DESKDOX EDMS

User Manual

Complete Help Center & Reference Guide

Published: May 19, 2026

Version: 2026.05

Scope: 127 articles across 14 sections

Publisher: Zbix Technologies Pvt Ltd

Support: support@zbixtechnologies.com

Website: https://www.deskdox.com

Table of Contents

CHAPTER 1

Getting Started

First-session guidance, core concepts, and orientation for new DeskDox users.

Getting Started · 1 min read · Reviewed 2026-05-13

Getting Started

What this helps you do

Get ready for daily DeskDox work in your first session.

Quick checklist

1. Sign in with your work account.
2. If prompted, complete 2FA code entry.
3. Open `Profile` and verify your details.
4. Open `Documents` and confirm folder access.
5. Open `My Tasks` and check pending approvals/signatures.
6. Open `Notification Settings` and set your preferred channels.
7. Open `Help` and bookmark key articles for your role.

If you do not see expected menus

- Your role may not include those permissions.
- A module may be feature-gated in your environment.
- Ask your administrator to verify your account scope.

Related reading

- User Manual: Getting Started
- User Manual: Dashboard and Navigation

Getting Started · 1 min read · Reviewed 2026-05-13

Glossary and Key Terms

Approval Task

A workflow step assigned to a user/role requiring approve or reject action.

Deep Search

DeskDox search interface combining query text and structured filters.

Document Details

Panel showing metadata, workflow state, activity, audit, versions, signatures, and permission context for a document.

Feature-gated

A module/feature that is conditionally enabled or disabled in a deployment.

File Request

A generated upload link used to collect files from external users into a selected folder.

Metadata

Structured fields attached to documents (for example category, type, dates, business identifiers) used for validation and retrieval.

Workflow Inbox

View of workflows a user is involved in, including status and progress context.

My Tasks

User action list for workflow approvals/signatures (and optionally invoice tasks in enabled deployments).

Signature Request

A formal signing workflow attached to a document, often with participant order and status tracking.

Emii

DeskDox assistant used for help/document guidance, subject to scope and configuration.

WhatsApp Link State

User account linkage state required before WhatsApp commands can access DeskDox actions.

CHAPTER 2

Dashboard and Navigation

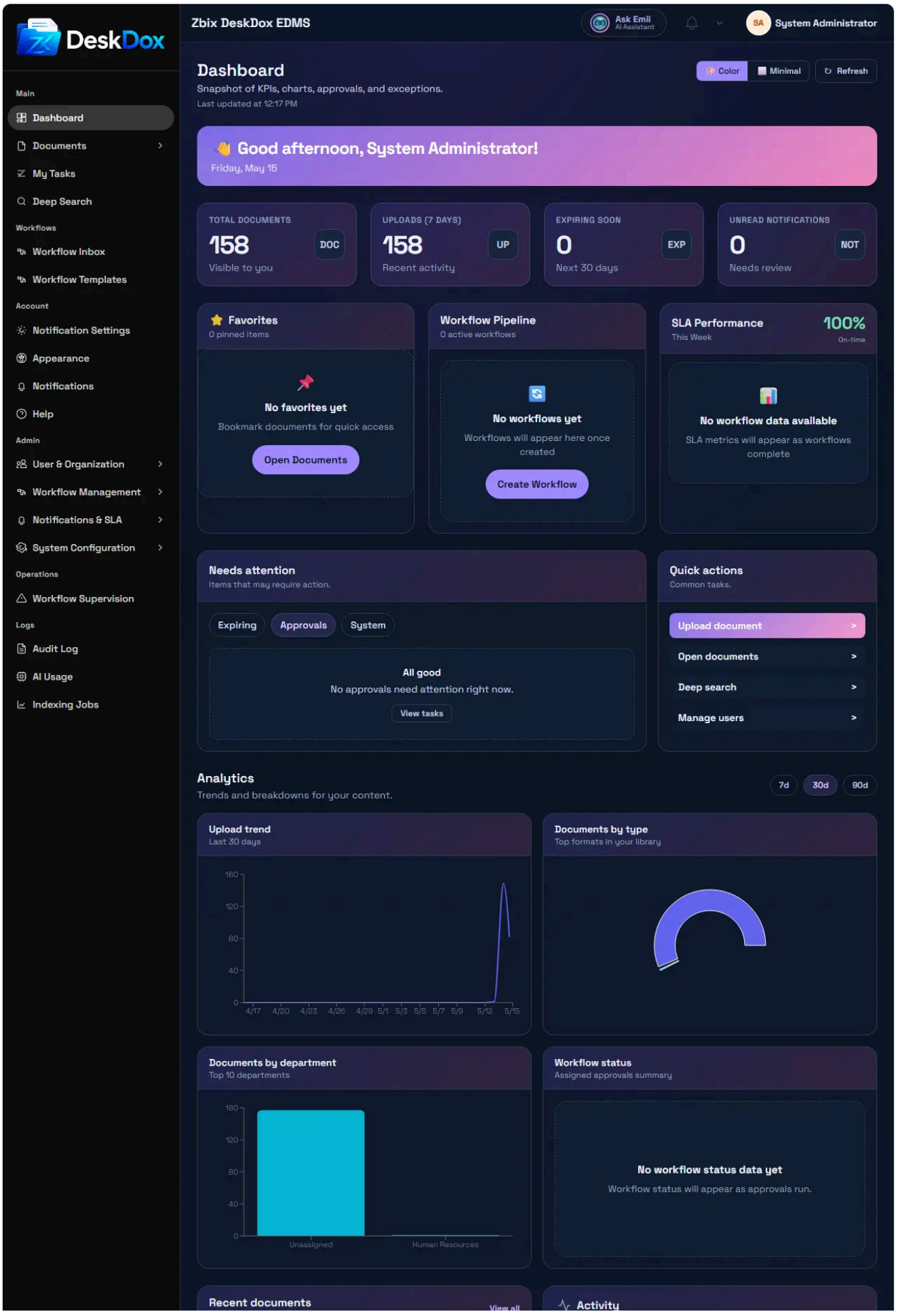
Dashboard metrics, topbar navigation, workspace orientation, and daily navigation patterns.

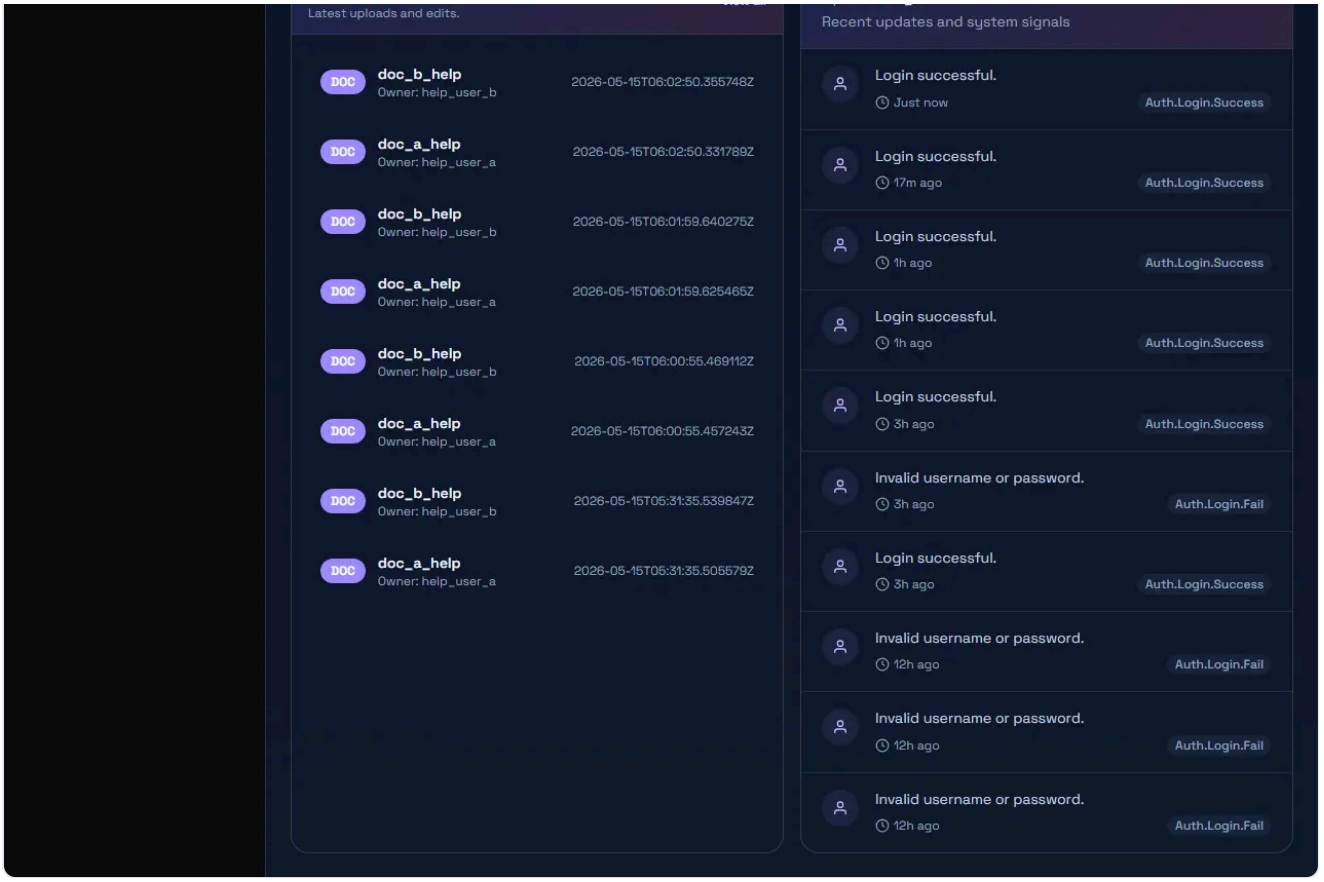
Dashboard and Navigation · 2 min read · Reviewed 2026-05-14

Dashboard Overview

What this helps you do

Use the Dashboard as the first summary view after sign-in. It brings together document counts, recent upload activity, expiring documents, unread notifications, favorite documents, workflow status, SLA performance, and attention or quick-action panels when those widgets are available to your account.


