashtag statistics include hashtags that were created or reused.

The following table describes the usage pattern statistics for hashtags:

Statistic	Description
Overview	The overview shows the following information: • Total Number of Hashtags • Created in the Last 30 Days
Total Number of Hashtags by Month	The line graph indicates the total number of hashtags that existed in the system during the previous 12 months.
Number of Hashtags per Day	The bar chart indicates the number of new hashtags created per day during the time period selected in the drop-down list.

See About the Charts, Graphs, and Downloadable Report Files for graph and chart features.

View Usage Patterns

Usage pattern statistics allow you to identify trends by viewing changes that occur over time.

When you click a system object in the left pane, the graphs and charts in the right pane show detailed statistics. The overview area at the top of the right pane shows averages for that system object. See About the Charts, Graphs, and Downloadable Report Files for graph and chart features.

Some graphs on this page 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.

For information on the system object statistics, see the following topics:

- Users
- Documents
- Shared Links
- Conversations
- One-on-Ones
- Messages
- Flags
- Favorites
- Likes

- Hashtags
- Devices

Usage Patterns: Users

To display the data for a particular group, enter the group name in the **Filter by Group** box. To return to the default search, All Groups, remove the group name from the search box and click the button next to it.

The following table describes the usage pattern statistics for users:

Statistic	Description
Overview	The overview shows the following information: • Average Conversations Created per User • Average Messages per User • Average Files per User • Average Flags per User • Open Flags per User
Total Number of Enabled Users by Month	The blue line in the graph indicates the number of users that existed on the system during the previous 12 months; this is the same data shown in the General Statistics page. The green line in the graph shows the number of active users: those who have signed in at least one time.
New Users per Month	The line graph indicates the trend in new user additions for the previous 12 months.
Users by Country	The pie chart indicates the percentage of users by country, based on the total number of users in Oracle Content and Experience Cloud and the country code in each user's profile.
Unique User Logins per Day	The bar chart indicates the number of logins by different users per day, for the time period you choose in the drop-down list.
Users by Login Frequency	The pie chart categorizes users by login frequency, based on the total number of logins to Oracle Content and Experience Cloud: • Daily: four days per week or more • Weekly: less than daily users but more than three logins per month • Monthly: less than weekly users but at least one login per month • Yearly: less than one login per month, but at least one login per year
Number of Conversations per User	The bar chart indicates the total number of conversations created by users.
Number of Messages per User	The bar chart indicates the total number of messages created by users.
Number of Files per User	The bar chart indicates the total number of files uploaded by users. When a file is uploaded, the system may 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 counted in the total.

See About the Charts, Graphs, and Downloadable Report Files for graph and chart features.

Usage Patterns: Documents

To display the data for a particular group, enter the group name in the **Filter by Group** box. To return to the default search, All Groups, remove the group name from the search box and click the button next to it.

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

Statistic	Description
Overview	The overview shows the following information: • Average Number of Files Added per Day • Average Content Size Added per Day (in MB)
Total Content Size	The line graph indicates the total storage space used by files on the system during the previous 12 months.
Amount of Content per Day	Indicates the amount of file content added per day, during the time period selected in the drop-down list.
Document Views by Month	Indicates the number of views of documents that occurred during the previous 12 months.
Document Views by Day	Indicates the number of document views that occurred per day, during the time period selected in the drop-down list.

See About the Charts, Graphs, and Downloadable Report Files for graph and chart features.

Usage Patterns: Shared Links

To display the data for a particular group, enter the group name in the **Filter by Group** box. To return to the default search, All Groups, remove the group name from the search box and click the button next to it.

The following table describes the usage pattern statistics for shared links:

Statistic	Description
Overview	The overview shows the following information: • Average Shared Links per User • Percentage of Files Shared
Number of Shared Links per User	The bar chart indicates the total number of shared links created by users.
Active Users vs. Shared Links Users per Month	The blue line in the graph indicates the number of active users that existed on the system during the previous 12 months; active users are those who have signed in at least one time. The green line in the graph indicates the number of users who added at least one shared links during the same time period.

See About the Charts, Graphs, and Downloadable Report Files for graph and chart features.

Usage Patterns: Conversations

To display the data for a particular group, enter the group name in the **Filter by Group** box. To return to the default search, All Groups, remove the group name from the search box and click the button next to it.

The following table describes the usage pattern statistics for conversations:

Statistic	Description
Overview	The overview shows the following information: • Average Number of Users per Conversation • Average Number of Messages per Conversation
Number of Conversations Created by Users	The bar chart indicates the total number of conversations created by users.
Number of Conversations of Which Users are Members	The bar chart indicates the total number of members in conversations.
Unique Conversations Entered per Month	The line graph indicates the number of unique conversations that were visited during each month for the previous 12 months.
Unique Conversations Entered per Day	The line graph indicates the number of unique conversations that were visited during each day for the time period selected in the drop-down list.

