NewgenONE OmniDocs

Administration Guide

Version: 12.0

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.

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

This administration guide describes how to manage various objects of OmniDocs such as Folders, Keywords, Users, Groups, Roles, Global Indexes, Data Classes, and Sites used in a Document Management System (DMS) and Image Volumes. It also describes how to configure OmniProcess, Search, Web API, and design the Dashboard.

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.

Revision history

Revision date	Description
October 2024	Initial publication

Intended audience

This administration guide is intended for the IT system administrator responsible for performing administrative operations such as creating users, groups, roles, folders, metadata, configuring search, workflows, repository view, and more. The reader must have a conceptual idea of running basic administrative operations. The reader must have administrative rights to access and configure different components for the end users.

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

OmniDocs is an **Enterprise Document Management** platform for creating, capturing, managing, delivering, and archiving large volumes of documents. It offers a highly scalable, unified repository for securely storing and managing documents in an enterprise. It also provides access to enterprise documents directly and through integration with business applications.

OmniDocs offers a centralized repository for enterprise documents and supports rights-based archival. It manages the complete lifecycle of documents through record retention, storage, and retrieval policies. It also supports exhaustive document and folder searches based on date, indexes, and general parameters as well as Full Text Search (FTS) on image and electronic documents.

The very basic operation of the system is to access documents from a remote site and working on them, without archival and retrieval hassles. In an enterprise-wide scenario, the **Document Management System (DMS)** can be centralized with the robust and efficient OmniDocs. Further, this DMS can also be accessed from any part of the world through OmniDocs Web.

Getting started

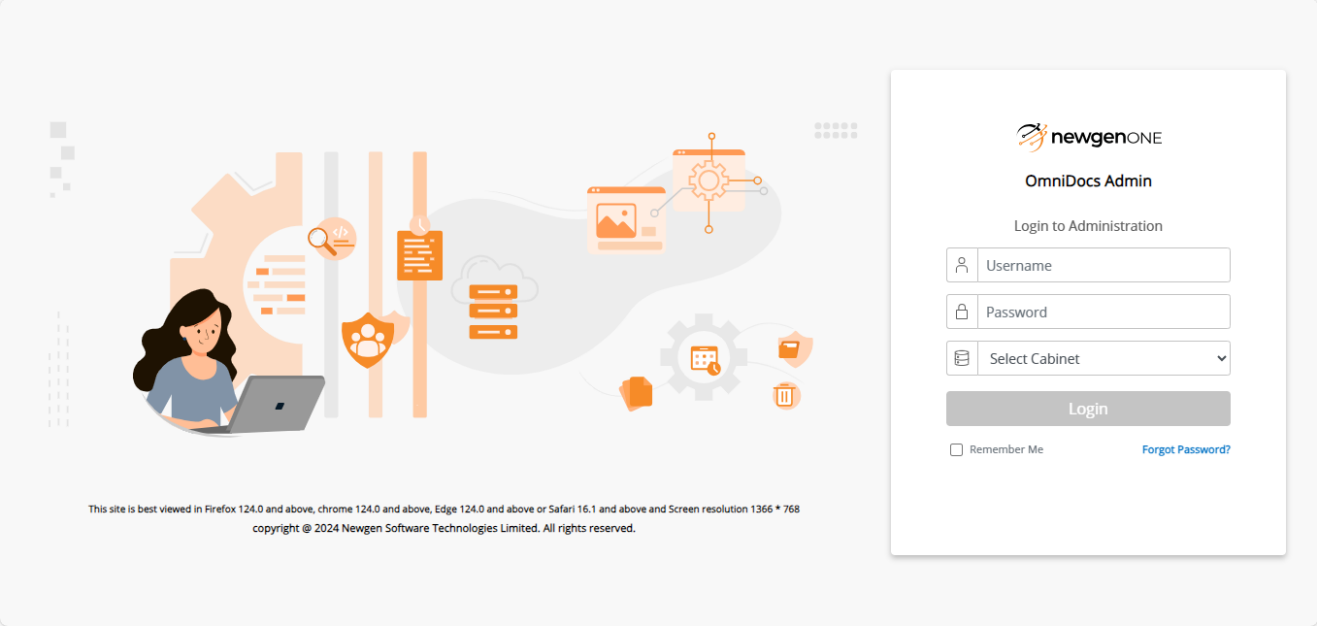
This chapter describes how to get started with Admin module.

Accessing OmniDocs Admin

This section describes how to access the Admin module.

To access the Admin, perform the below steps:

1. Launch a web browser.
2. In the browser address bar, enter the NewgenONE OmniDocs Admin URL in the following format: https://<Address of Application Server>: <Port Number>/ omnidocs/admin
3. Press **Enter**. The NewgenONE OmniDocs Login to Administration page appears.



4. Enter the following details:

Field	Description
Username	Enter the registered username.
Password	Enter the password associated with the username.
Select Cabinet	Select the Cabinet using the dropdown. This field appears if there two or more registered cabinets.
Captcha	Enter the captcha. • The captcha information does not appear if it is disabled by the administrator. • In case the captcha is unclear, click the **Refresh** icon to get a new captcha. • To listen the captcha, click the **Speaker** icon.
Remember Me	Select the checkbox to preserve your sign-in details.
Forgot Password	Use this option in case you forgot your password. For procedural details, refer to the Resetting password section.

5. Click **Login** to start the session. The NewgenONE OmniDocs Admin home page appears. It consists of the following tiles:

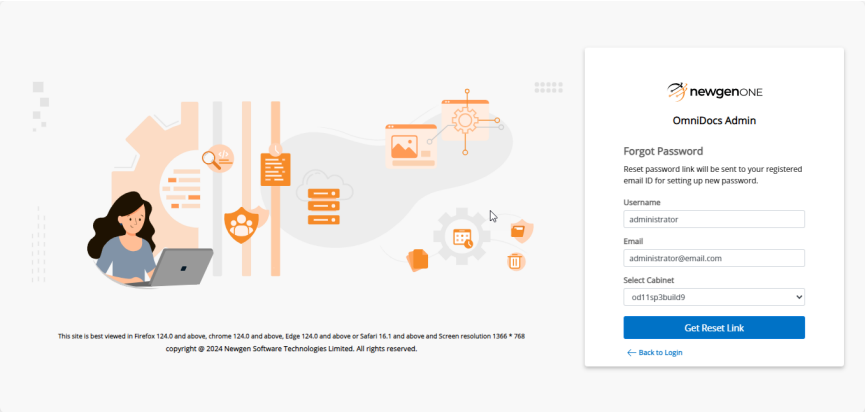
When signing for the first time, sign in as the supervisor and ensure you have all the rights and privileges similar to a supervisor.

- Administration
- Configure
- Personalize
- Management

Resetting a password

To reset your forgotten password, perform the below steps:

1. On the sign-in page of Newgen OmniDocs, click **Forgot Password?**. The Forgot Password dialog appears.

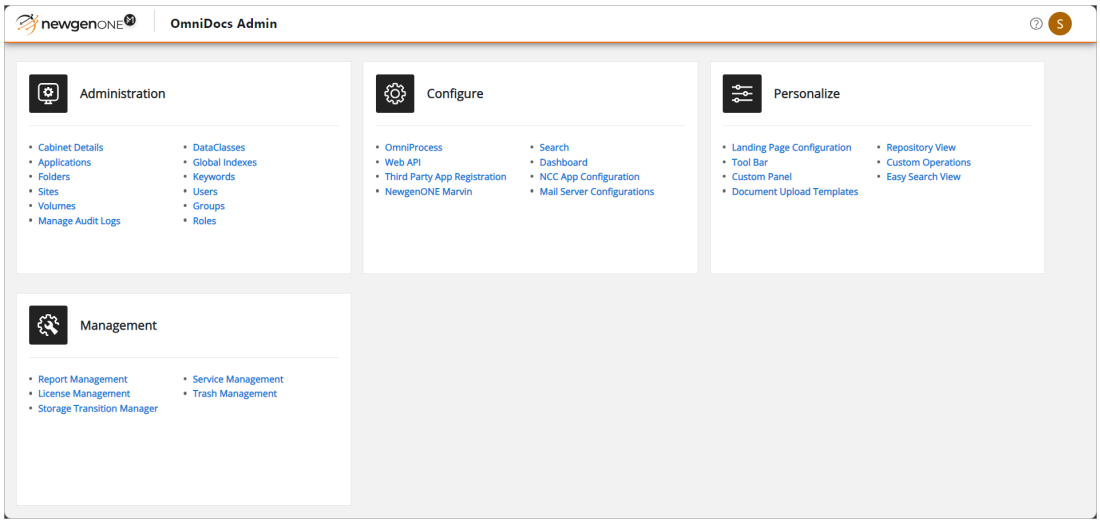


2. Specify the following details for the following fields:
   - Username — Enter your user name.
   - Email — Enter your registered email address.
   - Select Cabinet — Select the cabinet.

   This field appears if you have registered two or more cabinets.
3. Click **Reset Link**. A rest link and a set of instructions for resetting the password are shared on your registered email address.
4. Open the reset link. The Reset Password page appears.
5. Enter the new password and re-enter the password to confirm.
6. Click **Reset Password**. The password gets updated.

Exploring OmniDocs Admin interface

When you successfully sign in, the NewgenONE OmniDocs Admin home page appears. It consists of tiles with administrative tools that you can access directly.



The NewgenONE Marvin logo appears only if its engine settings are configured in the Admin Workspace. For more information, see Configuring NewgenONE Marvin settings.

The following tiles appear that contain direct access to their tabs:

- Administration
- Configure
- Personalize
- Management

Administration

Administration is a server-side tool that enables the supervisor to manage various objects of OmniDocs such as:

- Folders
- Keyword
- Users
- Cabinet Details
- Groups
- Applications
- Roles
- Dashboard Designer
- Global Indexes
- DataClasses
- Sites Used in DMS
- Image Volume

System Administration enables the following functions:

- Enables the Supervisor to create and work with the above-specified objects.
- Assign rights and privileges to various users and groups to access and retrieve documents from the Cabinet.
- Ensure security of information.

Using the administrative function, the Supervisor can:

- **Create Document Repository** such as folders and sub-folders for information management and hierarchical storage of documents.
- **Create Users and Groups and Assign Rights, Privileges and Roles** to work with folders and documents.
- **Create DataClasses** with multiple user-defined indexes for various data types.
- **Global Indexes and Keywords** to file and index documents for quick retrieval.
- **Perform Entire Document Lifecycle Management** by creating storage units such as Image Volumes and Sites to store and manage documents and images.

Cabinet Details

The Cabinet is a basic entity in the OmniDocs Document Management System. The OmniDocs engine has three types of Cabinets viz. Document Cabinet, Image Cabinet, and Document and Image Cabinet.

Document Cabinet refers to the database, which maintains the Document Management System information. All users, folders, and document information reside in this cabinet.

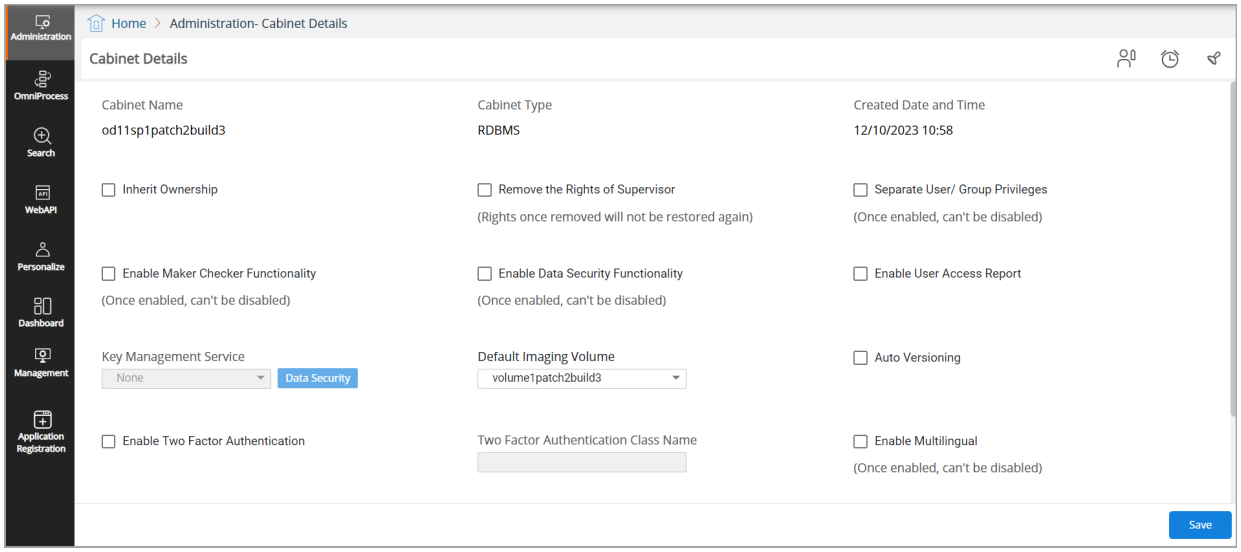
Image Server Cabinet refers to the database where volume and document storage information is stored.

The OmniDocs administrator can carry out the following activities:

- Modify the properties of a Cabinet.
- Modify the default volume for a Cabinet.
- Define rights at the object level and that can be used to assign rights to different objects.

To Access and View the Cabinet Properties:

1. In the home screen of OmniDocs Admin, go to **Administration** tile.
2. Click on the **Cabinet Details** link. The Cabinet Details screen appears. The top row displays the following information about the logged-in cabinet:
   - Cabinet Name: The name of the logged-in cabinet.
   - Cabinet Type: The database type.
   - Created Date and Time: The cabinet creation date and time.



3. The OmniDocs Admin can enable/disable the following functionalities from the Cabinet Details screen:
   - Inherit Ownership: Once this option is enabled from the Cabinet Details page, the ownership of the folder will be inherited to its sub-folders and documents even if the sub-folders and documents are created by some other users.
   - Remove the Rights of Supervisor: When applied, it removes the rights of the supervisor2, and converts it into a normal user. When this option is enabled, the rights and privileges of Supervisor2 can be changed as this user can be disassociated from the supervisor group.
   - **Separate User/Group Privileges**: If this option is enabled, then the option to provide privileges to the users and groups/roles gets separated. For example, when this option is disabled, then the privilege of creating user/group/role can be provided through a single operation. In case it is enabled, then the operation of creating the user and group/role gets separated.
   - Enable Maker Checker Functionality: To enable it, mark the Maker Checker Functionality checkbox. It must be noted that once this feature is enabled, it cannot be disabled. In Maker and Checker feature, for each transaction, there must be at least two individuals necessary for its completion. While one individual may Create a transaction, the other individual should be involved in Confirmation or Authorization of the same.
   - Enable Data Security Functionality
   - **Enable User Access Report**: To enable/disable it, mark/unmark the Enable User Access Report checkbox.
   - **Default Imaging Volume**: It is used to set the Default Imaging Volume. Click on the dropdown button and select the required default Imaging Volume.
   - **Auto Versioning**: This feature is provided for automatically creating the versions whenever any annotation is applied to the document. Mark/unmark the checkbox to enable/disable it.
   - Enable Two Factor Authentication
   - **Enable Multilingual**: Mark/unmark the checkbox to enable/disable it.
   - Assign Cabinet Rights
   - Configure Alarms
   - Manage Stamp
   - Register NewgenONE Marvin: Select this checkbox to enable the NewgenONE Marvin feature in OmniDocs.

Removing rights of supervisor

This feature when applied, removes the rights of the supervisor2, and converts it into a normal user. When this option is enabled, the rights and privileges of Supervisor2 can be changed as this user can be disassociated from the supervisor group.

To Remove the Rights of Supervisor:

1. Go to the **Cabinet Details** screen.
2. Select the **Remove the Rights of Supervisor** checkbox.
3. Click **Save** to save the modified cabinet properties. A Cabinet Properties Saved Successfully message appears.

Owner inheritance policy

Once this option is enabled from the Cabinet Details page, the ownership of the folder will be inherited to its sub-folders and documents even if the sub-folders and documents are created by some other users.

To Enable/Disable the Owner Inheritance Policy:

1. Go to the **Cabinet Details** screen.
2. Select the **Inherit Ownership** checkbox to enable or disable the Owner Inheritance Policy.
3. Click **Save** to save the modified cabinet properties. A Cabinet Properties Saved Successfully message appears.

Owner Inheritance at Cabinet Level

Users can enable/disable the owner inheritance policy at the cabinet-level.

1. Set Owner inheritance Policy at the cabinet-level.
2. Add folders at the root level with user inheritance policy enabled.
3. The owner of the new folder is inherited from the cabinet's owner.

Owner Inheritance at Folder Level

On Adding a New Folder:

On adding a new folder, an option is provided for setting the Owner Inheritance Policy in Add Folder dialog box.

Case 1: If the owner inheritance policy is enabled at parent folder of the newly added folder and it is also enabled for the new folder while adding it or no value is provided for ownership inheritance, then, ownership inheritance is enabled at this folder also and the owner of the document will be inherited from its parent folder.

Case 2: If the owner inheritance policy is enabled at the parent folder of the newly added folder but it is not enabled for the new folder while adding it, then, ownership inheritance is not enabled for the new folder. If an owner is set for the new folder, then he will be set as the owner otherwise login user will be the owner of the folder.

Case 3: If the owner inheritance policy is not enabled at the parent folder of the newly added folder but is set as enabled for the new folder while adding it, then, ownership inheritance is enabled for the new folder. If an owner is set for the new folder, then he will be set as the owner otherwise login user will be the owner of the folder.

Case 4: If the owner inheritance policy is not enabled for the parent folder of the newly added folder and it is not enabled for the new folder while adding it or no value is provided for ownership inheritance, then, ownership inheritance is not enabled for the new folder. If an owner is set for the new folder, then he will be set as the owner otherwise login user will be the owner of the folder.

Setting Owner Inheritance Policy for an Existing User

There is an option provided to set or unset the Owner Inheritance Policy in the Folder dialog box. There are two conditions while setting this policy at the folder level.

Condition 1: If the owner name is not declared and ownership inheritance is changed (set/unset), then ownership inheritance is enabled or disabled depending upon whether it is set or unset for this folder only.

Condition 2: If the owner name is declared then there can be the following possible cases:

1. If currently ownership inheritance policy is enabled, and no value is provided for new ownership inheritance or it remains as enabled then Owner change for those subfolders whose Owner Inheritance is I (along with their documents) Stop at subfolder whose Owner Inheritance is 'N'.
2. If currently ownership inheritance policy is enabled and now it is set as disabled, then Ownership inheritance policy will be set as disabled for this folder and owner changes for this folder only. No change at the subfolder level.
3. If currently ownership inheritance policy is not enabled and now also it is retained as disabled or no value is provided for Ownership Inheritance, then Ownership inheritance policy will be set as disabled for this folder and owner changes for this folder only. No change at the subfolder level.
4. If currently ownership inheritance policy is not enabled and now it is set as enabled, then ownership inheritance policy will be enabled for this folder and Owner change for those subfolders whose Owner Inheritance is I (along with their documents). Stop at subfolder whose Owner Inheritance is 'N'.

Copying a Folder

Case 1: If the user inheritance policy is enabled at the destination folder, then ownership inheritance policy becomes enabled at the folder that is copied as well as its subfolders. The owner of this folder as well as its subfolders (including documents) will be inherited from the destination folder.

Case 2: If the user inheritance policy is not enabled at the destination folder, then there will be no change in the ownership inheritance of the folder that is copied. The owner of this folder as well as its subfolders (including documents) is the person who is performing the copy operation.

Owner Inheritance at the Document Level

Adding Documents

When a new document is added to a folder, the Owner inheritance policy is verified for its Parent Folder. If it is set for the parent folder, the owner of the document remains the same as the owner of its parent folder.

If it is not set, the owner of the document will be the user who is adding the document.

Copying Documents

When a document is copied to a destination folder, the Owner inheritance policy is verified for its destination folder.

If it is set for the destination folder, the owner of the document remains the same as the owner of its parent folder.

If it is not set, then the owner of the document will be the user who is copying the document.

Data security

Making OmniDocs Data Security enabled means that sensitive data can be identified and marked as secured so that it can be stored in a way that it is only available in a readable form to a person who is authorized to view that information. This Data Security implementation covers many data security-related points. These are:

- Format of data being stored (AES-128 and 256 encrypted).
- Availability of data in a readable form on a web application to authorized people.
- Restriction on the visibility of sensitive information in logs and database from even those people who have complete/supreme authority on the Database Server or Application Server.

To Enable and Configure Data Security Functionality:

1. Go to the **Cabinet Details** screen.
2. Select the **Enable Data Security Functionality** checkbox.

   Once enabled, it cannot be disabled.

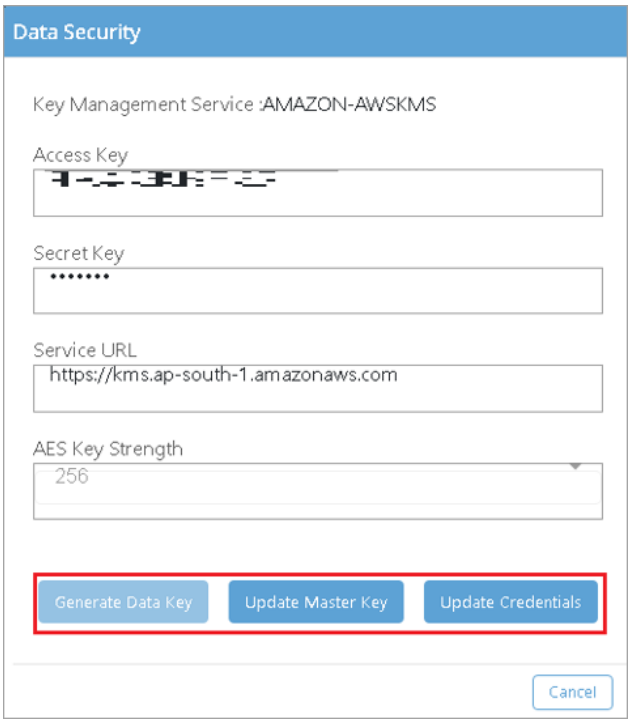
3. Select the required Key Management Service from the dropdown list.

4. Click **Data Security** link. The Data Security dialog appears.

    a. Provide the following details:
    - Access Key
    - Secret Key
    - Service URL
    - Select the AES Key Strength from the dropdown list. It is advised to select it carefully as this can be selected only once. After the first-time selection, this dropdown is disabled. The available options are:
    - 128
    - 256

    AES 256 encryption is available in Java, but it must be enabled explicitly. If AES 256 Encryption is selected, then to enable it, refer to the section AES 256 Encryption of NewgenONE OmniDocs 11.0 SP1 Patch 3 Configuration Settings Guide.

    b. Click **Generate Data Key** to generate Data Key for the first time.
    c. Click **Update Master Key** if the Key is to be updated.
    d. To update Credentials, re-enter the necessary details and click **Update Credentials**.



5. Click **Save** to save the modified cabinet properties. A Cabinet Properties Saved Successfully message appears.

Two-factor authentication

With the implementation of two-factor authentication, OmniDocs now has an extra layer of security. If enabled, the users trying to gain access to OmniDocs will have to provide another piece of information in the form of an OTP, in addition to their user credentials.

You can implement the two-factor authentication in the following two ways:

- Default two-factor authentication
- Custom two-factor authentication

Default Two-factor Authentication

The default two-factor implementation is an extended feature that is used for enhanced authentication of users while logging in to OmniDocs. An OTP is generated and sent to the registered email ID of the user. Upon successful validation of OTP, the user is allowed to log in to OmniDocs.

Before enabling the default Two-Factor Authentication, make sure you have configured the mail server. Also, email IDs of the users including the default users Supervisor and Supervisor2 must be registered in OmniDocs for sending OTPs to them. Members of the Second Factor Immune group are not required to pass through the two-factor authentication even if Two Factor Authentication is enabled.

Custom Two-factor Authentication

Way of providing the Class Name, for example, if a package name is *com.newgen.omni.jts.client* and the class name is *TwoFactor*, then enter the class name as follows:
com.newgen.omni.jts.client.TwoFactor

This class can reside in any JAR inside *modules\omnidocs_library\main*.

Taking a case of JBoss server, one possible path for the above class can be as given below:

jboss-eap-7.2\modules\omnidocs_library\main\ejbclient.jar\com.newgen.omni.jts.client

To enable the Two-Factor Authentication:

1. Go to the **Cabinet Details** screen.
2. Select the **Enable Two Factor Authentication** checkbox.

   To disable the already enabled Two-Factor Authentication, clear the Enable Two Factor Authentication checkbox.

3. Enter the Two Factor Authentication Class Name as given below:
   - For the default implementation: com.newgen.omni.jts.client.TwoFactorImplementation
   - For the default implementation with secret manager: com.newgen.omni.jts.client.SecretTwoFactorImplementation
   - For the custom implementation: The name of your custom defined class name.
4. Click on **Save** to save the modified cabinet properties. A message Cabinet Properties Saved Successfully appears.

To Log in to OmniDocs when Two-Factor Authentication is Enabled:

Members of the Second Factor Immune group are not required to pass through the two-factor authentication even if Two Factor Authentication is enabled.

1. Enter your login credentials in the OmniDocs login screen.
2. Click on **Login**.

   In the case your email ID is not registered, “Mail ID is not registered with user” message appears on clicking Login. In that case, get your email ID registered in OmniDocs. In the case mail server details are not registered, “Mail Server Details are not registered” message appears on clicking Login.

3. Two-Step Authentication screen appears.

   The Two-Step Authentication screen appears only if you have entered the correct login credentials. In the case of incorrect login credentials, “Invalid Login Information” message appears.

4. Enter the OTP that you have received on your registered email ID.
   - Click on Resend OTP link, if you have not received the OTP.

     The OTP is valid for 10 minutes. If the OTP validity time exceeds the defined limit, then you must re-generate the OTP again.

5. Click on Login.
   a. If the entered OTP is valid, you will be logged into OmniDocs.
   b. If the entered OTP is invalid, you are asked to re-enter the OTP.

      Your OTP is not valid if it has expired, or the entered OTP is incorrect.

   c. Enter the correct OTP and then click on Login again.

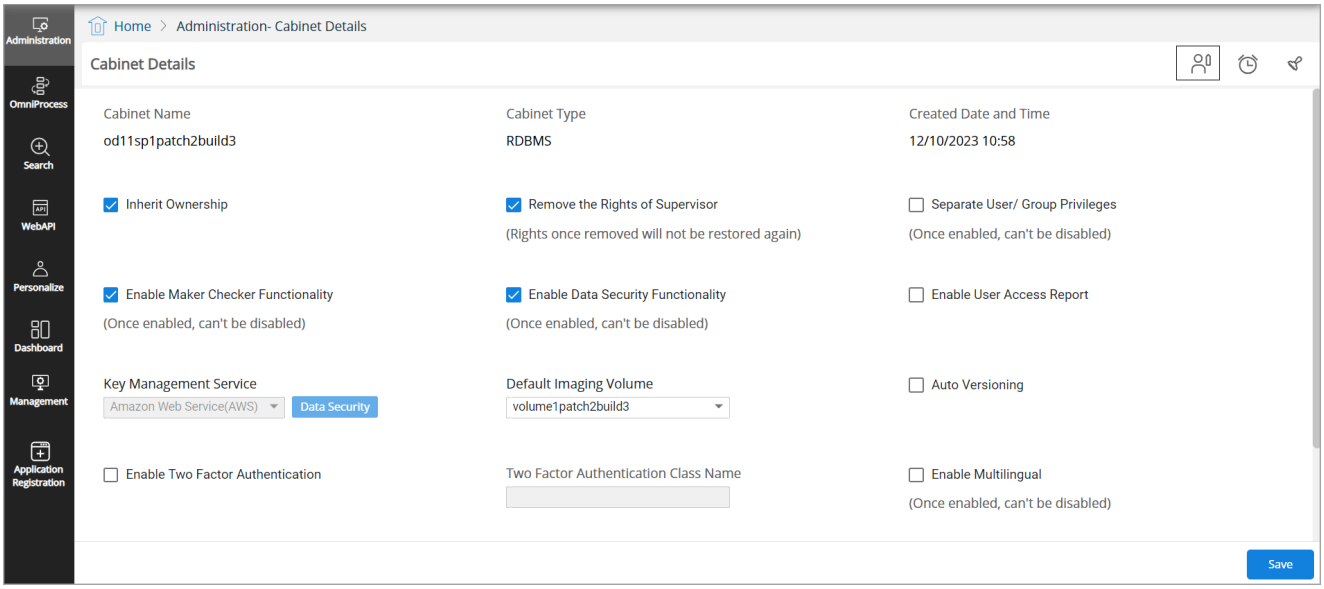
You get three chances to re-enter the OTP. When you have exhausted all three chances, you get redirected to the login screen. You must again follow the same process to gain access to OmniDocs.

Assigning rights on cabinet

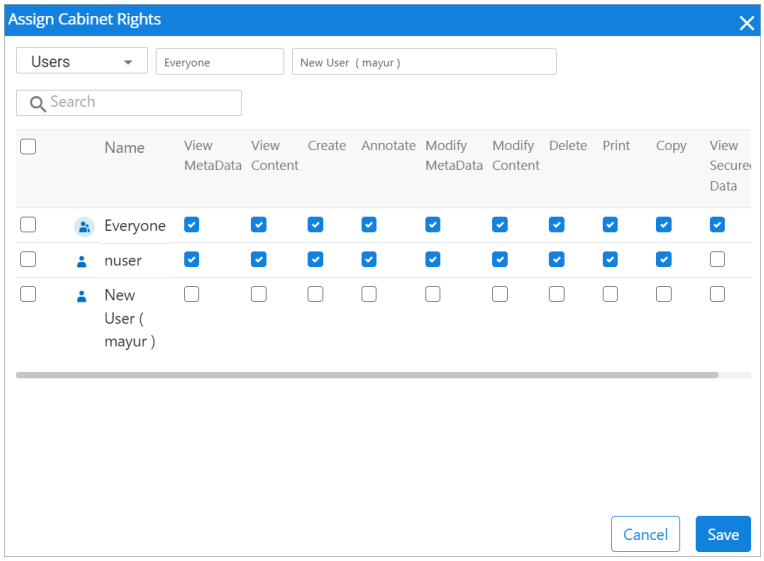
The Assign Cabinet Rights feature is used to assign rights to other OmniDocs users or groups or roles on the logged-in cabinet.

To Assign Rights to Users, Groups, and Roles on a Cabinet:

1. Go to the **Cabinet Details** screen.



2. Click on the **Rights** icon. The Assign Cabinet Rights dialog appears.
3. Add Users, Groups, and Roles to the Rights list.
4. To add users to the Rights list:
    a. Select Users from the Groups/Users/Roles dropdown list.
    b. Select or Type Group name in the associated combo box.



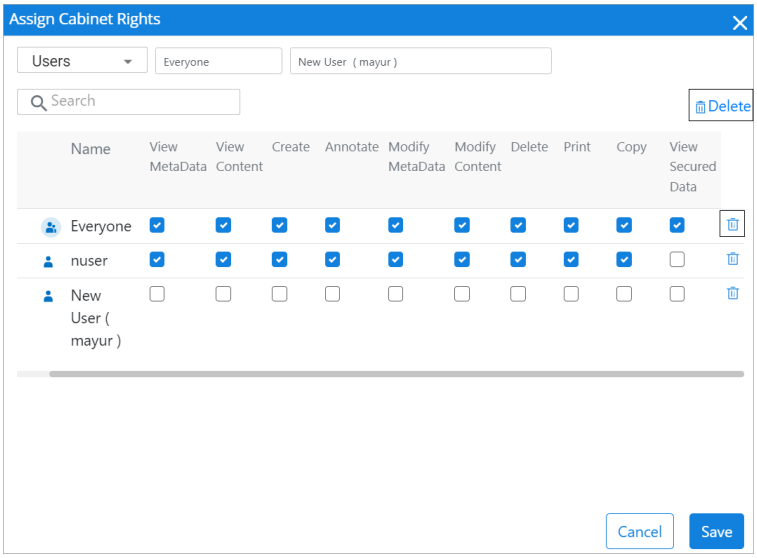
c. Select or Type User Name in the associated combo box.

5. To add groups to the Rights list:
   a. Select Groups from the Groups/Users/Roles dropdown list.
   b. Select or Type Group name in the associated combo box.
6. To add roles to the Rights list:
   a. Select the Role from the Groups/Users/Roles dropdown list.
   b. Select or Type Group name in the associated combo box.
   c. Select or Type User Name in the associated combo box.
7. As you select a User, Group, or Role, it gets added to the Rights list.
8. Now that Users, Groups, and Roles are added to the Rights list, you can assign Rights to them. Refer to the below table for the meaning of the different rights:

Fields	Description
View MetaData	It is used to give rights to users to view the metadata. With this right, the user will be able to see the list of folders and their metadata.
View Content	It is used to give rights to users to view the document content.
Annotate	It is used to give rights to users to apply annotations and notes on the documents. In case annotations are to be applied to the documents then View Content, Modify Content and Annotate Rights are required.
Modify MetaData	It is used to give rights to users to modify the metadata tagged with the documents/folders. The users can modify the metadata only if they have View Metadata and Modify Metadata rights.

Fields	Description
Modify Content	It is used to give rights to users to modify the document content. The Check-in and checkout features will work only if this right is provided. If Modify Content rights are provided then Modify Metadata rights are automatically assigned.
Delete	It is used to give rights to users to delete documents/ folders.
Print	It is used to give rights to users to print documents.
Copy	It is used to give rights to users to copy documents/ folders.
View Secured Data	It is used to give rights to users to view the data fields that are marked secured. Minimum view metadata and view secured data are required to view the secured data. This option will appear here if the Data Security feature is enabled on the cabinet.

9. To remove any User/Group/Role from the Rights list:
    a. To remove a single rights holder, click on the Remove button against the rights holder.
    b. To remove multiple Users/Groups/Roles simultaneously:
        i. Select the required users/groups/roles.
        ii. Click on the **Delete** button that appears after selecting two or more users.



10. Click **Save** to save the assigned rights.

Alarms

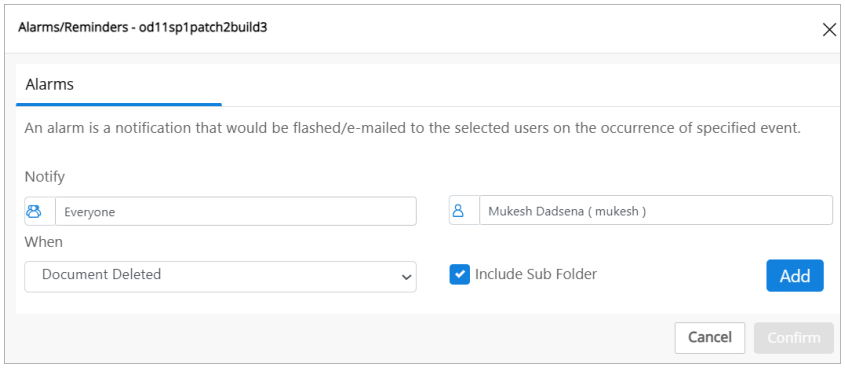
An alarm is a notification that would be flashed/e-mailed to the selected users on the occurrence of the specified event.

To Set Alarms at Cabinet Level:

1. Go to the **Cabinet Details** screen and click on the **Alarms** icon.
2. Alarms dialog box appears. It allows you to view existing and add new alarms.
3. Select or type the **Group** name and then the **User** to be notified. The options to select a Group and User are given in **Notify** section.

   The combo box to select User contains only those names that belong to the selected group.

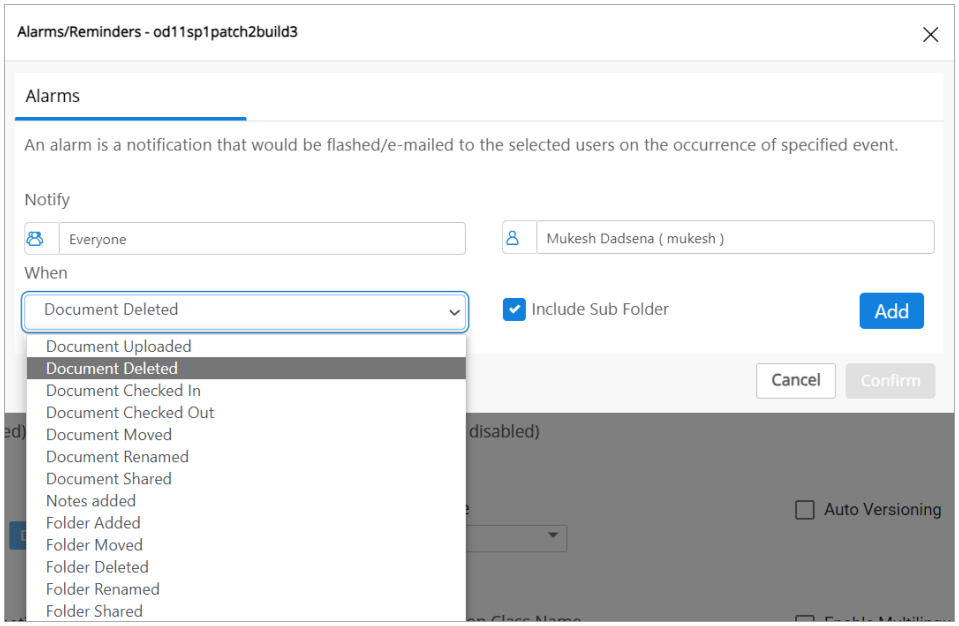
4. Select **Include Sub Folder** to apply the alarm on sub-folders also.



5. Select the desired event from the When dropdown list.
   The different types of document-level alarms which can be set on the folder are:

Alarms	Description
Document Uploaded	When any document will be uploaded to this folder, an alarm will be generated for the specified user.
Document Deleted	When any document will be deleted from this folder, an alarm will be generated for the specified user.
Document Checked In	When any document will be checked-in to this folder, an alarm will be generated for the specified user.
Document Checked Out	When any document will be checked-out from this folder, an alarm will be generated for the specified user.

Alarms	Description
Document Moved	When any document will be moved/copied to some other location from his folder, an alarm will be generated for the specified user.
Document Renamed	When any document from this folder will be renamed, an alarm will be generated for the specified user.
Document Shared	When any document will be shared from this folder, an alarm will be generated for the specified user.
Notes Added	When notes will be added to any document of this folder, an alarm will be generated for the specified user.
Folder Added	When any sub-folder will be added to this folder, an alarm will be generated for the specified user.
Folder Moved	When the folder will be moved, an alarm will be generated for the specified user.
Folder Deleted	When the folder will be deleted, an alarm will be generated for the specified user.
Folder Renamed	When the folder will be renamed, an alarm will be generated for the specified user.
Folder Shared	When the folder will be shared, an alarm will be generated for the specified user.



6. Click on **Add** to set the alarm. The added alarm appears in the Selected Alarms section.
    a. To remove an alarm from the list of Selected Alarms, click on (**Delete**) against the alarm that is to be deleted.

> Repeat the above steps to add more alarms.

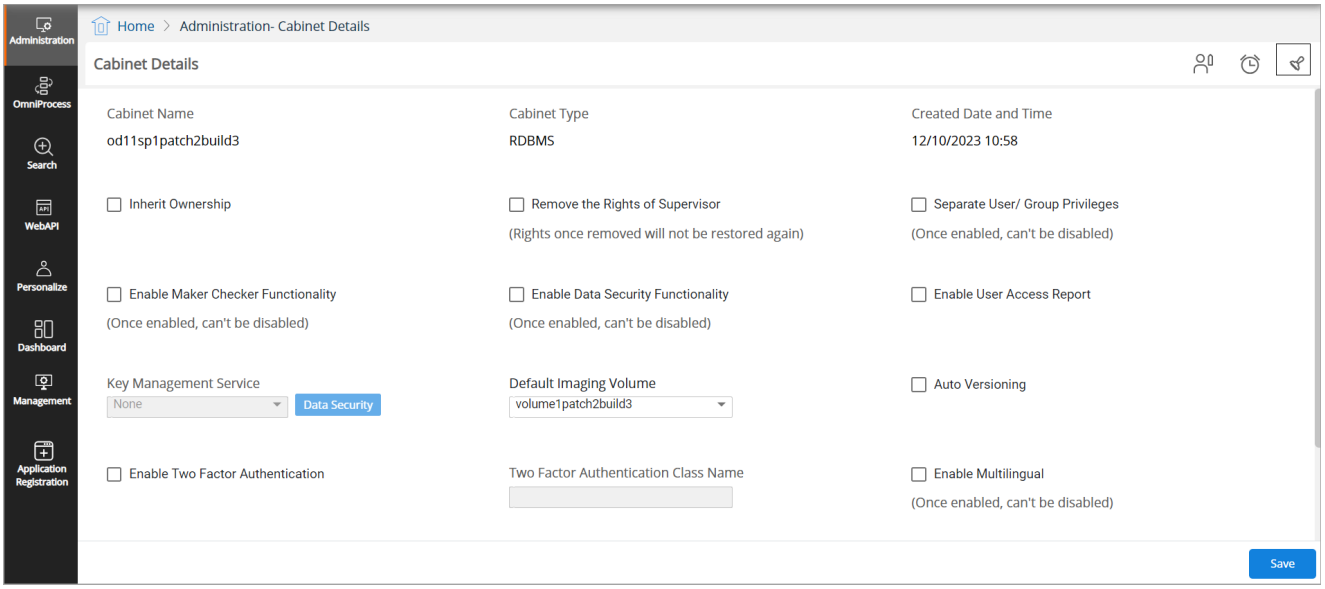
7. Click on **Confirm** to save the set alarm. A message “Selected Alarms have been set successfully” appears.

Stamps

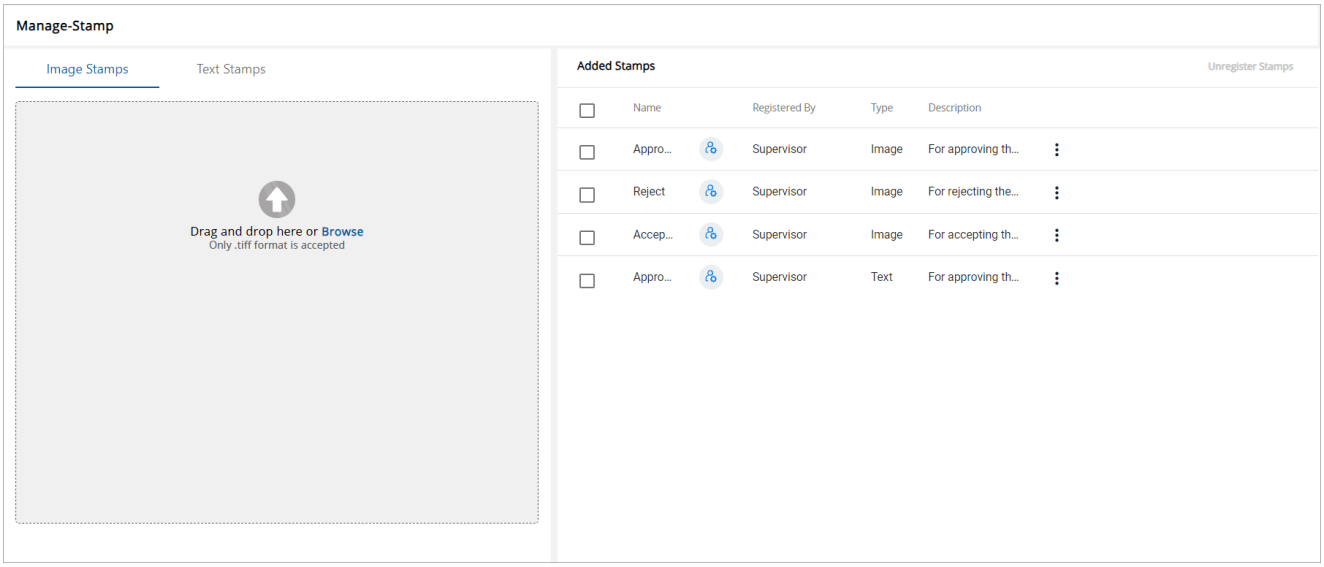
A stamp is an image, which can be applied to documents. Only registered stamps are available for use. There is no limit to the number of stamps you can register. You can unregister stamps, which are not required further. To replace a registered stamp, unregister the existing stamp and register the new stamp.

To Register Image Stamps:

1. Go to the **Cabinet Details** screen and click the **Manage Stamps** icon . The Manage Stamp screen appears.



2. Click **Browse** and select a required stamp. You can also drag and drop the required stamp in the Image Stamps section. Make sure to select a *.tif* image.



3. Enter the Name of the Stamp and Description. The fields marked with * are mandatory to fill.
4. Click **Register**. The Stamp Registered Successfully message appears. The added stamp appears in the Added Stamps list.

Register a new text stamp:

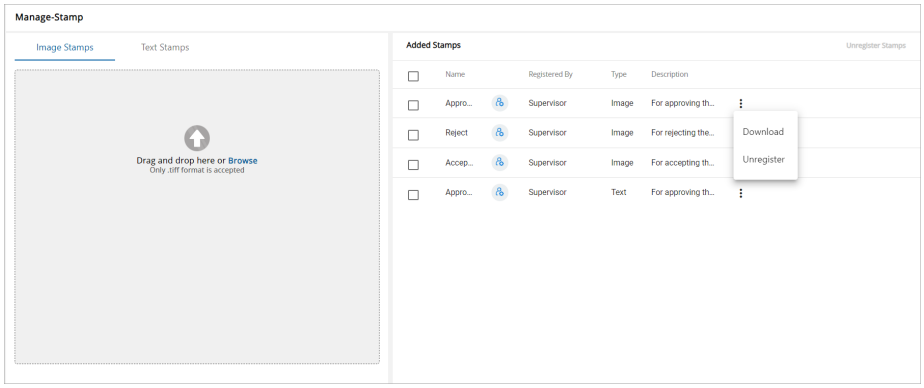
1. Click the **Text Stamps** tab and specify the following details:

Option	Description
Name of Stamp	Enter the name of the stamp.
Description	Enter the description of the stamp.
Stamp Text	Enter the stamp name which you want to create. Set the font, font size, color, and type.

2. Click **Register**. The Stamp Registered Successfully message appears. The added stamp appears in the Added Stamps list.

To Unregister a Stamp:

1. Go to the **Manage Stamp** screen.
2. Click the ⋮ **More Actions** button against a stamp to unregister it.
3. Select **Unregister**.
   - If you want to unregister multiple stamps simultaneously, then select the multiple stamps that you want to unregister and click Unregister Stamps. This Unregister Stamps button enables only if you have selected multiple stamps.



4. A message “Stamp Unregistered successfully” appears.

To Download a Registered Stamp:

1. Go to the **Manage Stamp** screen.
2. Click the ⋮ **More Actions** button against a stamp to download it.
3. Select **Download**.
4. The selected stamp gets downloaded onto your local drive.

Registering NewgenONE Marvin

NewgenONE Marvin is a Generative Artificial Intelligence (GenAI) through which you can generate questions and answers based on the chosen documents within a repository, search configuration, and easy search.

Prerequisites

To use NewgenONE Marvin capabilities, Text Extraction Manager (TEM) must be installed and integrated with NewgenONE OmniDocs.

You must register and configure its engine settings to use the NewgenONE Marvin feature in OmniDocs.

Registering NewgenONE Marvin

To register NewgenONE Marvin, follow the below steps:

1. On the home page, go to the **Administration** tile and select **Cabinet details**. The Cabinet Details page appears.
2. Select the **Register NewgenONE Marvin** checkbox.
3. Enter a valid license key for NewgenONE Marvin.

The NewgenONE Marvin license key is provided by Newgen.

4. Click **Validate** to verify.
   On successful license validation, a popup indicating the successful registration of NewgenONE Marvin appears. Furthermore, you can see the NewgenONE Marvin logo on top of the Home page and a NewgenONE Marvin on the Configure tile.
   For more information, see Configuring NewgenONE Marvin settings.

Applications

This functionality is used to segregate user licenses between various associated Newgen applications. As per this, only those Users who have been associated with the configured application will be able to access it. For example, if an OmniDocs user has not been associated with iBPS, then in such case that user cannot use iBPS.

A normal user can only access multiple Newgen applications, only if he has separate licenses for each one of them.

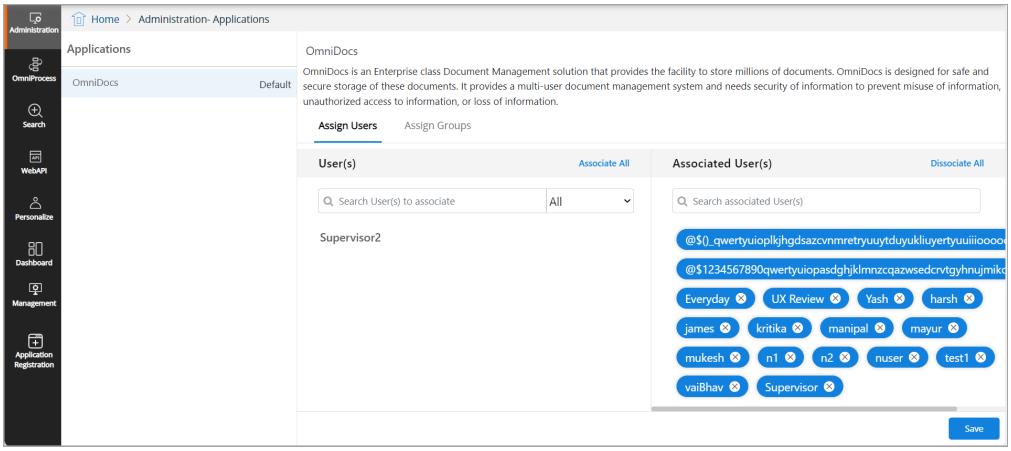
- Users of fixed type will be able to log in any number of times; there is no concurrency check for them. For users of another type, concurrency check is per the limit set on their user type.
- In the case of S type users, the same user can login multiple times at the same time. Users of another type can login only once at the same time.
- Only Supervisor and Supervisor2 users can login as both U type and S type. Other users will only login as per their user type.
- From the License Management page in OD Admin, a user with administrator rights can select different users and associate them to a particular application.

In addition to the following subsections, refer to the Application Specific Licensing for more understanding about Applications.

- Associate Users with the Application
- Associate Group Members with the Application

To Access Applications

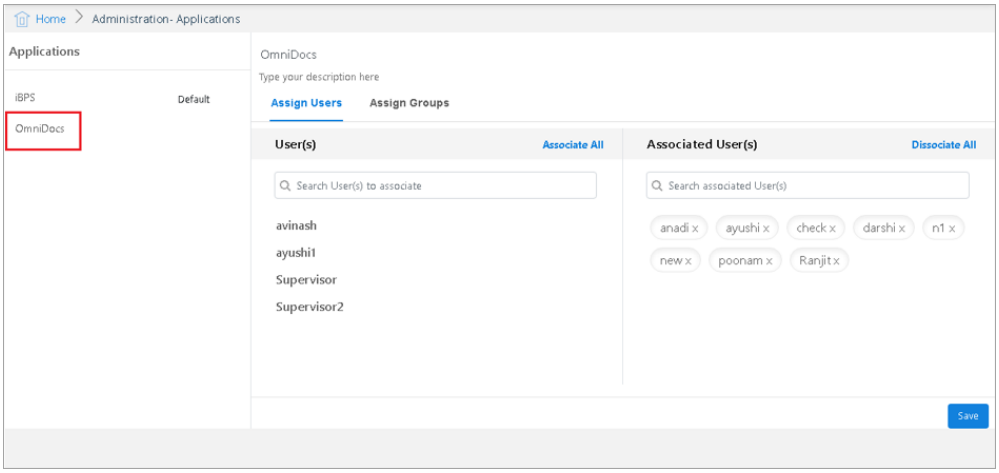
1. In the home screen of OmniDocs Admin, go to **Administration** tile and click on **Applications** link.
2. Applications screen appears. The left pane shows a list of applications, and the right pane shows the users and groups.



Associate users and groups with applications

To Associate Users and Groups with an Application:

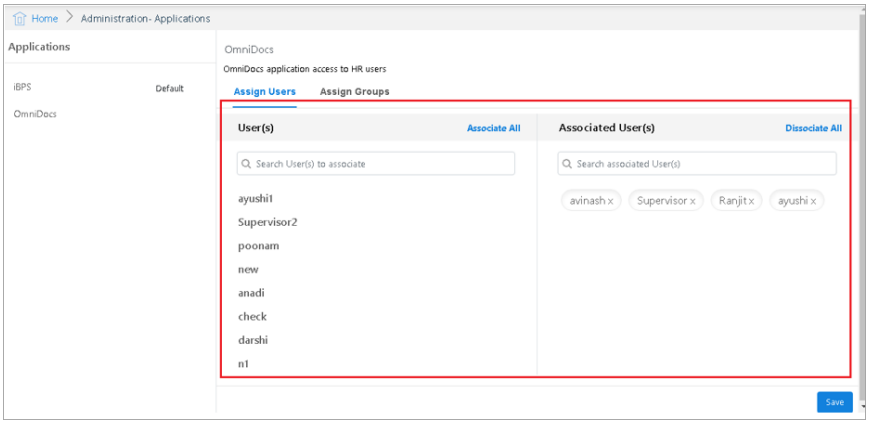
1. Go to the **Applications** screen.
2. A list of the configured Applications is shown in the left pane.
3. Choose the required **Application**.



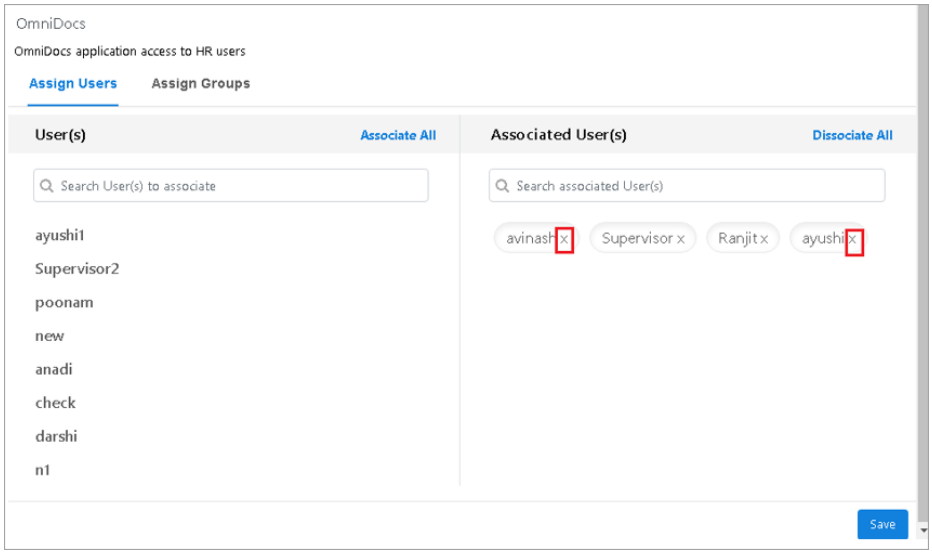
4. Specify a description of the selected application in the **Type your description here** textbox.
5. To **Associate/Disassociate Users**: Here, you can add users to access the selected application. You can also remove associated users and restrict them from accessing the application.
    a. Click on **Assign Users** tab.

b. Choose the required users from the list of Users or click on **Associate All** to associate all the users. As you click on a user name, it is moved to the Associated User(s) list.
   - You can also search for users to associate them to the application.

c. The selected users are added in Associated User(s) list.



d. To remove associated users and restrict them from accessing application:
   i. From the **Associated User(s)** list, click on the cross mark against the users to restrict them from accessing the application. As you remove a user from the **Associated User(s)** list, it is moved to the **User(s)** list.
      - You can also search for users to remove them from the application.

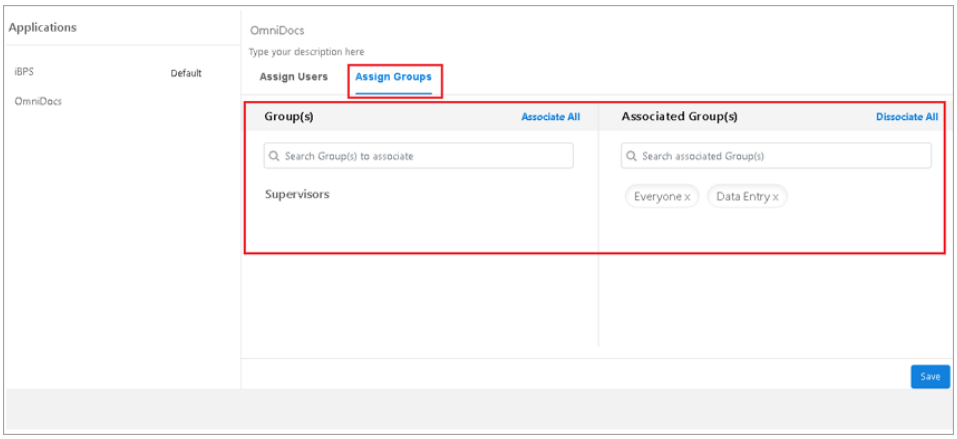


   ii. You can click on Dissociate All to remove all the associated users in one click.
      - On selecting this option, a warning message appears.
      - Click on **Yes** to proceed.

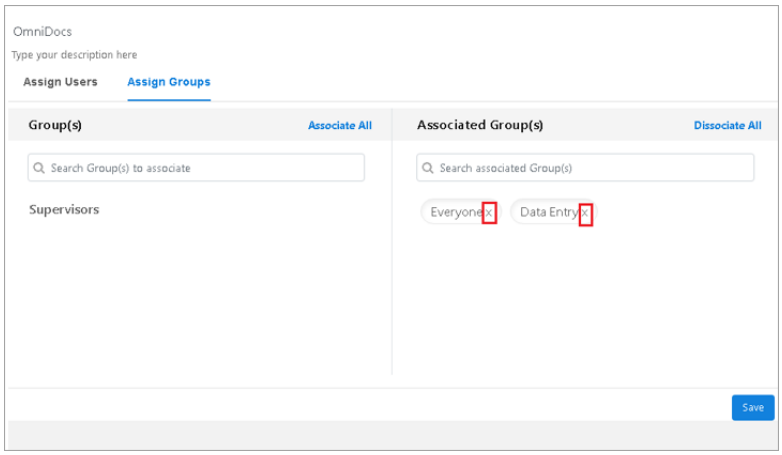
6. To **Associate/Disassociate Groups**: Here, you can add groups to access the selected application. You can also remove associated groups and restrict them from accessing the application.

You can select a group (or groups) and associate it with the application. In such a case, only the members of the selected group(s), not the group itself, will be associated with the application. Once the user has been associated with the application, he will remain associated even if he is removed from the group afterwards.

a. Click on **Assign Groups** tab.
b. Choose the required groups from the list of Groups or click on **Associate All** to associate all the groups. As you click on a group name, it is moved to the Associated Groups(s) list.
    - You can also search for groups to associate them to the application.
c. The selected groups are added in **Associated Group(s)** list.



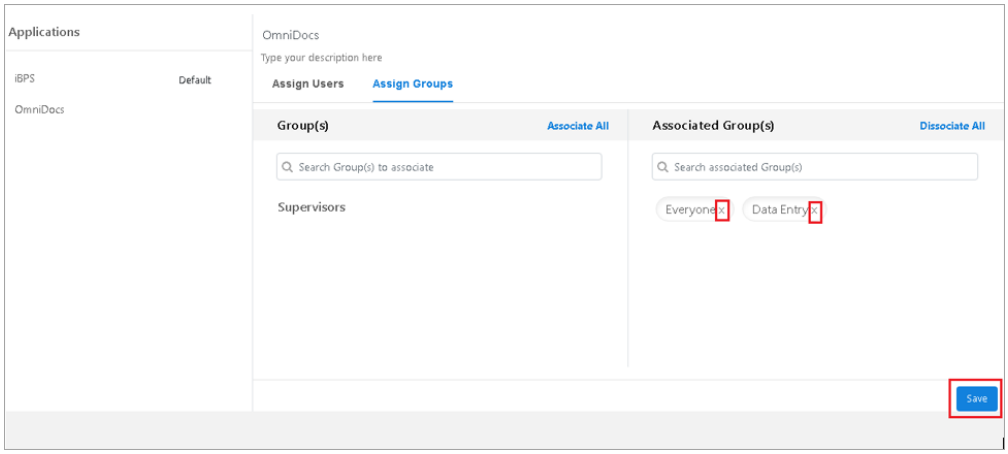
d. To remove associated groups and restrict them from accessing the application:
    i. From the **Associated Groups(s)** list, click on the cross mark against the groups to restrict them from accessing the application. As you remove a group from the **Associated Group(s)** list, it is moved to the **Group(s)** list.
        - You can also search for groups to remove them from the application.



    ii. You can click on Dissociate All to remove all the associated groups in one click.
        - On selecting this option, a warning message appears.

- Click on Yes to proceed.

7. Click on **Save** to save the selections.



Application-specific licensing

To associate application-specific licensing, perform the below steps:

1. In OmniDocs, following are the types of users:
   a. U type
   b. S type
   c. F type (Fixed users)
   d. External Portal users
   e. Internal Portal users
2. The new CD key will contain the following information **(Highlighted fields are new)**:
   a. **Client Name**
   b. **Application Name:** OmniDocs, OmniFlow, OmniScan and iBPS
      - There has been segregation of user licenses between the applications. Now, there would be a separate CD key for each Newgen product.
   c. **Environment Type:** Development, Testing, UAT and Production
      - There would be a separate CD key for each of the environments.
   d. The number of U type users that can be created.
   e. The number of U type users that can login at the same time.
   f. The number of fixed users that can be created.
   g. The number of S type users that can be created.
   h. The number of S type users that can login at the same time.
   i. The number of default S type users that can login at the same time.

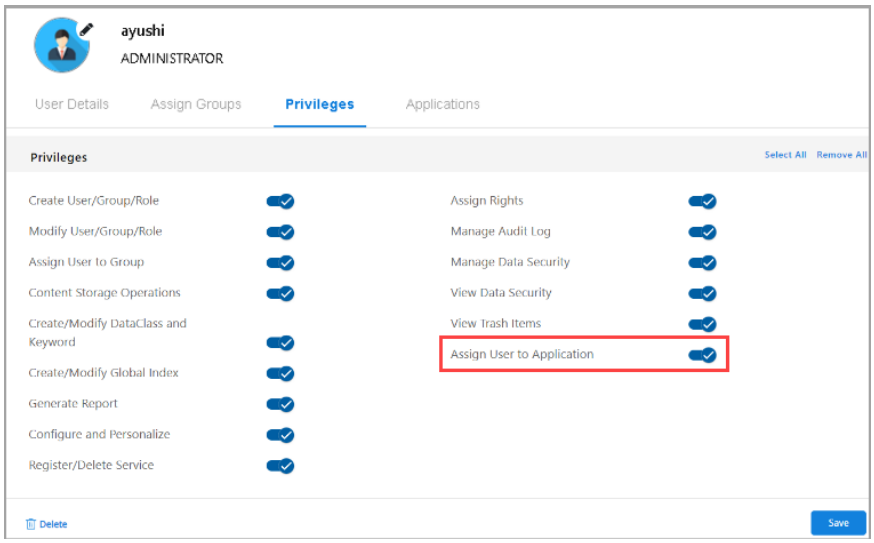
j. The number of External Portal users (E type) that can be created.
k. The number of External Portal users (E type) that can login at the same time.
l. The number of Internal Portal users (I type) that can be created.
m. The number of Internal Portal users (I type) that can login at the same time.
n. **Expiry Time:** The CD key generated through CD Key Generator will be valid only for 30 days. However, the installer of this version of OmniDocs will have no expiry.

3. CD key will always be unique for any combination and will be encrypted for maintaining security. T**he new CD key will be generated using the new CDKeyGenerato**r.
4. The **first application registered** in the cabinet will be set as the Default application of the cabinet. However, if there are more than one registered product in the cabinet, the default application can be changed from only OmniDocs UI.
5. **Fresh Installation**
   When a new cabinet of OmniDocs will be installed through installer, ClientName, ApplicationName and EnvironmentType will be set as Newgen, OmniDocs and Development, respectively and the license count for all the userTypes will be set to ten. OmniDocs will be set as the Default application.
6. **Cabinet Upgrade to a new version of OmniDocs**
   - When an existing cabinet will be upgraded through OSA, the old license count details for all user Types will remain the same. ApplicationName will be OmniDocs, ClientName will be empty and EnvironmentType would be Development. OmniDocs will be set as the Default application.
   - After upgrade of cabinet, if login is done through any other application/ utility/product which is sending application name and product name in connect cabinet, whether login is to be allowed or not in this case, is now made configurable based on a flag at the cabinet level, i.e., AllowCrossApplicationLogin. This flag is enabled by default at the time of upgrade to allow login of all the applications to maintain backward compatibility.
   - Once the AllowCrossApplicationLogin flag is disabled, then:
     - To allow login of other applications/utilities/products, the CD key of the corresponding products need to be registered in the cabinet through upgrade license in OSA, i.e., there would be a separate license used for each of the products. Association of the users should also be done with the products, however, it is not mandatory.
     - If the product name sent in Connect Cabinet, for example, is OmniFlow and the CD key of OmniFlow is not registered in the cabinet, the login

will not be allowed. This would be applicable for all the product names which are sent in connect cabinet.

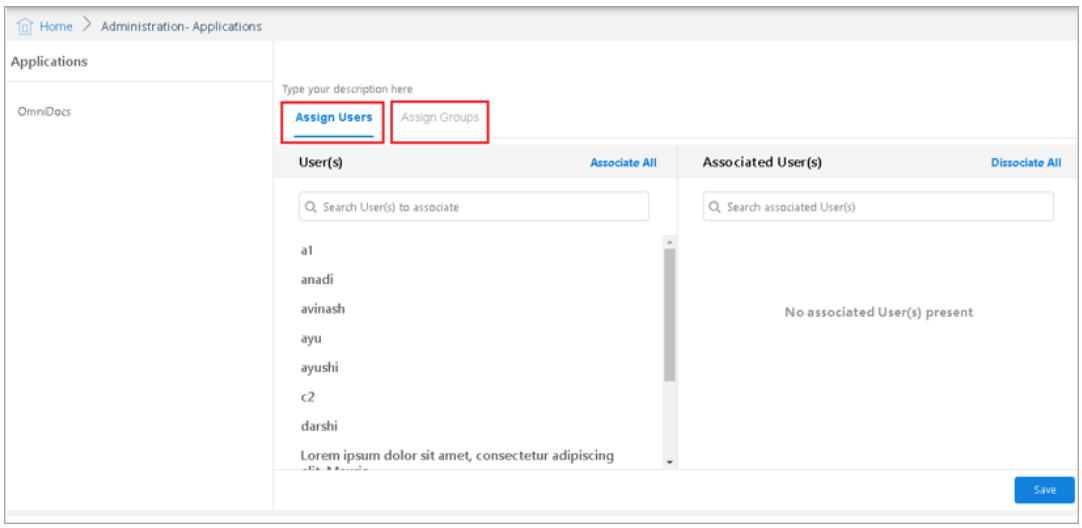
- If the product name in Connect cabinet is not sent, but the ApplicationName is sent, then the mapping of this application name should be present with some product in the new mapping table. Also, the CD key of the mapped product should be registered in the cabinet to allow login.
- If both Product and ApplicationName is not sent in Connect Cabinet, the license of the default application should be available to login.

7. **Registration of other Applications/Products:** The other products like OmniFlow, OmniScan and iBPS can be registered in cabinet through Upgrade License option in OSA by using the CD key of the corresponding ApplicationName.
8. **Upgrade License Information:** The license count of any userType for any Application can be upgraded through Upgrade License option in OSA by using the new CD key of the corresponding ApplicationName.
9. **Association and Disassociation of Users with Applications:** Each user can now be associated with the product he/she wants to use, in order to keep in check the consumption of the licenses of each product.
    a. **Changes in OmniDocs Admin for associating users with different applications.**
        i. **Changes in privileges:** A new privilege in privileges section is added for assigning users to application. Users having this privilege only can associate users to applications.



        ii. **User Association** to Application management is provided from the Administration tile of OmniDocs Admin.

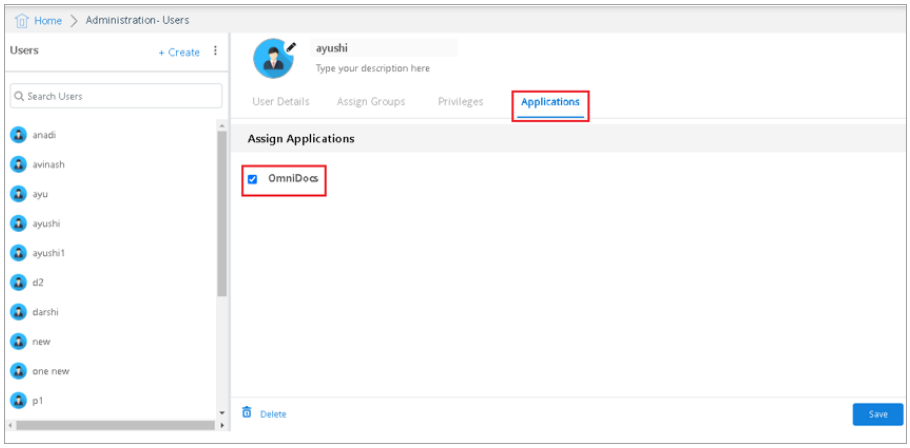
iii. For each application, there are two ways in which multiple users can be associated with an application. They can be associated either by selecting **Assign Users** or **Assign Groups**.



iv. One can select different users and associate them to a particular application. A user can be associated with more than one application. When this request is sent to the server, a check will be done whether the limit on the number of users that can be associated with that application has been reached for that user's license type. If yes, an error will be thrown.
In case, a request for multiple users is sent for the association but the license is not available for any of the user types among them, then the complete list of users would be rolled back and there would be no association.

v. One can also select a group (or groups) and associate it with the application. In this case, members of the selected group(s) will be associated with the application. Group itself will not get associated, only members of the group will get associated. Once the user has been associated with the application, he will remain associated even if he is removed from the group later on.
In case, the license is not available for any usertype among the group members, then no user in the group would be associated and the complete request would be rolled back. In case of multiple groups request also, if a license is not available for any of the group members of any group, there would be no association.

vi. The option is also provided for associating/disassociating users from applications from the user modification page.



b. **Changes in Add User:** ProductName is included in the input xml. The user, by default, would default associated with the product whose name is received in the xml otherwise no default association would be there. **AssociatedApplications** tag is included in the output xml which will contain the **Application indexes** with which the user got associated on creation.
    i. On adding a new user through OmniDocs UI, the user would by default get associated with OmniDocs. This is governed by the new **ProductName tag** in **AddUser input xml** which will be OmniDocs in this case.
    ii. On adding a new user through any other application or utility, the user would get associated with the product which is present in the **ProductName tag** in **AddUser input xml**.
    iii. **When product Name is sent in Add user**, the license limit of that user type for associating users to that product would be checked. Also, the license limit for that user type at cabinet level would be checked which will be the sum of all the maximum limits of all existing applications for that license type.
    iv. **When productName is not sent in Add user**, the license limit for that user type at cabinet level would be checked which will be the sum of all the maximum limits of all existing applications for that license type.

10. **License type** of users (whether **'U', 'S', 'E','I'**) would continue to be set from OmniDocs Admin as it is currently being done, and it will be same across different applications.
11. Changes in cabinet property:
    - **AllowCrossApplicationLogin** flag is introduced for configuring whether the user should be allowed to login if he is not associated with the product which is coming in connect cabinet.

- Also, it determines whether the concurrent licenses of other registered applications should be allowed to consume if the concurrent license of that particular userType of the given product is exhausted.

