



NewgenONE

Content Cloud

Administration Guide

Version: 2024.2

Disclaimer

This document contains information proprietary to Newgen Software Technologies Ltd. User may not disclose or use any proprietary information or use any part of this document without written permission from Newgen Software Technologies Ltd.

Newgen Software Technologies Ltd. makes no representations or warranties regarding any software or to the contents or use of this guide. It also specifically disclaims any express or implied warranties of merchantability, title, or fitness for any particular purpose. Even though Newgen Software Technologies Ltd. has tested the hardware and software and reviewed the documentation, it does not guarantee or imply that this document is error free or accurate regarding any particular specification. As a result, this product is sold as it is and user, the purchaser, is assuming the entire risk as to its quality and performance. Further, Newgen Software Technologies Ltd. reserves the right to revise this publication and make changes in its content without any obligation to notify any person, of such revisions or changes. Newgen Software Technologies Ltd. authorizes no Newgen agent, dealer or employee to make any modification, extension, or addition to the above statements.

Newgen Software Technologies Ltd. has attempted to supply trademark information about company names, products, and services mentioned in this document. Trademarks indicated below were derived from various sources.

Copyright © 2024 **Newgen Software Technologies Ltd.** All Rights Reserved.

No part of this publication may be reproduced and distributed without the prior permission of Newgen Software Technologies Ltd.

Newgen Software, Registered Office, New Delhi

E-44/13

Okhla Phase - II

New Delhi 110020

India

Phone: +91 1146 533 200

info@newgensoft.com

Contents

- Preface 5**
 - Revision history 5
 - About this guide..... 5
 - Intended audience 5
 - Related documents 6
 - Documentation feedback 6
- Introduction to NewgenONE Content Cloud 7**
- Getting started 8**
 - Registering a new tenant account..... 8
 - Signing in to NewgenONE Content Cloud 9
 - Resetting password..... 9
 - Exploring home page 10
 - Changing password 12
- Metering Dashboard 13**
 - Managing subscription plan 15
 - Filtering a business activity report 16
- Micro UI 18**
 - Creating a new Micro UI 18
 - Actions on Micro UI 23
 - Previewing Micro UI 23
 - Opening a Micro UI..... 23
 - Embedding code for Micro UI 23
 - Editing Micro UI 24
 - Deleting Micro UI 24
 - Using the Micro UI 24
 - Advance folder view 25
 - Document viewer 26
 - Folder View..... 27
 - Advance Search 28
- Roles Management..... 30**
 - Creating a role 30
 - Creating a class..... 33
 - Deleting a class..... 33
 - Creating a tag 34
- User Management..... 35**
 - Registering a new user 35
 - Operations on created users 36
 - Editing 36

- Deactivating 37
- Application Registration..... 38**
 - Registering an application..... 38
- Data Class Management..... 41**
 - Creating a Data Class..... 41
 - Modifying a Data Class..... 43
 - Deleting a Data Class..... 43
- Audit Log 44**
 - Filtering audit logs..... 46
 - Viewing API Log details 48

Preface

This chapter provides information about the purpose of this guide, details on the intended audience, revision history, and related documents for NewgenONE Content Cloud.

Revision history

Revision date	Description
October 2024	Initial publication

About this guide

This guide explains how to perform administrative operations for managing the Micro User Interfaces (UIs), roles, users, data class, and OAuth 2.0 application registration. This guide also describes the metering dashboard to have a comprehensive view of your user activities.

To ensure you are referring to the latest and most recent revision of this guide, download it from one of the following locations:



- [Newgen Internal Doc Portal](#), if you are a Newgen employee.
- [Newgen Partner Portal](#), if you are a Newgen partner.

Intended audience

This guide is intended for tenant administrators responsible for managing and monitoring the tenant created in the content services platform. The reader can be a knowledge worker with a basic understanding of using cloud native Software as a Service (SaaS) applications. The reader can also be a developer with a basic

understanding of web development concepts like consuming REST APIs and using iframes. The reader must have access to the Internet.

Related documents

The following documents are related to NewgenONE Content Cloud for Admin:

- NewgenONE Content Cloud User Guide for Micro UI
- NewgenONE Content Cloud Developer Guide

Documentation feedback

To provide feedback or any improvement suggestions on technical documentation, write an email to docs.feedback@newgensoft.com.

To help capture your feedback effectively, share the following information in your email.

- Document name
- Version
- Chapter, topic, or section
- Feedback or suggestions

Introduction to NewgenONE Content Cloud

NewgenONE Content Cloud allows you to register a new tenant account. This account provides you access to the microservices-based REST APIs for content services. It also offers a comprehensive view through the dashboard to view user activities under your tenancy, application registration for quick integrations, user and rights management, and Micro UI creation for file viewing capability.

Getting started

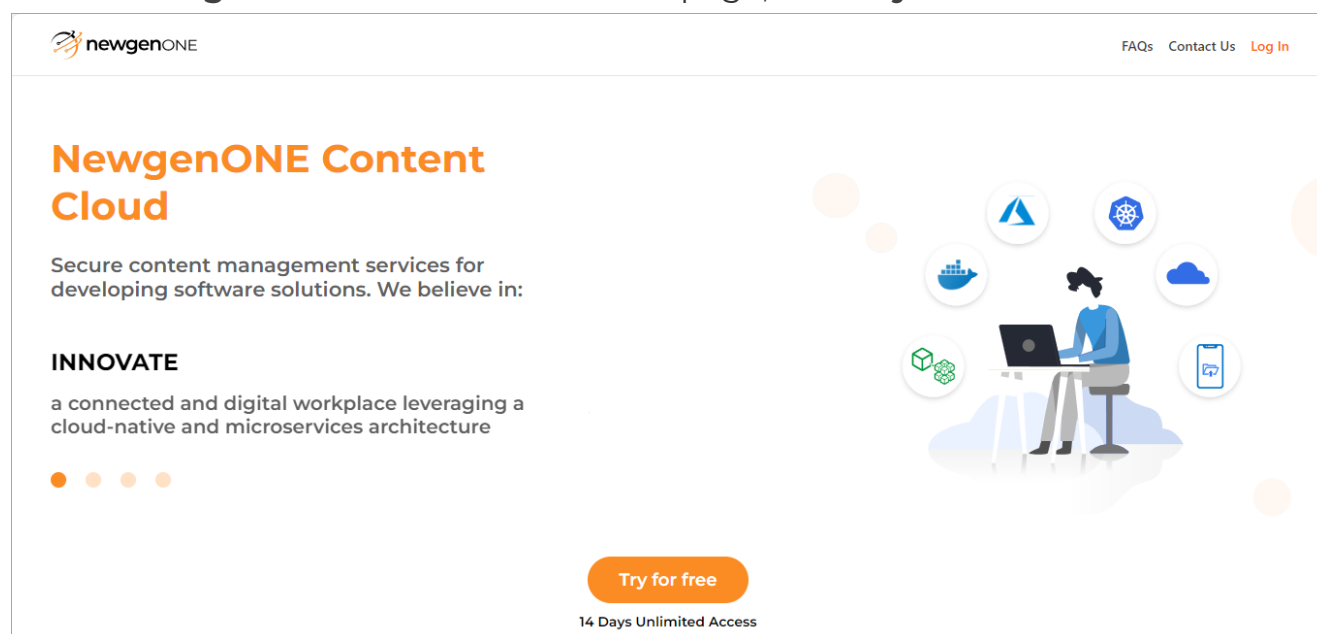
This chapter describes how to get started with the administration module of NewgenONE Content Cloud. It includes the following sections:

- [Registering a new tenant account](#)
- [Exploring home page](#)

Registering a new tenant account

To register a new tenant account, perform the following steps:

1. On the **NewgenONE Content Cloud** web page, click **Try for free**.



The page to sign up for a tenant account appears.

2. Fill the required details. Fields marked with * are mandatory to fill. The Password must follow the below criteria:
 - At least 1 capital letter.
 - At least 1 numeric.
 - At least 1 punctuation.
 - At least 8-16 characters.

- No space allowed.
3. Click **Sign Up** to receive an activation link on your registered email address.
 4. Go to your registered email and open the activation link mail.
 5. Click the **ACTIVATE ACCOUNT NOW** link to activate the registered account. Once the account is activated, you can sign in using your registered account details.

Signing in to NewgenONE Content Cloud

To sign in to NewgenONE Content Cloud Admin, perform the following steps:

1. Go to the NewgenONE Content Cloud web page.
2. Click **Log In** displayed on the top-right corner of the page. The section to enter sign-in details appears.
3. Enter your registered email address and click **Continue**. The message “Verification code has been sent to your registered email address.” appears.
4. Enter the verification code sent to your registered email address. If the verification code expires, you can request a new verification code using the **Resend** button.



The verification code is valid only for 10 minutes. You cannot reuse an expired verification code.

5. Click **Verify**. The additional fields to sign in appear. If the selected user is part of multiple Organizations, then click the **Organization Name** dropdown menu and select the required option.
6. Enter the remaining details and click **Sign In**. The NewgenONE Content Cloud Admin home page appears.

Resetting password

In case you forget the password of your registered email address, you can reset it from the Log In page.

To reset your password, perform the following steps:

1. On the Log In page, verify the email address and verification code. The additional fields to sign in appear.
2. Click the **Forgot password?** link to reset your password.


The page to enter your forgotten email address appears to receive a reset password link.

