



Tungsten CloudDocs Administrator's Guide

Version: 6.6.0

Date: 2024-07-28

TUNGSTEN
AUTOMATION

© 2024 Tungsten Automation. All rights reserved.

Tungsten and Tungsten Automation are trademarks of Tungsten Automation Corporation, registered in the U.S. and/or other countries. All other trademarks are the property of their respective owners. No part of this publication may be reproduced, stored, or transmitted in any form without the prior written permission of Tungsten Automation.

Preface

Use the information in this guide if you are the administrator who will configure and maintain Tungsten CloudDocs.

Related documentation

The full documentation set for CloudDocs is available at [CloudDocs Documentation](#) page.

In addition to this guide, the documentation set includes:

- *Tungsten CloudDocs Technical Specifications*: Provides information about the technical specifications for CloudDocs client.
- *Tungsten CloudDocs Help*: Provides information on how to use CloudDocs for document upload and management.

Table of Contents

Preface.....	3
Related documentation.....	3
Chapter 1: Introduction.....	6
The role of an administrator.....	6
Chapter 2: Before you start.....	8
Account owner privileges.....	8
Administrator privileges.....	8
Standard edition users.....	8
Professional and Enterprise edition users.....	8
Chapter 3: Get started.....	10
Important functions and concepts.....	10
Security.....	10
Manage account.....	11
Document organization.....	11
Manage users.....	13
Log in.....	13
Home page.....	14
Chapter 4: Administration.....	16
Account management.....	16
User management.....	17
Group management.....	19
Workflow group management.....	19
Reporting.....	20
Auditing.....	20
Archive audit tracking.....	20
Admin tracking.....	21
Load tracking.....	22
Import the configuration data into the global config table.....	23
Patterns for the column data.....	23
Configuration to store in the database.....	24
REST API to create or search annotations.....	25
Role-based redaction.....	25
Importing redaction data to CloudDocs.....	25
Chapter 5: How to.....	26
View and modify account information.....	26

Manage groups.....	27
Create a group.....	27
Define fields for a group.....	28
Add a field.....	28
Edit a field.....	30
Filters.....	31
Valid values.....	32
Examples for editing a field.....	33
Create a subgroup.....	36
Edit a subgroup.....	36
Add a user.....	37
Add privileges for a user at the subgroup level.....	39
Broadcast a message.....	39
Set rules for a document type.....	40
Create an annotation using the REST API.....	41
Search annotations using the REST API.....	42
View redaction by role.....	43
If redaction is disabled.....	44
If redaction is enabled.....	44
Assign Redaction Override role.....	44
Unassign Redaction Override role.....	47
Exception search.....	48

Chapter 1

Introduction

Tungsten CloudDocs is a cloud-based document storage platform that provides capture, storage, and protection of your business documents in a location that is accessible from anywhere, at any time.

This guide provides CloudDocs administrators with information on how to manage CloudDocs.

CloudDocs is designed to manage business documents using a defined business process enabling you to:

- Turn paper documents into electronic documents.
- Index documents to find them easily and quickly.
- Organize similar documents into groups and subgroups with secure access.
- Create a workflow to step documents through a business process (such as, review, approval, and more).
- Perform their jobs better and faster.

The role of an administrator

You can control who can use CloudDocs, how they can use it, and what security restrictions to apply for each user and a group. You can also track the user activity in the application.

Following is a summary of administrator's role:

- Create groups and subgroups with security parameters
- Configure groups and subgroups
 - Define fields
 - Assign users and grant privileges to them
 - Broadcast messages
 - Select Quick index or RapiDex
- Create users
 - Assign initial password
 - Change password
 - Enable/disable login
 - Assign group/subgroup memberships
 - Assign privileges
- Manage your account
 - View account information summary

- Upgrade version from standard to professional Edition
- Generate activity reports
 - By user
 - By group/subgroup
 - By date

Chapter 2

Before you start

Before you start, see the following information to know your role and privileges in Tungsten CloudDocs.

Account owner privileges

If you are the Tungsten CloudDocs account owner, you have the administrator privileges over all the groups and subgroups within your CloudDocs account.


Administrator privileges

If you are the administrator of one or more groups (as assigned by the account owner or another administrator), you have administrator rights over those groups (and their subgroups) assigned to you.

Standard edition users

If you use the standard edition of CloudDocs, make sure to follow the simple guidelines when loading documents into CloudDocs.

1. Scan or upload one document at a time. Do not combine different documents during a scan job or within a single upload file.
2. Use Quick Indexing to index each document. Quick Indexing is designed to index one document contained in a single file. You cannot index multiple documents that are contained in a single scan or upload file.

 Administrators can restrict the availability of quick index in the scan process or workflow queue.

Professional and Enterprise edition users

Professional and Enterprise edition users can use Quick Index or RapiDex to index documents. Administrators specify whether Quick Index or RapiDex is used for a group.

Use RapiDex to:

1. Index scanned or uploaded files that contain multiple documents.
2. Split files that contain multiple documents into individual document files.

Chapter 3

Get started


The following topics provide you basic information about Tungsten CloudDocs.

- [Important functions and concepts](#)
- [Log in](#)
- [Home page](#)

Important functions and concepts

You can configure and manage the options in CloudDocs. It can be configured to:

- Control group membership and privileges.
- Configure user screens by determining which index fields to display for each group and how they can be used.
- Create unique broadcast messages for each group.
- Configure how and when RapiDex is used. (Professional and Enterprise editions only)

 Here, "group" refers to both groups and subgroups.

Before you can manage Tungsten CloudDocs, understand the following functions and concepts:

- [Security](#)
- [Manage account](#)
- [Document organization](#)
- [Manage users](#)

Security

The security settings in CloudDocs helps you secure the access to the documents saved in the application.

You can address security requirements individually for groups, subgroups, and users. For example, Johan can be given different privileges for the various groups to which he belongs, such as the Sales and AP groups and Mary can be given administrator privileges for one group, such as the Contract Administration group, with privileges only to view her team's performance appraisal reports.

You can enforce more security by enabling and disabling users as needed, enforcing strict password policy, or dynamically changing user privileges.

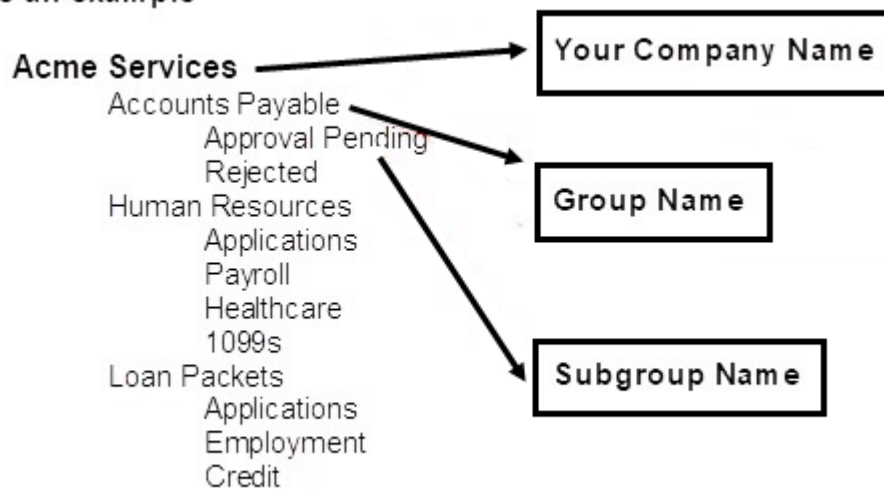
Manage account

Use account management to perform activities such as edit information about account owner and billing contacts, and upgrade your system by adding users.

Document organization

In Tungsten CloudDocs, documents are organized by groups and subgroups under your company. Users can belong to one or more groups or subgroups.

Here's an example



Groups and subgroups

A group is like a virtual file cabinet drawer that contains documents of any type. A subgroup is like a virtual file folder within a drawer.

Each group and subgroup can have its own security privileges, menu options, and documents that only members of the group can see or access. You can control the privileges of each group, and each member of a group, thereby securing the documents by keeping access to them separately.

You can create groups and subgroups with names that are meaningful to your company's organization or document management processes.

You can restrict "Search" or "View" access to documents contained within a group using subgroups. A subgroup is a filtered view of the documents contained in a group, and subgroup filters can be created using any index field or fields. In the example above, members of the "Approval Pending" subgroup can only see those documents that have "Approval Pending" status. When a document's status is changed, members of the "Approval Pending" subgroup will no longer be able to see or access it.

Work in a group

You can perform the following tasks within a group:

- Capture and Quick Index.
- Workflow Queues, Quick Index, and RapiDex (Professional and Enterprise editions only) .
- Workflow Queues and Search.
- Search, View Results, Edit, and Export.

To allow users to work with documents in a specific group, do the following:

1. Create the group.
2. Configure the index fields that are available for capturing, indexing, searching, and viewing.
3. Create one or more users for the group.
4. Assign privileges for each user in the group.

Work in a subgroup

You can perform the following tasks within a subgroup:

- Capture
- Search
- View results
- Edit
- Export
- Access Workflow Queues

To allow users to work in a specific subgroup, do the following:

1. Create group.
2. Create a subgroup.
3. Configure the index fields that are available for searching and viewing.
4. Create one or more users for the subgroup.
5. Assign privileges for each user in the subgroup.