DeskDox
Zbix DeskDox EDMS
Ask Emil
AI Assistant
SA
System Administrator
Main
Dashboard
Documents
My Tasks
Deep Search
Workflows
Workflow Inbox
Workflow Templates
Account
Notification Settings
Appearance
Notifications
Help
Admin
User & Organization
Workflow Management
Notifications & SLA
System Configuration
Operations
Workflow Supervision
Logs
Audit Log
AI Usage
Indexing Jobs
Dashboard
Snapshot of KPIs, charts, approvals, and exceptions.
Last updated at 12:17 PM
Color
Minimal
Refresh
Good afternoon, System Administrator!
Friday, May 15
TOTAL DOCUMENTS
158
DOC
Visible to you
UPLOADS (7 DAYS)
158
UP
Recent activity
EXPIRING SOON
0
EXP
Next 30 days
UNREAD NOTIFICATIONS
0
NOT
Needs review
Favorites
0 pinned items
No favorites yet
Bookmark documents for quick access
Open Documents
Workflow Pipeline
0 active workflows
No workflows yet
Workflows will appear here once created
Create Workflow
SLA Performance
This Week
100%
On-time
No workflow data available
SLA metrics will appear as workflows complete
Needs attention
Items that may require action.
Expiring
Approvals
System
All good
No approvals need attention right now.
View tasks
Quick actions
Common tasks.
Upload document
Open documents
Deep search
Manage users
Analytics
Trends and breakdowns for your content.
7d
30d
90d
Upload trend
Last 30 days
160
120
80
40
0
4/17
4/20
4/23
4/26
4/29
5/1
5/3
5/5
5/7
5/9
5/12
5/15
Documents by type
Top formats in your library
Documents by department
Top 10 departments
160
120
80
40
0
Unassigned
Human Resources
Workflow status
Assigned approvals summary
No workflow status data yet
Workflow status will appear as approvals run.
Recent documents
View all
Activity



KPI cards

The KPI cards are `Total documents`, `Uploads (7 days)`, `Expiring soon`, and `Unread notifications`.

These numbers are user-level summaries. They are filtered by the documents, notifications, and workflow information your account can access. KPI cards can be used as navigation shortcuts when your account has access to the related page. For example, document cards open document views and the unread notification card opens notifications.

Dashboard widgets

Dashboard widgets include `Favorites`, `Workflow Pipeline`, and `SLA Performance`. `Favorites` lists favorite documents and can provide an `Open Documents` action. `Workflow Pipeline` shows active workflow information and can provide a `Create Workflow` action. `SLA Performance` shows workflow SLA metrics when available.

Recent activity, needs-attention, and quick-action panels may appear when there is relevant data and your role can see those items.

Why counts differ

Dashboard counts can differ between users because DeskDox filters by role, folder access, direct document permission, ownership, department membership, workflow assignment, notification recipient, and administrator access. An administrator may see broader totals than a standard user.

Empty or stale dashboard

If the Dashboard appears empty, check whether you have document access, favorite documents, active workflows, unread notifications, or tasks assigned to you. If numbers do not update immediately, refresh the page and allow background indexing, workflow, notification, or analytics updates to finish.

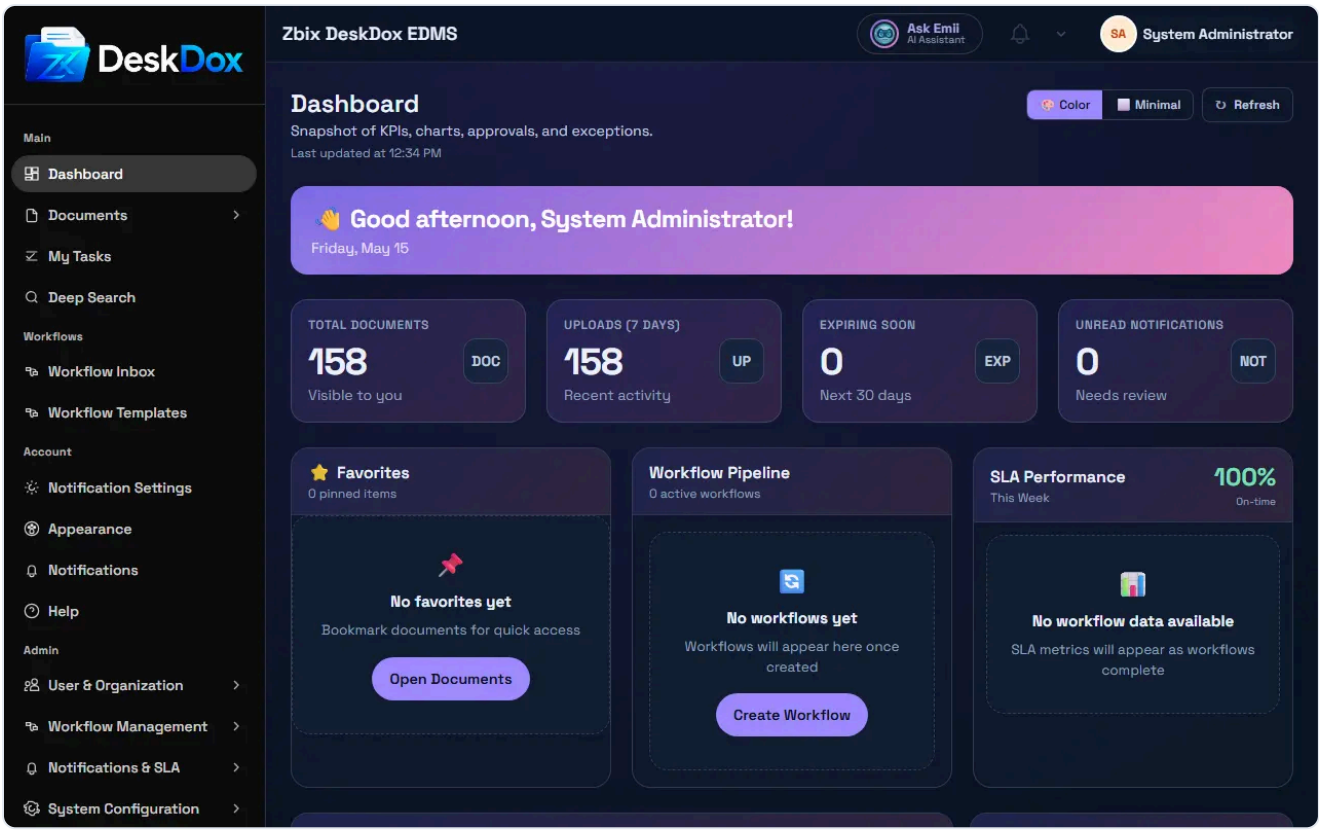
License notices are documented separately. License notices may appear only when the license state requires attention.

Dashboard and Navigation · 1 min read · Reviewed 2026-05-14

Topbar Overview

What this helps you do

Use the authenticated topbar to open Emii, check notifications, and reach account settings from the current page.



Topbar areas

The topbar includes the DeskDox logo area, global search or page search controls when available, the `Ask Emii AI Assistant` button, Help access, notifications bell, and the profile entry point.

Use search to find documents or Help Center information from the current context when that control is visible. Use `Ask Emii AI Assistant` to open Emii when available. Use Help to open guidance resources. Use the bell icon to open notifications. Use the profile initials or name to open account options such as `Account`, `Appearance`, and `Logout` when those menu items are visible.

Missing buttons

A topbar button can be missing because of permissions, feature configuration, license state, screen size, or a deployment setting. Use the topbar options shown in your account to access the available actions.

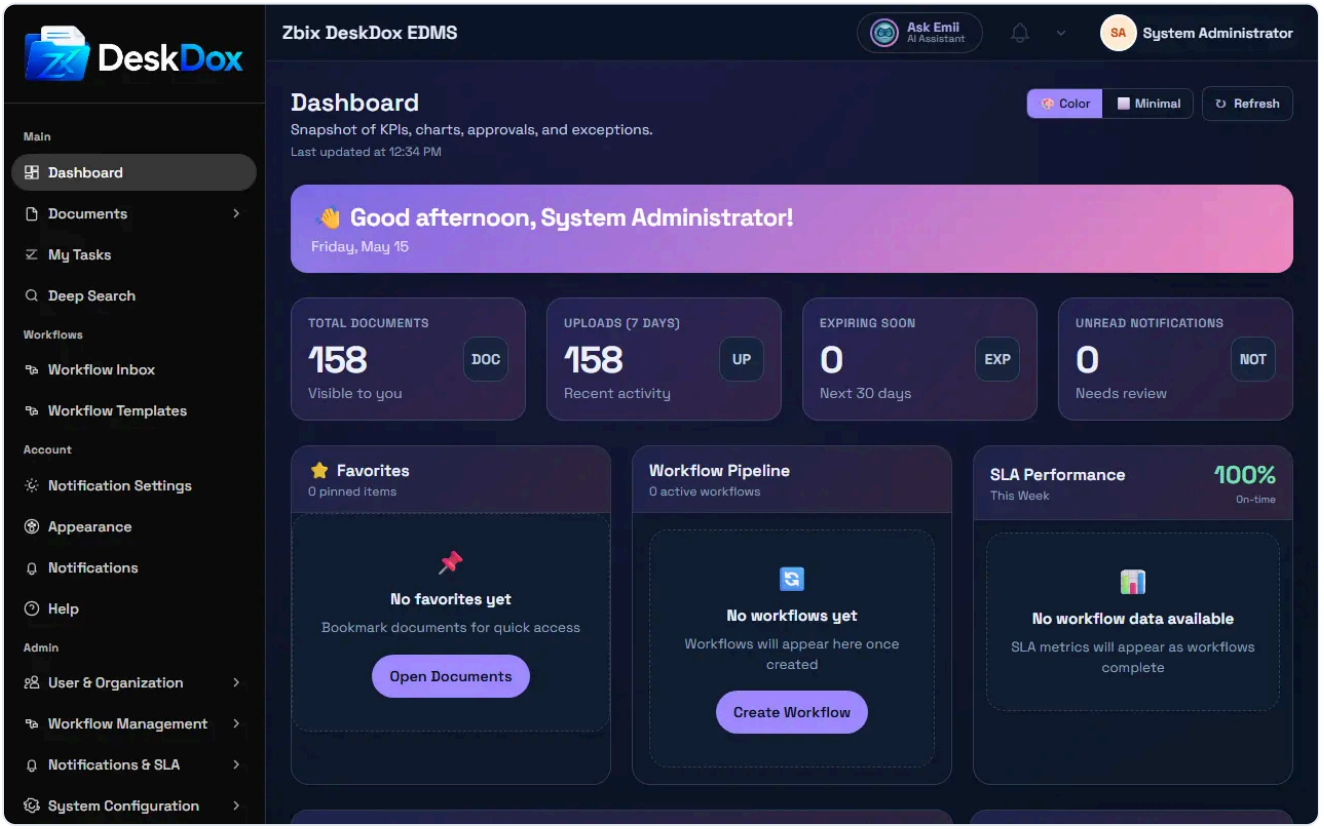
On smaller screens, topbar controls may move, collapse, or require opening a menu depending on the responsive layout.