3. Enter your email address and click **Send Verification Code**. The message “Verification code has been sent to your registered email address. appears.
4. Enter the verification code sent to your registered email address. If the verification code expires, you can request a new verification code using the **Resend** button.
5. Click **Verify**. The additional field to select the organization name appears. In case you are registered through multiple organizations, then select the required organization to continue.
6. Click **Send Link for Reset**. The Link to reset your password is sent to your registered email address.
7. Go to your registered email address and open the respective mail to reset your password.
8. Click the **CHANGE PASSWORD** link. The page to reset the password appears.
9. Enter the new password. The password must follow the below criteria:
 - At least 1 capital letter.
 - At least 1 numeric.
 - At least 1 punctuation.
 - At least 8-16 characters.
 - No space allowed.
10. Click **Change Password**. Once the password resets successfully, you can sign in with the updated password.




Exploring home page

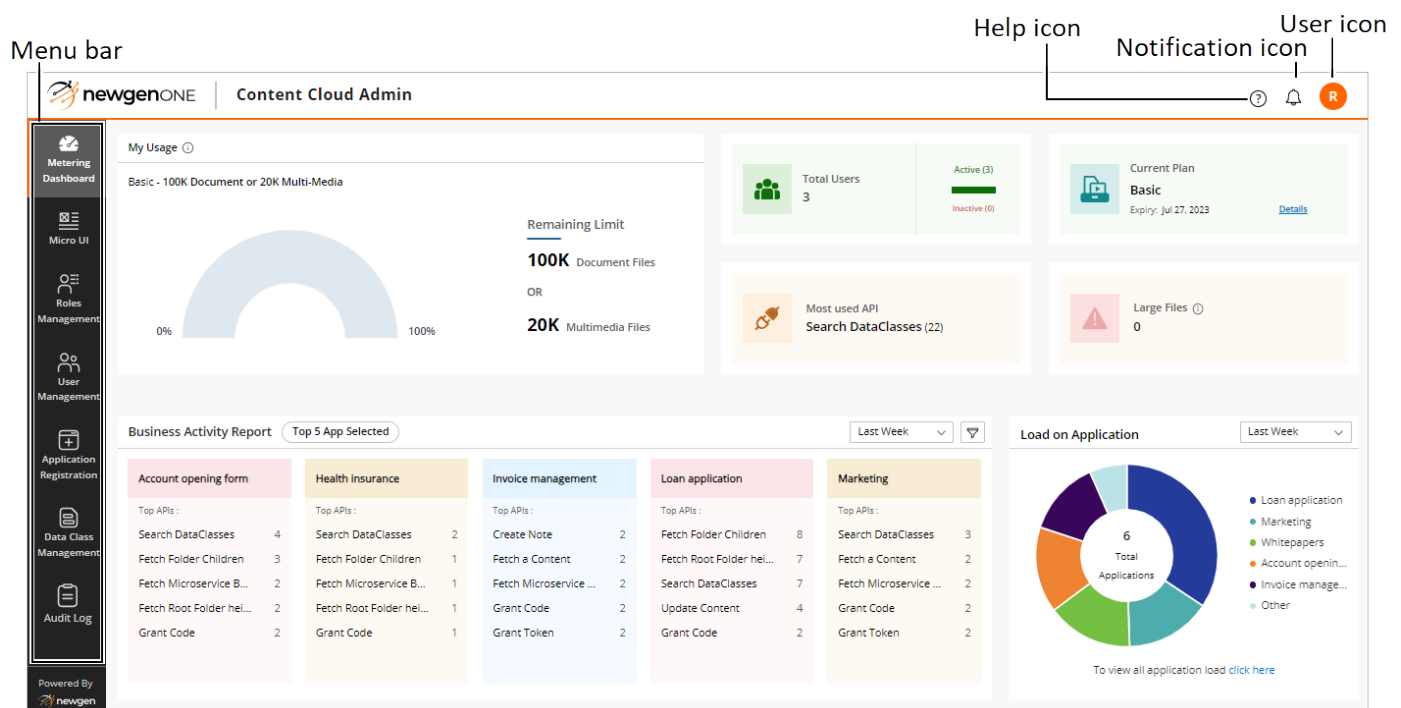
On successful sign-in, the NewgenONE Content Cloud Admin home page appears. You can view the following options on this page:

- **Menu bar** — The Menu bar allows you to access the following tabs:
 - [Metering Dashboard](#)
 - [Micro UI](#)
 - [Roles Management](#)
 - [User Management](#)
 - [Application Registration](#)
 - [Data Class Management](#)
 - [Audit Log](#)

- **Help icon** — Selecting the Help icon redirects you to the NewgenONE Content Cloud Administration Guide which helps you to understand and perform various administrative tasks.
- **Notification icon** — Selecting the Notification icon displays messages triggered by certain defined events. Whenever there is any notification, the notification icon  appears with a count in blue, indicating the number of notifications. Once you select a notification to mark it as read, its background changes to white.

The notifications are classified into the following categories:

- **Successful**  — Indicates that a certain activity was implemented successfully.
- **Information**  — Provides general information or updates.
- **Warning**  — Alerts you when your subscription plan is about to expire, you are currently in your grace period, or any other subscription plan expiry notifications.
- **User icon** — Selecting the User icon displays information about the signed-in user, including their username, organization name, and the number of subscription days remaining. It also allows you to change your password and sign out from the NewgenONE Content Cloud Admin module. You can raise a request for Newgen's executive support using the Request Support button. Additionally, you can view the API documentation and perform the required API operations using the API Guide & Try-out button.



Changing password

The NewgenONE Content Cloud Admin home page provides you with the option to change your login password.

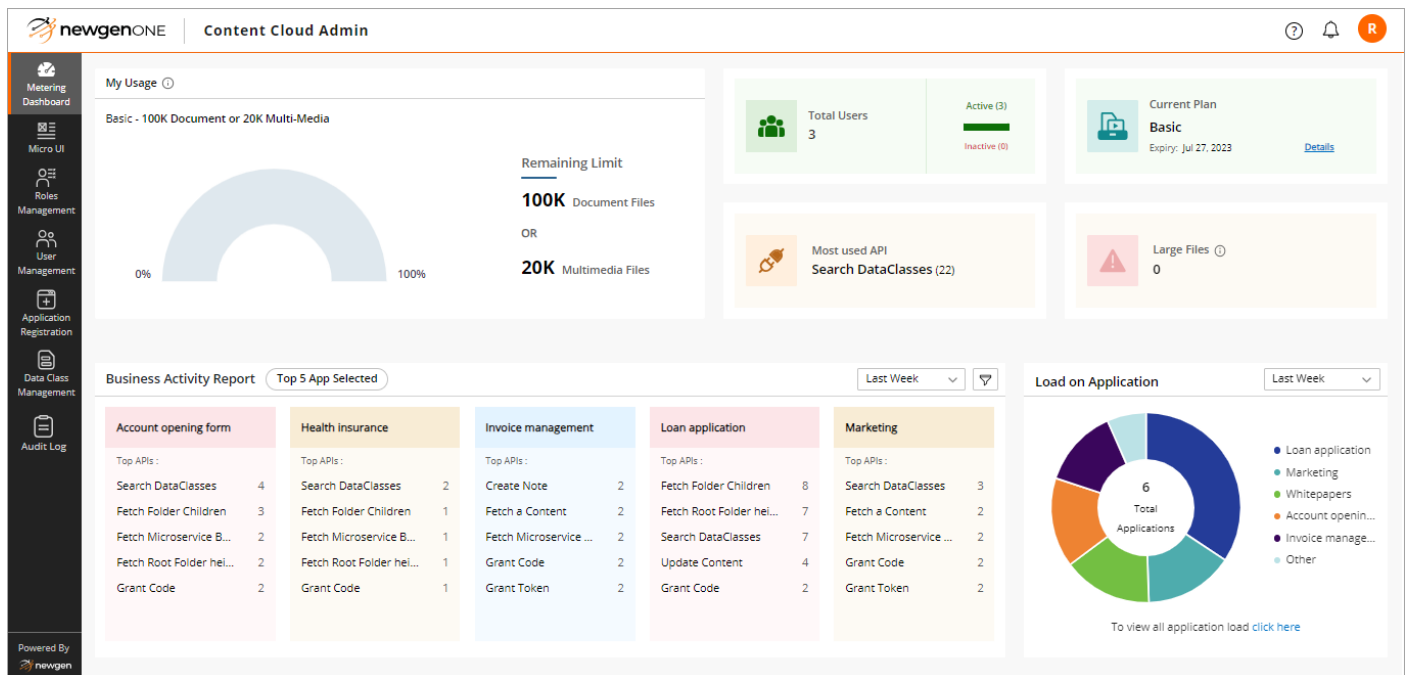
To set a new password, perform the following steps:

1. On the Admin home page, click the **User icon** displayed at the top-right corner of the page.
2. Select **Change Password**. The Change Password dialog appears.
3. Enter the required details. Fields marked with * are mandatory to fill. The password must follow the below criteria:
 - At least 1 capital letter
 - At least 1 numeric
 - At least 1 punctuation
 - At least 8-16 characters
 - No space allowed
4. Click **Change**. The message “Password has been reset successfully” appears.

Metering Dashboard


The Metering Dashboard empowers you with a comprehensive view of your user activities. It enables you to gain insights and make quick decisions for your strategic priorities.

To access the Metering Dashboard, on the NewgenONE Content Cloud Admin home page, click the **Metering Dashboard** tab from the menu bar. By default, the Metering Dashboard tab appears when you sign in to NewgenONE Content Cloud Admin.