Eworkstyle.ini (AllowCrossApplicationLogin)	AllowCrossApplicationLoginCheckbox on UI
Y	Visible
N	Hidden

AllowCrossApplicationLoginCheckbox	AllowCrossApplicationLogin in PDBCabinet
Checked	Y (default value for backward compatibility)
Unchecked	N

12. Changes in connect cabinet API – New tag for ProductName has been included.
    a. Check will be done if the product name is sent in input and is registered in cabinet.
        i. If the product name given is not registered, then if AllowCrossApplicationLogin flag is disabled, error will be thrown. Otherwise, login will be allowed with the default application. Audit of the same will be maintained in both the cases.
        ii. However, if the given product name is registered in the cabinet, the license of the given product name would be checked.
    b. If no product name is sent, then check will be done if the application name is sent in input.
        i. The existence of mapping of this application name is then checked with some registered product in the cabinet.
            - If mapping is not present, then if AllowCrossApplicationLogin flag is disabled, an error will be thrown. Otherwise, login will be allowed with the default application. Audit of the same will be maintained in both cases.
            - If mapping is present, then the registration of the mapped product is checked in the cabinet.
                - If the mapped product is registered, then the login would be allowed based on the license check.

- If the mapped product is not registered, then if AllowCrossApplicationLogin flag is disabled, an error will be thrown. Otherwise, login will be allowed with the default application. Audit of the same will be maintained in both the cases.

c. However, if the application name is also not sent in input, then login is meant for the default application and license of default application would be checked.
d. Check will be done if the login user has been associated with the application that was retrieved in the above point. If not, then this action will be stored that this user is making login from the application he has not been associated with.
    i. Further check will be done if the login user has been associated with any other application.
        - If not then, then further check will be done if the default application and the application retrieved are same or not.
            - If not then, the configuration flag (AllowCrossApplicationLogin) is maintained at the cabinet level to determine whether an error will be thrown, or the user be allowed to continue to login. Based on the configuration done, respective action will be taken.
        - If yes, then the configuration flag (AllowCrossApplicationLogin) is maintained at the cabinet level to determine whether an error will be thrown, or the user be allowed to continue to login. Based on the configuration done, respective action will be taken.
e. Check will be done if the concurrency limit is reached for that product and for that user's license type. If the limit is reached, based on above mentioned configuration flag, an error will be thrown, or user will be allowed to login after recording this action.
f. Even if the user can login beyond the maximum concurrency limit for the product, he won't be allowed to go beyond the maximum concurrency limit set for the cabinet.
g. The maximum concurrency limit of a cabinet for a license type will be the sum of all the maximum concurrency limits of all existing applications for that license type.

Supervisor and Supervisor2 users can be allowed to login to any application.

13. **Changes in UserProperty:**
    New tag AssociatedApplications has been added which contains the AppIndexes of all the applications with which the user is associated with.
14. **Changes in DeleteUser:**
    When a user will be deleted, if it has any associations with any registered application, those associations will also be removed. Audit Logging of the disassociation will be done.
15. **Changes in Reports:**
    a. Application License Usage Summary Report: It will generate the Report of the maximum and minimum license usage of the application between the specified Date ranges.
    b. Application License Violation Detail: It will generate the details of the instances when the license count of an application has been exceeded as well as when the user has logged-in to the application with which it was not associated between the specified Date ranges.
    c. LicenseSummaryReport: License Summary Report provides a summary of the number of licenses of each type for each application registered that are present in the system and the concurrent licenses available for the same.
16. New APIs have been provided for following functionalities:
    - Association and Disassociation of Users from applications.
    - Getting registered applications of the cabinet.
    - Getting associated users of an application.
    - Setting default application of the cabinet.
    - Generating Application License Summary Usage Report of an application.
    - Generating Application License Violation Details.
17. Following new tables have been created:
    - PDBApplicationLicenseDetails, for storing license information of each application.
    - PDBUserApplicationMapping, for storing the association of each user with individual applications.
    - PDBProductModuleMapping, for storing the mapping of the subproduct/ applications with the products.
    - PDBAdminLogTable, for storing the audit of association and dissociation of the users with applications.
    - PDBLicenseLogTable, for storing the audit when concurrency limit of any licenseType will be exceeded.
    - PDBConnectionAuditTrail, for storing the audit of all the login and logout operations success and failure.

18. **Changes in Other Applications:**
    a. All applications that connect with the cabinet need to send application name in ProductName in input and Subproduct names in ApplicationName in input xml.
    b. Currently, this change would be required for OmniDocs, iBPS/OmniFlow and OmniScan.
        i. OmniDocs would include OmniDocs, OmniDocs Mobile, Text Extraction Manager, Alarm Mailer, LDAP, Thumbnail Manager, MSAddIn, etc.
        ii. Similarly, IBPs/OmniFlow would include OmniApp, iBPS/OmniFlow desktop, BAM, MDM, PS, Process Designer, and other related components. Application for iBPS and OmniFlow components can be the same.
        iii. OmniScan would include OmniScan thick client and OmniScan Web.
19. **Changes for LDAP:**
    LDAP users association is not done by default with any application at the time of synchronization. However, their login would be assumed with default application.
20. **Points to Note:**
    a. Currently there would be no separate license server for managing licenses of all application across different clients and cabinets. Currently, there will also be no restrictions on multiple cabinets. License management will be done within the scope of a single cabinet.
    b. There may currently be no license-based restrictions at API level. This may be taken up in the next phase. Following approach can be taken at that time:
        i. In case iBPS/OmniFlow requires that OmniDocs users cannot access iBPS/OmniFlow APIs then restriction may be placed in these APIs.
        ii. In case OmniScan users and Custom Utilities should use only specific APIs of iBPS/OmniFlow/OmniDocs then a list of APIs allowed for each application may be required to be maintained.

New License Key will be mandatory if the client is upgrading to a new version of OmniDocs. Also, at the time of upgrade, license information will be stored in the cabinet as per new the format, but with OmniDocs as the default application. Though users of other applications may be able to login successfully, such actions will get logged and will be shown in the corresponding reports.

Working with folders

A folder is a repository for the documents which can contain documents and sub-folders.

OmniDocs Admin offers you the following features:

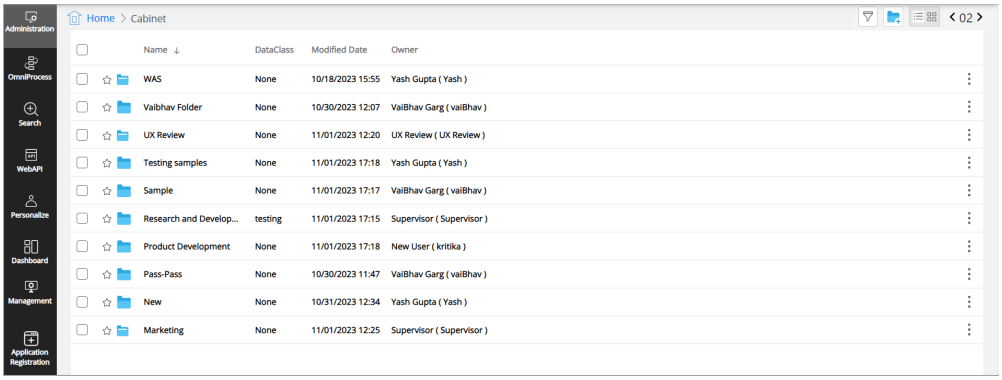
- It enables you to create a folder.
- It enables you to specify a Dataclass for the folder.
- It enables you to create an Image Volume, where you store the folder data.
- Provides the facility of viewing all the available folders and their properties.
- Allows you to modify the properties of the folder.

You can perform the following operations on the folders:

- Add a folder
- Add a sub-folder within a folder
- Manage rights for a particular folder
- Add a DataClass
- Delete a folder
- View and modify properties

To Access Folders:

1. In the home screen of OmniDocs Admin, go to **Administration** tile and click on **Folders** link.
2. The screen with all existing folders appears. It shows a list of existing folders.



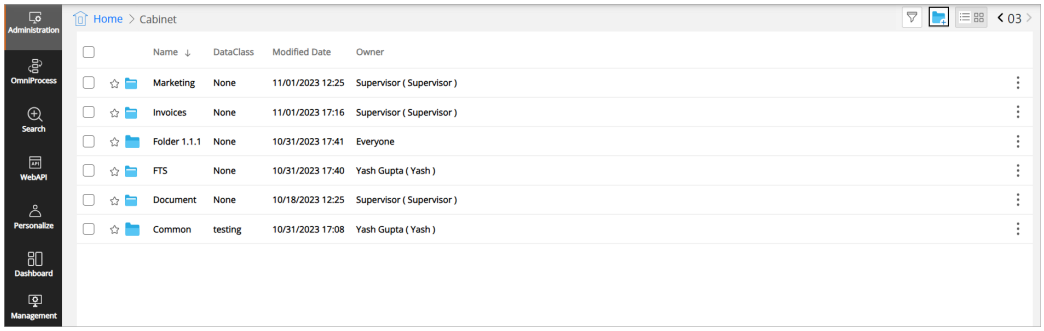
3. The following buttons appear on the operations bar:

Operations	Description
Search	It is used to search the required folders from the existing folders list.
Add Folder	It is used to add a new folder.
List View and Thumbnail View	Click on the List View button to change the view style to list view. Click on the Thumbnail View button to change the view style to thumbnail view.
01 Previous Batch and Next Batch	Click on Next Batch and Previous Batch buttons to traverse to next and previous pages, respectively.

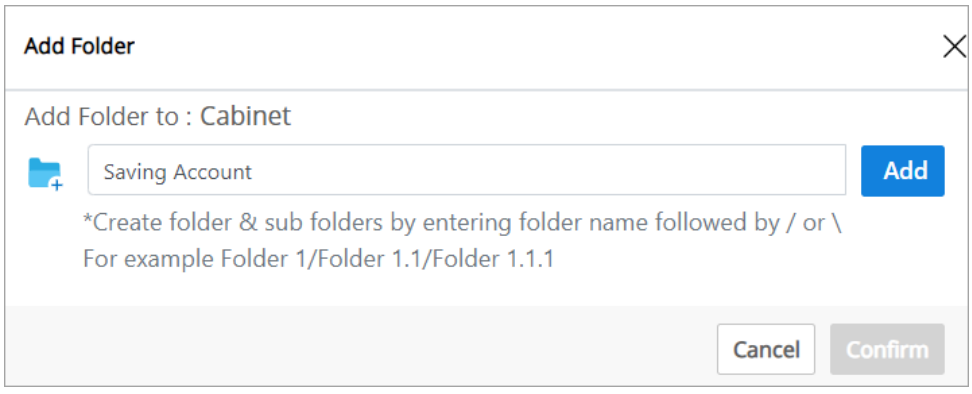
Adding a folder

To Add a Folder:

1. Go to **Folders**.



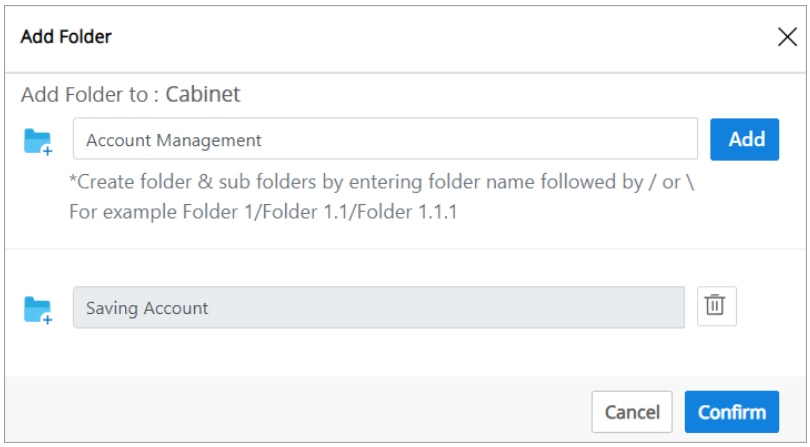
2. Click **Add Folder** icon. The Add Folder dialog box appears. The user can add Root Level folders (that is, under the shared cabinet) at this stage.



3. Type a folder name or URL to add.
4. Click **Add** to create the specified folder.

a. You can add multiple folders by repeating the above steps.

- You can create folder and sub-folder hierarchy here itself by entering folder name followed by / or \. For example: Folder 1/Folder 1.1/Folder 1.1.1.
- Users can also create folders containing forward slash in the name itself. Configuration flag is provided for this feature. By default, folder hierarchy will be created by the usage of the slash.



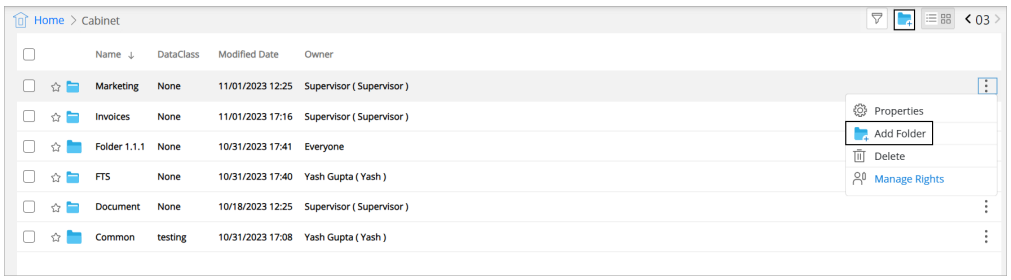
b. The added folders appear in a list form in the lower section of the dialog box.

c. Click **Delete** icon against the folder to delete it from the list.

5. Click on **Confirm** to add the listed folders in the cabinet. The message “Folder(s) added successfully” appears. The specified folders are added in the repository.

To Add a Sub-Folder within a Folder:

1. Click the desired folder within which you want to add a sub-folder. The folder information appears.
   a. The left pane shows list of folders created within the opened folder.
   b. The right pane shows the properties of the opened folder.
2. Click (Add Folder) icon.
   OR
   Click on More Actions button against the root folder and choose Add Folder.



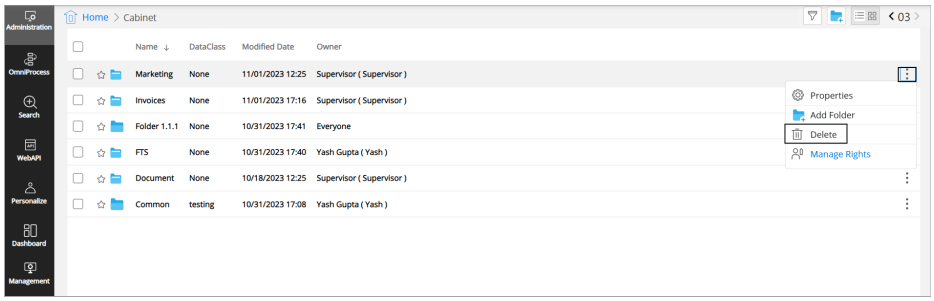
3. Add Folder dialog box appears.
4. The remaining steps are same as that of adding a folder.

Deleting a folder

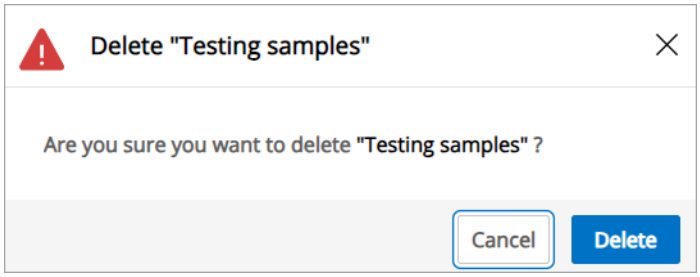
To Delete a Folder:

If a parent folder is deleted, then all its sub-folders are also deleted.

1. From the Repository screen:
   a. Click on **More Actions** button against the folder that you want to delete.
   b. Select **Delete**.



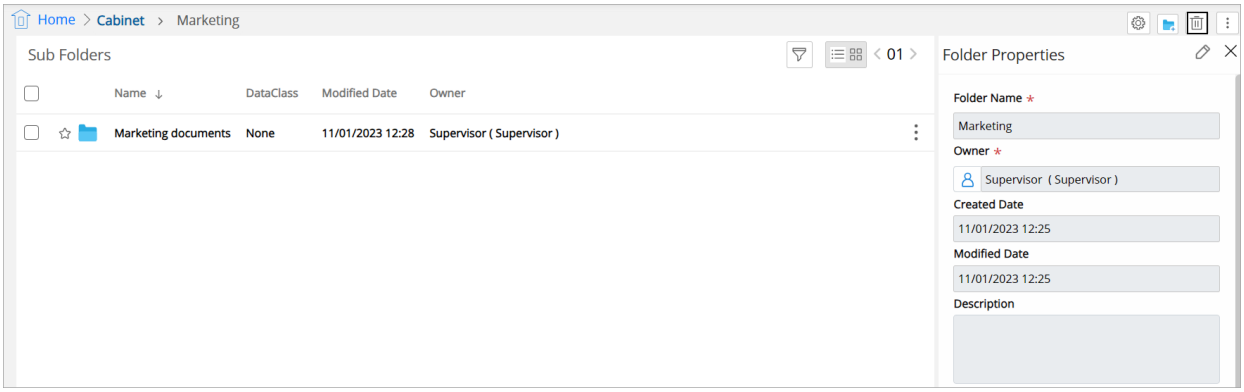
   c. Delete folder dialog box appears to confirm the deletion.



   d. Click on **Delete** to delete the selected folder.
   e. On confirmation, a message “Folder(s) deleted successfully” appears.

To delete a sub-folder, just open the parent folder and follow the above steps.

2. From the folder information screen:
   a. Open the folder that you want to delete.
   b. Click **Delete** icon displayed at the top-right corner of the screen.



c. Delete folder dialog box appears to confirm the deletion.
d. Click on **Delete** to delete the folder.
e. On confirmation, a message “Folder(s) deleted successfully”.

3. To delete multiple folders simultaneously:
   a. Click on **Select All** checkbox to select all the folders of the batch or select only those folders that you want to delete.
   b. On selecting two or more folders, Delete option appears.

   Click Items Selected icon to remove the selection of all the selected folders simultaneously.

   c. Click on **Delete**.
   d. Delete Folder dialog box appears to confirm the deletion.
   e. Click on **Delete** to delete the selected folder.
   f. On confirmation, a message “Folder(s) deleted successfully” appears. The deleted folders are removed from the list of folders and are moved to Trash.

Manage rights

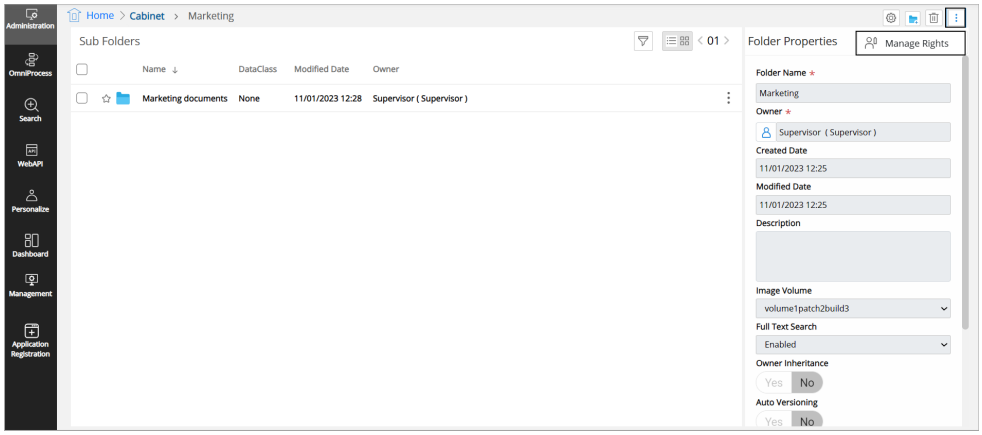
You can select the user(s) and/or group(s) to whom you want to give rights on any folder. Consequently, View Metadata, View Content, Modify Metadata, Modify Content, Annotate, Delete, Print, Copy and View Secured Data rights can be assigned to them.

There are three types of sharing:

Types	Description
Mark as Private	If you make any folder as Private, then no other members of your Cabinet would be able to access this folder.
Inherited	If you make a folder as Inherited, then the user(s)/group(s) would inherit the rights on this folder from its parent folder.
Share	Different types of rights like View Metadata, View Content, Modify Metadata, Modify Content, etc. can be assigned to the users using this option.

Manage Rights of Folder/Sub-Folder:

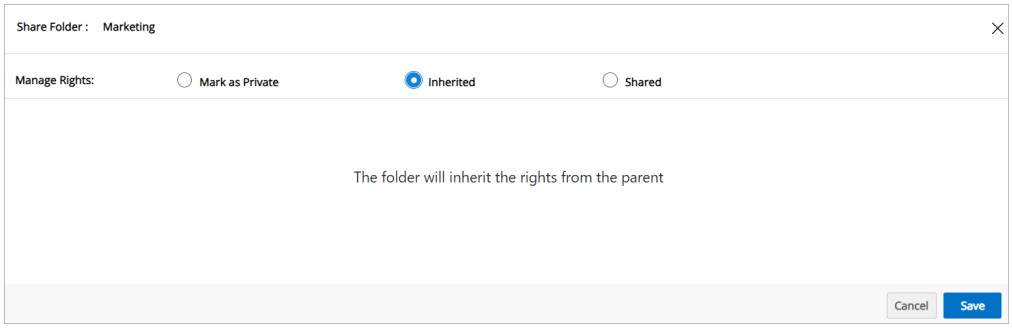
1. Go to **Repository** screen (for parent folder) or go to the folder information screen of the required parent folder (for sub-folder).
2. Click on **More Actions** against the folder/subfolder.
3. Click on **Manage Rights**. A dialog box to manage rights on the folder appears.



4. Select the required option. Depending on the requirement, select any one of the following:
   - **Mark as Private:** The folder will be visible only to the owner or the supervisor.
   - **Inherited:** The folder will inherit the rights of the parent.
   - **Share:** Refer to the below table:

Fields	Description
View MetaData	It is used to give rights to users to view the metadata. With this right, the user will be able to see the list of folders and their metadata.
View Content	It is used to give rights to users to view the document content.

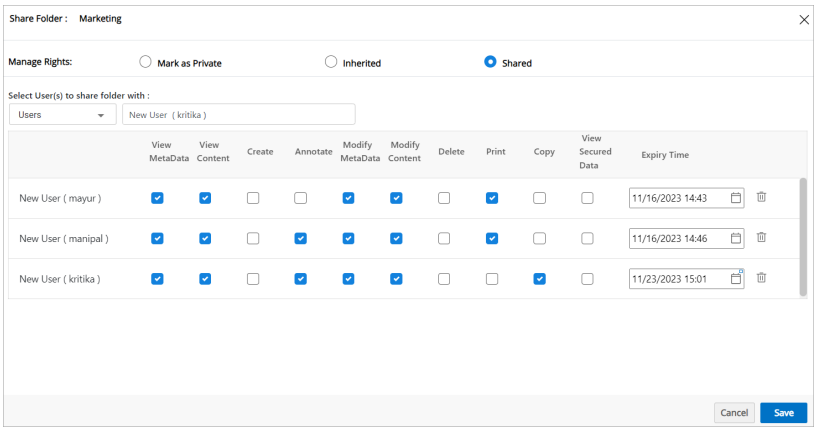
Fields	Description
Create	It provides the rights to add new documents and folders.
Annotate	It is used to give rights to users to apply annotations and notes on the documents. In case annotations are to be applied on the documents then View Content, Modify Content and Annotate Rights are required.
Modify MetaData	It is used to give rights to users to modify the metadata tagged with the documents/folders. The users can modify the metadata only if they have View Metadata and Modify Metadata rights.
Modify Content	It is used to give rights to users to modify the document content. The Check-in and checkout features will work only if this right is provided. If Modify Content rights are provided, then Modify Metadata rights are automatically assigned.
Delete	It is used to give rights to users to delete documents/ folders.
Print	It is used to give rights to users to print documents.
Copy	It is used to give rights to users to copy documents/ folders.
View Secured Data	It is used to give rights to users to view the data fields that are marked secured. Minimum view metadata and view secured data are required to view the secured data. This option will appear here if the Data Security feature is enabled on the cabinet.
Expiry Time	It is used to set expiry of the assigned rights. Click on the calendar icon and select the date and time to set the expiry.



5. To make the folder as Private:
    a. Select **Mark as Private**.
    b. Click on **Save**.
    c. A message “Folder properties have been saved successfully” appears.
6. To make the folder as Inherited:
    a. Select **Inherited**.
    b. Click on **Save**.
    c. A message “Folder properties have been saved successfully” appears.
7. To make the folder as Shared:
    a. Select **Share**.
    b. Select **Groups** and/or **Users** to share the folder with.
8. Select or type the required group or user from the dropdown.
    a. You can also add Roles associated with the selected groups or users.

> The folder can be shared with multiple Groups/Users/Roles.

    b. Role dropdown will appear only for those Groups and Users who have roles assigned to them.
    c. As per the requirement, assign necessary rights to the selected Groups or Users or Roles.
    d. Click on (**Remove**) against the group/user/role to delete that group/user/role from the list.
    e. Click on **Save** to save the added groups/users/roles and rights assigned to them.



    f. A message “Folder properties have been saved successfully” appears.

To Manage Rights of a Folder/Sub-Folder from Folder Information Screen:

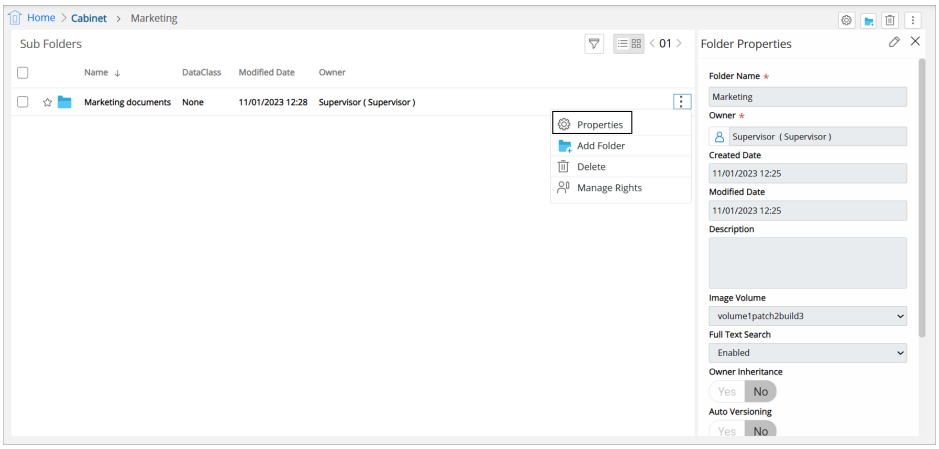
1. Click on the folder/sub-folder. The folder/sub-folder information screen appears.
2. Click on **Manage Rights** button.

3. A dialog box to manage rights on the folder appears.
4. Follow the step 4 specified for Manage Rights of Folder/Sub-Folder.

View folder properties

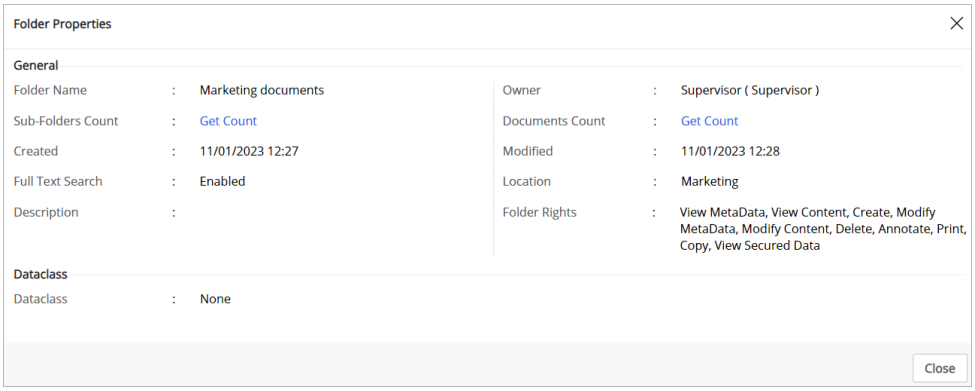
To View Folder Properties:

1. In the Repository screen:
   a. Click on **More Actions** button against the folder, the properties of which you want to view.
   b. Click on **Properties**.
2. From the folder information screen:
   a. Click on the Folder, the properties of which you want to view.
   b. The folder information screen appears.
   c. Click **Properties**.



3. Folder Properties dialog box displaying the properties of the selected folder appears.

To view the properties of a sub-folder, just open the parent folder and follow the above steps.



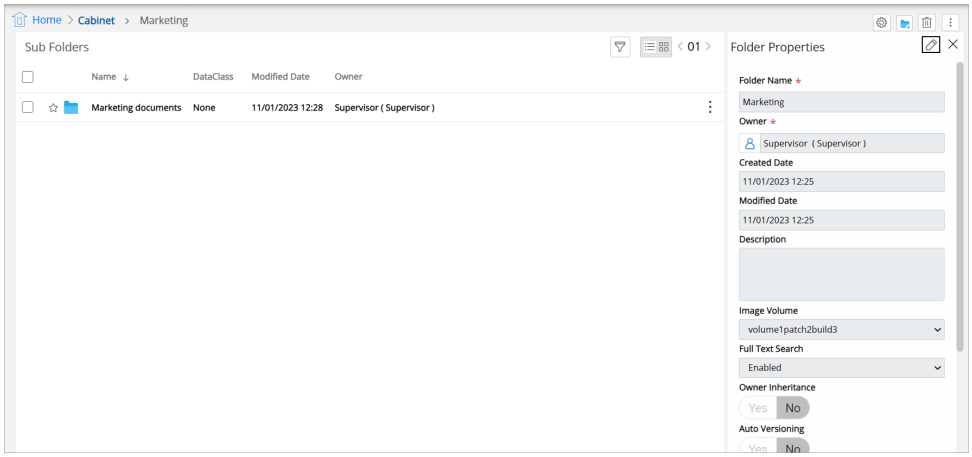
Modify folder properties

Folders are a manageable way to store documents. Folder properties dialog box allows you to view information such as name, owner, number of documents and sub-folders, Data Class etc.

If you have rights to modify folder properties, then only you can change the folder name, owner, description, and other metadata.

Modify Folder/Sub-Folder Properties:

1. Open the folder, the properties of which you want to modify.
2. The folder information screen appears. The right pane shows the properties, and the left pane shows a list of sub-folders.
3. Click **Edit** icon.



4. The folder properties appear in edit mode. Modify the following properties as required:
    a. **Folder Name:** Name of the folder.
    b. **Owner:** Owner of the folder.
        i. Click in the Owner textbox. Select Owner dialog box appears.
        ii. Choose a new owner of the folder. Select from User, Group or Role as the new owner.

> - The name of the folder can only be changed by its Owner or the Supervisor or the user having the modify metadata rights on a particular folder.
> - By default, the owner of the newly created folder will be the one who created it.

    c. **If User is selected:**
        i. Select or type group name in the associated combo box.
        ii. Select or type user name in the associated combo box.

d. **If Group is selected:**
    i. Select or type group name in the associated combo box.
e. **If Role is selected:**
    i. Select or type group name in the associated combo box.
    ii. Select or type user name in the associated combo box.
f. Click on **Confirm** to save the selection.
g. Created Date and Modified Date cannot be modified.
h. **Description:** Specify the folder description as required.
i. Image Volume: Select an Image Volume from the Image Volume dropdown list.
j. **Full Text Search:** Select Enabled or Disabled. If it is enabled, users can perform a Full Text Search on the folder while searching for specific information.
k. **Owner Inheritance:** Select Yes or No. If it is set as Yes, then the folder can inherit properties, data and rights from its parent folder.
l. **Auto Versioning:** Select Yes or No. If it is set as Yes, then the system will automatically update the changes taking place in the folder.
m. **Lock:** Select Yes to lock the folder. If it is already locked, then click on No to unlock it.
n. **Locked By:** If the folder is locked, then it gives the name of the user who has locked it.
o. **DataClass:** Users can tag one of the dataclasses created in the system with the folder as a metadata to retrieve them. Dataclass will be available as per the rights available to the users.
    i. Select the desired data class from the dropdown list. Changing Data Class dialog box appears, displaying an alert message.
    ii. Read the message carefully and click on Confirm to validate your selection. You can click on Cancel to abort data class change.

        Changing Data Class will reset all data fields.

    iii. On confirmation, the data class fields appear for data entry.
    iv. Enter or modify (for existing data class) the data class fields as required.

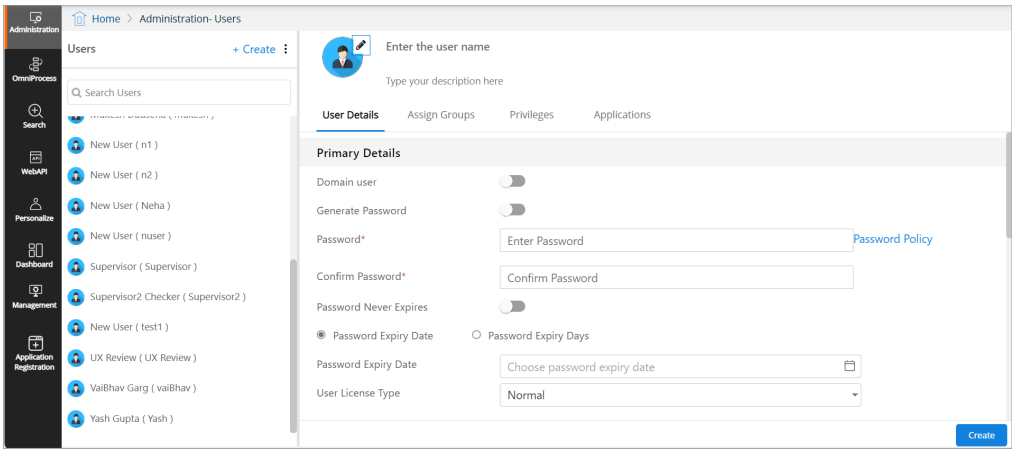
14. Click on **Save** to save the modified properties.
15. A message “Folder properties have been saved successfully” appears.

Working with users

This chapter includes creating a New User, Assigning Properties to a user, Assigning Groups to a user, Assigning Privileges to a user, Assigning Applications to a User, and Deleting a user.

To Access Users:

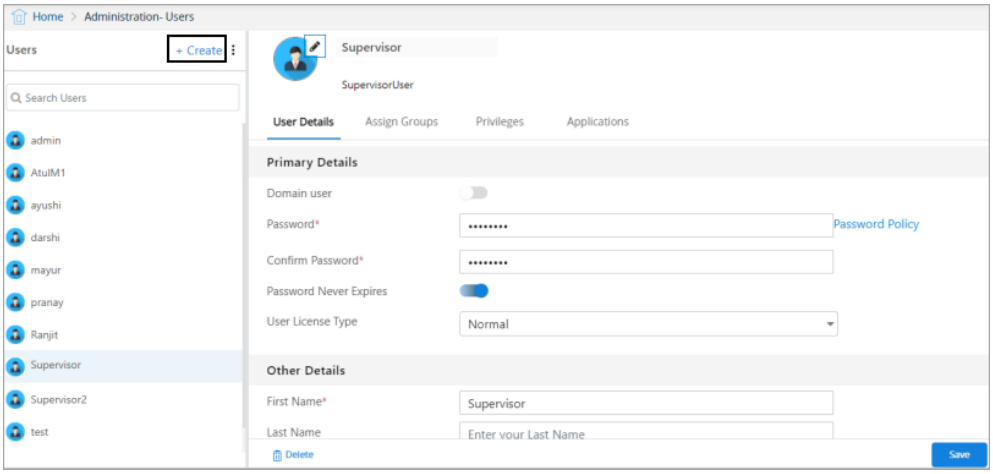
1. In the home screen of OmniDocs Admin, go to **Administration** tile and click on the **Users** link.
   Users screen appears. The left pane shows a list of existing users and the right pane shows the properties of the selected user.



Creating a new user

To Create a New User:

1. Click the Create link in the left pane. The Create link is enabled if you are viewing details of an existing user and disabled when you already on the user creation screen.
2. User Information screen appears with four primary tabs:
   a. User Details
   b. Assign Groups
   c. Privileges
   d. Applications



3. Enter the Primary Details as described below:
   - Domain User: If enabled, a domain user can login to the cabinet using his domain username and password.
   - Generate Password: If enabled, a password for the new user is generated by the OmniDocs.
   - Password and Confirm Password: Enter the password of the new user. Re-enter the password in the Confirm Password. These fields are disabled if the Generate Password is enabled.
   - Password Never Expires: Enable this field if you do not want the user password to expire. When you enable it, the Password Expiry Date and Password Expiry Days options get removed.
   - Password Expiry: The password expiry can be set either based on date or in number of days. Select either of the following options:
     - Password Expiry Date: Select the Password Expiry Date option to set password expiry based on the date.
     - Password Expiry Days: Select the Password Expiry Days option to set password expiry based on the number of days.
4. Select User License Type for the new user. The different license types are:
   - Normal User: These users can login into the system if the total logged in users are less than the maximum allowed users.
   - Fixed Type User: Fixed user will always be able to login. They are the most important users and always have login rights irrespective of any license.
   - S Type User: Can be used for external application login, A S-Type user can have multiple (concurrent) logged in sessions at the same time. For example: If there are a total of 100 S-type licenses in the system then an S-type user can login from 100 machines at the same time.
   - Internal Portal Users: Internal Portal User license works on ratio concept, for example, it's been considered that all users will not login on to a system at the

same time so If a total of 10 login sessions is allowed for the internal portal user then a maximum of 100 users can be created because only 10 users will login at one time conceptually.

- External Portal Users: Same as Internal Portal Users only ratio is different.

5. User Account Details are used to Lock the Account of the user, Add Expiry Date of the Account, or specify the Parent Group of the user.
6. Immediate Superior is used to assign and Immediate Superior of the user.
7. To create the user, click on Create.
8. The name of the new user is displayed on the list of Users in the left pane.

> The Administration module doesn't allow you to create users exceeding the number of licenses purchased. A message appears that more users cannot be created, as there are specified numbers of user licenses.

Assigning properties to a user

To Assign or Modify the Properties of a User:

1. Click a specific user from the Users list.
2. Enter or Modify the user information in the text boxes as described below:
   a. Type a password for the user in the **Password** text box.

      > Input to the Password text field is mandatory.

   b. Type the **password** again in the **Confirm Password** text box to verify that the data typed in the Password and Confirm Password text fields are the same.
   c. Check or uncheck if the password can be expired or not.

      > If Password Never Expires is set, then an administrator cannot set Password Expiry Date.

   d. Type the first name and last name of the user in the **First Name** and **Last Name** text boxes respectively (Advanced properties).

      > Input to the Last Name text fields is optional.

   e. Type the e-mail address of the new user in the **E-mail ID** text box.

      > Input to the E-mail ID text field is optional.

   f. Type the fax number of the new user in the **Fax Number** text box.

      > The Fax Number is optional.

g. Specify an expiry date for the user, in the **Expiry Date** text box.
h. Select the **User Active** option for enabling the access rights assigned to the User.

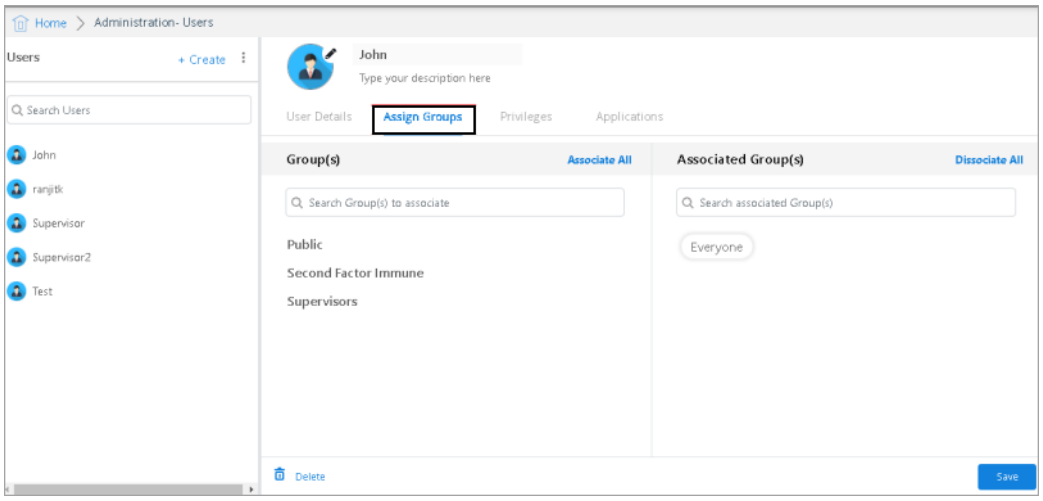
> By default, User Active option remains selected, you can clear the option to deny access to the User.

i. Select the parent group from the **Parent Group** box.
j. Select the **Immediate Superior**. This can be one of the following:
   - Role of a particular Group.
   - Any User.
   - No Superior option.
k. Type a relevant comment for the new user in the **Description** box.
l. Click on **Save** button to save the changes.

Assigning groups to a user

To Assign Groups to a New User:

1. Click the **user** from the Users list.
2. Click on the **Assign Groups** tab.

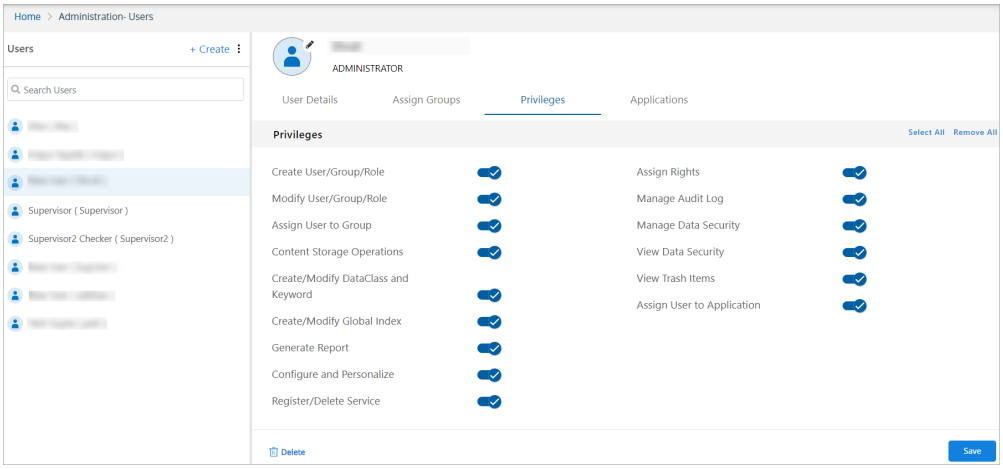


3. To assign a user to the group:
   - Click on a group from the **Group(s)** List to add it to the **Associated Group(s)** list.
   - If you want to add all the groups, then click on **Associate All**.
4. To remove a group from the Associated Group:
   - Click on the **X** button against the group to remove it from the **Selected Group(s)** list.
5. Click on **Save** to save the changes made to the user properties.

Assigning privileges to a user

To Assign Privileges to a New User:

1. Click the **user** from the Users list.
2. Click on the **Privileges** tab.



3. The following privileges options appear to enable or disable, allowing you to assign them to the user:

Privilege	Description
Create User/Group/Role	Allows the user to create new users, groups, or roles within the system.
Modify User/Group/Role	Allows the user to modify the properties of existing users, groups, or roles.
Assign User to Group	Allows the user to assign a user to a specific group within the system.
Content Storage Operations	Allows the user to manage operations related to Sites, Volume, and Storage Transition Manager.
Create/Modify DataClass and Keyword	Allows the user to create and modify DataClasses and keywords.
Create/Modify Global Index	Allows the user to create or modify global indexes.
Generate Report	Allows the user to generate system reports.

Privilege	Description
Configure and Personalize	Allows the user to manage components like Omniprocess, Search, Dashboard, WebAPI, and the components present in the Personalize tile, such as Landing Page Configuration, Repository View, Document Upload Templates, and many more, to personalize system settings.
Register/Delete Service	Allows the user to register and delete services within the system.
Assign Rights	Allows the user to assign specific rights and permissions to others.
Manage Audit Log	Allows the user to manage system audit logs.
Manage Data Security	Allows the user to manage data security.
View Data Security	Allows the user to view, but not modify, data security settings.
View Trash Items	Allows the user to view and take action on items in the system's trash.
Assign User to Application	Allows the user to assign other users to specific applications within the system.

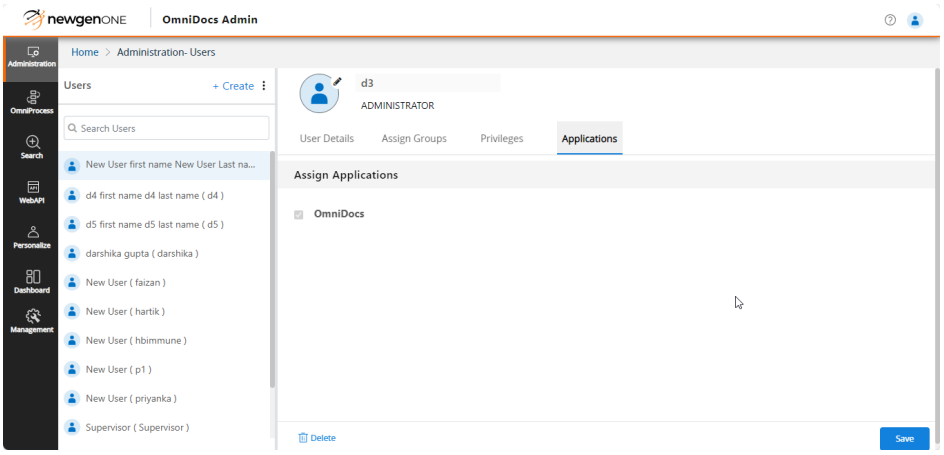
4. Click on **Save** to save the changes made to the user properties.

> Manage Data Security and View Data Security privileges will not appear in case Data Security Functionality is not enabled.

Assigning applications to a user

To Associate/Disassociate a User from Applications:

1. Click the user from the Users list.
2. Click **Applications** tab.

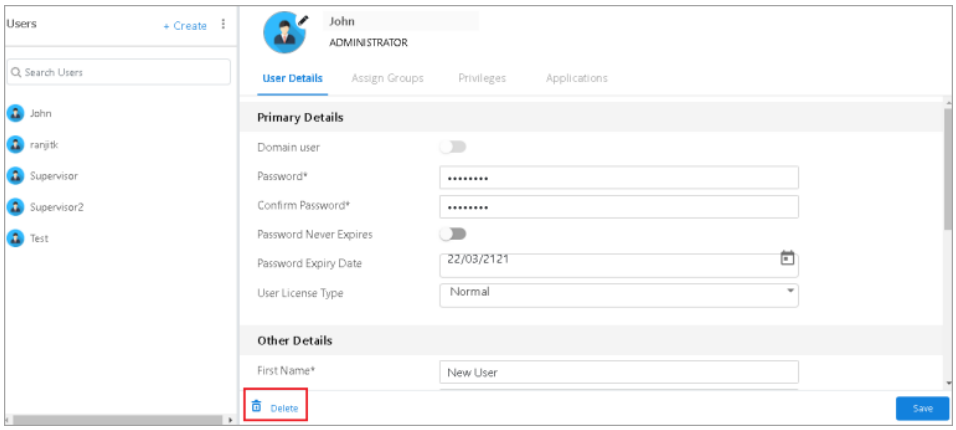


3. Select the required application to assign it to the user or clear the checkbox to remove it from the assigned application.
4. Click **Save** to save the changes made to the user properties.

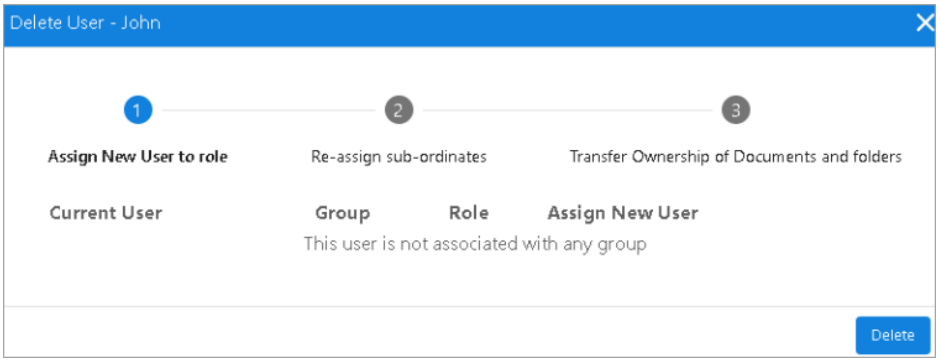
Deleting a user

To Delete a User: an owner can be any existing user/ group or role.

1. Click the user from the Users list.
2. Click on the **Delete**.



3. Delete User screen appears.



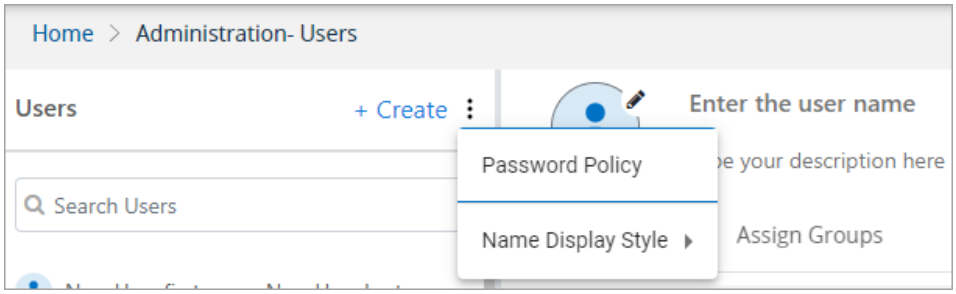
4. Before deleting a user, the administrator can transfer the ownership of documents and folders to some other existing users. Follow the below steps to transfer ownership:
    a. Go to the scheduler located at the below path and open *SchedulerConf.ini* file:
    <OmniDocs install drive>\Common Services for J2EE\Scheduler\conf
    b. Enter the **schedulerIpAddress** and save the file.
    c. Now, go to the **Service Management** and register a **Service Type**. For details refer to the Service management section.
    d. Go to <OmniDocs install drive>\Common Services for J2EE\Scheduler and run the *Scheduler.bat* file.
    e. Once the scheduled time is reached, the Status of the service registered in the Service Management for the transfer of the ownership gets changed from new to completed.
5. Click on **Delete** to delete the user.
6. The user is now deleted, and the transfer of ownership takes place.

Password policy

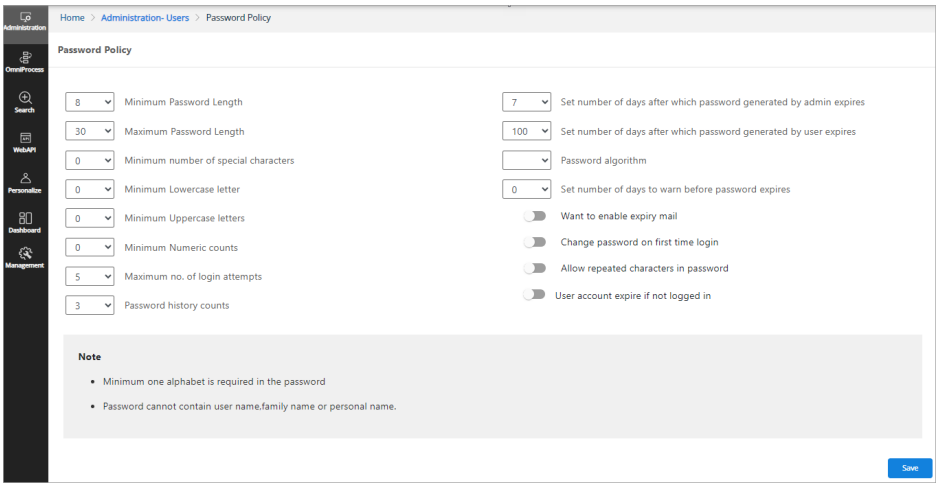
This feature provides the facility to protect passwords in a better way. Users can protect the passwords in many ways using various options provided in the Password Policy Manager.

To Manage Password Policy:

1. In the **Users** section, click on the ellipsis next to Create User link.
2. Click on **Password Policy**.



3. Password Policy screen appears.



4. Password Policy screen displays the various parameters on which a user can set the password, they are as follows:
    a. Minimum Password Length
        - The minimum number of characters can be set for the password.
        - The user needs to enter a password equal to or greater than this length.
        - The password length can be set by administrator members only.
    b. Minimum Number of Special Characters
        - A minimum number of special characters that the user must use while entering the password is configurable.
        - This operation can be done by admin members only.
    c. Maximum Number of Login Attempts
        - The number of attempts that can be made by the user for successful login is configurable.
        - Once that count reaches user gets locked.
        - This login attempt count can be set by administrator members only.
    d. Password History Count
        - It is configurable that how many previous passwords users cannot use while setting the new password.
        - This operation can be done by administrator members only.

e. Change Password on First-time Login
   - Once this flag is set as true, then for all users whose password is system generated or generated by administrator it is mandatory to change the password whenever a user logs in.
   - A user would not be able to login into OmniDocs unless a user changes his password.

f. No. of days after which password generated by the administrator will expire
   - It is used to define the number of days after which the password generated by the Administrator will expire. Selecting 0 (Zero) means the password will never expire. If this value is set to a value other than 0, then the new Password Expiry Time will set to Current Date + Number of Days.

g. No. of days after which password generated by a user will expire
   - It is used to define the number of days after which the password generated by the user himself will expire. Selecting 0 (Zero) means the password will never expire. If this value is set to a value other than 0, then the new Password Expiry Time will set to Current Date + Number of Days.

h. No. of days before password expiry to warn.
   This will set the number of days to give a warning to the user before the password expires. For example, a user is created on 1st September and is given a password expiry time of 30 days. Now if the value of the "No. of days before password expiry to warn" option is set as 5 days, the user will start getting alert after 25th Sep that your password will expire in so many days. Also, if the "enable expiry mail" checkbox is set as true, user will get a mail after password expiry.

i. Allow Repeated Characters in Password
   - This allows the use of repeated characters while creating a new password.

j. No. of days after which user account expires if the user does not log in to the system
   - It is the maximum number of days, after which the account expires if it is not used to log in to the system.

k. Lower Case Character Count
   - This sets the minimum number of Lower Case Character that should be present in the password.

l. Upper Case Character Count

- This sets the minimum number of Upper Case characters that should be present in the password.

m. Minimum Numeric Count

- This sets the minimum number of Numeric Case Character that should be present in the password.

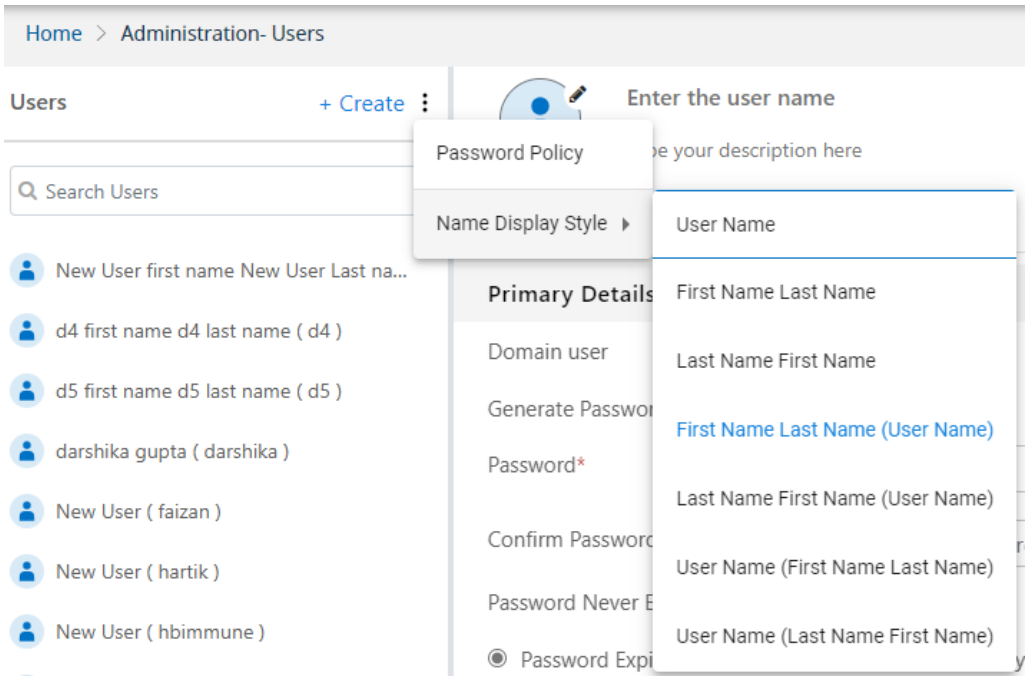
5. Select the values from the list and click **Save** to set the parameters. A summary of the selected password policy values appears.
6. Click on the **Save** button.
7. If no changes are required, then click on the **Cancel** button.

Name display style

It allows users to change the display style of username shown in the entire cabinet. The changes done here will affect the login panel of the user.

To change Name Display Style:

1. In the **Users** section, click on the ellipsis next to Create User link.
2. Click on **Name Display Style**.



3. Following styles are available:
   a. Username
   b. First name Last name
   c. Last name First name

d. First name Last name (Username)
e. Last name First name (Username)
f. Username (First name Last name)
g. Username (Last name First name)

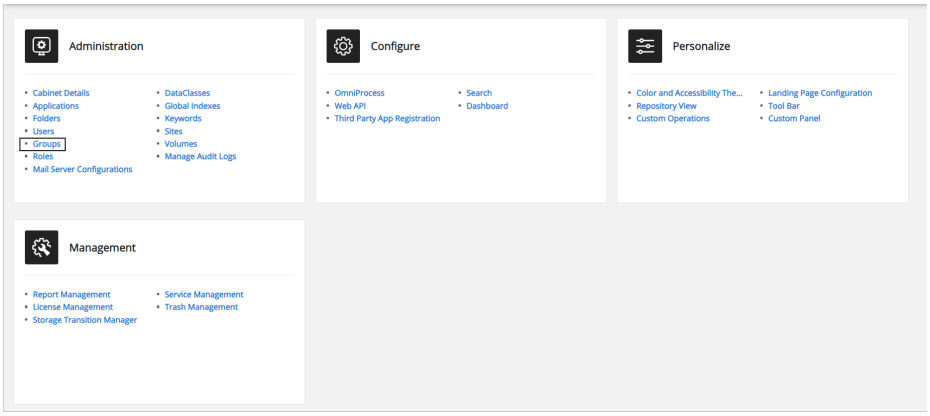
4. The selected style will be shown wherever the user name will be displayed.

Working with groups

This section includes group functions such as creating a group, Assigning Properties to a group, Assigning Users to a group, Assigning Privileges to a group, and Assigning Roles to users of a group.

To Access Groups:

1. In the home screen of OmniDocs Admin, go to **Administration** tile and click on the **Groups** link.



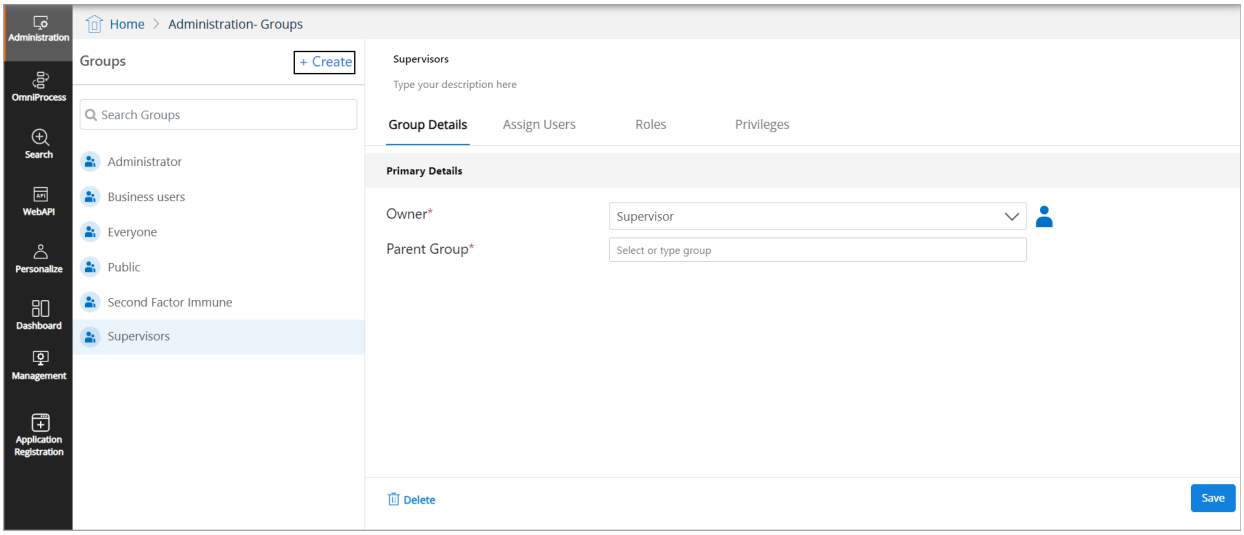
2. Groups screen appears. The left pane shows a list of existing groups and the right pane shows the properties of the selected group.

Creating a group

To Create a Group, perform the below steps:

1. Click the **Create** link in the left pane.
2. Group Information screen appears with four primary tabs:
   a. Group Details
   b. Assign Users

c. Roles
d. Privileges

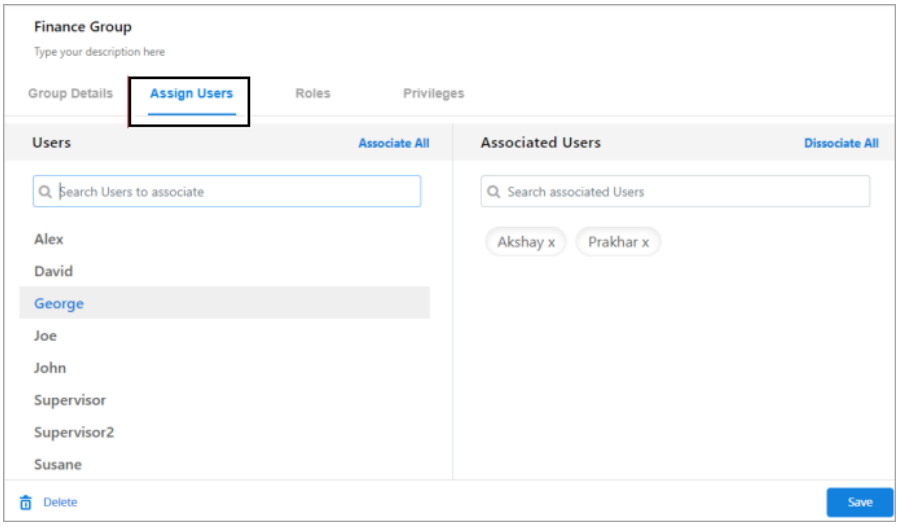


3. The list of groups in batches is shown in the left pane and the description of the group in the right pane.
4. Click on the **+Create** link given in the left pane.
5. Type the data in the text boxes as per the requirement in the right pane.
6. Enter the Group Name and Description.
7. You may modify the Owner by selecting from the **Owner list** box.
8. To select Owner, click on the drop-down option.
9. From this dialog box, assign ownership to the required **User/Group/Role**.
10. Once the ownership is assigned, you need to add the group type.
11. You may modify the Parent Group by selecting from the **Parent Group** list box.
12. Click the **Add** button to add the group to the list of Groups shown in the left pane of the Group Information screen.

Assigning users to a group

To Assign Users to the New Group:

1. Open Group information screen.
2. Click on the **Assign Users** tab on the right pane of the screen.



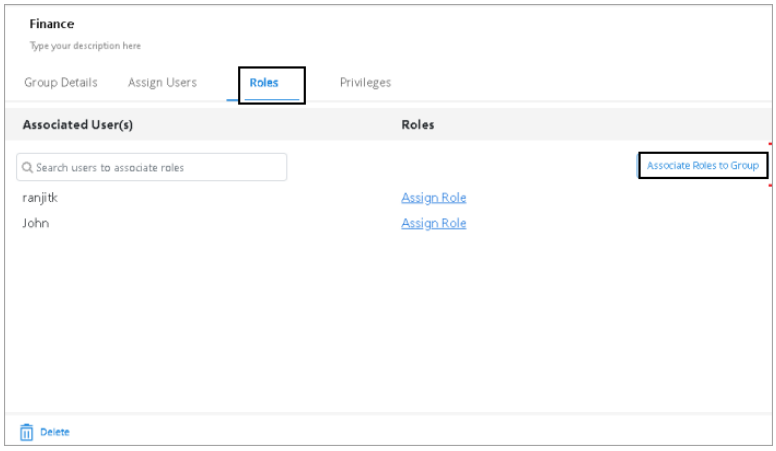
- **Users List:** It displays the list of all the users that are present in the cabinet.
- **Associated User(s) List:** It displays all the users who are added to the group.

3. To add a user to the group:-
   - Click on the user from the **Users** list.
   - If you want to add a particular user to all the groups then click on (**Associate All**) or vice versa.
4. To remove a user from the group:-
   - Click on the X button to delete a user from the **Associated User(s)** list or.
5. Click on the **Save** button to save the changes.

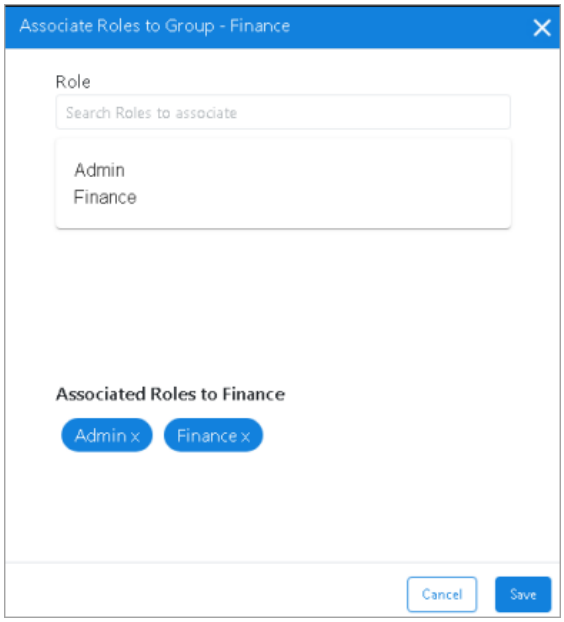
Assigning roles to users of a group

To Associate Roles to a Group:

1. Click on the required group to open its properties.
2. Click on the **Roles** tab.
3. Click **Associate Roles to Group** link.

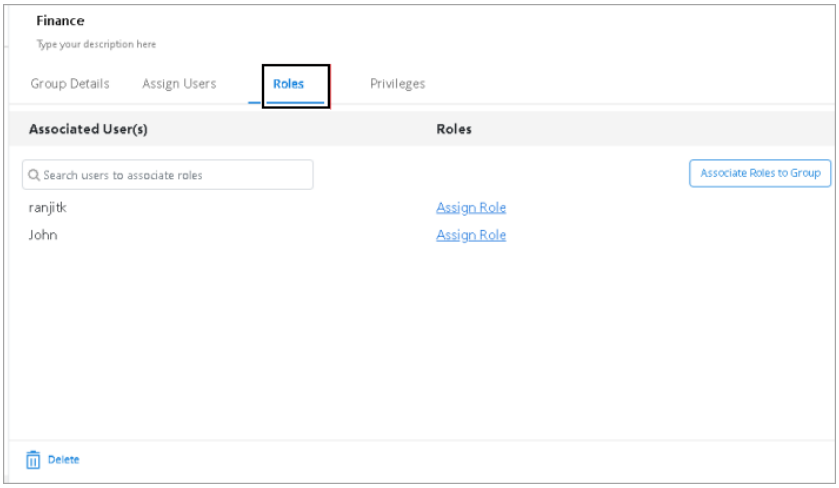


4. Associate Roles to Group dialog box appears.
5. Select a role from the list of **Roles**.
6. The selected roles appear in the **Associated Roles to <selected group name>** section.
7. Click **Save**. A message “Properties modified successfully” appears.

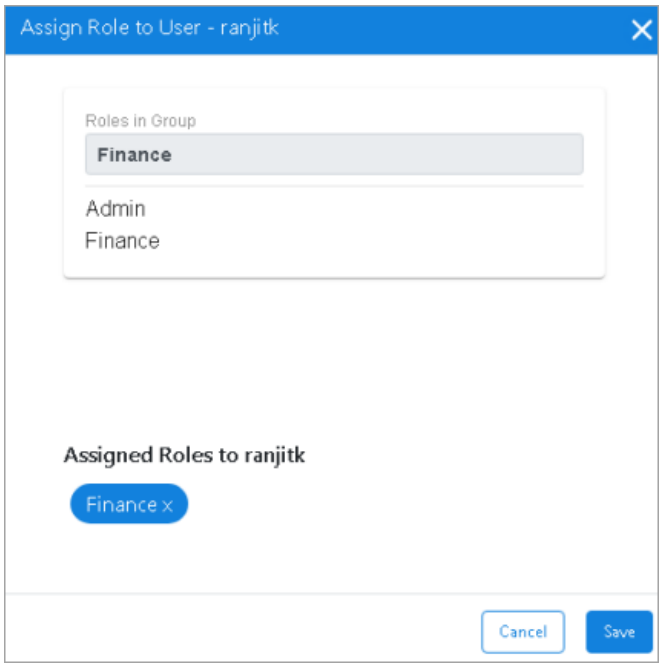


To Assign Roles to Users of a Group:

1. Click on the required group to open its properties.
2. Click on the **Roles** tab.



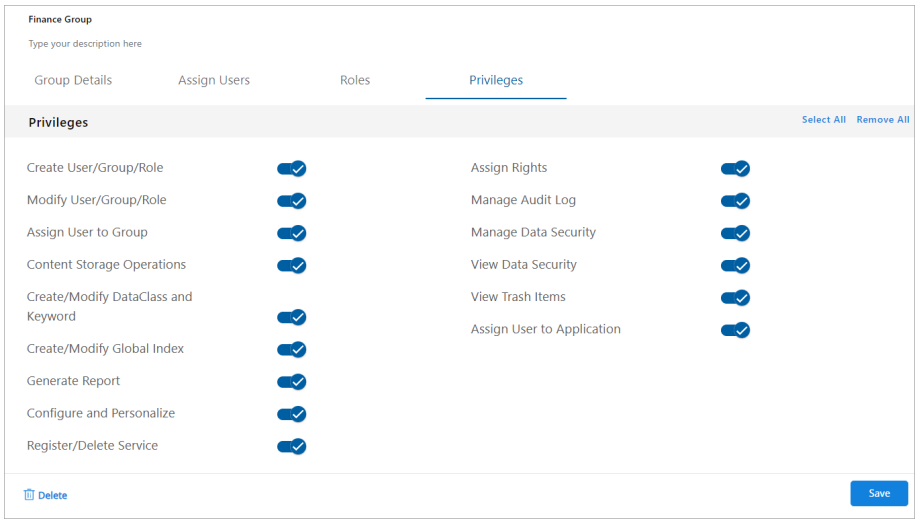
3. Click on the **Assign Role** link against the required user. Assign Role to User dialog box appears.
4. Select a role from the list of **Roles in Group** list.
5. Click **Save**. A message “Properties modified successfully” appears.



Assigning privileges to a group

You can assign privileges to the group as well. These privileges are applicable to all the users in that group.

1. Open Group information screen.
2. Select a **group**.
3. Click on the **Privileges** tab on the right pane of the screen.



4. Select the options from the privileges list to assign privileges to the Group.
5. Click on **Save** to save the changes made.

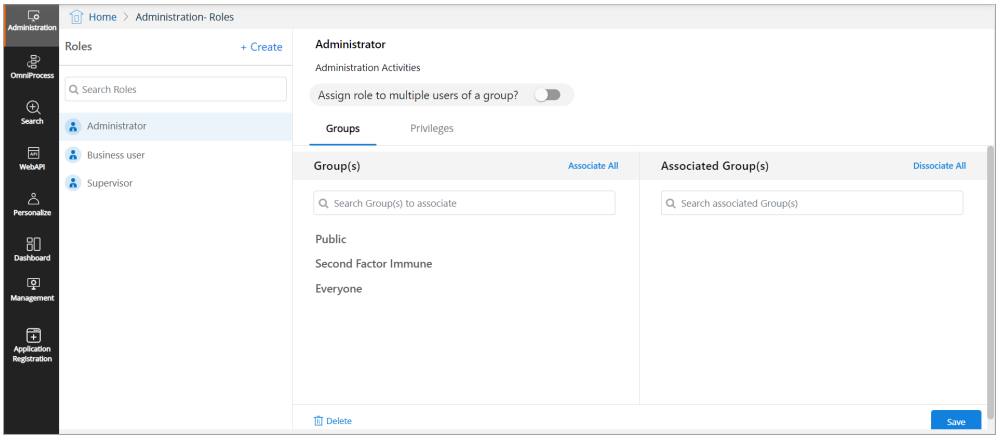
> Manage Data Security and View Data Security privileges will not appear in case Data Security Functionality is not enabled.