Document types

You can define documents by their "type," and can create your own list of document types.

Following are some example document types for Human Resources:

- Employment application
- Personal information form
- Form 1099
- Background consent form
- Confidentiality agreement

The document type is used to index a document during capture, search for a document of a particular type, or to restrict users so that they can only view documents of one or more types.

Manage users

You can manage the users in CloudDocs in the following ways:

- Create users.
- Assign users to groups and subgroups.
- Enable and disable users.
- Assign user roles (privileges).
- Create user activity reports.

Log in

As a system administrator, you will receive login instructions through email or when you create your Tungsten CloudDocs account.

To log in, a user ID and a password are required.

i User IDs are validated to ensure they are unique to CloudDocs and have a valid email address.

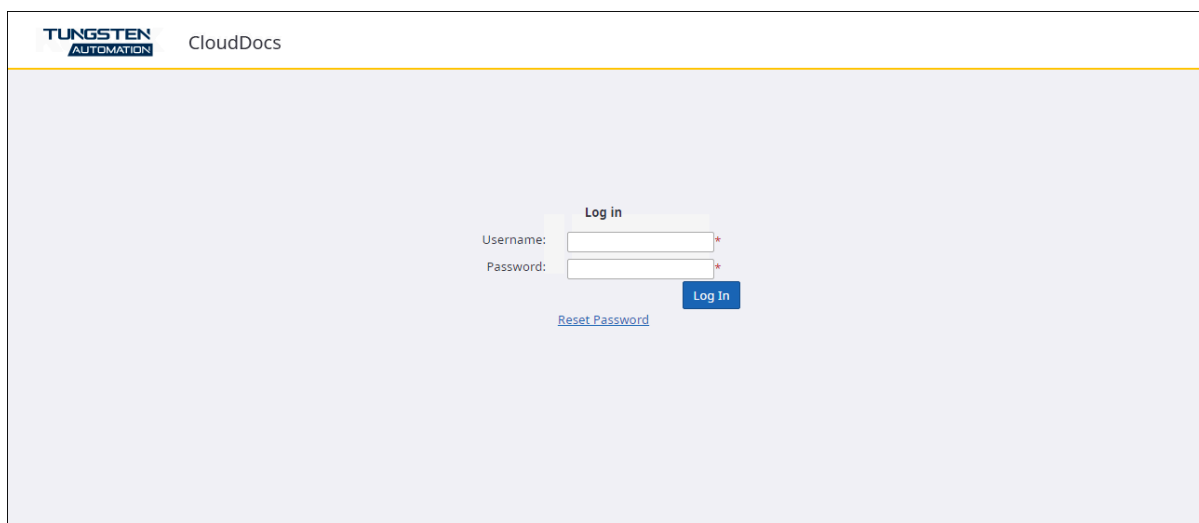
The password must be at least eight (8) characters long, must include at least one letter, and one number. It must not contain special characters such as spaces, dashes, and asterisks.

- Acceptable examples: laura555 or 478mac12
- Unacceptable examples: laura_555 or 81755512

The password is case-sensitive. For the user ID, you can use both upper and lowercase characters.

1. To log in to CloudDocs, enter <https://us.myclouddocs.net> in your browser.

The CloudDocs login page appears.



2. Enter your **Username** and **Password**, and click **Log In**.

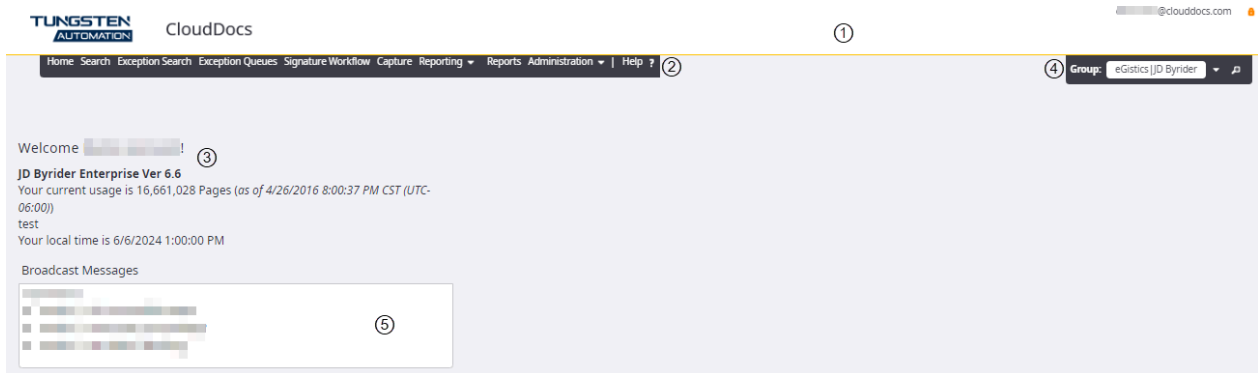
The Home page appears.



- If you forget your password or need to reset it for any reason, click **Reset Password** after entering your **Username**.
- If you enter an incorrect password three times, your account will be locked, and you must wait for a password timeout (30 minutes) before you can log in again.

Home page

The CloudDocs Home page presents a summary of the features you are authorized to use along with the ability to search CloudDocs.



The Home page includes the following elements.

S.no.	Element	Description				
1.	Header bar	<p>The header bar contains the following items:</p> <table border="1"> <tr> <td></td> <td>Click this logo to come back to the Home page from anywhere in the application.</td> </tr> <tr> <td>Username</td> <td> <p>Click the username to display the following options:</p> <p>Change Password: Allows you to change your login password.</p> <p>Logout: Logs you out of CloudDocs.</p> <p> You can access these options from anywhere in the application.</p> </td> </tr> </table>		Click this logo to come back to the Home page from anywhere in the application.	Username	<p>Click the username to display the following options:</p> <p>Change Password: Allows you to change your login password.</p> <p>Logout: Logs you out of CloudDocs.</p> <p> You can access these options from anywhere in the application.</p>
	Click this logo to come back to the Home page from anywhere in the application.					
Username	<p>Click the username to display the following options:</p> <p>Change Password: Allows you to change your login password.</p> <p>Logout: Logs you out of CloudDocs.</p> <p> You can access these options from anywhere in the application.</p>					
2.	Menu bar	Contains the menus and sub-menus.				
3.	User information	Displays user information such as user name, group selected, and application version.				
4.	Group search	Allows you to search and select an organization or group.				

S.no.	Element	Description
5.	Broadcast Messages	Displays the messages from other users of the application.

This guide only addresses the functions available under the **Administration** menu. Select the administrative tasks you wish to perform. You can set up CloudDocs for you and your users.

The screenshot displays the Tungsten CloudDocs Administration interface. At the top left is the logo for TUNGSTEN AUTOMATION. The main title is "CloudDocs". A navigation bar at the top contains the following items: Home, Search, Exception Search, Exception Queues, Signature Workflow, Capture, Reporting, Reports, Administration, and Help. The main content area shows a welcome message: "Welcome [username]!". Below this, it displays "JD Byrider Enterprise Ver 6.6" and "Your current usage is 16,661,028 Pages (as of 4/26/2016 8:00:37 PM CST (UTC-06:00))". There is also a "test" button and "Your local time is [time]". The "Broadcast Messages" section is visible, showing a list of messages with blurred content.

Chapter 4

Administration

Administration section contains information of:

- [Account management](#)
- [User management](#)
- [Group management](#)
- [Workflow group management](#)
- [Reporting](#)
- [Auditing](#)
- [Import the configuration data into the global config table](#)
- [REST API to create or search annotations](#)
- [Role-based redaction](#)

Account management

The account owner of CloudDocs (or any other user to whom the account owner gives account admin privileges) can view the following information:

- Account owner information
- Owner contact
- Billing contact
- Plan information
- Past invoices
- Past payments

You can also:

- Modify the information on this page.
- View monthly billing cycles, track your storage, view invoice details, and payment details.

For managing account settings, go to **Administration > Account Settings**. See [How to view and edit account information](#).

User management

You can create user accounts, assign users to one or more groups, and determine security privileges specific to each group.

User account information includes:

- Username
- Password
- Whether the account is enabled
- Privileges (by group)
- Comments

A user's privileges can change depending upon which group he or she belongs to. For example, User1 belongs to two groups: Group A and Group B, and has the following privileges:

Group A privileges	Group B privileges
<ul style="list-style-type: none"> • Administration • Capture Documents • Index Documents • Search and View Documents • Edit Index Fields 	<ul style="list-style-type: none"> • Search and View Documents

i Subgroups inherit a user's Group privileges. For example, if a group (such as HR) contains two subgroups (such as Employment Apps and Personal Forms), and privileges have only been defined at the group level, users will have the same privileges in both subgroups that they have in the group.

Once you create a user account, you cannot delete it.

In the following example, one user is defined for the HR Group. You can see the users that belong to any group by clicking the name of the group/subgroup. The name of the group is highlighted to indicate that it is selected.