The Metering Dashboard consists of the following sections:

Section	Description
My Usage	<p>This section displays your existing subscribed plan that includes the plan's total limit allotted, limit consumed, and the remaining limits. Here, the limit signifies the number of documents and multimedia files that you can upload into the organization's current system.</p> <p>In case you purchased an add-on plan, an add-on graph also appears in the My Usage section by default.</p> <p>You can also hover over the graph to see the extent of your current usage.</p>

Section	Description
Total Users	This section displays the total number of users existing on your tenant portal that includes the count of activated and inactivated users. The inactivated users are those who have been invited but have not registered on the NewgenONE Content Cloud portal under your tenancy.
Current Plan	This section displays your current subscribed plan and its expiration date. In the Current Plan section, you can click the Details link to view further details of your upcoming plan (if already requested and invoiced), current plan status, add-on plan status, and your overall plan history since your association with NewgenONE Content Cloud. For more details, refer to the Managing subscription plan section.
Most used API	This section displays the count of most consumed API by all the active users currently under your tenancy.
Large Files	This section displays the count of files that are larger than 500 MB in size. These files are not included in any of the subscription plans by default and are categorized separately.
Business Activity Report	The default setting of this section displays the top five most used applications and the top five APIs consumed within these applications. You can view the business activity report for a time duration ranging from the last one hour to the past one year and also get an option to choose a custom date range, based on your business requirements. Additionally, you can use the custom filter to obtain more details about a specific application and its associated APIs, allowing you to understand the corresponding number of requests and their average response time. For procedural details, refer to the Filtering a business activity report section.
Load on Application	<p>This section displays the percentage of loads on the top five most used applications. You can filter the required applications as per the time duration. You can also click the click here link to view the load and the total number of requests on each application in the tenant's current system.</p> <p> The click here link is displayed only if there are more than five applications registered.</p>

Managing subscription plan

This section explains how to manage your current subscribed plan.

In the Current Plan section of the Metering Dashboard tab, you can click the **Details** link to open the Plan Details page. This page contains detailed information about your upcoming plan (if already requested and invoiced), current plan status, add-on plan status, and your overall plan history since your association with NewgenONE Content Cloud.

The screenshot displays the 'Plan Details' page with a sidebar on the left containing navigation links: Metering Dashboard, Micro UI, Roles Management, User Management, Application Registration, Data Class Management, and Audit Log. The main content area is titled 'Plan Details' and includes a 'Large Files: 0' indicator.

Current Plan section:

Plan Name	Start Date	Expiry Date	Total Limit	Used Limit
Enterprise	May 6, 2024	May 6, 2025	1000K Docs or 200K Media	0 Docs & 0 Media(0.000%)

Below the table is a progress bar showing 0% usage of the 1000K Docs or 200K Media limit. Buttons for 'Request Add On' and 'Request Upgrade' are present.

Add On Plan section:

Plan Name	Start Date	Expiry Date	Total Limit	Used Limit	Status
Documents	May 6, 2024	May 6, 2025	100K Document	0 Documents (0%)	In Progress
Documents	May 6, 2024	May 6, 2025	100K Document	0 Documents (0%)	In Progress

A 'Request Add On' button is located at the top right of this section.

Plan History section:

Plan Name	Start Date	Expiry Date	Total Limit	Used Limit	Add on Plan
Basic	May 6, 2024	May 20, 2024	100K Docs or 20K Media	0 Docs & 0 Media (0%)	0

The page is powered by NewgenONE.

The Plan Details page consists of the following sections:

- Upcoming Plan** — This section displays your upcoming subscribed plan status which includes the requested upcoming plan name, start date, expiry date, and total limit allotted.

The Upcoming Plan section only appears if you have subscribed to a new plan before your current plan expires.
- Current Plan** — This section displays your current subscription plan status which includes your existing plan name, start date, expiry date, total limit allotted, and consumed limit of the plan. It also displays a progress bar that shows the consumption of your current plan limit.

In case your current plan is getting expired or you want to upgrade to a new plan, you can raise a request for it. To request an upgrade, renewal, or update in

your current plan, click **Request Upgrade**. A notification is sent to your Newgen representative.

- **Add On Plan** — This section displays the status of your subscribed add-on plan which includes the add-on plan category subscribed consisting of the add-on plan name, start date, expiry date, total limit allotted, and consumed limit of the add-on plan.

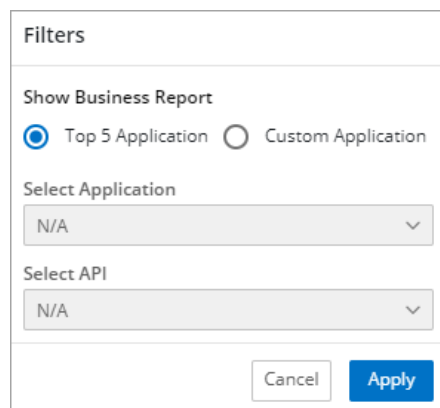
In case your current plan limit gets exhausted, you can raise a request for an add-on plan. The NewgenONE Content Cloud offers two add-on plans, one for storing documents and another for storing multimedia files. To request an add-on plan, click **Request Add On**. A notification is sent to your Newgen representative.

- **Plan History** — This section tracks all your subscription plans since your registration on the NewgenONE Content Cloud portal. It includes all the subscription plan names, their start dates, expiry dates, total limits allotted, consumed limit, and the status of the add-on plan throughout the years.

Filtering a business activity report

To filter a business activity report, perform the following steps:

1. On the Business Activity Report section, click the filter icon . The Filters dialog appears.



The image shows a 'Filters' dialog box with the following elements:

- Filters** (Title)
- Show Business Report** (Section Header)
- Two radio buttons: **Top 5 Application** (selected) and **Custom Application**.
- Select Application** (Label)
- A dropdown menu showing **N/A** with a downward arrow.
- Select API** (Label)
- A dropdown menu showing **N/A** with a downward arrow.
- At the bottom, there are two buttons: **Cancel** and **Apply**.

2. Click the **Custom Application** option.
3. From the **Select Application** dropdown list, select the required application.
4. From the **Select API** dropdown list, select the required API. Here, you can select multiple APIs simultaneously.

5. Click **Apply**. The filter gets applied and displays information about the selected API. You can clear the applied filter using the **Clear** button next to the filter icon.

Micro UI

The Micro UI capability in NewgenONE Content Cloud offers independent interfaces of the content service platform for consuming the microservices-based APIs. It allows the users to access and perform basic operations on files and folders stored in NewgenONE Content Cloud. Micro UIs are available for browsing through files and folders, it also displays interactive interfaces for documents, images, audio, videos, and so on. You can embed these pre-built Micro UIs into your application using the embeddable URL generated for each Micro UI.

To access the Micro UI tab, click the **Micro UI** tab from the menu bar. The tab displaying all created Micro UI appears. This tab allows you to search a specific Micro UI using the search box.

Creating a new Micro UI

The NewgenONE Content Cloud Micro UI home page provides you with the option to create a Micro UI.



- Once you create a new Micro UI, silently OAuth 2.0 application is also created with it. The created application appears in the Application Registration tab.
- Only the user who is part of the Admin role can create, edit, and delete a Micro UI.

To create a new Micro UI, perform the following steps:

1. On the Micro UI home page, click **+New Micro UI**. The Create New Micro UI page appears. This page comprises four tabs to configure a Micro UI:
 - **Basic Details**
 - **Login Details**
 - **Integration Type**
 - **Summary**

By default, the Basic Details tab appears on the Create New Micro UI page.

2. In the Basic Details tab, specify the following details:

- **Application Name** — Name of the Micro UI.
- **Window Title** — Tab name that appears on the browser. It contains a maximum of 50 characters.
- **Comments** — This optional field allows you to enter additional information related to the Micro UI. It contains a maximum of 128 characters limit.



- Fields marked with * are mandatory to fill.
- The Application Name and Window Title fields must follow the below criteria:
 - It contains a maximum of 1-50 characters limit.
 - Leading or trailing spaces are not allowed.
 - Special characters are not allowed except “-” and “_”.
 - Numbers are allowed.

3. Click **Next**. The Login Details tab appears. This tab consists of three different login configurations that are as follows:

- Login UI Flow: It provides information about **Your generated secret code**, **Redirect URI**, and **Whitelisted Domain** under **OAuth 2.0 Web Flow**.
- Auth Token Flow: It provides information about **Your generated secret code**. In this login configuration, generate a token from the OAuth authentication and append it to the generated embedded URL to access the user portal.
- Static Credential Flow: Enter the email-id, password, and confirm password. When run in a browser, the embedded URL allows you to sign in to the user portal directly without the credentials.



You can save the Micro UI configuration at any level by clicking **Save Draft** at the bottom left of each tab. The saved Micro UI appears on the Micro UI tab. You can click the **More actions** icon **⋮** against the Micro UI and select Edit to reconfigure the Micro UI.
The NewgenONE Content Cloud Micro UI does not allow you to perform the Preview and Embed Code actions on a Micro UI saved as a draft.

All the Login UI Flow and Auth Token Flow tab fields are filled automatically.

4. Click **Next**. The Integration Type tab appears.

5. Select the relevant integration type from the following list using the Integration Type dropdown:

- **Advance Folder View** — This integration allows the end user to add folders and files. For example, in a multi-level folder hierarchy, users view subfolders directly without accessing the main folder. Only forward navigation is permitted, and creating and uploading files and folders is allowed.
- **Document Viewer** — This integration allows the end user to view the documents.