Working with roles

A role is a logical entity. It represents the action to be performed by a particular user. The roles can be assigned to many users of the same group as well.

To Access Roles, perform the below steps:

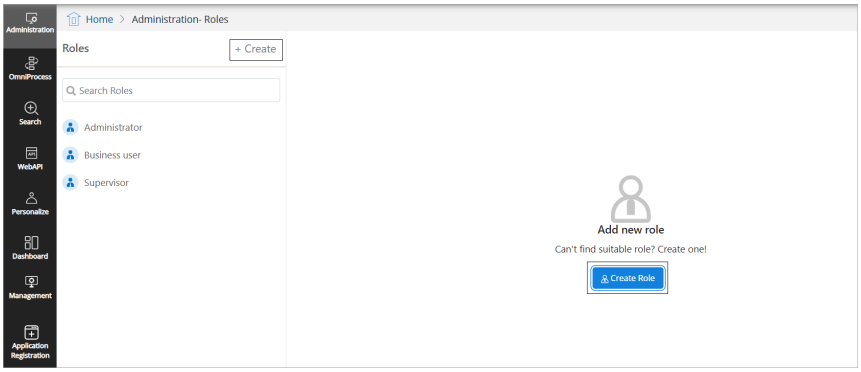
1. In the home screen of OmniDocs Admin, go to **Administration** tile and click **Roles** link.
2. Roles screen appears. The left pane shows a list of existing roles and the right pane shows the properties of the selected role.



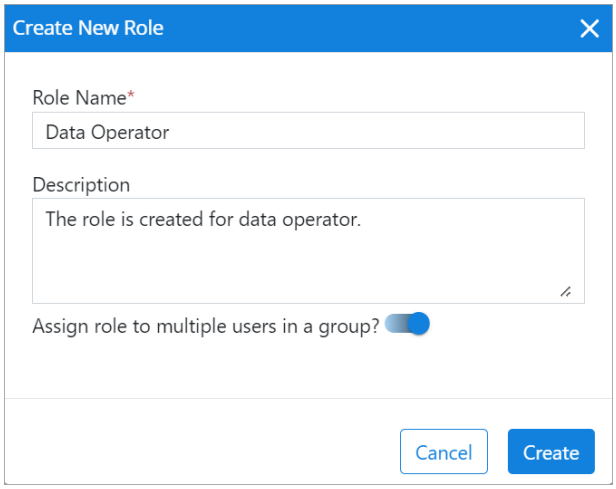
Creating a role

To Create a Role, perform the below steps:

1. Go to **Roles**.
2. Click **Create Role** link. A list of existing roles appears in the left pane of the screen.



3. Clicking on any of the roles shows their properties in the right pane.
4. Click **+ Create** link in the left pane. The Create New Role screen appears.

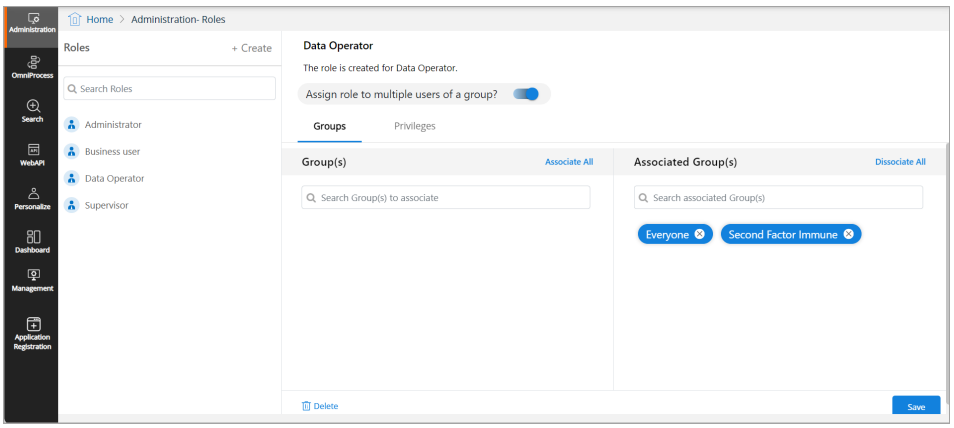


5. Type the name of the role in the Role Name text box.
6. Type the description of the role in the Role Description text box.
7. Select Assign role to multiple users in a group option if you need to assign the role to multiple users.
8. Click **Create** to create the role. A message “Role added successfully” appears.

Associating groups with a role

To Associate Groups with a Role:

1. Select the role from the Role list. The properties of the selected role are displayed in the right pane.
2. Click on the **Groups** tab. If any group is already associated with the role, it will appear in the Associated Group(s) list.
3. Select the group name from the **Group List** and add it to the **Associated Group(s)** list.
   - Click on the **Associate All** link to add all the groups in the associated group(s) list.
4. To remove a group from the Associated Groups(s), just click on the X button against the group to be removed.
   - Click on the **Dissociate All** link to remove all the groups from the Associated Groups(s).
5. Click on **Save** to save the changes made.



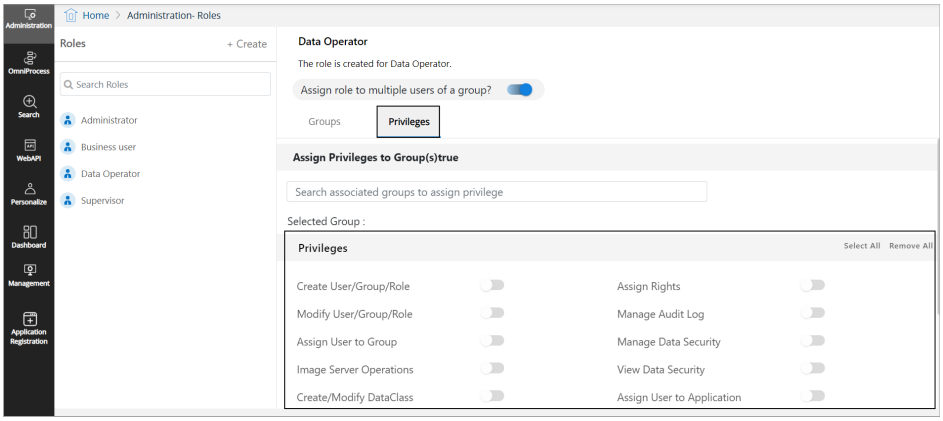
6. A message “Role modified successfully” appears.

Assigning privileges to a role

This feature is used to assign privileges to a role. A role must be associated with a group before privileges are provided to it.

To Assign Privileges to a Role:

1. Select the role from the Role list. The properties of the selected role are displayed in the right pane.
2. Click on the **Privileges** tab.
3. Click on **Search associated groups to assign privilege** and select a group.
4. Select the listed privileges to be assigned to the role. Or unselect the assigned privileges to remove the privileges.
5. Click on **Save** to save your selections.



6. A message “Role modified successfully” appears.

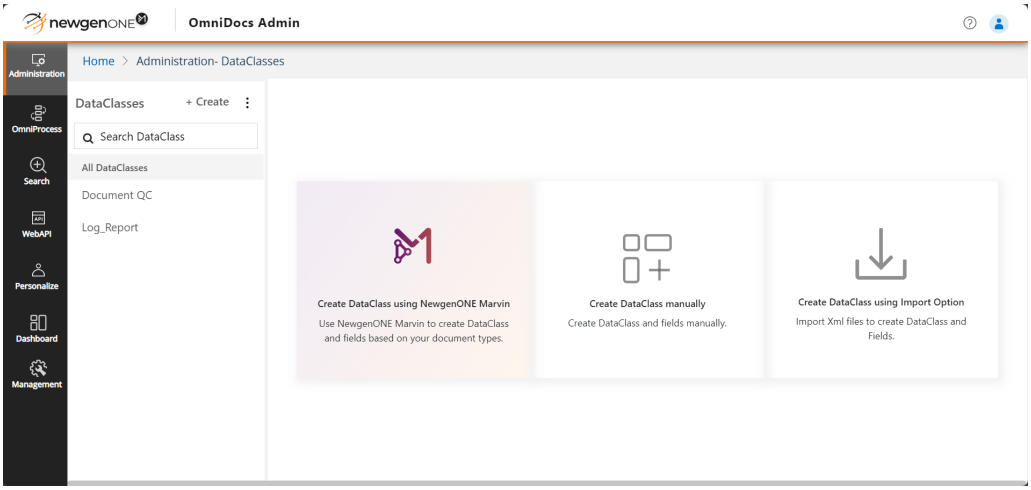
DataClasses

DataClass 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 DataClasses:

1. In the home screen of OmniDocs Admin, go to the **Administration** tile and click the **DataClasses**.
2. The Dataclasses screen appears with the following options:
    - Create DataClass using NewgenONE Marvin

- Create DataClass manually
- Create DataClass using Import Option



Creating DataClass usingNewgenONE Marvin

This feature allows you to easily create DataClasses using pre-defined categories and data fields provided by NewgenONE Marvin. To access data classes, in the OmniDocs Admin home screen, navigate to the Administration tile and click **DataClasses**.

To create a data class using NewgenONE Marvin, perform the following steps:

1. On the DataClasses screen, choose the option **Create DataClass using NewgenONE Marvin**.
   A list of predefined data class categories relevant to your business appears, such as loan agreements, account statements, KYC documents, and others.
2. Select the checkboxes against the required categories.
   You can choose all categories with a single click by selecting the **Following are the document types recommended for your line of Business (Banking)** checkbox.
3. Click the **Generate** button. The fields relevant to the selected categories appear to specify the details.
   The right pane comprises the following options:

Field	Description
DataClass	Allows you to enter the name of the dataclass.

Field	Description
Field Name	Displays you the field name.
Field Type	Displays you the field type.
Validation Type	Shows you to the validation type. It does not allow custom validations for data fields.
Drag and drop	Allows you to change the sequence of the fields.
Edit	Allows you to change the field type and validation type values.
Generate More Fields Button	Enables you to add extra fields to DataClass as suggested by NewgenONE Marvin.

4. Select the checkbox against the required field.
5. Click the **Create** button to finalize the DataClass.

For further steps, refer to the Common DataClass Configuration.

Importing DataClass

This option allows you to import DataClasses defined in an *XML* file.

To import data classes, perform the following steps:

1. On the DataClasses screen, choose the option **Create DataClass using Import Option**. The import dialog appears with the browse option for importing the DataClass.
2. Drag and drop the *.xml* file into the dialog or click **Browse** to select the file from your system.
   Once the file is selected, a list of DataClasses defined within the file appears.
3. If your *.xml* file contains multiple DataClasses, select the specific DataClass you want to import by checking the checkbox next to it.
4. Click **Import** to proceed with importing the selected DataClass(es).

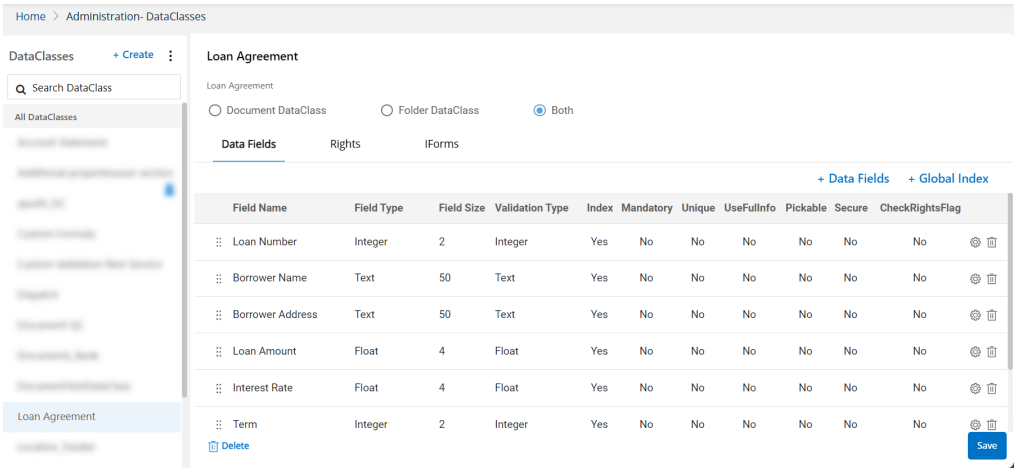
For further steps, refer to the Common DataClass Configuration.

Creating DataClass manually

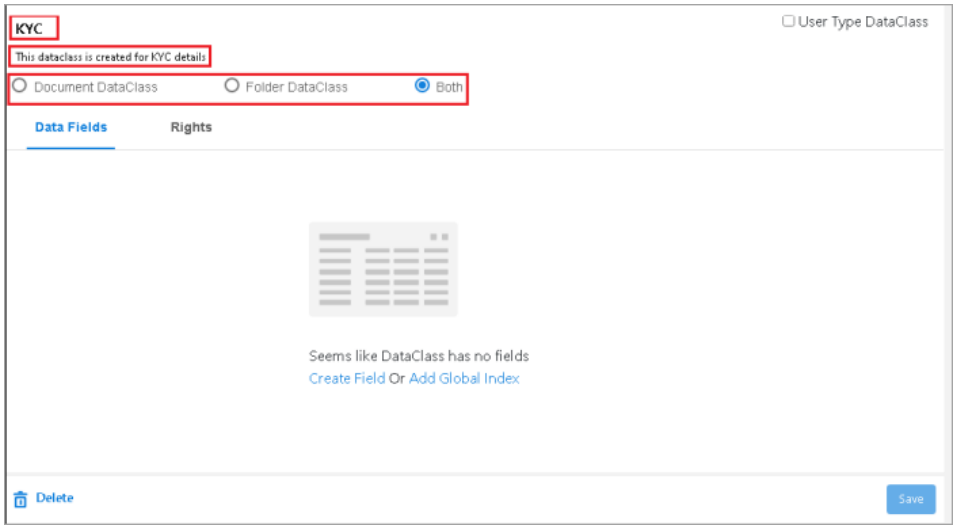
In the OmniDocs Admin, users have the option to manually create DataClasses. This method allows for custom configurations and tailored data organization within OmniDocs. To manually create DataClasses, navigate to the DataClasses section in the OmniDocs Admin portal and .

To Create a DataClass manually, perform the following steps:

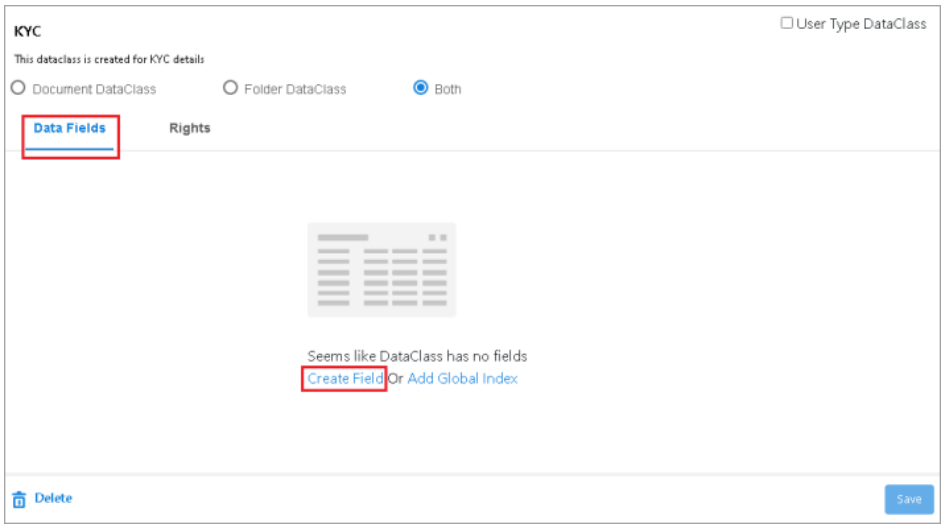
1. On the DataClasses screen, choose the option **Create DataClass manually**.



2. Enter a dataclass name in the **Name the DataClass here** textbox.
3. Enter a small description about the dataclass in the **Type your description here** textbox.
4. Select one of the following options:
   - **Document DataClass**: Select this option if you want to create a dataclass especially for documents.
   - **Folder DataClass**: Select this option if you want to create a dataclass especially for folders.
   - **Both**: Select this option if you want to create a dataclass that can be associated with both documents and folders.



5. To add dataclass fields using data field creation:
   a. Click on the **Data Fields** tab and then click on the **Create Field** link.

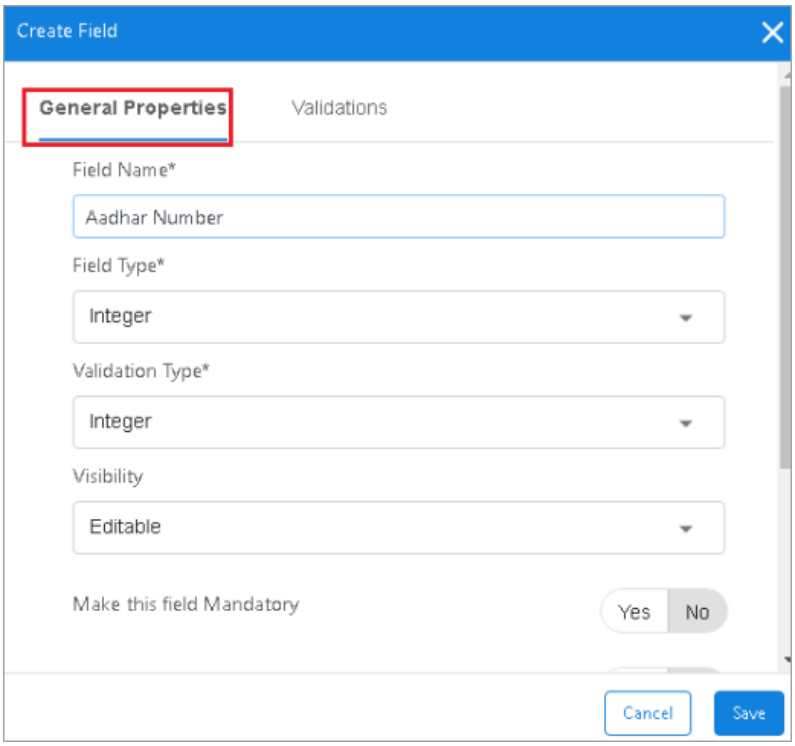


   b. Create Field dialog box appears.
   c. Specify **General Properties** as described below:

Fields	Description
Field Name	Enter the data field name.
Field Type	Select the required DataClass Type from the dropdown list. In the dropdown list, the following data types are available: • Integer • Long • Float • Text • Date & Time

Fields	Description
Validation Type	Select the required Validation Type from the dropdown list. The options in the Validation Type dropdown list depends on the selected Field Type. Refer to the section Validation Type for details.
Visibility	Select the required Visibility from the dropdown list. In the dropdown list, the following types of visibility are available: • Hidden: If this field is to be made hidden from the end-user. • Readonly: If this field is required to appear in read-only format to the end-user. • Editable: If this field is required to appear in editable format to the end-user.
Make this field Mandatory	Select Yes to make data entry of this field as mandatory. Select No if it is not mandatory to fill. To make the data entry to a field compulsory, the field can be defined as Mandatory. For example, if you are maintaining an Inventory list, the Item name and Item code can be made mandatory.
Enable Indexing	Select Yes to enable indexing on this field. Select No if indexing is not required.
Make this Field Secure	In case the Data Security Functionality is enabled, Make this Field Secure option appears for the Text Field Type. The Data Security feature can only be enabled at the time of Data Field creation. You cannot enable the Data Security feature in an already created Data Field. Select Yes to enable Field Security else select No.
Make this field Unique	Select Yes to make this field unique else select No. Only one field can be marked as unique. It means the value associated with this field cannot be duplicated.
Make this field Pickable	Select Yes to make any field Pickable so that field values can be chosen from a predefined list of values. As you mark this field as enabled, the DataClass gets saved and a new tab “Picklist” gets added for the pickable field being added. Refer to the section Set Picklist Values to add pickable values.

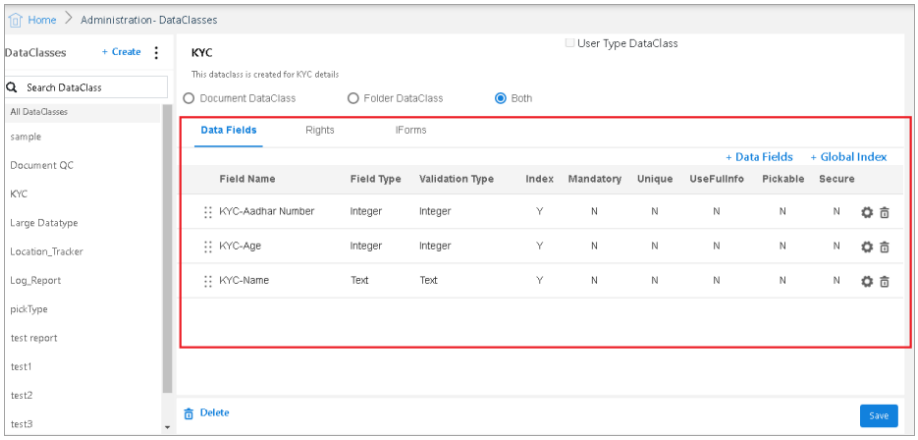
Fields	Description
Useful Information	Select Yes for displaying the field values of a particular dataclass in the column section of the repository or search else select No.



6. Set the **Validations** as required. The Validation fields depend on the selected Validation Type. Refer to the section Validations Tab for details. The below screenshot is of Validations when the Validation Type is an Integer.
7. Once all the field values are specified, click on **Save** to create the field.
8. A message “DataClass added successfully” appears.
9. Now, click on **Cancel** to close the Create Field dialog box or remain on this page to add more data fields.
10. To add dataclass fields using the **Global Index**:
    a. Click on the **Add Global Index** link.
    b. Add Global Index dialog box appears. It contains all the existing Global Indexes.

    The Global Index is defined separately.

    c. Select the required Global Indexes and click on **Confirm**.
    d. A message “DataClass added successfully” appears.
    e. Now, click on Cancel to close the Add Global Index dialog box and view the added data fields.



11. Click on the **Rights** tab to assign different rights to Users, Groups and Roles on a particular datacalss. Refer to the section Assigning Rights.
12. Click on **IForms** tab to map the DataClass fields with the IForm fields. Refer to the **iForm Builder** user manual to learn how to create forms using the iForm.

For further steps, refer to the Common DataClass Configuration.

Validation type

The options in the Validation Type dropdown list depend on the selected Field Type.

1. If the **Field Type** is selected as **Text**, then the following options are available for the **Validation Type**:

Validation Type	Description
Custom Regular Expression	Text (Only Alphabets)
Email ID	Text (Only Digits)
Text	URL
Text (Alpha-Numeric)	Custom Validation (Rest Service)
Text (Large Data): Using this field type, users can get the advantage of features of Froala Editor.	Custom Validation (Third Party JS)

2. If the **Field Type** is selected as **Integer**, then the following options are available for the **Validation Type**:

- Auto Sequence Generation
- Integer
- Custom Validation (Rest Service)
- Custom Validation (Third Party JS)

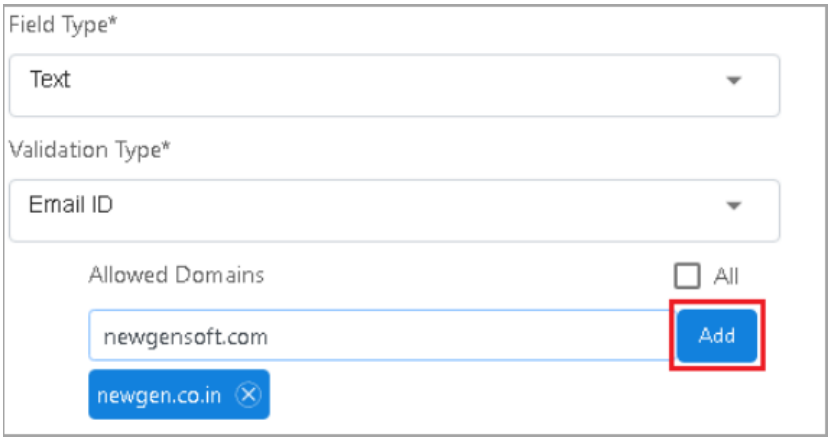
3. If the **Field Type** is selected as **Long**, then the following options are available for the **Validation Type**:
   - Long
   - Custom Validation (Rest Service)
   - Custom Validation (Third Party JS)
4. If the **Field Type** is selected as **Float**, then the following options are available for the **Validation Type**:
   - Currency
   - Float
   - Percentage
   - Custom Validation (Rest Service)
   - Custom Validation (Third Party JS)
5. If the **Field Type** is selected as **Date & Time**, then the following options are available for the **Validation Type**:
   - Date
   - Date Time
   - Custom Validation (Rest Service)
   - Custom Validation (Third Party JS)

Validation type-options

1. **Custom Regular Expression**: It appears when the Field Type is Text.
   If Validation Type is selected as **Custom Regular Expression**, then you are required to provide the following information:
   - Regular Expression: You can define custom regular expression for the validation of the data fields.
   - Example: The validation of the fields can be checked by entering the value in the example field.
   - Save these custom settings as a New Validation Type: If it is marked as enabled then a new textbox appears where you are required to enter a name for the **New Validation Type**. The next time you create a data field, this new validation type will be available for selection.

2. **Email ID:** It appears when the Field Type is Text.If Validation Type is selected as **Email ID**, then you are required to provide the following information:
    - Allowed Domains:
        1. Select the checkbox **All** to allow all the domains.

        2. Unselect the checkbox All to allow only the added domains and restrict the others. The Add textbox gets enabled on unselecting the All checkbox.
        3. Enter the domain name in the textbox and click on **Add**.



        4. To remove the added domain, click on the cross mark against the added domain.

3. **Custom Validation (Rest Service)**: It appears for Text, Integer, Long, Float and Date & Time Field Types.
   If Validation Type is selected as **Custom Validation (Rest Service)**, then you are required to provide the following information:
   - Save these custom settings as a New Validation Type: If it is marked as enabled then a new textbox appears where you are required to enter a name for the **New Validation Type**. The next time you create a data field, this new validation type will be available for selection.
   - Rest Service URL: You need to provide the URL of the Rest Service through which validation of the field types would be done.
4. **Custom Validation (Third Party JS):** It appears for Text, Integer, Long, Float and Date & Time Field Types.
   If Validation Type is selected as **Custom Validation (Third Party JS)**, then you are required to provide the following information:
   - Save these custom settings as a New Validation Type: If it is marked as enabled then a new textbox appears where you are required to enter a name for the **New Validation Type**. The next time you create a data field, this new validation type will be available for selection.
   - Third Party JS URL: You need to provide the URL of the Third Part JS through which validation of the field types would be done.
   - Function Name: Provide the Function Name of the third-party JS.
5. It appears for Integer, Long and Float Data Types.
   If Validation Type is selected as **Custom Formula**, then you are required to provide the following information:
   - Formula: It allows you to set a custom formula for a particular field. For example, if you want to calculate the Principal Interest whose formula is **Principal Interest is P*R*T/100**, then you can do the following:
   - You can set the above formula of Principal Interest as, @I=(@P*@R*T)/100. Where, I, P, R and T are different data fields of the DataClass.
   - To set the above formula, start with '**@**' and select the already created fields. You can use only '+','-','*','/'.
   - After specifying the formula, you can click on **Verify Formula** to check whether the formula is correct or not.

Common DataClass configuration

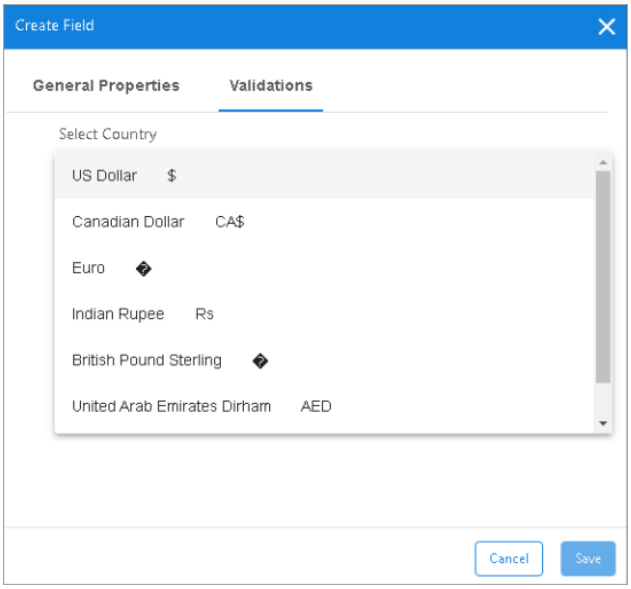
After creating or importing a DataClass using any of the available methods (Manually, NewgenONE Marvin, or Import Option), the following steps are common for configuring and managing the DataClasses:

- Validation type
- Modify dataclass
- Search for dataclasses
- Assigning rights
- User-type dataclass
- Set picklist values
- Delete dataclass
- Set field order
- Export import dataclasses
- Manage custom validation types

Validations tab

The Validation of the fields depend on the selected Validation Type.

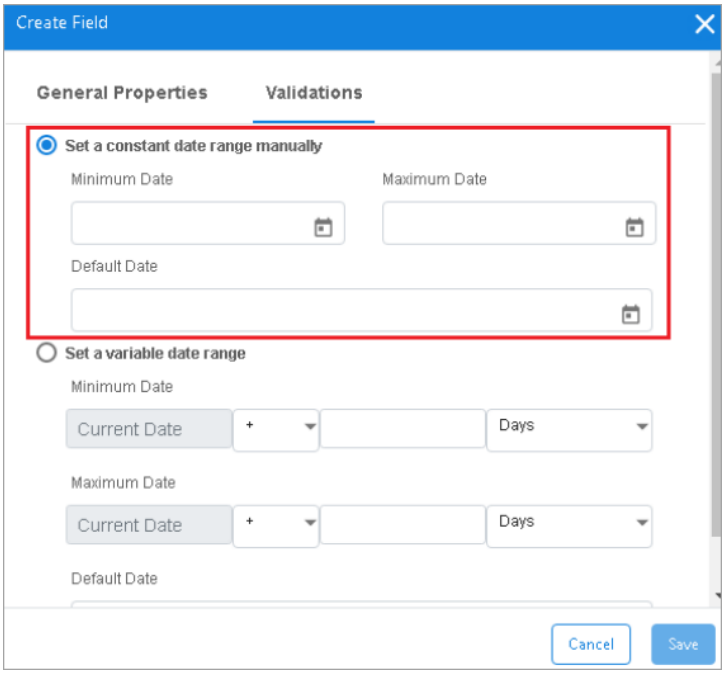
1. When the **Validation Type** is selected as either **Integer** or **Long** or **Float**, you are required to provide the following details to set validations:
   - **Min Value**: The minimum allowed value.
   - **Max Value**: The maximum allowed value.
   - **Default or Predefined Value**: In case the minimum and maximum ranges are defined, then the default or predefined value must be specified between this ranges. In case the minimum and maximum ranges are not defined, then the default or predefined value can be anything.
2. When the **Validation Type** is selected as **Currency**, you are required to provide the following details to set validations:
   - **Select Country**: Click on Select Country and choose a currency from the dropdown list.



- **Min Value**: The minimum allowed value.
- **Max Value**: The maximum allowed value.
- **Default or Predefined Value**: In case the minimum and maximum ranges are defined, then the default or predefined value must be specified between this range. In case the minimum and maximum ranges are not defined, then the default or predefined value can be anything.

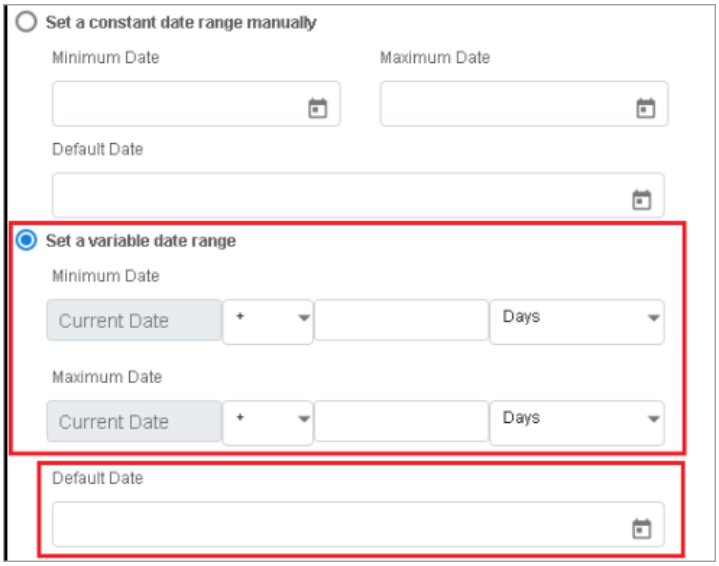
3. When the **Validation Type** is selected as **Percentage**, you are required to provide the following details to set validations:
   - **Min Percentage**: The minimum allowed value.
   - **Max Percentage**: The maximum allowed value.
   - **Default or Predefined Value**: In case the minimum and maximum ranges are defined, then the default or predefined value must be specified between this range. In case the minimum and maximum ranges are not defined, then the default or predefined value can be anything.
4. When the **Validation Type** is selected as either **Custom Regular Expression**, **Text**, **Text (Alpha Numeric)**, **Text (Large Data)**, **Text (Only Alphabets)**, **Text (Only Digits)** or **Email ID**, you are required to provide the following details to set validations:
   - **Min Characters**: The minimum number of allowed characters.
   - **Max Characters**: The maximum number of allowed characters.
   - **Default or Predefined Value**: In case the minimum and maximum ranges are defined, then the default or predefined value must be specified between this range. In case the minimum and maximum ranges are not defined, then the default or predefined value can be anything.

5. When the **Validation Type** is selected as **URL**, you are required to provide the following details to set validations:
   - **URL Type**: The URL type can be either HTTP or HTTPS or Both
   - **Min Characters**: The minimum number of allowed characters.
   - **Max Characters**: The maximum number of allowed characters.
   - **Default or Predefined Value**: In case the minimum and maximum ranges are defined, then the default or predefined value must be specified between this range. In case the minimum and maximum ranges are not defined, then the default or predefined value can be anything.
6. When the **Validation Type** is selected as **Date**, you are required to provide the following details to set validations:
   - **Set a constant date range manually**: Select this option to set the constant date range manually.

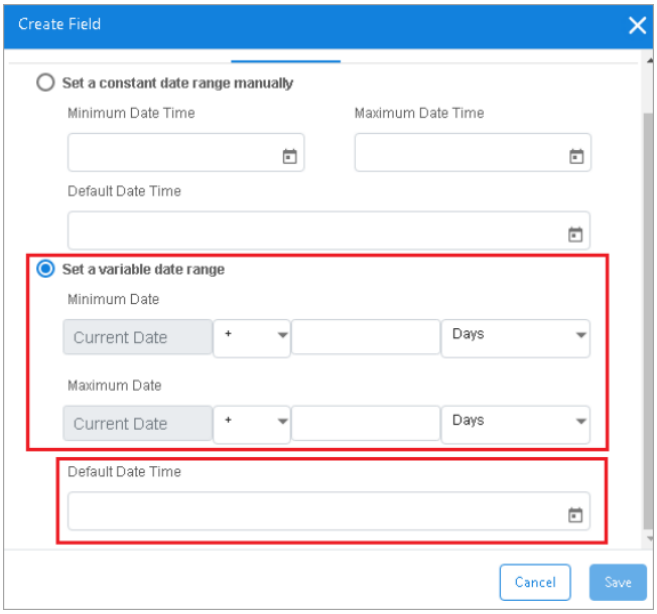


   - **Minimum Date**: The minimum allowed date.
   - **Maximum Date**: The maximum allowed date.
   - **Default Date**: In case the minimum and maximum ranges are defined, then the default date must be specified between this range. In case the minimum and maximum ranges are not defined, then the default date can be anything.
   - **Set a variable date range**: Select this option to set a variable date range.
   - **Minimum Date**: The minimum allowed date. It can be set as the **Current Date**, **+ or -** and the **number of Days/Months/Years**.
   - **Maximum Date**: The maximum allowed date. It can be set as the **Current Date**, **+ or -** and the **number of Days/Months/Years**.

- **Default Date**: In case the minimum and maximum ranges are defined, then the default date must be specified between this range. In case the minimum and maximum ranges are not defined, then the default date can be anything.



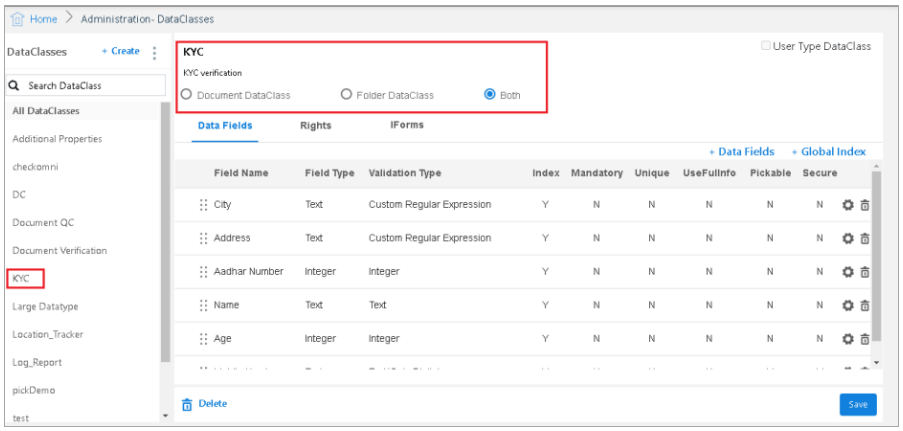
7. When the **Validation Type** is selected as **Date Time**, you are required to provide the following details to set validations:
   - **Set a constant date range manually**: Select this option to set the constant date range manually.
   - **Minimum Date Time**: The minimum allowed date time.
   - **Maximum Date Time**: The maximum allowed date time.
   - **Default Date**: In case the minimum and maximum ranges are defined, then the default date time must be specified between this range. In case the minimum and maximum ranges are not defined, then the default date time can be anything.
   - **Set a variable date range**: Select this option to set a variable date range.
   - **Minimum Date**: The minimum allowed date. It can be set as the **Current Date**, **+ or -** and the **number of Days/Months/Years**.
   - **Maximum Date**: The maximum allowed date. It can be set as the **Current Date**, **+ or -** and the **number of Days/Months/Years**.
   - **Default Date Time**: In case the minimum and maximum ranges are defined, then the default date time must be specified between this range. In case the minimum and maximum ranges are not defined, then the default date time can be anything.



Modify dataclass

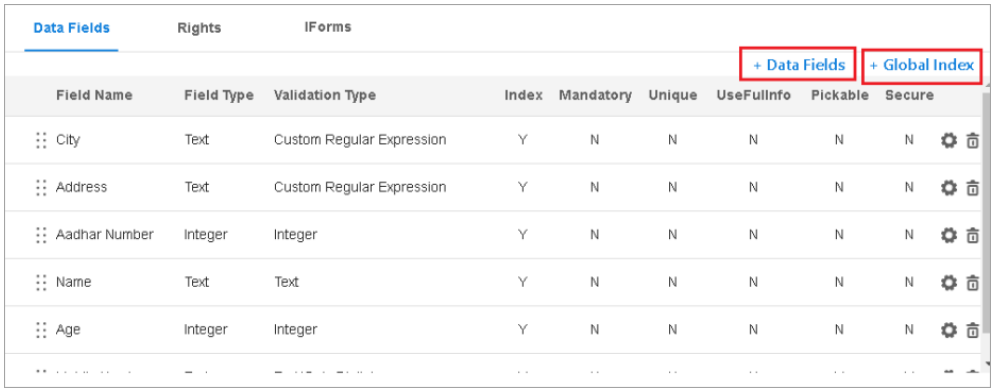
To Modify a DataClass and its Data Fields:

1. Open the DataClass that needs to be modified.
2. Change the DataClass **Name**, its **Description** and **Type** (Document/Folder/Both) as required.

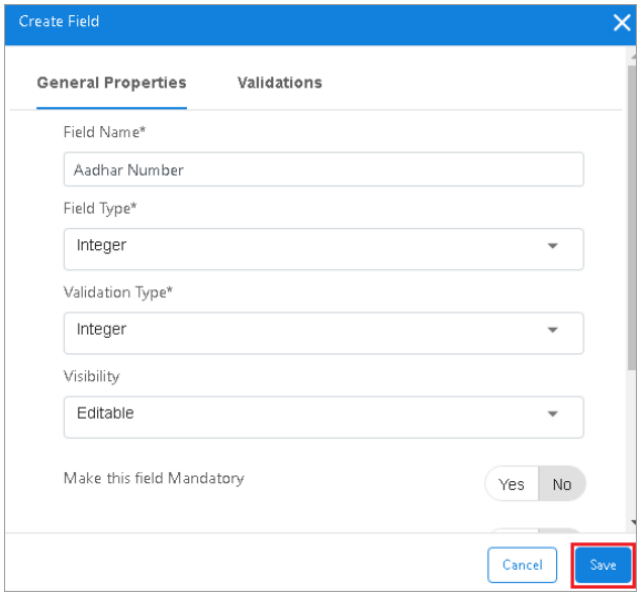


3. **To add more data fields**:
4. Click on the **+ Data Fields** link to create and add a new data field.
5. Create Field dialog box appears.
6. Follow the steps described for adding a data field in the section DataClass Creation.

7. Click on the **+ Global Index** link to add a data field using the already defined Global Index.
8. Global Indexes dialog box appears.
9. Follow the steps described for adding a data field using a Global Index in the section DataClass Creation.



10. **To modify a data field**:
    a. Click on **Modify Field** button against the desired data field.
    b. Create Field dialog box appears.
    c. Modify the value of the fields as required and click on **Save** to save the changes made.

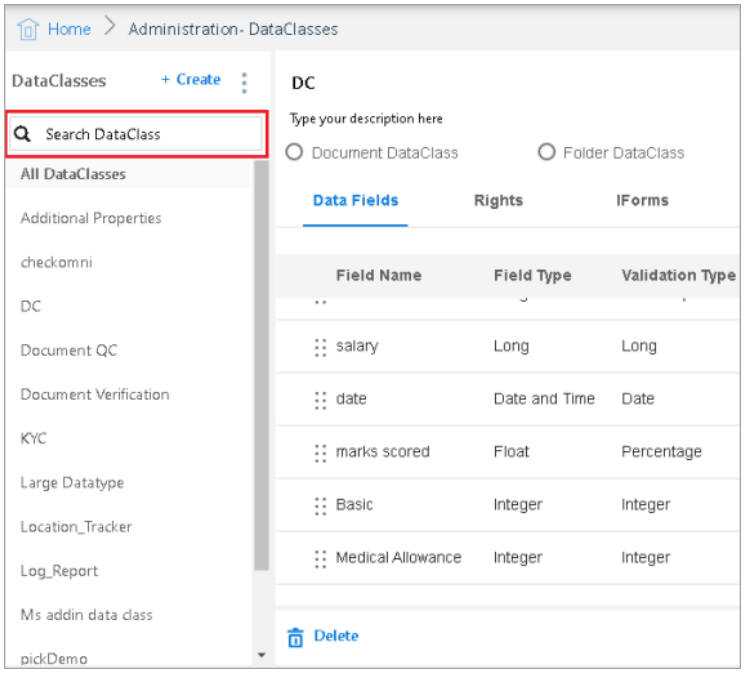


    d. A message "**DataClass modified successfully**" appears.

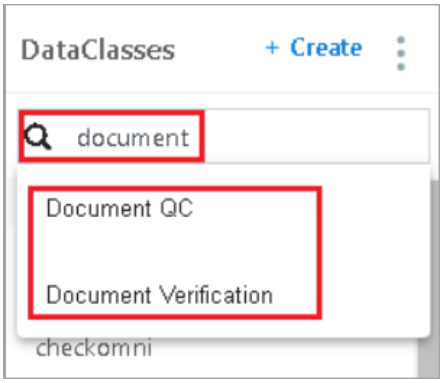
Search for dataclasses

To Search for any DataClass:

1. Click in the **Search DataClass** search text box.



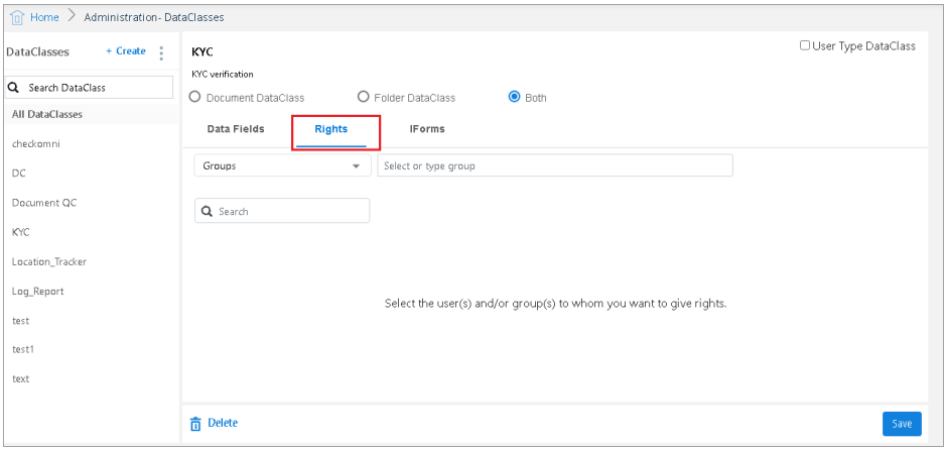
2. Enter the DataClass name to search for.
3. As you type the characters, the un-matching names keep on disappearing and in the end, only matched names are left in the dropdown list.



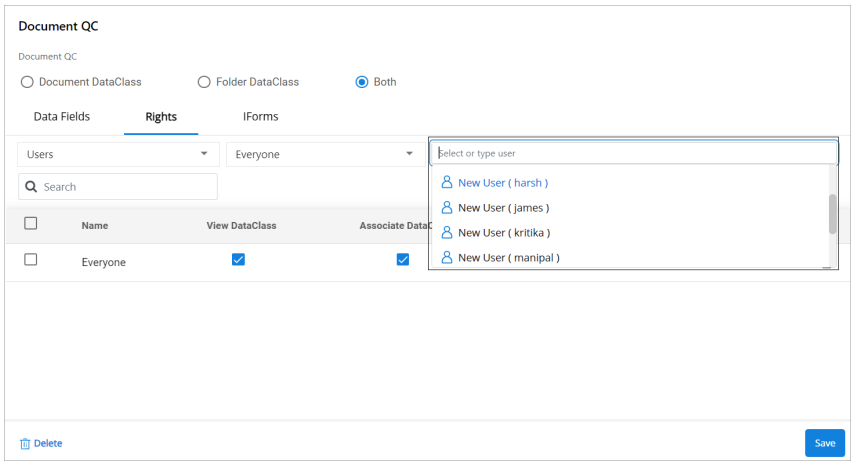
Assigning rights

To Assign Rights to Users, Groups and Roles on a DataClass:

1. Open the dataclass and click on the **Rights** tab.



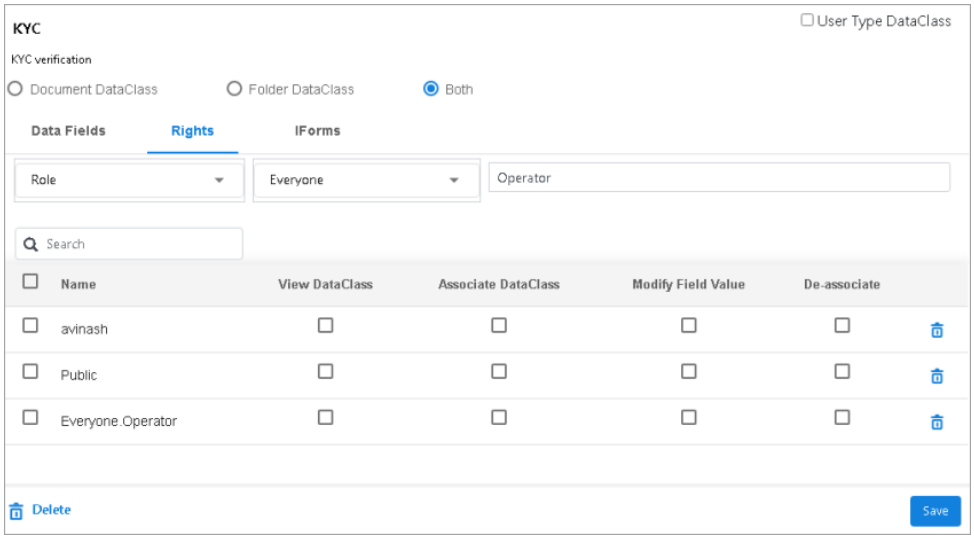
2. Add Users, Groups and Roles to the Rights list.
    a. To add users to the Rights list:
        i. Select **Users** from the Groups/Users/Roles dropdown list.
        ii. **Select or Type Group** name in the associated combo box.
        iii. **Select or Type User Name** in the associated combo box.



    b. To add groups to the Rights list:
        i. Select **Groups** from the Groups/Users/Roles dropdown list.
        ii. **Select or Type Group** name in the associated combo box.
    c. To add roles to the Rights list:
        i. Select the **Role** from the Groups/Users/Roles dropdown list.
        ii. **Select or Type Group** name in the associated combo box.

iii. **Select or Type User Name** in the associated combo box.

3. As you select a User, Group or Role, it gets added to the Rights list.



4. Now that Users, Groups and Roles are added to the Rights list, **you can assign Rights** to them.
   - **View DataClass**: It enables users/groups/roles to view DataClass in the list of available DataClasses. The rights holder can view all documents and folders with which this DataClass is associated. Users having no rights on the folder or document will not be able to view them. Users should have view rights on both (document/folders and DataClass associated with it) to view it.
   - **Associate DataClass**: When this right is given to the users/groups/roles on DataClass, they will be able to associate DataClass to documents and folders. When this right is given to users, View DataClass right is given by default.
   - **Modify Field Value**: It enables users to modify the field values of this DataClass. When this right is given, view DataClass right is given by default.
   - **De-associate DataClass**: It enables users to disassociate any DataClass from folders or documents they have rights on. When this right is given, view DataClass right is given by default.
5. To remove any Users/Groups/Roles from the Rights list:
   a. To remove a single User/Group/Role:
      i. Click on the **Remove** button against the rights holder.
   b. To remove multiple Users/Groups/Roles:
      i. Select the required rights holders.
      ii. Click on the **Delete** button that appears after selecting two or more users.
6. Click on **Save** to save the changes made to the DataClass definition.
7. A message "**DataClass modified successfully**" appears.

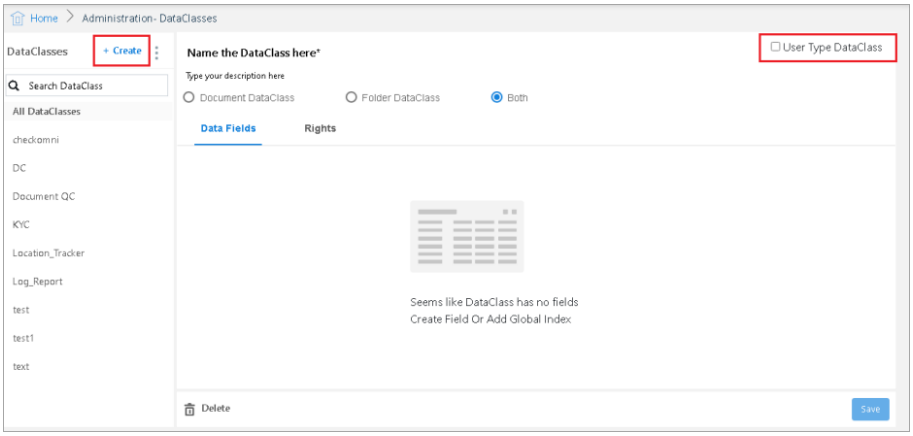
User-type dataclass

User-Type DataClass is used to add some additional properties for users. It can be created only once but can be associated with different users.

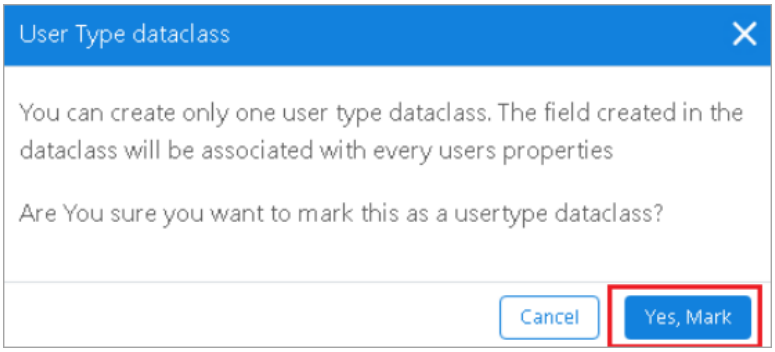
The feature to add User-Type DataClass appears if EnableUtypeDataClass=Y parameter is set to true (Y) in *eworkstyle.ini* file.

To Create a User-Type DataClass and associate it with different users:

1. Click on the **+Create** link given in the left pane of the DataClasses screen or open an existing DataClass and enable it as a User-Type DataClass.
2. Select the **User Type DataClass** checkbox to enable it.



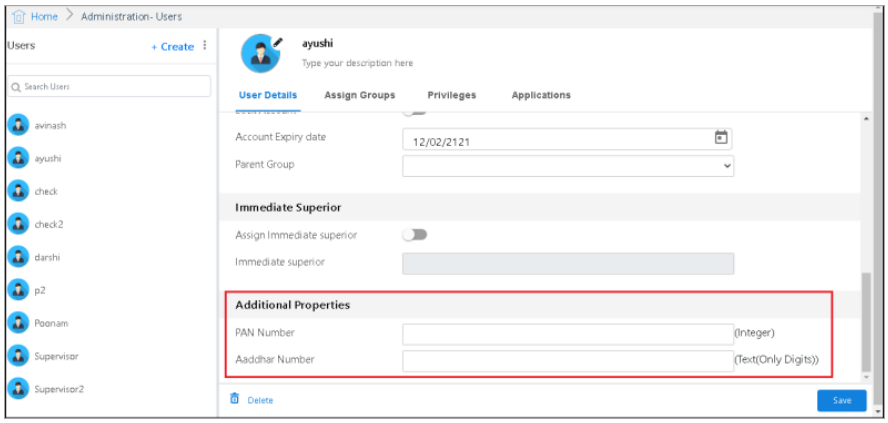
3. As you select the **User Type DataClass** checkbox, the following alert message appears.
   • Click **Yes, Mark** to confirm.



4. Now, create the data fields in the same way as described in the section DataClass Creation.

The User-Type Data Class can be modified and deleted in the same way as that of other data classes.

5. Now that the User-Type data class has been added, you can associate it with existing or new users. To do so, follow the given steps:
    a. Go to **Users** and click on **+Create** to create a new user or modify the properties of an existing user.
    b. As per the selection, the User properties screen appears.
    c. A new section with the name of the User-Type DataClass now appears in the user definition screen. The label name depends on the name of the User-Type DataClass defined.



    d. Specify all the field data for Additional Properties.
    e. Click on **Save** to save the user properties.

Set picklist values

As you mark any data field **Pickable**, a new tab "**Picklist**" gets added for the pickable field being created.

To Set Picklist Values:

1. Go to the **PickList** tab.
2. Select an option for **Get Values From**.
3. If **Custom UI** is selected, then provide the **Custom UI URL** to get the picklist values.
4. If **Web Service** is selected, then provide the **Rest Service URL** to get the picklist values.
5. If **Manual** is selected, then follow the below steps to add the **Input Values**.
6. Enter a value and click on **Add**.
7. Repeat the above step to add more values.
8. The added value appears in the lower section of the dialog box.

9. To mark any value as the Default, slide the button to the right.
   • An alert message appears.
   • Click on **OK** to proceed.
10. To **Remove** a Picklist Value:
    • Click on the **More** button against the picklist value and choose **Remove Value**.
    • Repeat the above step to remove more values.
11. To **Assign Rights** on the added picklist values:
12. Click on the **More** button against the picklist value and choose **Assign Rights**.
13. Rights on Picklist Values dialog box appears.
14. **To add users to the Rights list:**
    • Select **Users** from the Groups/Users/Roles dropdown list.
    • **Select or Type Group name in the associated combo box.**
    • **Select or Type User Name in the associated combo box.**
15. To add groups to the Rights list:
    • **Select Groups** from the Groups/Users/Roles dropdown list.
    • **Select or Type Group name in the associated combo box.**
16. To add roles to the Rights list:
    • Select the **Role** from the Groups/Users/Roles dropdown list.
    • **Select or Type Group name in the associated combo box.**
    • **Select or Type User Name in the associated combo box.**
17. As you select a User, Group or Role, it gets added to the Rights list.
18. To remove Users/Groups/Roles from the Rights list:
    a. To remove a single rights holder:
        i. Click on the **Remove** button against the rights holder.
    b. To remove multiple Users/Groups/Roles:
        i. Select the required Users/Groups/Roles.
        ii. Click on the **Delete** button that appears after selecting two or more names.
19. Click on **Save** to save the defined picklist values.
20. You can click on **Back** (top-left corner) to return to the Create Field dialog box.

Check Rights on the pickable data class values: The Check Rights option allows you to apply the assigned rights on the picklist values. The assigned rights do not work if this checkbox is cleared.

To apply rights on the picklist values, perform the following steps:

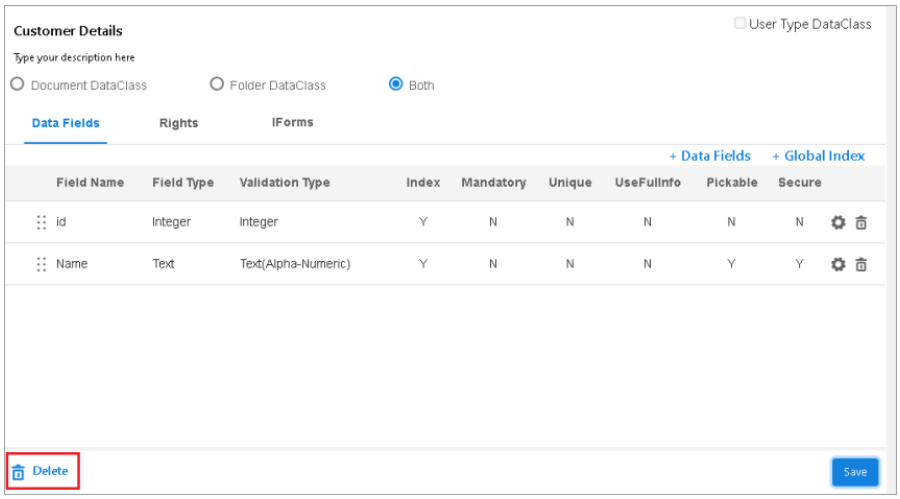
1. Open the data class having pickable data fields.

2. Click (**Modify Field**) icon against the required pickable data field. The Modify Field dialog appears.
3. Select the **CheckRights** checkbox and assign rights to users. To know how to assign rights to users on the picklist values, refer to steps described in the Set Picklist Values section.
4. Click **Save** after assigning rights.
5. Click **Save** to save the modified data class.

Delete dataclass

To Delete a DataClass:

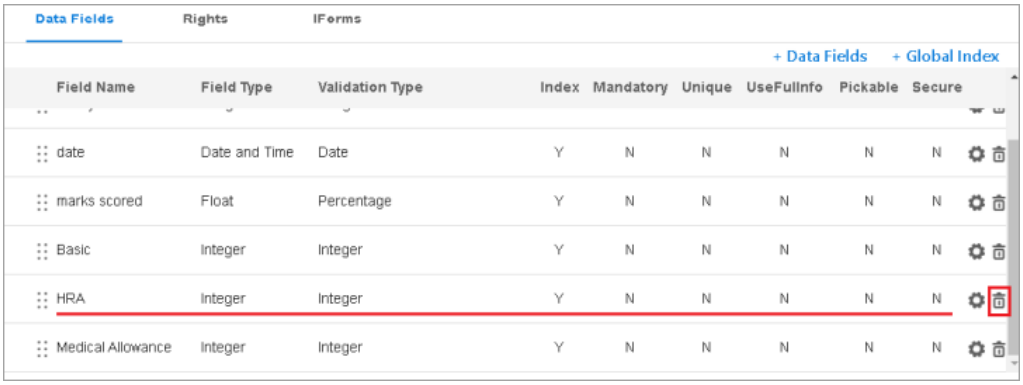
1. Open the dataclass to be deleted.
2. Click on the **Delete** button.



3. An alert message appears.
4. Click on **Confirm** to confirm the DataClass deletion.
5. A message "**DataClass deleted successfully**" appears.

To Delete a Data Field of a DataClass:

1. Open the dataclass, the fields of which is to be deleted.
2. Click on the **Delete Field** button against the fields, which is to be deleted.

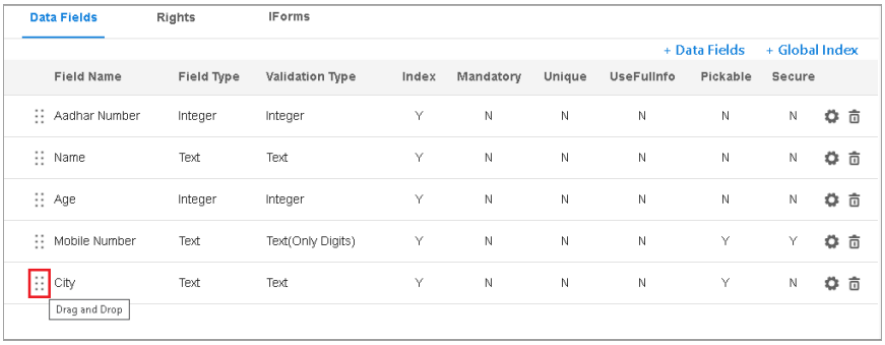


3. An alert message appears.
4. Click on **Confirm** to confirm the DataClass field deletion.
5. A message "**DataClass modified successfully**" appears.

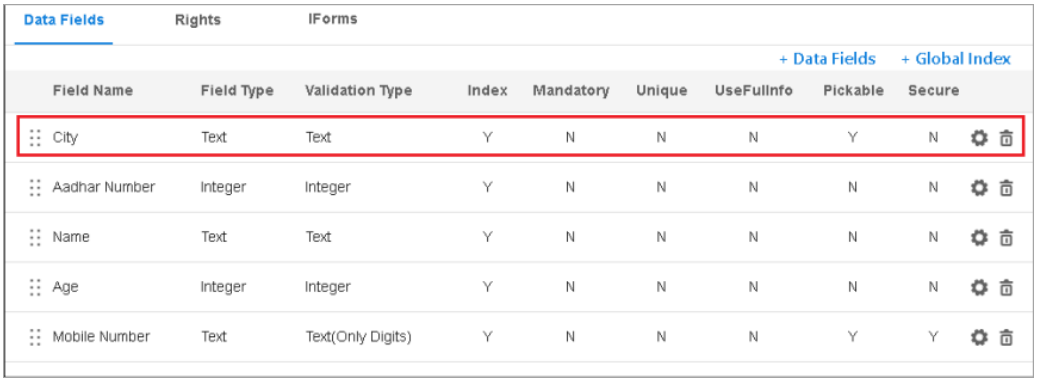
Set field order

To Set Field Order:

1. Open the list of **DataClass** data fields.
2. Drag the required data field by clicking and holding the six dots.



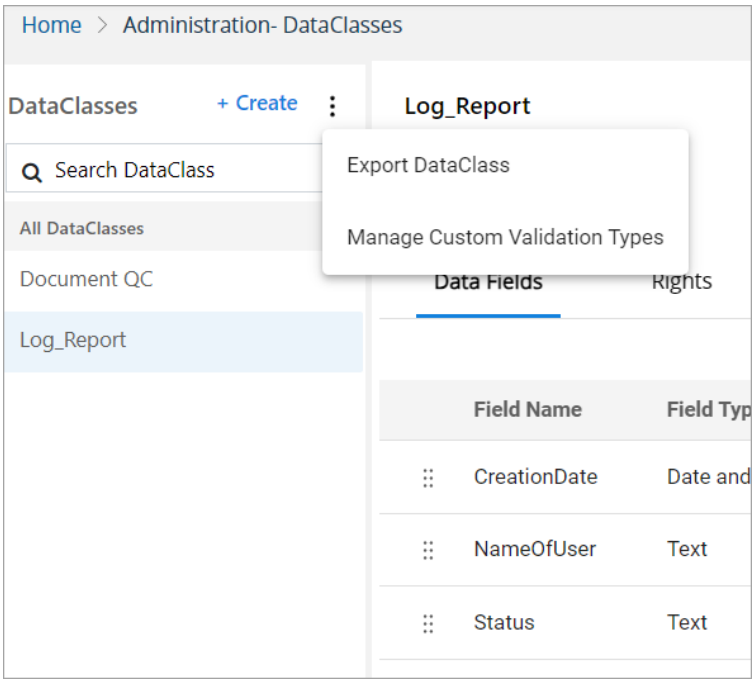
3. Drop it to the desired position.
4. As you drop the data field, a message "**Data Field Order Set Successfully**" appears.
5. The data field now appears at the dropped position.



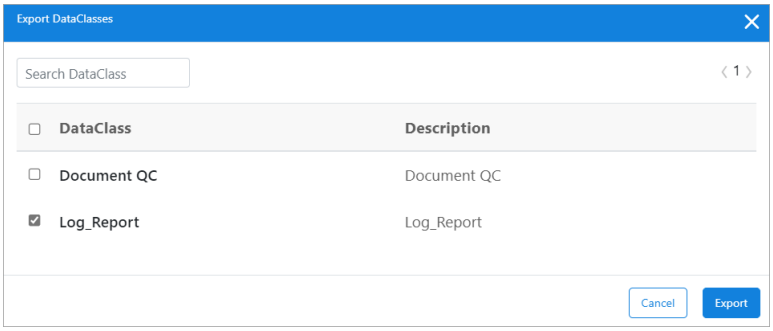
Export import dataclasses

To Export DataClasses:

1. Go to **DataClasses**.
2. Click on the **More Actions** button and choose **Export DataClass**.



3. Export DataClasses dialog box appears.
4. Select the desired DataClasses and click on **Export**.



You can search for a DataClass by entering its name in the search box.

5. The selected DataClasses will be downloaded in the form of an **XML file**.

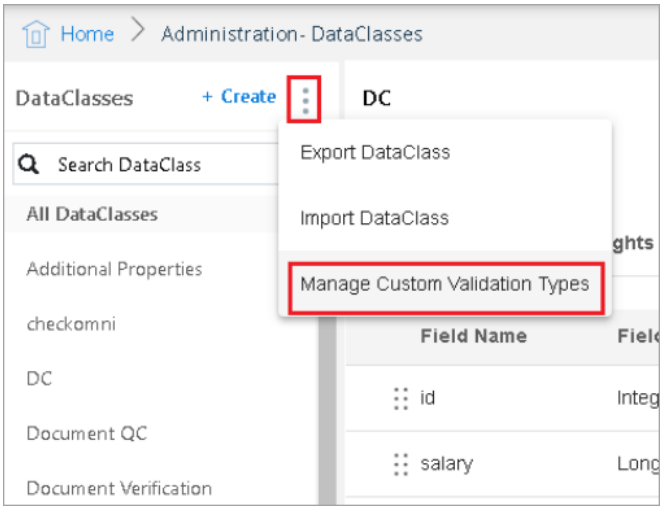
- In the home screen of Export DataClasses, the first batch of DataClass is displayed. For the first batch, the "Prev" button is disabled. For the last batch "Next" button is disabled.
- When the user clicks on the Next button, the next batch of DataClasses appears. From these subsequent batches of DataClasses, the users can select more DataClasses. During this process, DataClasses selected from the previous batches will also remain selected.

Manage custom validation types

Manage Custom Validation Types feature is used to delete the Custom Validation Settings saved during the DataClass data field creation.

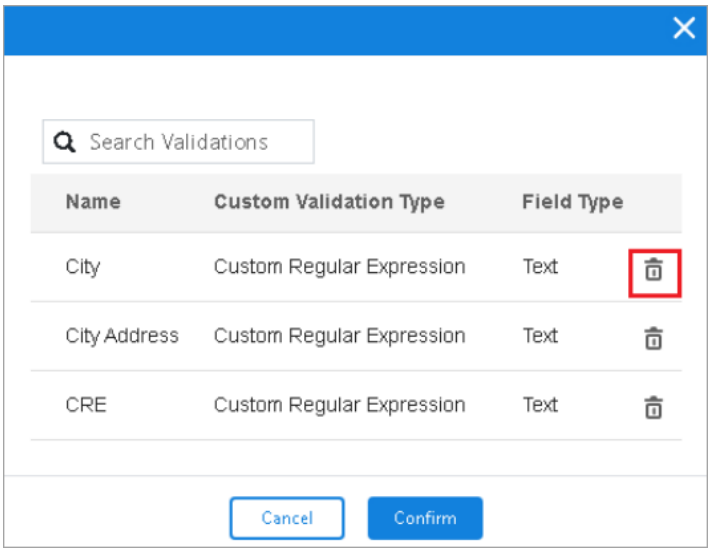
To Delete a Custom Validation Type:

1. Go to **DataClasses**.
2. Click on the **More Actions** button and choose **Manage Custom Validation Types**.



3. A dialog box appears.

4. Click on the **Delete** button against the desired validation type.



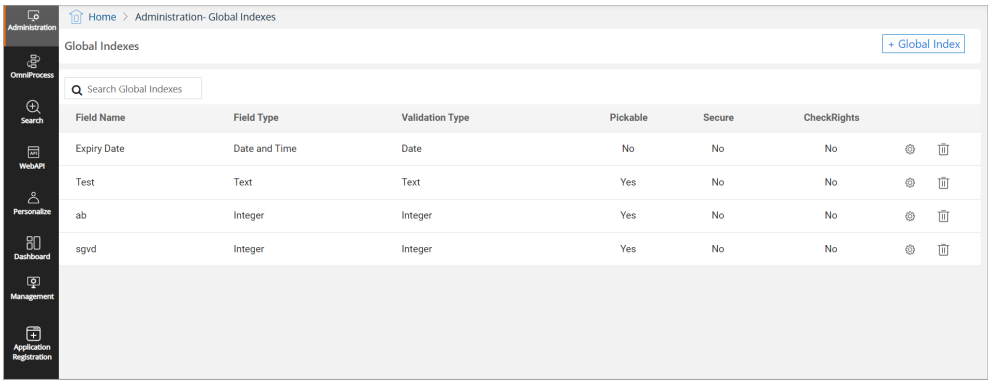
5. A confirmation message appears. Click on **Confirm** to confirm the deletion.
6. A message "**Custom Validation deleted Successfully**" appears.

Global indexes

Global Indexes are user-defined indexes or fields that can be associated to any document across different classes. Global Indexes provide a data field that can be searched for across the entire cabinet, retrieving documents of different DataClasses.

To Access Global Indexes:

1. In the home screen of OmniDocs Admin, go to **Administration** tile and click on the **Global Indexes** link.
2. Global Indexes screen appears. It shows the existing Global Indexes.