See About the Charts, Graphs, and Downloadable Report Files for graph and chart features.

Usage Patterns: Messages

To display the data for a particular group, enter the group name in the **Filter by Group** box. To return to the default search, All Groups, remove the group name from the search box and click the button next to it.

Keep in mind that message totals include membership messages; for example, if a user adds another user to a conversation, the message announcing the addition is counted as part of the message total.

The following table describes the usage pattern statistics for messages:

Statistic	Description
Overview	The overview shows the following information: • Average Messages per User • Average Messages per Conversation • Average Messages per One-on-One
Number of Messages per User	The bar chart indicates the number of messages created by users.
Total Messages	The pie chart indicates the percentage of messages that were created in conversations, one-on-ones, user walls, collection walls, and group walls, based on the total number of messages in the system.
Message Type Trend	The line graph shows trends in the locations where messages were posted during the previous 12 months.

See About the Charts, Graphs, and Downloadable Report Files for graph and chart features.

Usage Patterns: Flags

To display the data for a particular group, enter the group name in the **Filter by Group** box. To return to the default search, All Groups, remove the group name from the search box and click the button next to it.

The following table describes the usage pattern statistics for flags:

Statistic	Description
Overview	The overview shows the following information: • Average Flags per User • Open Flags per User • Cleared Flags per User
Number of Open Flags per User	The bar chart indicates the total number of open flags for users.
Number of Cleared Flags per User	The bar chart indicates the total number of cleared flags for users.
Number of Flags per User	The bar chart indicates the total number of flags that were assigned.
Active Users vs. Flags Users per Month	The blue line in the graph indicates the number of active users that existed on the system during the previous 12 months; active users are those who have signed in at least one time. The green line in the graph indicates the number of users who assigned at least one flag during the same time period.

See About the Charts, Graphs, and Downloadable Report Files for graph and chart features.

Usage Patterns: Favorites

To display the data for a particular group, enter the group name in the **Filter by Group** box. To return to the default search, All Groups, remove the group name from the search box and click the button next to it.

The following table describes the usage pattern statistics for favorites:

Statistic	Description
Overview	The overview shows the following information: • Average Favorites per User • Favorite Files • Favorite Folders • Favorite Conversations Favorite counts don't go down when items are removed as favorites.
Number of Favorites per User	The bar chart indicates the total number of items marked as favorites per user.
Favorites by Type	The pie chart categorizes favorites by type (conversations, files, and any other system objects), based on the total number of favorites in Oracle Content and Experience Cloud.
Active Users vs. Favorites Users per Month	The blue line in the graph indicates the number of active users that existed on the system during the previous 12 months; active users are those who have signed in at least one time. The green line in the graph indicates the number of users who have marked at least one item as a favorite during the same time period.

See About the Charts, Graphs, and Downloadable Report Files for graph and chart features.

Usage Patterns: Likes

To display the data for a particular group, enter the group name in the **Filter by Group** box. To return to the default search, All Groups, remove the group name from the search box and click the button next to it.

The following table describes the usage pattern statistics for likes:

Statistic	Description
Overview	The overview shows the following information: • Average Likes per User
Number of Likes per User	The bar chart indicates the total number of items marked as like per user.
Active Users vs. Likes Users per Month	The blue line in the graph indicates the number of active users that existed on the system during the previous 12 months; active users are those who have signed in at least one time. The green line in the graph indicates the number of users who have liked at least one item during the same time period.

See About the Charts, Graphs, and Downloadable Report Files for graph and chart features.

Usage Patterns: Hashtags

To display the data for a particular group, enter the group name in the **Filter by Group** box. To return to the default search, All Groups, remove the group name from the search box and click the button next to it.

Unless otherwise specified, hashtag statistics include hashtags that were created or reused.

The following table describes the usage pattern statistics for hashtags:

Statistic	Description
Top Hashtags	The list initially displays hashtags in order from most to least used, based on the entire history of the Oracle Content and Experience Cloud instance. You can choose to display the ranking for the last 30 days or the last 12 months using the drop-down list. You can search for a particular hashtag by typing its name in the **Search** box. Click a hashtag in the list to see the number of times it was used each month for the past 12 months; the information displays in the **Number of Hashtags per Month** line graph. Return to the global statistics by clicking the X icon above the graph.
Number of Hashtags per Month	The line graph initially displays the number of new hashtags per month for the entire history of the Oracle Content and Experience Cloud instance. If you click an individual hashtag in the **Top Hashtags** list, the line graph shows the number of times it was used each month for the past 12 months. Return to the global statistics by clicking the X icon above the graph.
Active Users vs. Hashtag Users per Month	The blue line in the graph indicates the number of active users that existed on the system during the previous 12 months; active users are those who have signed in at least one time. The green line in the graph indicates the number of users who have created at least one hashtag during the same time period.

See About the Charts, Graphs, and Downloadable Report Files for graph and chart features.