TUNGSTEN CloudDocs
AUTOMATION

Home Search Exception Search Exception Queues Signature Workflow Capture Reporting Reports Administration | Help ?

HR
 Employment Apps
 Personal Forms

User Management

Username	Last Name	First Name	Enabled	Last Login	Password Created
cdoc@clouddocs.com	Docs	Clyde	<input checked="" type="checkbox"/>	05/07/2024 01:44:21	05/06/2024
ddoc@clouddocs.com	Docs	Dana	<input checked="" type="checkbox"/>	05/06/2024 07:23:18	05/06/2024
			<input checked="" type="checkbox"/>	05/06/2024 08:41:34	05/06/2024

Find User: Find Add User

The following example describes how different users can be created and displayed for different groups. In this example, the subgroup Personal Forms is selected. Both Dana Docs and Clyde Docs are the members of this group.

TUNGSTEN CloudDocs
AUTOMATION

Home Search Exception Search Exception Queues Signature Workflow Capture Reporting Reports Administration | Help ?

HR
 Employment Apps
 Personal Forms

User Management

Username	Last Name	First Name	Enabled	Last Login	Password Created
cdoc@clouddocs.com	Docs	Clyde	<input checked="" type="checkbox"/>	05/07/2024 01:44:21	05/06/2024
ddoc@clouddocs.com	Docs	Dana	<input checked="" type="checkbox"/>	05/06/2024 07:23:18	05/06/2024

Find User: Find Add User

If this is the only group of which Clyde is a member, he would only see Personal Forms in the Group list box on the Home page. Consequently, Clyde would only have access to documents that meet certain display characteristics defined for the subgroup.

For managing users, go to **Administration > Users**. See [Add a user](#).

Group management

A group is a place to store documents of a particular type. For example, a group called Human Resources (HR) could be used as the master repository for HR documents.

A subgroup provides a filtered view into the documents contained in a group.

Before you create your groups, you must have:

1. The business functions for which you will be storing documents (AP, HR, Loans, and more).
2. The different document types used for each business function (invoices, applications, proof of employment, and more).

See [Document organization](#) for more information.

Once you create a group, you cannot delete it.

If you use a template, such as HR, when you first sign up for CloudDocs, that group is automatically created. Do not create the same group.

To manage groups, go to **Administration > Group Settings**.

See [Create a group](#) and [Group management](#) for more information.

After defining groups and subgroups, you can [define fields for a group](#) and [broadcast a message](#) for users.

Workflow group management

Workflow allows you to create a sequence of processes to ensure that an item or a document that you upload is complete.

You can only manage workflow groups if a workflow is enabled for your group. If you need to enable this feature, contact [Tungsten Automation Support](#).

The Workflow group settings allow you to create a workflow group, edit a workflow group, and add users to a workflow group. You can create workflow groups to categorize the items in the workflow queue. For example, for items that do not contain the information about the scan date, you can create a workflow group Update Scan Date, and add them to it. Later, you can assign the users to the workflow group to work on the items in the workflow.

To manage Workflow groups, go to **Administration > WF Group Settings**.

Reporting

In CloudDocs after processing a document, you can remove the document from the application if there is no further requirement of the document. Therefore, you can free an amount of space for the next items in the pipeline.

Using document audit, you can define a set of rules to identify such items that can be removed from the application. However, this feature does not remove any item from the application, instead, the user is notified about the list of items that satisfy the set rule. Later, the user can decide on the list of items identified. Rules are defined against a document type in the application.

For example, to get the list of processed items that are in the application for more than two months, you can set a rule to notify the user about the list of items of a document type that have completed a time period of two months from the processed date.

To set rules for a document type, go to **Administration > Reporting > Document Audit**. See [Set rules for a document type](#).

Auditing

Auditing helps you generate an activity report of users and administrators.

You can generate a summary report of all the activities performed by a user or administrator in the application in a period of time. You can also generate a summary or detailed report of items scanned or uploaded to the application in a period.

Auditing includes the following three types of reports:

1. [Archive audit tracking](#)
2. [Admin tracking](#)
3. [Load tracking](#)

Archive audit tracking

Archive audit tracking allows you to generate the Search activity report of users in a group. You can generate a report for a single user or all the users in the group. The report provides you information about the Search activity performed by the user for the selected time period.

To generate an audit report:

1. Go to **Administration > Auditing > Archive audit tracking**.
The **Audit Report** page appears.

The screenshot shows the 'Audit Report' form in the Tungsten CloudDocs interface. At the top left is the 'TUNGSTEN AUTOMATION CloudDocs' logo. A navigation bar contains links for Home, Search, Exception Search, Exception Queues, Signature Workflow, Capture, Reporting, Reports, Administration, and Help. The form itself has the following fields:

- Group:** A dropdown menu with 'HR' selected.
- Date:** Two date pickers separated by 'to', both showing '//'.
- User:** A dropdown menu with '(All)' selected.
- Report Type:** Two radio buttons, 'Search' (which is selected) and 'Archive'.
- Search:** A blue button located below the Report Type options.

2. Select **Group** having users whose activity report is to be generated.
3. Using date picker, select the date range for which you want to generate the user activity report.
4. Select the **User** to generate his activity.
Alternatively, you can also select **(All)** to generate a report of all the users in the group.
5. Select either **Report Type**:
 - a. **Search:** Generates audit report with information about the search criteria used by the user(s).
 - b. **Archive:** Generates audit report with information about tasks performed by the user(s) on an item.
6. Click **Search**.
The list of users with their user ID, activity time, and activity done or search criterion appears. Click **Export to CSV** to download the report in CSV format (if supported).

Admin tracking

Use this option to generate an administrator activity report. The report gives information about admin activities such as creating a group, creating a user, and the last login time of the administrator.

1. Go to **Administration > Auditing > Admin Tracking**.
The **Admin Report** page appears.

2. Follow the steps from 2 through 4 of [Archive audit tracking](#).
3. Select either **Report Type**:
 - **Administrative**: Generates a report about activities such as, creating a user, editing group, and creating a group.
 - **Authentication**: Generates a report about activities such as logging in to the application, reset user password, and change the login password.
4. Click **Search** to generate the report.
5. Click **Export to CSV** to download the report in CSV format.

Load tracking

This option generates a report of item details that were scanned or uploaded to the application in a specified period of time.

1. Go to **Administration > Auditing > Load Tracking**.
The **Load Report** page appears.

2. Follow the steps from 2 through 3 of [Archive audit tracking](#).

3. Select either **Report Type**:
 - **Summary**: Generates a report with information such as process date, item count, and page count.
 - **Detail**: Generates a detailed report with information such as file name, load date, and process date.
4. Click **Search** to generate the report.
Click the **Download** button to download the report in CSV format.

Import the configuration data into the global config table

Importing the configuration data from the .config file to the database allows you to perform the changes to the application's settings at runtime without redeploying via the Octopus, or reducing the server uptime.

To handle the configuration data in the database:

1. Import the configuration data into the global config table using the following pattern for the column data:
 - a. **Process code**: Stores the identity of the project or the application which the configuration information targets to.
 - b. **Key**: The name of the configuration data (for AppSettings) of XPath, to define the exact address of the configuration. The XPath should be in the basic form, without the predicates, wildcard characters, and for selecting the multi-nodes.
 - c. **Value**: Stores the corresponding configuration data as in the text.
 - d. **Computer name**: Stores the computer name that hosts the application.

During the application runtime, application reads the configuration data from the global config table when needed, based on the computer name, process code and the key. The loaded data is then combined with the current configuration to form the configuration as a whole.



- To start the application, some configuration stays on the .config file.
 - Connection string: The starting point of loading the configuration data.
 - Project or application identification (example: code, name, and others).
- If the global config table is not found, the project or application is loaded using the configuration file.

Patterns for the column data

There are two approaches for storing the data in the global config table.

Key-Value: Apply this approach for the AppSettings and ConnectionStrings sections.

XPath-as-key: Apply this approach for all the sections including the AppSettings section, ConnectionStrings section, and other supported custom configurations.

The following table shows the pattern data for the two approaches.

Pattern data	Key-Value	XPath-as-key
Process code	Stores the identity of the project or the application which the configuration information targets to.	Stores the identity of the project or the application which the configuration information targets to.
Misc	Section name of the supported configuration.	-
Key	Key name of the configuration data.	The XPath defines the exact address of the configuration. The XPath value should be in the basic form, without the predicates, wildcard characters, and the multi-nodes.
Value	Corresponding configuration data.	Corresponding configuration data.
Computer name	The name of the computer that hosts the application.	The name of the computer that hosts the application.

Configuration to store in the database

Configuration section	Can be stored	Approach
AppSettings	<ul style="list-style-type: none"> All <add> tags and its content. Stored with XPath. 	<ul style="list-style-type: none"> Key-Value XPath-as-key
ConnectionStrings	<ul style="list-style-type: none"> All the <add> tags and its content. The provider name attribute of connection string. 	<ul style="list-style-type: none"> Key-Value XPath-as-key
DataConfiguration	Only the values of the default database attribute.	-
<ul style="list-style-type: none"> LoginProviderService ColdService ImageArchiveService PdfService SaveAuditLogService ValidationService 	All the <add> tags and its content within the <providers> tag.	XPath-as-key
Nlog	All the <target> and <logger> tags.	XPath-as-key
ApplicationSettings	All the content within the application settings section.	XPath-as-key
System.ServiceModel	All the <endpoint> tags and its content within the <client> tag.	XPath-as-key

i The database cannot store the administrator database connection string and the project or application identification (process code) from the Context Info section of the .config file.