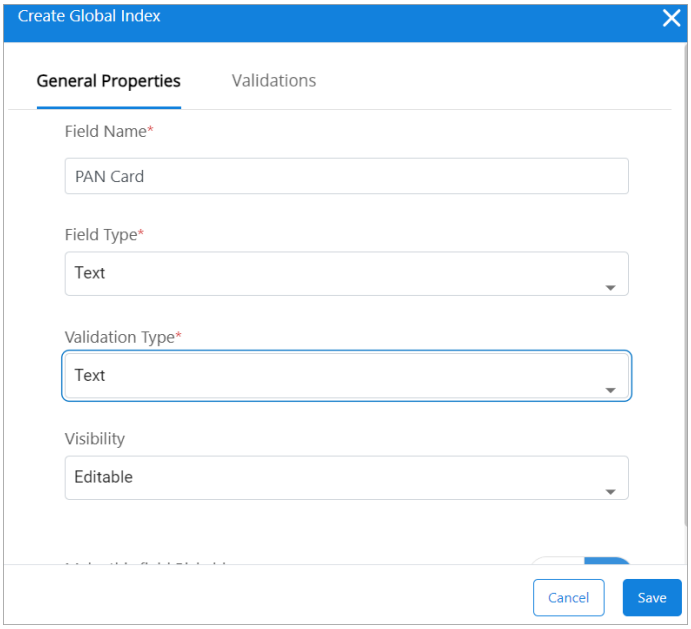
Global index creation

To Add a Global Index:

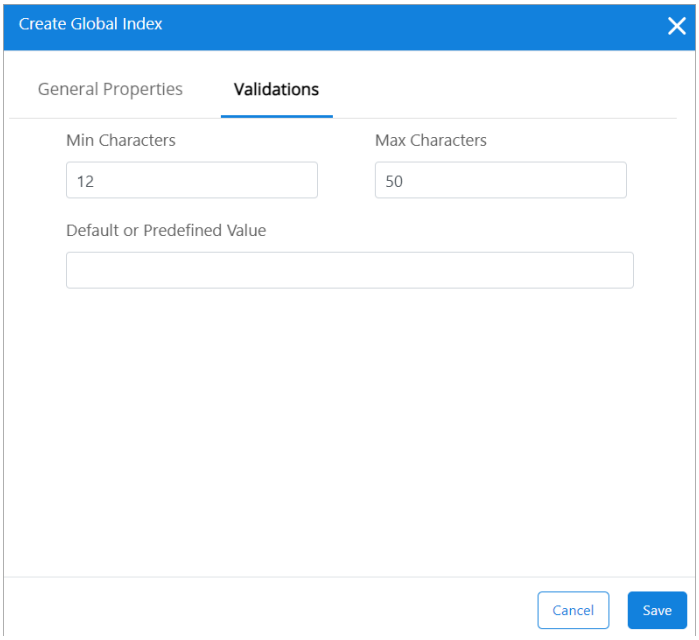
1. Click on the **+ Global Index** link.
2. Create Field dialog box appears.
3. Specify **General Properties** as described below:

Fields	Description
Field Name	Enter the Global Index name.
Field Type	Select the required Field Type from the dropdown list. In the dropdown list, the following data types are available: • Integer • Long • Float • Text • Date & Time
Validation Type	Select the required Validation Type from the dropdown list. The options in the Validation Type dropdown list depends on the selected Field Type. Refer to the section Validation Type for details.
Visibility	Select the required Visibility from the dropdown list. In the dropdown list, the following types of visibility are available: • Hidden: If this field is to be made hidden from the end-user. • Readonly: If this field is required to appear in read-only format to the end-user. • Editable: If this field is required to appear in editable format to the end-user.
Make this field Pickable	Select Yes to make any field Pickable so that field values can be chosen from a predefined list of values. As you mark this field as enabled, the Global Index gets saved and a new tab “Picklist” gets added for the pickable field. Refer to the section Set Picklist Values to add pickable values.

Fields	Description
Make this Field Secure	In case the Data Security Functionality is enabled, Make this Field Secure option appears for the Text Field Type. The Data Security feature can only be enabled at the time of Data Field creation. You cannot enable the Data Security feature in an already created Data Field. Select Yes to enable Field Security else select No.



4. Set the **Validations** as required. The Validations depend on the selected Validation Type. Refer to the section Validations Tab for details. The below screenshot is of Validations when the Validation Type is Integer.
5. Once all the field values are specified, click on **Save** to add the Global Index.



6. A message “Global Index added successfully” appears.

Validation type

The options in the Validation Type dropdown list depend on the selected Field Type.

1. If the **Field Type** is selected as **Text**, then the following options are available for the **Validation Type**:

Validation Type	Description
Custom Regular Expression	Text (Only Alphabets)
Email ID	Text (Only Digits)
Text	URL
Text (Alpha-Numeric)	Custom Validation (Rest Service)
Text (Large Data)	Custom Validation (Third Party JS)

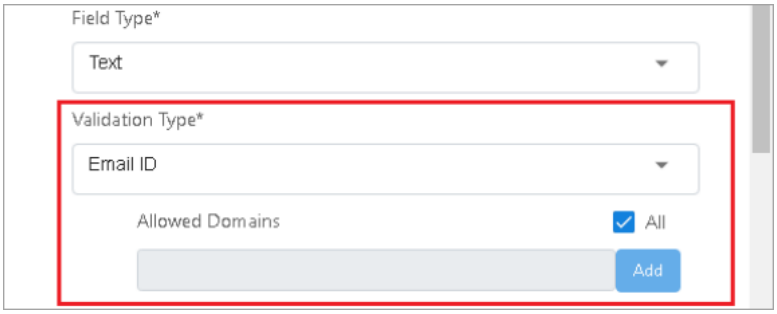
2. If the **Field Type** is selected as **Integer**, then the following options are available for the **Validation Type**:
   • Auto Sequence Generation
   • Integer
   • Custom Validation (Rest Service)
   • Custom Validation (Third Party JS)
3. If the **Field Type** is selected as **Long**, then the following options are available for the **Validation Type**:
   • Long
   • Custom Validation (Rest Service)
   • Custom Validation (Third Party JS)
4. If the **Field Type** is selected as **Float**, then the following options are available for the **Validation Type**:
   • Currency
   • Float
   • Percentage
   • Custom Validation (Rest Service)
   • Custom Validation (Third Party JS)

5. If the **Field Type** is selected as **Date & Time**, then the following options are available for the **Validation Type**:
   - Date
   - Date Time
   - Custom Validation (Rest Service)
   - Custom Validation (Third Party JS)

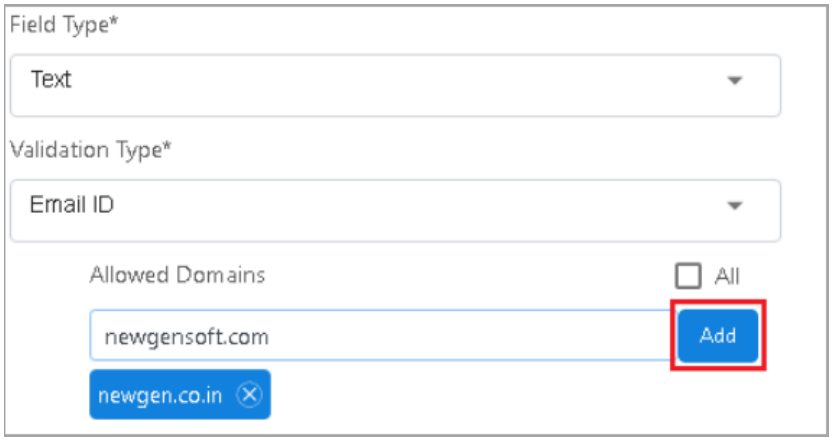
Validation type-options

1. **Custom Regular Expression**: It appears when the Field Type is Text.
   If Validation Type is selected as **Custom Regular Expression**, then you are required to provide the following information:
   - Regular Expression: You can define custom regular expression for the validation of the data fields.
   - Example: The validation of the fields can be checked by entering the value in the example field.
   - Save these custom settings as a New Validation Type: If it is marked as enabled then a new textbox appears where you are required to enter a name for the **New Validation Type**. The next time you create a data field, this new validation type will be available for selection.

2. **Email ID:** It appears when the Field Type is Text.If Validation Type is selected as **Email ID**, then you are required to provide the following information:
   - Allowed Domains:
     1. Select the checkbox **All** to allow all the domains.



2. Unselect the checkbox All to allow only the added domains and restrict the others. The Add textbox gets enabled on unselecting the All checkbox.
3. Enter the domain name in the textbox and click on **Add**.



4. To remove the added domain, click on the cross mark against the added domain.

3. **Custom Validation (Rest Service)**: It appears for Text, Integer, Long, Float and Date & Time Field Types.
   If Validation Type is selected as **Custom Validation (Rest Service)**, then you are required to provide the following information:
   - Save these custom settings as a New Validation Type: If it is marked as enabled then a new textbox appears where you are required to enter a name for the **New Validation Type**. The next time you create a data field, this new validation type will be available for selection.
   - Rest Service URL: You need to provide the URL of the Rest Service through which validation of the field types would be done.

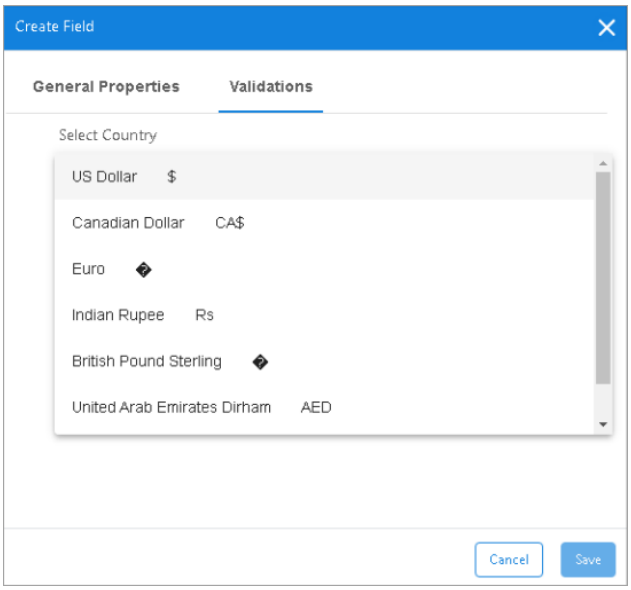
4. **Custom Validation (Third Party JS):** It appears for Text, Integer, Long, Float and Date & Time Field Types.
   If Validation Type is selected as **Custom Validation (Third Party JS)**, then you are required to provide the following information:
   - Save these custom settings as a New Validation Type: If it is marked as enabled then a new textbox appears where you are required to enter a name for the **New Validation Type**. The next time you create a data field, this new validation type will be available for selection.
   - Third Party JS URL: You need to provide the URL of the Third Part JS through which validation of the field types would be done.
   - Function Name: Provide the Function Name of the third-party JS.
5. It appears for Integer, Long and Float Data Types.
   If Validation Type is selected as **Custom Formula**, then you are required to provide the following information:
   - Formula: It allows you to set a custom formula for a particular field. For example, if you want to calculate the Principal Interest whose formula is **Principal Interest is P*R*T/100**, then you can do the following:
   - You can set the above formula of Principal Interest as, @I=(@P*@R*T)/100. Where, I, P, R and T are different data fields of the DataClass.
   - To set the above formula, start with '**@**' and select the already created fields. You can use only '+','-','*','/'.
   - After specifying the formula, you can click on **Verify Formula** to check whether the formula is correct or not.

Validations tab

The Validation of the fields depend on the selected Validation Type.

1. When the **Validation Type** is selected as either **Integer** or **Long** or **Float**, you are required to provide the following details to set validations:
   - **Min Value**: The minimum allowed value.
   - **Max Value**: The maximum allowed value.
   - **Default or Predefined Value**: In case the minimum and maximum ranges are defined, then the default or predefined value must be specified between this ranges. In case the minimum and maximum ranges are not defined, then the default or predefined value can be anything.

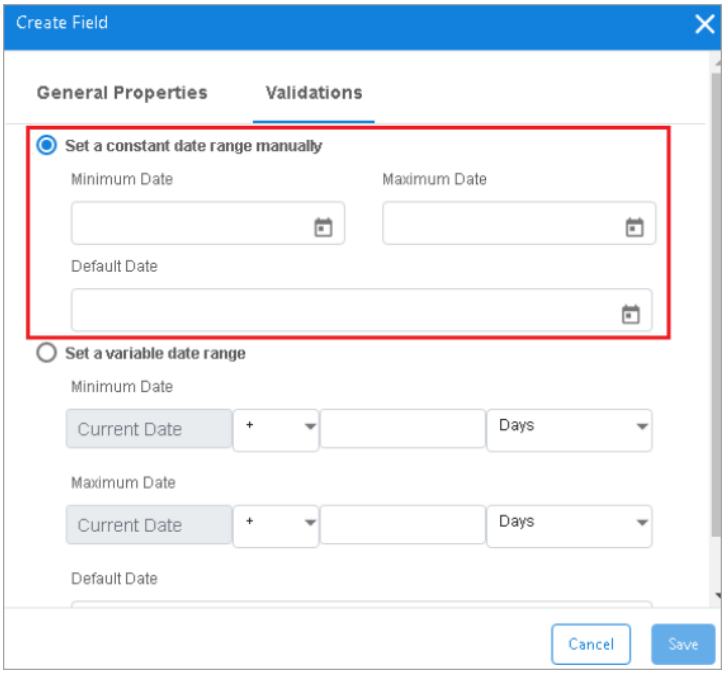
2. When the **Validation Type** is selected as **Currency**, you are required to provide the following details to set validations:
   - **Select Country**: Click on Select Country and choose a currency from the dropdown list.



   - **Min Value**: The minimum allowed value.
   - **Max Value**: The maximum allowed value.
   - **Default or Predefined Value**: In case the minimum and maximum ranges are defined, then the default or predefined value must be specified between this range. In case the minimum and maximum ranges are not defined, then the default or predefined value can be anything.
3. When the **Validation Type** is selected as **Percentage**, you are required to provide the following details to set validations:
   - **Min Percentage**: The minimum allowed value.
   - **Max Percentage**: The maximum allowed value.
   - **Default or Predefined Value**: In case the minimum and maximum ranges are defined, then the default or predefined value must be specified between this range. In case the minimum and maximum ranges are not defined, then the default or predefined value can be anything.
4. When the **Validation Type** is selected as either **Custom Regular Expression**, **Text**, **Text (Alpha Numeric)**, **Text (Large Data)**, **Text (Only Alphabets)**, **Text (Only Digits)** or **Email ID**, you are required to provide the following details to set validations:
   - **Min Characters**: The minimum number of allowed characters.
   - **Max Characters**: The maximum number of allowed characters.

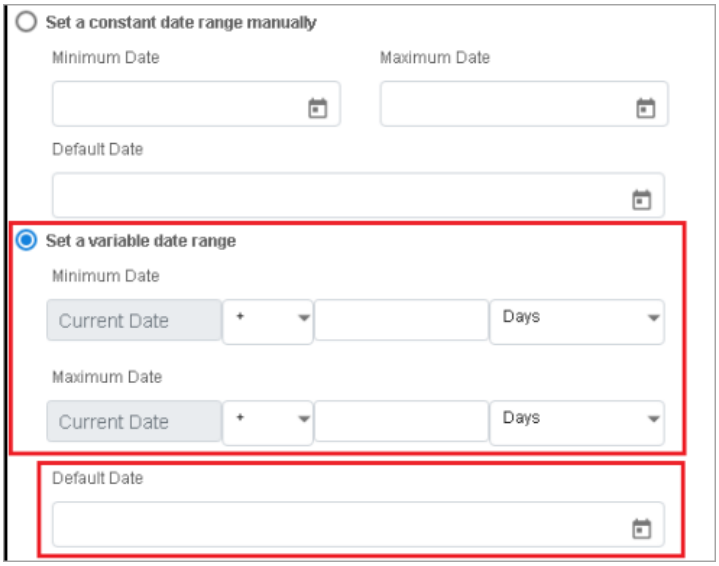
- **Default or Predefined Value**: In case the minimum and maximum ranges are defined, then the default or predefined value must be specified between this range. In case the minimum and maximum ranges are not defined, then the default or predefined value can be anything.

5. When the **Validation Type** is selected as **URL**, you are required to provide the following details to set validations:
   - **URL Type**: The URL type can be either HTTP or HTTPS or Both
   - **Min Characters**: The minimum number of allowed characters.
   - **Max Characters**: The maximum number of allowed characters.
   - **Default or Predefined Value**: In case the minimum and maximum ranges are defined, then the default or predefined value must be specified between this range. In case the minimum and maximum ranges are not defined, then the default or predefined value can be anything.
6. When the **Validation Type** is selected as **Date**, you are required to provide the following details to set validations:
   - **Set a constant date range manually**: Select this option to set the constant date range manually.

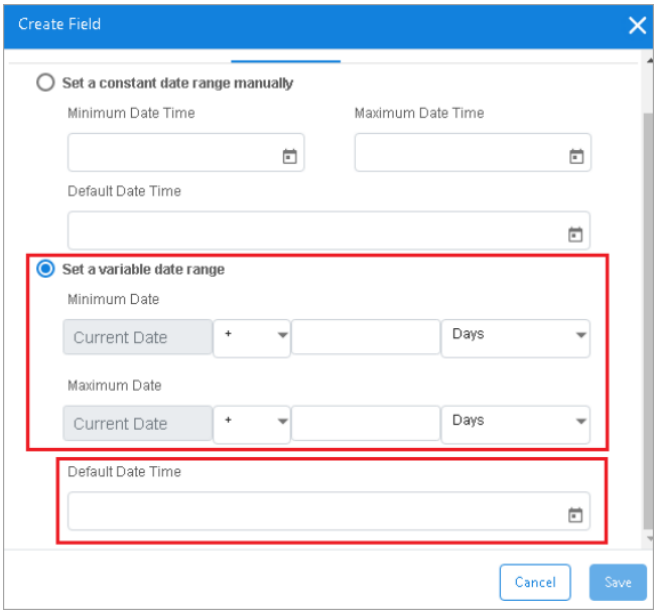


   - **Minimum Date**: The minimum allowed date.
   - **Maximum Date**: The maximum allowed date.
   - **Default Date**: In case the minimum and maximum ranges are defined, then the default date must be specified between this range. In case the minimum and maximum ranges are not defined, then the default date can be anything.
   - **Set a variable date range**: Select this option to set a variable date range.

- **Minimum Date**: The minimum allowed date. It can be set as the **Current Date**, **+ or -** and the **number of Days/Months/Years**.
- **Maximum Date**: The maximum allowed date. It can be set as the **Current Date**, **+ or -** and the **number of Days/Months/Years**.
- **Default Date**: In case the minimum and maximum ranges are defined, then the default date must be specified between this range. In case the minimum and maximum ranges are not defined, then the default date can be anything.



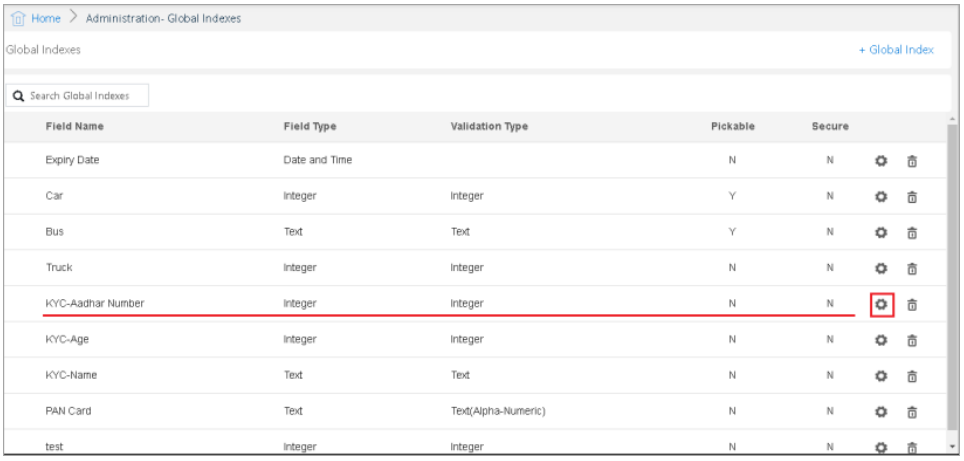
7. When the **Validation Type** is selected as **Date Time**, you are required to provide the following details to set validations:
   - **Set a constant date range manually**: Select this option to set the constant date range manually.
   - **Minimum Date Time**: The minimum allowed date time.
   - **Maximum Date Time**: The maximum allowed date time.
   - **Default Date**: In case the minimum and maximum ranges are defined, then the default date time must be specified between this range. In case the minimum and maximum ranges are not defined, then the default date time can be anything.
   - **Set a variable date range**: Select this option to set a variable date range.
   - **Minimum Date**: The minimum allowed date. It can be set as the **Current Date**, **+ or -** and the **number of Days/Months/Years**.
   - **Maximum Date**: The maximum allowed date. It can be set as the **Current Date**, **+ or -** and the **number of Days/Months/Years**.
   - **Default Date Time**: In case the minimum and maximum ranges are defined, then the default date time must be specified between this range. In case the minimum and maximum ranges are not defined, then the default date time can be anything.



Modify global index

To Modify a Global Index:

1. Go to the Global Index screen.
2. Click on **Modify Field** button against the Global Index to modify.



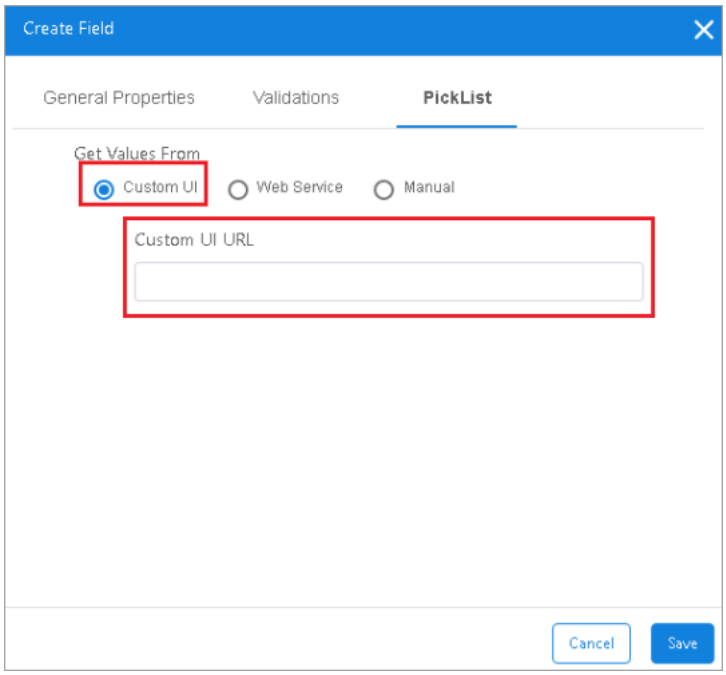
3. Create Field dialog box appears.
4. Modify the value of the fields as required and click on **Save** to save the changes made.
5. A message "**Global Index modified successfully**" appears.

Set picklist values

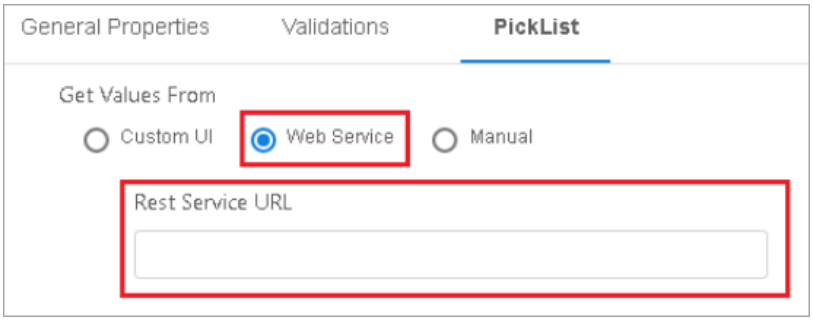
As you mark any field as enabled for **Make this field Pickable**, the Global Index gets saved and the Create Field dialog box gets closed. When this Global Index is opened for modification, a new tab "**Picklist**" appears in addition to the General Properties and Validations tabs.

To Set Picklist Values:

1. Open the Global Index to modify
2. Go to the **PickList** tab. The PickList tab appears for only the pickable Global Indexes.
3. Select an option for **Get Values From**.

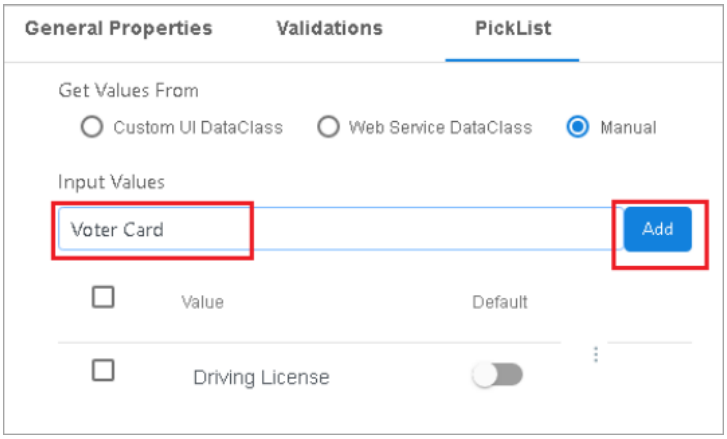


4. If **Custom UI** is selected, then provide the Custom UI URL.
   a. If Web Service is selected, then provide the Rest Service URL.

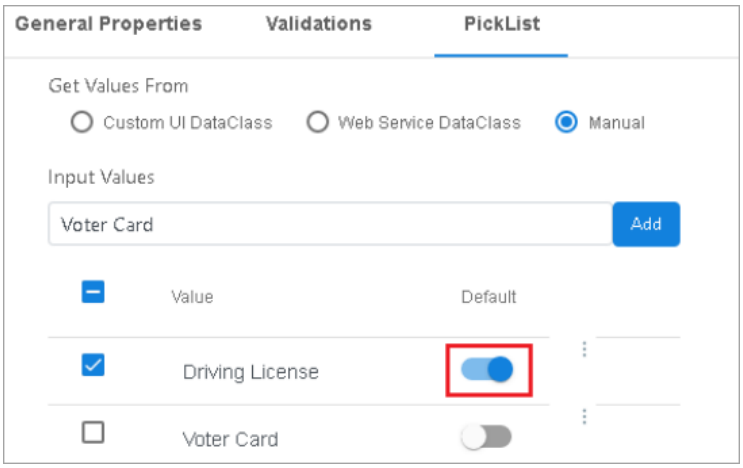


   b. If Manual is selected, then follow the below steps to add the Input Values.

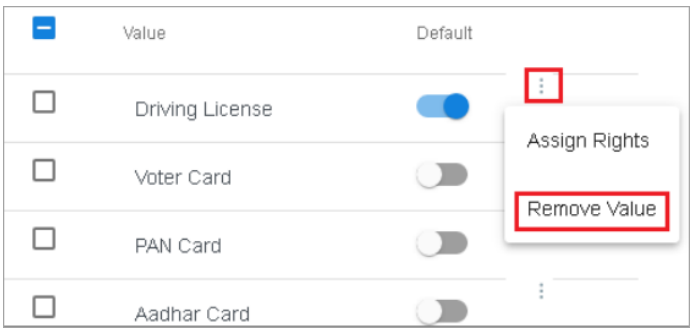
i. Enter a value and click on Add.
ii. Repeat the above step to add more values.
iii. The added value appears in the lower section of the dialog box.



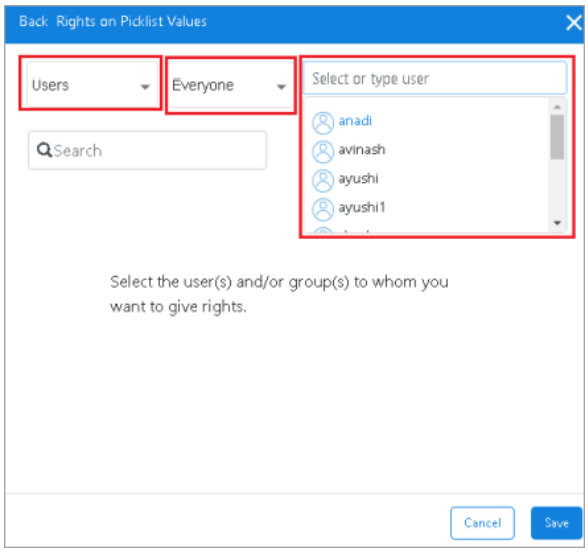
iv. To mark any value as the Default, slide the button to the right.
- An alert message appears.
- Click on **OK** to proceed.



v. **To Remove a Picklist Value:**
- Click on the More button against the picklist value and choose Remove Value.
- Repeat the above step to remove more values.



vi. To Assign Rights on the added picklist values:
    i. Click on the **More** button against the picklist value and choose Assign Rights.
    ii. Rights on Picklist Values dialog box appears.
    iii. **To add users to the Rights list:**
        • Select Users from the Groups/Users/Roles dropdown list.
        • Select or Type Group name in the associated combo box.
        • Select or Type User Name in the associated combo box.



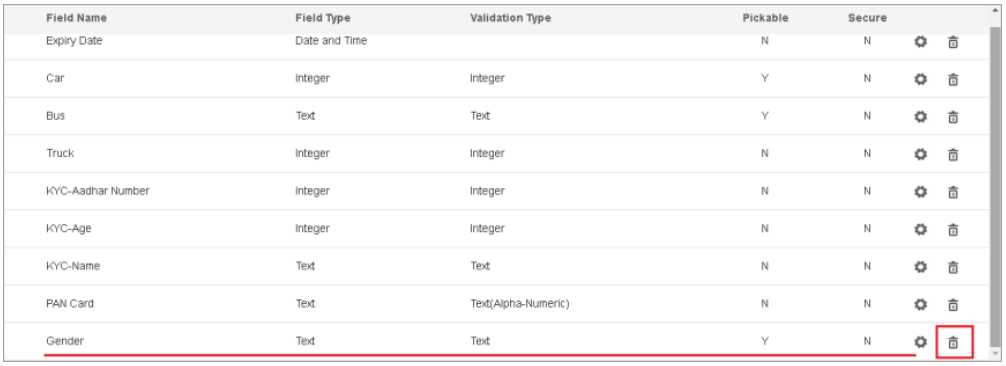
    iv. **To add groups to the Rights list:**
        • Select Groups from the Groups/Users/Roles dropdown list.
        • Select or Type Group name in the associated combo box.
    v. **To add roles to the Rights list:**
        • Select the Role from the Groups/Users/Roles dropdown list.
        • Select or Type Group name in the associated combo box.
        • Select or Type User Name in the associated combo box.
    vi. As you select a User, Group or Role, it gets added to the Rights list.
    vii. **To remove Users/Groups/Roles from the Rights list:**
        • To remove a single rights holder, click on the Remove button against the rights holder.
        • To remove multiple Users/Groups/Roles, select the required Users/Groups/Roles.
        • Click on the Delete button that appears after selecting two or more names.
    viii. Click on **Save** to save the defined picklist values.
        • You can click on **Back** (top-left corner) to return to the Create Field dialog box.

ix. On saving, a message “Global index modified successfully” appears.

Delete global index

To Delete a Global Index:

1. Click on the **Delete Field** button against the Global Index to be deleted.



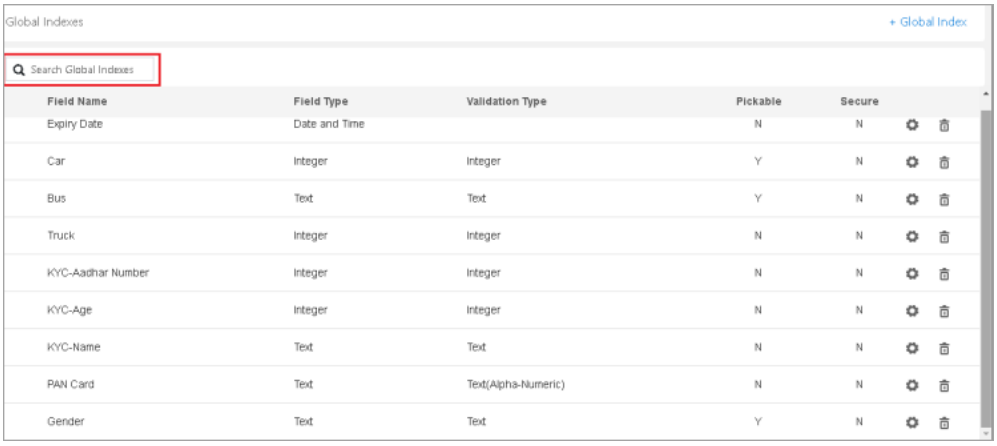
Field Name	Field Type	Validation Type	Pickable	Secure
Expiry Date	Date and Time		N	N
Car	Integer	Integer	Y	N
Bus	Text	Text	Y	N
Truck	Integer	Integer	N	N
KYC-Aadhar Number	Integer	Integer	N	N
KYC-Age	Integer	Integer	N	N
KYC-Name	Text	Text	N	N
PAN Card	Text	Text(Alpha-Numeric)	N	N
Gender	Text	Text	Y	N

2. An alert message appears.
3. Click on **Confirm** to confirm the deletion.
4. A message “**Global Index deleted successfully**” appears.

Search for global indexes

To search for Global Indexes:

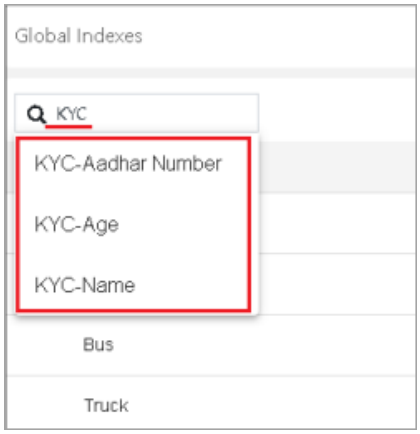
1. Click in the **Search Global Indexes** search text box.



Field Name	Field Type	Validation Type	Pickable	Secure
Expiry Date	Date and Time		N	N
Car	Integer	Integer	Y	N
Bus	Text	Text	Y	N
Truck	Integer	Integer	N	N
KYC-Aadhar Number	Integer	Integer	N	N
KYC-Age	Integer	Integer	N	N
KYC-Name	Text	Text	N	N
PAN Card	Text	Text(Alpha-Numeric)	N	N
Gender	Text	Text	Y	N

2. Enter the Global Index name to search for.

3. As you type the characters, the un-matching names keep on disappearing and in the end, only matched names are left in the dropdown list.



Working with keywords

Keywords are the words that you associate with a document. These help in fast and a quick retrieval of documents. The keywords are of two types:

- Authorized Keywords
- UnAuthorized Keywords

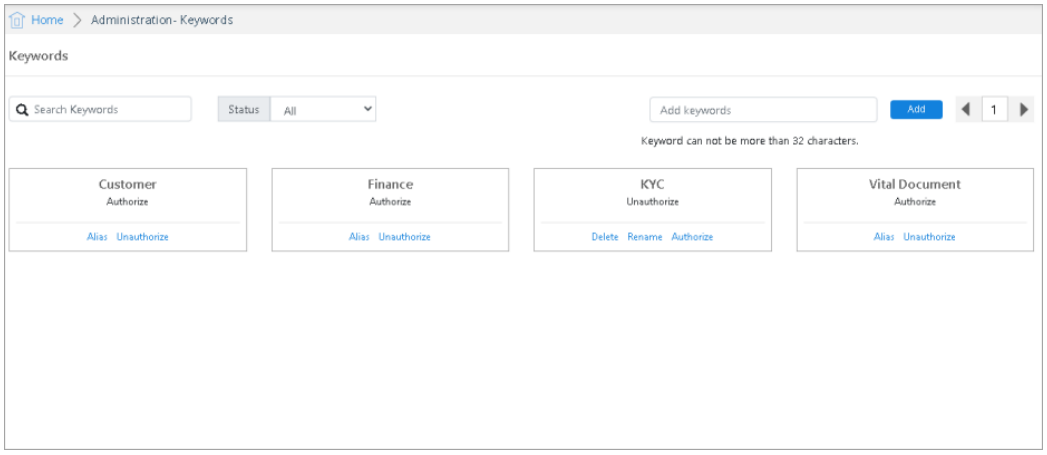
The OmniDocs Admin helps to create only the Authorized keywords that can be attached with the various documents.

You can perform the following operations on the keywords using OmniDocs Admin:

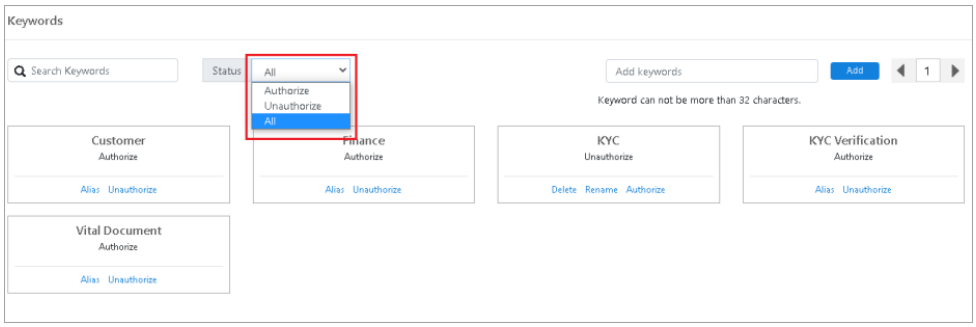
- Add keywords
- Modify the status of keywords from Authorized to UnAuthorized and vice-versa
- Add/Delete Alias for Authorized keywords
- Rename UnAuthorized keywords
- Delete UnAuthorized keywords

To Access Keywords:

1. In the home screen of OmniDocs Admin, go to **Administration** tile and click on the **Keywords** link.
2. Keywords screen appears. It shows the existing keywords.



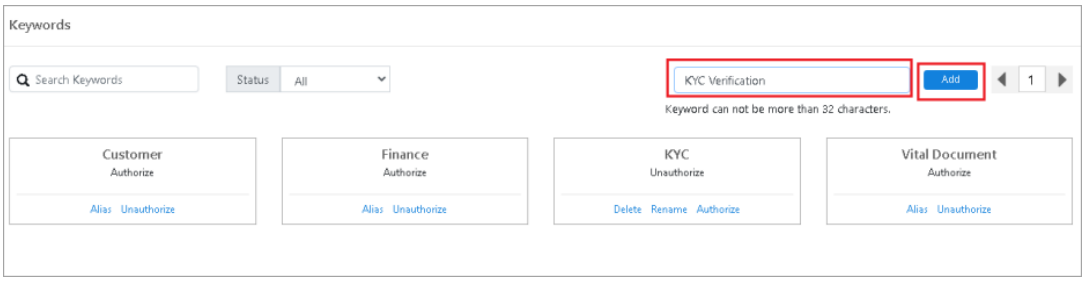
3. Click on the Status dropdown list and choose:
   - **Authorize**: To view the authorized keywords
   - **Unauthorize**: To view the unauthorized keywords
   - **All**: To view all the keywords



Adding keywords

To Add a Keyword:

1. Enter the keyword and click on **Add** button.

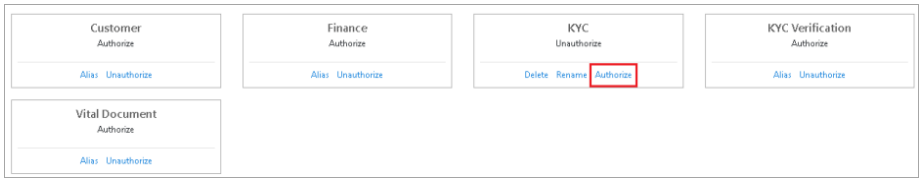


2. A message “Keyword added successfully” appears.
3. By default, the keyword you add is of Authorize type.

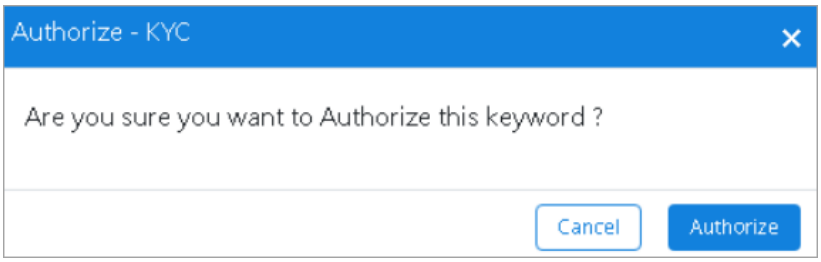
Modifying status of a keyword

To Modify the Status of a Keyword:

1. Go to the **Keywords** list.
2. Depending on the status of the keyword, you can click on:
   - Authorize to change the keyword status from unauthorize to authorize.
     - A dialog box to confirm the selection appears.

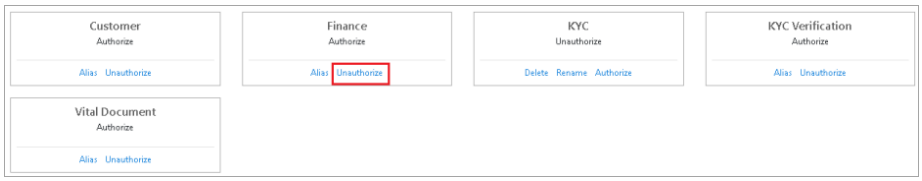


     - Click on **Authorize** to confirm.

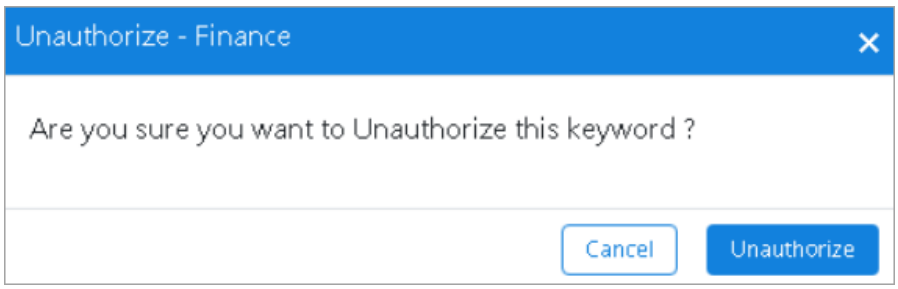


     - A message “Status changed successfully” appears.
   - Unauthorize to change the keyword status from unauthorize to authorize.

- A dialog box to confirm the selection appears.



- Click on **Unauthorize** to confirm.

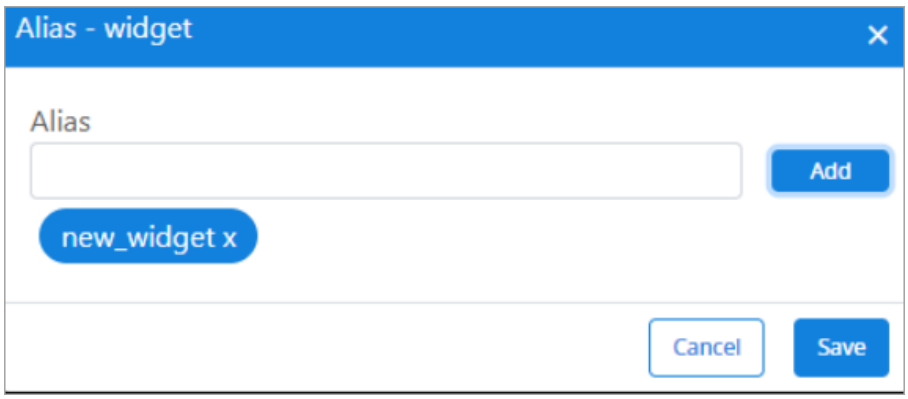


- A message “Status changed successfully” appears.

Adding or deleting alias for authorized keywords

To Create an Alias for an Authorized keyword:

1. Go to the **Keywords** list.
2. Select a Keyword, which has authorized status.
3. Click on the **Alias** link. Add Alias dialog box appears.
4. Specify the **Alias** name for the keyword.
5. Now, click the **Add** button.

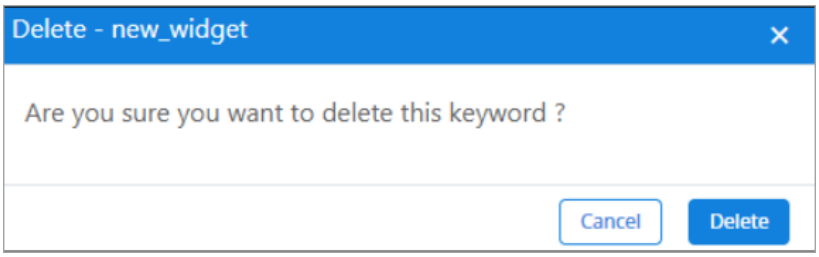


6. The Alias list shows the alias names you have added to a keyword in batches.
7. Repeat steps 4 and 5 to continue adding alias names to the keyword.
8. Click on **Save** to save the alias names.

All alias names that you add to a keyword are shown in the Keyword list as Authorized keywords. You can also create alias names for an UnAuthorized keyword by modifying the status of the UnAuthorized keyword to Authorized keyword.

To Delete Alias Names from the Alias list on the Add Alias screen:

1. Select the **Alias** names from the Alias list on the Add Alias screen.
2. If the alias is authorized, then you must unauthorize that alias first.
3. Click on **Delete**.



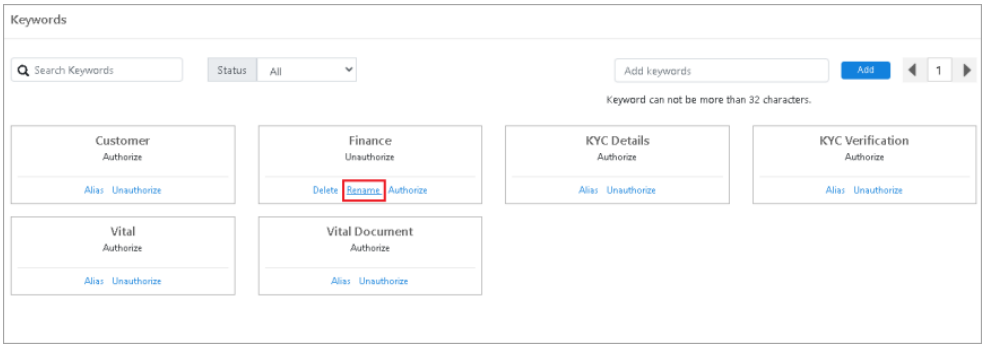
4. A message “Keyword deleted successfully” appears.

Besides the keywords, the alias names that you create for a keyword are added to the Keyword list as distinct keywords. When you delete an alias of a keyword from the Alias list of the Add Alias screen, the alias name is not deleted from the Keyword list.

Renaming an unauthorized keyword

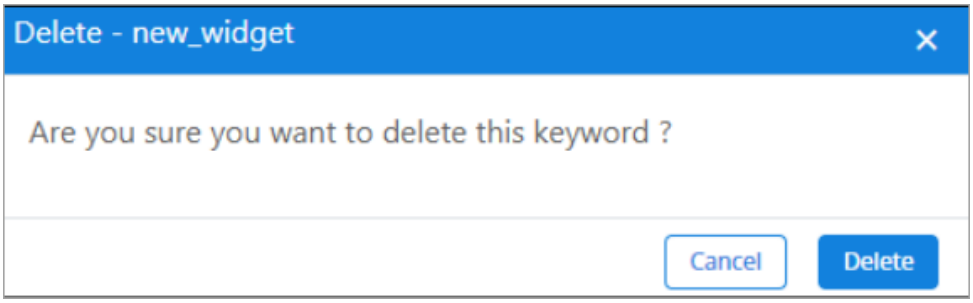
To Rename an Unauthorized Keyword:

1. Select an **Unauthorized keyword** from the Keyword list.
2. The Delete, Rename and Authorize links are available.
3. Click on **Rename** link.



4. Rename Keyword screen appears, showing the keyword name that you need to rename.

5. Type the new name for the keyword in the **New Name** text box.
6. Click on **Rename** to save the changes.



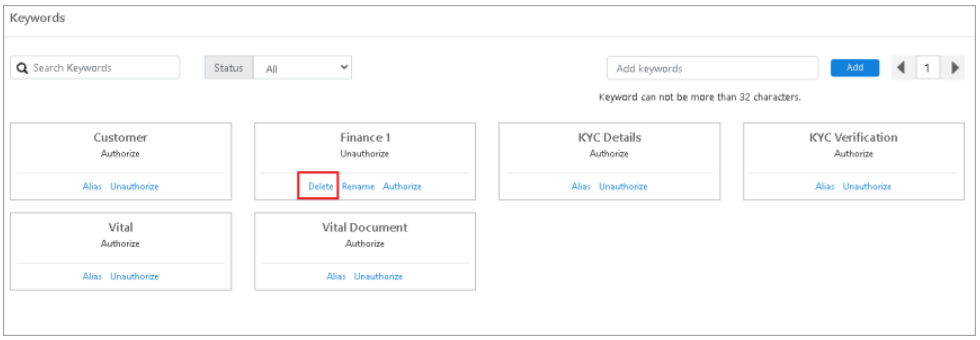
7. A message “Name changed successfully” appears.
8. If you click **Rename** on the Rename keyword screen, the old keyword name is removed from the Keyword Information screen, which shows the new name of the keyword.

> You can rename an Authorized keyword; by modifying the status of the Authorized keyword to UnAuthorized and then perform the Rename action on it.

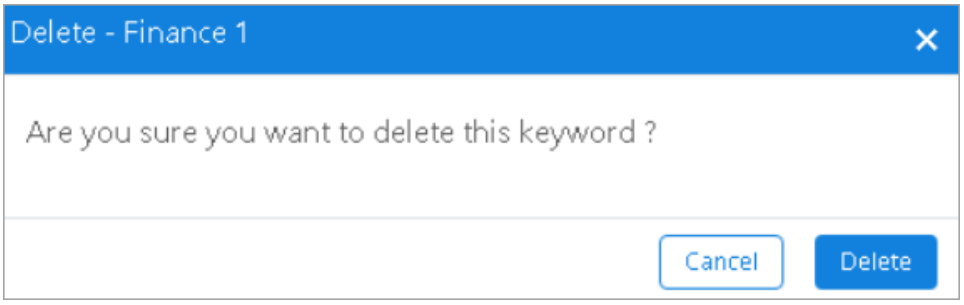
Deleting an unauthorized keyword

The OmniDocs Admin enables you to delete keywords associated with documents. You can delete only the UnAuthorized keywords. To delete a Keyword:

1. Select an **UnAuthorized keyword** from the Keyword list. The Delete, Rename and Authorize links are available.
2. Click on **Delete**.



3. Delete Confirmation dialog box appears.
4. Click on **Delete** to delete the Unauthorized keyword from the Keyword list.



5. A message “Keyword deleted successfully” appears.

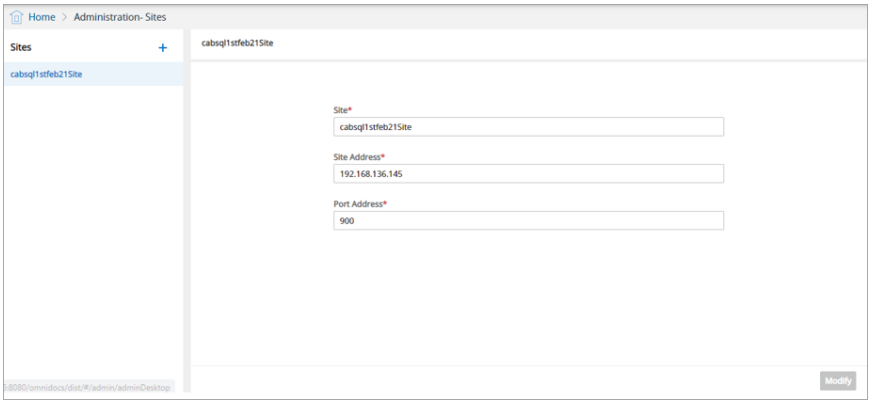
> You can delete an Authorized keyword, by modifying the status of the Authorized keyword to UnAuthorized and then perform the Delete action on it.

Sites

A site represents an SMS. A site is identified by two attributes: SMS IP (the IP of the Server where SMS is running) and SMS Port (the Port on which SMS is listening). A site serves as a repository for volumes, each consisting of multiple volblocks. Site name serves as a logical name for identifying sites. Home site for any volume is the site where that volume was originally added. If a volume is replicated on some other site(s) then the site in which it is originally added is the home site and the site(s) where the volume is replicated are the replicate site(s).

To Access Sites:

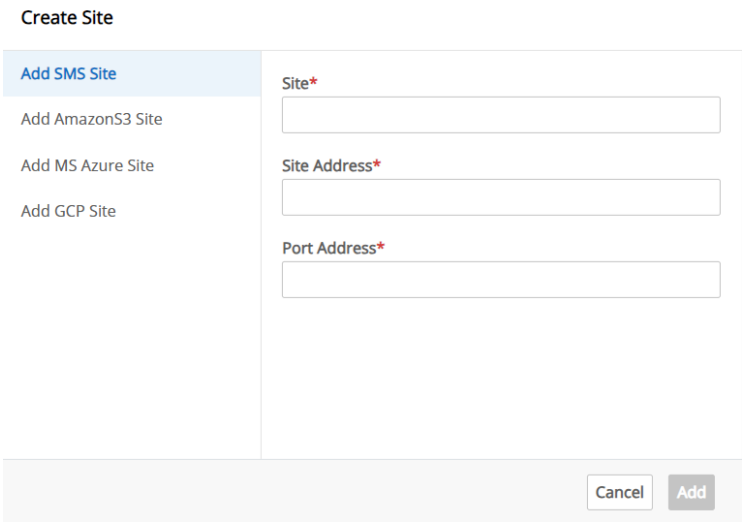
1. In the home screen of OmniDocs Admin, go to **Administration** tile and click on the **Sites** link.
2. Sites screen appears. The left pane shows the already added sites and the right pane shows the properties of the selected site.



Adding sites

To Add a New Site:

1. To add a new site, click on **+** (**Add Site**) icon.
2. Create Site dialog box appears.
3. Click on:
   - **Add SMS Site** to add a new SMS Site.
   - **Add Amazon S3 Site** to add a new Amazon S3 Site.
   - **Add GCP Site** to add a new GCP Site.
   - **Add MS Azure Site** to add a new MS Azure Site.



Add SMS site

To Add a New SMS Site:

1. Click on **Add SMS Site** link from the left pane and specify the following details:
   - **Site:** Name of the new site.
   - **Site Address:** The IP of the machine where the SMS server is running.
   - **Port Address:** The port address on which the SMS Server is running.
2. Click on **Add** to save the entered details. A message “Site successfully created” appears.

To create a volume based on the registered SMS site, refer to the section Volumes.

Add Amazon S3 site

To Add a New Site at Amazon S3 Server:

1. Click on **Add Amazon S3 Site** link from the left pane and specify the following details:
   - **Site:** Name of the new Amazon S3 site.
   - **Role Based:** Select/unselect the checkbox to enable or disable the role-based access on Amazon S3 bucket.
   - **Region:** The Region textbox gets enabled on selecting the Role Based checkbox. Provide a value for the region. Example: US-East-1
   - **Access Key:** Provide the AWS Access Key.
   - **Secret Key:** Provide the AWS Secret Key.
2. Click on **Add** to save the entered details. A message “Site successfully created” appears.

To create a volume based on the registered Amazon S3 site, refer to the section Volumes.

Add GCP site

To Add a New Site on GCP Server:

1. Click on the **Add GCP Site** link from the left pane and specify the following details:
   - **Site:** Name of the new HCP site.
   - **Access Key:** Provide the AWS Access Key.
   - **Secret Key:** Provide the AWS Secret Key.
2. Click on **Add** to save the entered details. A message “Site successfully created” appears.

To create a volume based on the registered GCP site, refer to the section Volumes.

Add Azure site

To Add a New Site on Microsoft Azure Server:

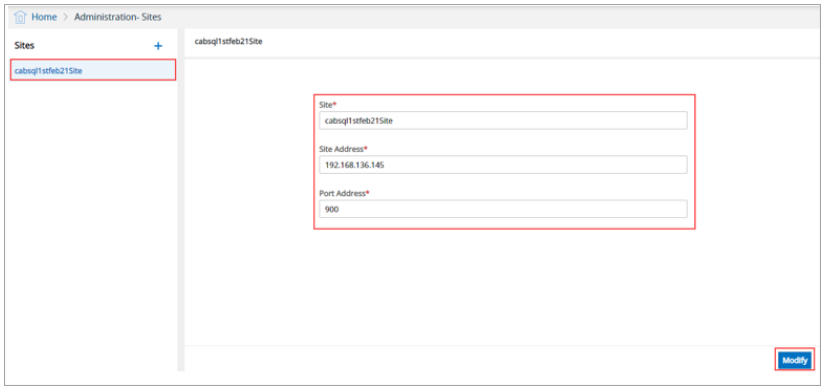
1. Click on **Add MS Azure Site** link from the left pane and specify the following details:
   - **Site:** Name of the new Azure site.
   - **Account Name:** Provide the Azure Account ID.
   - **Account Key:** Provide the Azure Account Password.
2. Click on **Add** to save the entered details. A message “Site successfully created” appears.

To create a volume based on the registered Azure site, refer to the section Volumes.

Modifying sites

To Modify a Site:

1. Go to **Sites**.
2. Open the site to modify.
3. Modify the Site details as required and click on **Modify**.

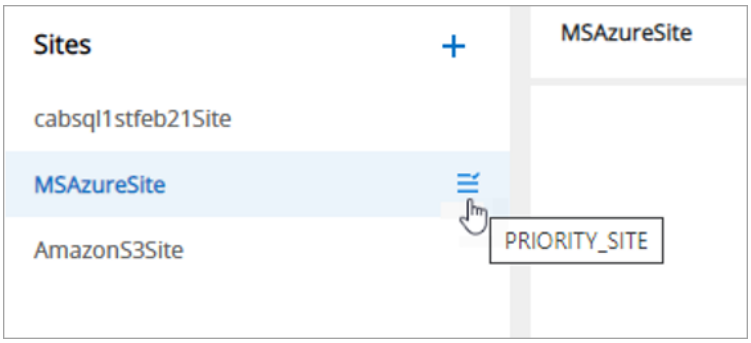


4. A message “Site Modified Successfully” appears.

Make priority site

To Make a Site as Priority Site:

1. Go to the **Sites** list.
2. Hover over the site that you want to mark as the priority site.
3. Click on the **MAKE_PRIORITY_SITE** button.
4. A message “<Site Name> is made the preferred site successfully” appears.



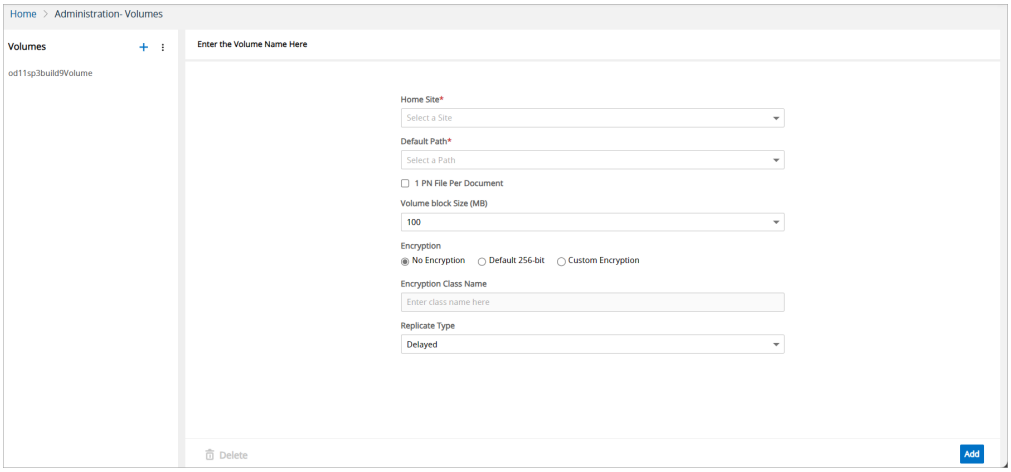
5. The selected site is now marked as PRIORITY_SITE.

Volumes

A volume is a logical unit, which can have multiple volume blocks. Image storage at a particular Site is divided into logical storage units called image volumes. An image volume is used to group several image-volume blocks where each image volume block corresponds to a document data file, which is a group of one or more document files concatenated. There is no limit on the physical storage occupied by an image volume. Every volume has a default volume path, which is a label on SMS, which corresponds to a physical location on SMS.

To Access Volumes:

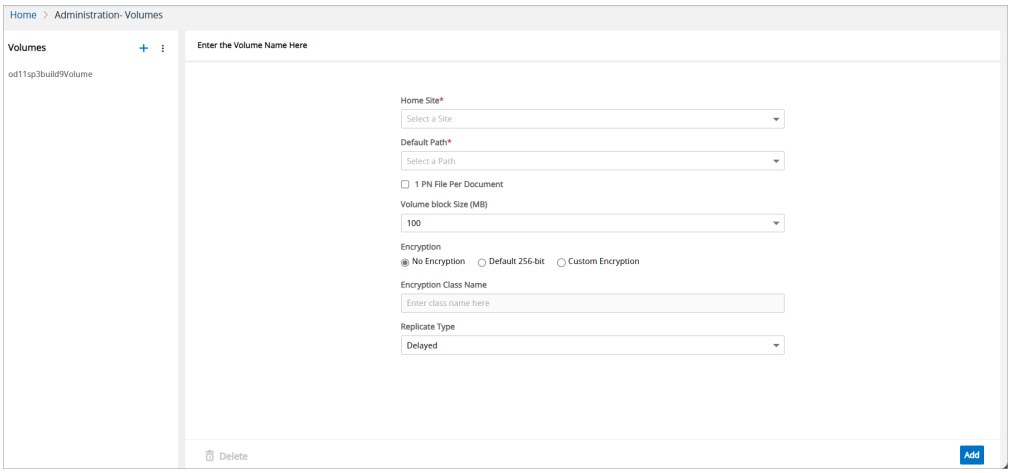
1. In the home screen of OmniDocs Admin, go to **Administration** tile and click on the **Volumes** link.
2. Volumes screen appears. The left pane shows the already added Volumes and the right pane shows the properties of the selected Volume.



Creating volume

To Create an Image Volume:

1. On the Volumes screen, click the **+ (Add Volumes)** link. The screen to add a new Volume appears.



2. Specify the following details:

Fields	Description
Enter the Volume Name Here	Enter a new volume name in Enter the Volume Name Here text box.
Home Site	Select a home site from the dropdown list, which includes registered sites for SMS, Amazon S3, GCP, and MS Azure storage. For details on the site registration, refer to the section Sites.

Fields	Description
Default Path	Choose the default path from the list. The options change based on your selected Home Path as: • SMS: for storing data on an SMS site • Bucket: for Amazon S3 storage • GCP bucket: for Google Cloud Platform storage • Azure Blob Storage: for Microsoft Azure storage
1 PN File Per Document	Select this checkbox to store only one file per physical node (PN) for each document, ensuring that each document is saved in a separate PN file.
Volume block Size (MB)	Select a volume block size from the Volume block Size (MB) dropdown list.
Encryption	Select Encryption type from the below options: • No Encryption • Default 256-bit • Custom Encryption: If this option is selected, then you must provide the Encryption Class Name.
Encryption Class Name	This field enables if you have selected the above Encryption options as Custom Encryption.
Replication Type	Select a replication type from the Replication Type dropdown list. Select one of the following options: • Immediate • Delayed

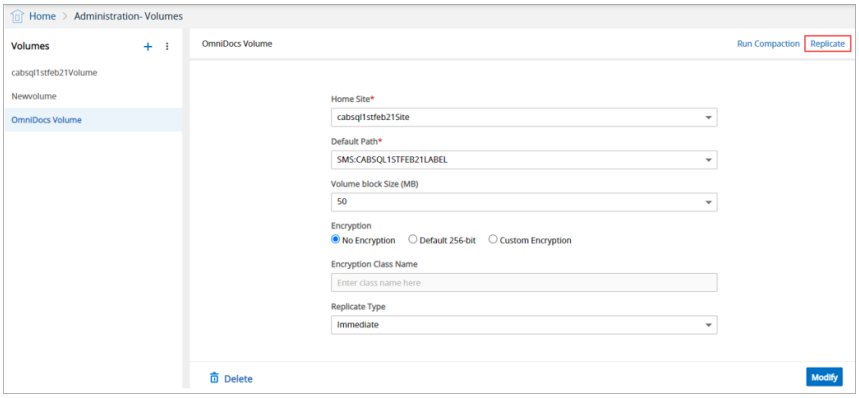
3. Click **Add** to save the specified details. The message “Volume added successfully” appears.

- If Custom Encryption option is selected and the Encryption Class Name is not mentioned, then Volume will be encrypted using the default encryption method. If the Encryption Class Name is specified, then the Volume will be encrypted using the custom-defined encryption method.
- While adding a new volume, users can select the Custom Encryption option to encrypt the volume.
- Once Custom Encryption option is selected or cleared, then users cannot modify it later. Option to change this property is disabled and its value remains the same as set while adding the volume.

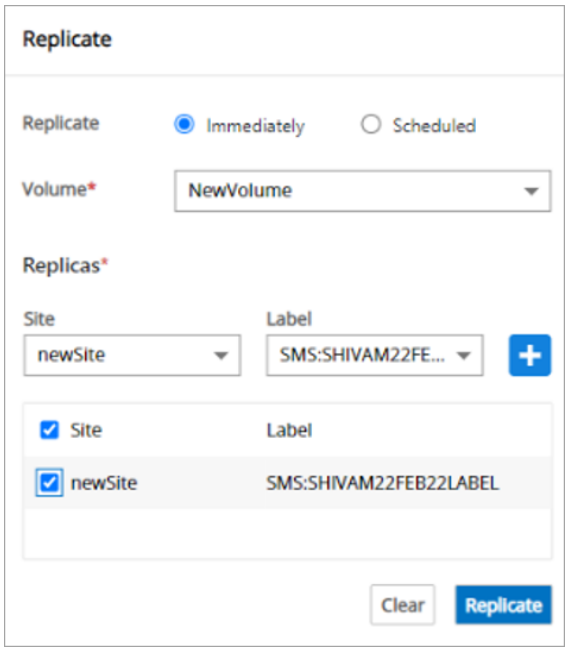
Replicating volume

To Replicate a Volume:

1. Open the properties of a Volume.
2. Click the **Replicate link** to create replica(s) of the selected volume. The Replicate dialog box appears.



3. Select the **Replicate** method between **Immediately** and **Scheduled**.
   - **Immediately**
     a. Select a Volume from the dropdown list.
     b. In Replicas section:
        a. Select a Site on which the selected volume must be replicated.



        b. Select a Label for the selected volume site.

c. Click on (Add) icon to add it to the Replica Site(s) list.

c. Select the site where volume needs to be replicated.

d. Click on **Replicate** to replicate the selected volume. The message "Replication successful" appears.

- **Scheduled**

a. Enter a new **Job Name**.

b. Select a **Volume** from the dropdown list.

c. In the **Replicas** section:

   a. Select a **Site** on which the selected volume must be replicated.

   b. Select a **Label** for the selected volume site.

   c. Click on **(Add)** icon to add it to the Replica Site(s) list.

d. Specify the Schedule details as follows:

   - Frequency (in days)
   - Time (in HH:MM)
   - Execute for (in hours)
   - Polling Interval (in HH And/Or MM)

e. Click on **Add Job**.

f. Once added, it will be shown in the **Manage Jobs** section, in the right pane.

g. Manage Jobs allows you to:

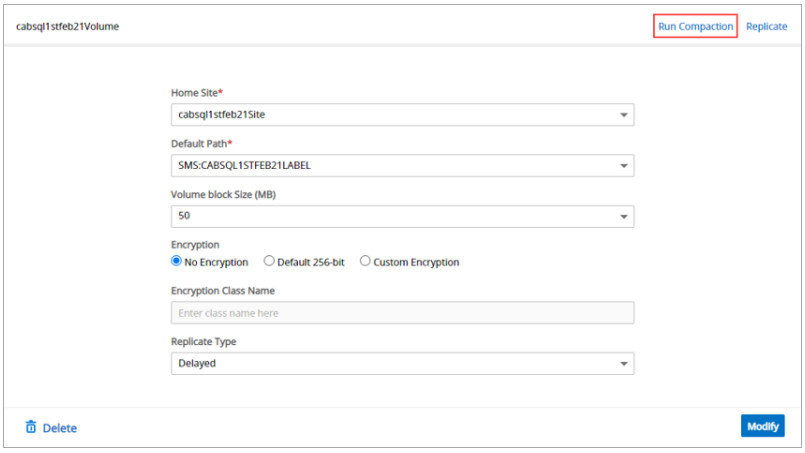
   - View the last execution time, execution start time, execution end time, and status.
   - **Modify** and **Delete** the added job.

Running compaction

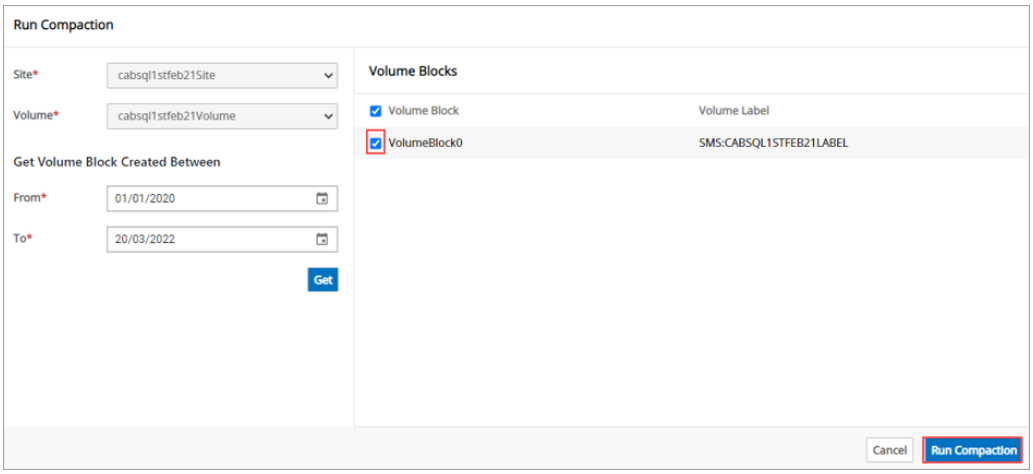
To Compact Volumes:

Volume compaction is the release of unused disk space occupied by the volume. Delete document functionality of the image server API marks a document for deletion and does not releases the physical space. The task of revoking the unused space is done during volume compaction.

1. Open the properties of a Volume.
2. Click on **Run Compaction**. The Run Compaction dialog box appears.



3. Set the dates for **From** and **To** date fields.
4. Click on **Get** to get the list of volume blocks created between the selected dates.
5. The list of volume blocks appears in the right pane.
6. Select the required **Volume Block** and click on **Run Compaction**.

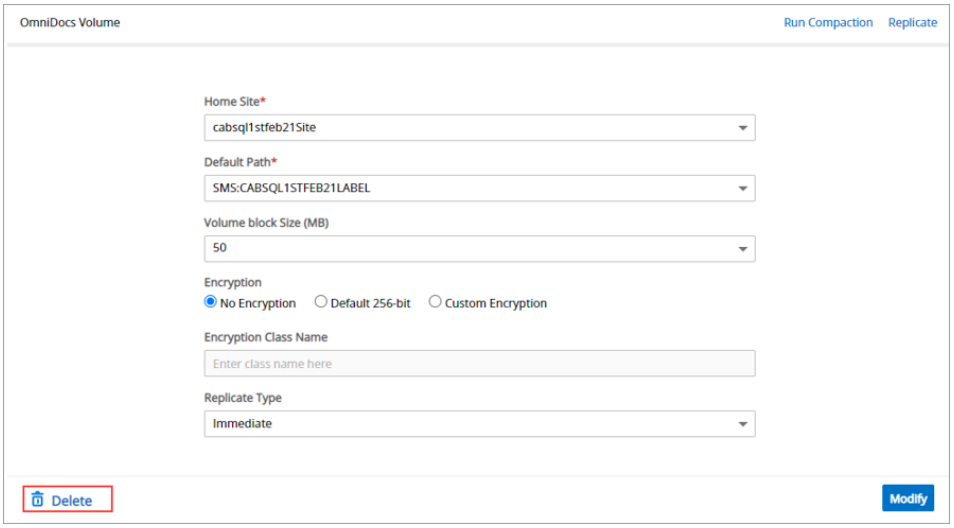


7. A message “Volume Compacted Successfully” appears.

Deleting volume

To Delete a Volume:

1. Select the volume that needs to be deleted.
2. The properties of the selected Volume appear in the right pane.
3. Click on **Delete**. The message “Volume deleted successfully” appears.