Usage Patterns: One-on-Ones

To display the data for a particular group, enter the group name in the **Filter by Group** box. To return to the default search, All Groups, remove the group name from the search box and click the button next to it.

The following table describes the usage pattern statistics for one-on-one conversations:

Statistic	Description
Overview	The overview shows the following information: • Average One-on-Ones per User
Number of One-on-Ones per user	The bar chart indicates the total number of one-on-one conversations created by users.
Active Users vs. One-on-Ones per Month	The blue line in the graph indicates the number of active users that existed on the system during the previous 12 months; active users are those who have signed in at least one time. The green line in the graph indicates the number of one-on-one conversation users during the same time period.

See About the Charts, Graphs, and Downloadable Report Files for graph and chart features.

Usage Patterns: Devices

To display the data for a particular group, enter the group name in the **Filter by Group** box. To return to the default search, All Groups, remove the group name from the search box and click the button next to it.

The following table describes the usage pattern statistics for devices:

Statistic	Description
Logins by Device Type	The pie chart categorizes logins by device type, based on the total number of logins to Oracle Content and Experience Cloud. The Java API "device" represents programmatic logins.
Device Type Trend	The line graph shows trends in device logins during the previous 12 months.

See About the Charts, Graphs, and Downloadable Report Files for graph and chart features.

View Adoption Information

The **Adoption** page helps you assess the user adoption of Oracle Content and Experience Cloud by showing statistics for new users, churned users, length of consistent usage, and a ranked list of the users in your environment, based on their activity level.

Keep these considerations in mind when viewing the data on the **Adoption** page:

- The graphs on this page show data for the previous 12 months. If you do not have a complete month of data on your system yet, the graphs will be empty.
- An *active user* is a user who has signed in at least once during the time period being measured.
- The statistics do not include deactivated users (such as users who left the company) or internal users (such as non-visible users created to run automated processes). If a previously deactivated user is re-activated, that user is counted as a returning user.

To display the data for a particular group, enter the group name in the **Filter by Group** box. To return to the default search, All Groups, remove the group name from the search box and click the button next to it.

The following table describes the **Adoption** page:

Statistic	Description
Active User Base Changes	The bar chart shows the following metrics describing active users: • New Users: number of users who were active for the first time during the month. • Returning Users: number of users who were active during the month who were not active the previous month, but who were active at some time in the past. • Leaving Users (Churn): number of users who were not active during the month, but who were active the previous (contiguous) month. • Net Change (line graph superimposed on the bar chart): the number of new users plus returning users, minus leaving users.
Monthly Churn Rate	The line graph indicates the percentage of leaving users over time; that is, the percentage of the total number of users who were not active during the month but who had been active the previous (contiguous) month.
Average Consecutive Months of Use	The line graph indicates, for each month, the average months of consecutive use of all users in the system, prior to and including that month.
Top Users	The table shows a ranked list of the users in your environment, based on their activities. Users receive a ranking value for each column; the overall rank is based on the average of all individual rankings. The statistics are based on the entire history of the Oracle Content and Experience Cloud instance.

View Reports and Metrics

Reports and metrics enable you to see information about your system usage and activity.

From the **Reports and Metrics** page, you can perform the following actions:

- Run reports
- If you have a non-metered subscription, you can also monitor service activity

> **Note:**
>
> If you have a Universal Credits subscription, you can view service metrics from My Services. To sign in to My Services, use one of the following methods:
>
> - Click the **Access your Cloud Services** link in the email with the subject: “Welcome to Oracle Cloud. Your Oracle Public Cloud Services are ready for use.”, and enter your user name and password.
> - Sign in from Oracle Cloud. See Sign In to Your Account From the Oracle Cloud Website in *Getting Started with Oracle Cloud*.

Run Reports

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 and Experience Cloud web application as an administrator, click **Analytics** in the navigation menu.
2. In the **Analytics** menu, click **Reports and Metrics**.
3. Select a report:
   - **User List:** Shows basic system information about each user in the Oracle Content and Experience Cloud instance. The report is displayed in order by user ID (email address).
     - **User ID**—The system-assigned numerical ID for the user. This is the user's unique identifier within the system, of the form `/ServiceRoot/GUID/` 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 (T) or disabled (F) on the system.
     - **Service Administrator**—Indicates the roles for the user. T means the user is assigned the role. F means the user isn’t assigned the role. If all user role entries are **F**, the user is an Employee without any additional roles.
   - **User Logins by Device Type:** Shows each user and the number of logins using each client/device. The report is displayed in user name order.
   - **Documents Usage Log:** Shows the following information about the documents in your system, within the last three months:
     - **Activity**—The type of activity performed (upload, view, download, delete).
     - **Activity Date**—The date the activity occurred.
     - **User**—The user that performed the activity.
     - **Type**—The target of the activity (file or folder).
     - **Name**—The name of the file or folder.