`Dashboard and Navigation · 2 min read · Reviewed 2026-05-14`

Ask Emii from the Topbar

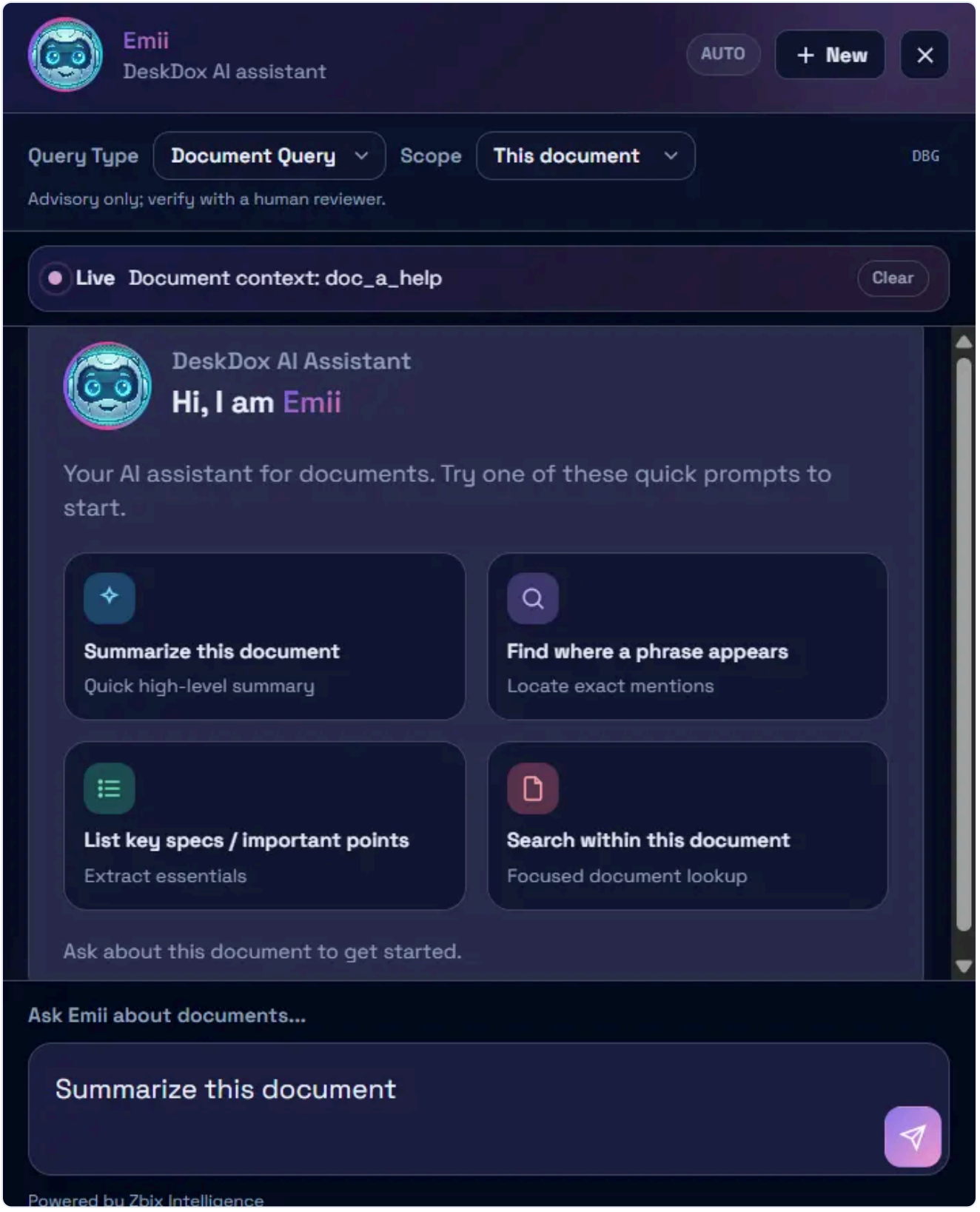
What this helps you do

Open Emii from the authenticated topbar and choose the right kind of question.



Open Emii

Click `Ask Emii AI Assistant` in the topbar when it is visible. The assistant panel opens from the topbar when the feature is available to your account. Panel layout, query type selection, advisory notes, and `New chat` controls may vary by configuration.



Help / Guidance vs document questions

Use Help / Guidance for DeskDox product questions such as how to use the Dashboard, where notifications appear, or how to change theme settings. Help / Guidance answers from available Help Center content and cites the article it used when a source is available.

Use document questions when you want Emii to answer from uploaded document content. Document answers depend on the documents your account is permitted to access, whether the content has been indexed, and whether document AI is enabled for your deployment.

Citations and advisory notes

When Emii answers from Help Center content, citations show the source article or section. Treat Emii as guidance, not approval authority. If an advisory note is visible, read it before acting on high-impact decisions.

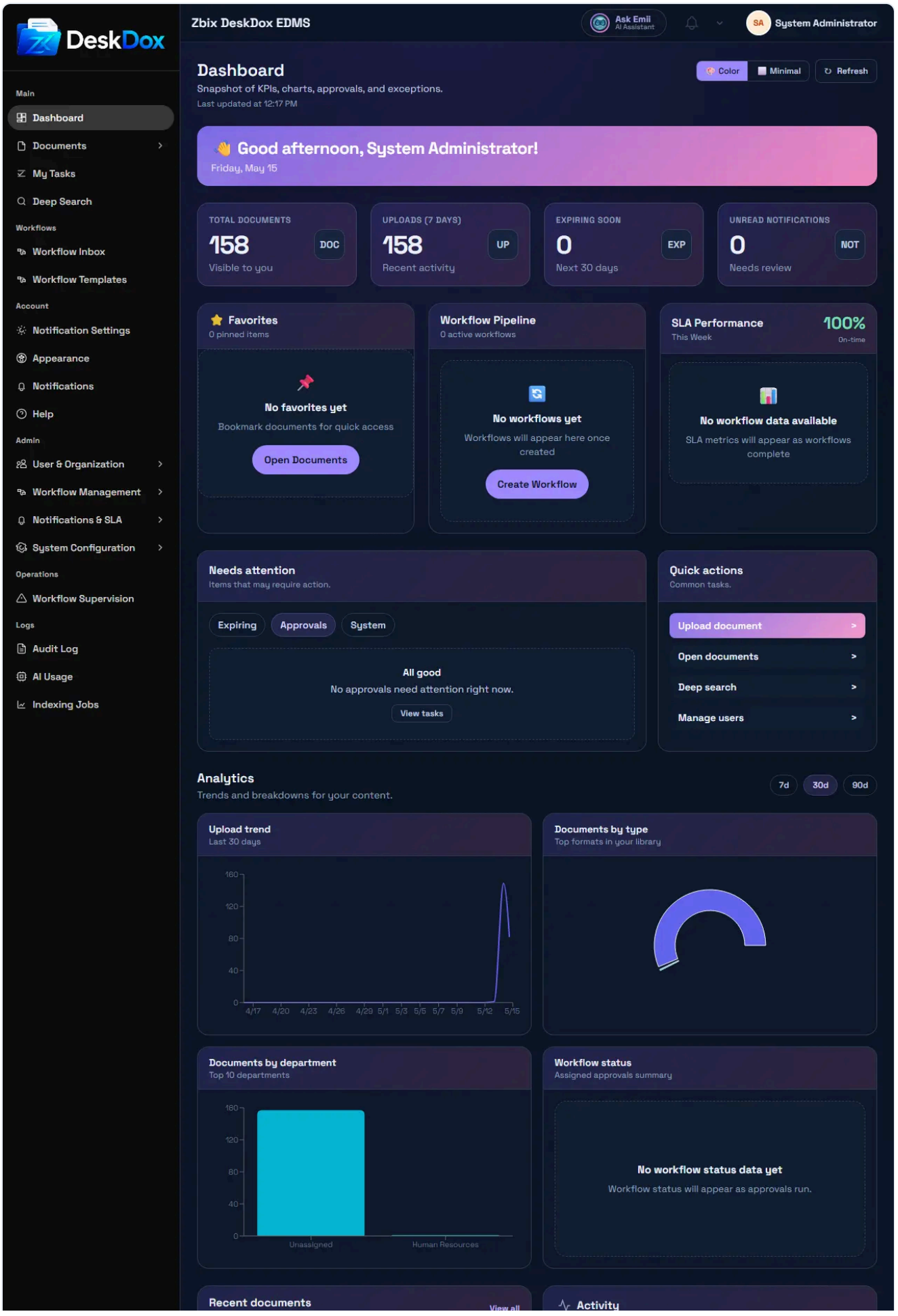
Emii follows DeskDox access controls. It should not use Help Center articles or document content that are unavailable to your account. If an answer is incomplete, refine the question, check whether the relevant help article or document exists, and confirm that you have permission to view it.