- **Folder View** — This integration allows the end user to select a specific path to view a document. For example, in a multi-level folder hierarchy, users view subfolders directly without accessing the main folder. Only forward navigation is permitted, and creating or uploading files and folders is not allowed.
- **Advance Search:** This integration allows you to select a specific path to search content within files and folders. For instance, in a multi-level folder hierarchy, it lets you search contents in subfolders directly without needing to access the main folder.

6. Specify the details as follows:

Field	Applicable integration types	Description
Integration Type	Advance Folder View, Document Viewer, Folder View, Advance Search	It provides information about the type of MicroUI.
Enable Header	Advance Folder View, Document Viewer, Folder View, Advance Search	Enables the NewgenONE header on the user interface. Select the checkbox to enable the header.
Enable Comments	Document Viewer	Allows the user to comment on a file.
Enable FTS	Advance Search	Allows the user to search the files and folder.
Layout	Advance Folder View, Document Viewer, Folder View	It allows you to select a layout for the user to display the folder list. The available layout options are as follows: <ul style="list-style-type: none"> • List and Grid View — Select this option to display the folder list in both list and grid view. • List view — Select this option to display the folder list in the list view. • Grid View — Select this option to display the folder list in grid view.
Zoom Level	Document Viewer	Set the zoom level of the document viewer. By default, Fit to Width is selected. This is only applicable to the document viewer integration type.

Field	Applicable integration types	Description
Document Viewer Layout	Advance Folder View, Document Viewer, Folder View, Advance Search	<p>It allows you to set the view of the document for the user. The available document viewer layout options are as follows:</p> <ul style="list-style-type: none"> • Full Screen — Select this option to view the files in full-screen mode. • Embedded View — Select this option to view the file in embedded form. By default the first file in the folder is open.
Search On	Advance Search	It allows you to specify whether to apply the search to documents, folders, or both.
Batch Size	Advance Search	Specify the number of results that you want to display after searching. It displays a minimum of 15 and a maximum of 50 at a time.
Look In Folder	Advance Folder View, Folder View, Advance Search	It allows you to select the folder for the operations you can perform. It lets you view the subfolder directly without accessing the main folder. Only forward navigation is permitted and you cannot create and upload the files only in case of folder view.

Field	Applicable integration types	Description
Operations Allowed	Advance Folder View, Document Viewer, Folder View, Advance Search	<p>It allows you to select the different actions for the user to perform on a folder and file. The actions are as follows:</p> <ul style="list-style-type: none"> • Rename — This operation allows the user to rename folders and files. • Download — This operation allows the user to download files. • Move — This operation allows the user to move folders and files into another folder available in the folder list. • Copy — This operation allows the user to create a copy of folders and files in another folder available in the folder list. • Delete — This operation allows the user to delete folders and files. • Audit Log — This operation allows the user to view the audit logs. • Versioning — This operation allows the user to update the version of the documents.

7. Click **Next**. The message “Micro UI created successfully” appears.
8. The Summary tab appears and provides the following details:
 - The summary of the published Micro UI.
 - The **Embeddable URL** and **Embeddable Code**. You can copy the embeddable URL and use the published Micro UI in a separate browser tab. You can also copy the embeddable code and embed it into the source code of an application to use the published Micro UI.
 - To delete the created Micro UI, click the **More actions** icon  at the page's top-right corner and select **Delete**.
 - Click **Preview** to view the published Micro UI. The Preview page appears.
 - Click **Finish** to exit from the Micro UI configuration page.

Actions on Micro UI


The supported actions of Micro UI are described in the following sub-sections:

- [Previewing Micro UI](#)
- [Opening a Micro UI](#)
- [Embedding code for Micro UI](#)
- [Editing Micro UI](#)
- [Deleting Micro UI](#)

Previewing Micro UI

The Preview feature allows you to view a published Micro UI interface that appears to the end user.

To preview a Micro UI, perform the following steps:

1. On the Micro UI page, click the **More actions** icon  against the required Micro UI.
2. Select **Preview**. The Preview page of the selected Micro UI appears.

Opening a Micro UI

This feature allows you to open and view the selected Micro UI in a separate browser tab.

To open a Micro UI in a separate browser tab, perform the following steps:

1. On the Micro UI page, click the **More actions** icon  against the required Micro UI.
2. Select **Open**. The selected Micro UI opens in a separate browser tab.

Embedding code for Micro UI

This feature allows you to copy the embeddable URL and use the Micro UI in a separate browser tab. You can also copy the embeddable code and embed it with the other application to consume the Micro UI services.

To access the embed code, perform the following steps:

1. On the Micro UI page, click the **More actions** icon ... against the required Micro UI.
2. Select **Embed Code**. The Embed Code dialog appears.
3. Copy the Embeddable URL and Embeddable Code to use the published Micro UI as per your requirement.

Editing Micro UI

This feature allows you to modify a published Micro UI.

To modify a Micro UI, perform the following steps:

1. On the Micro UI page, click the **More actions** icon ... against the required Micro UI.
2. Select **Edit**. The Update Micro UI page appears. For further procedural details refer to the [Creating Micro UI](#) section.
3. Click **Update** to save the modifications. The message “Micro UI updated successfully” appears.

Deleting Micro UI

This feature allows you to delete a published Micro UI.

To delete a Micro UI, perform the following steps:

1. On the Micro UI tab, click the **More actions** icon ... against the required Micro UI.
2. Select **Delete**. The Delete Micro UI dialog appears.
3. Click **Delete** to confirm the deletion. The message “Micro UI deleted successfully” appears.

Using the Micro UI

The Micro UI capability allows you to perform various operations such as adding folders, uploading new files, viewing documents, playing audio and video files, and so on. The different types of Micro UIs available are as follows:

- [Advance folder view](#)
- [Document viewer](#)
- [Folder View](#)
- [Advance Search](#)

Advance folder view

The Advance folder view Micro UI allows you to add new folders and files to the Micro UI. The following options are available on the Advance folder view home page:

- **Folder view panel** — The folder view panel consists of the existing folders in the Folder List type of Micro UI. You can view the existing folders with their Folder Name, Owner, Last Modified On, and Actions.



Explore Sample Application is a system generated folder. You can only perform the View Properties action on this folder.

- **Layout** — This feature allows you to arrange the layout of the listed folders as List View or Grid View.

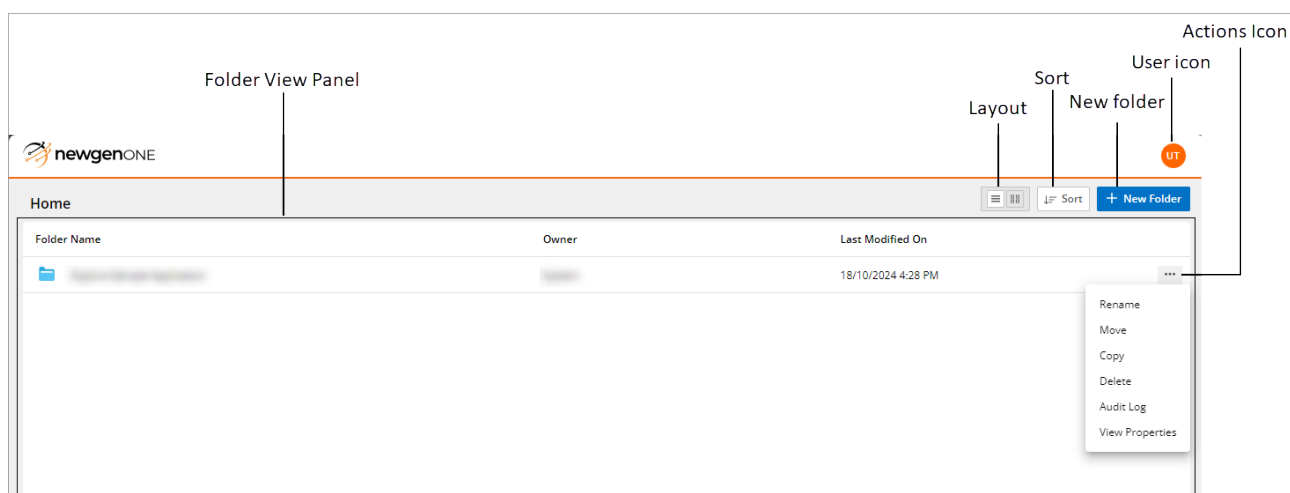


The Layout option appears only if the Layout is selected as List and Grid view while creating the Micro UI.

- **Sort** — This feature allows you to sort the listed folder in ascending or descending order with respect to the folder name or recent folder modification date.
- **New folder** — This feature allows you to add a new folder. The added folder appears in the folder view panel.
- **User icon** — The User icon contains the information about the signed-in user. Clicking on this icon allows you to view and perform various tasks such as view the user name, view the user's organization name, view subscription days left, reset password, and sign out from the Micro UI user module.
- **Actions icon** — This icon allows you to access various operations for folders and files such as rename, download, move, copy, delete, audit log, and view properties.



The actions that appear on clicking the Actions icon are defined while creating the Micro UI. By default, the View Properties action is enabled for all folders.



Document viewer

The Document Viewer Micro UI allows you to view the documents in the document viewer. The following options are available on the document viewer page:

- **Standard toolbar** — You can perform various operations using tools on the Standard toolbar such as selection, print, adjusting the page size, zoom, and so on.
- **User icon** — The User icon contains the information about the signed-in user. Clicking this icon allows you to view and perform various tasks such as view the user name, view the user's organization name, view subscription days left, reset password, and sign out from the Micro UI user module.
- **Show Comment** — This feature allows you to add, modify, and delete comments on a document. You can perform the following actions in the comment section:
 - **Add a comment** — This option allows you to add a comment to a document. The added comment appears in the comment section.
 - **Edit** — This option allows you to modify the added comment.
 - **Delete** — This option allows you to delete the added comment.