REST API to create or search annotations

In Generic Web Service, REST API (Annotation API) is added to create or search the annotations of a document in a specific module.

You can use the REST API to:

- [Create an annotation](#)
- [Search annotations](#)

Role-based redaction

Administrators need to restrict document access to specific users, especially if sensitive information must be hidden or redacted. Other users with high privileges can see the entire document, where no information is redacted. Outside sources such as a Tungsten TotalAgility and other products feed image and redaction coordinates.

Users with redaction override role can see the document with and without redactions. All other users can only view the redacted version of the document.

Importing redaction data to CloudDocs

Image provider produces item records with text and redactions to send to CloudDocs RestAPI.

An item record contains:

- Image and a metadata
- Redaction data

Redaction information contains a list of redactions and each redaction contains page number, top margin, left margin, height, and width in pixels.

An item record containing image, metadata, and redactions are imported to CloudDocs archive:

- Image is uploaded to the cloud storage.
- Metadata is saved to the database.
- Redactions data is saved to the database if this field has a value.

For more information on redaction, how to "Assign redaction override role", and "Assign no redaction override role", and "Exception search", see [View Redaction by role](#).

Chapter 5

How to

The following topics explain you how to perform administrative tasks in CloudDocs:

- [View and modify account information](#)
- [Add a user](#)
- [Manage groups](#)
- [Define fields for a group](#)
- [Create a subgroup](#)
- [Edit a subgroup](#)
- [Broadcast a message](#)
- [Set rules for a document type](#)
- [Create an annotation using the REST API](#)
- [Search annotations using the REST API](#)
- [View redaction by role](#)

View and modify account information

You can view and modify account settings if you are the account owner or the user to whom the account owner has given account administrator privileges.

1. On the CloudDocs Home page, go to **Administration > Account Settings**.
The **Account Settings** page appears.
2. Configure the settings as appropriate.
 - **Account information**
Form of Payment: Click **Edit** to change the current payment information
 - **Billing contact**
Click **Edit** to change contact information regarding billing.
 - **Plan information**
 - a. **User Seats:** Click **Edit** to add user seats.
 - b. **Active User Accounts:** Click **Users** to switch to the User Management page.

As you go through monthly billing cycles, you can see the exact storage you are currently using (**Usage**), invoice details (**Invoices**), and payment details (**Payments**).

Manage groups

You can create a group, add fields to a group, and broadcast information to users when they log in.

Create a group

You can create a group to manage documents in CloudDocs.

1. On the CloudDocs Home page, go to **Administration > Group Settings**.

The **Organization Management** page appears.

By default, the **Group Administration** tab is open, and your organization's name appears at the top of the organizational structure. Groups are always added under your organization name.

2. Click **Add Group**.

The **Group Details** section appears.

3. Configure the following details for the group.

Name	A name for the group, such as HR.
Description	Optional. A description for the group, such as Human Resource documents.
Code	A unique CloudDocs generated code. It is a read-only setting.
Enabled	If selected, the group becomes active and can be accessed by users with required privileges. (Default = Selected).
Restrict access	<p>If selected, restricts access to CloudDocs to specific IP addresses or ranges.</p> <div style="background-color: #e6f2ff; padding: 5px; border: 1px solid #add8e6;"> <p>i If you select this option at the time of creating a group, the Group Access Administration tab becomes available where you can specify the IP address or range of addresses that are valid for this group. See Assign access to groups.</p> </div>
Enable Challenge Response	If selected, forces the user to answer a challenge question every time they log in.
Allow Cookie for Challenge Response	<ul style="list-style-type: none"> • If selected, creates a PC-specific cookie to remember the initial challenge response and the user is not challenged again during login. • If clear, the user is challenged every time they log in if the Enable challenge response is selected. This is not recommended for PCs that allow users to share operating system logins.
Force Challenge Response onto Subgroups	If selected, the challenge response options are applied to the group's subgroups.

4. Click **Save**.

Assign access to groups

You can specify the IP address or range of addresses that are valid for a group at the time of creating it.

1. In the **Organization Management** page, go to **Group Administration > Group Details** and select **Restrict Access**.

The **Group Access Administration** tab appears.

2. Enter the IP address or range of addresses.
3. Click **Add**.



- The group members can only access the group from the IP addresses specified here. For example, if this group should only be accessed from your business offices, you would only include valid business IP addresses.
- Make sure that each IP address is correct. If an invalid IP address is specified, all the users will be locked out of the group.

4. To specify if an IP address is enabled, click **Edit** next to the desired address and select the box. To delete an IP address, click **Delete**.

Define fields for a group

You can manage the field creation, characteristics, and usage during document capture and search. You can define the fields that are used during capture, indexing, and search. You can define the characteristics of a field, such as the behavior of the field, the values accepted by the field, and if the fields can receive stored values as a result of reference data lookup.

Index fields are used to identify and locate documents. Using index fields, you can manage how documents are organized and used in CloudDocs. You can also use the index fields to provide search and display filters which help you control user access to documents.

This section describes the various fields that are available along with the many options that determine how a field is used for indexing, search, display, and basic document management.

Add a field


1. On the CloudDocs Home page, go to **Administration > Group Settings** and select **Field Administration**.

The **Field Management** page appears.

2. Major tasks in CloudDocs are organized by module. On the **Module** list, select either:
 - **Document search:** To define fields for Search and Results pages.
 - **Work queue:** To define fields used during Capture and Indexing (RapiDex and QuickIndex).
3. The **Fields** tab displays the list of available fields with the following details.

Type	This is a system field whose value cannot be edited.
------	--


Field	<p>Fields can be defined to contain text, amounts, numbers, times, and dates, or system values. The fields can be system defined or user-defined.</p> <ul style="list-style-type: none"> • User-defined fields: These fields are defined by the user. These include: <ul style="list-style-type: none"> • Alpha(N): Contains or display one or more alpha-numeric values. • Amount(N): Contains or display monetary values. • Bit(N): Fields with a checkbox. If the checkbox is selected, the system stores the value as 1, otherwise 0. • Date(N): Fields that contain or display the date in the format MM/DD/YY. • DocType: Fields that contain or display one or more user-defined document types. • Numeric: Fields that contain or display one or more numeric values. • System-defined fields: The system fields are automatically assigned by the CloudDocs when the fields are captured. These fields already have a descriptive name and labels, but most are simply called Alpha1, Amount2, Date1, and so on. <ul style="list-style-type: none"> • LoadTableID: Contains a system-generated identifier for a scan transmission or file upload. • PageCount: Contains a system-generated value that represents the total number of pages within a document file. • ProcessDate: Contains a system-generated date when a document was scanned or uploaded.
Label	This heading displays either the default or user-defined field label.
Display on Search	<p>If selected, this option indicates the field is selected for module:</p> <ul style="list-style-type: none"> • Document Search: The field is displayed on the Search page. • WorkQueue: No effect.
Require on Search	<p>If selected, the field is required to perform a search.</p> <ul style="list-style-type: none"> • Document Search: The field is required to perform a search. • WorkQueue: No effect.
Display on Results	<p>If selected, the field is displayed for the selected module.</p> <ul style="list-style-type: none"> • Document Search: The field is displayed on the Search Results page. • WorkQueue: The field is displayed in the Work Queue, RapiDex, and Quick Index pages.
Display Order	If selected, it indicates the numerical order in which the field is displayed.

Field Dependency	<p>This option indicates if the field is dependent on another field according to the following information:</p> <ul style="list-style-type: none"> • Parent: If selected, this field serves as a key field for all Child fields. A Parent key field is used to look for and retrieve any related Child field values while using the indexing Reference Data Lookup feature. This can dramatically speed up the indexing process for index values that already exist in CloudDocs. For example, if Social Security Number is used as a Parent field for other records such as name, address, telephone number, and more, the data for those fields (if they exist in CloudDocs) is automatically located and filled-in using the value of the designated Parent field. <p>It is recommended that only one field be designated as Parent.</p> <ul style="list-style-type: none"> • Child: CloudDocs checks the Parent field to see if any values for the Child field are already stored. If they are stored, they are retrieved automatically during indexing. • Independent: CloudDocs does not attempt the search for previously stored values.
Editable	<p>If selected, this index field can be edited on the Search results page.</p> <div data-bbox="565 863 1450 919" style="background-color: #e6f2ff; padding: 5px;">  The system-defined fields cannot be edited. </div>

4. Click **Add more fields** to add fields for use during searching and indexing.
A list of available fields is displayed.
5. Click **Add to Field List** to add it.

Edit a field

Once you have added the field, you can edit it if you have permissions.

 Each subgroup automatically inherits the fields defined for the parent group. You can independently change, add, or disable a subgroup's fields without affecting the parent group's fields.

You can add filters and add valid values. See [Filters](#) and [Valid values](#).