- **GUID**—The unique identifier of the file or folder.
- **Folder Name**—The name of the parent folder.
- **File Size**—The size of the file, in megabytes.

Columns are all sortable when downloading CSV to Excel. For the onscreen report, it is sorted by activity date in descending order (most recent activity at the top). No other field is sortable on the screen.

Click on any report to export the data as a CSV file.

The reports are based on the entire history of your Oracle Content and Experience Cloud instance, except for **Documents Usage Log**, which is based on the last three months of activity.

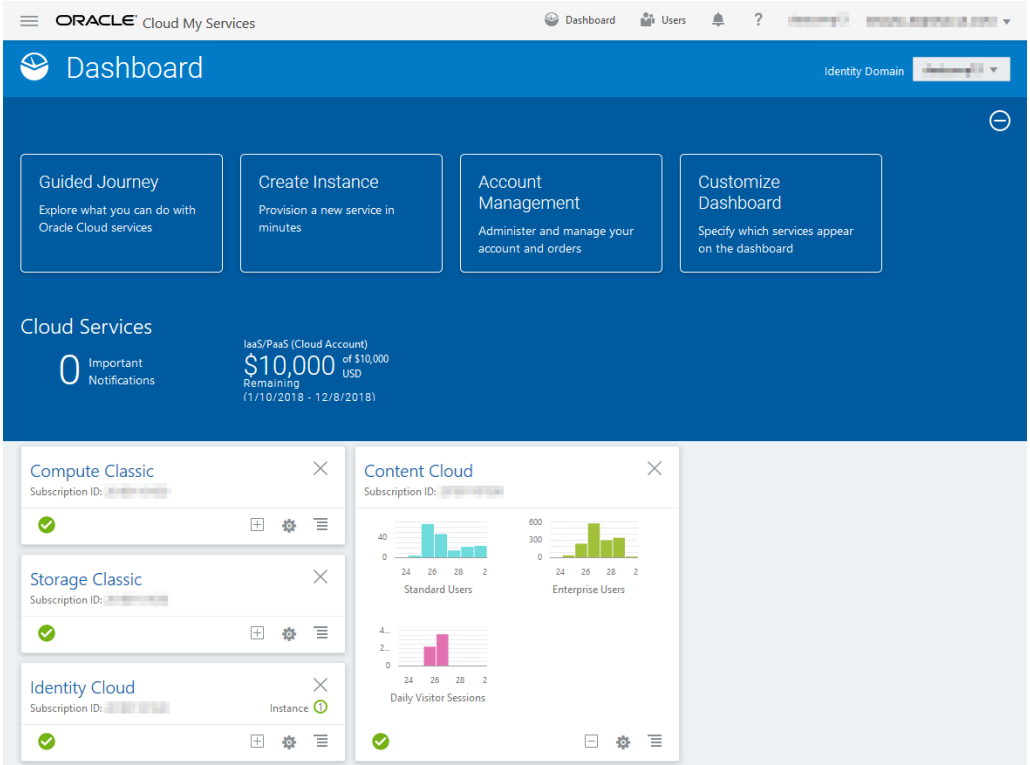
Monitor Service Activity

You can check the overall status of your active Oracle Cloud services in the My Services dashboard. You can view the overall service status, outages, and uptime percentages for the past 14 days. You can also see the storage used, and other details. 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.

To sign in to My Services, use one of the following methods:

- Click the **Access your Cloud Services** link in the email with the subject: “Welcome to Oracle Cloud. Your Oracle Public Cloud Services are ready for use.”, and enter your user name and password.
- Sign in from Oracle Cloud. See Sign In to Your Account From the Oracle Cloud Website in *Getting Started with Oracle Cloud*.

Only four metrics show on the dashboard. To change the metrics you see on the dashboard, click



Metrics for Universal Credits Subscriptions to Oracle Content and Experience Cloud

The following metrics apply to Universal Credits subscriptions to Oracle Content and Experience Cloud:

Metric	Description
Standard Users	Displays the number of standard users registered on this service instance. To view additional usage metrics, click **Standard Users**.
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**.
Daily Visitor Sessions	Displays the number of daily visitor sessions recorded on this service instance. To view additional usage metrics, click **Daily Visitor Sessions**. See Understand Visitor Sessions.

Metrics for Non-Metered Subscriptions to Oracle Content and Experience Cloud

The following metrics apply to non-metered subscriptions to Oracle Content and Experience Cloud:

Metric	Description
Purchased Content and Experience Standard Users	Displays the number of standard users registered on this service instance. To view additional usage metrics, click **Purchased Content and Experience Standard Users**.
Purchased Content and Experience 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 **Purchased Content and Experience Enterprise Users**.
Purchased Content and Experience Daily 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 **Purchased Content and Experience Daily Visitor Sessions**. See Understand Visitor Sessions.