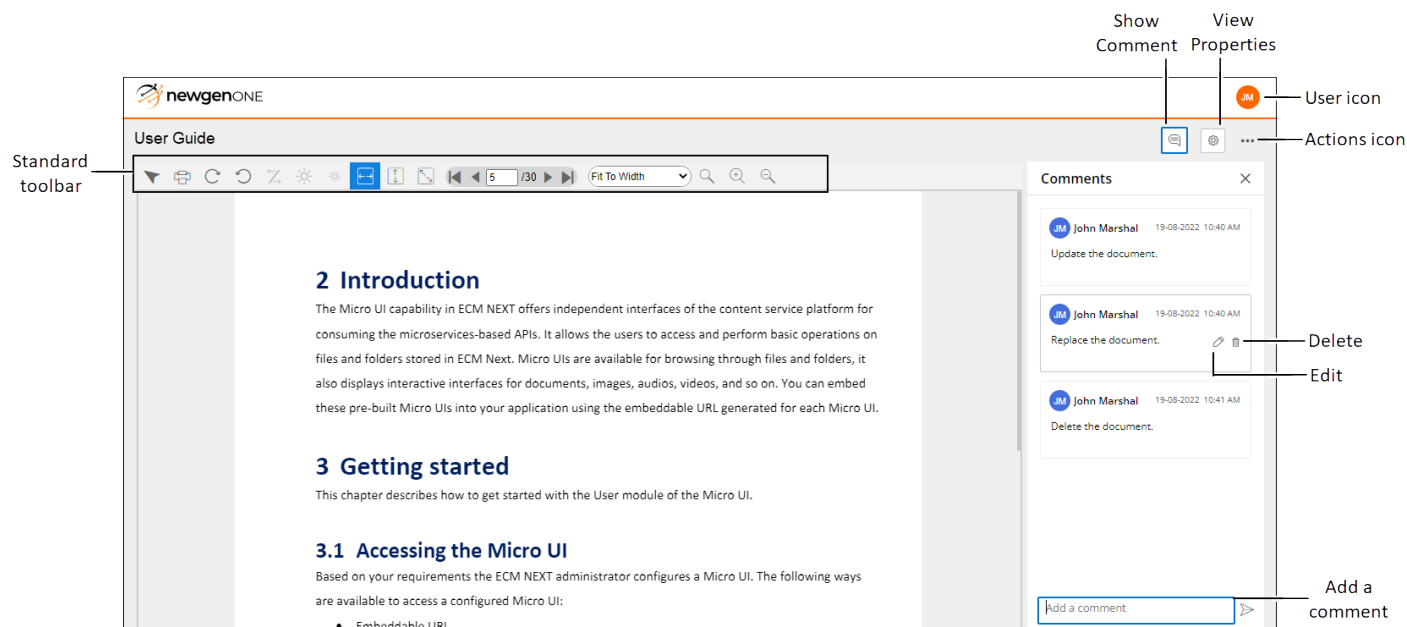
The Edit and Delete options on a comment are enabled only for those users who have added that comment.

- **Actions icon** — This icon allows you to access various operations for a document such as rename, download, move, copy, delete, audit log, and view properties.



The actions that appear on clicking the Actions icon are defined while creating the Micro UI. By default, the View Properties action is enabled for all documents.

- **View Properties** — This feature displays the details of a document.



Folder View

The folder view Micro UI allows you to only view the existing folders and files on the Micro UI. Creating new files and folders in the folder view is not allowed.

The following options are available on the folder list home page:

- **Folder view panel** — The folder view panel consists of the existing folders in the Folder List type of Micro UI. You can view the existing folders with their Folder Name, Owner, Last Modified On, and Actions.



Explore Sample Application is a system generated folder. You can only perform the View Properties action on this folder.

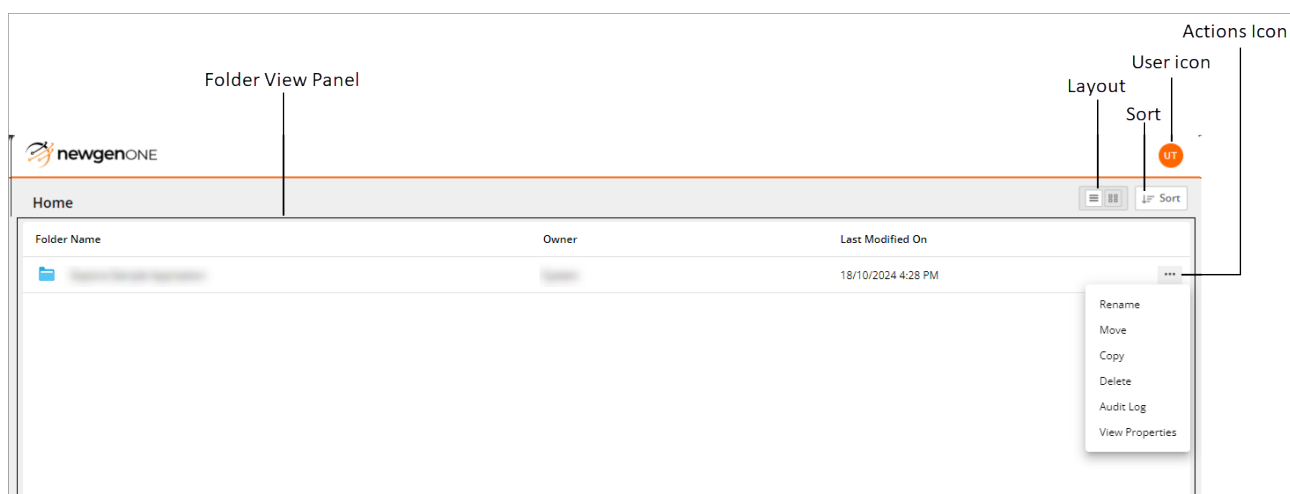
- **Layout** — This feature allows you to arrange the layout of the listed folders as List View or Grid View.



The Layout option appears only if the Layout is selected as List and Grid view while creating the Micro UI.

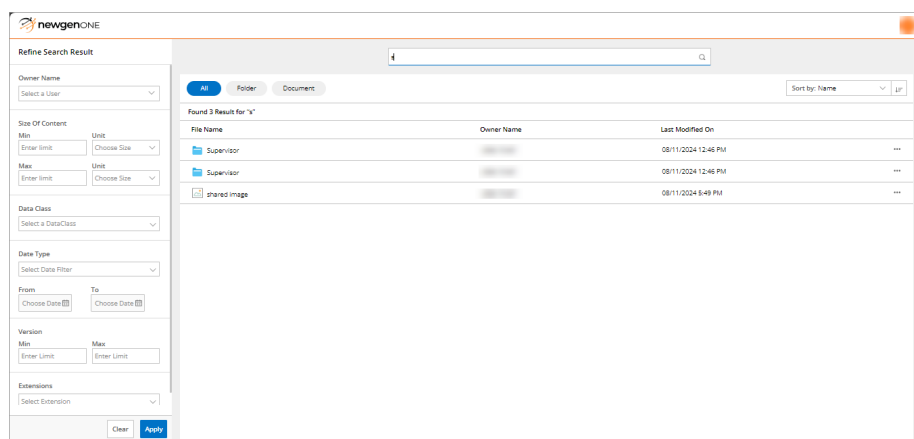
- **Sort** — This feature allows you to sort the listed folder in ascending or descending order with respect to the folder name or recent folder modification date.

- **User icon** — The User icon contains the information about the signed-in user. Clicking on this icon allows you to view and perform various tasks such as view the user name, view the user's organization name, view subscription days left, reset password, and sign out from the Micro UI user module.
- **Actions icon** — This icon allows you to access various operations for folders and files such as rename, download, move, copy, delete, audit log, and view properties.



Advance Search

The advanced search folder enables searching within document and folder content and displaying files and folders that contain the specified information as the search result. You can search any file or folder present by typing the name on the search bar and sort the data by name or its revised date time.



Refine Search Result

The refine search results tab lets you apply filters to narrow down the search and generate specific, relevant data. The tab consists of the following filters:

Filter	Description
Owner Name	Specify the owner's name to search for data created by that owner.
Size of Content	It allows you to search for files based on their size. Applying this filter requires setting the minimum and maximum size limits for the files along with the units.
Data Class	It allows filtering of files and folders based on their associated data class.
Date Type	It allows filtering of files and folders based on their creation or revision date. You specify a date range to search for folders created within those dates.
Version	It allows the filtering of files based on their versions. You specify a range to search for folders created within those versions.
Extensions	It allows filtering of files and folders based on the extensions.

To apply the filters, click **Apply**.

View Properties

To view the properties of a specific file or folder, perform the following steps:

1. Hover over to the specific file or folder and click **...**.
2. Click **View Properties**. The properties of the file or folder are displayed.


Roles Management

Roles Management allows you to create and manage the type of access a user has in an organization. For example, a user may have access across all folders and files, while another user may have only read permission, and other users may have both read and write permissions. It is to be used in conjunction with a security classification. You can associate the created role with an application or a user.

To access the Roles Management tab, click the **Roles Management** tab from the menu bar. The tab displaying all the created roles appears. This tab allows you to search for a specific role using the search box.