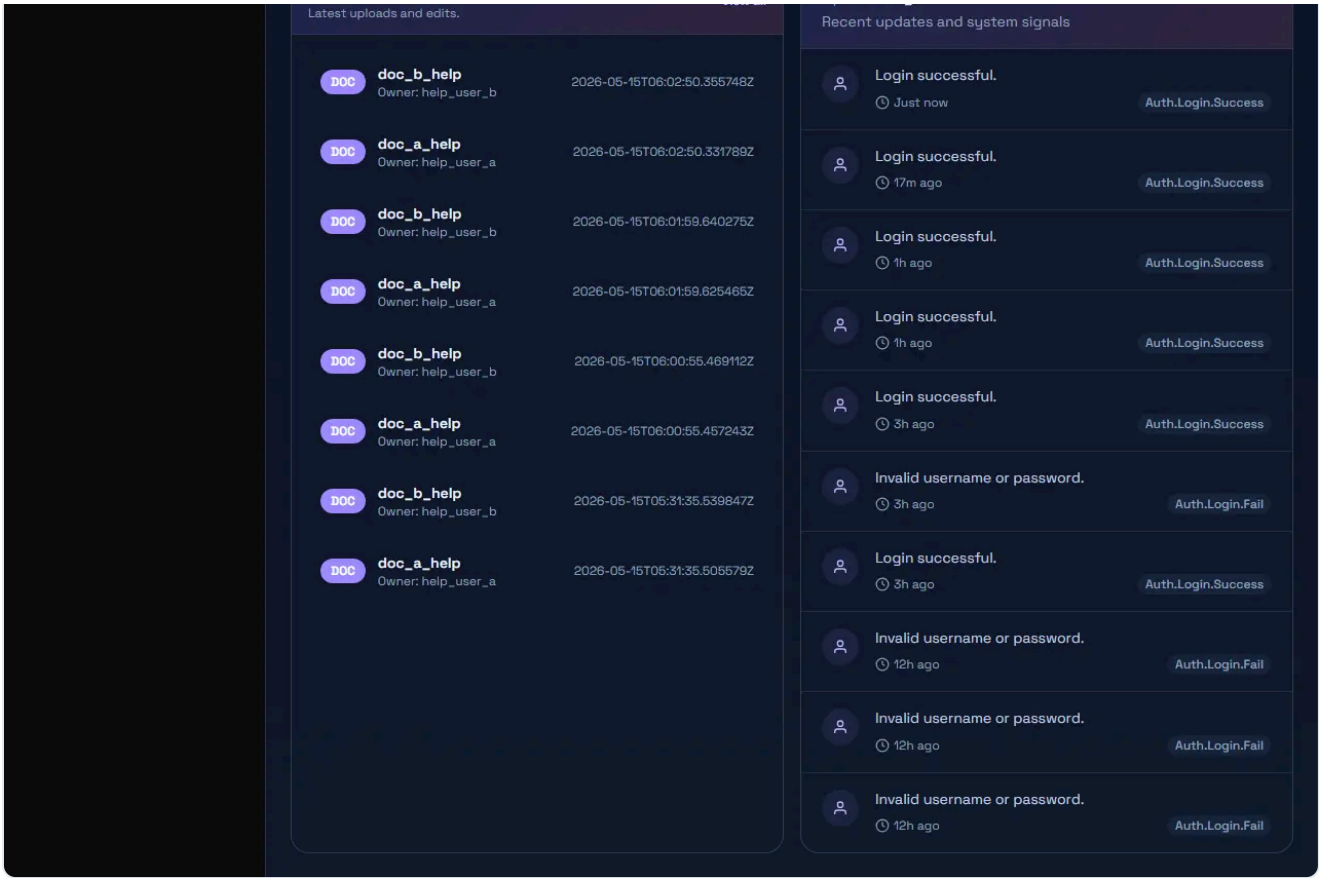
Dashboard and Navigation · 2 min read · Reviewed 2026-05-14

Dashboard KPIs and Widgets

What this helps you do

Understand the Dashboard cards and widgets without assuming that every user sees the same totals.


DeskDox
Zbix DeskDox EDMS
Ask Emil
AI Assistant
SA
System Administrator
Main
Dashboard
Documents
My Tasks
Deep Search
Workflows
Workflow Inbox
Workflow Templates
Account
Notification Settings
Appearance
Notifications
Help
Admin
User & Organization
Workflow Management
Notifications & SLA
System Configuration
Operations
Workflow Supervision
Logs
Audit Log
AI Usage
Indexing Jobs
Dashboard
Snapshot of KPIs, charts, approvals, and exceptions.
Last updated at 12:17 PM
Color
Minimal
Refresh
Good afternoon, System Administrator!
Friday, May 15
TOTAL DOCUMENTS
158
DOC
Visible to you
UPLOADS (7 DAYS)
158
UP
Recent activity
EXPIRING SOON
0
EXP
Next 30 days
UNREAD NOTIFICATIONS
0
NOT
Needs review
Favorites
0 pinned items
No favorites yet
Bookmark documents for quick access
Open Documents
Workflow Pipeline
0 active workflows
No workflows yet
Workflows will appear here once created
Create Workflow
SLA Performance
This Week
100%
On-time
No workflow data available
SLA metrics will appear as workflows complete
Needs attention
Items that may require action.
Expiring
Approvals
System
All good
No approvals need attention right now.
View tasks
Quick actions
Common tasks.
Upload document
Open documents
Deep search
Manage users
Analytics
Trends and breakdowns for your content.
7d
30d
90d
Upload trend
Last 30 days
160
120
80
40
0
4/17
4/20
4/23
4/26
4/29
5/1
5/3
5/5
5/7
5/9
5/12
5/15
Documents by type
Top formats in your library
Documents by department
Top 10 departments
160
120
80
40
0
Unassigned
Human Resources
Workflow status
Assigned approvals summary
No workflow status data yet
Workflow status will appear as approvals run.
Recent documents
View all
Activity



KPI cards

- `Total documents` counts documents visible to your account.
- `Uploads (7 days)` counts recently uploaded documents visible to your account.
- `Expiring soon` counts visible documents approaching expiry.
- `Unread notifications` counts unread notifications for your account.

These cards are clickable when your account has access to the related page. Document cards open document views, and the unread notification card opens notifications. If a card is not clickable in your environment, use the related menu page instead.

Widgets

`Favorites` lists favorite documents and can provide `Open Documents`. `Workflow Pipeline` shows active workflow status and can provide `Create Workflow`. `SLA Performance` shows workflow SLA metrics when workflow data is available. Needs-attention, quick-action, recent activity, or task panels may be visible depending on data, role, permission, and configuration.

Permission filtering

Dashboard figures are not global system totals for every user. They are filtered by access to documents, folders, workflows, notifications, department scope, and administrative permissions. This is why your

Dashboard can show fewer documents or different workflow numbers than another user's Dashboard.

Refresh and count differences

Counts may lag briefly after uploads, workflow updates, notification reads, or lifecycle changes. If the Dashboard count differs from the document list, refresh the page, clear document filters, check expired or deleted views, and confirm you are comparing the same permission scope.

CHAPTER 3

Documents

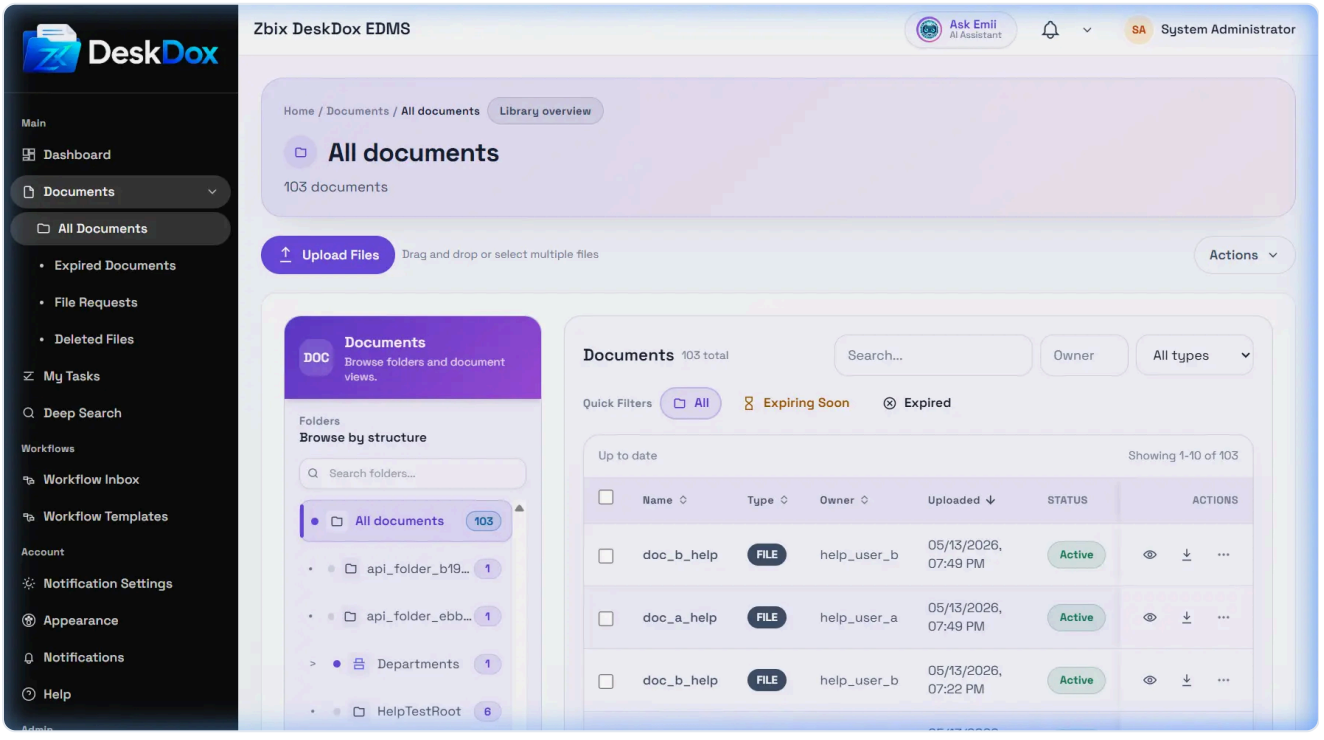
Upload, find, preview, share, and manage records across document workspaces.