1. In the **Field Administration** tab, select **Fields > Edit** to modify the field.
The **Details** tab is displayed. By default, the **Appearance** section expands and displays the field details.
2. Change the details as needed. See the [Examples for editing a field](#).
3. To add filters, expand **Filters**. See [Add a filter for a field](#).
4. To add a valid value, expand **Valid Values**. See [Add a valid value](#).

Filters

Filters are typically used to limit or specify index field values used to perform a search and display results.

i Filters are only used with the Document Search module and are not used with the Workflow Queue module.

For example, you have a Human Resources group that serves as the master repository for several document types, including Employee Application. Under Human Resources group, you have a subgroup, Applications.

To make sure the users of the Applications subgroup have access only to the documents of Employee Application, you can define a filter in the Applications subgroup for the DocType field. This field displays a list of document types from which to choose when searching for or indexing documents. .

The filter requires that the Document Type matches the Value defined elsewhere for Employee Application (refer to Valid values for more information). To create a filter for a user-defined valid value, you must first know its name. For instance, if the name of the valid value for Employee Application is EmpApp, the filter should be "equals EmpApp".

You can also create filters for numbers, amounts, or dates.

You can create more than one filter for a field.

Add a filter

1. In the **Field Administration** tab, select **Fields > Edit** to modify the field.
The **Details** tab appears. By default, the **Appearance** section expands and displays the field details.
2. Expand the **Filters** section.
3. On the **Operators** list, select the operator.
The values available in the Operator list depends on the type of field defined. The Operator values available for each field type are as follows:

Operator value option	Alpha	Numeric	Amount	Bit	Date	DocType
Equals	X	X	X	X	X	X
NotEqualTo	X	X	X	X	X	X
LessThan		X	X		X	
LessThanOrEqualTo		X	X		X	
GreaterThan		X	X		X	
GreaterThanOrEqualTo		X	X		X	
Between		X	X		X	
Contains	X	X	X			X

Operator value option	Alpha	Numeric	Amount	Bit	Date	DocType
StartsWith	X	X	X			X
EndsWith	X	X	X			X

The selected operator affects the values entered in the **Value From** and **Value To** fields.

- In the **Value From** and **Value To** fields, add an appropriate value.
For example, to create a filter between 1000-15000 for an amount field, in **Operators** list, select **Between** in the **Values From** field and enter **1000**, and in the **Values To** field, enter **15000**.
- Click **Save**.

Valid values

Valid values are used to select from multiple index field values, when searching or indexing a document. You can generate your own valid values and find them in the field details.

Add a valid value

- In the **Field Administration** tab, select **Fields > Edit** to modify the field.
The **Details** tab appears. By default, the **Appearance** section expands and displays the field details.
- Expand the **Valid Values** section.
- In the **Value** box, enter the value that CloudDocs will use as an internal reference. Example, EMPBENESUPP.
- In the **Display Value** box, enter a value that is displayed to the user. Example, BENEFITS SUPPLEMENT.
- Click **Add**. The new value is added to the list of valid values.
To delete a valid value, click **Delete X** for the field.

Once the field values are defined, users can see these values on **Search** or **Quick Indexing** pages and the administrators can see these values on **Search** page.

Edit valid values for a subgroup field

As valid values are passed down from a parent group to its subgroups, it is not necessary to redefine the valid values for each subgroup.

You can change the display values for a subgroup. The change is reflected only for that subgroup.

When you define a field for a subgroup, you cannot see the values that are defined at the parent level. However, you can change how the parent's valid value is displayed for the subgroup you are defining.

- While defining a field for a subgroup, enter the name of the parent group's valid value in the **Value** box.
- In the **Display Value** box, enter the value you want the user to see for the subgroup.

3. Click **Add**.

Examples for editing a field

The following examples illustrate how to edit the following six index fields to provide a meaningful name to each field.

Index field types	Meaningful names
ProcessDate	Capture Date
Numeric1	Employee ID
Date	Hire Date
DocType	Document Type
Alpha1	First Name
Alpha2	Last Name

ProcessDate field example settings

You can change the name of the system variable "ProcessDate" to "Capture Date".

The "ProcessDate" system variable contains the date the document is scanned or uploaded (captured) in CloudDocs. Changing the name to something more meaningful does not change the actual variable name; it only changes the way the name is displayed to group users.

1. Click **Edit** next to the field in the **Fields** tab.
The **Details** page appears.
2. Change the **Field Label** to **Capture Date**.
3. Ensure both **Display on Search** and **Display on Results** are selected.
4. To avoid the user to enter a value in the search field, uncheck the **Require on Search** option.
5. To display this field as first in the list, enter **1** in the **Display Order** field.
6. As this field will not be used in the **Reference Data Lookup** process, select **Independent** for **Field Dependency**.
7. As this is a system variable, ensure the **Editable** setting is not selected.
8. Click **Update Field** to save the changes and return to the **Fields** tab.
The label for the **ProcessDate** field changes to **Capture Date**.

Numeric1 field example settings

You can change the name of the system variable "Numeric1" to "Employee ID".

1. Select **Edit** next to the field in the **Fields** tab.
The **Details** page appears.
2. Change the **Field Label** to **Employee Id**.
3. Ensure both **Display on Search** and **Display on Results** are selected.
4. To avoid the user to enter a value in the search field, uncheck the **Require on Search** option. .
5. To display this field second in the list, enter **2** in the **Display Order** field.
6. Select **Parent** for the **Field Dependency** setting.

The **Field Dependency** determines whether a field is used during **Reference Data Lookup**. If a field is specified as a **Parent**, it is used as a key to search for related **Child** field values during indexing.

For example, if you are indexing multiple documents for employee ID 343-99-333, and Employee ID is defined as a Parent field. When you enter the number and tab out of the Employee ID field, CloudDocs uses the value to search previously stored index values to automatically populate any related Child fields (such as First Name, Last Name, Address, Phone Number, Hire Date, and more).

7. Select Editable.

If a field is editable, the field's index value can be changed by authorized users on the Results page in the Search feature. Only the index fields are editable.

You can prevent individual users from editing index field values by disabling the **EditArchive** option when you define their Assigned Roles.

8. Click Update Field to save the changes and return to the **Fields** tab.

The Label for the "Numeric1" field changes to "Employee ID".

Date1 field example settings

In this example, we will change the name of the variable "Date1" to "Hire Date".

1. Select **Edit** next to the field in the **Fields** tab.
The **Details** page appears.
2. Change the **Field Label** to **Hire Date**.
3. Ensure both **Display on Search** and **Display on Results** are selected.
4. To avoid the user to enter a value in the search field, uncheck the **Require on Search** option.
5. To display this field third in the list, enter **3** in the **Display Order** field.
6. Select **Child** for **Field Dependency**.
7. Select **Editable**.
8. Click **Update Field** to save the changes and return to the **Fields** tab.
The label for the **Date1** field changes to **Hire Date**.

DocType field example settings

In this example, we will change the name of the variable "DocType" to "Document Type".

1. Click **Edit** next to the field in the **Fields** tab.
The **Details** page appears.
2. Change the **Field Label** to **Document Type**.
3. Ensure both **Display on Search** and **Display on Results** are selected.
4. To avoid the user to enter a value in the search field, uncheck the **Require on Search** option.
5. To display this field fourth in the list, enter **4** in the **Display Order** field.
6. Select **Independent** for **Field Dependency**.
7. Select **Editable**.
8. Click **Update Field** to save the changes and return to the **Fields** tab.
The label for the **DocType** field changes to **Document Type**.

Valid values for document types

In addition, define five Valid Values to use as document types for the DocType field:

- Application for Employment
- Confidentiality Agreement
- Offer Letter
- Personal Information Form
- W-4

For each of the document types listed above, do the following:

1. In the **Field Management** page, select **Details > Valid Values**. In the **Value** box, enter the internal name you want for the document type (such as EmpAppl for the Application for Employment document or ConfAgreement for Confidentiality Agreement).
2. In the corresponding **Display Value** box, enter the name to display (such as, Application for Employment and Confidentiality Agreement).
3. Click **Add** to add to the list.
To remove a document from the list, click **Delete** next to the desired document value.

Alpha1 field example settings

In this example, we will change the name of the variable "Alpha1" to "First Name".

1. Click **Edit** next to the field in the **Fields** tab.
The **Details** page appears.
2. Change the **Field Label** to **First Name**.
3. Ensure both **Display on Search** and **Display on Results** are selected.
4. To avoid the user to enter a value in the search field, uncheck the **Require on Search** option.
5. To display this field fifth in the list, enter **5** in the **Display Order** field.
6. Select **Child** for **Field Dependency**.
7. Select **Editable**.
8. Click **Update Field** to save the changes and return to the **Fields** tab.
The label for the **Alpha1** field changes to **First Name**.

Alpha2 field example settings

Here you will change the name of the variable Alpha1 to First Name.

Apply the same settings that were specified for the Alpha1 field except that the **Field Label** should be Last Name, and the **Display Order** setting should be **6**.


Create a subgroup

You can create a subgroup within a group.

Subgroups offer a filtered view of group documents. Subgroups can restrict user access to documents based on specific filters. A subgroup inherits all the fields defined for the parent group.