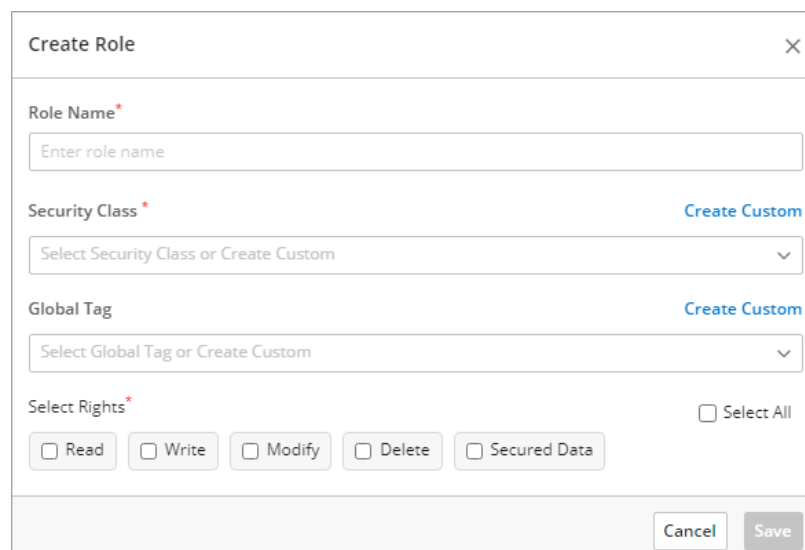
Creating a role

The Roles Management tab allows you to create roles that you can associate with the available users to perform the desired tasks.

 Only the user who is part of the Admin role can create, edit, and delete a role.

To create a role, perform the following steps:

1. On the Roles Management tab, click **+ Create Role**. The Create Role dialog appears.




The 'Create Role' dialog box is shown with the following fields and options:

- Role Name ***: A text input field with the placeholder 'Enter role name'.
- Security Class ***: A dropdown menu with the placeholder 'Select Security Class or Create Custom'. A **Create Custom** link is visible to the right.
- Global Tag**: A dropdown menu with the placeholder 'Select Global Tag or Create Custom'. A **Create Custom** link is visible to the right.
- Select Rights ***: A section containing five checkboxes: **Read**, **Write**, **Modify**, **Delete**, and **Secured Data**. A **Select All** checkbox is located to the right of these options.
- At the bottom right, there are **Cancel** and **Save** buttons.

2. Specify the following fields:

Field	Action
Role Name	<p>Enter a required role name. It must follow the below criteria:</p> <ul style="list-style-type: none"> • It contains a maximum of 1-50 characters limit. • Digits or special characters are not allowed. • Spaces are allowed.
Security Class	<p>Security classification allows the admin user to impose restrictions on other users for accessing certain documents. To apply an appropriate level of security for different roles, the NewgenONE Content Cloud provides the following level of security hierarchy:</p> <ul style="list-style-type: none"> • Secret • Top Secret • Confidential • Non-confidential <p>You can also create a custom class using the Create Custom link displayed above the dropdown box. For more information, refer to the Creating a class section.</p>
Global Tag	<p>Select a global tag from the Global Tag dropdown list. You can also create a custom tag using the Create Custom link displayed above the dropdown box. For more information, refer to the Creating a tag section.</p>


Field	Action
Select Rights	<p>Select the rights to assign with the role. The following rights are available:</p> <ul style="list-style-type: none"> • Read — It allows you to perform the following operations: <ul style="list-style-type: none"> ◦ Download file ◦ View files and folders ◦ Listing of files and folders • Write — It allows you to perform the following operations: <ul style="list-style-type: none"> ◦ Upload file ◦ Add folder ◦ Create versions • Modify — It allows you to perform the following operations: <ul style="list-style-type: none"> ◦ Rename files and folders ◦ Add and update the security class of files and folders ◦ Add and update global tag on files and folders ◦ Update file and folder • Delete — It allows you to perform the following operations: <ul style="list-style-type: none"> ◦ Delete file ◦ Delete folder • Secure Data — It allows you to secure the selected data class fields. Based on the rights (Read, Write, Modify, and Delete) assigned to the end-users, they can perform a suitable operation on the secured field. Otherwise, the data in the secure field appears as masked. <p>Click the Select All checkbox to select all rights.</p> <p> To ensure files and folders appear in the repository list, a minimum Read right must be added. In case Read right is not applied, files and folders do not visible in the list at the user's end.</p>



Fields marked with * are mandatory to fill.

3. Click **Save** to add the configured role. The added role appears on the Roles Management tab.



You can Edit and Delete the added role using the **More actions** icon  against the required role. Only the Edit right is available for the system-generated role.

Creating a class

Security class is a tag that can be applied to a document or folder based on which the security clearance of a document can be managed.

 Only the user who is part of the Admin role can create, edit and delete a class.


To create a class, perform the following steps:

1. On the Roles Management home page, click **Class Library**. The Class Library page appears. All created classes appear on this page.
2. Click **+ Create Class** to create a new class. The Security Class dialog appears.
3. Specify the following details:
 - **Security Class Name** — This mandatory field allows you to enter the required class name. It must follow the below criteria:
 - It contains a maximum of 1-50 characters limit.
 - Digits or special characters are not allowed.
 - Spaces are allowed.
 - **Description** — This optional field allows you to enter additional information related to the security class. It contains a maximum of 128 characters.
4. Click **Save** to add the configured class. The added class appears on the Class Library home page.

Deleting a class


This feature allows you to delete an added class.

To delete a class, perform the following steps:

1. On the Class Library page, click the **More actions** icon  against the required class.
2. Select the **Delete** option. The Delete Security Class dialog appears.
3. Click **Delete**. The message “Security Class deleted successfully” appears.


Creating a tag

Roles Management allows you to create tags that can be applied to a document or folder based on which the security clearance of a document can be managed.

 Only the user who is part of the Admin role can create, edit, and delete a tag.

To create a tag, perform the following steps:

1. On the Roles Management tab, click **Tag Library**. The Tag Library page appears. All created tags appear on this page.
2. Click **+ Create Tag** to create a new tag. The Global Tag dialog appears.
3. Specify the following details:
 - **Global Tag Name** — This mandatory field allows you to enter the required tag name. It must follow the below criteria:
 - It contains a maximum of 1-50 characters limit.
 - Digits or special characters are not allowed.
 - Spaces are allowed.
 - **Description** — This optional field allows you to enter additional information related to the global tag. It contains a maximum of 128 characters.
4. Click **Save** to add the configured tag. The added tag appears on the Tag Library page.

 You can Edit and Delete the added Tags using the **More actions** icon  against the required Tag.

User Management

User Management allows you to register and manage user operations. It deals with operations like user registration, editing, deactivation of the registered user, and so on.

To access the User Management tab, click the **User Management** tab from the menu bar. The page displaying all the registered users with their name, email, role, and status appears. You can search for a specific user using the search box that appears on the page.

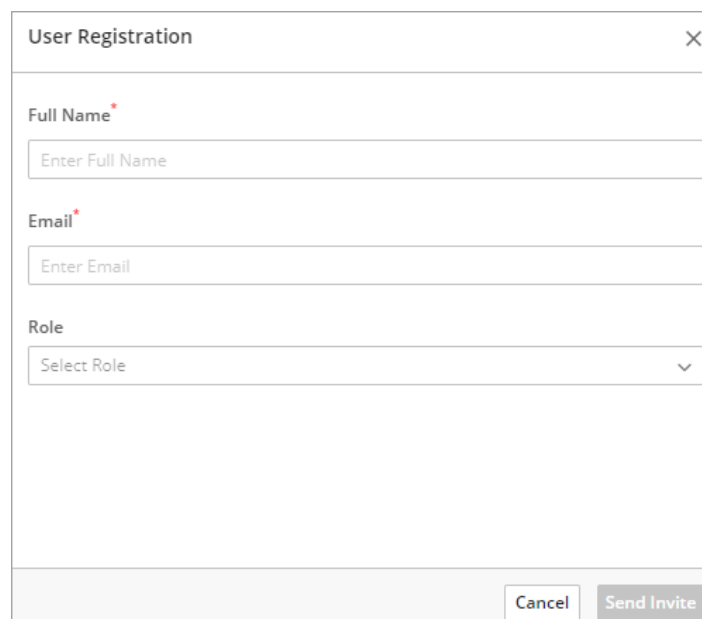
Registering a new user

The User Management tab allows you to register and manage users inside a tenant account. You can also edit and deactivate the registered users.

 Only the user who is part of the Admin role can register and deactivate a user.

To register a new user, perform the following steps:

1. On the Roles Management tab, click **+ User Registration**. The User Registration dialog appears.



The image shows a 'User Registration' dialog box with a close button (X) in the top right corner. It contains three input fields: 'Full Name' with a red asterisk, 'Email' with a red asterisk, and 'Role' which is a dropdown menu. Below these fields are two buttons: 'Cancel' and 'Send Invite'.

User Registration	
Full Name *	<input type="text" value="Enter Full Name"/>
Email *	<input type="text" value="Enter Email"/>
Role	<input type="text" value="Select Role"/>
<div>Cancel Send Invite</div>	

2. Specify the following fields:

- **Full Name** — Enter the full name of the required user.
- **Email Address** — Enter the email address of the defined user.
- **Role** — Select a role from the dropdown list.



Fields marked with * are mandatory to fill.

3. Click **Send Invite** to send an invitation link to the defined user's email address from where the user can join. To join the invitation, the user must follow the below steps:

- Go to the email address where the invitation is sent.
- Open the invitation mail.
- Click **SETUP YOUR ACCOUNT NOW**. It redirects to the Create Password page.
- Enter a required password. The password must contain:
 - At least 1 capital letter.
 - At least 1 numeric.
 - At least 1 punctuation.
 - At least 8-16 characters.
 - No space allowed.
- Click **Create Password**. The message "The password has been created" appears.