Documents · 1 min read · Reviewed 2026-05-13

Documents Overview

What this helps you do

The Documents page is the main workspace for finding, opening, uploading, previewing, sharing, and managing documents that your account is allowed to see.



Folder tree and document table

The folder tree shows root folders and subfolders available to you. Selecting a folder filters the document table to that location. The table shows the documents you can access, with columns such as name, type, folder, owner, status, uploaded date, and updated date.

Visible documents are permission-driven

The Documents page does not necessarily show every document in the system. It shows documents visible through folder permission, direct document permission, ownership, sharing, workflow assignment, department membership, or administrator access. Folder permission controls access to a folder and documents inherited from it. Document permission grants access to a specific document even if broader folder access is not available.

Why users see fewer documents

If you cannot find a file, check the selected folder, search filters, status filters, expired/deleted pages, and whether the document belongs to another user or department. A document may be hidden because you do not have folder access, direct document access, workflow involvement, or ownership.

Documents · 1 min read · Reviewed 2026-05-13

Document List Actions

What this helps you do

Use the document table to inspect document status, select rows, run bulk actions, export a list, or open row-level actions.

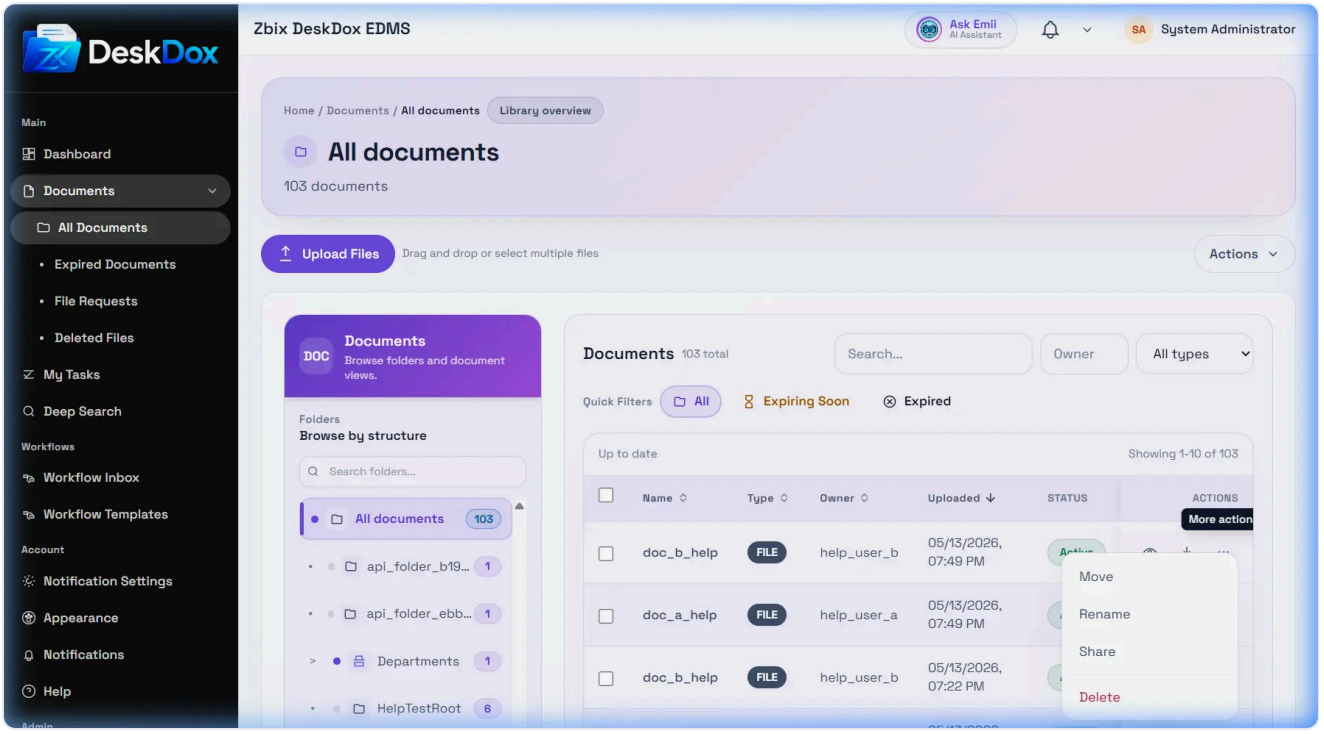


Table columns

The table can show `Name`, `Type`, `Folder`, `Owner`, `Status`, `Uploaded`, and `Updated`. Click a document name to open details. Use the row checkbox to select one document, or `Select all` to select visible rows.

Bulk and row actions

When documents are selected, the bulk toolbar can show `Apply Workflow`, `Bulk Delete`, `Bulk Move`, and `Clear selection`. Use `Export CSV` to export the visible list when available. The row action menu can include rename, move, delete, preview, share, email, workflow, and metadata actions.

Permission-based actions

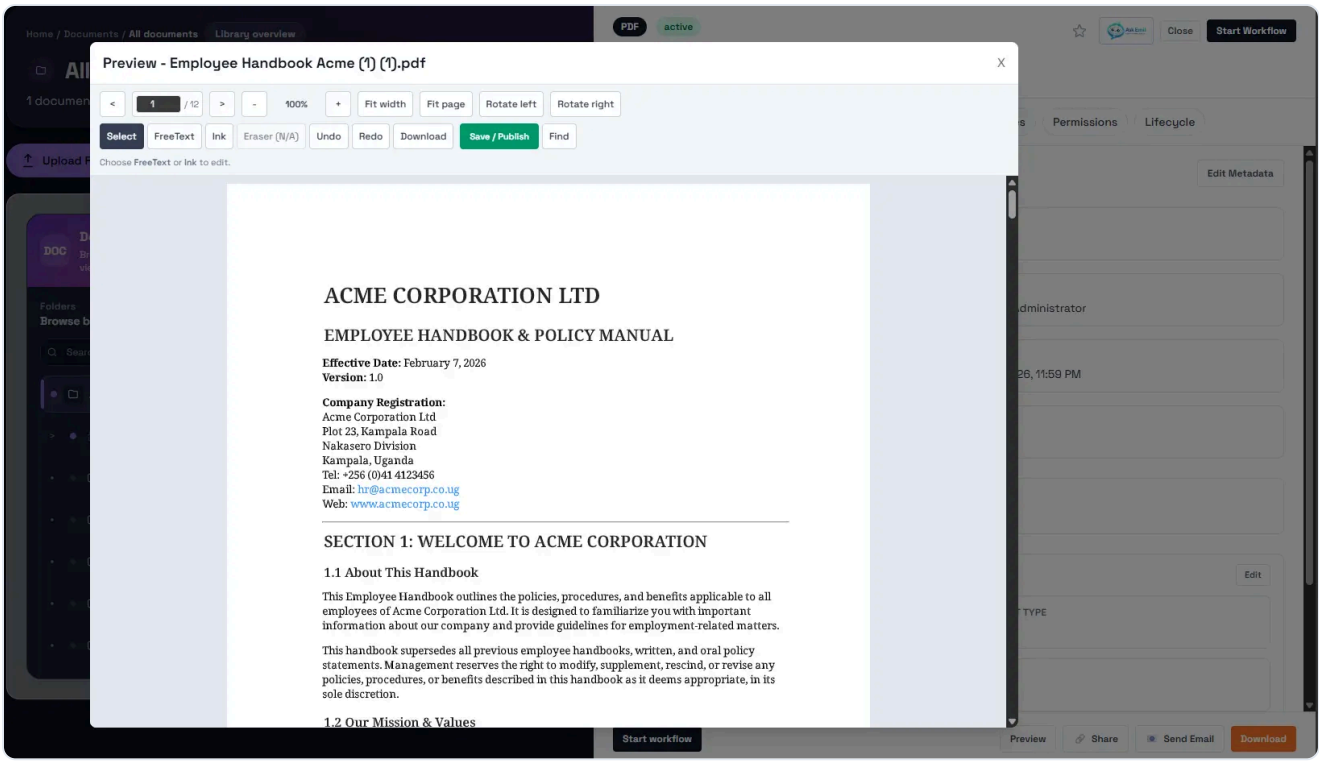
Actions are hidden or disabled when your role, folder permission, document permission, ownership, workflow state, lifecycle state, or license does not allow them. If you can view a document but cannot delete it, you likely have view access without delete permission.

Documents · 2 min read · Reviewed 2026-05-13

Preview and Review a Document

What this helps you do

Use the Preview modal to view a document in the browser before deciding whether to download the original file, start a workflow, share it, or inspect its details.



Open preview

Open the document row action menu and choose `Preview`, or open the Document Detail Drawer and click `Preview` in the footer. You need view permission for the document. Download permission is separate, so a user may be able to preview a document without being allowed to download the original file.