Once a subgroup is created, it cannot be deleted.

1. In the **Organization Management** page, select **Group Administration** and click the level of organization, such as HR group, to create a subgroup.
2. Click **Add Group**.
The **Group Details** page appears.
3. Enter a name for the subgroup, such as Employment Apps.
4. Enter a description for the subgroup, such as Employment Applications (HR) (Optional).
5. Select the following options:
 - **Enabled**
 - **Enable challenge response**
 - **Allow cookie for challenge response**
 - **Force challenge response onto subgroups**


 See [Create a group](#) for description of the above options.

6. Click **Save**.
A **Group saved successfully** message appears and the new subgroup is added under the selected group. For example, the Employment Apps subgroup appears under HR group.

Edit a subgroup

Once a subgroup is created, you can modify the subgroup, such as modify the **Document Type** field to restrict the members of the subgroup to search and view specific documents only.

For example, restrict the Employment Apps subgroup to search and view the Employment Application documents only and not allow access to any other Human Resource documents.

 Make sure the document type is already defined at the group level. See [Example for Document Type settings](#).

To edit the subgroup, do the following:

1. On the CloudDocs Home page, go to **Administration > Group Settings**.
The **Organization Management** page appears. By default, the **Group Administration** tab is open.
2. Select the **Employment Apps** subgroup created in the previous section and click **Field Administration**.
The **Field Management** page appears.

3. Click **Edit** next to the **DocType** field.
The **Details** page appears.
4. Clear the **Display on Search** option to limit the subgroup access to specific documents, such as **Employment Applications**, rather than the entire list of document types. .
5. Clear **Editable** to prevent the users from changing the **Document Type** from the **Results** screen.

i To prevent a document from being indexed incorrectly, keep **Editable** and **Display on Results** selected. Authorized users can then change the **Document Type** as needed.

6. Add a filter to prevent editing of this field.
 - a. Under the **Filters** section, click **Add** to display the **Filter Builder** settings.
 - b. Set the **Operator** setting to **Equals**.
 - c. In the **Value From** box, enter the name of the field that you defined at the time of creating the group. For example, enter **EmpAppl** as the **Field Name** of the **Employee Application** field you defined when the **HR group** was created.
This ensures that only **Employment Applications** can be searched for and displayed by members of this subgroup.
 - d. Click **Save** to save the new filter.
The filter is added to the **Filters** list.
7. Click **Update Field** to save the changes.


Add a user


You can create users, assign users to one or more groups, and assign security privileges to users specific to each group.

i The privileges assigned to a group also applies to all the subgroups within that group. If you want to assign privileges to only a subgroup, select the subgroup and assign privileges.

1. On the CloudDocs Home page, select **Administration > Users**.
The **User Management** page appears. This page lists the groups over which you have administrative control.
2. On the group organization tree, click the group or subgroup to which you want to add a user, such as HR.
3. Click **Add User**.
The **Adding new user** page appears.
4. In the **User Details** section, configure the following information for the new user.

Email Address	The email address of the user. It is the user's login ID.
First Name	The first name of the user.
Last Name	The last name of the user.

Enabled	If selected, indicates that the user is active.
Password	The password for the user. <div style="background-color: #e6f2ff; padding: 5px; border: 1px solid #add8e6;"> <p> Remember this password as you need to provide this password to the new user. After using this password for the first time, the user must create a new password.</p> </div>
Verify Password	Enter the password again for verification.

5. Assign privileges for this user.
6. To assign privileges to this user, select a group or subgroup from the **Available** box. For example, choose the **HR** group.
7. Click the **Assign** icon .

The **Assign Roles** dialog box is displayed and the following privileges are available.


Privilege	Description
Account Admin	The user has full administration privileges for this account, group and its subgroups, and users.
Admin	The user has full administration privileges for this group and its subgroups, and users.
Archive	The user can search the document repository and view results.
Audit	The user can create and view audit reports.
Capture Document	The user can scan and upload documents.
Delete WorkQueue	The user can delete individual items from the workflow queue.
Edit Archive	The user can edit index fields in the document repository when results are displayed.
Exception	The user can use Quick Index or RapiDex to index documents in workflow queues.
Group Admin	The user can create and manage groups and subgroups but cannot create users.
User Admin	The user can create and manage users but cannot create groups.

8. Select the privileges the user needs. For example, select all privileges except **Edit Archive**.
9. Click **OK**.

The group is added to the **Assigned** list.

To review or change the privileges assigned to the group, select the group in the **Assigned** box and click **Edit**. Make changes as needed and click **OK**.

To delete the privileges for the group, select the group in the **Assigned** column and click **Remove**.


 You cannot remove privileges a user has at the group level. The privileges that a user does not have at the group level can be added for them in a subgroup. See Add privileges for a user at the subgroup level.

10. In the **Comments** box, add appropriate additional information, such as "User1 has all the privileges except editing index fields for the group".
11. Click **Save**.
The user will have access to the selected group and all the subgroups within that group.

Add privileges for a user at the subgroup level

By default, all the privileges assigned to a user at the group level are also available at the subgroup level. You can assign a privilege to a user at the subgroup level if that privilege is not assigned at the group level.

For example, in the HR group, User1 was not granted access to edit archive index fields. You can only grant User1 privileges for the subgroup Employment Apps. .

1. Select **Employment Apps** in the **Available** column. See the Assign privileges step in [Add a user](#).
2. Click the Assign icon .
3. In the **Assign Roles** dialog box, select **Edit Archive**.
4. Click **OK**.
5. In the **Comments** box, add appropriate additional information, such as "User1 can edit index fields for Employment Apps, but cannot do so for the HR group or any other subgroup within the HR group".
6. Click **Save**.
User1 can edit index fields for the Employment Apps documents only and not for other group or subgroup.

Broadcast a message

Create messages to communicate information to users.

1. On the CloudDocs **Home** page, select **Administration > Group Settings > Broadcast Administration**.
The **Broadcast Message Management** page appears.
2. Click **Create Message**.
The **Edit Message** page appears.
3. Configure the following settings for the message.

Message Text	The message you want to display on the Home page when users log in.
Start Date/Time	The date and time you want the message to first appear on the Home page in the format MMDDYY and HH:MM.
End Date/Time	The date and time you want the message to stop appearing on the Home page in the format MMDDYY and HH:MM.
Organization	Select the group or subgroup for which you want the message to appear.
Active	If selected, activates the selections for this message. If clear, the message will not appear.
Include Child Groups	If selected, displays the message for the subgroups within the selected group.

- Click **Save** to save your entries.

The **Messages** tab will have all the messages you saved. Click **Exit** to cancel any entries or changes and return to the **Messages** tab.

To edit a message, on the **Messages** tab, click **Edit** for the message. Make changes as needed and click **Save**.

Set rules for a document type

You can set audit rules to filter the documents that are about to expire.

- Go to **Administration > Reporting > Document Audit**.

The **Document Audit Rules** page appears.

Document Audit Rules


Save

Parent Field: Contract#

Document Type	Required	Expire Rule: example (30 day(s) after Process Date)			
24HOURHOLD	<input checked="" type="checkbox"/>	Value: 30	Day(s)	after Process Date	X
45SQUARE	<input checked="" type="checkbox"/>	Value: 30	Day(s)	after Process Date	X
ABDISCLOSURE	<input checked="" type="checkbox"/>	Value: 1	Day(s)	after Process Date	X
ACHCANCEL	<input checked="" type="checkbox"/>	Value: 3	Month(s)	after Origination Date	X
ACHPOLICY	<input checked="" type="checkbox"/>	Value: 40	Day(s)	after Modified Date	X
ACHSPEC	<input type="checkbox"/>	Value: <input type="text"/>	<input type="text"/>	after <input type="text"/>	
ADDENDUM	<input type="checkbox"/>	Value: <input type="text"/>	<input type="text"/>	after <input type="text"/>	
ADDLINFO	<input type="checkbox"/>	Value: <input type="text"/>	<input type="text"/>	after <input type="text"/>	
ADDLITEMS	<input type="checkbox"/>	Value: <input type="text"/>	<input type="text"/>	after <input type="text"/>	
AFFIDAVIT	<input type="checkbox"/>	Value: <input type="text"/>	<input type="text"/>	after <input type="text"/>	
AFFIDAVITOSR	<input type="checkbox"/>	Value: <input type="text"/>	<input type="text"/>	after <input type="text"/>	
AGREEINS	<input type="checkbox"/>	Value: <input type="text"/>	<input type="text"/>	after <input type="text"/>	


- Select the **Document Type** for which you want to set the rules.
- Enter the number of days, months, or years of expiry in the **Value** box and select **Day(s)**, **Month(s)**, or **Year(s)** from the drop-down box.

4. Select the date after which you want a notification to be triggered. The available options are:
 - **Process Date:** Select this option to send notification after the set period from the processed date.
 - **Modified Date:** Select this option to send notification after the set period from the item modified date.
 - **Origination Date:** Select this option to send notification after the set period from the item origination date.
 - **Date Of Signature:** Select this option to send notification after the set period from the date of signature.
5. Click **Save** to save the rule.