Operations on created users

The following operations are available to perform on the created user:

- [Editing](#)
- [Deactivating](#)

Editing


To edit the user information, perform the following steps:

- On the User Management tab, click the **More actions** icon  against the required user.

2. Select the **Edit** option. The Update User dialog appears. You are only allowed to update the roles associated with the selected user.
3. Modify the Role as required.
4. Click **Update** to save the modification.

Deactivating

To deactivate a user, perform the following steps:

1. On the User Management tab, click the **More actions** icon  against the required user.
2. Select the **Deactivate** option. The Deactivate User dialog appears.



Once you deactivated a particular user ID, then you cannot join the same user ID again.

3. Click **Deactivate**. The user gets deactivated.

Application Registration

Application Registration allows you to leverage the OAuth 2.0 authentication and authorization mechanism of NewgenONE Content Cloud for the integration purpose of any custom application. It helps to integrate an application scope rather than a user scope. This is useful for integrations where users and corresponding rights may be managed by invoking the application.

To access the Application Registration tab, click the **Application Registration** tab from the menu bar. The page displaying all the registered applications appears. You can search for a specific application using the search box that appears on the page.

Registering an application

The Application Registration tab allows you to register an application.

 Only Admin user can register, edit, and delete an application.

To register an application, perform the following steps:

1. On the Application Registration tab, click **+ Register Application**. If there is no application registered earlier, then you can also register an application using the **+ New App Registration** displayed on the right pane. The Register Application page appears. This page comprises four tabs to register an application:
 - Configure Platform
 - Client Credentials
 - Security Settings
 - Summary

By default, the **Configure Platform** tab appears to configure the application.

2. Specify the following fields:
 - **Application Name** — Enter the application name. It must follow the below criteria:
 - It contains a maximum of 1-50 characters
 - Leading or trailing spaces are not allowed.

- Special characters are not allowed “-” and “_”.
- Numbers are allowed.

• **Please Select platform** — Select the required platform where you want to host the registered application. The following options are available:

- **Web** — Select this option to configure for browser client applications and then follow the below step:
 - Specify the **Redirect URI** where the registered application redirects. The following are the validation criteria of Redirect URI:
 - It must be unique.
 - It must be unique.
 - The character length must be less than 256.
 - It does not contain wildcard characters.
 - It must start with HTTPS or http://localhost.
 - It must be a valid URL.
 - Only 5 redirect URIs can be added.
 - Click **Add URI** to add the specified URI.


 Redirect URI associated with a Micro UI cannot be edited or deleted.

- **Server** — Select this option to configure for web or application server-based applications.

3. Click **Next**. The Client Credentials tab appears. This tab allows you to generate a Client Secret to access the registered application.

 Secret associated with a Micro UI cannot be deleted.

4. Click **+ Generate Client Secret**. The Client Secret dialog appears. The generated secret code appears in the **Your Generated Secret Code** field.

 If you edit the Expiry Period of a saved Client Secret, then the Secret Code updates automatically. Due to this change, the URL of the associated Micro UI or the OAuth 2.0 client is impacted. It is recommended that you must update the latest Micro UI URL or OAuth 2.0 client wherever it is needed.

5. Select an expiry date from the **Select Expiry Period** dropdown list. Or, click the **Create Custom** link to set a required expiry date that is not available in the dropdown list.

- If you have selected the Server option to host your application as described in Step 2, then an additional field **Select Role** appears.
- Select an appropriate option from the **Select Role** dropdown list.

6. Click **Save** to finalize the expiry period for the generated Secret Code. The added Client Secret code appears in the Client Credentials tab.



You can Preview, Edit, and Delete the generated Client Secret code using the **More actions** icon **...** against it.

7. Click **Next**. The Security Settings tab appears.
8. Specify the following information:
 - If you have selected the Web option to host your application as described in Step 2, then specify the **Whitelisted Domain** to access the registered application and click **Add** to save the specified whitelisted domain. The following are the validation criteria of Whitelisted Domain URI:
 - It must be unique.
 - The character length must be less than 256.
 - It does not contain wildcard characters.
 - It must start with HTTPS or http://localhost.
 - It must be a valid URL.



Whitelisted domains associated with a Micro UI cannot be edited or deleted.

- If you have selected the Server option to host your application as described in step 2, then follow the below steps:
 - From the right pane, add a required whitelisted IP address. It must follow the below criteria:



You can Edit and Delete the added IP address using the **More actions** icon **...** against the required IP address.

- It contains a maximum of 7-15 characters limit.
- IP addresses with wildcards are allowed.

Example:

192.12.12.1, 192.12.11.*, 192.12.*, and so on are valid.

192.*, 192.12.12*, and so on are not valid.

- Click **Browse File** that appears on the left pane to upload a certificate from your system. The following certificate file types are supported:
 - crt
 - .cer



Once the domain is added, you can Edit and Delete the added domain using the **More actions** icon **...** against it.

9. Click **Finish**. The Summary tab appears. This tab displays the details of the registered application.

Data Class Management

The Data Class is a set of indexes that can be associated with any document or folder by providing a unique entity to them. These indexes store the values provided so that the user can perform a search on them.

To access the Data Class Management tab, click the **Data Class Management** tab from the menu bar. The page displaying all the existing data classes appears. You can search for a specific data class using the search box that appears on the page.

The following actions are available to perform on a data class:

- [Creating a Data Class](#)
- [Modifying a Data Class](#)
- [Deleting a Data Class](#)

Creating a Data Class


To create a data class, perform the following steps:

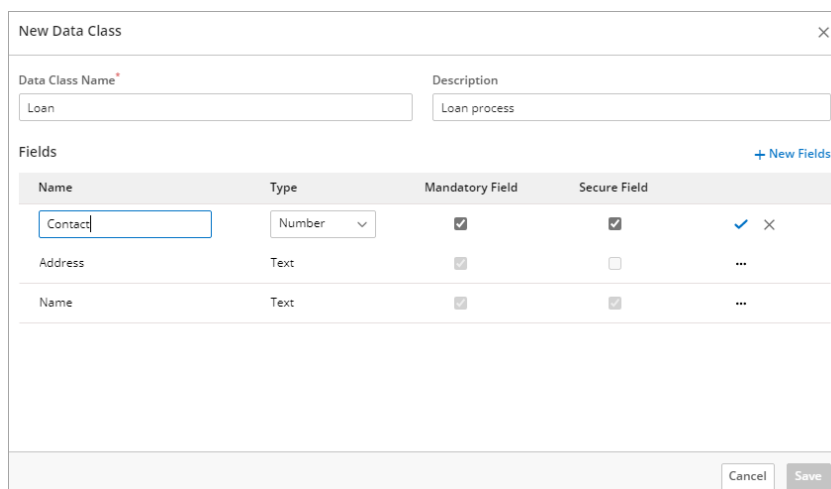
1. Click **Data Class Management** from the menu bar.
2. Click **+ New Data Class**. The New Data Class dialog appears.
3. Specify the following fields:
 - **Data Class Name** — It is a mandatory field that specifies the name of the required data class. The name of the data class field must follow the below criteria:
 - The maximum number of characters limit is 50.
 - Only alphanumeric values with special characters hyphen (-) and underscore (_) are allowed and numeric value at the start of the text is not allowed.
 - **Description** — It is an optional field to provide a brief description of the specified data class. The maximum character limit for this field is 128 characters.



To create a Data Class, you must add a minimum of one field within a data class.

4. Click **New Fields** to add the required fields with the entered data class. The section to add new fields appears.
5. Specify the following fields:

Field	Description
Name	It specifies the associated field name within the data class. This field allows only alphanumeric values with special characters such as hyphen (-) and underscore (_). The numeric values at the start of the text are not allowed.
Type	It specifies the type of content allowed for entered data class field. The following types are available to select: <ul style="list-style-type: none"> • Text • Date • Integer Number • Decimal Number
Mandatory Field	It allows you to set or modify the mandatory field for data class until it gets associated with any folder or document.
Secure Field	It allows you to secure the selected data class fields. Based on the rights (Read, Write, Modify, and Delete) assigned to the end-users, they can perform a suitable operation on the secured field. <div>  Once a data class field is saved as secured, it does not allow you to clear the Secure Field checkbox while modifying a field. </div>




New Data Class

Data Class Name: Description:

Fields [+ New Fields](#)

Name	Type	Mandatory Field	Secure Field	
Contact	Number	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/>
Address	Text	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> <input checked="" type="checkbox"/>
Name	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>

6. Click the check icon  to add the entered data class field. To add more fields within the data class, repeat the above steps.

7. Click **Save** to finalize the added data class fields. The added data class appears on the Data Class Management tab's home page.

Modifying a Data Class

To modify a data class, perform the following steps:

1. In the Data Class Management tab, click the **More actions** icon **...** against a required data class and select **Edit** to modify its properties.
The Edit Data Class dialog appears. Here, you can perform the following actions:
 - Add new data class fields – Refer [Creating a Data Class](#) section for procedural details.
 - Delete the existing data class fields – To delete an existing data class field, perform the following steps:
 - a. click the **More actions** **...** icon against the specific field and select **Delete**. The Delete Data Class Field appears.
 - b. Click **Delete** to confirm the deletion of the selected field.
 - d. Click **Save** to finalize all the modifications.

Deleting a Data Class

To delete a data class, perform the following steps:

1. In the Data Class Management tab, click the **More actions** icon **...** against a required data class to delete it.



You can delete only those data classes that are not associated with any folder, document, or media files at the user's end.