Metrics for Non-Metered Subscriptions to Oracle Documents Cloud Service

The following metrics apply to Oracle Documents Cloud Service subscriptions:

Metric	Description
Purchased Documents Storage	Displays the amount of storage space in GB allocated to this service instance. To view additional usage metrics, click **Purchased Documents Storage**.
Purchased Documents Users	Displays the number of users registered on this service instance. To view additional usage metrics, click **Purchased Documents Users**.
Purchased Documents Interactions	Displays the number of interactions allocated to this service instance. To view additional usage metrics, click **Purchased Documents Interactions**.

Viewing Service Details

Click and select **View Details** to see details about your service:

- **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. See View Billing Metrics.
- **Resource Quotas:** Displays information about the purchased resources, including purchased amounts, remaining balances, and start and end dates for purchase. You can also configure alert rules to monitor the resource usage.
- **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. See View Business Metrics.

- **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.
- **Status:** Displays the service status of each active instance.

> **Note:**
>
> Some of these details are currently unavailable if you have a Universal Credits subscription.

See also Exploring the My Account Dashboard in *Managing and Monitoring Oracle Cloud*.

A

Troubleshoot

This section helps you troubleshoot administrative functions for Oracle Content and Experience Cloud.

- 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
- I need to check the service utilization metrics
- Users can't connect to the service using the sync client
- I need to find out who deleted a file or folder
- I need to downsize my instance
- Users can't sign in after migration (storage overage)

I can't access the administration pages

Make sure you have been granted the Oracle Content and Experience Cloud Administrative role for the service instance.

1. Sign in to My Services using one of the following methods:
   - Click the **Access your Cloud Services** link in the email with the subject: "Welcome to Oracle Cloud. Your Oracle Public Cloud Services are ready for use.", and enter your user name and password.
   - Sign in from Oracle Cloud. See Sign In to Your Account From the Oracle Cloud Website in *Getting Started with Oracle Cloud*.
2. In the dashboard, next to the service you want to check, click and select **View Details**.
3. The icons at the top of the Overview page represent the roles you've been assigned for the service. Hover over an icon to see the role name.

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

1. After you sign in to the Oracle Content and Experience Cloud web application as an administrator, click **Settings** in the Administration area of the navigation menu.
2. In the **Settings** 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 and Experience Cloud web application as an administrator, click **Settings** in the Administration area of the navigation menu.
2. In the **Settings** 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.

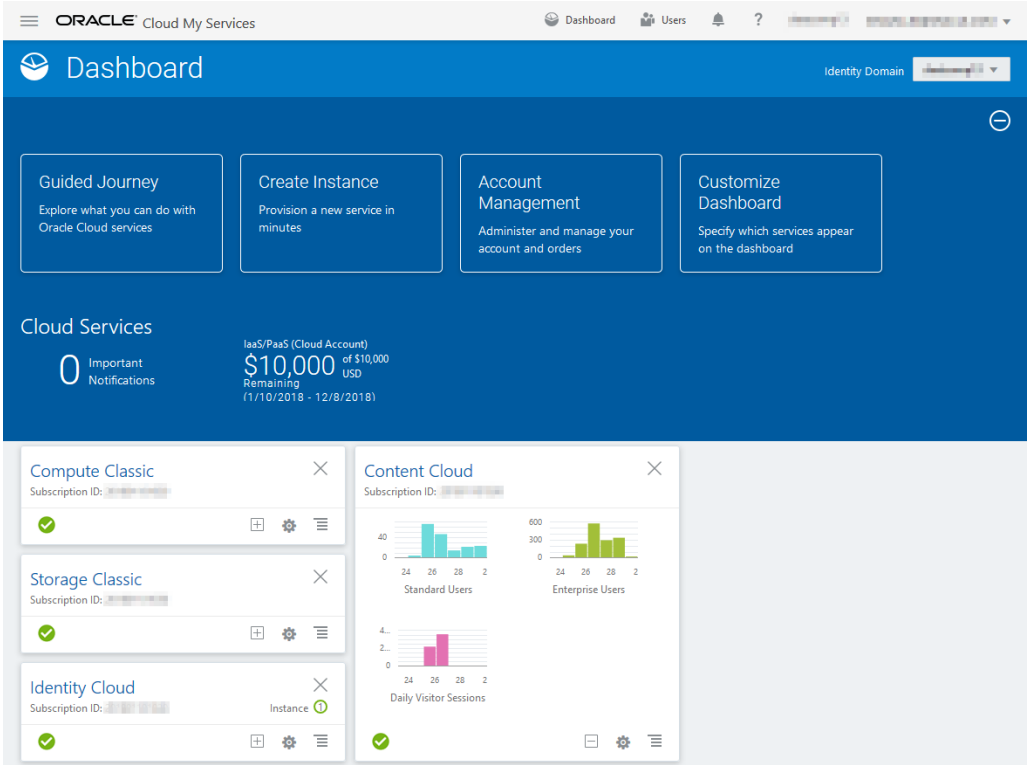
Users are provisioned on their first login, so this is handled on a first-come, first-serve basis.