Supported preview behavior

PDF files open directly in the preview viewer. Office files and image files may be converted to a PDF preview depending on tenant configuration. The preview is a browser-friendly copy for review. `Download` retrieves the original file or the active document version when your permission allows it.

Missing PDF or failed preview

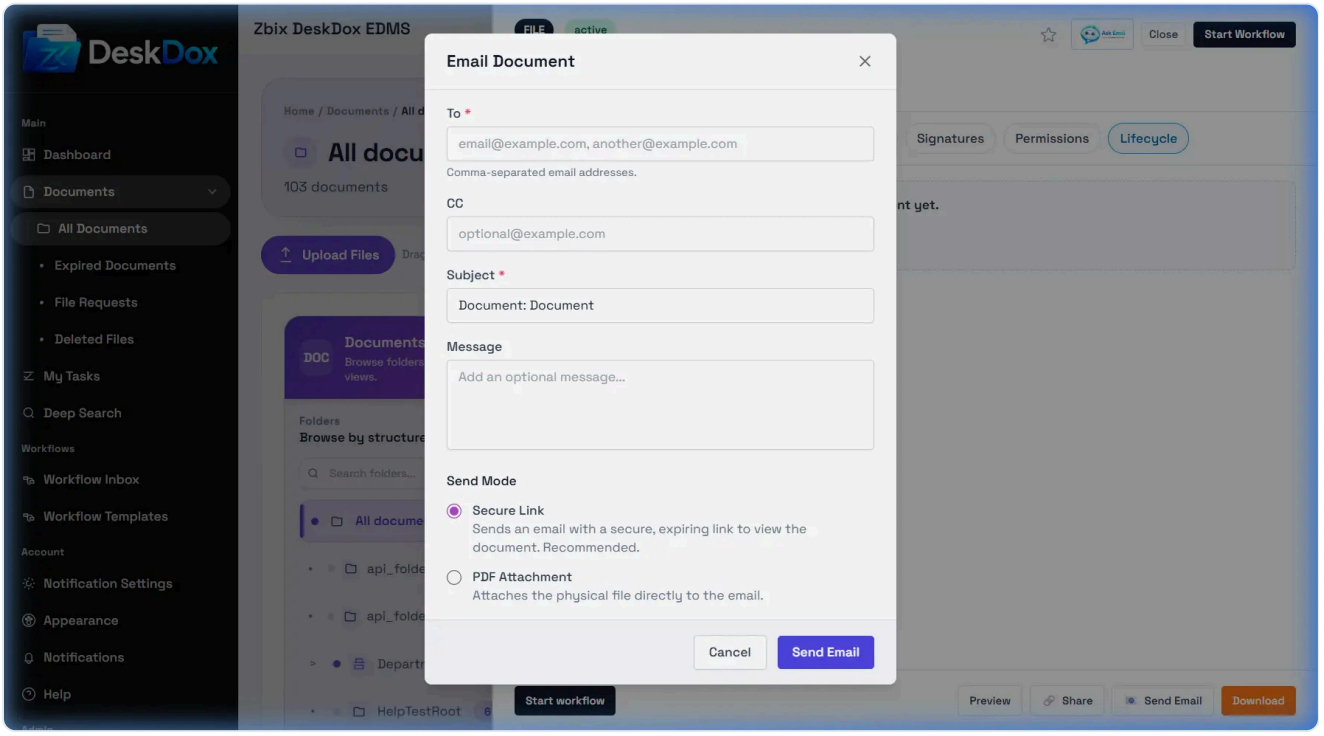
`Missing PDF` means DeskDox does not have a generated PDF preview available for that document/version. Check whether the original file exists, whether the file type is supported, whether the preview/converter worker is running, and whether preview generation has failed. If the preview keeps failing but the original downloads successfully, escalate to the administrator responsible for the converter or preview worker.

Documents · 1 min read · Reviewed 2026-05-13

Send a Document by Email

What this helps you do

Use the Email Document modal to send a document notification, secure link, or attachment behavior supported by your DeskDox configuration.



Send email

Open the document row action menu or Document Detail Drawer and choose `Email` or `Send Email`. Enter the recipient, subject, and body/message, then send. Depending on configuration, the email may include a secure/public link rather than attaching the original file.

Your DeskDox configuration determines whether document email sends a secure/public link, an attachment, or another approved delivery method. If you are unsure which mode is enabled, check with your administrator before sending sensitive documents.

Link and mail dependencies

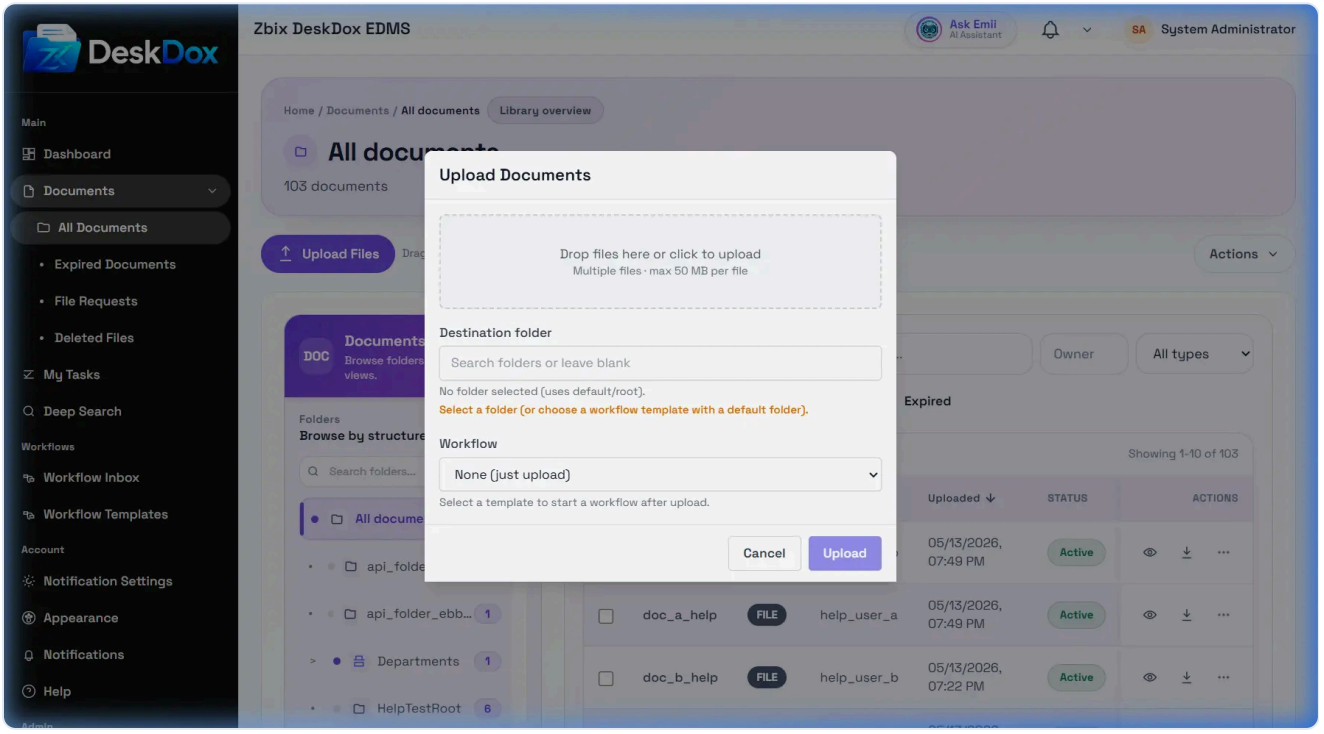
If email uses secure links, the public/secure link feature must be available and valid. If sending fails or times out, check recipient address, link status, link expiry, SMTP/mail server configuration, and whether the document is still accessible. Email send attempts and access changes can appear in audit history.

Documents · 2 min read · Reviewed 2026-05-13

Upload Documents

What this helps you do

Use the Upload Documents modal to add files to DeskDox, place them in the correct folder, complete required metadata, and start a workflow during upload when your workspace is configured for it.



Before you upload

You need access to the Documents module and upload permission on the destination folder. Folder access is usually driven by department membership, folder permissions, document ownership rules, or administrator rights. If the folder list is empty or the Upload Files button is hidden, ask an administrator to check your role, department assignment, and folder permission.

Upload steps

1. Open `Documents`.
2. Select the destination folder from the folder tree, or select it inside the upload modal if the modal asks for a folder.
3. Click `Upload Files`.
4. Drag files into the upload area or click `Choose Files`.

5. Confirm the destination folder.
6. Select a workflow if a workflow selector is shown.
7. Complete all required metadata fields, including expiry metadata when required.
8. Submit the upload.

After upload, the document appears in the document table for users who can view that folder or document. If a workflow was selected, DeskDox creates the workflow instance after the file and metadata pass validation.

Required metadata and expiry metadata

Required metadata may include document type, category, reference number, owner, department, effective date, expiry date, or workflow-specific fields. Expiry metadata is required when lifecycle or retention rules need a date to calculate expiry. The error `Required expiry metadata field is missing` means the upload is blocked until the required expiry field is filled with a valid date/value.