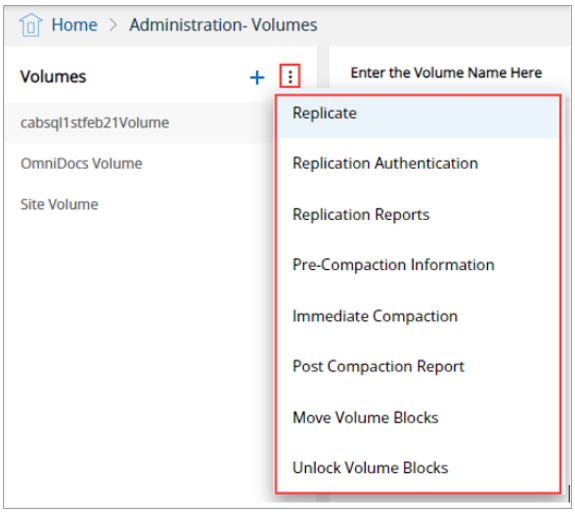


Cases when a Volume cannot be deleted:

- If the selected volume is the default volume of the cabinet, then it cannot be deleted. When you try to delete this volume, a message box appears that says “Volume has been associated with the cabinet”.
- If the selected volume consists of some documents, then it cannot be deleted. When you try to delete this volume, a message box appears that says “This volume contains some documents. Volume cannot be deleted”.
- To delete such a volume, you need to permanently delete all the documents lying in the selected volume by pressing the **Shift +Delete** keys.

Volume properties

Volume Properties can be accessed through the ellipsis button along with Add Volume button.



Replicate

To Create Replication of a Volume:

1. Click on **Replicate** using the ellipsis button. The Replicate dialog box appears.
2. The remaining steps are the same as that of Replicate Volume (step 3 onwards).

Replication authentication

To Add Replication Authentication to a Volume:

1. Click on **Replication Authentication** using the ellipsis button. The Replication Authentication dialog box appears.
2. Fill out the details:
   - Username — Enter the username.
   - Password — Enter the password associated with the username.
   - Retry Count — Enter the password retry count.

- Retry Interval (sec) — Enter the retry interval time in seconds.

3. Click on **Save** to save the entered authentication details.

Pre-compaction information

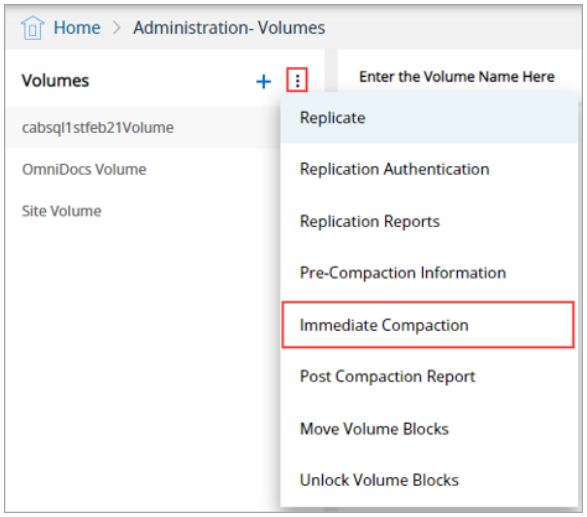
To View Pre-Compaction Information:

1. Click on **Pre-Compaction Information** using the ellipsis button. The Pre-Compaction Information dialog box appears.
2. After viewing the information, you can click on the **Cancel button** to close the dialog box.

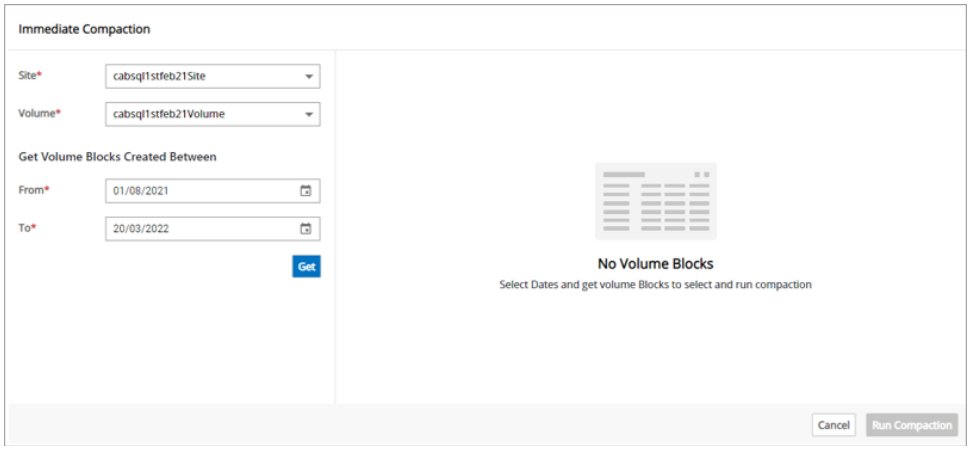
Immediate compaction

To Run Immediate Compaction:

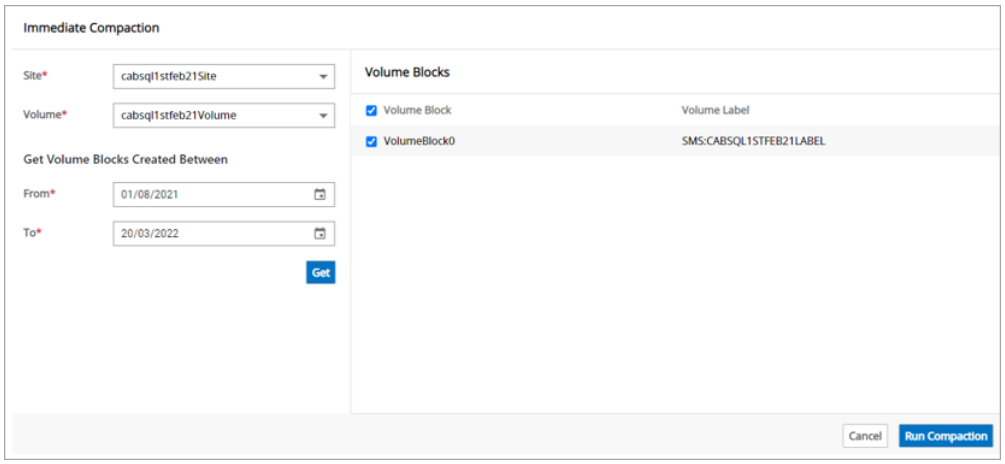
1. Click on **Immediate Compaction** using the ellipsis button.



2. Immediate Compaction dialog box appears.
3. Select **Site** and **Volume** from the respective dropdown lists.
4. Set the dates for **From** and **To** date fields.
5. Click on **Get** to get the list of volume blocks created between the selected dates.



6. The list of volume blocks appears in the right pane.
7. Select the required **Volume Block** and click on **Run Compaction**.

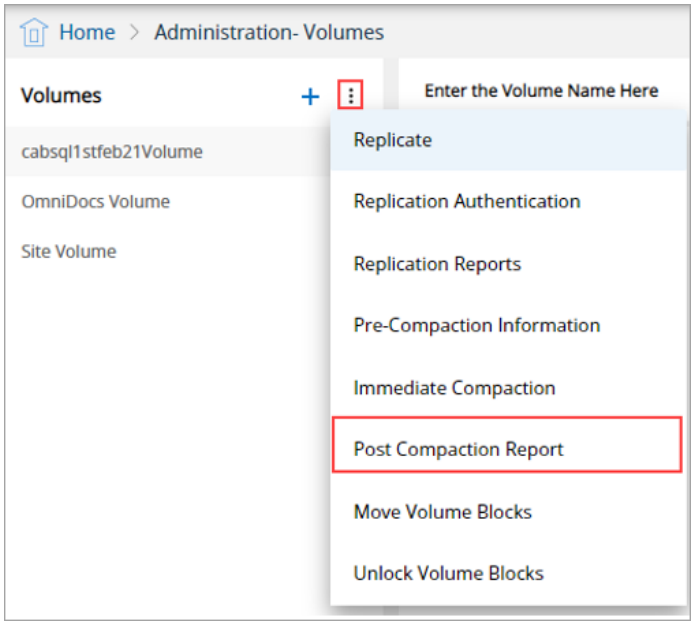


8. A message “Volume Compacted Successfully” appears.

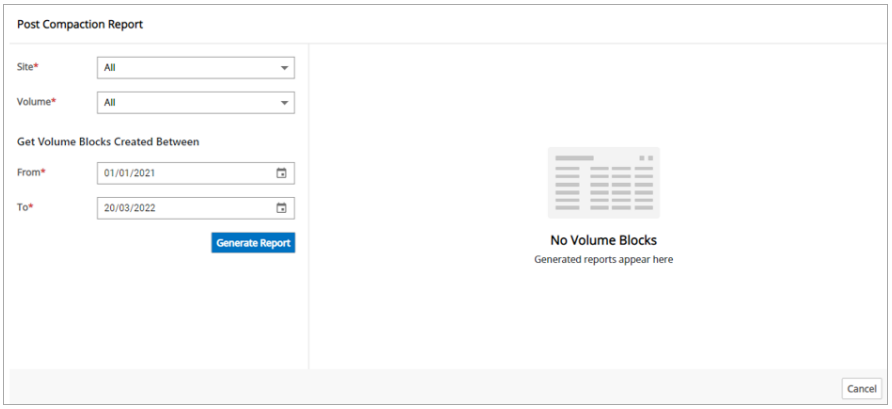
Post compaction report

To View Post Compaction Report:

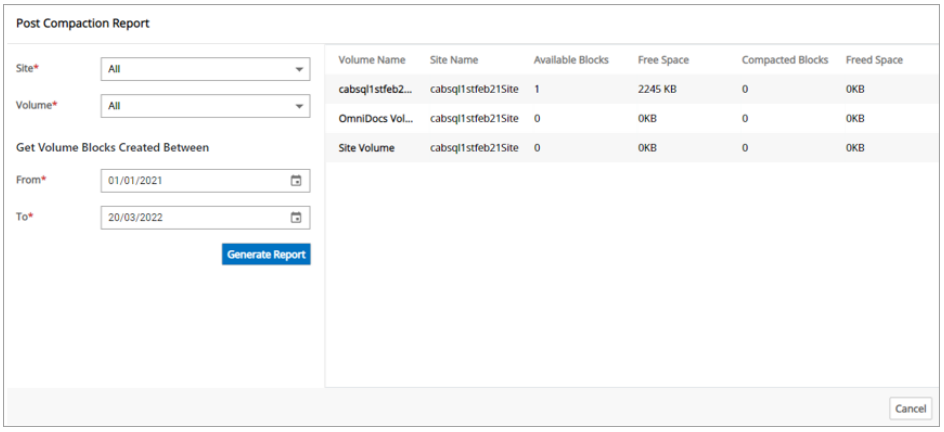
1. Click on **Post Compaction Report** using the ellipsis button.



2. Post Compaction Report dialog box appears.
3. Select **Site** and **Volume** from the respective dropdown lists.
4. Set the dates for **From** and **To** date fields.
5. Click on **Generate Report** to view the post-compaction report.



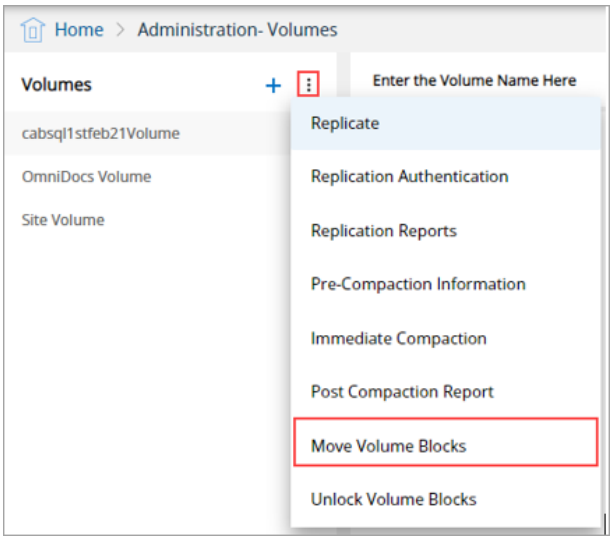
6. The post-compaction report appears in the right pane.
7. After viewing the report, you can click on the **Cancel** button to close the dialog box.



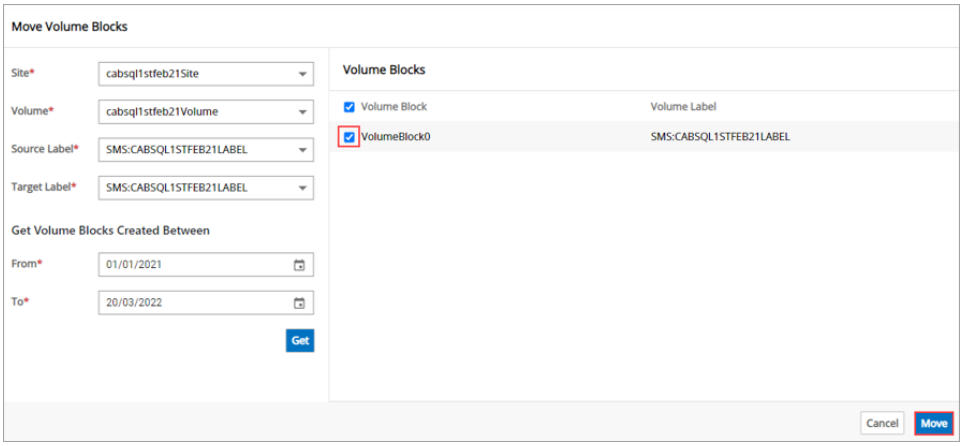
Move volume blocks

To Move Volume Blocks:

1. Click on **Move Volume Blocks** using the ellipsis button.



2. Move Volume Blocks dialog box appears.
3. Select **Site** and **Volume** from the respective dropdown lists.
4. Select the **Source Label** and **Target Label** to move the blocks from one label to another label.
5. Set the dates for **From** and **To** date fields.
6. Click on **Get**.
7. The list of volume blocks available in the Source Label appears.
8. Select the required volumes and click on **Move**.

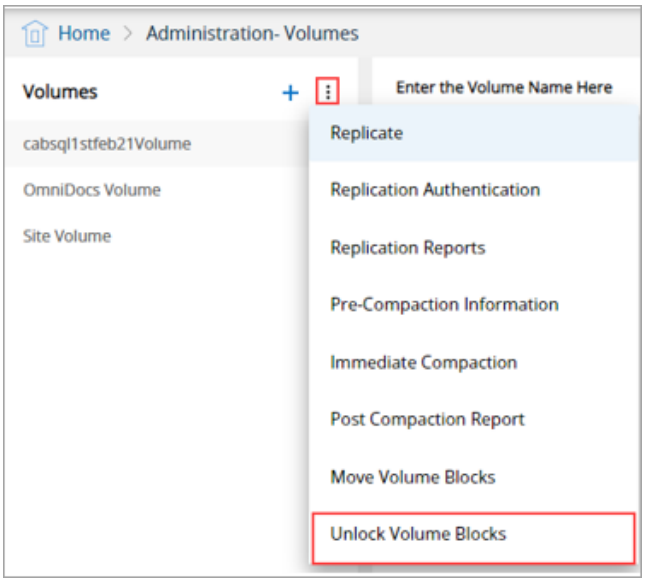


9. A message “Blocks have been moved successfully” appears.

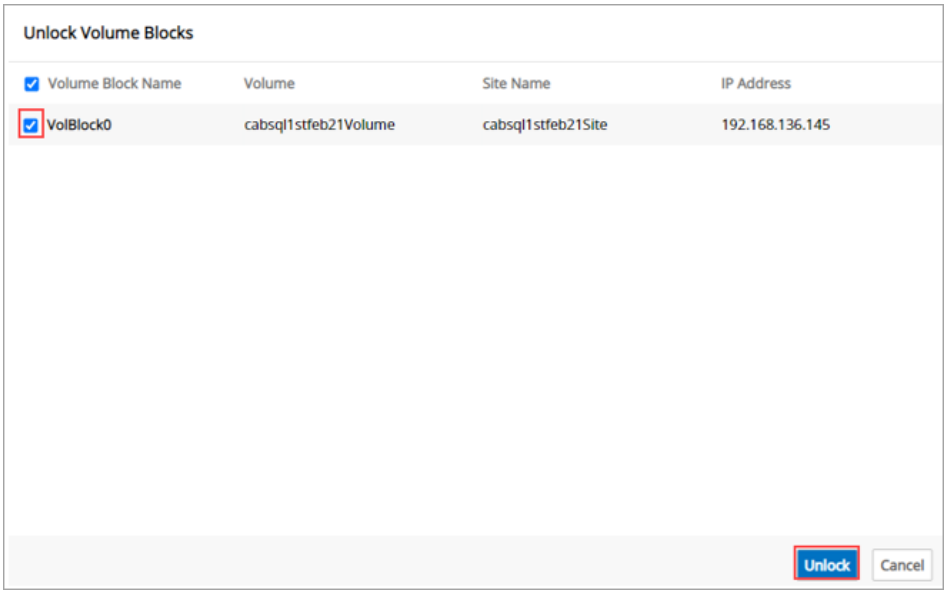
Unlock volume blocks

To Unlock Volume Blocks:

1. Click **Unlock Volume Blocks** using the ellipsis button.



2. Unblock Volume Blocks dialog box appears. It shows a list of all the locked volume blocks.
3. Select the desired volume block and click **Unlock** to unlock it.



4. A message “Successfully unlocked volume” appears.

Maker checker

Maker-checker (or Maker and Checker) is one of the central principles of authorization in the Information Systems of financial organizations. In the Maker Checker feature, for each transaction, there must be at least two individuals necessary for its completion. While one individual may create a transaction, the other individual should be involved in Confirmation or Authorization of the same. Here, the segregation of duties plays an important role. In this way, strict control is kept over system software and data thus bringing OmniDocs Administrative operations under the preview of Dual-Authorization i.e., Maker and Checker to strengthen the security of DMS.

The operations that come under the preview of Maker-Checker are:

- Add User
- Add Group
- Add Role
- Modify User Properties
- Modify Group Properties
- Modify Role Properties
- Delete User
- Delete Group
- Delete a Role

Some of the key features of Maker-Checker are:

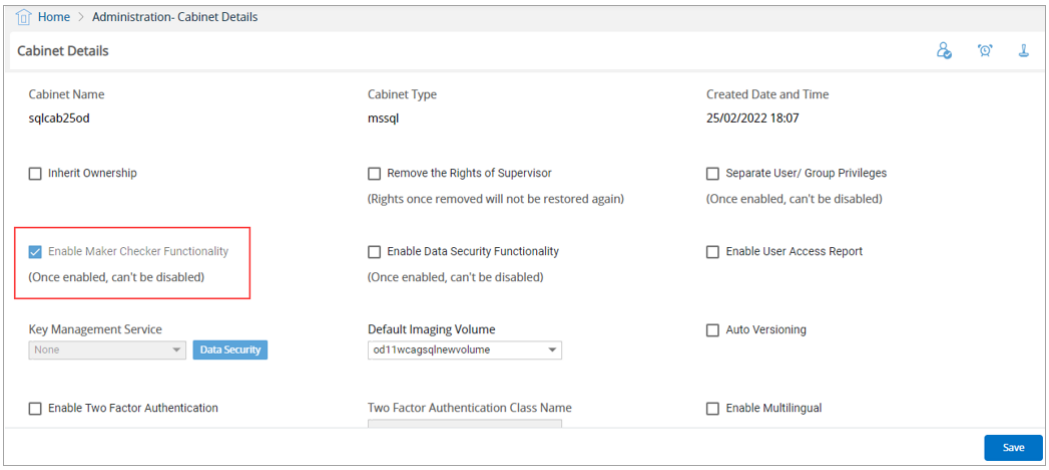
- Maker and Checker users have been differentiated on the basis of privileges.
- For a single request, Maker and Checker cannot be the same.
- The maker will initiate the request for change and Checker or the user having Checker privilege can approve/reject the request.

- Request once accepted by Checker will be reflected as a change in the system. Also, for all rejected requests, the Checker must state the reason for disapproval.
- Requests once sent by any Maker can be approved by any Checker and in case, he rejects the request then he should state the reason for rejection in comments.
- For every Request Made for verification by Maker User and every request verified by Checker, auditing is done.

To Enable Maker Checker:

1. Go to **Administration** tile and click on the **Cabinet Details** link.
2. Mark the checkbox **Enable Maker Checker Functionality**.

Once Maker Checker is enabled, it can't be disabled.



Maker Checker ini Settings

S.No	Parameter Name	Values	Meaning
1	MakerChecker	0	Maker Checker functionality disabled.
		1	Maker Checker functionality enabled.
2	PendingRequestBatchSize	10	Depicts the batch size of the list. It can be modified according to user preference.
3	SentRequestBatchSize	10	Depicts the batch size of the list. Can be modified according to user preference.
4	OperatedRequestedBatchSize	10	Depicts the batch size of the list. Can be modified according to user preference.

After enabling the Maker Checker functionality, it appears in the Administration tile.

Maker requests

Adding/Modifying/Deleting a User:

While creating a user, when you click on **Create** after entering the required user details, a request for approval is sent to the checker and a message **Request has been sent for approval** appears.

Similarly, while modifying properties of an existing user such as password change, a request for approval is sent to the checker after clicking on Save.

Also, on deleting a user, the user deletion is sent for approval.

Adding/Modifying/Deleting a Group

While creating a Group, when you click on **Add** after entering the required group details, a request for approval is sent to the checker and a message **Request has been sent for approval** appears.

Similarly, while **modifying** group properties, a request for approval is sent to the checker after clicking on Save.

Also, on **deleting** a group, the group deletion is sent for approval.

Adding/Modifying/Deleting a Role:

While creating a Role, when you click on **Create** after entering the required role details, a request for approval is sent to the checker and a message **Request has been sent for approval** appears.

Similarly, while modifying role properties, a request for approval is sent to the checker after clicking on Save.

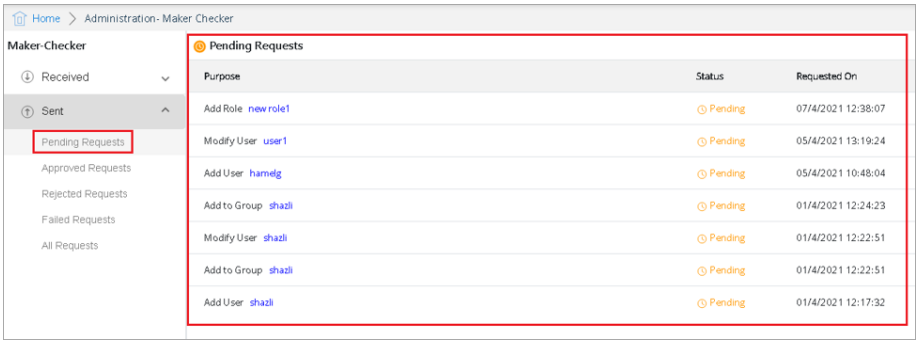
Also, on deleting a role, the role deletion is sent for approval.

To View the Sent Requests and Their Status

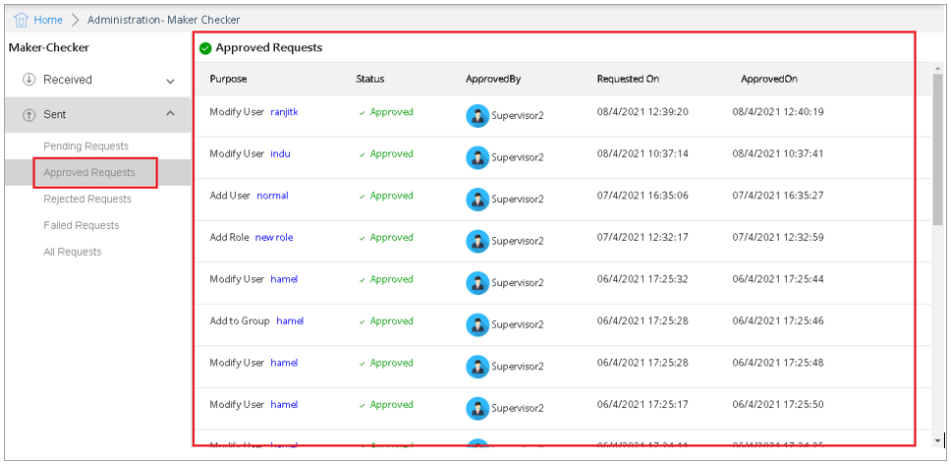
1. Go to the Home screen and click on the Maker Checker link.
2. Maker Checker screen appears.
    a. The left pane shows the following two tabs:
        - Received: It shows the different requests received by the Checker.

- Sent: It shows the different requests sent by the Maker.

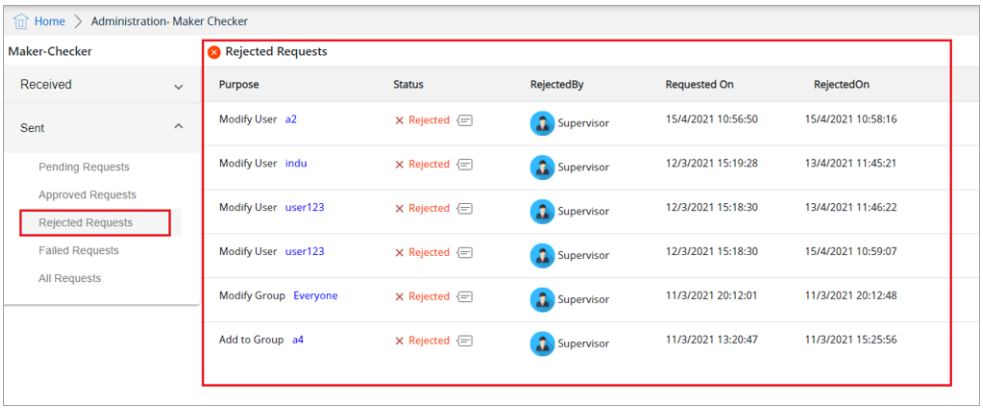
3. Click on the Sent tab. It displays the categorization as Pending Requests, Approved Requests, Rejected Requests, Failed Requests, and All Requests.
   a. Pending Requests are the requests that are still pending to be approved by the Checker. You can click on the hyperlinks to view the details.



   b. Approved Requests are the requests that are approved by the Checker. You can click on the hyperlinks to view the details.

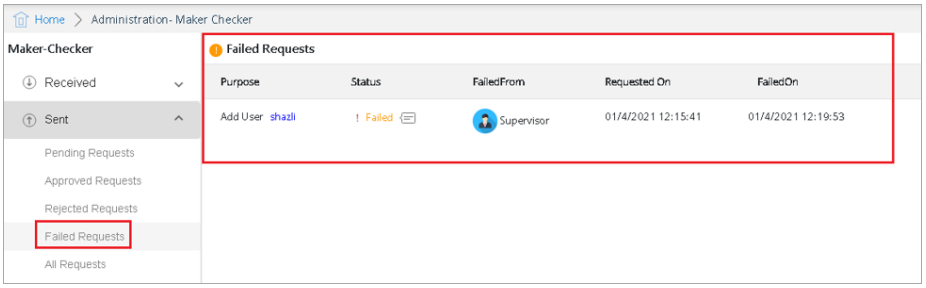


   c. Rejected Requests are the requests that are rejected by the Checker. You can click on the hyperlinks to view the details.

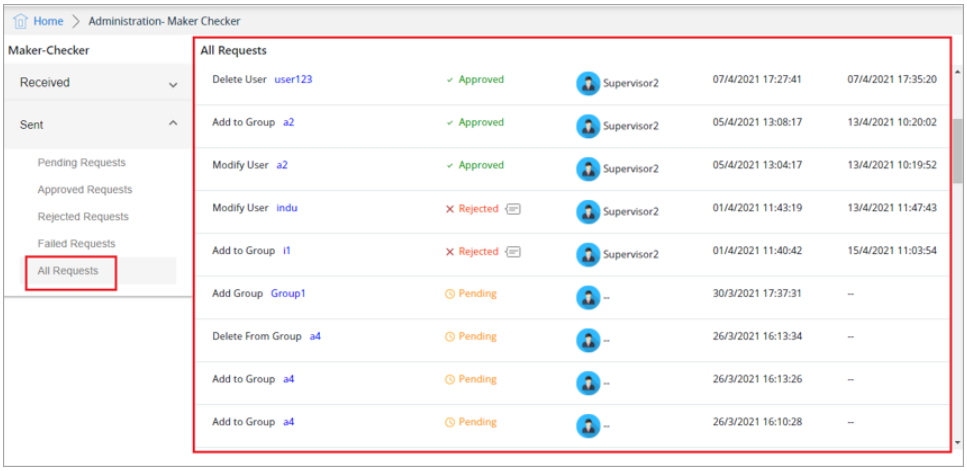


   d. Failed Requests: The same request sent to any other checker will get failed in case it has been approved by some checker. For example, a delete user

request is sent to two checker users. If one checker approves the request of deleting the user, then the other checker will not be able to take any action on the request as the user is already deleted from the system.



4. All Requests show a list of all the requests that are made by the maker to the checker. It also shows the status of all the requests.



Checker actions - approving and rejecting

The checker users can approve or reject the requests made by the maker users.

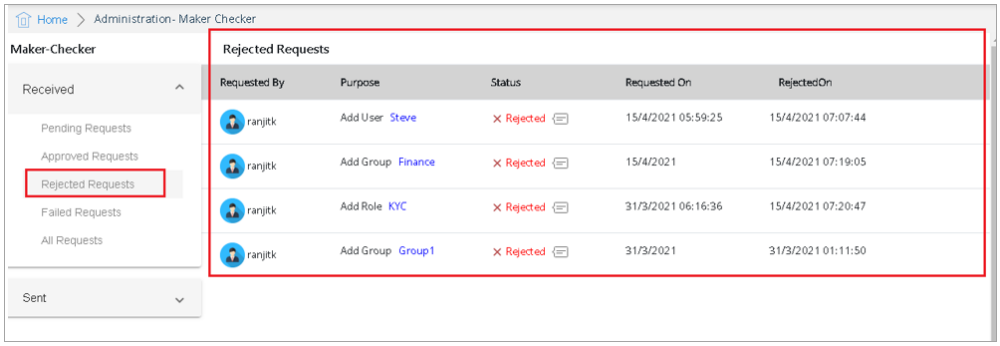
To View the Received Requests and Take Actions on them:

1. Login to **OmniDocs Admin** using the checker credentials.
2. Go to the Home screen and click on the **Maker Checker** link.
3. Maker Checker screen appears.
    a. The left pane shows the following two tabs:
        i. Received: It shows the different requests received by the Checker.
        ii. Sent: It shows the different requests sent by the Maker.
4. Click on the **Received** tab.

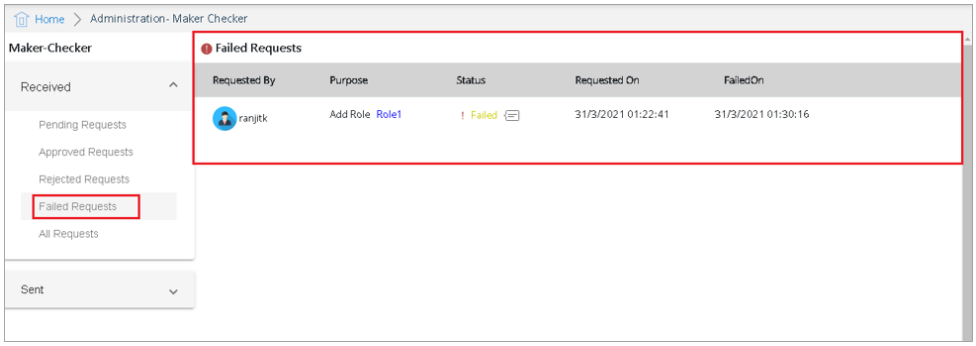
a. It displays the categorization as Pending Requests, Approved Requests, Rejected Requests, Failed Requests, and All Requests. By default, All Requests are shown.
    - Pending Requests are the requests that are still pending to be approved or rejected by the Checker.
        - To approve a request, click on **Approve** against the desired request, enter your reason for approval and click on **OK**.
        - On approval, a message “Request approved successfully” appears.
    - To reject a request, click on Reject against the desired request, enter your reason for rejection and click on **OK**.
        - On rejection, a message “Request rejected successfully” appears.

b. **Approved Requests** are the requests that are approved by the Checker. You can click on the hyperlinks to view the details.

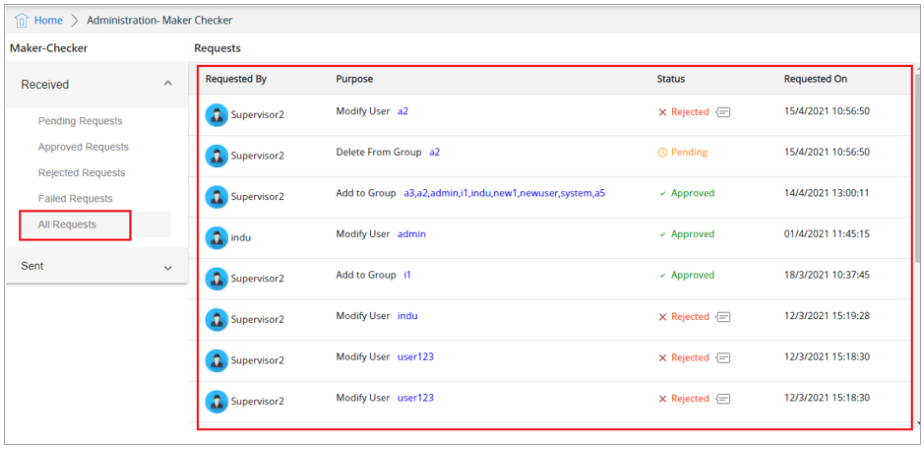
c. **Rejected Requests** are the requests that are rejected by the Checker. You can click on the hyperlinks to view the details.



d. **Failed Requests:** The same request sent to any other checker will get failed in case it has been approved by some checker. For example, a delete user request is sent to two checker users. If one checker approves the request of deleting the user, then the other checker will not be able to take any action on the request as the user is already deleted from the system.



e. **All Requests** show a list of all the requests that are handled by the checker. It also shows the status of all the requests.



Manage audit logs

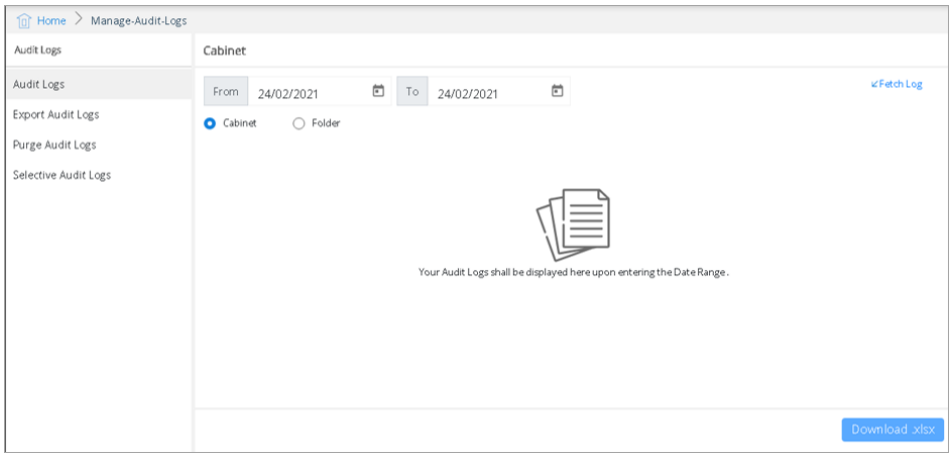
Audit Log is an account of the operations that are performed on the specified object (viz. cabinet, folder, or document) by any of the members of the cabinet.

Log can be generated for all operations Users perform in the System example, Login and Logout, adding Folders, changing Folder Properties, Uploading documents, etc. These logs are very useful for monitoring user activities.

The OmniDocs provides various enhancement features of Audit Trail that helps the OmniDocs Administrator select the user action for which the OmniDocs Administrator needs to generate an audit trail.

To Access Manage Audit Logs:

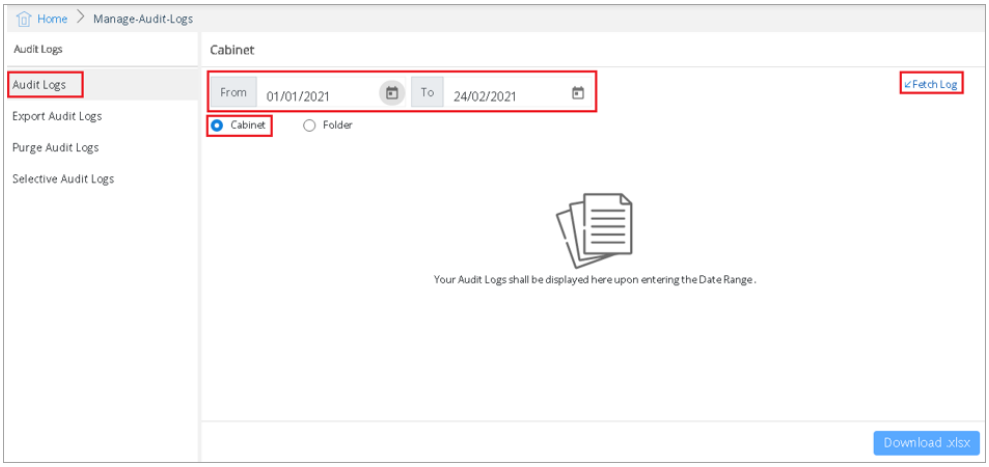
1. In the home screen of OmniDocs Admin, go to **Administration** tile and click on the **Manage Audit Logs** link.
2. Manage Audit Logs screen appears.



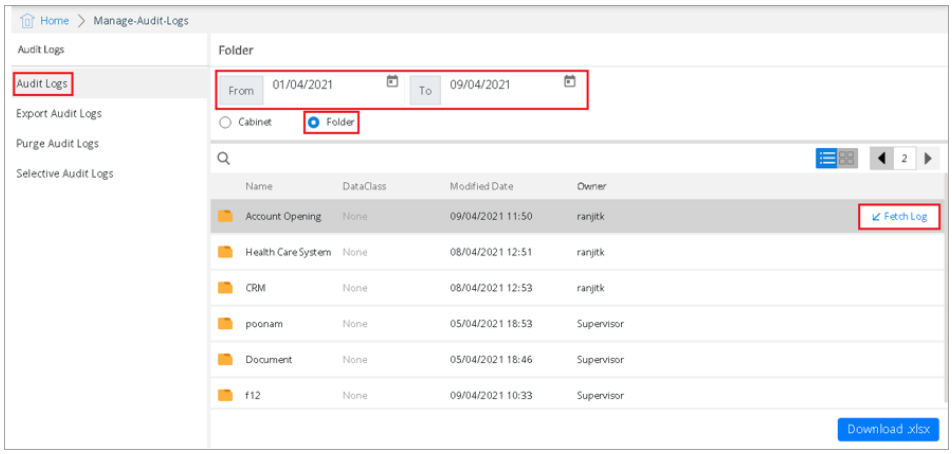
View audit logs

To View the Cabinet Audit Logs:

1. Click on the **Audit Logs** link given in the left pane.
2. Set the date range using the **From** and **To** fields.
3. Select the **Cabinet** option.
4. Click on **Fetch Log** to view the logs.

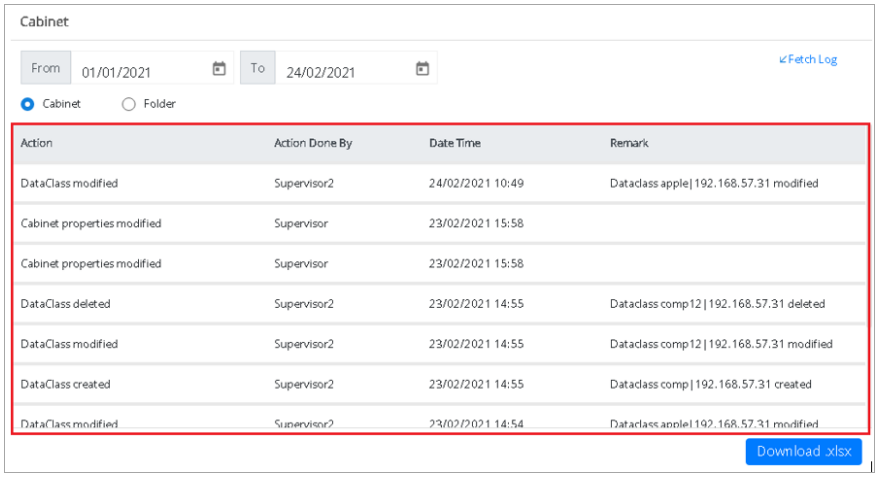


5. The audit logs are generated and shown in a tabular format.

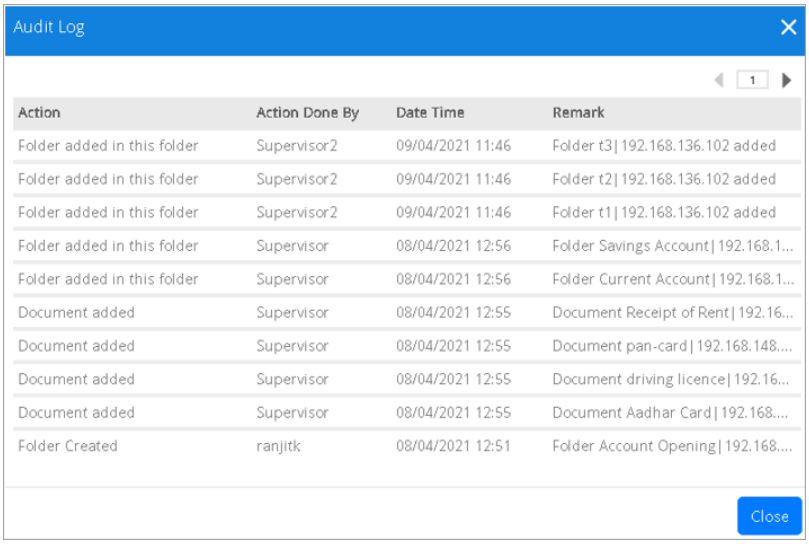


To View the Folder Audit Logs:

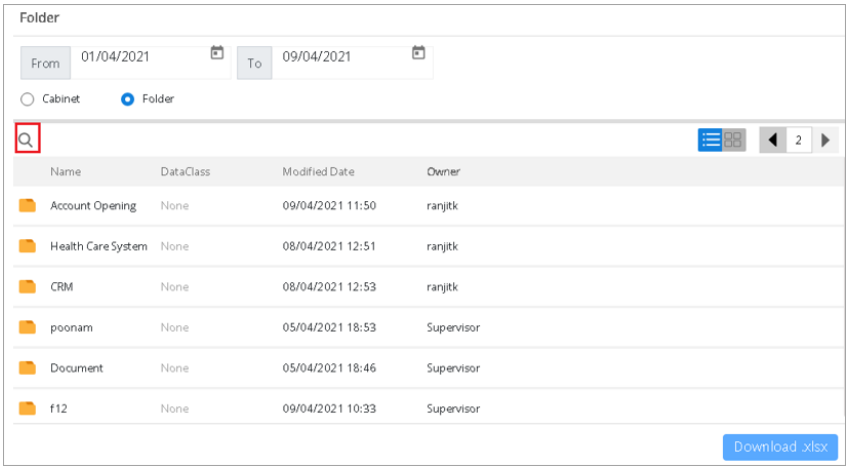
1. Click on the **Audit Logs** link given in the left pane.
2. Set the date range using the **From** and **To** fields.
3. Select the **Folder** option. All the folders created in the cabinet appears.
4. Click on **Fetch Log** against the folder, the audit logs of which you want to generate.
    - The **Fetch Log** link appears when you hover over the mouse pointer over any folder.



5. The audit logs of the selected folder are generated and shown in a tabular format.

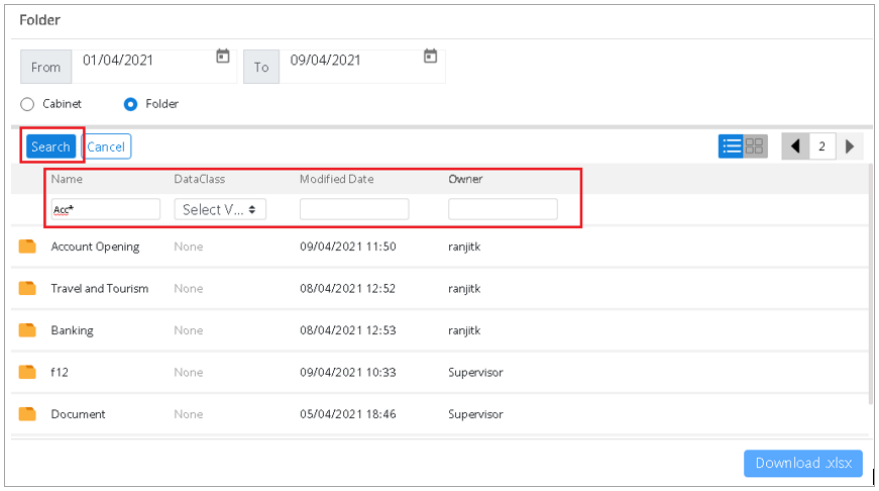


6. To search and view the audit logs of a particular folder:
   a. Click on the **Search** icon.



   b. Specify the following search criteria and click on the **Search** button. The search can be performed based on all or one of the search criteria.
      - Name

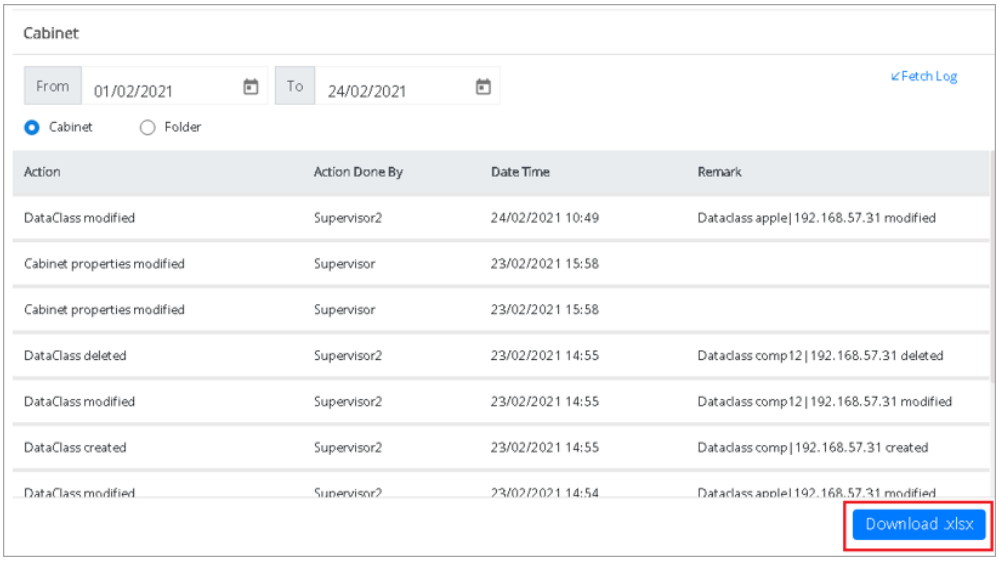
- DataClass
- Modified Date
- Owner



Download audit logs

To Download Audit Logs:

1. Generate the Cabinet/Folder **Audit Logs**.
2. Click **Download.xlsx**. The audit logs are downloaded in the form of an XLSX file.



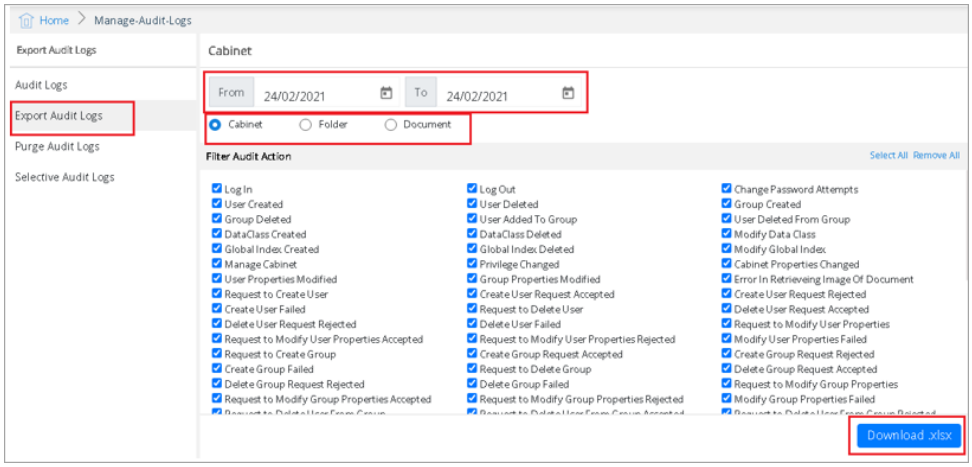
Export audit logs

The export of Audit Logs feature enables you to transfer Audit Log data to an excel file. This process of transfer of Audit Log data is known as export of Audit Log.

The export of Audit Log depends on the volume of data that you need to export and makes maximum use of the central processing unit of the server computer. As a result, the export of Audit Log is a time-dependent process.

To Export the Audit Logs:

1. Click on the Export Audit Logs link given in the left pane.
2. Set the date range using the From and To fields.
3. Select the Cabinet/Folder/Document option.
4. Select the required Audit Actions that you want to see in the audit log file to be exported.
    - You can click on Select All to select all the audit actions in one go or click on Remove All to remove all the selected actions.
5. Click on **Download .xlsx**.



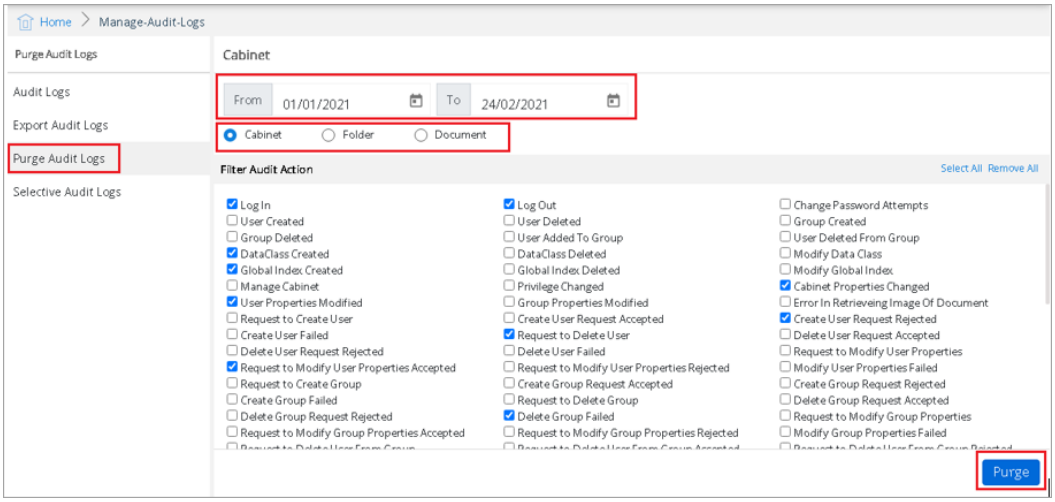
6. The audit logs are downloaded in the form of an XLSX file.

Purge audit logs

The Purge Audit Logs feature enables you to select or purge an action from a specific category between ranges of dates. You can set the range of dates using the From and To, for which the audit logs are to be generated.

You can select a category (Cabinet/Folder/Document) to generate audit log for all actions in that category or for a specific action in that category.

To Purge Audit Logs:



1. Click on the **Purge Audit Logs** link given in the left pane.
2. Set the date range using the From and To fields.
3. Select the Cabinet/Folder/Document option.
4. Select the required Audit Actions that you want to purge.
    - You can click on Select All to select all the audit actions in one go or click on Remove All to remove all the selected actions.
5. Click **Purge**. A message **Purge is done successfully** appears.

Configure

This section provides information on configuring various components and features in OmniDocs. The configuration options available include:

- OmniProcess
- Search
- Web API
- Dashboard
- Third Party App Registration
- NCC App Configuration
- NewgenONE Marvin
- Mail Server Configurations

OmniProcess configuration

OmniProcess is used in case of distributed scanning and centralized processing of files. These files consist of business object documents such as:

- Credit Card Application
- Insurance Policy
- Loan Application and more

Following are two primary aspects of OmniProcess:

Maker	Maker is the person responsible for file creation comprised of data entry and upload tasks
Checker	Checker is the person responsible for quality check, document verification and authorization.

OmniProcess lets administrator create workflows for document intensive processes that allows processing of transactions uploaded through OmniScan, created in OmniDocs from import or new documents.

OmniProcess is comprised of:

- Create Process
- Execute Process
- Process Reports
- Process Summary

Creating a process

To Create a Process:

1. In the Home screen of OmniDocs Admin, go to **Configure** tile and click **OmniProcess** link.
2. OmniProcess – Create New screen appears. It is comprised of the following tabs:

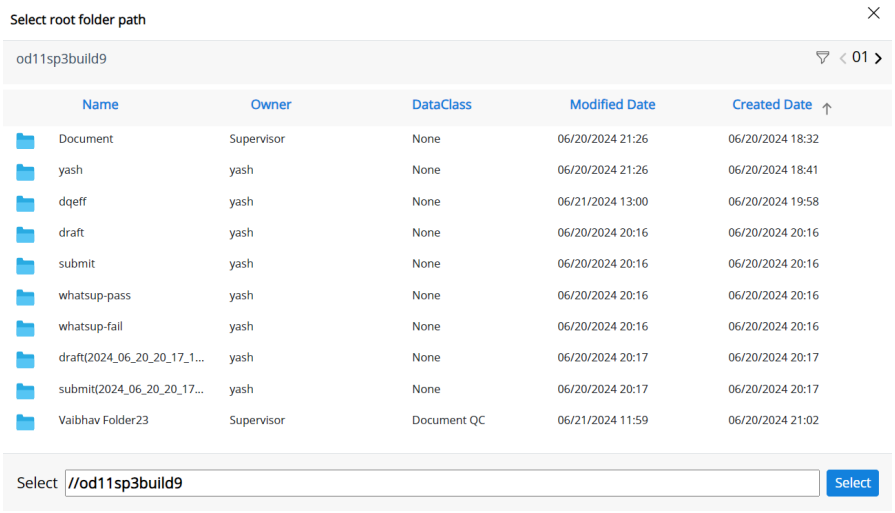
Tabs	Description
Basic Details	This tab allows the administrator to define the basic details of the process. It includes: • Process name • Process object (folder or document) • Set the root folder path at which folders and documents can be added to the system • Set upload method
DataClass	This tab is used to associate the data class with the process.
Action Definition	This tab is used to assign the User group to perform data entry and documents upload, and Checker group to work on the process.
Display Settings	This tab is used to configure output settings and document view settings.
Configure Operations	This tab is used to configure operations on folders and documents. For the Process Object Folder, operations on both folder and document can be configured. For the Process Object Document, operations on only document can be configured.
Report	This tab is used to enable or disable various reports associated with the process configured.

Tabs	Description
Summary	This tab gives a summary of the configured process.

Basic details

Provide the following basic details:

1. Enter process name in **Process name** textbox.
2. **Select process object** from the given options:
   - **Folder**: Select **Folder** option if multiple documents are required to be uploaded for the process.
   - **Document**: Select **Document** option if a single document is required to be uploaded for the process.
3. Select root folder path where you would want the user to save the folders and documents.
   a. Click on **Browse**.
   b. Select the root folder path screen appears. It shows a list of all the folders present in the logged-in cabinet.
   c. Click the navigation icon < 01 > to go to the next page and previous page, respectively.



   d. Click on the desired folder. The root folder path of the selected folder appears in the textbox given at the bottom of the screen.
      i. A folder can be searched based on pre-defined filter criteria. Refer to the Filter folder.
   f. Click on **Select** to select the root path.

g. The selected root folder path appears in the Select root folder path textbox.

4. Set upload method is used to set methods for uploading supporting documents.
   • Mark the checkboxes against the desired methods to select them.

Checkboxes	Description
Browse from system	This method is used to upload documents from the user's local drive.
OmniScan	This method is used to upload documents from Newgen OmniScan. OmniScan is an advanced, distributed document scanning solution for a high volume document scanning and data capture directly into configured OmniProcess.
CSV	This method is used for uploading documents in bulk with indexing.

Multiple upload methods can be selected.

5. Click on **Next** to save this step and move to the next step, i.e., Data Class.
6. If you click on **Next** without specifying the required fields, alert messages appear just below the unfilled fields. This holds true for other steps as well.

This holds true for all those tabs where data is required to be specified.

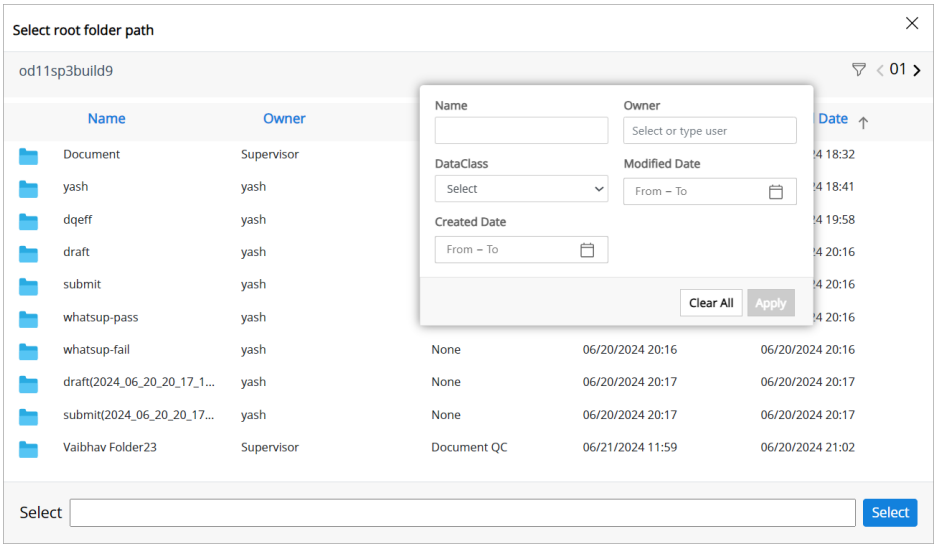
7. "Configuration saved in draft successfully" message appears.

On clicking Next, the configuration is saved as a draft so that the process creation can be continued at some later time also.

Filter Folder for root folder path

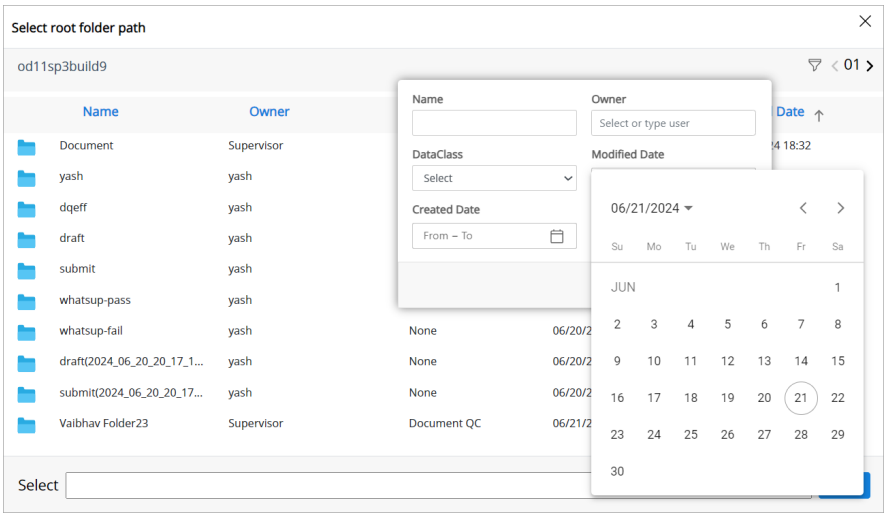
To search and select the root folder path, follow the below steps:

1. Click the **Filter** icon. The filter criteria required to perform folder filter appear as shown.



2. The folder filter can be performed on the basis of one or all of the following:

Fields	Description
Name	Name of the folder
Owner	Name of the owner of the folder
Data Class	Name of the data class associated with the folder
Modify Date	Modification date of the folder. You can specify a particular date under Equals to or a Range of two dates between which the folder was modified.
Created Date	Created date of the folder. You can specify a particular date under Equals to or a Range of two dates between which the folder was modified.
Clear All	Allows you to reset the filter options.

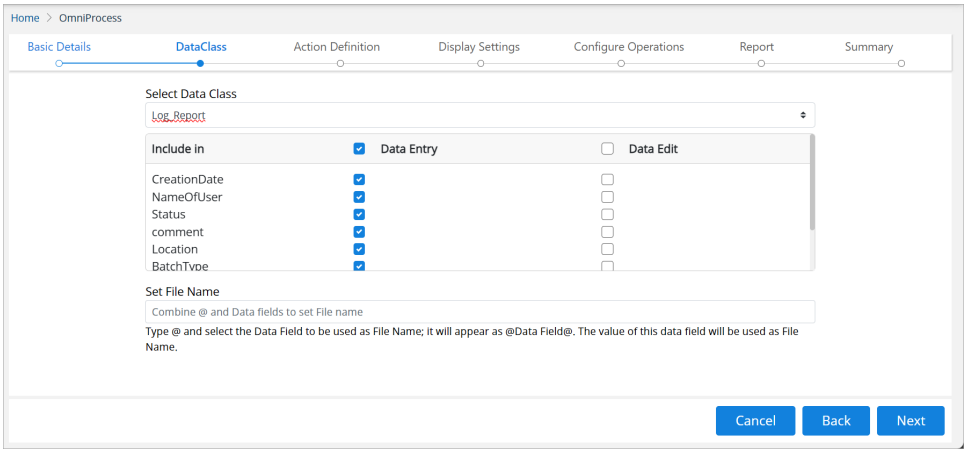


4. Click on **Apply**. The filter result is displayed on the basis of specified filter criteria.
5. Click on the desired folder.
6. Click on **Select** to select it as the root folder path.

Data class

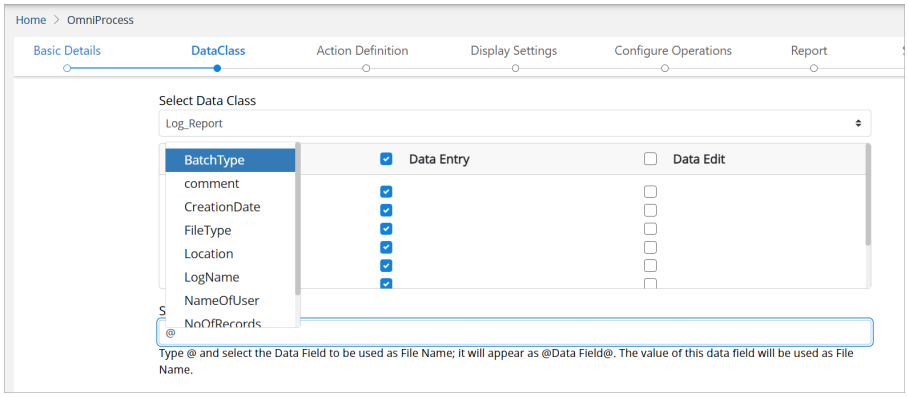
Data class step is used to associate the data class to the process being created. To associate a data class to the process, follow the below steps:

1. Select or type the name of the desired data class.
    a. As you click in **Select Data Class** combo box, a dropdown containing all the data classes created in the logged-in cabinet appears.
    b. Click on the desired data class to select it.
    c. You can also enter the data class name in the **Select Data Class** combo box. As you type the name, the suggestive names appear in the form of the dropdown list.
    d. Choose options against the data class fields if you want to include them for **Data entry** (during upload) and **Data edit** (for checker).

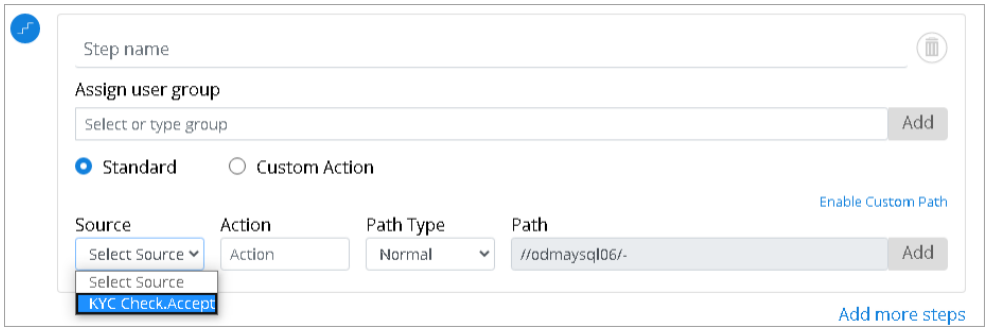


2. Enter a file name in **Set File Name** textbox.
    a. Type @ and select the Data Field to be used as a File Name. It will appear as @Data Field@.
    b. As you type @ in the text box, a list of all the data fields of the selected data class appears in a dropdown list.

> Multiple fields can be selected as an object name.



3. Click on **Next** to save this step and move to the next step, i.e. Action Definition. Click on Back to go to the previous step, Basic Details.



4. Delete button, appearing in the lower-left corner of the screen, is used to permanently delete the configuration.
    a. On clicking **Delete**, an alert message box appears asking for confirmation of the deletion.
    b. Click on **Confirm** to delete the configuration, else click on **Cancel**.The next step appears and a message "Configuration saved in draft successfully".

> On clicking Next, the configuration is saved as a draft so that the process creation can be continued at some later time also.

Action definition

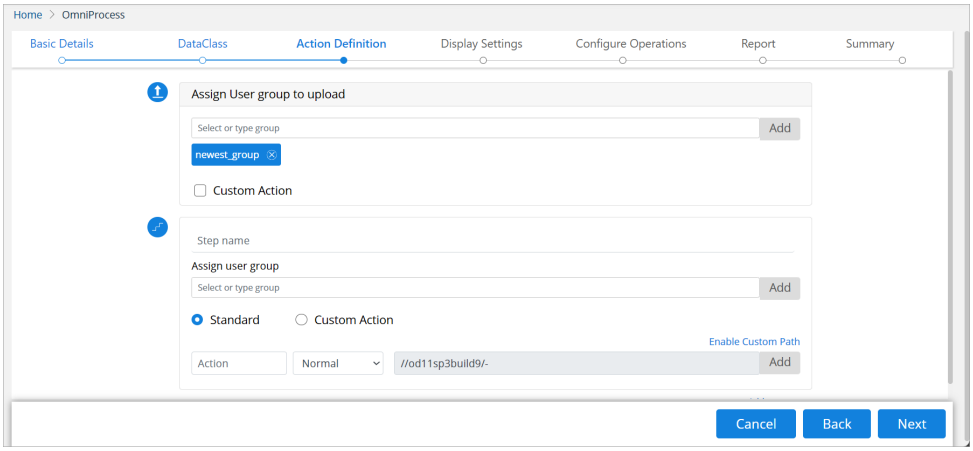
Action definition step is used to assign:

- The User group to perform documents uploads.
- The Checker group to work on the process created.

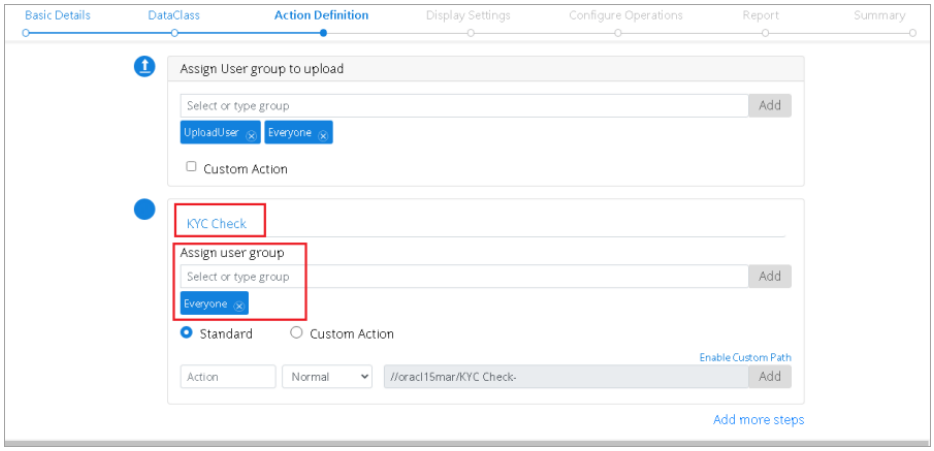
To assign the user group, follow the below steps:

1. Select from the dropdown or type the group name in **Assign User group to upload** combo box.
    a. As you click on the user group, it gets added just below the **Assign User group to upload** combo box.
    b. To specify a custom group name (new group), type the desired name and click on **Add**.

> The group created here will not have any user. The administrator will have to assign user(s) to this group through System Administrator.

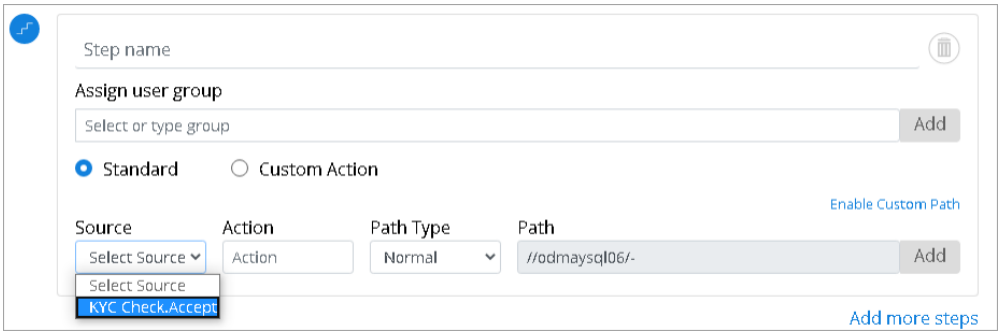


    c. Click on the cross mark against the selected user group to remove it.
    d. **Custom Action:** Select Custom Action to launch custom pages on click of configured actions. This allows the user doing the data entry to perform any custom action on the instrument (Folder/Document).
2. Enter **Step name**.
3. Assign user group to perform the task associated with the above step.
    a. Select or type the group name in **Assign group name** combo box.
    b. As you select the user group, it gets added just below the **Assign group name** combo box.
    c. To specify a custom group name, type the desired name and click on **Add**.
    d. Click on the cross mark against the selected user group to remove it.



4. **Standard/Custom Action**:
    a. Standard: Select Standard for standard action definition.
    b. **Custom Action**: Select Custom Action to launch custom pages on click of configured actions. This allows the checker to perform any custom action on the instrument (Folder/Document).
    c. When **Standard** is selected:
    d. Enter the action name in the **Action** text box.
    e. Select **Normal** for normal movement of instruments and **LoopIn** for backward movement of instruments.
    f. On selecting LoopIn, you can select **Upload** from the dropdown that appears next to LoopIn.
    g. On selecting Normal, the archival path is shown.
    h. **Enable Custom Path**: Using this option, the user can create a dynamic folder path. The first folder name must be a constant and then type @ and select the Data Field to be used as dynamic Folder Name. Only mandatory Data Field will appear in the dropdown. It will appear as @Data Field@. The value of this data field will be used as the Folder Name.
    i. Click on **Disable Custom Path** to disable dynamic folder path creation.
    j. Click on **Add** to add the action.
    k. On the basis of the specified **Step name** and **Action name**, a folder is created within the root folder. The processed object (folder/document) will be moved to this folder.
    l. Depending on the requirement, more than one action can be added.
    m. The added action can be removed by clicking on .
    n. When **Custom Action** is selected:
    o. Enter action name in the **Action** textbox.
    p. Enter the **Path** of the jsp file to be called for this custom action.
    q. Click on **Add** to add the custom action.

5. Click on **Add more steps** to add more steps, if required in the process.
6. Repeat steps from **2 to 4**.



7. In addition to the above steps, you are required to select the **Source** which will be a destination of the previous step. Again, based on the Action name movement will take place.
   - The **Source** dropdown contains the names of previous steps.
   - Click on (**Edit**) to modify step details and (**Delete**) to delete the added step.
   - Click on **Next** to save this step and move to the next step, i.e. Display Settings.
   - Click on **Back** to go to the previous step, Data Class.
   - The next step appears and a message "Configuration saved in draft successfully" appears.