I need to check the service utilization metrics

Service metrics are published on the My Services page. To sign in to My Services, use one of the following methods:

- Click the **Access your Cloud Services** link in the email with the subject: “Welcome to Oracle Cloud. Your Oracle Public Cloud Services are ready for use.”, and enter your user name and password.
- Sign in from Oracle Cloud. See Sign In to Your Account From the Oracle Cloud Website in *Getting Started with Oracle Cloud*.

The dashboard shows you the current status of the service, the used storage, and the total documents uploaded in the past day. The service availability and up-time information are continually updated, but the remainder of the metrics are updated once a day, so the metrics shown are gathered from the previous day.



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 and Experience Cloud 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 **Movetotrash** or **Moverevisiontotrash**.

Click to export the data as a CSV file.

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 and Experience Cloud, 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 Transfer File Ownership and Add Users.
2. Modify the service:
   a. Sign in to My Services using one of the following methods:
      - Click the **Access your Cloud Services** link in the email with the subject: "Welcome to Oracle Cloud. Your Oracle Public Cloud Services are ready for use.", and enter your user name and password.
      - Sign in from Oracle Cloud. See Sign In to Your Account From the Oracle Cloud Website in *Getting Started with Oracle Cloud*.
   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 and Experience Cloud 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 My Services, using one of the following methods:
   - Click the **Access your Cloud Services** link in the email with the subject: "Welcome to Oracle Cloud. Your Oracle Public Cloud Services are ready for use.", and enter your user name and password.
   - Sign in from Oracle Cloud. See Sign In to Your Account From the Oracle Cloud Website in *Getting Started with Oracle Cloud*.
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 and Experience Cloud page should show Oracle Content and Experience Cloud 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 and Experience Cloud page, update the number of users to accommodate the storage needs for the instance. Each user gets 100GB storage. So, if the email said you were exceeding your storage by 500GB, you'd need to add 5 users.

B

Supported Software, Devices, Languages, and File Formats

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

Topics

- Supported Web Browsers
- Supported Software
- Supported Mobile Devices
- Supported Languages
- Supported File Formats

Supported Web Browsers

Oracle Content and Experience Cloud supports the following web browsers:

- Microsoft Internet Explorer: version 11*
- Microsoft Edge: version 12*
- Mozilla Firefox and Firefox Extended Support Release (ESR): version 35 or higher
- Google Chrome on Windows: version 45 or higher
- Apple Safari on Mac: version 9 or 10
- Apple Safari for iOS: on supported Apple devices
- Google Chrome for Android: on supported Android devices

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

Supported Software

Oracle Content and Experience Cloud supports the following software:

- Microsoft Windows: 7, 8.1, 10 (32- and 64-bit)

> **Note:**
>
> Oracle Content and Experience Cloud relies on Internet Explorer's embedded browser controls, so you must have Internet Explorer 11 or higher installed on your system. You don't need to use Internet Explorer as your browser.

- Microsoft Office 2010, 2013, 2016
- Microsoft Outlook 2010, 2013, 2016
- Apple Mac: OS X 10.11 (El Capitan), macOS 10.12 (Sierra), macOS 10.13 (High Sierra)

> **Note:**
>
> The new Apple File System (APFS), available in macOS 10.13 (High Sierra), is supported. If you upgraded an older HFS+ file system to APFS, you must delete your old Oracle Content account using the desktop app preferences menu and then add it again on the new APFS volume.

Supported Mobile Devices

Oracle Content and Experience Cloud mobile apps can run on the following devices:

- Apple iPhone and iPad: running iOS 10 or 11
- Android phones and tablets: running Android 5.0 or higher

Supported Languages

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

- Czech (cs)
- Danish (da)
- German (de)
- Greek (el)
- English (en)
- Spanish (es)
- Finnish (fi)
- French (fr)
- French - Canada (fr_CA)
- 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 and Experience Cloud can handle document content, file names, conversation messages, etc. in many additional languages.

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 *Managing Content with Oracle Content and Experience Cloud*.

Service administrators can configure a fallback language to be used if no web browser locale setting is available. See Set the Default Time Zone and Language.

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 and Experience Cloud can display or play the content of a wide variety of files directly in the web client or mobile apps.

Supported Audio and Video File Formats

Here are a few best practices:

- It's best to use MP4 formats.
- Keep file sizes less than 10 MB. Files over 10 MB aren't full-text indexed.
- Maximum upload size for a file is 5 GB.
- File names are limited to the characters and length supported by Windows and Macintosh.

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 and Experience Cloud 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 and Experience Cloud interface.