Troubleshooting

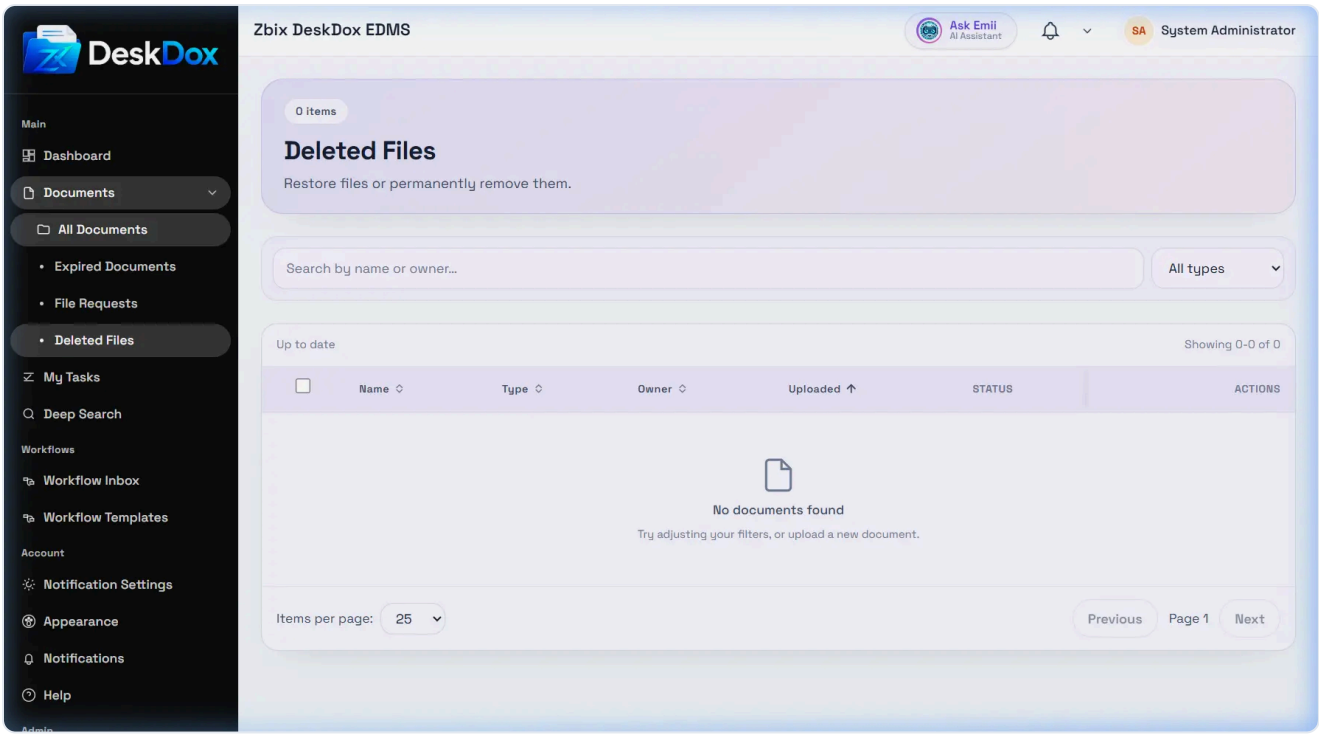
If `Upload Files` is not visible, check that your role allows upload and that you have upload access to at least one folder. If the upload fails, check file type, file size, folder selection, required metadata, workflow selection, and network connectivity. If the document uploads but is not showing, clear filters, refresh the folder, and confirm you are viewing the folder where the file was uploaded.

Documents · 1 min read · Reviewed 2026-05-13

Deleted Files

What this helps you do

Use Deleted Files to review documents that were removed from normal document lists but are still retained by DeskDox when soft delete is enabled.



Page contents

Columns can include `Name`, `Type`, `Owner`, `Uploaded`, `Status`, and `Actions`. Soft-deleted documents may be restorable. Permanently deleted documents are removed according to tenant policy and may not be recoverable from the app.

Restore and delete actions

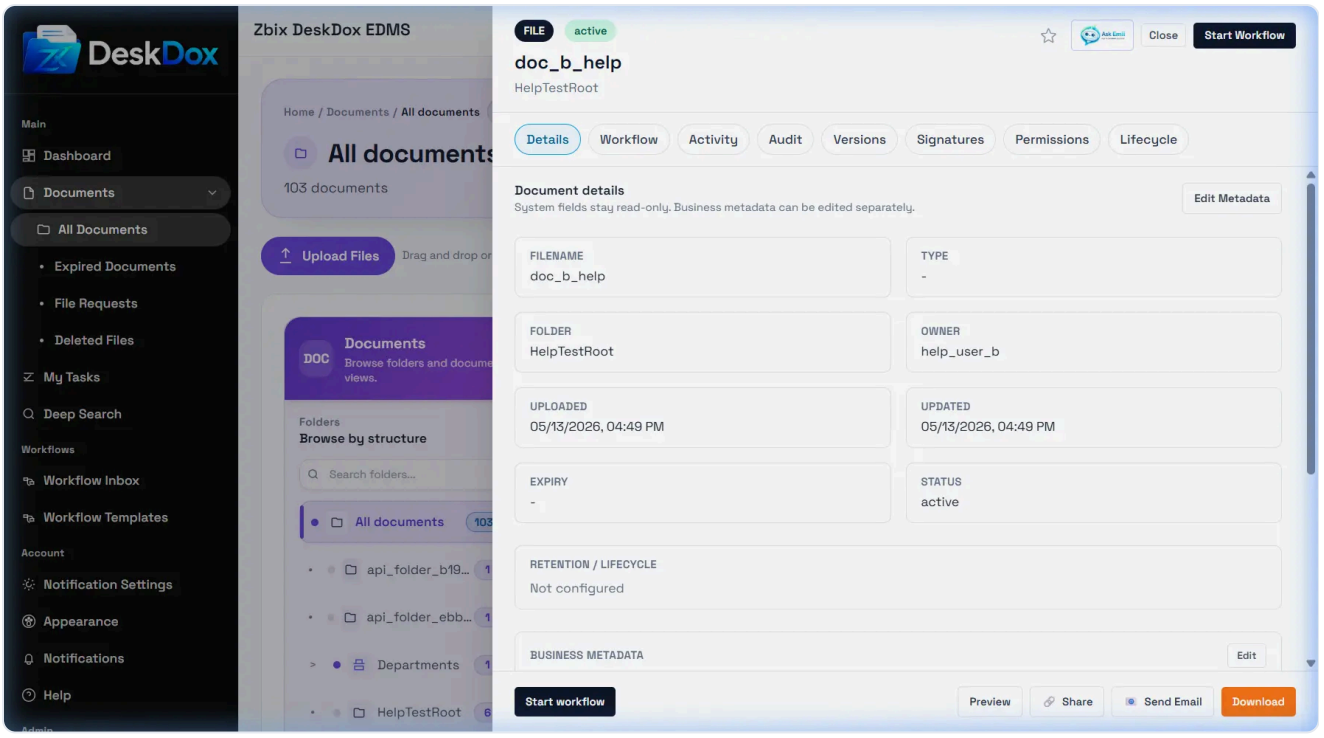
Use `Restore` when available to return a soft-deleted document to an accessible location. Permanent delete, if implemented and enabled for your role, should be used only according to retention and compliance policy. Delete and restore activity is audited.

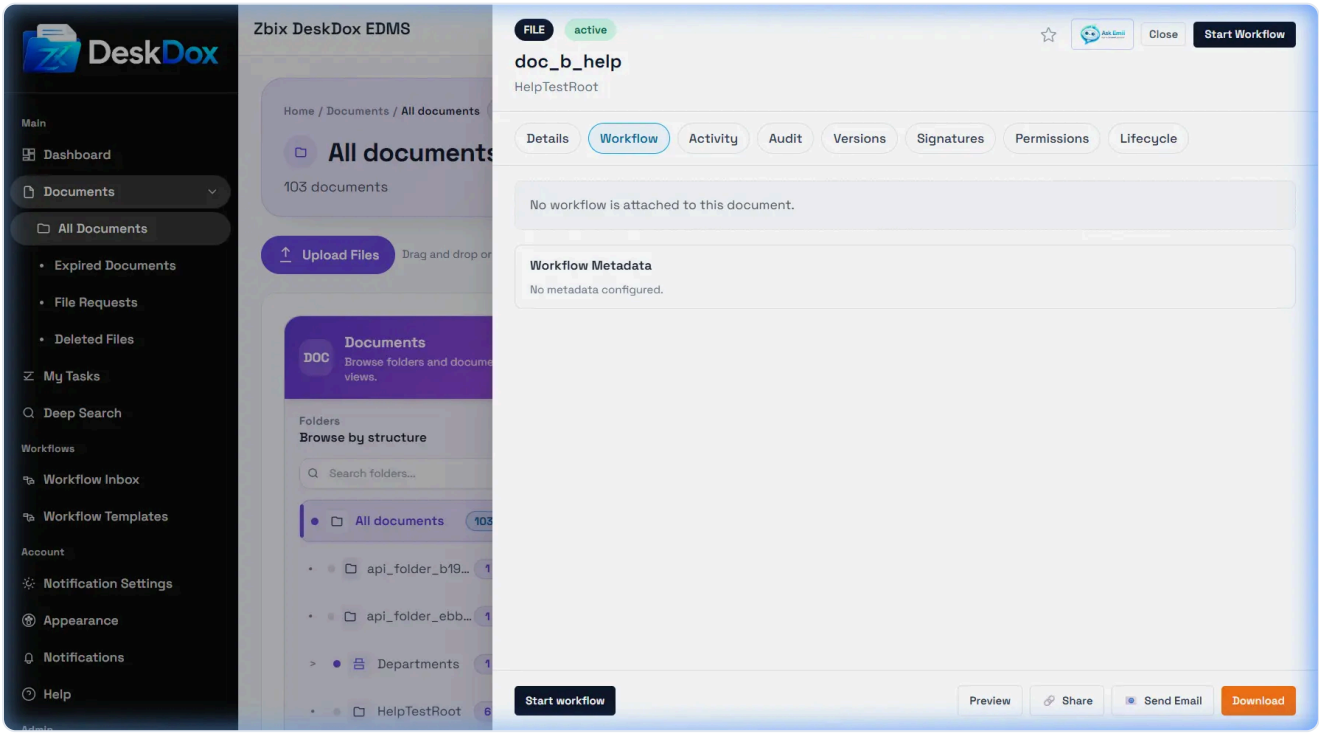
Documents · 1 min read · Reviewed 2026-05-13