 A rule is cleared automatically after the set expiry period is completed.

Create an annotation using the REST API

Call `"/api/annotations/create"` using a REST API POST action and create an annotation with the following information.

 Elements marked with * are mandatory.

Request Headers

Element	Data type	Description
OrgCode*	String	A unique client-specific string provided by Tungsten Automation. Example: DemoOrgCode
SecurityToken*	Base64 string	The token generated based on the token request.

Request body: The request body is in the JSON format based on the following elements.

Element	Data type	Description
Module*	String	A unique module code in the database. Example: ARCHIVE
RefID*	Integer	The transaction ID or the document ID to which the annotations belong.
Comments*	String	A long text data representing the actual annotation information.

Success Response: Returns the following information in the JSON format.

Element	Data type	Description
Module	String	A unique module code in the database. Example: ARCHIVE
RefID	Integer	The transaction ID or the document ID to which the annotation belongs.
HttpStatus	Integer	HTTP response status codes indicating whether a specific HTTP request is successfully completed.


Element	Data type	Description																		
Data	String	The annotation record created in the JSON format with the following structure: <table border="1" data-bbox="602 411 1471 743"> <thead> <tr> <th>Element</th> <th>Data type</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>AnnotationID</td> <td>Integer</td> <td>The annotation ID.</td> </tr> <tr> <td>RefID</td> <td>Integer</td> <td>The transaction ID or the document ID to which the annotation belongs.</td> </tr> <tr> <td>Comments</td> <td>String</td> <td>A long text data representing the actual annotation information.</td> </tr> <tr> <td>UserID</td> <td>String</td> <td>The user who creates the annotation</td> </tr> <tr> <td>LastModifiedDate</td> <td>String</td> <td>The date and time value in UTC.</td> </tr> </tbody> </table>	Element	Data type	Description	AnnotationID	Integer	The annotation ID.	RefID	Integer	The transaction ID or the document ID to which the annotation belongs.	Comments	String	A long text data representing the actual annotation information.	UserID	String	The user who creates the annotation	LastModifiedDate	String	The date and time value in UTC.
Element	Data type	Description																		
AnnotationID	Integer	The annotation ID.																		
RefID	Integer	The transaction ID or the document ID to which the annotation belongs.																		
Comments	String	A long text data representing the actual annotation information.																		
UserID	String	The user who creates the annotation																		
LastModifiedDate	String	The date and time value in UTC.																		

Error response: Returns the following information in the JSON format.

Element	Data type	Description
Module	String	A unique module code in the database. Example: ARCHIVE
RefID	Integer	The transaction ID or the document ID to which the annotation belongs.
HttpStatus	Integer	HTTP response status codes indicating whether a specific HTTP request is successfully completed.
Data	String	Error information.

Search annotations using the REST API

Call "/api/annotations/search" with a REST API POST action and search annotations using the information below.

 Elements marked with * are mandatory.

Request Headers

Element	Data type	Description
OrgCode*	String	A unique client-specific string provided by Tungsten Automation. Example: DemoOrgCode
SecurityToken*	Base64 string	The token generated based on the token request.

Request body: The request body is in the JSON format based on the following elements.

Element	Data type	Description
Module*	String	A unique module code in the database. Example: ARCHIVE
RefID*	Integer	The transaction ID or the document ID to which the annotations belong.

Success Response: Returns the following information in the JSON format.

Element	Data type	Description																		
Module	String	A unique module code in the database. Example: ARCHIVE																		
RefID	Integer	The transaction ID or the document ID to which the annotations belong.																		
HttpStatus	Integer	HTTP response status codes indicating whether a specific HTTP request is successfully completed.																		
Data	String	An array of annotation records created in the JSON format with the following structure: <table border="1" data-bbox="630 653 1463 1014"> <thead> <tr> <th>Element</th> <th>Data type</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>AnnotationID</td> <td>Integer</td> <td>The annotation ID.</td> </tr> <tr> <td>RefID</td> <td>Integer</td> <td>The transaction ID or the document ID to which the annotation belongs.</td> </tr> <tr> <td>Comments</td> <td>String</td> <td>A long text data representing the actual annotation information.</td> </tr> <tr> <td>UserID</td> <td>String</td> <td>The user who creates the annotation</td> </tr> <tr> <td>LastModifiedDate</td> <td>String</td> <td>The date and time value in UTC.</td> </tr> </tbody> </table>	Element	Data type	Description	AnnotationID	Integer	The annotation ID.	RefID	Integer	The transaction ID or the document ID to which the annotation belongs.	Comments	String	A long text data representing the actual annotation information.	UserID	String	The user who creates the annotation	LastModifiedDate	String	The date and time value in UTC.
Element	Data type	Description																		
AnnotationID	Integer	The annotation ID.																		
RefID	Integer	The transaction ID or the document ID to which the annotation belongs.																		
Comments	String	A long text data representing the actual annotation information.																		
UserID	String	The user who creates the annotation																		
LastModifiedDate	String	The date and time value in UTC.																		

Error response: Returns the following information in the JSON format.

Element	Data type	Description
Module	String	A unique module code in the database. Example: ARCHIVE
RefID	Integer	The transaction ID or the document ID to which the annotations belong.
HttpStatus	Integer	HTTP response status codes indicating whether a specific HTTP request is successfully completed.
Data	String	Error information.


View redaction by role

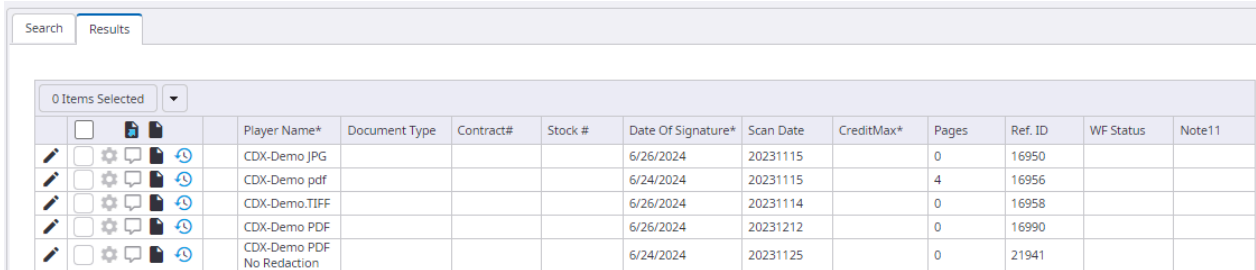
CloudDocs redaction can be enabled or disabled by the administrators of the organization.











To enable or disable it, do the following.

1. From the menu bar, go to **Administration**.
2. Select **Group Settings**.
3. Click **Preferences Administration** tab.
4. Search **RedactionEnabled** and select **true** to enable it and **false** to disable it.
5. Click **Save** to save the settings.

If redaction is disabled

If redaction is disabled, the **Results** page only displays **View Item**  for documents without redactions. Documents with redactions do not appear.



0 Items Selected		Player Name*	Document Type	Contract#	Stock #	Date Of Signature*	Scan Date	CreditMax*	Pages	Ref. ID	WF Status	Note1
		CDX-Demo.JPG				6/26/2024	20231115		0	16950		
		CDX-Demo.pdf				6/24/2024	20231115		4	16956		
		CDX-Demo.TIFF				6/26/2024	20231114		0	16958		
		CDX-Demo.PDF				6/26/2024	20231212		0	16990		
		CDX-Demo.PDF No Redaction				6/24/2024	20231125		0	21941		

If redaction is enabled

If redaction is enabled, the user has access only to the redacted documents in the Results page. You can assign either role to allow overriding redactions.

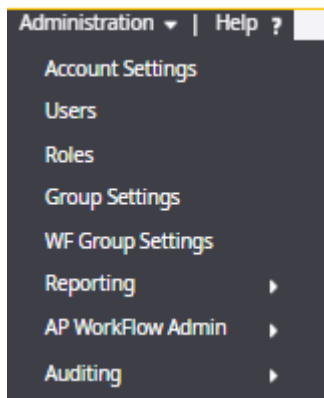
- [Redaction override role](#)
- [No redaction override role](#)

Assign Redaction Override role

A user with the redaction override role can access both the redacted and unredacted versions of the document.

To assign the Redaction Override role, do the following.

1. In the menu bar, go to **Administration > Users**.



The **User Management** page appears.