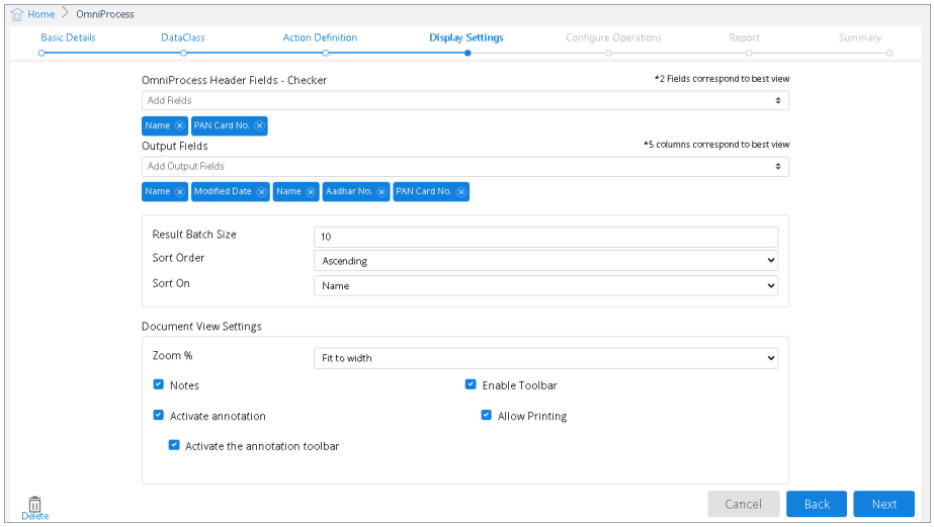
   On clicking Next, the configuration is saved as a draft so that the process creation can be continued at some later time also.

Display settings

Display settings step allows the administrator to configure output settings and document view settings. To configure display settings, follow the below steps:

1. To configure **Output settings**:
   a. **OmniProcess Header Fields (Checker)**: Users will be able to see the selected data fields on the header of checker's step of OmniProcess.
   b. **Output Fields**: The selected fields will be visible in the columns of the search results.
   c. **Sort order**: Select the required sort order from the dropdown list.
   d. Selecting **Ascending** will give the search result in the ascending order.
   e. Selecting **Descending** will give the search result in the descending order.
   f. **Sort on**: Select the required Sort on option from the dropdown list. The result will be sorted on the basis of the field selected in Sort on.

2. To configure **Document View Settings**:
    a. Select **Zoom %** for document display.
    b. Check/un-check **Enable Menu bar** checkbox to enable/disable menu bar.
    c. Check/un-check **Notes** checkbox to enable/disable writing of notes.
    d. Check/un-check **Allow Printing** checkbox to enable/disable printing of documents.
    e. Check/un-check **Enable Toolbar** checkbox to enable/disable toolbar in the OpAll Viewer.
    f. Check/un-check **Enable Annotation** checkbox to enable/disable annotation.



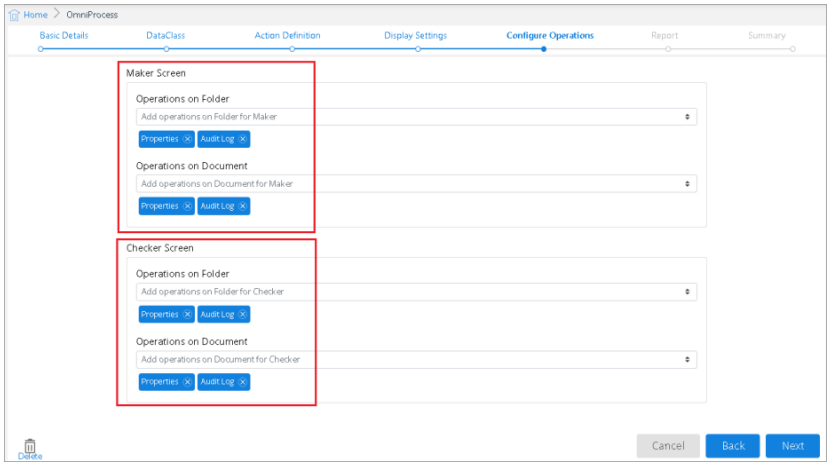
3. Click on **Next** to save this step and move to the next step, i.e., Configure Operations.
4. Click on **Back** to go to the previous step, Action definition.
5. The next step appears and a message "Configuration saved in draft successfully".

> On clicking Next, the configuration is saved as a draft so that the process creation can be continued at some later time also.

Configure operations

Configure Operations feature is used enable operations that can be performed on documents and folders. In case of Process Object for Document, operations on documents can be configured. In case of Process Object for Folder, operations on both documents and folders can be configured.

1. Add the required operations that can be performed on folder and document for both maker and checker screens by clicking on the respective dropdown lists.



2. Click on **Next** to save this step and move to the next step, i.e., Report.
3. Click on **Back** to go to the previous step, Display Settings. The next step appears and a message "Configuration saved in draft successfully" appears.

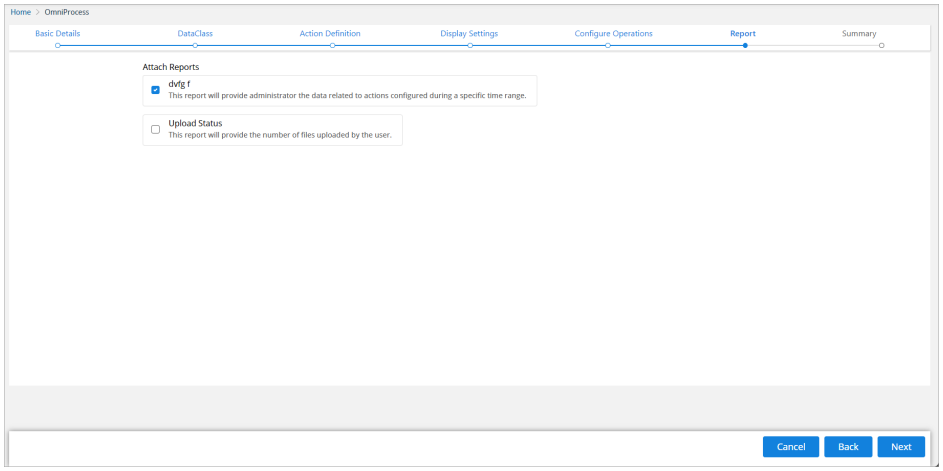
> On clicking Next, the configuration is saved as a draft so that the process creation can be continued at some later time also.

Report

Report step is used to enable or disable various reports associated with the configured process.

> - The reports are auto-created based on the action name and steps created in Action definition.
> - A user can select the reports which will be available under OmniDocs > Reports for end-user.
> - By default, the reports based on actions are pre-selected.

1. Select the desired Reports to be attached against this Process.
2. Click on **Next** to save this step and move to the next step, i.e., Summary.



3. Click on **Back** to go to the previous step, Configure Operations.
4. The next step appears and a message "Configuration saved in draft successfully" appears.

> On clicking Next, the configuration is saved as a draft so that the process creation can be continued at some later time also.

Summary

Summary step displays the summary of the configured process. You can review all the steps and if anything is missing or is inappropriate, go back to that particular step and make corrections.

To download the process summary as a PDF, follow the given steps:

1. Click on **Download** given at the lower-left corner of the screen.

> The download button appears only in the Summary tab.

2. The process summary is downloaded as a PDF document.
3. The process can be deleted by clicking on **Delete** button.
4. **Process Execution:**
    a. In order to make the configured process operational, it has to be executed. Follow the below steps to execute the configured process:
    b. Click on **Execute**.
    c. **"Process created successfully!**" message appears.

Duplicate

Duplicate feature is used to make a copy of the configuration with a different name. It will open in Draft, allowing you to change the root folder and other settings as needed. The Duplicate button is given at the lower-left corner of the screen.

To make a duplicate copy of any configuration, follow the below steps:

1. Open the desired configuration.
2. Click on **Duplicate**.
3. Duplicate dialog box appears.

1. Enter a new name of the process in **Enter New OmniProcess Name** textbox.
2. Click on **Save**.

   The Process will open in Draft, allowing the user to change the root folder and other settings as needed.

3. Configuration saved in draft successfully message appears.
4. The duplicate process is saved in the draft section of OmniProcess.
5. Since the duplicate process is saved in draft, it must be executed to make it operational.To do so:
6. Open the duplicate process from the draft section.
7. Modify the settings if required.
8. Click on **Execute** (in summary tab). The steps to modify and execute the process are the same as that of creating a process.

Operations on created OmniProcesses

The following operations can be performed through the OmniProcess tab of the Admin tools bar:

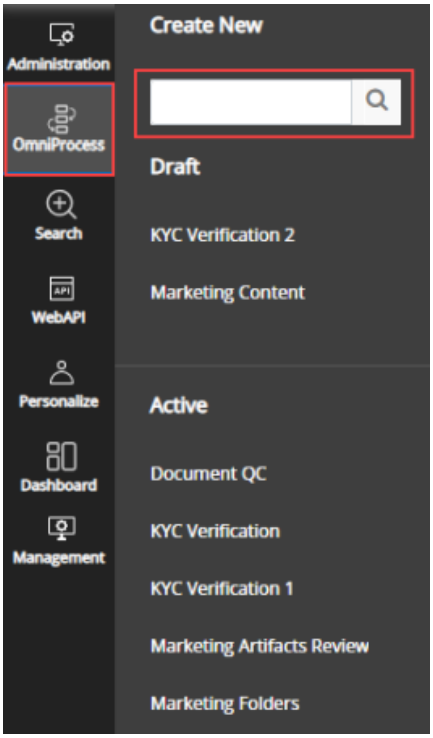
- Create a new process
- Search processes
- View and modify a process saved as draft: The processes saved as draft are listed in **Draft** section
- View active or executed processes: The active processes are listed in **Active** section

Click on **OmniProcess** tab of the OmniDocs Admin Menu bar to view its options.

Search Processes

To Search Any Process (both active and draft):

1. Click in the search textbox.



2. Enter the desired process name.
3. As you type the characters, the un-matching names keep on disappearing and in the end, only matched names are left in the lists of draft processes and active processes.

Saved Processes

The process is saved as draft after completion of each step so that the process creation can be continued at some later time also. To view and start working on such processes, follow the given steps:

1. Click on **OmniProcess** tab of the OmniDocs Admin Menu bar.
2. The processes saved as draft are listed under **Draft**.
3. Click on the desired draft process.
4. The selected process opens in edit mode, allowing you to continue and complete the remaining steps.
5. Configure this and the remaining steps as described in Create Processes section.

Active Processes

The active processes are those processes which are executed and are ready for use in OmniDocs Web. All such processes are listed in **Active** section. To view the configured steps of an active process, follow the below steps:

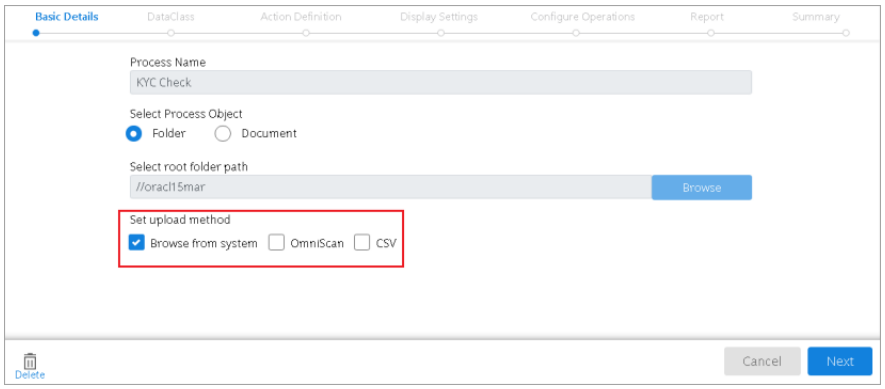
1. Click on the **OmniProcess** tab on the OmniDocs Admin menu bar.
2. Click on the desired **Active process**. The selected process opens at the summary step.
3. Click **Back** to go to the previous step.

OmniProcess Modification

This option is used to modify the properties of an already created OmniProcess. Only those OmniProcess can be modified which are created by users. The system defined process cannot be modified.

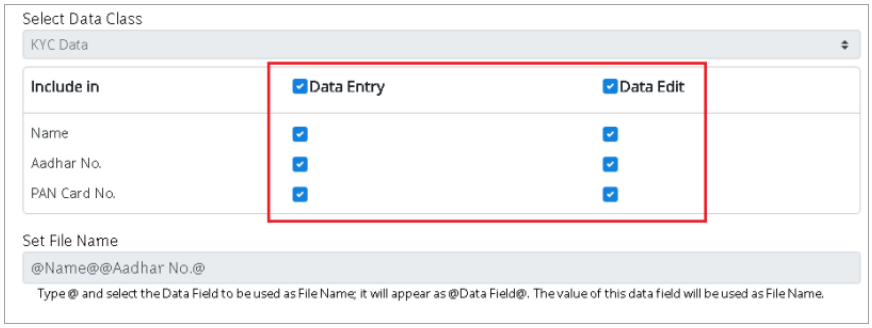
To modify an existing OmniProcess:

1. Open the desired configuration.
2. Click on **Back**, given at the bottom-right of the screen, to go the previous tab. Keep moving back until you reach the Basic Details tab.
3. **Basic Details** tab: In Basic Details tab you can only modify the **Set upload method**. The other fields are non-editable.
    a. Modify the upload method as per the requirement.
    b. Click on **Next** to move to the next tab, i.e., Data Class.



4. **Data Class** tab: In Data Class tab you can only modify the selections made for the data fields, i.e., Data Entry and Data Edit. The other fields are non-editable.

a. Modify the **Data Entry** and **Data Edit** selections as per the requirement.
b. Click on **Next** to move to the next tab, i.e., Action Definition.

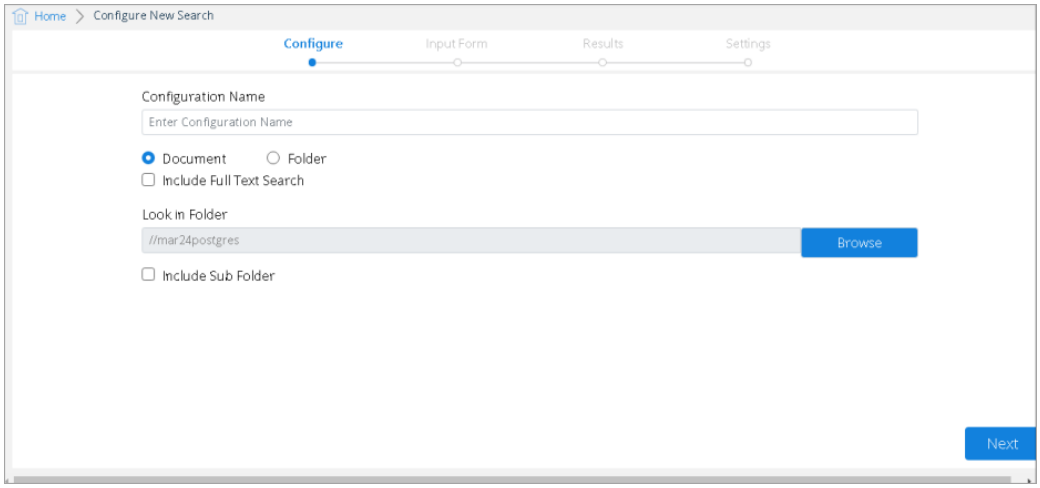


5. **Action Definition** tab: In Action Definition tab you can add and remove groups from **Upload** and **Checker Steps**. **Custom Action** can also be enabled or disabled in the Upload section.
   a. Add or remove **groups** as per the requirement.
   b. Click on **Next** to move to the next tab, i.e., Display Settings.
6. **Display Settings** tab: In the Display Settings tab, you can modify all the fields.
   a. Modify the selections as per the requirement.
   b. Click on **Next** to move to the next tab, i.e., Configure Operations.
7. **Configure Operations** tab: In the Configure Operations tab, you can add and remove folder and document operations.
   a. Modify the selections as per the requirement.
   b. Click on **Next** to move to the next tab, i.e., Report.
8. **Report** tab: In the Report tab you can add and remove reports.
   a. Modify the selections as per the requirement.
   b. Click on **Next** to move to the next tab, i.e., Summary.
9. **Summary** tab: The Summary tab just gives a summary of the configured process. So, you cannot modify anything here.
   a. Once the required modifications are done, click on **Modify** to save the properties.
   b. Modify OmniProcess Configuration dialog box appears to confirm if this OmniProcess is to be updated or not.
   c. Click on **Confirm**.
   d. On confirmation, "**Process is modified Successfully**" message appears.

Search configuration

To Create a New Search Configuration, perform the below steps:

1. In the Home screen of OmniDocs Admin, go to **Configure** tile.
2. Click **Search**. The Configure New Search screen appears.

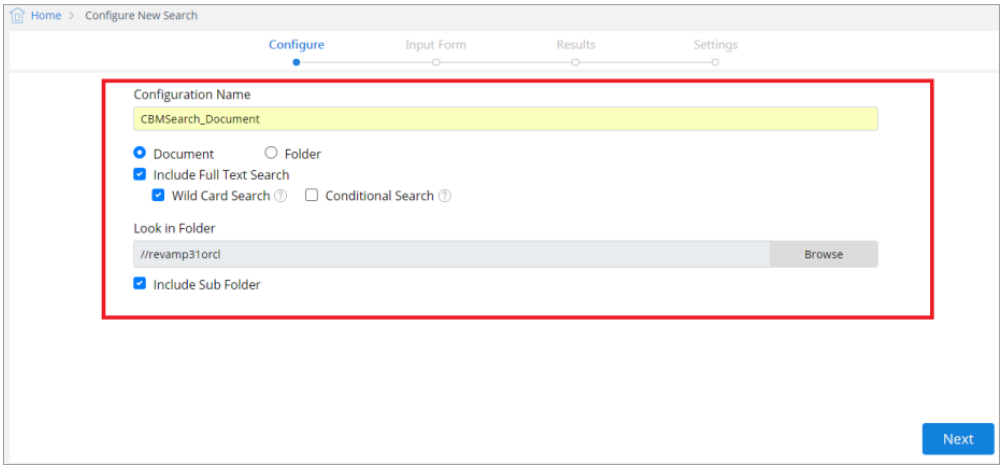


3. Specify the details for the following fields:

Fields	Description	
Configuration Name	Enter the Name for your Search Configuration. For example Search on Marketing documents.	
Document/ Folder checkbox	Select the Document or Folder checkbox for which you want to create the Search Configuration. The Search Configuration can be created for either Document or Folder at a time.	
Include Full Text Search	Select this checkbox to search a particular text in the document. This option appears only if you select the Document checkbox.	
	Wild Card Search	This search is used when AND is used between all the Search Terms and it perform search. For this case, each word gets a Wild Card search separately (except the text in quotes), and then the results are ANDed. For example, insurance banking returns the documents that contain either of the two words or the two words together.
	Conditional Search	This is query search that you have ebtered and sent for search without modifying or changing it in any manner. For example,

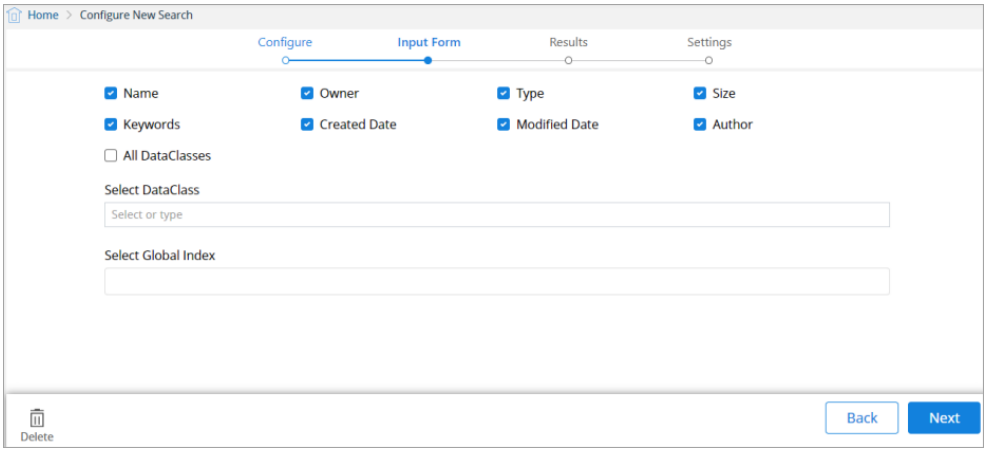
Fields	Description	
		insurance or banking, returns the documents that contain either of the specified words.
Look in Folder	Click **Browse** and select the folder where you want to perform the Folder or Document search.	
Includes Sub Folder	Select **Include Sub-Folder** checkbox option to include the subfolders in the search process.	

4. After specifying the details, click **Next**.



The Input Form section appears along with Configuration Saved in draft successfully message.

If you select Folder on the Configure page, Select Global Index does not appears.



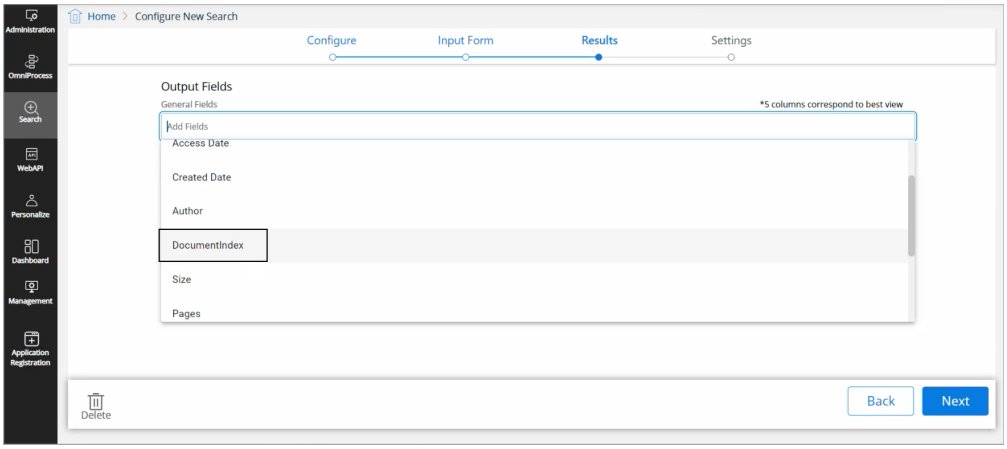
5. Select the required input parameters on which you want to perform the search. The available input parameters are as follows:

Input Parameters	Description
Name	Name of the Document or Folder.
Owner	Name of the Owner who created the Document or Folder.
Type	Type of Document.
Size	Size of the Document or Folder.
Keywords	Select Keywords based on which you can select the Document or Folder.
Created Date	Select this option to perform certain operations based on the Document or Folder Creation Date.
Modified Date	Select this option to perform certain operations based on the Document or Folder Modification Date.
Author	Enter the author of the document.
All Data Classes	Select this checkbox to enable search on all the data classes. On selecting All Data Classes, Select Data Class dropdown gets disabled. You can either select **All Data Classes** or a particular data class.

6. Select the required **DataClass** from the dropdown.
7. Click **Set Advance Settings** to apply a logical operator on Data Class fields.

> In the case of Set Advance Setting, you can search on DataClass field for multiple values as well. In case All DataClasses option is selected, the option to enable the Set Advance Setting for all the data classes appear.

8. Similarly, select the required **Global Index** from the dropdown. It appears if the search is configured for documents.
9. Click **Next** to move to the next section. The Results section appears.
   The Configuration Saved in draft successfully message appears.
10. In the **Output Fields**. select the fields you want to show in the columns during the Output Search.
11. To remove already added Output Field, click **x** icon given against the added fields.
12. To add an Output Field, click **Add Output Fields** and select the required Output Field from the dropdown. Additionally, you can select the Document Index.



If you select Document Index in Results, it serves as a unique identifier for documents in the Search tab within the OmniDocs module.

13. In the **Operations on Document and Folder**, select the operations that you want in the Output Search.
16. To remove already added Search Operations, click **x** icon given against the added fields.
17. To add a Search Result Operation, click **Add Search Result Operations** and select the required Search Result Operation from the dropdown.

Operation on Folder does not appear for a document type search configuration.

18. Once, all the inputs are provided, click **Next** button. The Settings section appears.
19. Specify the details for the following fields:

Fields	Description	
Assign User Group	Select the User Group from the dropdown to whom you want to assign the default rights of this Search Configuration.	
Result Settings	Make the required changes in this section to configure the Result Output view. The available fields are as follows:	
	Result Batch Size	Enter the required batch size.
	Sort Order	Select the required sort order from the available dropdown.
	Sort On	Select this option to sort the results based on specified sorting.

Fields	Description		
Document View Settings	Make the required changes in this section to configure the Document Output view. The available fields are as follows:-		
	Enable Property	Select this property to enable the Property feature in the OpAll Viewer.	
	Enable Menubar	Select this property to enable the Menubar feature in the OpAll Viewer.	
	Enable Toolbar	Select this property to enable the Toolbar feature in the OpAll Viewer.	
		Enable Annotations	Select this property to enable the Annotations feature in the OpAll Viewer.
		Enable Printing	Select this property to enable the Printing feature in the OpAll Viewer.
	Enable Notes		Select this property to enable the Notes feature in the OpAll Viewer.
	Enable Thumbnails		Select this property to enable the Thumbnails feature in the OpAll Viewer.
	Zoom%		Select the default Zoom % from the dropdown.

21. After specifying the details, click **Save**. The Search Configuration is created successfully message appears.

Web API configuration

OmniDocs Web API is a web-based integration framework for the integration of any external application with OmniDocs.

Using WEB API, a user can:

- Create an application for configuring any external system for Image Enabling.
- Configure the Display functionality to customize the View as to whether a single document or document list is to be displayed.
- Define Security settings to specify the timeout period so that the Image Enabling View being shown to the user will expire after the specified time.

- Access to Image Enabling View can be restricted by specifying a list of servers which will be granted access.
- Generate and use Sample integration code to be used in an external application for carrying out the integration activity.

Creating a Web API

To Configure a New Web API:

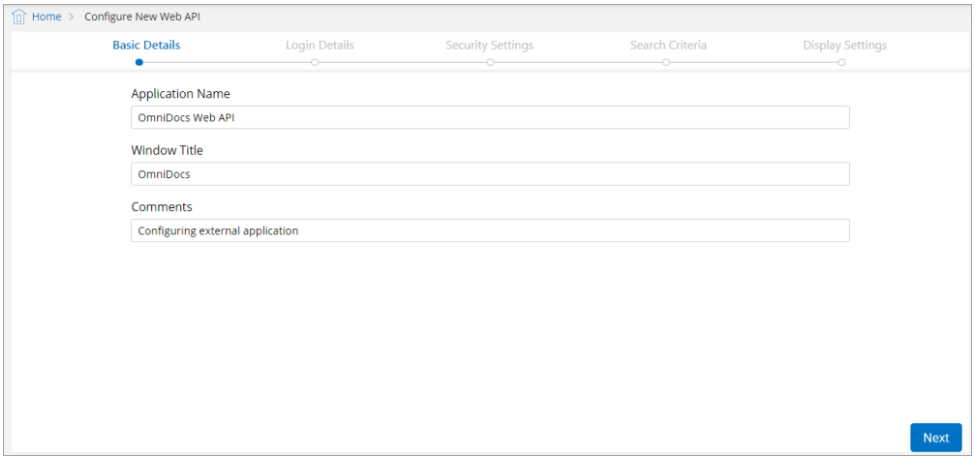
1. In the Home screen of OmniDocs Admin, go to **Configure** tile and click on **Web API** link.
2. Configure New Web API screen appears. It is comprised of the following tabs:
   - Basic Details
   - Login Details
   - Security Settings
   - Search Criteria
   - Display Settings

Basic details

To work with Basic Details tab, follow the given steps:

1. Provide the following basic details:

Fields	Description
Application Name	Name of the new application.
Window Title	Name of the window title. The title specified here would be the title of the window opened after the integration URL is accessed.
Comments	A brief description about the new application.



2. Click on **Next** to save this step and move to the next step, i.e., Login Details.
   - If you click **Next** without specifying the required fields, alert messages appear just below the unfilled fields. This holds true for other steps as well.

   This holds true for all those tabs where data is required to be specified.

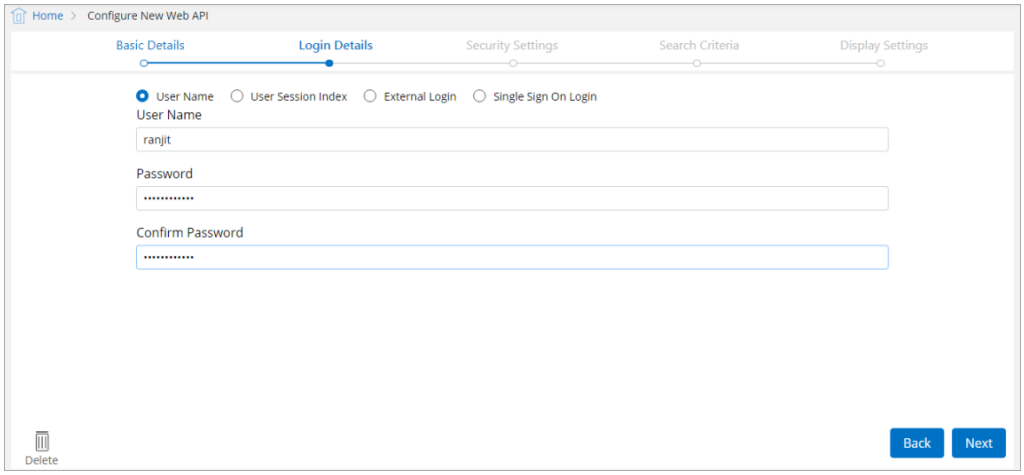
"Configuration saved in draft successfully" message appears.

On clicking Next, the configuration is saved as a draft so that the Web API creation can be continued at some later time also.

Login details

Login Details tab is used to specify the connection details to access the application.

1. **Connection Details**: Select the option as User Name, User Session Index, External Login or Single Sign on Login for establishing a connection with the cabinet.
   - **User Name**: If User Name is selected then the user will enter the credentials here only. The user will give **User Name**, **Password** and will **Confirm Password**. Now, these user credentials will be used for establishing a connection with the cabinet and this user should exist in this cabinet.
   - **User Session Index**: In this case, the user will send userDBId to access the Web API.
   - **External Login**: In this case, the user will enter credentials when trying to connect with the cabinet.
   - **Single Sign on Login**: It is like External Login. The only difference is that the login credentials will be authenticated by LDAP. In case the SSO is not set up on the machine, the SSO login option will not be visible.



2. Delete button, appearing in the lower-left corner of the screen, is used to permanently delete the configuration.
    a. On clicking **Delete**, an alert message box appears asking for confirmation of the deletion.
    b. Click on **Confirm** to delete the configuration, else click on **Cancel**.
3. Click on **Next** to save this step and move to the next step, i.e., Security Settings. Click on **Back** to go to the previous step, Basic Details.
4. The next step appears and a message "Configuration saved in draft successfully" appears.

> On clicking Next, the configuration is saved as a draft so that the Web API creation can be continued at some later time also.

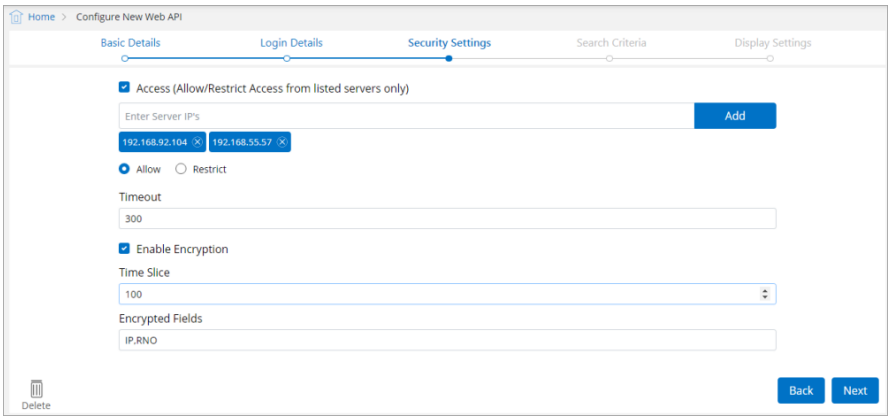
Security settings

To specify security settings, follow the given steps:

1. **Access (Allow/Restrict Access from listed servers only):** When this checkbox is enabled, then the user can enter the machine IPs to which the Admin wants to allow access or restrict access.
2. Enter the Server IP and click on **Add**. Multiple IPs can be added one by one.
    - The added IP can be removed by clicking on .
3. Select:
    - **Allow** to allow access to the above-mentioned IPs.
    - **Restrict** to restrict access to the above-mentioned IPs.
4. **Timeout:** Specify the timeout in seconds. The time specified here would be the time for which the integrated application would remain open.

5. **Enable Encryption:** Select the checkbox to send the parameters mentioned in **Encrypted Fields** textbox in an encrypted format. Mention the time in **Time Slice** textbox. This is the time for which the application URL will work. This time is in milliseconds.
6. Click on **Next** to save this step and move to the next step, i.e., Search Criteria. Click on **Back** to go to the previous step, Login Details.
7. The next step appears and a message "Configuration saved in draft successfully" appears.

> On clicking Next, the configuration is saved as a draft so that Web API creation can be continued at some later time also.



Search criteria

To specify search criteria, follow the given steps:

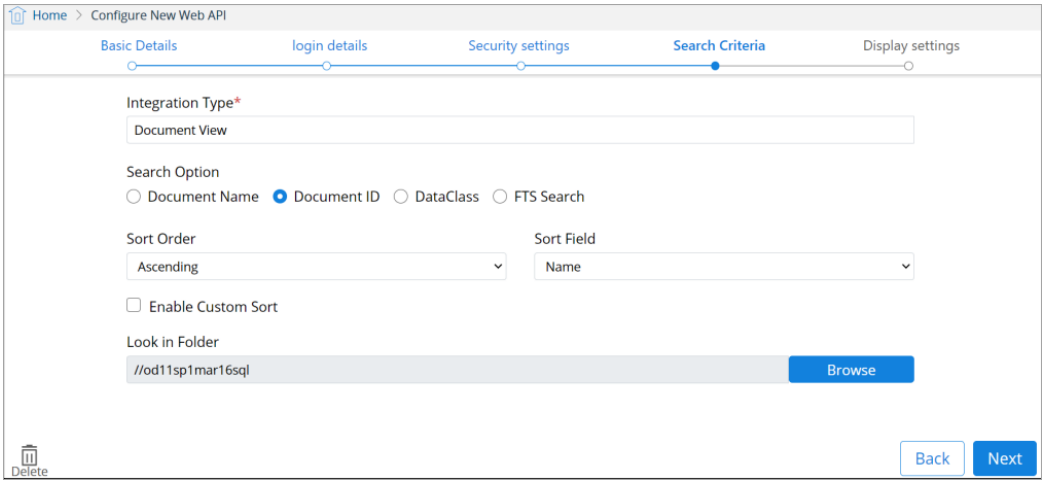
1. **Integration Type**: Select the integration type from the dropdown list. This defines the type of search that will be used by the integrated application to perform the search action.
   The following are the available integration types:
   - **Document View**: It allows you to view a particular document by searching based on document name or document ID or index-based search can be made (using data class). The searched document gets opened in the OpAll viewer. In this integration, it is suggested to use document ID for search.
   - **Folder View**: It allows you to search the document list of a particular folder. Folder search can be made on the basis of folder name or index based-search can be made (using data class). The document list of the searched folder is

shown, and the first document gets opened in the OpAll viewer. You can view any document from the available list.

- **Advance Folder View**: You can search a folder based on the folder name or folder ID. Index-based search can be made using data class. The advance view for searched folder displays the folder and its subfolders, data class applied on the folder along with the fields values and document list. The first document from the document gets opened in the OpAll viewer. You can open any document from the available list.
- **Easy Search**: Folders or documents are searched based on the Easy Search.
- **Configured OmniProcess**: Folders or documents are searched based on the configured OmniProcess.
- **Configured Search (Document and Folder)**: Folders or documents are searched based on the configured search.

2. **Search Option:** Select the search option on the basis of which search will be made. The options are Document Name, Document ID, and Data Class.
3. **Sort Order**: Sorting order can either be **Ascending** or **Descending**.
4. **Sort Field**: Select the desired field from the dropdown list.
5. **Enable Custom Sort**: Select this checkbox to enable custom sort. On selecting this checkbox you are required to specify **Custom Sort Class** and **Custom Sort Method**.
6. **Look in Folder**: Click on **Browse** and select the folder where the search will be carried out.
7. Click on **Next** to save this step and move to the next and the final step, i.e., Display Settings. Click on **Back** to go to the previous step, Security Settings.
8. The next step appears and a message "Configuration saved in draft successfully" appears.

On clicking Next, the configuration is saved as a draft so that Web API creation can be continued at some later time also.



Display settings

To configure display settings, follow the given steps:

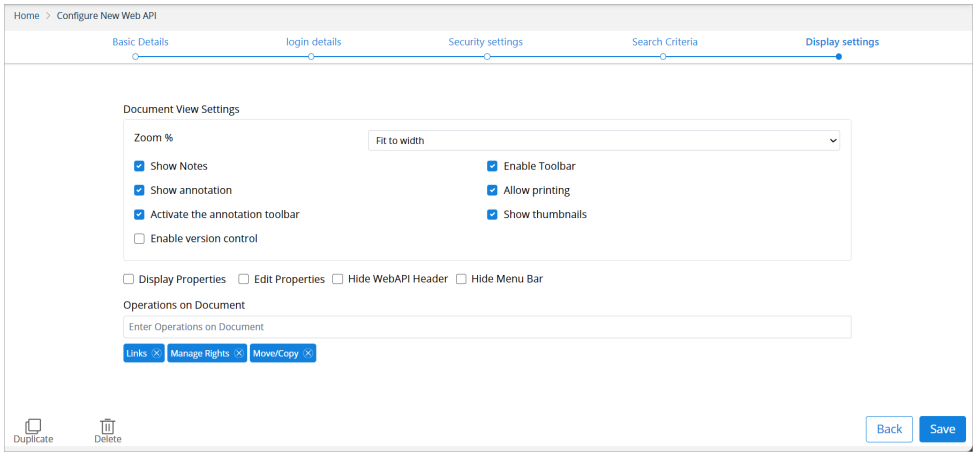
1. To configure the **Document View Settings**:
    a. Select **Zoom %** for document display. The size of the window that would open after the integration can be set here.
    b. Check or un-check **Show Notes** checkbox to enable or disable notes.
    c. Check or un-check **Show Annotation** checkbox to enable or disable the display of OpAll annotation.
    d. Check or un-check **Activate the anotation toolbar** checkbox to enable or disable the document toolbar.
    e. Check or un-check **Enable version control** checkbox to enable or disable document versioning.
    f. Check or un-check **Enable Toolbar** checkbox to enable or disable the OpAll annotation toolbar.
    g. Check or un-check **Allow printing** checkbox to enable or disable printing of documents.
    h. Check or un-check **Show thumbnails** checkbox to enable or disable the display of thumbnails in OpAll.
2. **Display Properties**: Select this checkbox to display properties for the end-users.
3. **Edit Properties**: Select this checkbox to enable edit properties for the end-users.
4. **Hide WebAPI Header**: Select this checkbox to disable the WebAPI header for the end-users.
5. **Hide Menu Bar**: Select this checkbox to disable the menu bar for the end-users.

For all Web API integration types, the batch size can range from 5 to 100.

6. **Operations on Document**: Select the desired operations that can be performed on a document. You can select multiple operations one by one. The options are:

Move/Copy	Delete	Manage Rights	Links	Alarms/ Reminders
Checkin/ Checkout	Download	Versions	Duplicate	Mail
Audit Log	Assign to FilePlan	Request	Print	Properties

   - An added operation can be removed by clicking on .
7. Click on **Save** to save the Web API configuration details and make it operational.
   - You can click on **Back** to go to the previous step, Search Criteria.



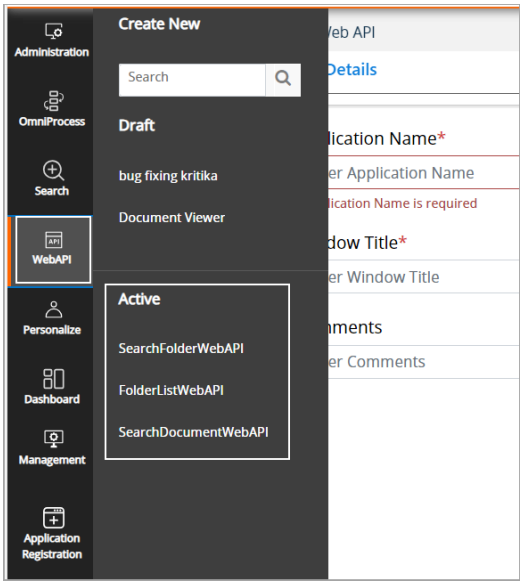
"Web API Configuration is created successfully" message appears.

Duplicate

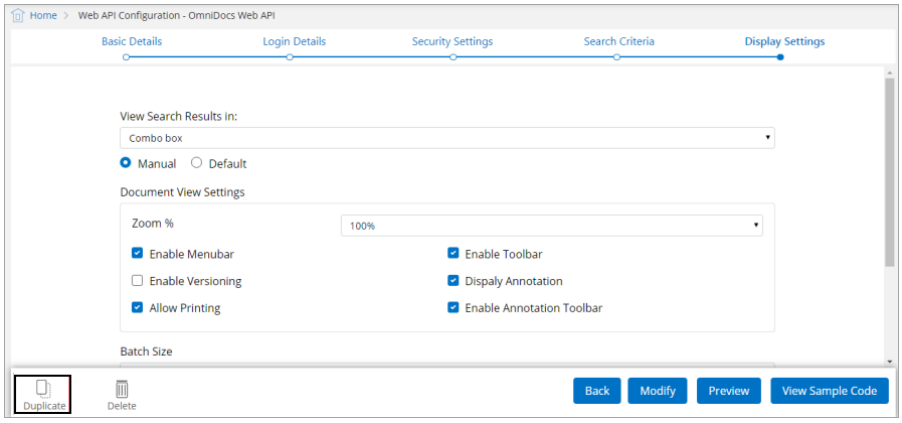
Duplicate feature is used to make a copy of the configured Web API with a different name. It will open in Draft, allowing you to modify the various settings as needed. The Duplicate button is given in the lower-left corner of the Display Settings tab.

To make a duplicate copy of configured Web API, follow the below steps:

1. Open the **Active** Web API from the Web API tab of the OmniDocs Admin Menu bar. The selected Web API appears.

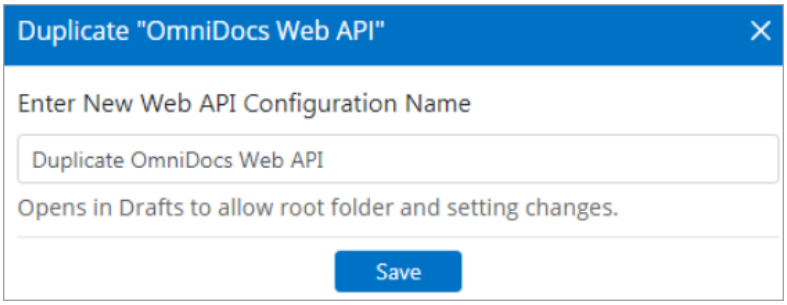


2. Click on **Duplicate**. The Duplicate dialog box appears.



3. Enter a new name of the Web API in **Enter New Web API Configuration Name** text box.
4. Click on **Save**.

> The duplicate configuration will open in the Draft so that required modifications can be done in it, as per the requirement.



5. The duplicate configuration is saved in the **Draft** section of Web API.

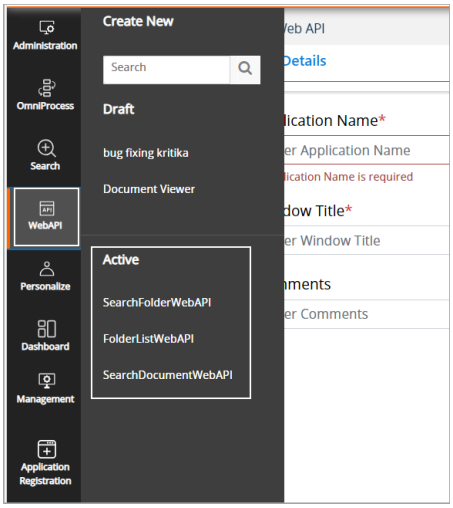
6. Since the duplicate Web API is saved in draft, it must be saved to make it operational.
   To do so:
   a. Open the duplicate Web API from the **Draft** section.
   b. Modify the settings by revisiting all the tabs.
   c. Click on **Save** in the **Display Settings** tab.
   d. Once saved, it will move to the **Active** section.

Operations on created Web API

The following operations can be performed through the OmniProcess tab of the Admin tools bar:

- Create a new Web API: Click on **Web API** tab of the OmniDocs Admin Menu bar and click on **Create New** link and refer to the following tabs:
- Basic Details
- Login Details
- Security Settings
- Search Criteria
- Display Settings
- Search Web APIs
- View and modify a Web API saved as draft: The processes saved as draft are listed in **Draft** section.
- View Active or Saved Web APIs: The active processes are listed in **Active** section.

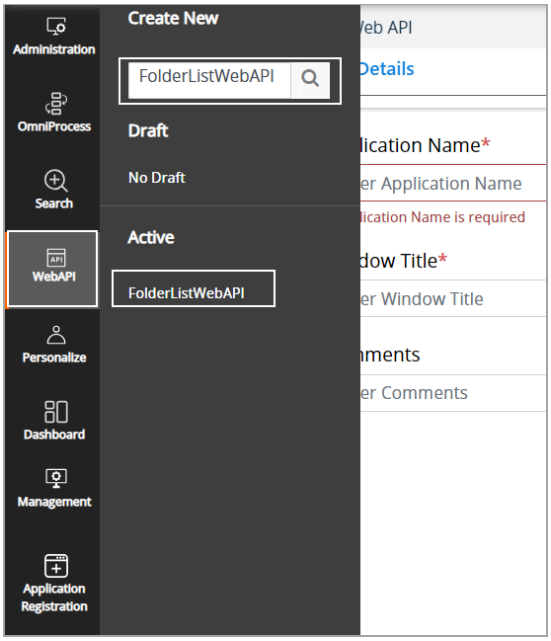
Click on **Web API** tab of the OmniDocs Admin Menu bar to open the Web API tray.



Search Web API

To search any Web API (both Active and Draft), follow the below steps:

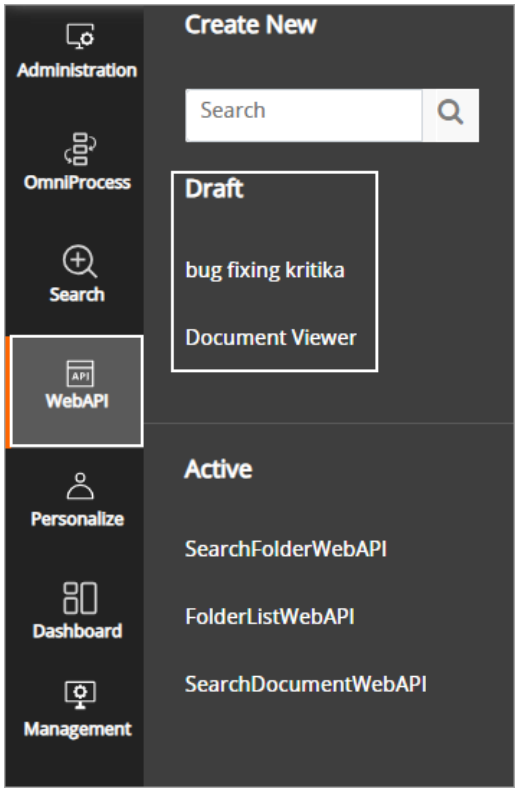
1. Open the Web API tray from the left menu bar and click in the search text box.
2. Enter the desired Web API name.
3. As you type the characters, the un-matching names keep on disappearing and in the end; only the matched names are left in the lists of Draft and Active sections.



Web APIs Saved in Draft

The configuration is saved as draft after completion of each step so that its completion can be continued at some later time also. To view and start working on such Web APIs, follow the given steps:

1. Open the **Web API** tray.
2. The Web APIs saved as draft are listed under **Draft**.

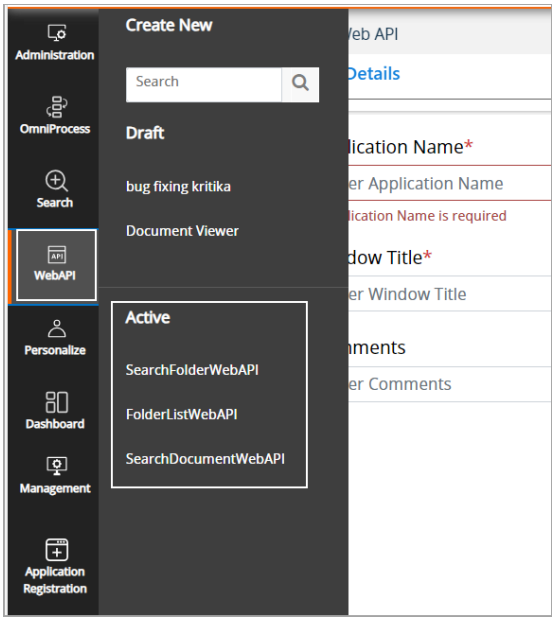


3. Click on the desired Web API from the Draft list to open it.
4. It opens in edit mode, allowing you to continue and complete the remaining steps.
5. Configure this and the remaining steps as described in Create Web API section.

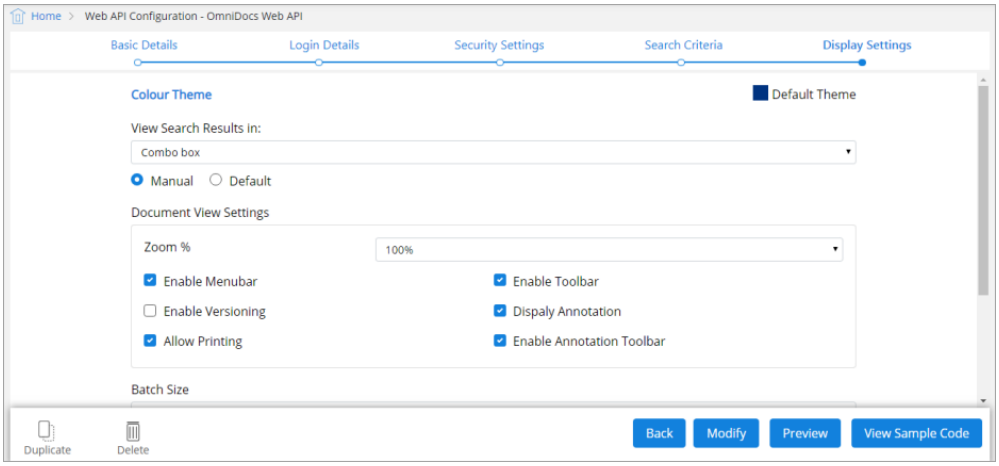
Active Web APIs

To view and modify the configured steps of an active Web API, follow the given steps:

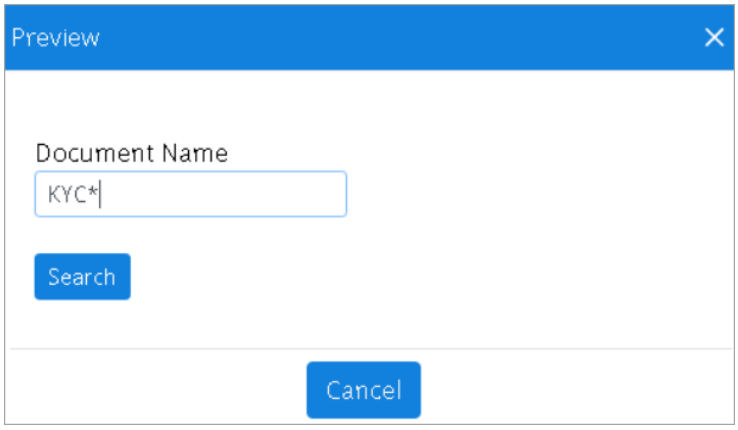
1. Open the **Web API** tray.
2. The active Web APIs are listed under **Active**.



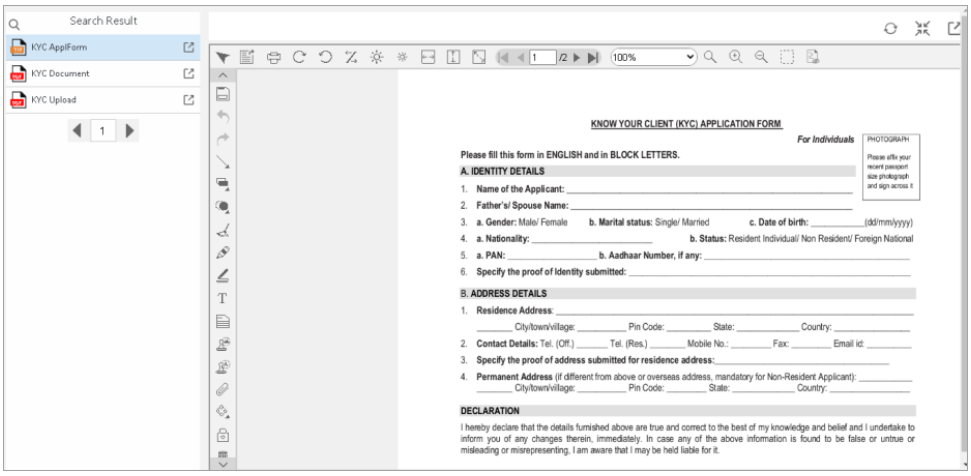
3. Click on the desired active Web API. The selected Web API opens at the Display Settings step.
4. Click on **Back** to go to the previous step.



5. Click on **Modify** to save the changes made to the configuration. A confirmation message for the same appears.
6. Click on **Preview** to test the search condition. Preview dialog box, displaying the search criteria, appears.
    a. Enter the **Search Criteria** and click on **Search**.



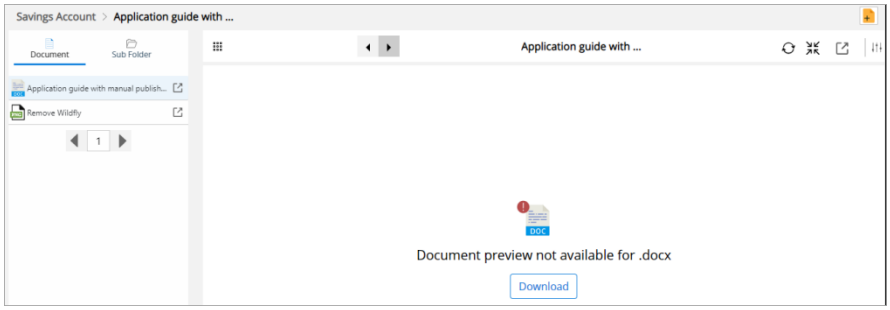
b. All records satisfying the search condition are displayed as per the configured search criteria.



c. In the case of Advance Folder View as the Integration Type, you can add documents directly to the folder that appears in the search result. To add documents, follow the given steps:

i. Click **Preview** on the Display Settings tab of the Web API configured for Advance Folder View. The Preview dialog appears.

ii. Enter the **Folder Name** and click **Search**. The search result appears.



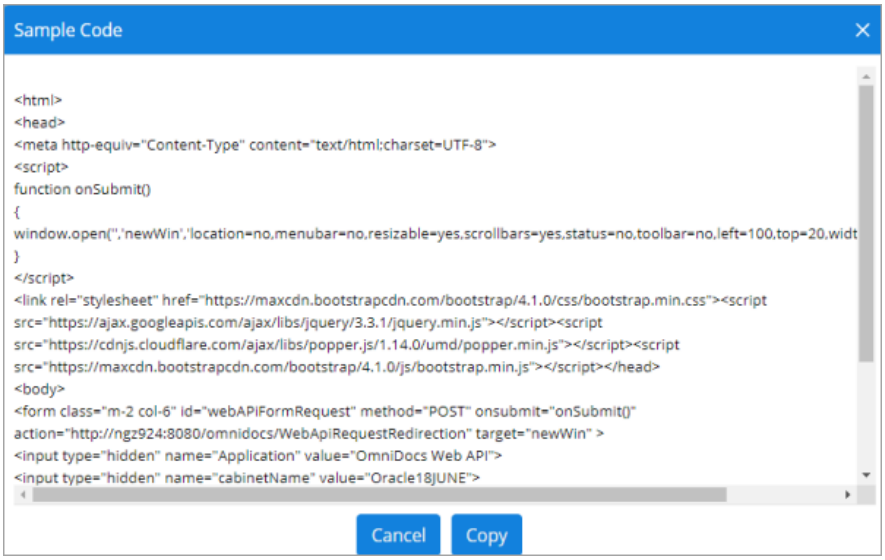
iii. Click the (**Add Folder**) icon on the top-right corner of the screen. The Add Document dialog appears.

iv. Add the required document using the Drag and drop or Browse features.

v. Click **Save and Upload More** or **Save and Close** as per the requirement. The document gets added to the folder.

> To learn more about adding documents to folders, refer to the *Newgen OmniDocs User Guide*.

7. Click on **View Sample Code** to see the sample code generated. This sample code is to be used while integration, the sample code generated contains the search criteria entered while creating the Web API.
   a. Click on **Copy** to copy the sample code and **Cancel** to close the dialog box.



Encryption support

OmniDocs Web API is a web-based integration framework for the integration of any external application with OmniDocs. In this module of WEB API, an application is a logical entity that refers to an external application like workflow or ERP. The external application can be Image Enabled with OmniDocs documents by creating a reference application here which will contain all the configurations like OmniDocs cabinet information to access OmniDocs cabinet for displaying documents in Image Enabling GUI.

Steps to follow:

Here, Encryption Support is a new feature that has been added to WEB API, you need to follow these steps to enable encryption support:

Under Encrypted Fields, mention the following parameters:

- For Document View integration:

Search Option	Encypted Fields
Document Name	IP, RNO , DocumentName
Document Id	IP, RNO , DocumentId

- For Folder View and Advance Folder View integration:

Search Option	Encypted Fields
Folder Name	IP, RNO , FolderName
Folder ID	IP, RNO , FolderIndex

- For Search Option Data Class in each integration:

S. No.	Data Class	Fields	Encrypted Fields
1.	Document QC	Document ID	IP, RNO , Document ID
		Department	IP, RNO , Department
2.	Location_Tracker	Batch_Type	IP, RNO , Batch_Type
		Batch_Name	IP, RNO , Batch_Name
		Status	IP, RNO , Status
		CO	IP, RNO , CO
		Hub	IP, RNO , HUB
		Branch	IP, RNO , Branch
		Comment	IP, RNO , Comment
3.	Log_Report	Log Name	IP, RNO , LogName
		No Of Records	IP, RNO , NoOfRecords
		File Type	IP, RNO , FileType
		Creation Date	IP, RNO , CreationDate
		Name Of User	IP, RNO , NameOfUser
		Status	IP, RNO , Status
		Comment	IP, RNO , comment
		Location	IP, RNO , Location
		Batch Type	IP, RNO , BatchType

To add multiple fields in the Encrypted Fields section, add a comma (,) and keep adding the fields to be encrypted.

For the encryption:

1. Encrypt the respective field values using the *DataEncryption.java* file present in the *Security.jar* in *OmniDocs 12.0*.
2. Copy and paste the respective encrypted field values to the OmniDocs Web API Preview screen.
3. Repeat the above steps for all encrypted fields and hit **Search** to launch the search process.

RMS process

This option allows the **OmniDocs Administrator** to configure an **RMS** (Record Management System) **Tool** through which its basic functions can be performed through **OmniDocs Web**.

To Configure a New RMS Process:

1. In the Home screen of OmniDocs Admin, go to **Configure** tile.
2. Click **RMS Process** link. The RMS Process - Configuration tab appears.
3. The Configuration tab consists of the following fields:

Fields	Description	
Name	Give a name to the configuration that you are going to create.	
Configuration On	Specify that you are going to create the configuration on Record or File Part. For both, select both Record and File Part checkboxes.	
Type	Select the required Type from the dropdown list. You can select one of the following five types:	
	Incoming Request	Select this to enable listing of all the logged-in user's incoming requests.
	Incoming Items	Select this type to enable listing of granted requests for the logged-in user.

Fields	Description	
	Items with me	Select this type to enable listing of all the items accepted by the logged-in user.
	Outgoing Request	Select this type to enable listing of all the requests made by the logged-in user.
	Items Transferred	Select this type to enable listing of all the items which have been transferred by the logged-in user
RMS Action	Action depends on the Type selected. Select any or all the actions. Depending on the Type selected, the different actions can be:	
	Incoming Request	• Generate Transfer Note: It will be used when the logged-in user wants to dispatch items to another user. • Reject: It will be used when the logged-in user wants to reject request(s).
	Incoming Items	• Reject: It will be used when the logged-in user wants to reject an item. • Receive: It will be used when the logged-in user wants to receive an item.

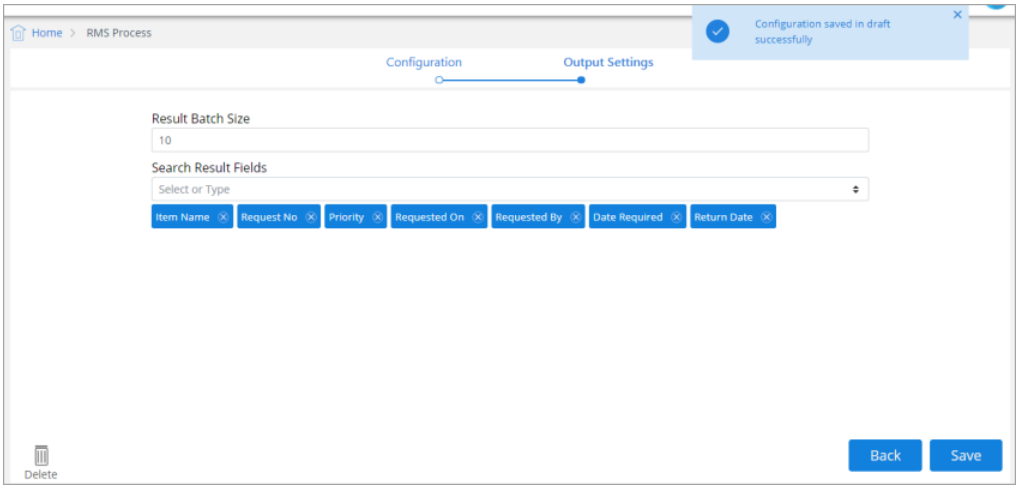
Fields	Description	
	Items with me	• GenerateTransfer Note: It will be used when the logged-in user wants to dispatch items to another user. • Return: It will be used when the logged-in user wants to return back the item to the sender.
	Outgoing Request	• ReRequest: It will be used when the logged-in user wants to re-send the request. • Remind: It will be used when the logged-in user wants to remind the other user for action on the request for the requested item. • Delete: It will be used when the logged-in user wants to delete an outgoing request.
	Items Transferred	No Action: No action can be taken on the transferred items.
Search Criteria	The options in Search Criteria section depends on the Type selected in the Configuration section. Specify the search criteria as required. Depending on the Type selected, the different Search Criteria can be:	
	Incoming Request	
	Priority	Select this option to configure search on the basis of High, Medium or Low priority.

Fields	Description	
	Requested By	Select this option to configure search on the basis of the name of the users who have made the requests.
	Requested On	Select this option if you want to configure the search process using days or date on which the requests were received.
	Date Required	Select this option if you want to configure the search on the basis of date required.
	Return Date	Select this option if you want to configure the search on the basis of the return date.
	Incoming Items	
	Sent By	Select this option to configure search on the basis of the name of the users who have sent the items.
	Mode	Select this option to configure search on the basis of the modes of the incoming items. The different modes can be Requested, Forwarded, Rejected, Moved and Returned.
	Sent On	Select this option if you want configure the search process on the basis of day/date on which items were sent.
	Items with me	

Fields	Description	
	Sent By	Select this option to configure search on the basis of the name of the users who have sent the items.
	Mode	Select this option to configure search on the basis of the modes of the incoming items. The different modes can be Requested, Forwarded, Rejected, Moved and Returned.
	Date Received	Select this option if you want to configure the search process using day/date on which items were received.
	Return Date	Select this option if you want to configure the search process using day/date on which items were returned.
	Outgoing Request	
	Priority	Select this option to configure search on the basis of High, Medium or Low priority.
	Requested Status	Select this option to configure search on the basis of the status of the sent request. The status can be pending, granted or rejected.
	Requested By	Select this option to configure search on the basis of the name of the users who have made the requests.

Fields	Description	
	Requested On	Select this option if you want to configure the search process using days or date on which the requests were received.
	Date Required	Select this option if you want to configure the search on the basis of date required.
	Return Date	Select this option if you want to configure the search on the basis of return date.
	Items Transferred	
	Recipient	Select this option to configure search on the basis of the name of the recipients (user/role) who have received the transferred items.
	Status	Select this option to configure search on the basis of the status of the transferred items. The status can be Pending, Yet to Dispatch, Received or Rejected.
	Sent On	Select this option if you want to configure the search process on the basis of day/ date on which items were sent.

4. Once Inputs are provided, click on the **Next** button.
5. Output Settings section appears.



6. Output Settings section consist of the following fields:

Fields	Description	
Result Batch Size	Enter the Result Batch Size. The Batch Size refers to the search result batch size. If the batch size is specified as 10, then the numbers of search results displayed will 10 per page.	
Search Result Fields	Administrator can select the list of columns which will be shown in search results. Select the Search Result Fields by clicking on the Edit link button.	
	Incoming Request	
	Item Name	Item Name displays the name of the item for which the request is being made.
	Request No	Request Numbering is an administrative function, which defines the way in which the request number and transfer notes are to be numbered.
	Priority	The priority of the request.
	Requested On	Date on which the documents are requested.
	Requested By	User who requested the Documents.
	Date Required	Date on which the documents are required.

Fields	Description	
	Return Date	Date on which the documents will be returned.
	Incoming Items	
	Item Name	Item Name displays the name of the item for which the request is being made.
	TransferNo	Transfer numbering is an administrative function, which defines the way in which the request number and transfer notes are to be numbered.
	SentBy	User who sent the documents.
	SentOn	Date on which the documents were sent.
	Mode	Mode in which the documents are present at the moment.
	Items With Me	
	Item Name	Item Name displays the name of the item for which the request is being made.
	Request No.	Request numbering is an administrative function, which defines the way in which the request number and transfer notes are to be numbered.
	Transfer No.	Transfer numbering is an administrative function, which defines the way in which the request number and transfer notes are to be numbered.
	Data Received	Date on which the documents are received.
	Granted Till	Date till which the Documents are granted.
	Outgoing Request	
	Item Name	Item Name displays the name of the item for which the request is being made.

Fields	Description	
	Request No	Request numbering is an administrative function, which defines the way in which the request number and transfer notes are to be numbered.
	Priority	Priority of the request.
	Requested On	Date on which the Documents were requested.
	Requested To	User to whom the request is made.
	Date Required	Date on which the documents will be returned.
	Return Date	Date on which the documents will be returned.
	Status	Status of the class, file or file part.
	Item Transferred	
	Item Name	Item Name displays the name of the item for which the request is being made.
	Request No.	Request numbering is an administrative function, which defines the way in which the request number and transfer notes are to be numbered.
	Transfer No.	Transfer numbering is an administrative function, which defines the way in which the request number and transfer notes are to be numbered.
	Sent To	User to whom the items were transferred.
	Sent On	Date on which the items were transferred.
	Status	Status of the class, file or file part.

7. Click on **Save Configuration** to save the created configuration.
8. Configuration Added Successfully message appears at the top of the screen.

Operations on Configured RMS Processes

1. Open the **RMS Process** tray from the left menu bar.
2. Click on any of the existing **RMS Process** configurations.
3. The selected configuration properties screen appears.
4. Make the necessary modifications in the **Configuration** section.
5. Click on **Modify** button to save the modifications done.**Output Settings** section appears.
6. Make the necessary modifications in the **Configuration** section.
7. Click on **Modify** button to save the modifications done.

Dashboard designer

A dashboard for the end-users can be configured in the OmniDocs Admin module. By default, the Knowledge workers dashboard will be the default dashboard.

In dashboard designer, you can select a maximum of six and minimum of three widgets while creating a new dashboard or changing the existing ones. You can select different layouts for the selected number of widgets in the dashboards. Users will also be able to add a custom widget while configuring the dashboard.

Users will be able to change the name of the dashboard. The administrator can provide rights on the dashboards and based on the rights users will be able to see the dashboard in the web module. In case, there are rights on more than one dashboard, the users will be able to view the default dashboard as per alphabetical order. If in case there are no rights available on more than one dashboard, then users will only be able to see the Knowledge workers dashboard. In the Web Module, under the Profile Settings there is an option to change the default dashboard using the dashboard settings.

A designed dashboard can be previewed in the Admin module itself. Locations of the widgets can be interchanged in the dashboard while configuring them. Once a widget is removed from the dashboard, the layout suggestions are also changed. It is as per the number of widgets remaining in the dashboard.

To access the **Dashboard designer**, in the Home screen of OmniDocs Admin, go to **Configure** tile and click **Dashboard** link.

User personas for OmniDocs dashboard

The following user personas are available for OmniDocs Dashboard. Apart from these, a user can add a new dashboard also.

- **Dashboard for OmniProcess Users:** This dashboard is designed for the users who use OmniProcess extensively.
- **Dashboard for Knowledge Workers:** This dashboard is designed for the users who mostly search and then work on the content.
- **Dashboard for Senior Management:** This dashboard is designed for the senior-most group of people in the organization.

The OmniProcess Users persona have widgets like OmniProcess:

1. My pending Tasks –the list of all steps containing items on which users must work
2. Favourite/Pinned OmniProcess Step-A particular OmniProcess step that is marked as a favorite
3. Recently completed tasks –the list of the OmniProcess steps on which users have worked
4. My searches
5. Alarms & Reminders

There is a Knowledge Workers Dashboard having widgets as mentioned below:

1. Favourites (items marked as favourites by the logged-in user)
2. Checked out by me (items checked-out by the logged-in user)
3. My Searches
4. Recently Accessed
5. Alarms and Reminders

Knowledge Workers Dashboard is a default dashboard provided to the users. There is also a Senior Management Dashboard having widgets as mentioned below:

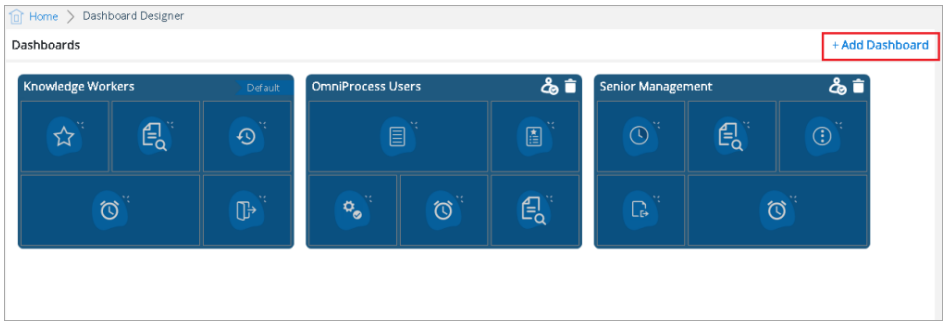
1. Tasks pending at checker step (it shows the list of checker steps on which users have on)
2. Total items checked out by different users
3. My Searches
4. Alarms & Reminders

5. A summary of actions performed on documents through graphical representation (giving the list of actions like number of documents forwarded, deleted, modified, checked out & shared).