2. Select the **Delete** option. The Delete Data Class dialog appears.
3. Click **Delete** to permanently delete the data class.

Audit Log

Audit Log allows you to keep track of API consumption and actions performed using the NewgenONE Content Cloud Admin module.

For example, the accounts payable department of an organization can leverage the Audit Log feature to monitor API usage and track actions performed within an application, ensuring compliance and streamlining audit processes. This ensures transparency and accountability in managing financial documents and transactions.

To access the Audit Log tab, click the **Audit Log** tab from the menu bar.


The screenshot shows the NewgenONE Content Cloud Admin interface. The sidebar on the left contains navigation options: Metering Dashboard, Micro UI, Roles Management, User Management, Application Registration, Data Class Management, and Audit Log. The main area displays the Audit Log tab. At the top, there are 'Filters' and 'Refresh' buttons. Below the filters, there are tabs for 'API Log' and 'Operational Log'. The 'API Log' tab is selected, showing a table of API calls. The table has columns: Date & Time, API Name, Status, Request URL, Method, Application Name, and User Name. The table shows 12 entries, with the first 11 visible. The first entry is a POST request for Grant Token at 05/06/2024 2:54 PM. The last entry is a GET request for Validate Token at 05/06/2024 9:52 AM. The interface also includes a 'Showing 1 - 11 of 12' indicator and a 'Download' button.

Date & Time ↑	API Name	Status	Request URL	Method	Application Name	User Name
05/06/2024 2:54 PM	Grant Token	Success	http://ncc.newgendocker.com:443/ecmapi/appservice/a...	POST	DefaultApp	None
05/06/2024 2:54 PM	Grant Code	Success	http://ncc.newgendocker.com:443/ecmapi/appservice/a...	POST	DefaultApp	None
05/06/2024 11:15 AM	Search Users	Success	http://ncc.newgendocker.com:443/ecmapi/userregisters...	GET	DefaultApp	Ryan
05/06/2024 11:15 AM	Fetch All User Roles	Success	http://ncc.newgendocker.com:443/ecmapi/roleservice/...	GET	DefaultApp	Ryan
05/06/2024 11:15 AM	Fetch All Applications	Success	http://ncc.newgendocker.com:443/ecmapi/appservice/a...	GET	DefaultApp	Ryan
05/06/2024 11:15 AM	Fetch All User Roles	Success	http://ncc.newgendocker.com:443/ecmapi/roleservice/...	GET	DefaultApp	Ryan
05/06/2024 9:52 AM	Search Users	Success	http://ncc.newgendocker.com:443/ecmapi/userregisters...	GET	DefaultApp	Ryan
05/06/2024 9:52 AM	Fetch a Content	Success	http://ncc.newgendocker.com:443/ecmapi/contentservi...	GET	DefaultApp	Ryan
05/06/2024 9:52 AM	Validate Token	Success	http://ncc.newgendocker.com:443/ecmapi/appservice/a...	GET	DefaultApp	Ryan
05/06/2024 9:52 AM	Validate Token	Success	http://ncc.newgendocker.com:443/ecmapi/appservice/a...	GET	DefaultApp	None

The Audit Log tab contains the following sub-tabs:

- **API Log** — This is a default tab that opens while selecting the Audit Log tab from the menu bar. This tab displays the following details:

Option	Description
Date & Time	Displays the list of the date and time when the specific APIs were called.

Option	Description
API Name	Displays all the API names that are consumed.
Status	Displays the success or failure status of all the consumed APIs.
Request URL	Displays the list of request URLs for all consumed APIs that includes the request parameters of each APIs. You can copy the request URL by hovering over a specific URL and then clicking the copy icon  against the URL.
Method	Displays the list of API methods depending on the request type. The following are the API methods: <ul style="list-style-type: none"> • GET — To request data from a specified resource. • PUT — To send data to a server to create a resource. • POST — To send data to a server to update a resource. • DELETE — To delete the specified resource.
Application Name	Displays the list of application names associated with the specific APIs.
User Name	Displays the list of users who have consumed the specific APIs.

- **Operational Log** — Selecting this tab displays the following details:

Option	Description
Date & Time	Displays the date and time of the action performed.
User Name	Displays the username of the admin user who has performed or approved any action.
Action Performed	Displays the action or activity performed by an admin user.
Description	Displays a brief description of the action performed.

Following are the additional options available on the Audit Log tab:

- **Filters** — This option allows you to filter the audit log for the specified period. For more details, see [Filtering audit logs](#).
- **Download** — Selecting this option downloads audit logs to your local machine. The audit logs are downloaded in the CSV format.
- **Refresh** — Selecting this option refreshes the list of generated audit log.

Filtering audit logs

You can filter the API Log or Operational Log for a specified period, such as the last 24 hours, the last 48 hours, or any specific date range. Additionally, you can filter the required audit log results based on API details such as status, method, API name, user name, and application name. The filter results appear in batches of 20 logs at a time.

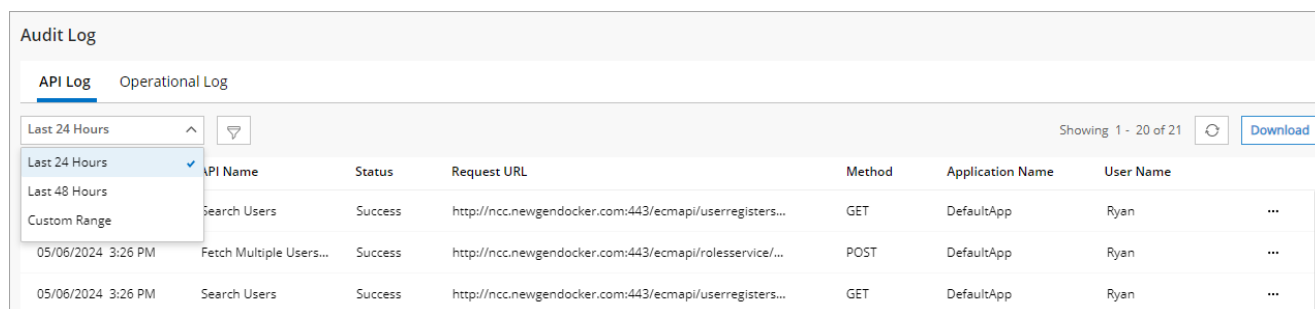
You can filter the audit logs on the following bases:

- Based on time period
- Based API details


Filtering audit logs based on time period

To filter audit logs based on time period, perform the following steps:

1. From the API Log or Operational Log tab, click the time range filter dropdown.



2. Select one of the following options:

- **Last 24 Hours** — Selecting this option displays the audit logs of the last 24 hours.
- **Last 48 Hours** — Selecting this option displays the audit logs of the last 48 hours.
- **Custom Range** — Selecting this option allows you to filter audit logs for a specific date range as follows:
 - a. From the time range filter dropdown options, select the **Custom Range** option.
 - b. In the **From** and **To** fields, select the calendar icon  and specify a required date range.
 - c. Click **Save**. The audit logs for the selected date range appear.

Filtering audit logs based on API details

To filter audit logs based on API details, perform the following steps:

1. From the API Log or Operational Log tab, click the filter icon .

Filters

Clear

Status

All

Method

All

API Name

All

User Name

All

Application Name

All

Cancel

Apply

API Log Filter

Filters

Clear

Action Performed

All

User Name

All

Cancel

Apply

Operational Log Filter

2. Specify the following details:

- In case of applying filter query for API Log:

Field	Description
Status	<p>Allows you to set a filter query by selecting one of the following API status codes:</p> <ul style="list-style-type: none"> • 200 — OK: The request was successful. • 201 — Created: The request was successful and a new resource was created. • 400 — Bad Request: The server does not understand the request due to invalid syntax. • 500 — Internal Server Error: The server encountered an unexpected condition that prevented it from fulfilling the request. • 404 — Not Found: The requested resource is not available on the server.
Method	<p>Allows you to set a filter query by selecting one of the following API methods:</p> <ul style="list-style-type: none"> • GET — To request data from a specified resource. • POST — To send data to a server to update a resource. • DELETE — To delete the specified resource. • PUT — To send data to a server to create a resource.

Field	Description
API Name	Allows you to set a filter query by selecting the specific API.
User Name	Allows you to set a filter query by selecting the specific username.
Application Name	Allows you to set a filter query by selecting the specific application name.

- In case of applying filter query for Operational Log:

Field	Description
Action Performed	Allows you to set a filter query by selecting the specific action performed.
User Name	Allows you to set a filter query by selecting the specific username.

You can reset or clear the selected fields of the Filter dialog by clicking the **Clear** button.

3. Click **Apply**. The filter results appear.

You can review and then download the filter result in the CSV format by clicking the **Download** button.

Viewing API Log details

API Log allows you to view the detailed summary, request body, and response body of the specific API call. The admin user can utilize these details to debug and monitor API interactions.

To view API log details, from the API Log tab, click the **More actions** icon ... against the required API and select **View Details**. The Detailed Info screen appears displaying the following information:

Tab	Description
Summary	<p>Displays a detailed summary of the selected API. It contains the following information:</p> <ul style="list-style-type: none"> • Date & Time • API Name • Method • Status • Application Name • Application ID • User IP Address • User Name • User ID • Request URL • Response Time
Request	<p>Displays the request body of the selected API.</p> <p>You can copy the request body by clicking the Copy button.</p>
Response	<p>Displays the response body of the selected API.</p> <p>You can copy the response body by clicking the Copy button.</p>