The following formats are supported for viewing directly:

- Internet Explorer: mp4
- 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	
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	
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	✓

Extension	Description	Full-Text Indexed
dot, dotx	Microsoft Word templates	✓
wri	Microsoft Write	
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	✓
txt*, text*, list, log, c, cpp, h, java, json, key, bat, sh, m, md, mm, plist	Plain-text files (various)	* ✓
tif, tiff	TIFF images	

C

Oracle Documents Cloud

If you have an older non-metered subscription, you might have an entitlement to Oracle Documents Cloud. The user interface is basically the same as Oracle Content and Experience Cloud, but some of the set up is different.

- If you previously used Oracle Documents Cloud Service, you need to migrate to Oracle Content and Experience Cloud after you renew your subscription. See Migrate to Oracle Content and Experience Cloud
- If you have a non-metered subscription with an Oracle Documents Cloud entitlement and you need to create an instance, see Create an Oracle Documents Cloud Service Instance.
- The user roles in Oracle Documents cloud are slightly different than in Oracle Content and Experience Cloud. See User Roles in Oracle Documents Cloud.

> **Note:**
>
> Oracle Documents Cloud *service users* are the same as Oracle Content and Experience Cloud *standard users*. Any feature described in the documentation as associated with *enterprise users* isn't available in Oracle Documents Cloud.

Migrate to Oracle Content and Experience Cloud

If you previously used Oracle Documents Cloud Service, you need to migrate to Oracle Content and Experience Cloud after you renew your subscription.

Things to know before you renew your subscription and migrate to Oracle Content and Experience Cloud:

- Each user gets 100GB storage. You add storage by purchasing more users. To ensure you have enough storage, you should purchase enough users to cover the 500GB 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 1000GB storage, so you'd want to purchase 10 standard and/or enterprise users in Oracle Content and Experience Cloud.
- 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 My Services using one of the following methods:
   - Click the **Access your Cloud Services** link in the email with the subject: "Welcome to Oracle Cloud. Your Oracle Public Cloud Services are ready for use.", and enter your user name and password.
   - Sign in from Oracle Cloud. See Sign In to Your Account From the Oracle Cloud Website in *Getting Started with Oracle Cloud*.
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 and Experience Cloud page should show Oracle Content and Experience Cloud 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 User 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 Add Users.

For troubleshooting, see Users can't sign in after migration (storage overage).

Next, create groups for the roles in your organization. See Create Groups for Your Organization.

Create an Oracle Documents Cloud Service Instance

If you have a non-metered subscription with Oracle Documents Cloud, follow the instructions in this topic to create a service instance.

If you haven't subscribed to Oracle Cloud, activated your service, set up your cloud account, or you're not sure what type of subscription you have, see Subscribe to Oracle Cloud.

To create an Oracle Documents Cloud instance with a non-metered subscription:

1. Click the **Access your Cloud Services** link in the email with the subject: "Welcome to Oracle Cloud. Your Oracle Public Cloud Services are ready for use.", and enter your user name and password.
2. Sign in from Oracle Cloud:
   a. Go to http://cloud.oracle.com.
   b. Click **Sign In**.
   c. From the **Cloud Account** menu, select **Cloud Account with Identity Cloud Service**.
   d. In the **Cloud Account Name** field, enter the name of your cloud account.
   e. Click **My Services**.
   f. Enter the user name and password for your cloud account.
3. On the Create New Oracle Documents Cloud Service 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 and Experience Cloud** from the list.
Product	Select **Documents Cloud Service** from the list.
Number of Users	Enter the number of users 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 a Documents Cloud Service entitlement.
Additional Number of Storage Packs	Enter the additional number of storage packs you need for this instance. One storage pack equals 100GB of storage.
Additional Number of Interaction Packs	Enter the number of interaction packs you expect to use with this instance each month. One interaction pack equals 50,000 additional interactions per month.
Administrator Details	Enter the administrator's email, user name, first name, and last name.

See Create a Service Instance in *Getting Started with Oracle Cloud*.

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 and Experience Cloud. The first email includes a link to My Services (click the link to your instance). The second email includes a link to the Oracle Content and Experience Cloud web client.

Next, create groups for you organization. See Create Group Standards for Your Organization and Create Groups for Your Organization.

User Roles in Oracle Documents Cloud

There are several predefined user roles for Oracle Documents Cloud which define what users can do. Some functionality is available only to users with specific user roles. People can hold multiple user roles as needed. For example, you might want to designate one person as both an *account administrator* and a *service administrator*. These user roles are assigned by the *identity domain administrator*. See Add Users for information on assigning user roles.

Visitors can view certain sites, use public links, and view Oracle Content and Experience Cloud content embedded in apps or websites. Anonymous users (users that aren't signed in) are counted as visitors. See Change Site Security in *Creating Experiences with Oracle Content and Experience Cloud*.

Any users that need to actually *use* Oracle Content and Experience Cloud 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 and Experience Cloud *standard users*. Any feature described in the documentation as associated with *enterprise users* isn't available in Oracle Documents Cloud.