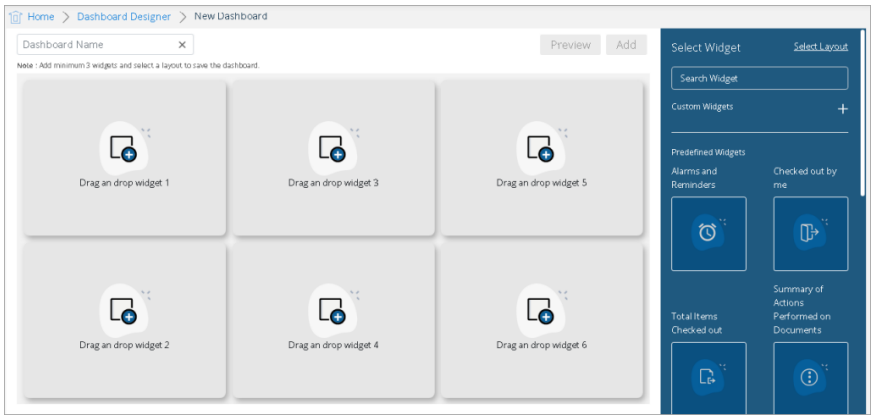
Adding a dashboard

To Add a Dashboard:

1. Click on **Add Dashboard** button on the top-right of the screen.



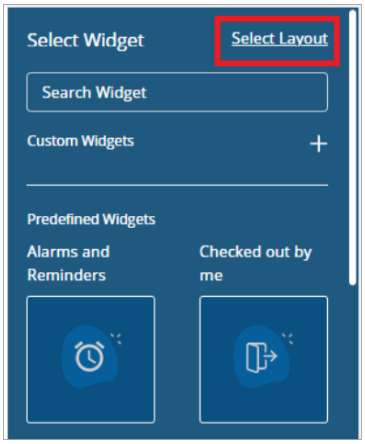
2. New Dashboard screen appears.



3. Enter the name of the dashboard on the top left in the **New Dashboard** textbox.
4. Select the widgets that you want to add to the dashboard. You can drag the widgets from the right panel and drop them in the designer pane.

> A user can select six widgets maximum and three widgets minimum while creating a new dashboard or changing the existing ones.

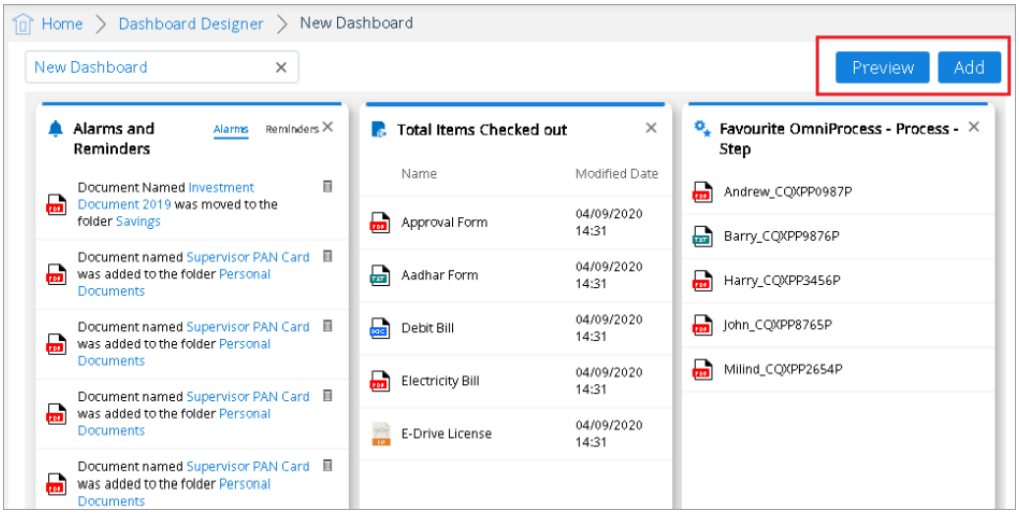
5. Now, click **Select Layout** on the right pane.



6. It will show different layout styles based upon the number of widgets you have chosen.

   For example, the above screen shows the different types of layouts for four widgets.

7. Choose the layout style.
8. Click **Preview button** which is along with Add button to preview the final dashboard look.
9. Click **Add** button otherwise.

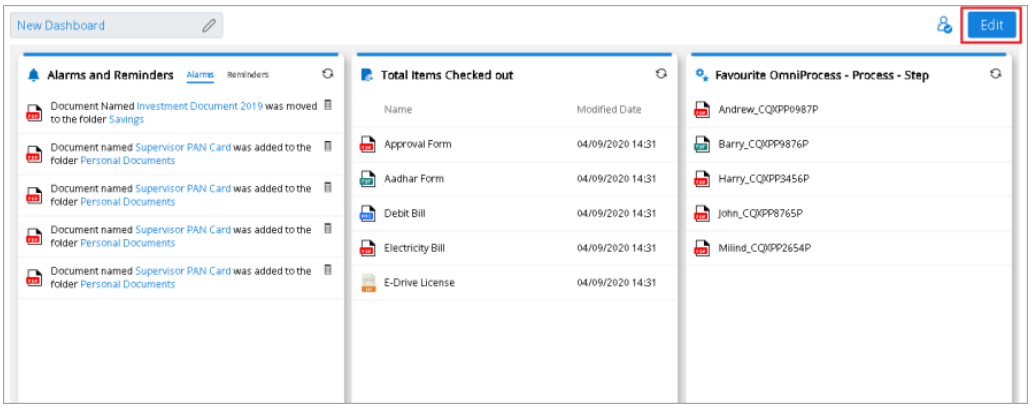


10. Dashboard Added Successfully message will appear for the confirmation.

Editing a dashboard

To Edit a Dashboard:

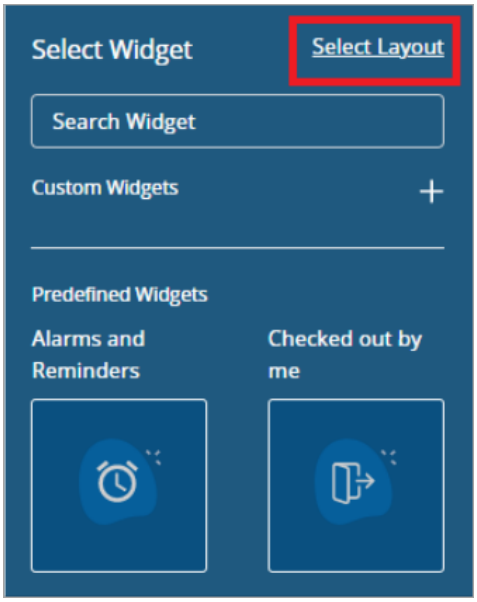
1. Open an existing dashboard to modify and click on the **Edit** button.



2. Select the widgets that you want to add/remove to the dashboard. You can drag the widgets from the right panel and drop them in the designer pane.

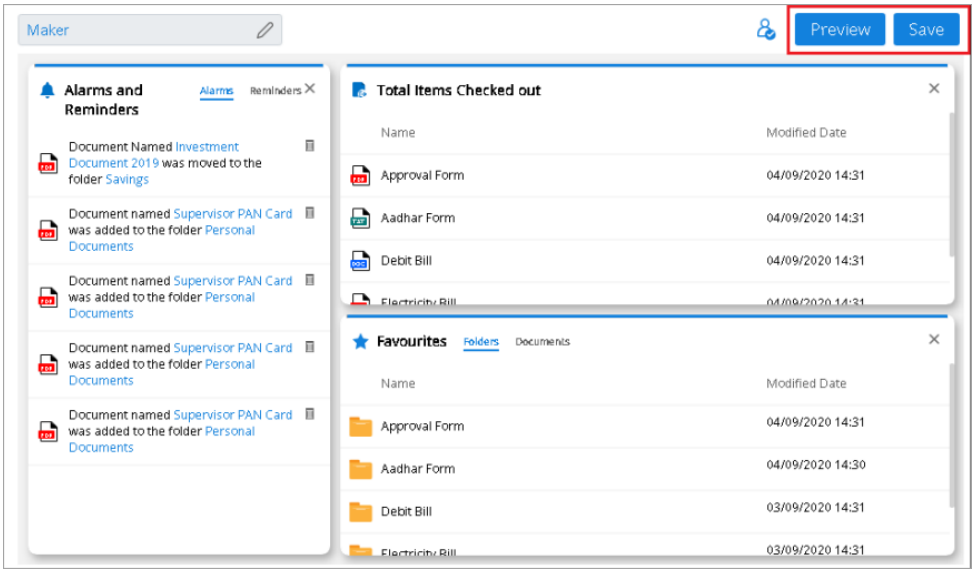
> A user can select six widgets maximum and three widgets minimum while creating a new dashboard or changing the existing ones.

3. Now, click on **Select Layout** on the right pane.



4. It will show different layout styles based upon the number of widgets you have chosen.
5. Choose the layout style.

6. Click on the **Preview button** which is along with Add button to preview the final dashboard look. Click on **Save** button otherwise.

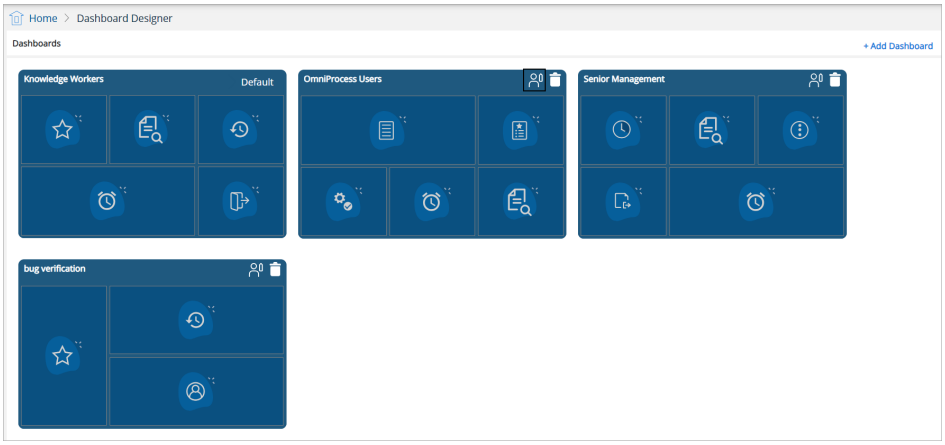


7. Dashboard configuration is saved successfully message will appear for the confirmation.

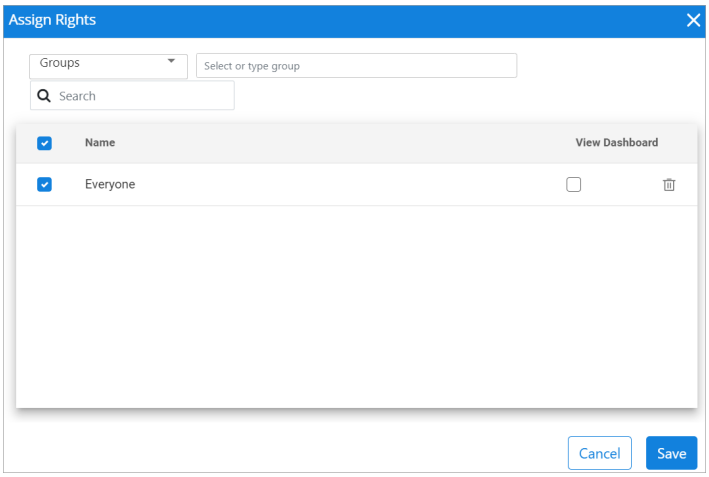
Assigning rights

To Assign Rights on the Dashboard:

1. Click on the existing dashboard.
2. Click on the **Assign Rights** button.
   OR
   open an existing dashboard and click on **Assign Rights**.



3. Assign Rights dialog box appears:

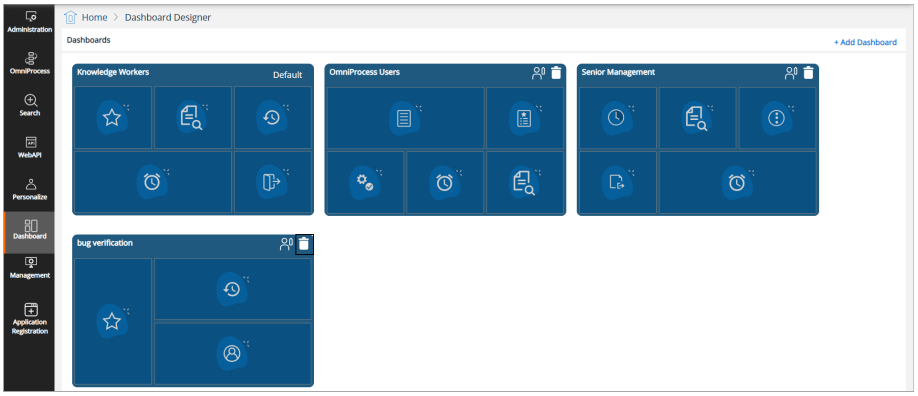


4. Select between **Groups** and **Roles**.
5. Now, select the group name to whom you want to give rights.
6. Further, choose the rights to view the dashboard or not.
7. Click on the **Trash** icon in the row to delete the groups or the roles.
8. Click on the **Save** button to save the changes.
9. Click on the **Cancel** button if you do not want to save the modifications or click on the X button.
10. Rights Assigned Successfully message will appear for the confirmation.

Deleting a dashboard

To Delete a Dashboard:

1. Go to the dashboard screen and locate the existing dashboard that you want to delete.
2. Click on the **Delete**.



3. Delete configuration confirmation dialog box appears.

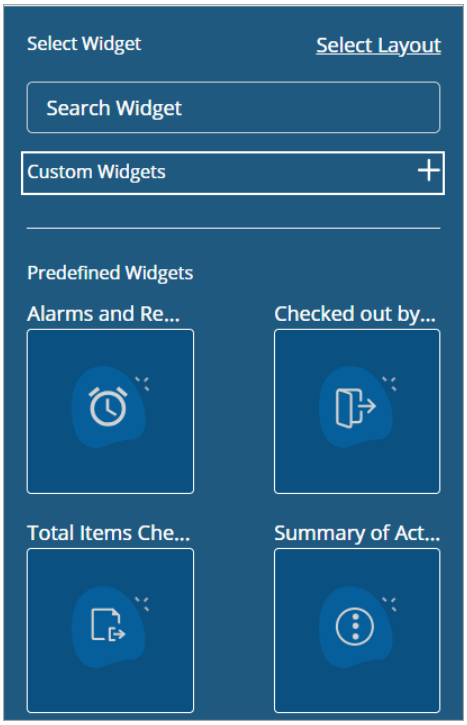
4. Click on **Confirm** to delete the dashboard, otherwise click on the Cancel.
5. Deleted Dashboard Successfully message will appear for the confirmation.

Custom widgets

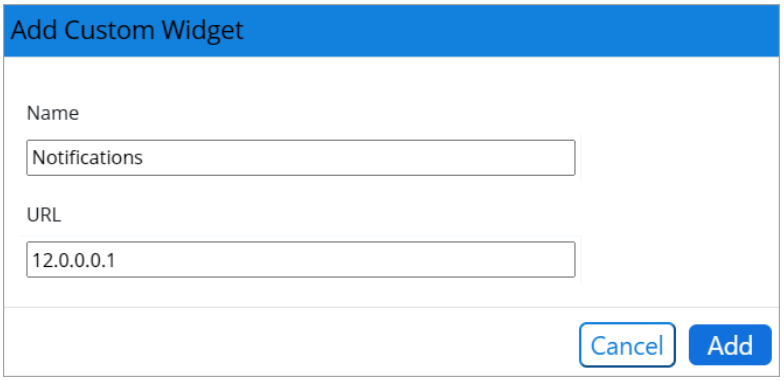
In OmniDocs Dashboard Designer, a user can create customized widgets as per the requirement.

To Create Custom Widgets:

1. Click on **Add Dashboard** button on the top right of the screen.
2. New Dashboard screen appears.



3. Click on **+** (**Custom Widgets)** on the right pane.
4. Add Custom Widget dialog box appears.

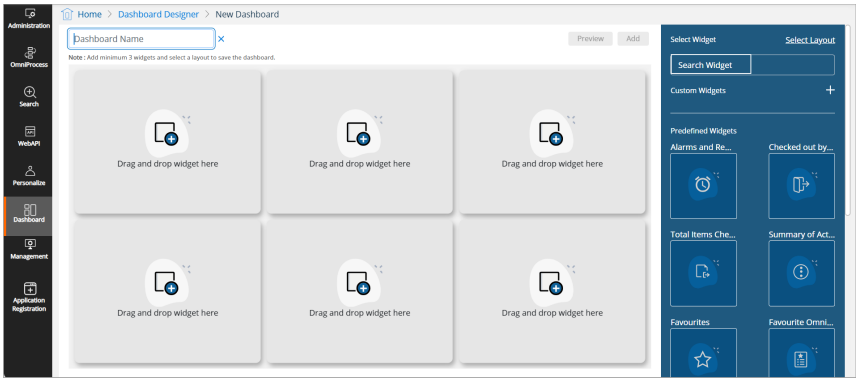


5. Fill out the widget **Name** and **URL**.
6. Click on **Add** button.

Searching a widget

In OmniDocs Dashboard Designer, a user has the option to search the widgets using the Search Widgets option. To search widgets, follow the given steps:

1. Go to the widgets pane.
2. Click on **Search Widget** in the right pane of dashboard designer.



3. Type the name of the widget that you want to search.

Predefined widgets

The predefined widgets are as follows:

Favourites

Users can mark the folders & documents as favourites from the repository. This widget represents the list of the items marked as favourite by the logged in user.

Favourite OmniProcess step

In OmniDocs, a user can mark a particular OmniProcess Step as favourite. This widget represents the list of tasks under a particular favourite marked OmniProcess Step by the logged in user.

Checked out by me

This widget represents the list of the documents checked out by the logged in user.

Total items checked out

This widget represents the total checked out items in the entire cabinet.

Summary of actions performed on documents

This widget provides a summary of actions that are performed on documents. The data can be fetched out for a particular week/month/current date.

Recently accessed

This widget represents the documents and folders recently accessed by the logged-in user.

OmniProcess - my tasks

This widget allows a user to view all the OmniProcess steps on which the logged in user has been provided rights. The pie chart is used to represent the total number of items present in a particular step and colour coding is provided for the representation of the different steps and the items present in it.

Profile

This widget helps the users to view basic user information related to the logged-in users. A user can view details like user-id, full name, last name, e-mail id. This widget also gives details like user password expiry, last login details. A user can do the profile settings and change the password through this widget.

My searches

Using this widget, a user can view search configurations and saved searches on which the user has rights.

Alarms and reminders

This widget shows all the notifications in the form of alarms and reminders which can be dismissed from the widget itself.

OmniProcess - recently completed tasks

A user can view the recently completed tasks of OmniProcess.

Tasks pending at checker step

In OmniDocs, a user can check the tasks list that are pending at the checker step.

NCC App Configuration

To access NewgenONE Content Cloud (NCC) data, organizations need an NCC access token, which can be obtained by registering an NCC application within Omnidocs.

To access the NCC App Configuration component, go to the Home screen of OmniDocs Admin, navigate to the Configure tile, and click the **NCC App Configuration** link. The NCC App Configuration screen appears.

To configure the NCC App configuration, perform the following steps:

1. From the NCC App Configuration screen, click **Configure** and specify the following details:

Field	Description
Tenant ID	Enter the tenant ID of your organization.
Organization Name	Enter your organization name.
Email ID	Enter the email ID associated with the NCC account.
Password	Enter the password for the NCC account.
App ID	Enter the application ID.
Redirect URL	Enter the redirect URL.
Secret Key	Enter the secret key to access the application.

2. Click **Save Changes** to configure the NCC App.

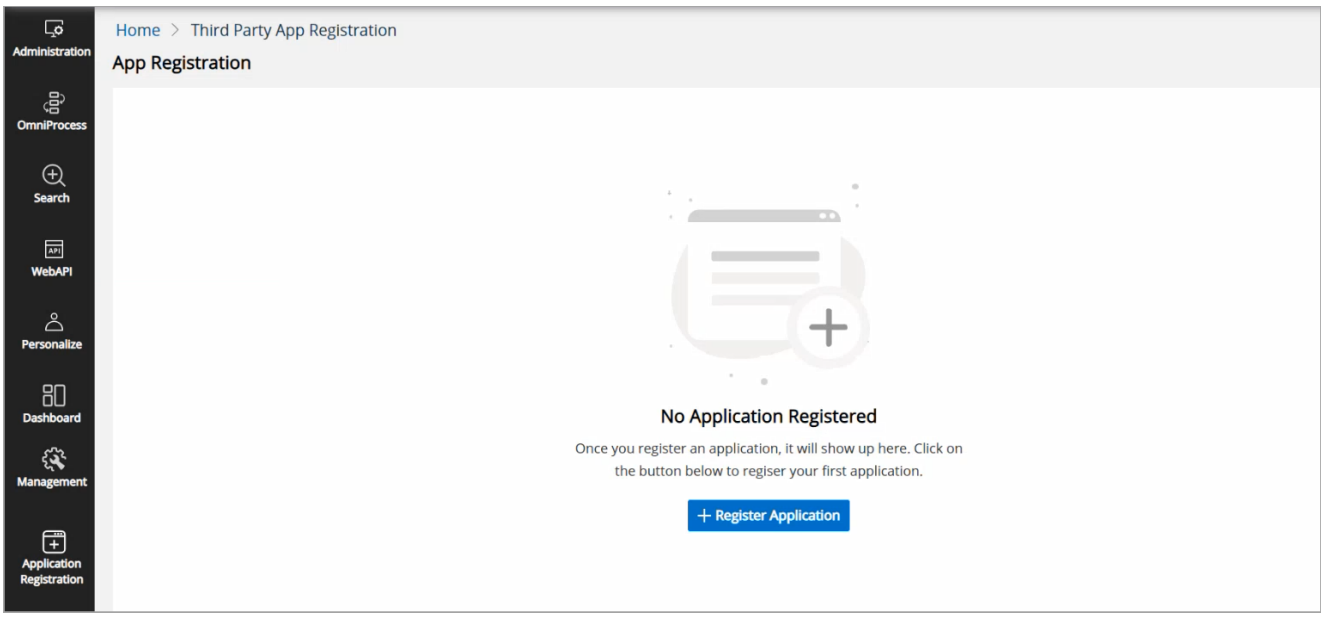
These details help in obtaining the NCC access token, which is then used for making subsequent NCC calls.

Registering Third Party App

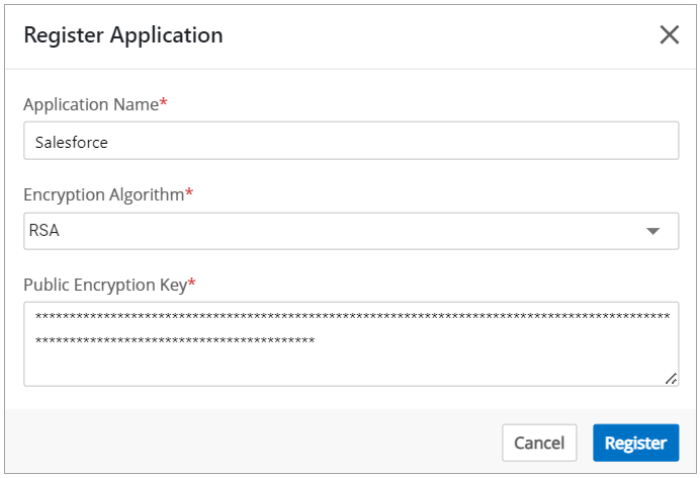
This section allows you to register the third party application in the OmniDocs. The OmniDocs users will get authenticated through OAuth only after registering third party application and OmniDocs.

To register the third party app, perform the below steps:

1. Go to **Configure** tile.
2. Click **Third Party App Registration**. The App Registration page appears.



3. Click **+Register Application**. The Register Application dialog appears.



Specify the details for the following fields:

Fields	Description
Application Name	Enter the third party application name that you want to register.
Encryption Algorithm	Select the RSA using dropdown.
Public Encryption Key	Enter the public encryption key. It is used to encrypt the data and send the data back to client or third party application.

4. Click **Register**. The App gets registered.

5.
- After the App registration, share the following details of the third party application to connect with OmniDocs:
  - Username
  - Password
  - App ID
  - Session Expiry Time

  Once done, OmniDocs returns the access details including session valid (encrypted using the client's public key) and access token tags.

  The data gets decrypted at client's end using client's private key. Further extended session time tag will be sent to OmniDocs in encrypted format which will be decrypted by the OmniDocs' private key.
- If OAuth is enabled, then the *isEncryptForCustom* value must be set to A.

Configuring NewgenONE Marvin settings

To use the NewgenONE Marvin feature in OmniDocs, you need to register and configure its engine settings in the Admin Workspace. These configuration settings include the engine name, model name, secret key, and engine URL.

For more information on how to register NewgenONE Marvin, see Registering NewgenONE Marvin.

To configure the NewgenONE Marvin settings, perform the following steps:

1. On the Admin Desktop home screen, go to the Configure tab.
2. Click **NewgenONE Marvin**.
   The Set-Up for NewgenONE Marvin page appears.
3. Turn the **Enable Marvin capabilities** toggle on. By enabling this toggle, you can now use the NewgenONE Marvin functionality in OmniDocs for question-and-answer generation.
4. Enter the following information in the corresponding fields:

Field	Description
Engine	It refers to the OpenAI model. It can be OpenAI-GPT-3.5 and OpenAI-GPT-4.
Model	It refers to the OpenAI model version for that specific engine. Select the required model version from the dropdown list.
Secret Key	It refers to the secret key allowing the OmniDocs to use the OpenAI APIs to generate AI-based content.
Engine URL	It indicates the engine URL.
Region	Select the geographical region where the service is used. Options include India, Asia Pacific, US, Canada, Australia and New Zealand, the Middle East, and Africa.
Line of Business	Select the appropriate industry or sector that aligns with your organization. Options include Banking, Insurance, Healthcare, and Government.

5. Click **Save Changes**.
   If the engine settings are configured correctly, you can then use the NewgenONE Marvin feature in OmniDocs.

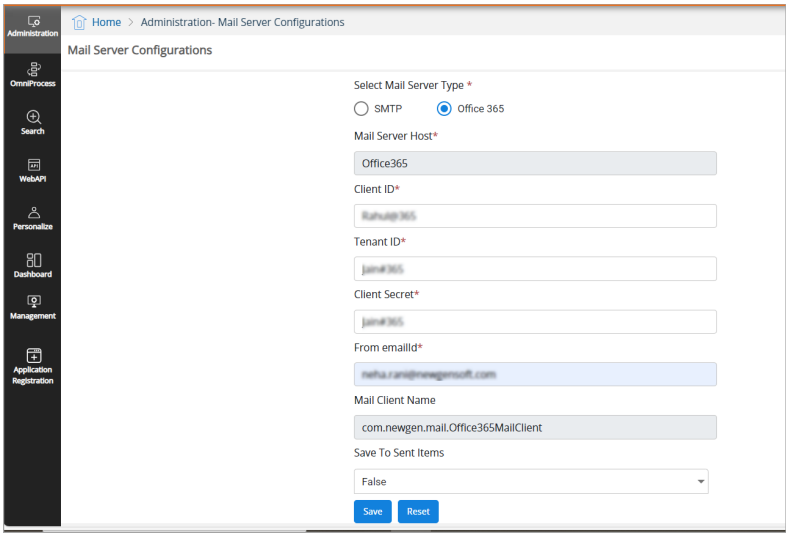
For information on how to use the NewgenONE Marvin feature, refer to the *NewgenONE OmniDocs User Guide* and *NewgenONE OmniDocs Easy Search User Guide*.

Configuring mail server

The Mail Server Configuration allows you to define mail server properties. It is used centrally across the product to send emails irrespective of the features. Defining mail server properties is mandatory for operations such as default two-factor authentication, alarm mailer, forgot password, forwarding documents, and other operations where mailing is required.

To define the Mail Server Configuration, perform the following steps:

1. In the home screen of Admin, go to **Administration** tile.
2. Click the **Mail Server Configurations** link. The Mail Server Configurations page appears.



3. Select the Mail Server Type as **SMTP** or **Office 365** option.
4. In the SMTP, specify the mail configuration details for the following fields:

Field	Description
Mail Server Host	The name of the outgoing mail server.
User Name	The email ID that you must use for sending emails.
Password	The password associated with the above email ID.
Mail Server Port	The mail server port that you must use for sending emails.
SSLEnabled	Select True if SSL is enabled, otherwise select False.

Field	Description
TLSEnabled	Select True if TLS is enabled, otherwise select False.

5. In the Office 365, specify the mail configuration details for the following fields:

Field	Description
Mail Server Host	Office365 is used as the mail server host. It is a non-editable field.
Client ID	The Client ID that you received after registering on the Azure application.
Tenant ID	The Tenant ID that you received after registering on the Azure application.
Client Secret	The Client Secret that you received after registering on the Azure application.
From emailId	The email ID that must be used for sending emails.
Mail Client Name	com.newgen.mail.Office365MailClient is as the mail client name. It is a non-editable field.
Save To Sent Items	Select True to save the sent emails to the sent items folder of the mailbox.

5. Click **Save Changes** to save the properties of the mail server.

The Reset button resets the field values to the previously saved state.

Personalize

This chapter consists of:

- Landing page configuration
- Repository view
- Tool bar
- Custom operations
- Custom Panel
- Easysearch View
- Multilingual Operations
- Document Upload Templates

Accessing Personalize

Go to NewgenONE OmniDocs Admin. Under the **Personalize** tile, click the desired operation to open it.

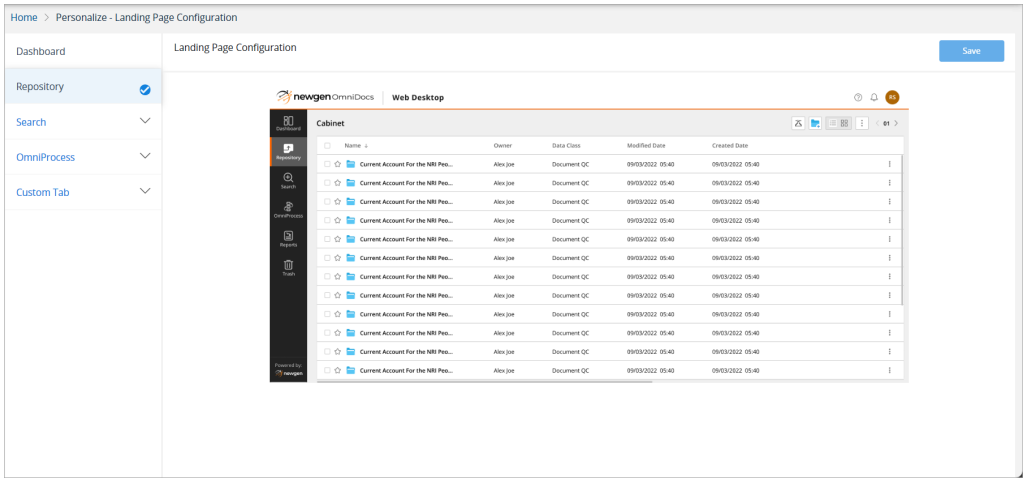
Landing page configuration

Landing Page Configuration allows the administrator to set the Landing Page for OmniDocs Web users from the various system tabs:

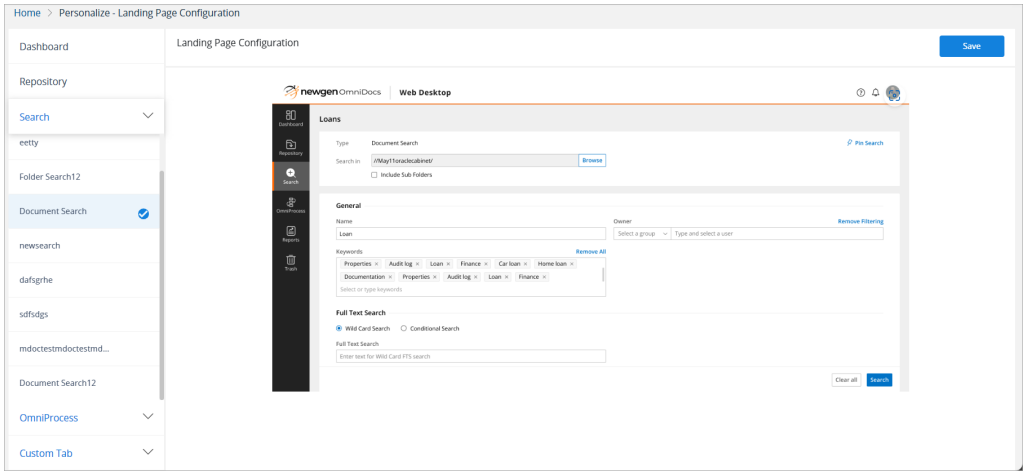
- Repository
- Search (Document Search, Folder Search and other searches configured by the **administrator**)
- OmniProcess (My Tasks)
- Custom Tabs (user-defined custom tabs)

To Configure Landing Page

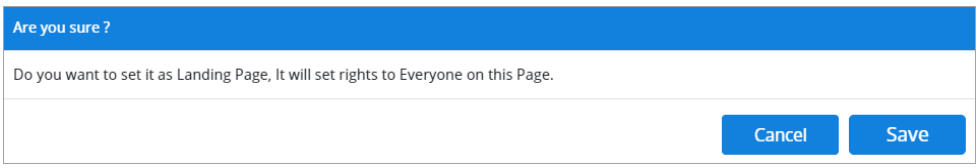
1. Go to **Personalize** tile and click on **Landing Page Configuration** link.
2. **Landing Page Configuration** screen appears. A list of all the pages that you can select as a landing page is given in the left pane.



3. Click on ⌄ against the tab to open its tray and select the desired landing page.
4. A tick mark appears against the selected landing page.
5. Click on **Save**.



6. A message box appears. Click on **Save** to confirm your selection.



7. The configuration has now been modified and confirmation message for the same appears in the top-right corner of the screen.
8. Now, login to OmniDocs Web and you will land on the page which is selected from the OmniDocs Admin.

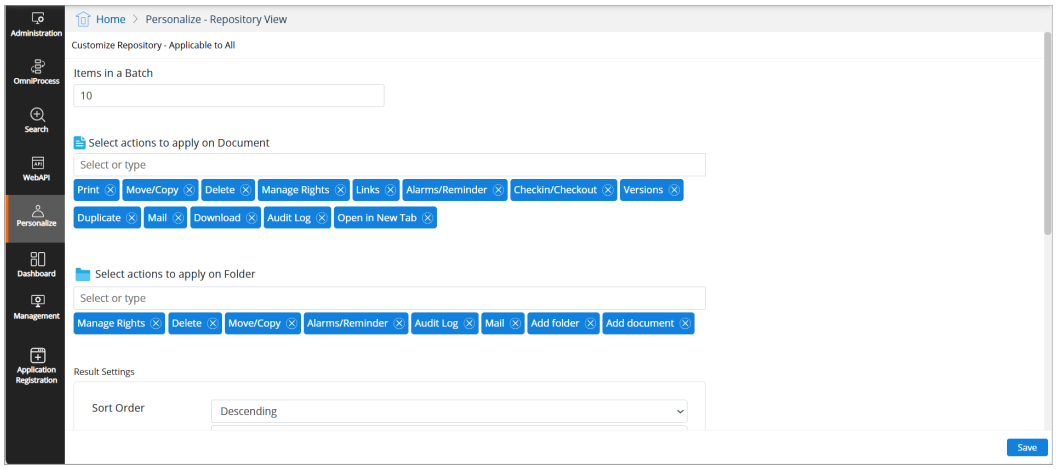
Repository view

Repository view allows you to personalize the repository view for cabinet users.

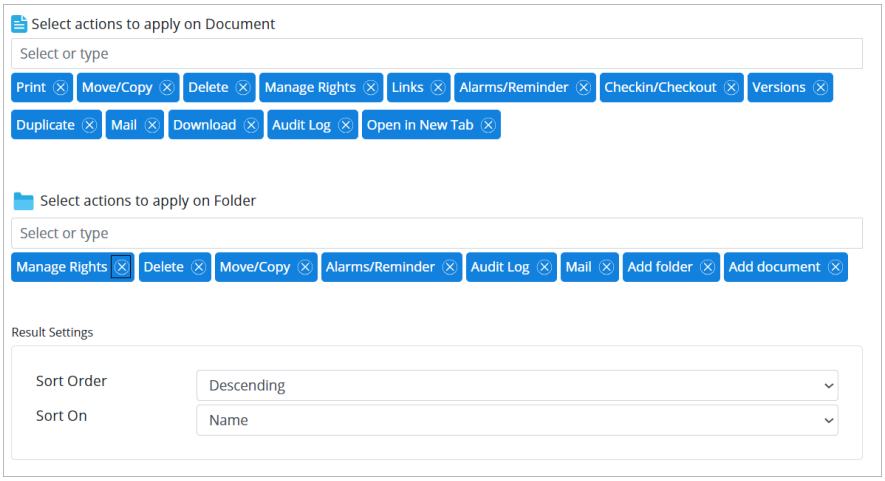
The NewgenONE OmniDocs users can configure the repository view according to their requirements. However, they can only select from the configurations made available by the administrator user.

To configure the Repository View, perform the below steps:

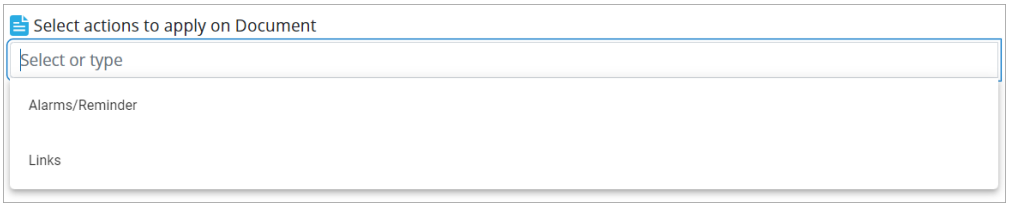
1. Go to **Personalize** tile
2. Click **Repository View**. The Repository View page appears.



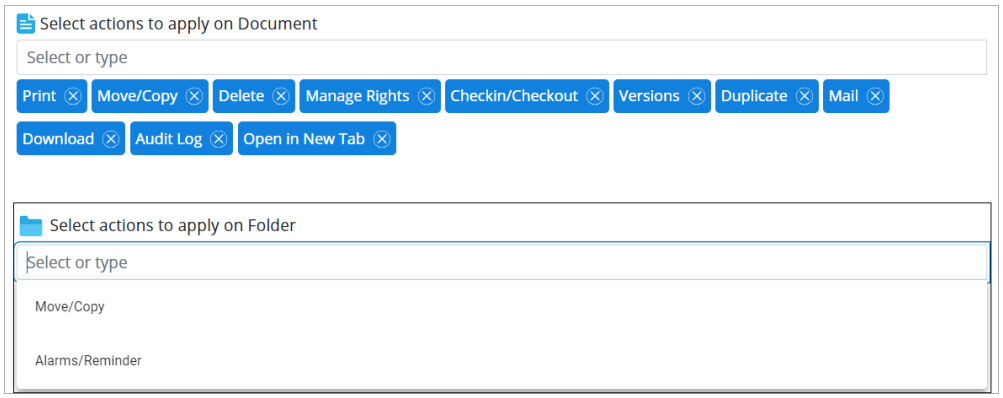
3. In the **Items in a Batch** textbox, enter the items number that you want to display in a batch. The batch size can range from 5 to 100. The default batch size is 10. This setting controls the display of folders, sub-folders, and documents.
4. In the **Select actions to apply on Document** textbox, select the actions that you want the OmniDocs users to perform on documents. By default, all the operations are selected.
   - To remove any action, click **Remove** .



- To change the order of existing and custom operations, you can drag them to the desired position.
- To apply any action, select the action from the dropdown that contains only not applied actions.



5. In the **Select actions to apply on Folder** textbox, select the operations that Web users can perform onfolders. By default, all the operations are selected.
   - To remove any action, click **Remove** .
   - To apply any action, select the action from the dropdown that contains only not applied actions.



6. In the **Result Settings and Document View Settings**, configure the result and document settings according to your requirement.
7. In the Select Columns, select the items to include in the column list of a repository.
   - To include any item, drag it from the listed items and drop it into the blue box.

- To remove any item from the selected columns, drag and drop it back into the **Select Columns** list.
- The selected items can be reordered through drag and drop.

8. Click **Save**. The Repository View gets configured.

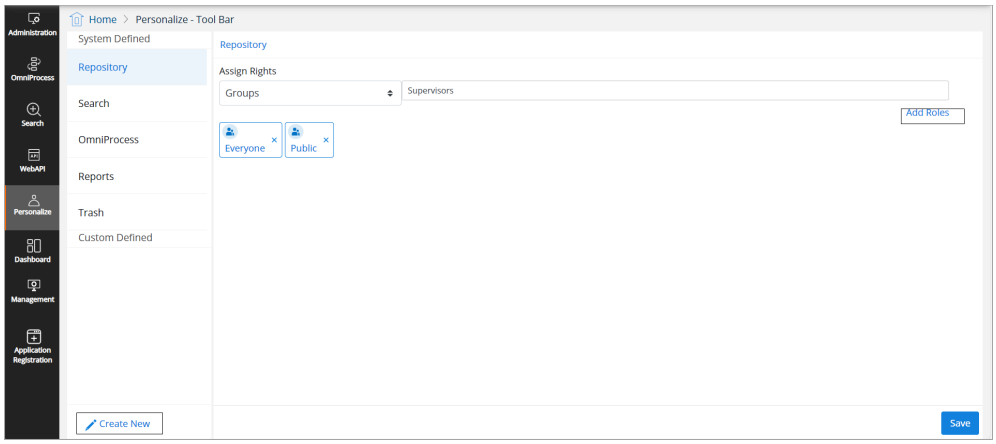
Tool bar

It allows the administrator to hide tabs from the Web users by not giving rights to them on those tabs. Those tabs will not be visible to the Web users and therefore, they cannot perform any action related to those tabs.

If any tab is set as the landing tab, then the administrator cannot hide that tab from end-users in the Web module.

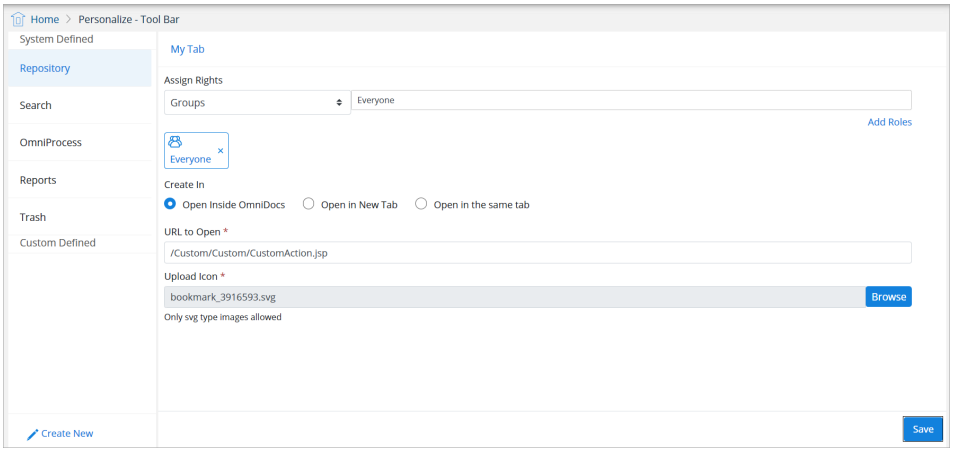
To Configure Toolbar View

1. Go to **Personalize** tile and click on **Tool Bar** link.
2. **Tool Bar** screen appears. The System Defined and Custom Defined tabs are given in the left pane.
3. **Repository** tab: Click on it to assign rights on the Repository tab.
   a. Click on **Assign Rights** and select **Groups/Users** from the dropdown.
   b. Select the desired group and users from the next dropdown list.
   c. On selecting the user name or the group name, it gets added as a patch. Click on the cross mark against the added user/group to remove it.



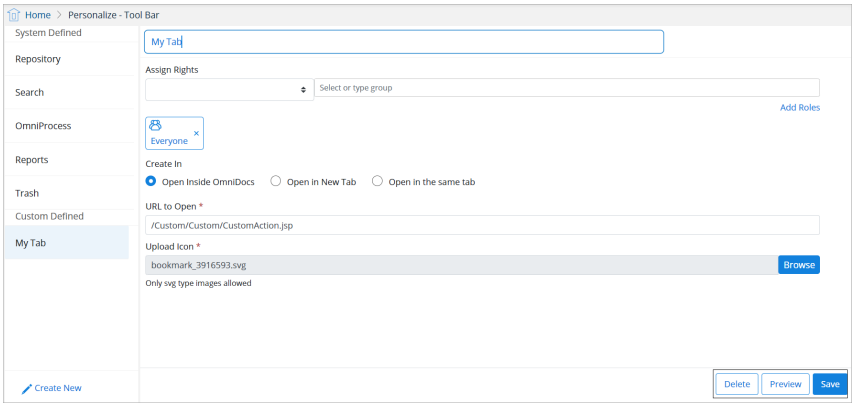
   d. Click on **Add Roles** link to assign rights to a role. The Add Role link appears on selecting Groups from Assign Rights dropdown list.
   e. Click on **Save** to save the assigned rights.

4. Similarly (as mentioned for Repository tab) you can assign rights for **Search**, **OmniProcess**, **Reports** and **Trash** tabs.
5. **Custom Defined** tabs: Click on **Create New** link to create a new custom defined tab.
    a. **Name of Tab**: Enter the name of the new tab.
    b. **Assign Rights** to Users/Groups/Roles (refer to the steps mentioned for Repository tab).
    c. **Create In**: The user gets the option to open the Custom JSP in the same tab or a new tab or inside OmniDocs. The **Open Inside OmniDocs** option is used to open the page inside OmniDocs. The **Open in the Same Tab** option is used to open the page inside the tab and **Open in New Tab** option is used to open the page in a new tab.
    d. **URL to Open**: Path of the component that needs to be displayed when the Web user clicks on the custom tab. It can be a jsp/html or any other view.
    e. **Upload Icon**: Path of the custom tab icon. Click on **Browse** to select the tile icon image file. The icon must be in .svg format.
    f. Click on **Save** to save the defined custom tab.



    g. To Delete and Modify the Custom-defined tab:
        i. Click on the required custom-defined tab to open its properties.
        ii. Click on:
            • **Save** to save the modified properties.
            • **Delete** to delete the custom-defined tab.

> The defined custom tab will appear in the web module of OmniDocs. An example of such a tab is shown below in point number 6.



6. Now login to OmniDocs Web with the user to whom the access rights are granted for this personal tab. The new personalized tab is added in the menu bar.

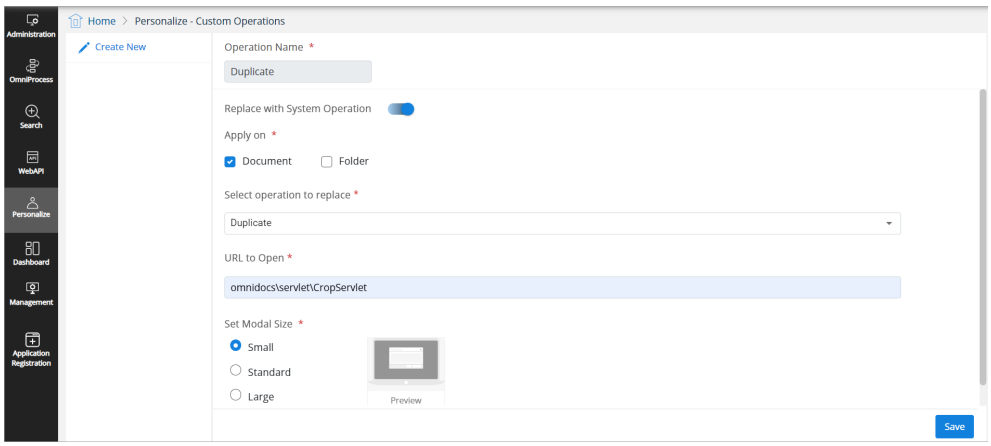
Custom operations

Custom operations allows you to use the custom framework in OmniDocs to execute custom operations on documents and folders.

To use this feature in OmniDocs Web module, provide the details related to the custom operation from OmniDocs Admin module.

To define a custom operation, perform the below steps:

1. Go to **Personalize** tile and click **Custom Operations** link. The Custom Operations page appears.



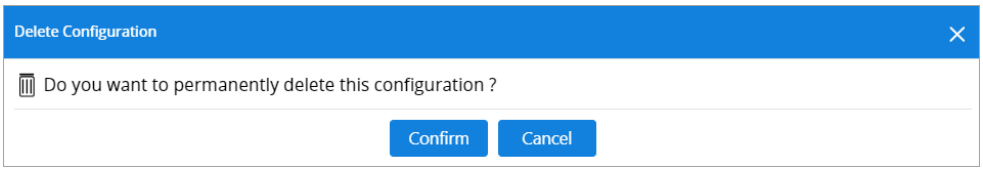
2. Enter the details for the following fields:

Field	Description
Operation Name	Enter the operation name.

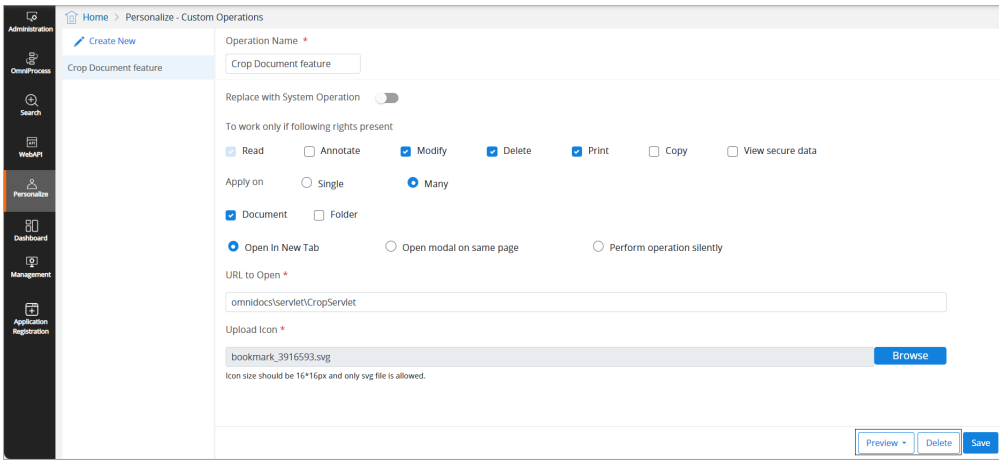
Field	Description
Replace with System Operation	Select this toggle to replace the system operations with custom operation. In case this toggle button is disabled, then your custom operations get added as it is, and will not replace your system default operations.
To work only if following rights present	Select the rights checkbox that you want to apply to the specified operation. Based on these rights, the Custom operation appears to the user in OmniDocs.
Apply on	Select one of the following checkbox: • Single — Applies on single document or folder. • Many — Applies on multiple document or folder.
	• **Document** — Select this checkbox to apply the operation on documents. • **Folder** — Select this checkbox to apply the operation on folders.
Open in New Tab	Select this option to view custom operations in new tab.
Open modal on same page	Select this option and specify the modal size.
Perform operation silently	If you don't want to launch a new UI in modal or in a new tab, then select this option. The action gets performed at the backend without launching any UI.
Select operation to replace	Select the operation using dropdown that you want to replace. The selected operation appears as the Operation Name. This field appear if you enable the Replace with System Operation toggle.
URL to Open	Enter the custom URL that you want to configure for specific custom operation.
Upload Icon	Click **Browse** and upload the icon to select the operation icon image file. The icon must be in *.svg* format.

Field	Description
Set Modal Size	Select one of the following options: • Small • Standard • Large This field appears if you select the Open modal on same page and Select operation to replace options.

3. Click **Save**. The Configuration added successfully message appears.
   The added Custom Operation appears in the left pane.
4. Double-click the added operation. The Operation appears in editable mode on right pane.
5. Change the properties and click **Save**. The Configuration gets modified.
6. Click **Delete**. The Delete Configuration dialog appears.



7. Click **Confirm**. The Configuration deleted successfully message appears.
8. Click **Preview**. The Preview dialog appears for the selected operation.
   For example, you have created the custom operation for Crop Document Feature and their properties are as follows:



- You can crop a portion of the document and save it as a new document. You must configure custom operations through the Admin Module.
- It works for a single document.
- To open the URL, use *omnidocs\servlet\CropServlet*.
- You can also use an icon for that operation, and it must be in SVG format.
- You can also define the rights on which the crop feature works.

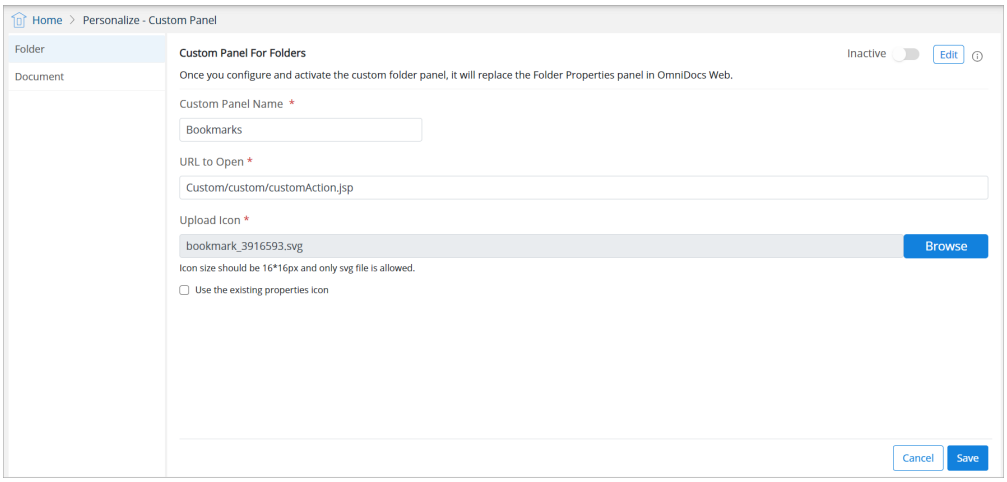
To view the added custom operation for documents or folder in the OmniDocs, you must add that custom operation in the personalized repository view.

Custom panel

The custom panel allows you to configure a new custom panel and replace it with the document and folder properties panel in the OmniDocs module.

To configure the custom panel, perform the below steps:

1. Go to **Personalize** tile.
2. Click **Custom Panel**. The Personalize - Custom Panel page appears.



3. Specify the details for the following fields:

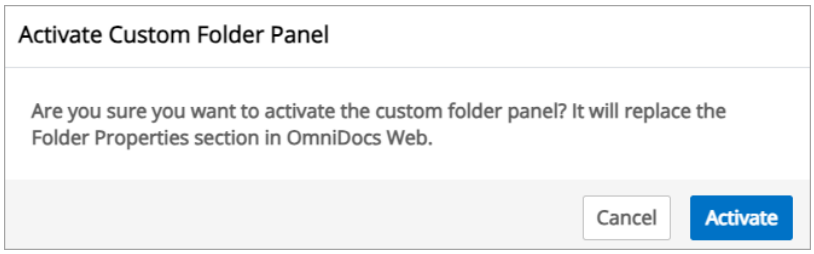
Fields	Description
Custom Panel Name	Enter the Custom Panel Name that you want to configure for documents and folders.
URL to Open	Enter the Custom Panel Name.
Upload Icon	Click **Browse** and upload the icon for the specified custom panel. The logo must be in SVG format.
Use the existing properties icon	Select this checkbox to use the existing properties icon.
Activate	Enable this toggle to activate the custom panel. For more information, refer to the activate the custom panel section. This field appears only for the saved configurations.

Fields	Description
Edit	Click this option to modify the configured custom panel. This option appears if you have deactivated the custom panel.

4. After specifying the details, click **Save**. The Configuration added successfully.

To activate the custom panel for folder or document, perform the below steps:

1. Go to the **Custom Panel**. The Personalize-Custom Panel page appears.
2. Navigate to the **Folder** or **Document** given the left pane.
3. Click the **Folder** or **Document** to configure the custom panel for folders or documents. The custom panel configuration screen appears for folders or documents.
4. Click the **Activate** option. The Activate Custom Folder Panel dialog appears.



5. Click **Activate**. The Configuration Modified successfully.

Easy Search view

With Newgen OmniDocs Easy Search, you can search for documents, folders, and media files, and simplify searches with filters and sorting options. You can search folders and content based on filters such as document name, folder name, owner, notes, annotations and more. It enables you to perform different types of searches such as fuzzy search, proximity search, boolean search, and more.

Searching for files and folders

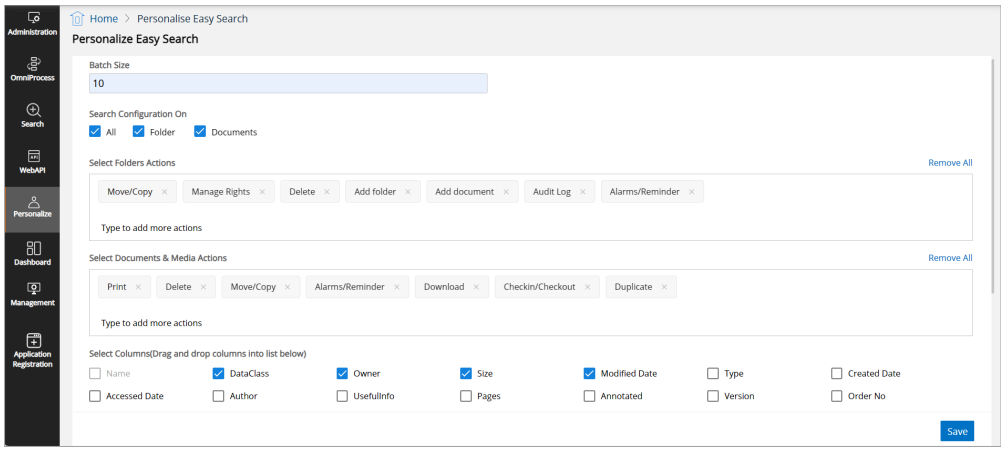
This section allows administrators to configure the following actions in Easy Search:

- Set Batch Size
- Configure columns of search results

- Configure documents view settings
- Configure search results sorting

To configure above-listed actions, perform the below steps:

1. Go to **Personalize**.
2. Click **Easysearch view**. The Personalize Easy Search page appears with the following options:



Options	Description
Batch Size	Use this option to set the batch size of search results. It can range from 5 to 100.
Search Configurations On	Use this option to perform the Easy Search on either folders, documents and media, or on both simultaneously. • All — Select this checkbox to enable search on folder, documents and media. • Folder — Select this checkbox to enable the search on the folders. • Documents and Media — Select this checkbox to enable the search on documents and media.
Select Folders Actions	Use this option to select the operations that you want to allow on the Folders. To add more actions, enter the operation name. Else, click **Remove All** to remove selected actions.
Select Documents & Media Actions	Use this option to select the operations that you want to allow on the Document and Media. To add more actions, enter the action name. click **Remove All** to remove selected actions.

Options	Description
Select Columns View Fields	Use this option to select the columns such as Accessed Date, DataClass, Owner, Size, and more. After selecting the columns, you can view them as a Column Field.
Manage Columns	Use this option to manage the Columns sequencing of operations. For changing the column's sequencing of operations, you can drag and drop the columns according to your requirement. The selected columns in Select Columns View Fields appear in the Manage Columns.
Document View Settings	Use this option to set the document view settings using the dropdown.
Sort Settings	Use this sort settings to sort the search results on the columns like Document or Folder name, Owner and more in ascending or descending order.

3. Click **Save** to apply the selected operations on Easy Search.

Multilingual definition

This feature will be a part of the Personalize tab and will be configurable through the *eworkstyle.ini*. If the flag value is set to **Y**, the feature becomes visible in the Admin module. The flag to enable/disable this feature is **DisplayMultilingualSubTile**.

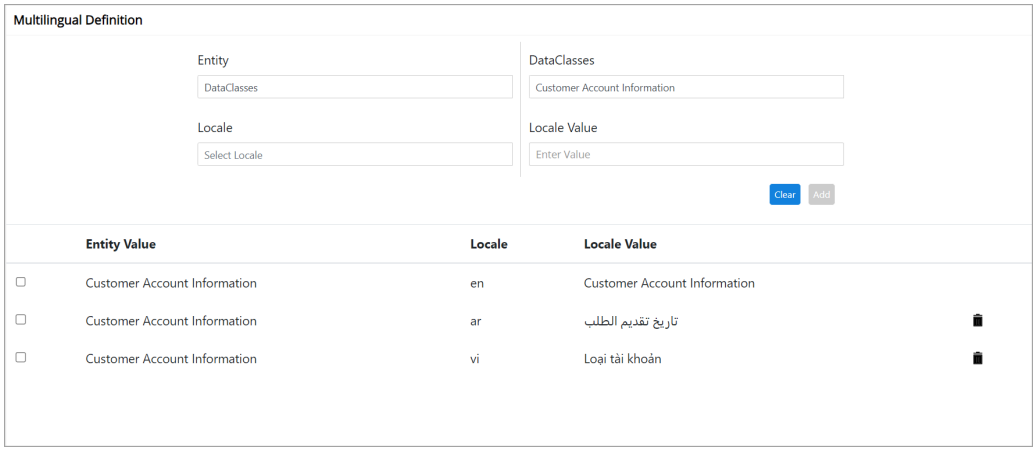
This feature enables users to add values for metadata, such as DataClasses, Global Indexes, Role, Group and their field values, in different locales. Once configured, users can view the metadata in the defined locale after selecting their respective browser locale.

The inclusion of Role and Group metadata is specific to RMS and is not applicable to OmniDocs. In OmniDocs, only DataClasses, Global Indexes, and their field values are supported for localization across different locales.

By default, the available languages for translation are Vietnamese and Arabic.

For instance, a bank can leverage the multilingual feature to enhance its operations by translating metadata related to services, such as account information and transaction history. When adding a DataClass for customer information, the bank can provide

translations in Vietnamese and Arabic. This allows employees in different regions to access and manage information in their preferred language. This approach improves communication and understanding, ensuring that bank staff can effectively serve their clients while fostering greater operational efficiency.



Document Upload Templates

The Document Upload Templates feature allows you to configure templates for uploading documents. These templates enable the association of specific metadata fields with documents during upload. You can set metadata fields such as global index, author, description, dataclass, and keywords. Furthermore, you can rearrange these fields and mark them as mandatory.

To access this feature, navigate to the Configure tile from the OmniDocs home page, and click **Document Upload Templates**. The Document Upload Templates screen appears displaying a default template where DataClass and Keywords are selected in the visibility options for metadata tagging. You can edit this template or create a new one.

To create a new document template, perform the following steps:

1. From the left pane of the Document Upload Templates screen, Click **+Create Template**.

2. Enter the following details in the fields:

Field	Description
Template Name	Allows you to give a name to the template.
Description	Allows you to add a description for the template.

3. You can select following metadata fields for different document upload templates as follows:
    - **Global Index** — A unique identifier for the document.
    - **Author** — The name of the person who created the document.
    - **Description** — Any description that users want to add with the document.
    - **Dataclass** — The classification or category of the document.
    - **Keywords** — Tags or keywords users want to associate with the documents for quick retrieval.

    You can rearrange the sequencing of metadata fields by holding the drag icon ⠿ next to the specific field and moving it to the required position.

4. Select the Mandatory checkbox next to the field you want define as mandatory.
5. Click **Create** to save the template.

To edit a created template, perform the following steps:

1. From the left pane on the Document Upload Templates page, select a specific template and click the **Edit** button displayed in the right pane.
2. Make the necessary changes to the template, such as modifying the metadata fields, rearranging them, or marking them as mandatory.
3. Click the **Save Changes** button to save the modifications made to the template or click **Reset Changes** to revert the template to its previous state before any edits.

You can delete a template by clicking **Delete**. However, you cannot delete the last remaining template, and there must always be at least one template left in the template list.

Management

This chapter consists of:

- Report Management
- License Management
- Service Management
- Trash Management
- Storage Transition Manager

Report management

The Reports Management feature allows you to extract detailed and summary reports on users, documents, and folders related data. It helps in making important decisions and setting policies. You can export all reports in XLS and CSV file formats for future use.

To Access System Reports:

1. On the Home screen of OmniDocs Admin, go to the Management tile.
2. Click **Report Management**. The Report Management screen appears.

Manage rights

This option allows you to control the access and permissions for specific reports within OmniDocs. You can select the user(s) or group(s) to share a report, granting them read access based on their roles and responsibilities.

To give rights on the report, perform the following steps:

1. From the left pane of the Report Management screen, select a specific report. The option related to the selected report appears in the right pane.
2. Click the **Manage Rights** button, the Manage Rights page appears.

3. Click the **Add User(s)/Group(s)** button, the Manage User/Group Rights dialog appears displaying the following options:

Option	Description
Select Type	Allows you to choose between group and user.
Add All	Allows you to select all the users or groups in one click.
Available User or Group	Displays you the available user or group to assign rights.
Selected User or Group	Displays you the selected user or group.
Search	Allows you to search the user or group.
Remove All	Allows you to remove all the users or groups in one click.

4. Click the user or group in the available list to add it to the selected user or group list.
5. Click the **Save** button, the selected users or groups given rights on the report.

To remove rights from the report, perform the following steps:

1. Click the **Manage Rights** button. The Manage Rights page appears with the list of right-assigned users or groups.
2. Click the delete icon against the desired user or group to remove.
   On clicking the delete icon, a dialog box seeking your confirmation appears.
3. Click **Remove** to delete the selected user or group, else tap **Cancel** to abort the process.
   You can delete all the users or groups at once by clicking the **Remove All** button.

Application license usage summary report

Application license usage summary report is used to generate the report of maximum and minimum license usage of the application between the specified date ranges.

To generate the application license usage summary report, perform the following steps:

1. Click the calendar icon to specify the date range. The date range includes the From and To dates.
2. From the Application Name dropdown, select a specific application.

3. Choose the file format in which you want to export the summary report. The following are the supported file formats:
   • XLS — To generate the summary report in XLS format.
   • CSV — To generate the summary report in CSV format.
4. Click **Generate Report**. The report is generated and downloaded in the selected file format.

Application license violation details

Application license violation details generate reports on instances when the license count of an application is exceeded. It also tracks when a user logs into an application with which they are not associated.

To generate the application license violation report, perform the following steps:

1. Click the calendar icon to specify the date range. The date range includes the From and To dates.
2. From the Application Name dropdown, select a specific application.
3. Choose the file format in which you want to export the violation details. The following are the supported file formats:
   • XLS — To generate the summary report in XLS format.
   • CSV — To generate the summary report in CSV format.
4. Click **Generate Report**. The report is generated and downloaded in the selected file format.

Cabinet summary report

OmniDocs cabinet summary report provides information on the most common attributes of cabinets. It also provides details like the total number of documents, folders, users, groups, data classes, global indexes, and more.

To generate the cabinet summary report, perform the following steps:

1. Select the Include Cabinet Tree checkbox if you want to add the cabinet tree.
2. Choose the file format in which you want to export the summary report. The following are the supported file formats:
   • XLS — To generate the summary report in XLS format.
   • CSV — To generate the summary report in CSV format.
3. Click **Generate Report**. The report is generated and downloaded in the selected file format.

Data definition ACL report

Data definition ACL report provides the rights available to users on data classes.

To generate the data definition ACL report, perform the following steps:

1. Choose the file format in which you want to export the report. The following are the supported file formats:
   • XLS — To generate the summary report in XLS format.
   • CSV — To generate the summary report in CSV format.
2. Click **Generate Report**. The report is generated and downloaded in the selected file format.

Document creation report

Document creation report generates the report and provides information on created documents for a specific time period.

To generate the document creation report, perform the following steps:

1. Select from the Look In option, either Cabinet for documents from a cabinet directory or Folder for a specific folder.
2. Click the calendar icon to specify the date range. The date range includes the From and To dates.
3. Choose the file format in which you want to export the report. The following are the supported file formats:
   • XLS — To generate the summary report in XLS format.
   • CSV — To generate the summary report in CSV format.
4. Click **Generate Report**. The report is generated and downloaded in the selected file format.

Document creation summary report

Document creation summary report generates a report to provide the total number of documents created along with its folder names during the time period specified.

To generate the document creation summary report, perform the following steps:

1. Select from the Look In option, either Cabinet for documents from a cabinet directory or Folder for a specific folder.
2. Click the calendar icon to specify the date range. The date range includes the From and To dates.
3. Select the Include Leaf Flag checkbox if you want to add the leaf flag.
4. From the Select A Level dropdown, select a specific level.
5. Choose the file format in which you want to export the report. The following are the supported file formats:
   • XLS — To generate the summary report in XLS format.
   • CSV — To generate the summary report in CSV format.

6. Click **Generate Report**. The report is generated and downloaded in the selected file format.

Folder creation report

Folder creation report generates the report and gives you the information on folders created during the time period specified.

To generate the folder creation report, perform the following steps:

1. Select from the *Look In* option, either *Cabinet* for documents from a cabinet directory or *Folder* for a specific folder.
2. Click the calendar icon to specify the date range. The date range includes the *From* and *To* dates.
3. Choose the file format in which you want to export the report. The following are the supported file format:
   • XLS — To generate the summary report in XLS format.
   • CSV — To generate the summary report in CSV format.
4. Click **Generate Report**. The report is generated and downloaded in the selected file format.

Document reconciliation report

The document reconciliation report generates a report that describes the documents. It provides various options, such as Look In to locate documents or folders at either the cabinet level or the folder level and Date Range to locate documents within a specified time span. Additionally, you can make your choice based on the data class and the associated fields.

To generate the document reconciliation report, perform the following steps:

1. Select from the Look In option, either Cabinet for documents from a cabinet directory or Folder for a specific folder.
2. Click the calendar icon to specify the date range. The date range includes the From and To dates.
3. From the Select Data Class dropdown, select a specific data class.

4. Click **Generate Report**. The report is generated and downloaded in the selected file format.

Document data report

The document data report allows you to generate detailed reports on documents. You can obtain document-related information at the cabinet or folder level. Additionally, there is an option to generate reports for documents associated with a particular data class.

To generate the document data report, perform the following steps:

1. Select from the Look In option, either Cabinet for documents from a cabinet directory or Folder for a specific folder.
2. Select from the Report Criteria option, either All Document for all documents or Data Class for a specific data class.
3. Choose the file format in which you want to export the report. The following are the supported file formats:
   • XLS — To generate the summary report in XLS format.
   • CSV — To generate the summary report in CSV format.
4. Click **Generate Report**. The report is generated and downloaded in the selected file format.

Folder data report

The folder data report allows you to generate detailed reports on folder data. It provides an option to get the folder related information at the cabinet level or of some specific folder. The option is available to get the report of folders on which a particular data class is associated.

To generate the folder data report, perform the following steps:

1. Select from the Look In option, either Cabinet for documents from a cabinet directory or Folder for a specific folder.
2. Select from the Report Criteria option to Data Class for a specific data class.
3. Choose the file format in which you want to export the report. The following are the supported file formats:

- XLS — To generate the summary report in XLS format.
- CSV — To generate the summary report in CSV format.

4. Click **Generate Report**. The report is generated and downloaded in the selected file format.

General report

The general report generates a report giving descriptions of the documents or folders. It provides you with various options such as Look In to locate documents or folders either at cabinet level or folder level, date range to locate within a specified span of time. Further, you can also generate reports based on the data class and the fields associated with them.

To generate the general report, perform the following steps:

1. Select from the Look In option, either Cabinet for documents from a cabinet directory or Folder for a specific folder.
2. Click the calendar icon to specify the date range. The date range includes the From and To dates.
3. Select from the Search option, either Document to search within documents or Folder to search from folder.
4. Select from the Report Criteria option, either All Document for all documents or Data Class for a specific data class.
5. Choose the file format in which you want to export the report. The following are the supported file formats:
   - XLS — To generate the summary report in XLS format.
   - CSV — To generate the summary report in CSV format.
6. Click **Generate Report**. The report is generated and downloaded in the selected file format.

License summary report

The license summary report provides you the summary of the number of licenses of each type for each application registered in the system and also the concurrent licenses available for the same.

To generate the license summary report, perform the following steps:

1. From the Application Name dropdown, select a specific application.
2. Choose the file format in which you want to export the summary report. The following are the supported file formats:
   • XLS — To generate the summary report in XLS format.
   • CSV — To generate the summary report in CSV format.
3. Click **Generate Report**. The report is generated and downloaded in the selected file format.