2. Select the desired user from the list, such as Alexey Kovalev.

User Management

Username	Last Name	First Name	Enabled	Last Login	Password Created
[blurred]	[blurred]	[blurred]	<input checked="" type="checkbox"/>	05/09/2024 09:38:22	04/29/2024
[blurred]	[blurred]	[blurred]	<input checked="" type="checkbox"/>	04/04/2023 07:07:37	04/04/2023
[blurred]	[blurred]	[blurred]	<input type="checkbox"/>	12/06/2012 16:25:28	12/06/2012
[blurred]	[blurred]	[blurred]	<input checked="" type="checkbox"/>	04/19/2016 19:37:22	03/09/2016
[blurred]	[blurred]	[blurred]	<input type="checkbox"/>	03/19/2015 17:09:37	03/09/2015
[blurred]	[blurred]	[blurred]	<input checked="" type="checkbox"/>	02/08/2023 07:04:24	N/A
[blurred]	[blurred]	[blurred]	<input checked="" type="checkbox"/>	N/A	N/A
[blurred]	[blurred]	[blurred]	<input checked="" type="checkbox"/>	11/04/2022 16:00:27	12/31/2033
[blurred]	[blurred]	[blurred]	<input checked="" type="checkbox"/>	04/26/2016 15:41:24	04/15/2016
[blurred]	[blurred]	[blurred]	<input checked="" type="checkbox"/>	08/10/2020 09:06:12	08/10/2020
[blurred]	[blurred]	[blurred]	<input checked="" type="checkbox"/>	08/11/2020 09:44:04	08/11/2020
alexey.kovalev@kofax.com	Kovalev	Alexey	<input checked="" type="checkbox"/>	10/18/2022 04:49:11	N/A
[blurred]	[blurred]	[blurred]	<input type="checkbox"/>	10/25/2013 14:36:57	08/27/2013
[blurred]	[blurred]	[blurred]	<input type="checkbox"/>	03/14/2013 15:44:17	02/25/2013
[blurred]	[blurred]	[blurred]	<input type="checkbox"/>	12/17/2012 14:22:40	12/06/2012

1 2 3 4 5 6 7 8

User Details

Email Address

First Name

Last Name

Enabled

Password

Verify Password

Privileges

Available

- Panini
 - 123test1
 - AddGroup

→

Assigned

- Panini
- eGistics

3. Select **Privileges**.
 4. Select the group to assign the **Redaction Override** role, such as Panini.
 5. Click **Edit**.
- The **Assign Roles** dialog box appears.


Assign Roles:


<input type="checkbox"/> Account Admin	<input type="checkbox"/> Merge Documents
<input checked="" type="checkbox"/> ACS Reports	<input type="checkbox"/> Redaction Override
<input checked="" type="checkbox"/> Admin	<input checked="" type="checkbox"/> Reports
<input checked="" type="checkbox"/> Audit	<input checked="" type="checkbox"/> User Admin
<input checked="" type="checkbox"/> Capture Document	<input checked="" type="checkbox"/> Versioning
<input checked="" type="checkbox"/> Delete Repository	<input checked="" type="checkbox"/> View Document Audit
<input checked="" type="checkbox"/> Delete WorkQueue	<input checked="" type="checkbox"/> Work Queue
<input checked="" type="checkbox"/> Document Search	<input checked="" type="checkbox"/> Workflow Admin
<input checked="" type="checkbox"/> Edit Results	<input type="checkbox"/> Workflow ReadONLY
<input checked="" type="checkbox"/> eGistics User	<input checked="" type="checkbox"/> Workflow Search
<input checked="" type="checkbox"/> Group Admin	<input checked="" type="checkbox"/> Workflow User


OK Cancel

6. Select **Redaction Override**.
7. Click **OK** to save the settings.

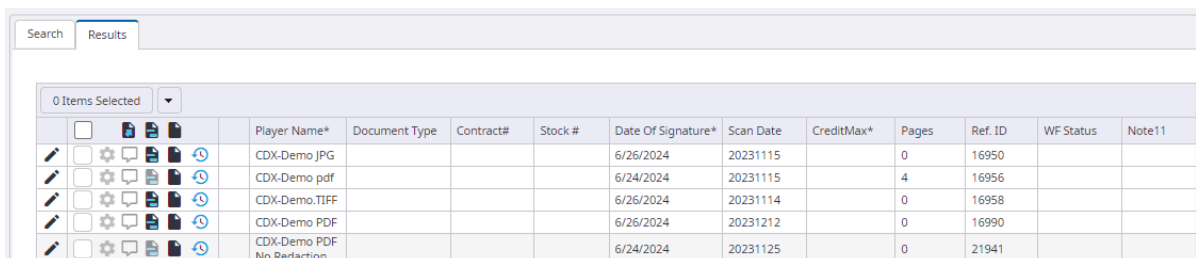
i The following items appear for each search operation that the user performs in the redaction override role.











- **View Item** 

The document is without redactions.
- **View Redacted Item** 

The document contains redactions, but are not visible to the user due to the override role.
- **View Item** 

This is the original document, unredacted.



0 Items Selected		Player Name*	Document Type	Contract#	Stock #	Date Of Signature*	Scan Date	CreditMax*	Pages	Ref. ID	WF Status	Note11
		CDX-Demo.JPG				6/26/2024	20231115		0	16950		
		CDX-Demo.pdf				6/24/2024	20231115		4	16956		
		CDX-Demo.TIFF				6/26/2024	20231114		0	16958		
		CDX-Demo PDF				6/26/2024	20231212		0	16990		
		CDX-Demo PDF No Redaction				6/24/2024	20231125		0	21941		

Confirm the redaction

When you assign the Redaction Override role to a user, ensure that the redaction is not visible.

You can do the following.

1. Search for the documents in a group that has redaction enabled.
Results page displays both the redacted and the unredacted documents.
2. Click on **View Redacted Item** to view it.
The redaction is not visible in the document.

i You do not have to check the other two items because they are without redactions. .

Confirm the redaction in the exported PDF


Additionally, you can download the PDF and check if the redaction is applied.










You can do the following.

1. On the table header, click **Exported Redacted Item(s) to PDF** .
2. Open the PDF.
The redaction is not visible due to the override role.

Unassign Redaction Override role

When Redaction Override is unselected in Assign Roles, the user is not assigned a redaction override role. The user only sees the redacted version of the documents and cannot access the unredacted version.

The user only sees **View Redacted Item**  on the Results page for each search operation that the user performs.

Search		Results										
2 Items Selected												
		Player Name*	Document Type	Contract#	Stock #	Date Of Signature*	Scan Date	CreditMax*	Pages	Ref. ID	WF Status	Note11
		CDX-Demo.JPG				6/26/2024	20231115		0	16950		
		CDX-Demo.TIFF				6/26/2024	20231114		0	16958		
		CDX-Demo.PDF				6/26/2024	20231212		0	16990		
		CDX-Demo.PDF				6/26/2024	20231125		11	23601		
		CDX-Demo.JPG				6/26/2024	20231115		3	23669		

Confirm the redaction

If a user is unassigned redaction override role, make sure that the redaction is visible.


You can do the following.

1. Search for the documents in a group that has redaction enabled.
The **Results** page displays **View Redacted Item**.
2. Click on **View Redacted Item**.
The redaction is visible in the document.

Confirm the redaction in the export PDF

Additionally, you can download the PDF and check if the redaction is applied.

You can do the following.

1. On the table header, click **Export Redacted Item(s) to PDF**  to export it.
2. Open the PDF.
The redaction is visible in the document.



- By default, the redaction color is black (Hex code: #000000), which can be changed to other colors using the app setting key - `RedactionColor`, in the global config table of the database.
- By default, the redaction type is solid rectangle, but it can be changed to pattern rectangle by the app setting key - `RedactionPatternEnabled`, in the global config table of the database.
- The user should not be able to find or view the text hidden behind the redactions.

Exception search

Documents scanned or uploaded with the Capture function contain no redaction data. As a result, the View Redacted Item icon is gray on the search Results page.

0 Items Selected		Player Name*	Document Type	Contract#	Stock #	Date Of Signature*	Scan Date	CreditMax*	Pages	Ref. ID	WF Status	Alpha11
		Q test exception 1	24HOURHOLD	<abc		5/12/2024	20240512	No	1	23751	InWorkflow	
		Q test queues to search	24HOURHOLD	asdf	123	4/1/2024	20240401	No	1	23771		scsc
		Q test upload to queues 1	24HOURHOLD	Q test	123	5/7/2024	20240514	No	1	23773	InWorkflow	123
		Q test required field	24HOURHOLD	Q test	123	5/20/2024	20240506	No	1	23790	REJECTED	Test
		Q test upload tiff	24HOURHOLD	Q test	123	5/20/2024	20240520	No	1	23791	REJECTED	Test

However, if you want to support redaction for scan or upload, provide redaction data for that document in item redaction table in the database.

The table below displays the columns in the item redaction table.

Field Name	Data Type	Description
OrganizationId	Integer	The organization the item belongs to
UserId	Integer	The user who creates redaction data
TableName	String	ItemWorkFlow
RefId	Integer	ItemWorkFlow primary key value
RedactionData	String	JSON data
LastUpdated	Datetime	The date and time in UTC when the item was created or updated

The table below lists the file extensions and output content types that support redaction.

File Extension (Single Item)	Document Type	Content Type (MIME Type)
tif tiff	Tagged Image File Format	Application/PDF
jpg jpeg jpe jfif pjpeg pjp	JPEG images	Application/PDF
pdf	Adobe Portable Document Format	Application/PDF

File Extension (Multiple Items)	Document Type	Content Type
tif tiff	Tagged Image File Format	Application/PDF i When you select multiple items to download: <ul style="list-style-type: none">• Multiple source types are combined into one PDF.• If source types contain any unsupported file extensions under File Extension (Multiple Items) column, error appears.• Redaction is applied to the document before merging.
jpg jpeg jpe jfif pjpeg pjp	JPEG images	
pdf	Adobe Portable Document Format	