Each user assigned a user 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 user 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.

User Role (user role name in bold)	Access and Actions	Notes
Account administrator	Account administrators use the My Account application to perform the following actions: • 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. See My Account Adminsitration in *Managing and Monitoring Oracle Cloud*.	Account administrators are set up when the account is created. They use their Oracle account to sign in to Oracle Cloud and access My Services or My Account. If you need account administrator access and don't have it, contact your primary account administrator. See Roles and User Accounts Predefined in My Services in *Getting Started with Oracle Cloud*. If you want account administrators to use Oracle Content and Experience Cloud and modify the service configuration, they must also be assigned the *service user* role.
Identity domain administrator (**Identity Domain Administrator**)	From the My Services application: • Create and manage user accounts. • Assign and manage user roles, including creating custom user roles. See Roles and User Accounts Predefined in My Services in *Getting Started with Oracle Cloud*.	Assigned at the domain level. Works across multiple services. See Roles and User Accounts Predefined in My Services in *Getting Started with Oracle Cloud*. Identity domain administrators perform the same functions that a service administrator can, plus they handle administrative duties related to users. There is only one service per identity domain for Oracle Content and Experience Cloud. One administrator performs the duties of the *service administrator* and the *identity domain administrator*.
Entitlement administrator The format of the role name is *service-name_SE service name Based Entitlement Administrator*; for example, **documents_SE Documents Service Based Entitlement Administrator**.	From the My Services application: • Create, manage, and view details of service instances. Applies when you're subscribed to an entitlement to create multiple instances of Oracle Content and Experience Cloud. • Monitor status of service instances, and export instance metrics data. See Subscribe to Oracle Cloud.	Assigned at the service level. See Roles and User Accounts Predefined in My Services in *Getting Started with Oracle Cloud*.

User Role (user role name in bold)	Access and Actions	Notes
Service administrator (**Oracle Documents Cloud Administrator**)	From the My Services application: • Assign user roles. • Change user passwords and challenge questions. • Configure, monitor, and manage service instances. From Oracle Content and Experience Cloud **Administration: Settings** interface: • 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 sites settings such as whether sites can be created and installing the default site templates. • Configure application settings such as those described in Integrate with Oracle Process Cloud Service, Integrate with Oracle Eloqua Cloud Service, and Manage Custom Applications. Some of these features are currently unavailable if you have a universal credits subscription. • Configure custom properties (must also have **Oracle Content and Experience Cloud Enterprise User** role). • View reports.	Service administrators must also be assigned the *service user* role to be able to use Oracle Content and Experience Cloud.

User Role (user role name in bold)	Access and Actions	Notes
	From Oracle Content and Experience Cloud **Analytics** interface: • View service usage statistics to help you analyze system needs or issues.	
Site administrator (**Oracle Content and Experience Cloud Site Administrator**)	From Oracle Content and Experience Cloud **Sites** page: • Create sites. From Oracle Content and Experience Cloud **Developer** page: • Create templates, components, and themes. See Configure Sites and Assets Settings	This role applies if your service administrator configured Oracle Content and Experience Cloud to allow only site administrators to create sites, templates, or components. Site administrators must also be assigned the *service user* role to be able to use Oracle Content and Experience Cloud.
Developer (**CECDeveloperUser**)	From Oracle Content and Experience Cloud **Sites** page: • Create, edit, and publish sites as long as this feature hasn't been limited to *site administrators*. From Oracle Content and Experience Cloud **Developer** page: • Create templates, components, and themes as long as these features haven't been limited to *site administrators*.	Developers must also be assigned the *service user* role to be able to use Oracle Content and Experience Cloud.

User Role (user role name in bold)	Access and Actions	Notes
Service user (**Oracle Documents Cloud Service User**)	From Oracle Content and Experience Cloud, *service users* have access to: • 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 *site administrators*. • Create templates, components, and themes as long as these features haven't been limited to *site administrators*. • 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 and Experience Cloud must be assigned the *service user* role. This role isn't assigned by default to any user.
Visitor (**Oracle Content and Experience Cloud Visitor**)	Access sites restricted to *visitors*.	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 Change Site Security in*Creating Experiences with Oracle Content and Experience Cloud*. Visitors don't require a license. Visitor usage is counted as part of daily visitor sessions. See Understand Visitor Sessions.

User Role (user role name in bold)	Access and Actions	Notes
Integration user (**Social Network Integration User**)	Used to impersonate another user while performing operations through the Social REST endpoints of the REST API for Collaboration.	Create a dedicated “Integration User” and assign it the integration user role. \This role is for an internal user, not an actual person. Users assigned this role can’t use the Oracle Content and Experience Cloud user interface. See “Social Resource” in REST API for Collaboration.
External user (**CECExternalUser**)	Reserved for future use.	Do not use this role. Users assigned this role can’t use the Oracle Content and Experience Cloud user interface.