Folder creation summary report

The folder creation summary report generates the report and provides you with the total number of folders created along with the folder name during the time period specified.

To generate the folder creation summary report, perform the following steps:

1. Select from the Look In option, either Cabinet for documents from a cabinet directory or Folder for a specific folder.
2. Click the calendar icon to specify the date range. The date range includes the From and To dates.
3. Select the Include Leaf Flag checkbox if you want to add the leaf flag.
4. From the Select A Level dropdown, select a specific level.
5. Choose the file format in which you want to export the report. The following are the supported file formats:
   • XLS — To generate the summary report in XLS format.
   • CSV — To generate the summary report in CSV format.
6. Click **Generate Report**. The report is generated and downloaded in the selected file format.

Document data summary report

The document data summary report enables you to generate the document data summary report. It provides an option to get the document summary at the cabinet

level or folder level. The option is available to get report of documents on which a particular data class is associated.

To generate the document data summary report, perform the following steps:

1. Select from the Look In option, either Cabinet for documents from a cabinet directory or Folder for a specific folder.
2. Select from the Report Criteria option, either All Document for all documents or Data Class for a specific data class.
3. Select the Include Leaf Flag checkbox if you want to add the leaf flag.
4. From the Select A Level dropdown, select a specific level.
5. Choose the file format in which you want to export the report. The following are the supported file formats:
   • XLS — To generate the summary report in XLS format.
   • CSV — To generate the summary report in CSV format.
6. Click **Generate Report**. The report is generated and downloaded in the selected file format.

Folder data summary report

The folder data summary report enables you to generate the folder data summary report. It provides an option to get the folder related information at the cabinet level or of some specific folder. The option is available to get report of folders on which a particular data class is associated.

To generate the folder data summary report, perform the following steps:

1. Select from the Look In option, either Cabinet for documents from a cabinet directory or Folder for a specific folder.
2. Select from the Report Criteria option to Data Class for a specific data class.
3. Select the Include Leaf Flag checkbox if you want to add the leaf flag.
4. From the Select A Level dropdown, select a specific level.
5. Choose the file format in which you want to export the report. The following are the supported file formats:
   • XLS — To generate the summary report in XLS format.
   • CSV — To generate the summary report in CSV format.
6. Click **Generate Report**. The report is generated and downloaded in the selected file format.

User login info report

User login info report generates the report of the users who have logged in between the specified date range.

To generate the user login info report, perform the following steps:

1. Click the calendar icon to specify the date range. The date range includes the From and To dates.
2. Choose the file format in which you want to export the report. The following are the supported file formats:
   • XLS — To generate the summary report in XLS format.
   • CSV — To generate the summary report in CSV format.
3. Click **Generate Report**. The report is generated and downloaded in the selected file format.

Folder ACL report

Folder ACL report generates the report of rights available to users on folders.

To generate the folder ACL report, perform the following steps:

1. Select from the Look In option, either Cabinet for documents from a cabinet directory or Folder for a specific folder.
2. Select the Include Leaf Flag checkbox if you want to add the leaf flag.
3. From the Select A Level dropdown, select a specific level.
4. Choose the file format in which you want to export the report. The following are the supported file formats:
   • XLS — To generate the summary report in XLS format.
   • CSV — To generate the summary report in CSV format.
5. Click **Generate Report**. The report is generated and downloaded in the selected file format.

System access report

System access report retrieves the details of users logged in the applications like OmniDocs, and iBPS for the defined duration. It can be generated for three months, on a daily, and monthly basis.

To generate the system access report, perform the following steps:

1. Select from the Report Type option, either Daily for the daily report or Monthly for the monthly report for the selected duration of time.
2. Click the calendar icon to specify the date range. The date range includes the From and To dates.
3. From the Application Name dropdown, select a specific application.
4. Enter the number of hours for login to the user in the User Login Duration field.
5. Choose the file format in which you want to export the report. The following are the supported file formats:
   • XLS — To generate the summary report in XLS format.
   • CSV — To generate the summary report in CSV format.
6. Click **Generate Report**. The report is generated and downloaded in the selected file format.

Document without data definition report

Document without data definition report generates the report of the total number of documents in a folder that have no data class associated with them.

To generate the document without data definition report, perform the following steps:

1. Select from the Look In option, either Cabinet for documents from a cabinet directory or Folder for a specific folder.
2. Select the Include Leaf Flag checkbox if you want to add the leaf flag.
3. From the Select A Level dropdown, select a specific level.
4. Choose the file format in which you want to export the report. The following are the supported file formats:
   • XLS — To generate the summary report in XLS format.
   • CSV — To generate the summary report in CSV format.

5. Click **Generate Report**. The report is generated and downloaded in the selected file format.

User document report

The user document report generates the report of the number of documents uploaded by each user within a folder.

To generate the user document report, perform the following steps:

1. Select from the Look In option, either Cabinet for documents from a cabinet directory or Folder for a specific folder.
2. Choose the file format in which you want to export the report. The following are the supported file formats:
   • XLS — To generate the summary report in XLS format.
   • CSV — To generate the summary report in CSV format.
3. Click **Generate Report**. The report is generated and downloaded in the selected file format.

User access detail report

User access summary report generates the report of logged in period for users in OmniDocs between the specified date range. Use the Select Group List filter to display specific results.

To generate the user access detail report, perform the following steps:

1. Click the calendar icon to specify the date range. The date range includes the From and To dates.
2. Click **+Add Users**, and a dialog appears to add users for inclusion or exclusion from the report.
3. Choose the file format in which you want to export the report. The following are the supported file formats:
   • XLS — To generate the summary report in XLS format.
   • CSV — To generate the summary report in CSV format.
4. Click **Generate Report**. The report is generated and downloaded in the selected file format.

User access summary report

User access summary report generates the report of the signed-in period for users in OmniDocs between the specified date range. Use the Select Group List filter to display specific results.

To generate the user access summary report, perform the following steps:

1. Click the calendar icon to specify the date range. The date range includes the From and To dates.
2. Click **+Add Users**, and a dialog appears to add users for inclusion or exclusion from the report.
3. Choose the file format in which you want to export the report. The following are the supported file formats:
    - XLS — To generate the summary report in XLS format.
    - CSV — To generate the summary report in CSV format.
4. Click **Generate Report**. The report is generated and downloaded in the selected file format.

Folder data field report

The folder data field report provides you the information on folders and a summary of documents present inside it. It provides an option to get the folder related information at the cabinet level or of some specific folder. The option is available to get the report of folders on which a particular data class is associated.

To generate the folder data field report, perform the following steps:

1. Select from the Look In option, either Cabinet for documents from a cabinet directory or Folder for a specific folder.
2. Click the calendar icon to specify the date range. The date range includes the From and To dates.
3. Select from the Report Criteria option to Data Class for a specific data class.
4. Choose the file format in which you want to export the report. The following are the supported file formats:
    - XLS — To generate the summary report in XLS format.
    - CSV — To generate the summary report in CSV format.

5. Click **Generate Report**. The report is generated and downloaded in the selected file format.

Maker-checker report

Make-checker report provides information for dual authorization in user, group, or role related operations.

Pending Request Report:

The pending request report provides you with the data related to all pending requests during a specific time range. It generates a report providing the total number of request details that are pending in the system.

To generate the pending request report, perform the following steps:

1. Select from the Maker list option, either Include User to include the users or Exclude User to exclude user from the report.
2. Click **+Add Users**, and a dialog appears to add users for inclusion or exclusion from the maker list.
3. Select the Request Date checkbox to enable the date range.
4. Click the calendar icon to specify the date range. The date range includes the From and To dates.
5. From the Requested Operations dropdown, select the required requested operations.
6. Choose the file format in which you want to export the report. The following are the supported file formats:
    - XLS — To generate the summary report in XLS format.
    - CSV — To generate the summary report in CSV format.
7. Click **Generate Report**. The report is generated and downloaded in the selected file format.

Approved Request Report:

The approved request report provides you with the data related to all requests approved by the checker during a specific time range. It generates a report providing the total number of request details that are approved in the system.

To generate the approved request report, perform the following steps:

1. Select from the Maker list option, either Include User to include the users or Exclude User to exclude the user from the maker list.
2. Click **+Add Users**, and a dialog appears to add users for inclusion or exclusion from the report.
3. Select the Request Date checkbox to enable the date range.
4. Click the calendar icon to specify the date range. The date range includes the From and To dates.
5. From the Requested Operations dropdown, select the required requested operations.
6. Select from the Checker list option, either Include User to include the users or Exclude User to exclude user from the checker list.
7. Click **+Add Users**, and a dialog appears to add users for inclusion or exclusion from the maker list.
8. Select the Request Date checkbox to enable the date range.
9. Click the calendar icon to specify the date range. The date range includes the From and To dates.
10. From the Requested Operations dropdown, select the required requested operations.
11. Choose the file format in which you want to export the report. The following are the supported file formats:
    - XLS — To generate the summary report in XLS format.
    - CSV — To generate the summary report in CSV format.
12. Click **Generate Report**. The report is generated and downloaded in the selected file format.

Rejected Request Report:

The rejected request report provides you with the data related to requests rejected by the checker during a specific time range. It generates a report providing the total number of request details that are rejected in the system.

To generate the rejected request report, perform the following steps:

1. Select from the Maker list option, either Include User to include the users or Exclude User to exclude the user from the maker list.
2. Click **+Add Users**, and a dialog appears to add users for inclusion or exclusion from the maker list.

3. Select the Request Date checkbox to enable the date range.
4. Click the calendar icon to specify the date range. The date range includes the From and To dates.
5. From the Requested Operations dropdown, select the required requested operations.
6. Select from the Checker list option, either Include User to include the users or Exclude User to exclude user from the checker list.
7. Click **+Add Users**, and a dialog appears to add users to the list to include or exclude from the checker list.
8. Select the Request Date checkbox to enable the date range.
9. Click the calendar icon to specify the date range. The date range includes the From and To dates.
10. From the Requested Operations dropdown, select the required requested operations.
11. Choose the file format in which you want to export the report. The following are the supported file format:
    - XLS — To generate the summary report in XLS format.
    - CSV — To generate the summary report in CSV format.
12. Click **Generate Report**. The report is generated and downloaded in the selected file format.

Failed Request Report:

The failed request report provides you with the data related to all failed requests with comments during a specific time range. It generates a report providing the total number of request details that failed in the system.

To generate the failed request report, perform the following steps:

1. Select from the Maker list option, either Include User to include the users or Exclude User to exclude the user from the maker list.
2. Click **+Add Users**, and a dialog appears to add users for inclusion or exclusion from the maker list.
3. Select the Request Date checkbox to enable the date range.
4. Click the calendar icon to specify the date range. The date range includes the From and To dates.
5. From the Requested Operations dropdown, select the required requested operations.

6. Select from the Checker list option, either Include User to include the users or Exclude User to exclude user from the checker list.
7. Click **+Add Users**, and a dialog appears to add users to the list to include or exclude from the checker list.
8. Select the Request Date checkbox to enable the date range.
9. Click the calendar icon to specify the date range. The date range includes the From and To dates.
10. From the Requested Operations dropdown, select the required requested operations.
11. Choose the file format in which you want to export the report. The following are the supported file formats:
    - XLS — To generate the summary report in XLS format.
    - CSV — To generate the summary report in CSV format.
12. Click **Generate Report**. The report is generated and downloaded in the selected file format.

Advanced Request Report:

The advanced request report provides you with the data related to all pending, approved, rejected, and failed requests during a specific time range.

To generate the advanced request report, perform the following steps:

1. Select from the Maker list option, either Include User to include the users or Exclude User to exclude the user from the maker list.
2. Click **+Add Users**, and a dialog appears to add users to the list to include or exclude from the maker list.
3. Select the Request Date checkbox to enable the date range.
4. Click the calendar icon to specify the date range. The date range includes the From and To dates.
5. From the Requested Operations dropdown, select the required requested operations.
6. Select from the Checker list option, either Include User to include the users or Exclude User to exclude user from the checker list.
7. Click **+Add Users**, and a dialog appears to add users to the list to include or exclude from the checker list.
8. Select the Request Date checkbox to enable the date range.
9. Click the calendar icon to specify the date range. The date range includes the From and To dates.

10. Select the Requested Operations from the dropdown to select the desired user.
11. Select the State from the dropdown to select the current state of the report.
12. Choose the file format in which you want to export the report. The following are the supported file formats:
    - XLS — To generate the summary report in XLS format.
    - CSV — To generate the summary report in CSV format.
13. Click **Generate Report**. The report is generated and downloaded in the selected file format.

Group privilege report

Group privilege report generates the report of groups with assigned privileges between the specified date range.

To generate the group privilege report, perform the following steps:

1. Click the calendar icon to specify the date range. The date range includes the From and To dates.
2. Choose the file format in which you want to export the report. The following are the supported file formats:
   - XLS — To generate the summary report in XLS format.
   - CSV — To generate the summary report in CSV format.
3. Click **Generate Report**. The report is generated and downloaded in the selected file format.

Group role privilege report

Group role privilege report generates the report of roles with assigned privileges between the specified date range.

To generate the group role privilege report, perform the following steps:

1. Click the calendar icon to specify the date range. The date range includes the From and To dates.
2. Choose the file format in which you want to export the report. The following are the supported file formats:
   - XLS — To generate the summary report in XLS format.

- CSV — To generate the summary report in CSV format.

3. Click **Generate Report**. The report is generated and downloaded in the selected file format.

User listing report

The user listing report generates the report of users created between the specified date range. Use Select Group List filter to display specific results.

To generate the user listing report, perform the following steps:

1. Click the calendar icon to specify the date range. The date range includes the *From* and *To* dates.
2. Click **+Add Group**, and a dialog appears with the available group list. Select the required groups and click **save**.
3. Choose the file format in which you want to export the user listing details. The following are the supported file formats:
   - XLS — To generate the summary report in XLS format.
   - CSV — To generate the summary report in CSV format.
4. Click **Generate Report**. The report is generated and downloaded in the selected file format.

Dormant user report

The dormant user report generates the report of users who are not signed in to OmniDocs between the specified date range. Use the Select Group List filter to display specific results.

To generate the dormant user report, perform the following steps:

1. Click the calendar icon to specify the date range. The date range includes the From and To dates.
2. Click **+Add Group**, and a dialog appears with the available group list. Select the required groups and click **save**.
3. Choose the file format in which you want to export the violation details. The following are the supported file formats:

- XLS — To generate the summary report in XLS format.
- CSV — To generate the summary report in CSV format.

4. Click **Generate Report**. The report is generated and downloaded in the selected file format.

Failed login attempt report

The failed login attempt report generates the report of users who failed while logging into OmniDocs between the specified date range. Use Select Group List filter to display specific results.

To generate the failed login attempt report, perform the following steps:

1. Click the calendar icon to specify the date range. The date range includes the From and To dates.
2. Click **+Add Group**, and a dialog appears with the available group list. Select the required groups and click **save**.
3. Choose the file format in which you want to export the violation details. The following are the supported file formats:
   - XLS — To generate the summary report in XLS format.
   - CSV — To generate the summary report in CSV format.
4. Click **Generate Report**. The report is generated and downloaded in the selected file format.

License management

License Management allows you to select the users and assigns them as a fixed user for sign in to the OmniDocs. CD Key generates the license for users logging into OmniDocs at the time of creating a cabinet.

The types of licenses are as follows:

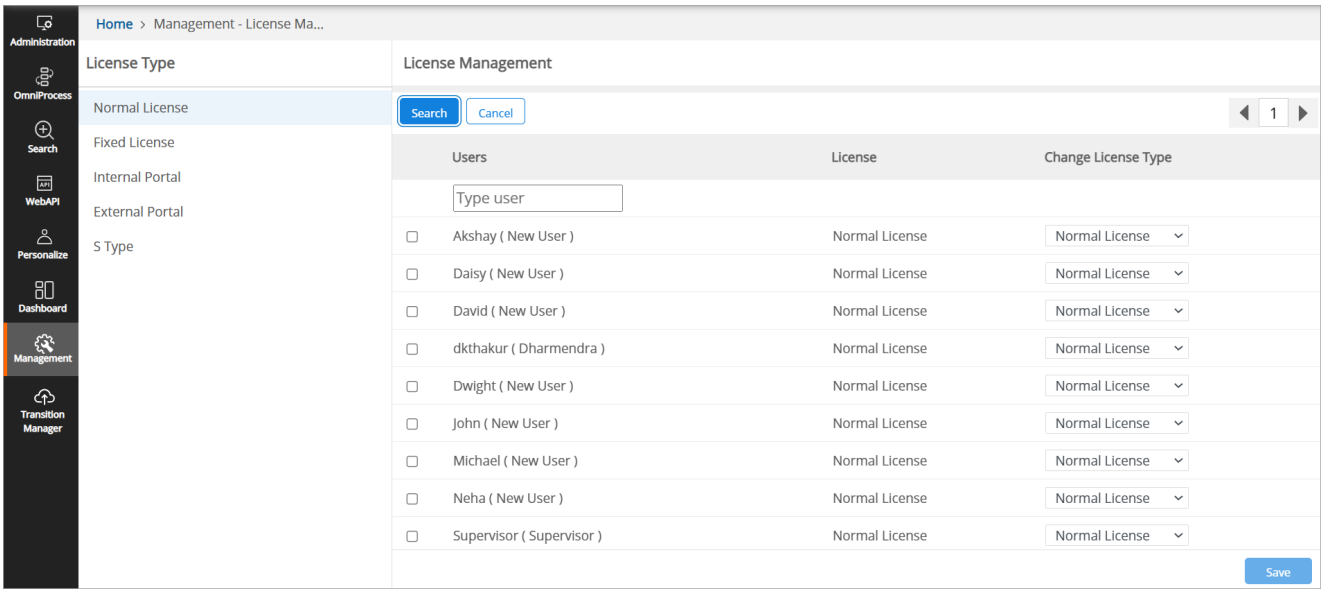
- Normal License
- Fixed License
- Internal License

- External License
- S-Type

Working with license management

To access the License Mangement, perform the below steps:

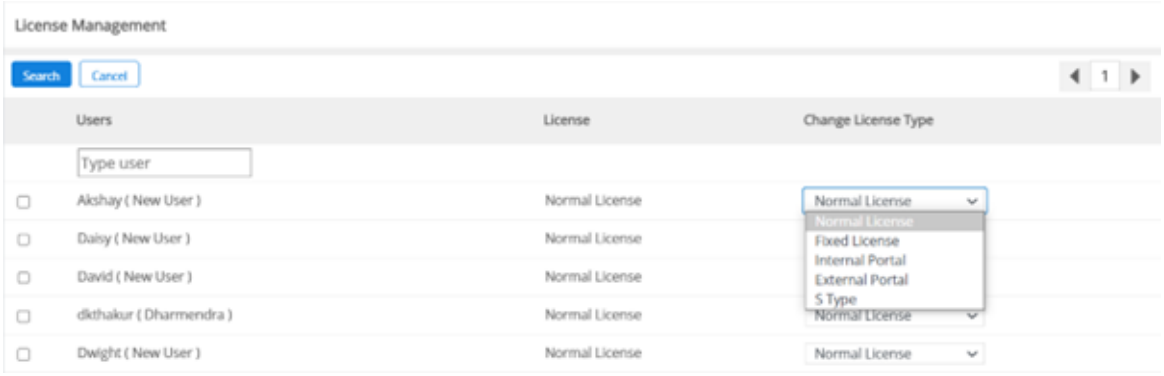
1. Go to the **License Management** under **Management** Tab. The License Management page appears.



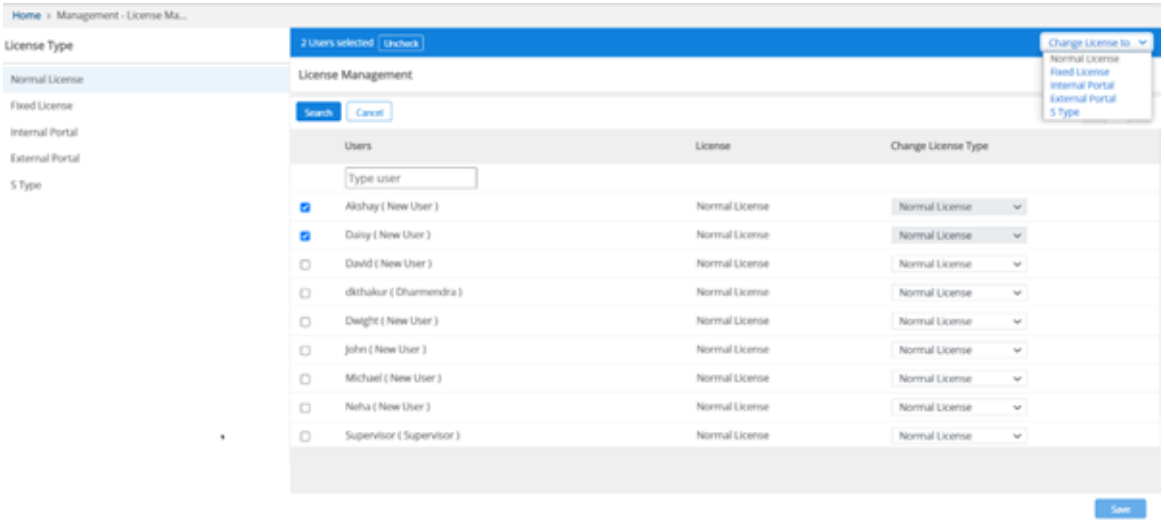
2. License Management page appears with the following options:
   a. License Type – Displays the type of license on the left pane. To view specific license users, click License Type such as **Normal License** or **Fixed License**.
   b. Change License Type – Allows you to change the user license. To change the license, perform the below steps:
      a. Go to the License such as Normal License, select the checkbox given against the user name.

         You can search user with its name using the search bar.

      b. Go to the **Change License Type** on the right pane. Select the license type using the dropdown and change it to other license.



c. To change multiple user license, select the license using the **Change License to** option given on upper-right pane.

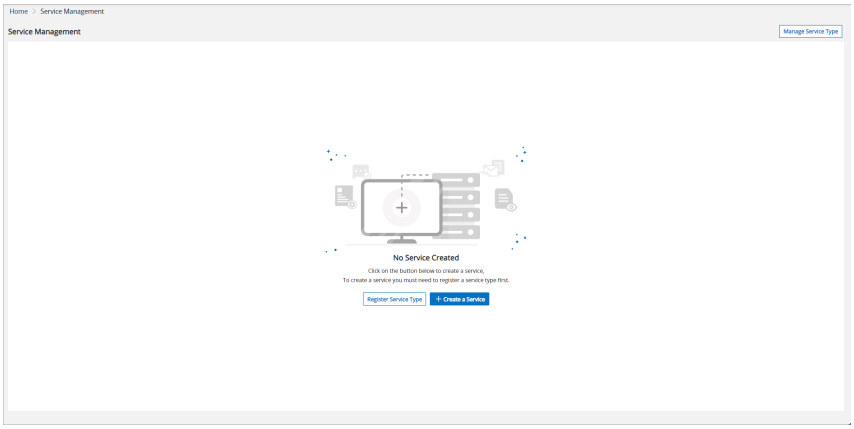


3. Click **Save**. The License gets changed.

Service management

Service Management provides a common architecture to schedule services like volume compaction, delete user, and others.

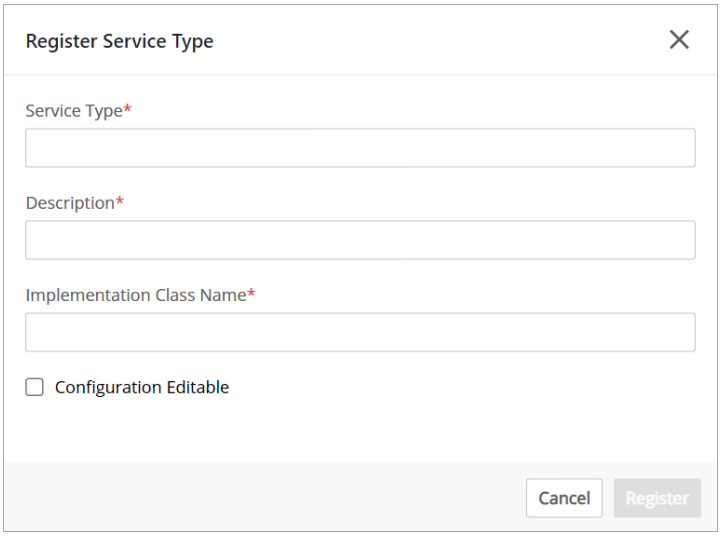
To work with Service Management, navigate to the **Management** tile on the Home screen of OmniDocs Admin, then click **Service Management**. The Service Management screen appears.



Manage Service Type

To register the service type as compaction, perform the following steps:

1. From the Service Management screen, click **Register Service Type**. The Register Service Type dialog appears.



This dialog comprises the following options to specify:

Option	Description
Service Type	Give the name as *Compaction* to the service type.
Description	Enter a brief description to register the service type.
Implementation Class Name	Enter the following class name for compaction: *com.newgen.comp.ExecuteCompaction* .
Configuration Editable	Select this option if you want to make the configuration editable.

2. Click **Register**. The service type created successfully.

To register service type as transfer ownership, perform the following steps:

1. From the Service Management screen, click the **Register Service Type** Button. The Register Service Type dialog appears.
   This dialog comprises the following options to specify:

Option	Description
Service Type	Give the name as *transferownership* to the service type.
Description	Enter a brief description to register the service type.
Implementation Class Name	Enter the following class name for compaction: *com.newgen.TransferOwnerShip.Process OwnershipTransfer*
Configuration Editable	Select this option if you want to make the configuration editable.

2. Click **Register**. The service type created successfully.

To register service type as STM, perform the following steps:

1. From the Service Management screen, click **Register Service Type**. The Register Service Type dialog appears.
   This dialog comprises the following options to specify:

Option	Description
Service Type	Give the name as *STM* to the service type.
Description	Enter a brief description to register the service type.

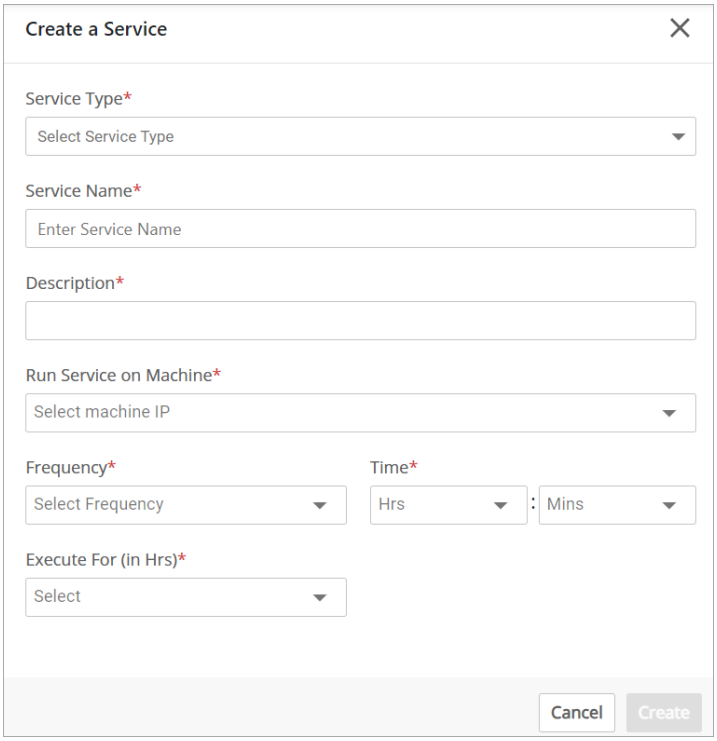
Option	Description
Implementation Class Name	Enter the following class name for compaction: *com.newgen.migration.TimeBasedDocumentMigration*
Configuration Editable	Select this option if you want to make the configuration editable.

2. Click **Register**. The service type created successfully.

Manage Service(s)

To register service(s) as compaction, perform the following steps:

1. From the Service Management screen, click **+Create a Service**. The Create a Service dialog appears.



This dialog comprises the following options to specify:

Option	Description
Service Type	Select *user-compaction* as the service type from the dropdown list.
Service Name	Enter the service name to register the service.
Description	Enter a brief description to register the service.

Option	Description
Run Service on Machine	Select a service machine from the dropdown.
Frequency	Select the frequency of the service from the dropdown.
Time	Select the time of the service schedule in hours and minutes
Execute for (in Hrs)	Select the service execution duration, from the options available in the dropdown list.

Specify SchedulerLocation=<IP Address of Remote Machine Where Scheduler *Service is installed*> in *eworkstyle.ini*.

2. Click the **Next** button, the Configure tab appears with the following options:

Option	Description
Username	Enter your username in the field.
Password	Enter the password.
Volume(s)	Select the volume from the dropdown.
Batch Size	Select the batch size from the dropdown.
Volume Compaction Percentage	Select the volume compaction percentage from the dropdown.

3. Click the **Create** button to create the service.

To register service(s) as transfer ownership, perform the following steps:

1. From the Service Management screen, click **+Create a Service**. The Create a Service dialog appears.
   The dialog comprises the following options:

Option	Description
Service Type	Select *transferownership* as the service type from the dropdown list.
Service Name	Enter the service name to register the service.
Description	Enter a brief description to register the service.
Run Service on Machine	Select a service machine from the dropdown.
Frequency	Select the frequency of the service from the dropdown.

Option	Description
Time	Select the time of the service schedule in hours and minutes
Execute for (in Hrs)	Select the service execution duration, from the options available in the dropdown list.

2. Click the **Create** button to create the service.

To edit the service, click the edit icon . After modifying the service, click **Modify** to save the changes.

To generate compaction report, perform the following steps:

1. In the Manage Service Type screen, click the report icon against the required service. The Generate Compaction Report dialog appears with the following options:

Option	Description
Volume(s)	Select the volume from the dropdown.
VolumeSite(s)	Select the volume site from the dropdown.
Date Range	Click the calendar icon to specify the date range. The date range includes the *From* and *To* dates.

2. Click **Generate**. The report of the selected service type appears.

To delete the service, perform the following steps:

1. Click the delete icon against the desired service. A confirmation dialog box appears.
2. Click **Delete** to delete the selected service type.

Trash management

Trash Management enables you to view the folders and documents deleted by all users. You can also restore the deleted folders and documents from the trash repository to the source repository.

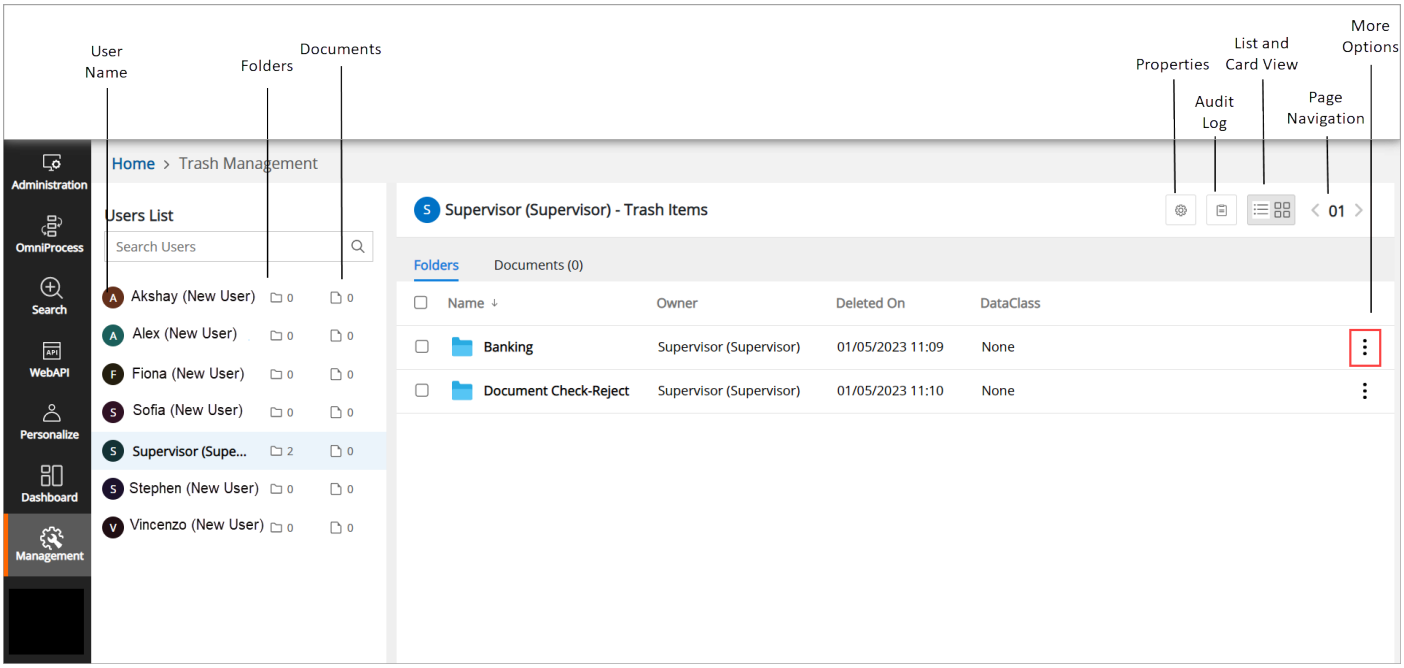
To access the trash management, perform the below steps:

1. Go to the **Management** tile.
2. Click **Trash Management**. The Trash Management screen appears. It displays the documents and folders deleted by all users.

For more information, refer to the Exploring trash management interface section.

Exploring trash management interface

After clicking **Trash Management**, the Trash Management home screen appears.



The Trash Management consists of the following options:

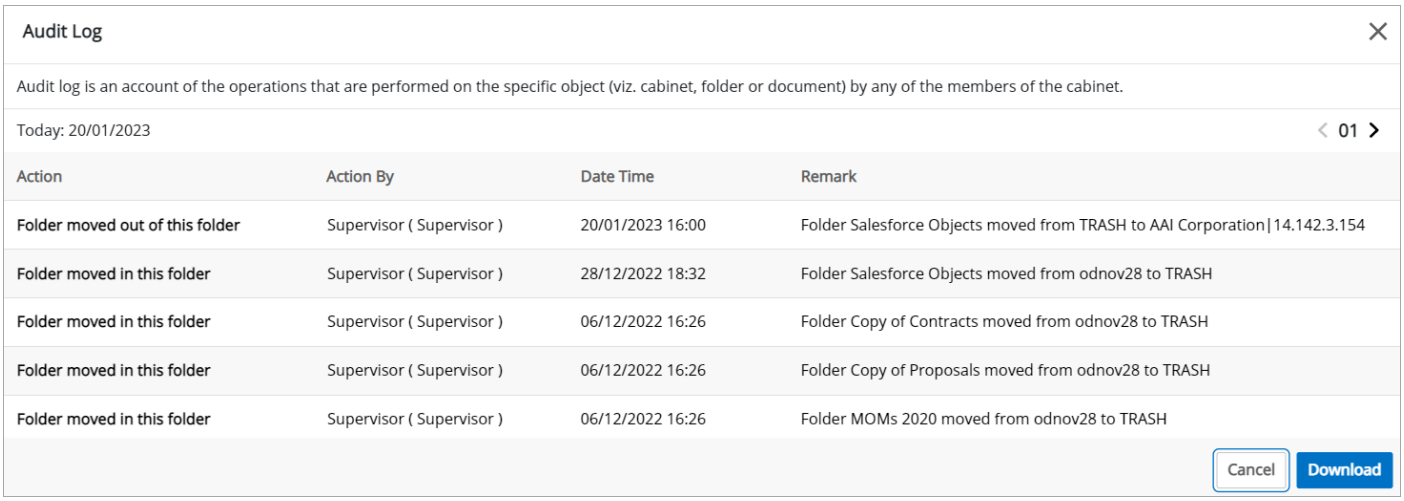
Options	Description
Search box	Allows you to search the user with its name.
User Name	Displays the user name.
Folders	Displays the user deleted folders.
Documents	Displays the user-deleted documents.
Properties	Displays the properties of the trash folder under which all deleted documents and folders are present.

Options	Description
Audit Log	Displays the list of operations performed by administrators on deleted documents and folders.
List and Card View	Allows you to change the view of deleted folders and documents in the list and card format. Select the user to view the deleted folders and documents in the left pane.
Page Navigation	Allows you to navigate the previous and next pages.
More Options	Allows you to perform the following operations: • Properties • Move • Delete Permanently

Viewing and downloading the audit log

Audit Log displays the list of operations performed by administrators on deleted documents and folders.

To view the audit logs of actions performed within the Trash Management Module, go to **Trash Management** and click the **Audit Log** icon. The Audit log dialog appears.



To download the audit log report, click **Download**. The audit log gets downloaded in *xls* format.

Performing trash management operations

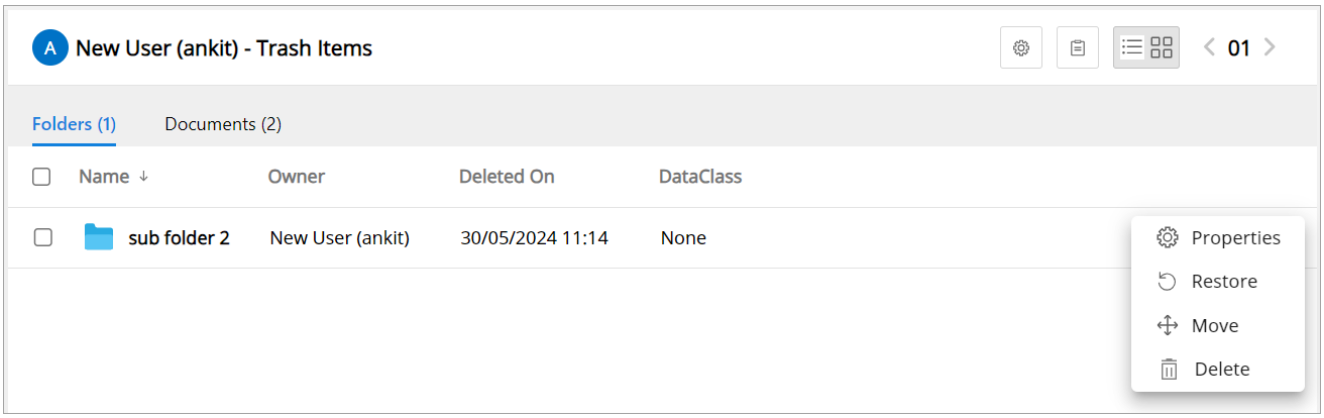
You can click the More Options icon ⋮ next to the required folder or document on the Trash Management screen to perform the following operations::

- Viewing Properties
- Restoring deleted documents or folders
- Move deleted documents or folders
- Delete Permanently

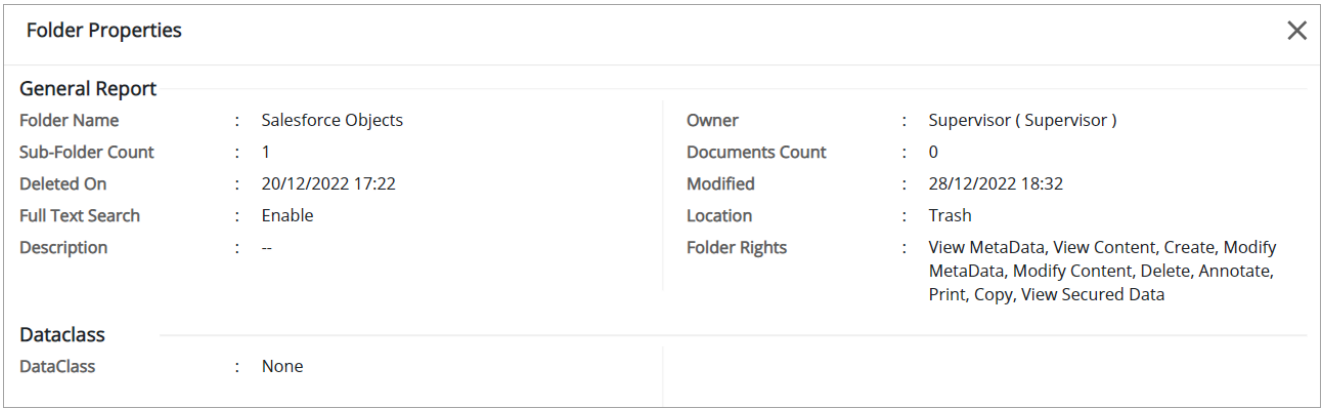
Viewing Properties

To view the folder or document properties, perform the following steps:

1. Click the More Options icon ⋮ against the folder or document.



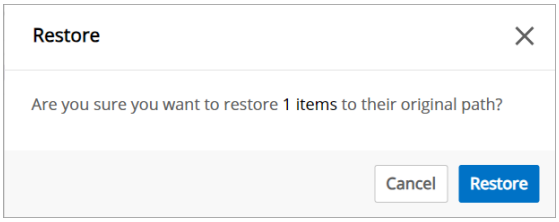
2. Select **Properties**. The Folder Properties screen appears.



Restore

To restore a folder or document, perform the following steps:

1. Click the More Options icon against the desired folder or file.
2. Select **Restore** from the options. A dialog box appears, asking for permission to restore to the original path.



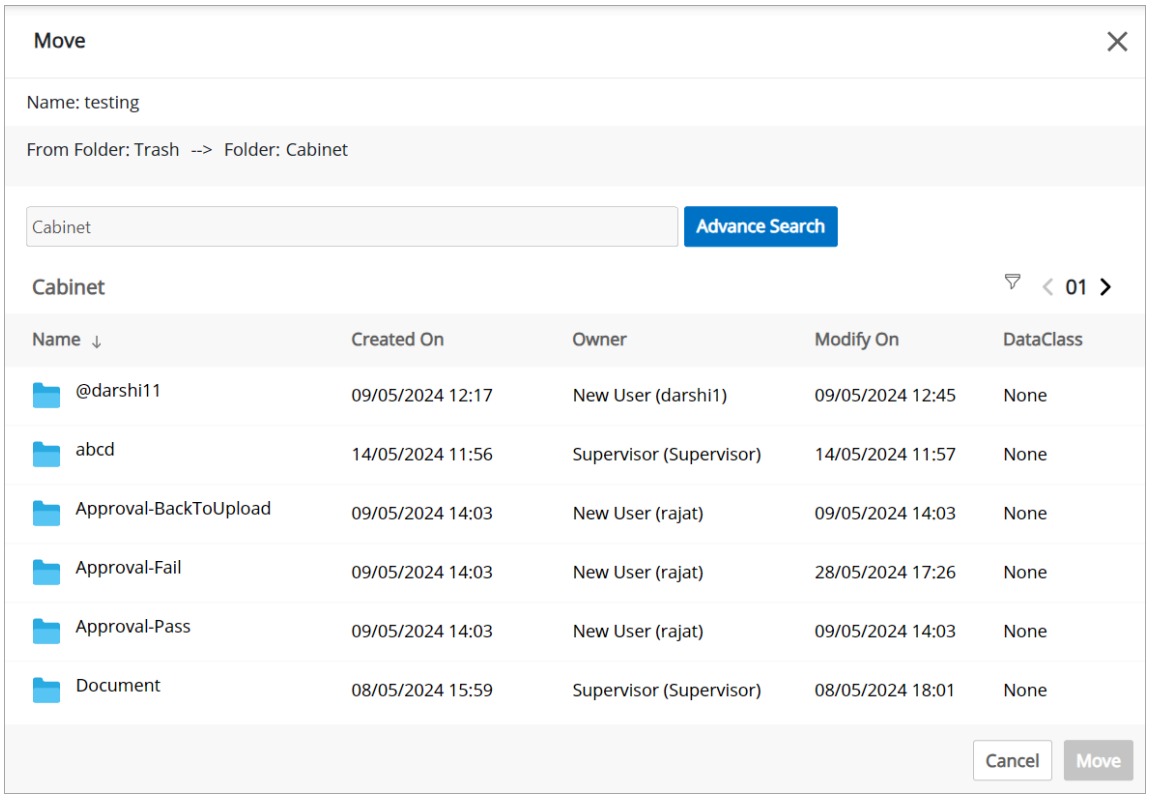
3. Click **Restore**.

Move

To move the deleted folder or document, perform the following steps:

1. Click the More Options icon ⋮ against the folder or document you want to move.
2. Select **Move**. The Move dialog appears with the following options:
    - Advanced Search — This option allows you to search with the folder name and its dataclass.
        - To perform an advanced search on folders, click **Advanced Search**.
        - Enter the folder name or select the dataclass using the dropdown. Then, click **Search**.
        - Select the folder and click **Move**.
    - Filter — To filter the documents or folders, click the filter icon and specify the following:
        - **Name** — Enter the folder or document name.
        - **Created On** — Select the date on which the folder or document was created.
        - **Owner** — Enter the user name.
        - **Modify On** — Select the modification date using the datepicker.

- **Dataclass** — Select the dataclass using the dropdown and click **Search**.



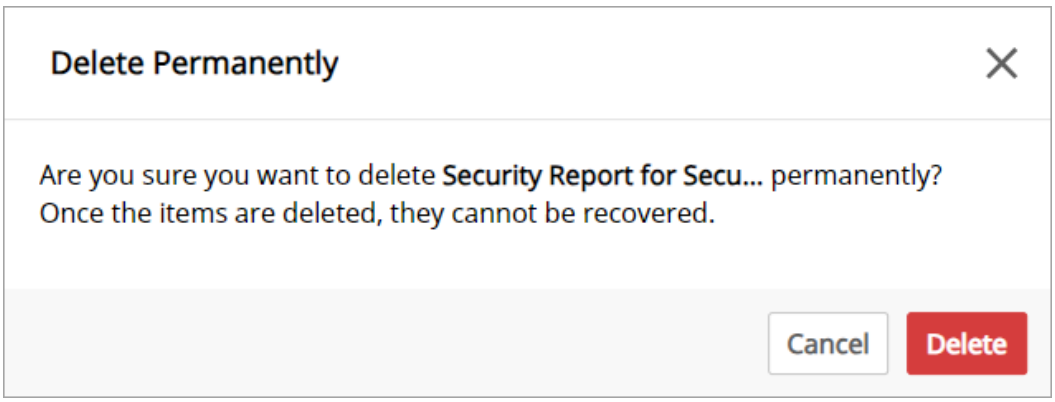
3. Upon selecting the folder or document, click **Move**.

> To move multiple folders or documents, select the checkbox given against the desired folders or documents and click **Move**.

Delete Permanently

To delete the folders or documents permanently, perform the following steps:

1. Click the More Options icon ⋮ against the desired folder or document.
2. Select **Delete**. The Delete dialog appears.



3. Click **Delete**. The folder or document gets deleted permanently.

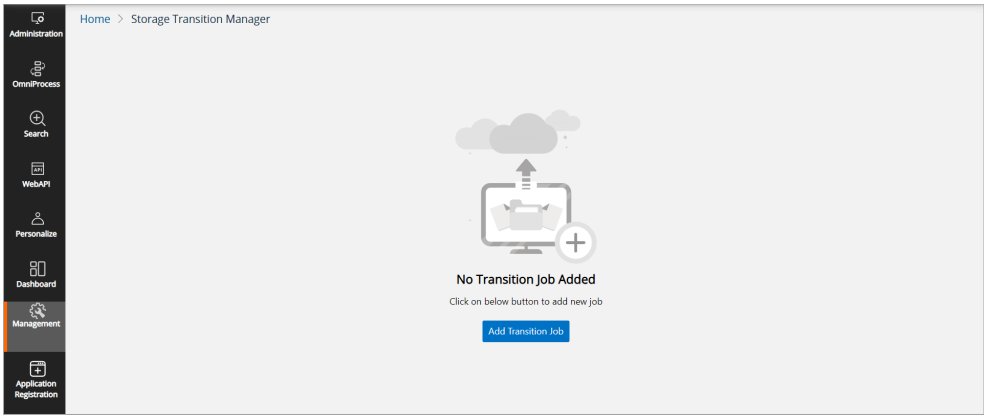
To delete multiple folders or documents permanently, select the checkbox given against all the folders and documents. Then, click **Delete**.

Storage Transition Manager

The Storage Transition Manager allows you to migrate your on-premises documents to cloud sites. The supported cloud sites include Amazon S3, Azure Blob, HCP Site, and more. To migrate the documents, configure the service by adding a transition job.

To access the Storage Transition Manager, perform the below steps:

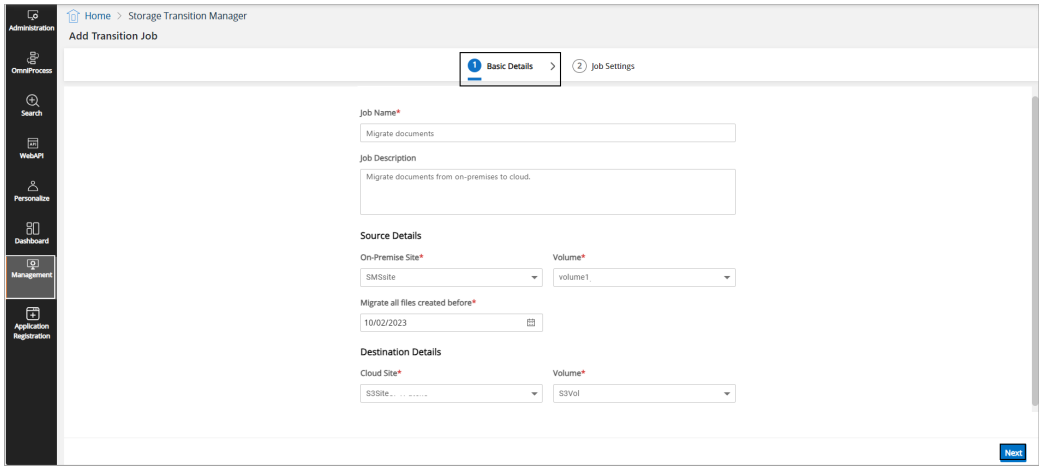
1. On the home page of Newgen OmniDocs Admin, go to **Management** tile.
2. Click **Storage Transition Manager**. The Storage Transition Manager page appears.



Adding a Transition Job

To add a transition job, perform the below steps:

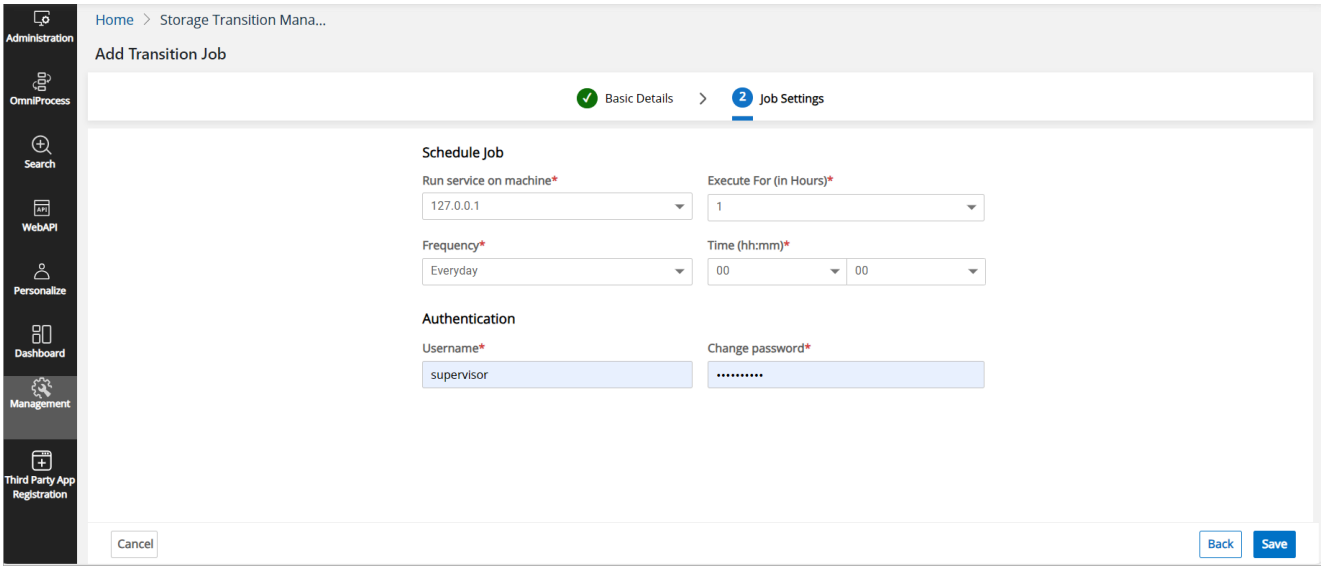
1. Go to **Storage Transition Manager**. The Storage Transition Manager page appears.
2. Click **Add Transition Job**. The Basic Details tab appears.



3. In the **Basic Details** tab, specify the following fields:

Fields	Description
Job Name	Enter the job name. For example, Migrate Documents.
Job Description	Enter the job description for the above specified job name. For example, Migrating documents from on-premises to a Cloud site.
On-Premise Site	Select the On-Premise site where you have stored all the documents from the dropdown.
Volume	Select the volume corresponding to the above selected site from the dropdown.
Migrate all files created before	Select the date using date picker. Then, the Storage Transition Manager migrates all documents created before the selected date.
Cloud Site	Enter the Cloud site to which you want to migrate the documents.
Volume	Select the volume corresponding to above selected site from the dropdown.

4. Click **Next**. The Job Settings tab appears.



5. In the **Job Settings** tab, specify the following fields:

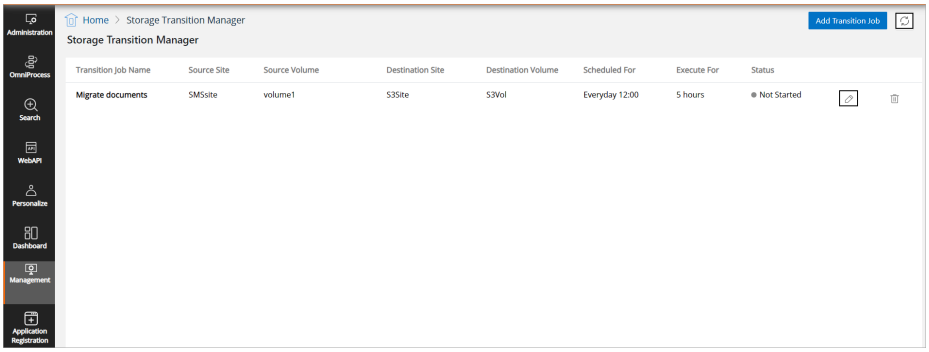
Fields	Description
Run service on machine	Enter the machine's IP address where you want to run this transaction job.
Execute For (in Hours)	Select the hours for executing the transaction job.
Frequency	Select the frequency from the dropdown for the day on which the job runs.
Time (hh:mm)	Select the hours and minutes from the dropdown for the specified time when the job runs.
Username	Enter your registered username.
Change password	Enter the password associated with your username.

6. Click **Save**. The Transaction Job saved successfully message appears.

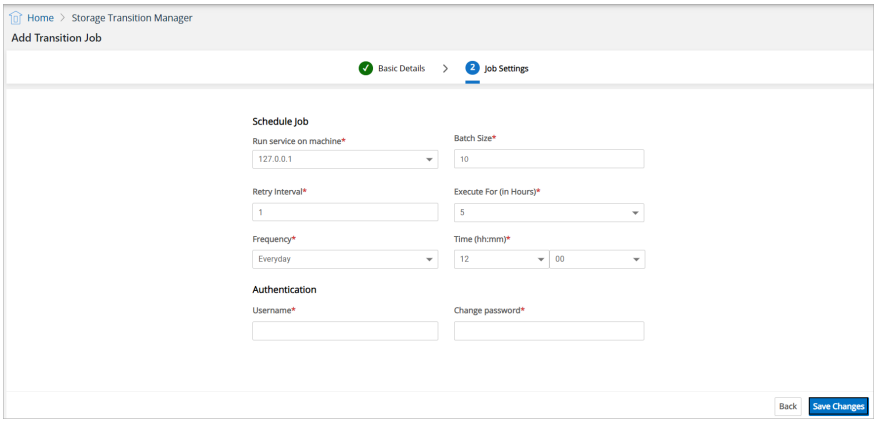
Viewing and modifying a Transition Job

To view and modify a transition job, perform the below steps:

1. Go to **Storage Transition Manager**. The Storage Transition Manager page appears with the list of scheduled transition job(s).



2. To reload the scheduled job page, click **Refresh** icon.
3. Click **Edit** icon. The Job page appears in the editable mode.

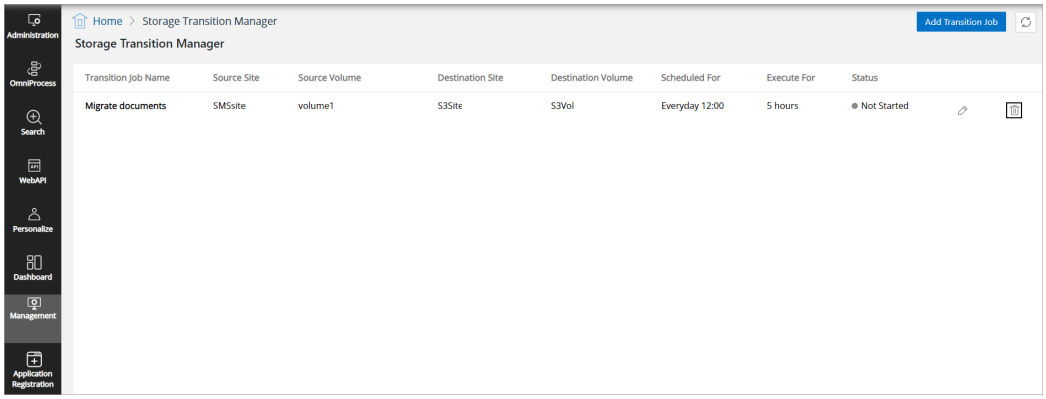


4. Make the changes and click **Save Changes**. The transaction job saved successful message appears.

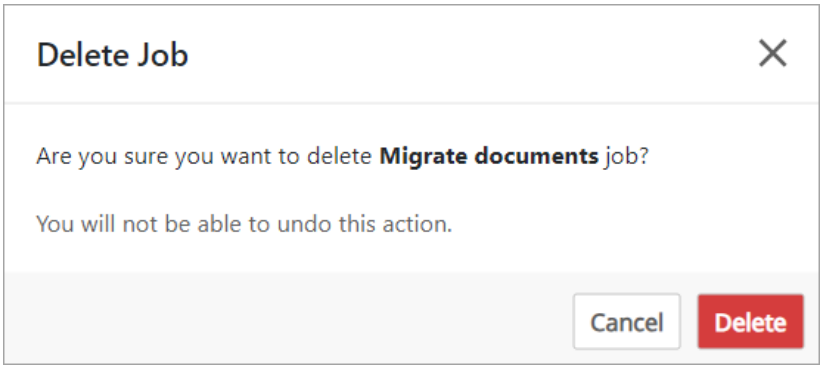
Deleting a Transition Job

To delete a Transition Job, perform the below steps:

1. Go to **Storage Transition Manager**. The Storage Transition Manager page appears with the list of scheduled transition job(s).



2. Click **Delete** icon given against the scheduled job . The Delete Job dialog appears.



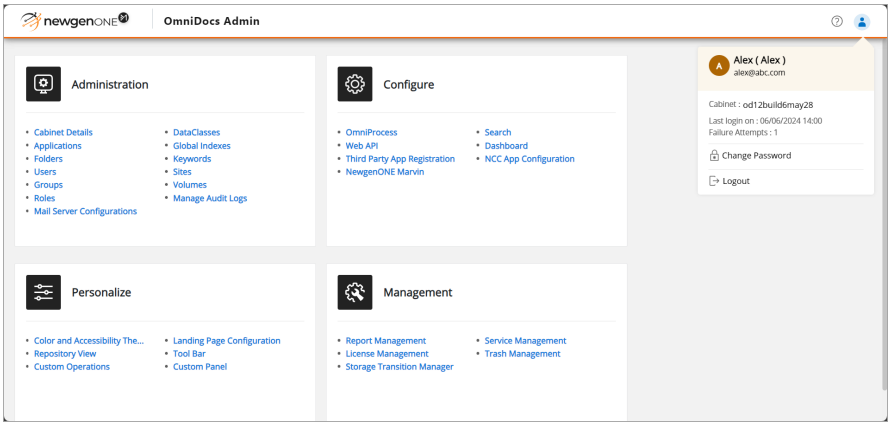
3. Click **Delete**. The Transaction job deleted successfully message appears.

User profile

This chapter provides information related to your OmniDocs administration account such as username, email ID, cabinet, and more.

To access your user profile, perform the following steps:

1. Click the user icon to open user's profile drawer.



2. The user's profile drawer contains the following information and functions:

Field	Description
User Name	The user name of the signed-in user.
Email ID	The email ID of the signed-in user, if configured.
Cabinet Name	Name of the cabinet to which the user has signed in.
Last Login Time.	Date and time at which the signed-in user had last visited.
Failure Attempts	The number of unsuccessful login attempts.
Change Password	Click to change the password.
Logout	Click to sign out from the OmniDocs Admin module.

Change password

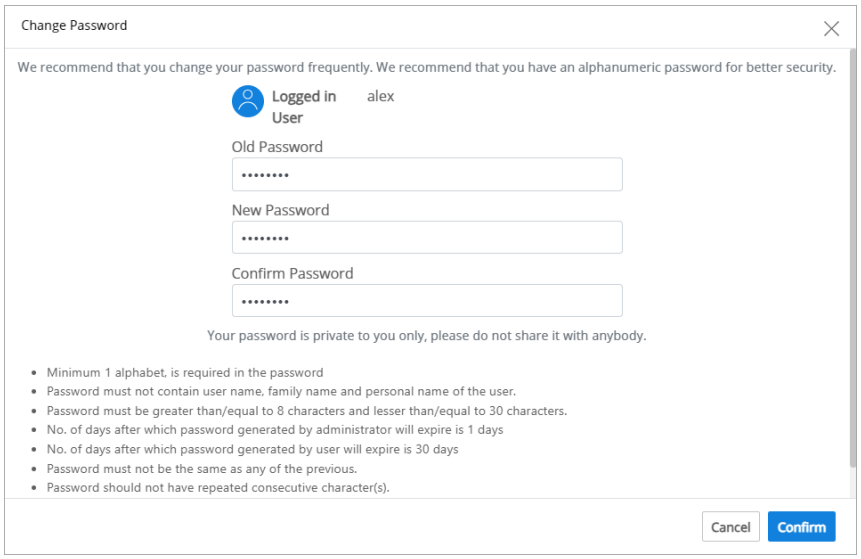
Change Password is used to change the current password of the logged in user.

To Change Password, follow the given steps:

1. Click on **User icon**.
2. Click on **Change Password**. Change Password dialog box appears.
3. Specify the details as listed below:

Fields	Description
Old Password	Enter current password.
New Password	Enter a new password.
Confirm Password	Re-type the new password.

4. Click on **Confirm** to save the new password.



Limitations on Setting a Password

1. The maximum length of the password can be up to 32 characters.
2. The password entered is case sensitive.
3. Leading and trailing spaces are not allowed.
4. Special characters like: “\ / | + - & ^ % $ # @,!” are not allowed.

If the user tries to log in to OmniDocs using a previous expired password, then a message is displayed stating “Your password has expired. Please change your password.”

Shortcut keys for OmniDocs operations

You can navigate through the entire OmniDocs Admin module using the following shortcut keys:

Shortcut Keys	Actions
Tab	Move forward.
Shift+Tab	Move backward.
Space	Select or remove the selection of the checkbox.
Enter	Execute selected action,

Troubleshooting OmniDocs Admin issues

This section provides information on the troubleshooting of OmniDocs Admin issues.

Web API issues and their resolutions

1. **Issue:** No document error appears while viewing documents from Web API.
   • **Resolution**: To resolve this issue, perform the following steps:
   a. Check if the user has view permission or not. To view any document, the user must have view permission on that document.
   b. Check if the correct document index is passing.
   c. Check if the document matches the search criteria.
2. **Issue:** Getting invalid login information error in Web API.
   • **Resolution**: To resolve this issue, perform the following steps:
   a. Check the saved password and verify it with the current password. Update the password if it has changed.
   b. Check if you are using an external user and the password is not encrypted in the URL.
3. **Issue:** Getting session expire error in Web API.
   • **Resolution**: To resolve this issue, perform the following steps:
   a. Check the time-out value defined in the Web API configuration in OmniDocs Admin.
   b. Use an S-type user to set login details**.**

OmniProcess issues and their resolutions

1. **Issue:** Unable to view those documents in OmniProcess that are added from OmniScan.
   • **Resolution**: Make sure that OmniScan adds folders and documents only inside the Submit folder corresponding to the OmniProcess being used.
2. **Issue:** How to create a dynamic field based on a data class field value in OmniProcess?

- **Resolution**: For creating a dynamic action path in Action Definition, make sure there is a constant Folder Path followed by dynamic data class fields separated by /@.
  Refer to the following example:*<CabinetName>/<OmniProcessRootFolder>/<ConstantFolderName>/@DCField1@/@DCField2@odcabinet/OPPool/Accepted/@DCField1@/@DCField2@*

  Only the mandatory data class field must be used in the dynamic Action Path. Do not use any optional data class field in the Action Path.

3. **Issue:** How to create a dynamic field based on a data class field value in OmniProcess?
   - **Resolution**: For creating a dynamic action path in Action Definition, make sure there is a constant Folder Path followed by dynamic data class fields separated by /@.Refer to the following example:
4. **Issue:** OmniProcess is not working and throwing errors while adding documents after modifying the associated data class.
   - **Resolution**: Never modify the data class once it is associated with OmniProcess. If required, create a new OmniProcess with the same steps and use it.
5. **Issue:** Unable to create OmniProcess while keeping action name as Submit.
   - **Resolution**: Do not keep any action name like Submit or words that are used in the scripting language. Requests containing such words are blocked by OmniDocs Security filter to avoid cross-site scripting attacks.
6. **Issue:** Notes are not visible in the Drafts section.
   - **Resolution**: Notes are not shown in the Drafts section due to security reasons. If notes are visible in the Draft section, then the information will be exposed to each one in the maker group.
7. **Issue:** Unable to add the Next step if only Custom Action is present in OmniProcess.
   - **Resolution**: Next step cannot be added without adding at least one standard action in the previous step as only a standard action can be the Source for any action in the Next step. A custom action cannot be a Source for any action.

HCP issues and their resolutions

1. **Issue**: Facing HCP connectivity issues.
   - **Resolution**: To achieve HCP connectivity, make sure that the *HCP. jar* file is available in both the **EJB** and **WEB** containers. Also, verify that the *HCPbucket* tag is present in the *IS.ini* file located in the *Newgen/NGConfig* folder for both the **EJB** and **WEB** containers.

2. **Issue**: SSL handshake fails during HCP server connection
   - **Resolution**: Create and deploy a new cacerts file by adding the HCP server domain to the file. Then, copy the cacerts file to the *$JAVA_HOME/jre/lib/security/* directory for both **EJB** and **WEB** containers.
3. **Issue**: Unable to save HCP credentials from the UI.
   - **Resolution**: Update the HCP details in the database by running the following SQL query:
     update ishcp set HNameSpace = '<HCP URL>' where HSiteId = ?;
4. **Issue**: Unable to save large files.
   - **Resolution**: Modify the ingress file to allow larger file uploads by adding the following annotation:
     nginx.ingress.kubernetes.io/proxy-body-size: 8m
     For additional information, refer to the *Kubernetes Ingress-NGINX Documentation* for best practices on managing file size limits.
5. **Issue**: Unable to view documents.
   - **Resolution**: Clear the content of the following configuration files:
     Newgen/NGConfig/ngdbini/odwebini/odcablist.ini
     Newgen/NGConfig/ngdbini/odwebini/admin.ini
     Newgen/NGConfig/ngdbini/Custom/{CABINET_NAME}/odcablist.ini
     Newgen/NGConfig/ngdbini/Custom/{CABINET_NAME}/admin.ini
     After clearing the files, re-register the cabinet by accessing the registration URL at *https://<Host-Path URL of OmniDocsWeb container>/omnidocs/register*.

Glossary

Terms	Description
Action	Action refers to a particular task that has to be automated. For example, it can be a Leave Request, Purchase Request, Bill Approval, Loan Sanction Request etc. Post Item is defined in the Administration Desktop.
Administration Desktop	For administering the Cabinets, Administration Desktop is maintained. Administration includes creation of users, groups, data classes, assignment of rights etc.
Alias	Synonyms that can be associated with a keyword
Authorize	Keywords for Cabinets are also created from the OmniDocs Desktop. But they can be authorized by Administration Desktop. Administrator authorizes the keywords made by users. Authorized Keywords cannot be modified.
Audit Trail	Audit Trail is a log on all the actions performed on the OmniDocs.
Cabinet	The cabinets are central storage units that can be connected to desktop through a server.
Commit Type	Immediate commit type enables to saves the changes directly in the database. Delayed commit type enables to save the changes in the scratch directory and then save them in database as you click the Commit command button in the Volume Properties.
Compact	Compact means freeing disk space by deleting the already committed files.
Connect	Establishes the connection with the registered cabinet.
Data Class	Set of indexes that can be associated with the documents or folder for providing the unique entity to them.

Terms	Description
Disconnect	Disconnects the registered cabinet. The documents and folders under the cabinet are not accessible if you disconnect the cabinet.
DOB Format	File format supported by Newgen OmniDocs. It saves the document image along with the data and annotations associated with it, as one file.
Everyone Group	Everyone group includes all the users created by the Administration Desktop. This group is not displayed in the group list, so you cannot modify it. But you can assign rights collectively to all the users by assigning the rights to Everyone group.
Filter	Sorting on the related keywords by specifying the keyword with or without wild cards. (Wild card means *,#- for example avi*)
Folder	Folder is a repository for the documents.
Global Index	Global indexes are user-defined indexes or fields that could be associated to any document across the Cabinet. These indexes can be either associated with the data class or defined separately.
Group	The users can be clubbed together as a Group.
Image Server	Stores the document images in form of volume blocks.
Inbox	System folder for the Cabinet that contains all the messages and documents received by the users across the network.
Keywords	Words you would like to associate with the documents, so that you can perform search on them.
Locked	A particular user can lock a particular folder such that no other user can change the folder properties. The users can access documents present under that folder.
Mandatory	To make the data entry compulsory with an index, it can be defined as Mandatory. For example, if you are maintaining the Inventory list, the Item name and Item code indexes can be made mandatory.
Move Volume Block	Moving the contents of the volume block to another Disk.

Terms	Description
Omni Server	Caters to the request to the OmniDocs Desktop users, brings data and document images from database and image storage respectively. It is divided into two parts: Image Server and Transaction Server.
Privileges	Specific rights assigned to the specific user by Administrator. It enables the user to perform certain administrative functions. There are seven privileges.
Register	Registers the Cabinet for accessing the documents and folders under it.
Rights	Rights are defined as access permission for the users, for accessing an object. There are 5 rights – READ, CREATE, MODIFY, DELETE and ANNOTATE.
Supervisor	Supervisor has full rights on the Administration Desktop.
Supervisory Group	Supervisors are clubbed as a supervisory group and they are responsible for creating the objects for Cabinets.
Sites	Sites store the information on the Image Volumes and Volume Blocks.
SMS	SMS (Storage Management Server) is software that manages all kinds of storage devices used by you through a common front end.
Send Items	Send Items folder contains a copy of all the messages sent by the users across the network.
Transaction Server	Transaction Server listens to the request of the OmniDocs Desktop client and fetches the document image from the database.
Trash	Trash folder contains the deleted documents. If the documents are deleted from the trash folder, they cannot be restored back.
Unauthorize	You can modify or delete only unauthorized keywords and create alias for only Authorized keywords.
Unique Key	Unique key means the value associated with that index cannot be duplicated.

Terms	Description
Unregister	Unregisters the selected-Cabinet. After unregistering the Cabinet, it cannot be viewed on the Administration Desktop.
User	To access the Cabinets, you should be a user of that cabinet.
Volume	Volume is a logical entity that includes several Volume blocks.
Volume Block	Volume Block corresponds to a data file and provides the actual physical storage for the documents.