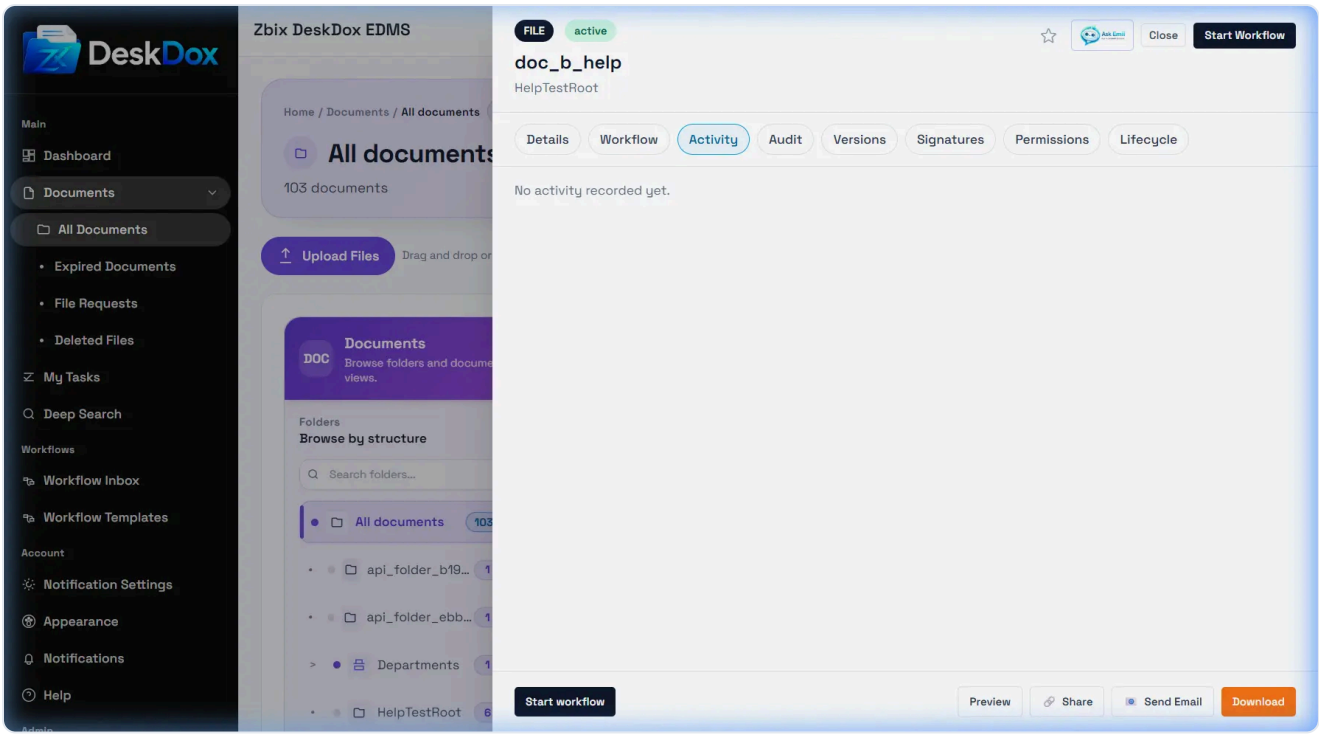
Document Detail Drawer

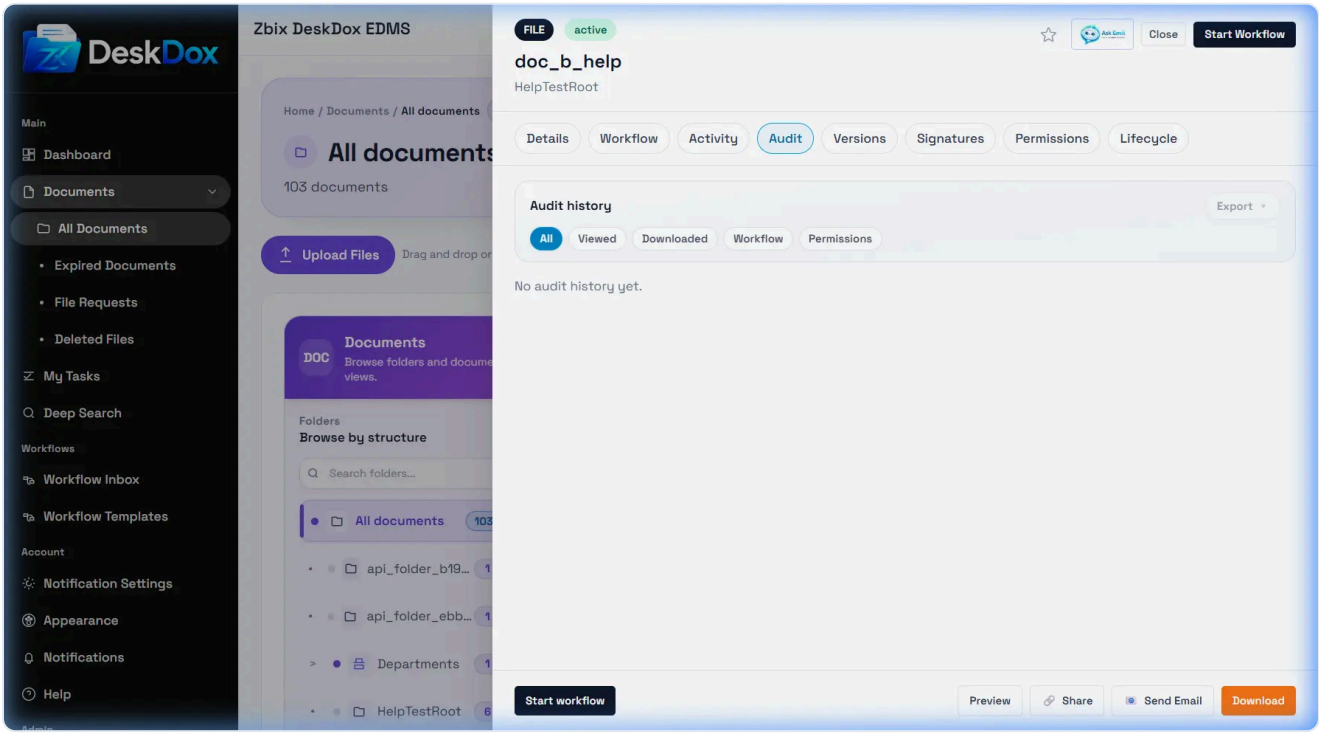
What this helps you do

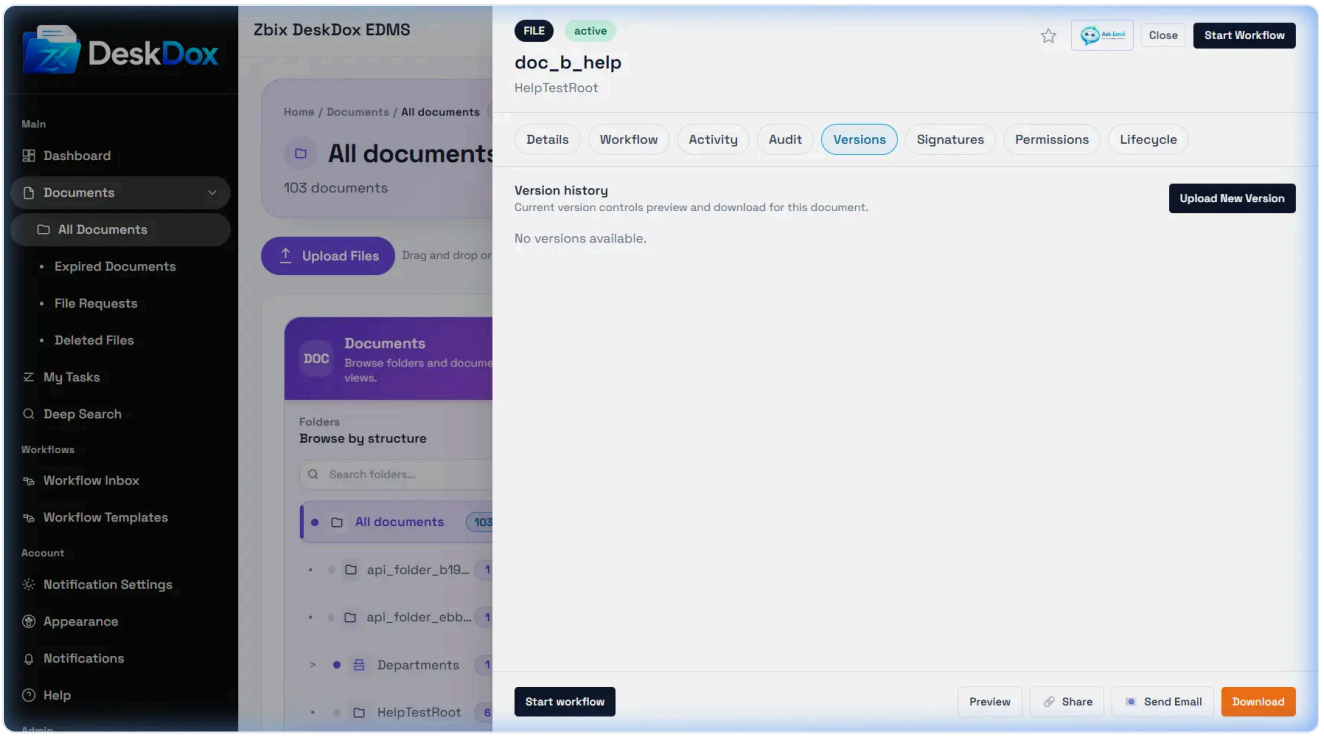
Open the Document Detail Drawer to inspect one document's metadata, workflow, activity, audit trail, versions, signatures, permissions, lifecycle status, and available actions.

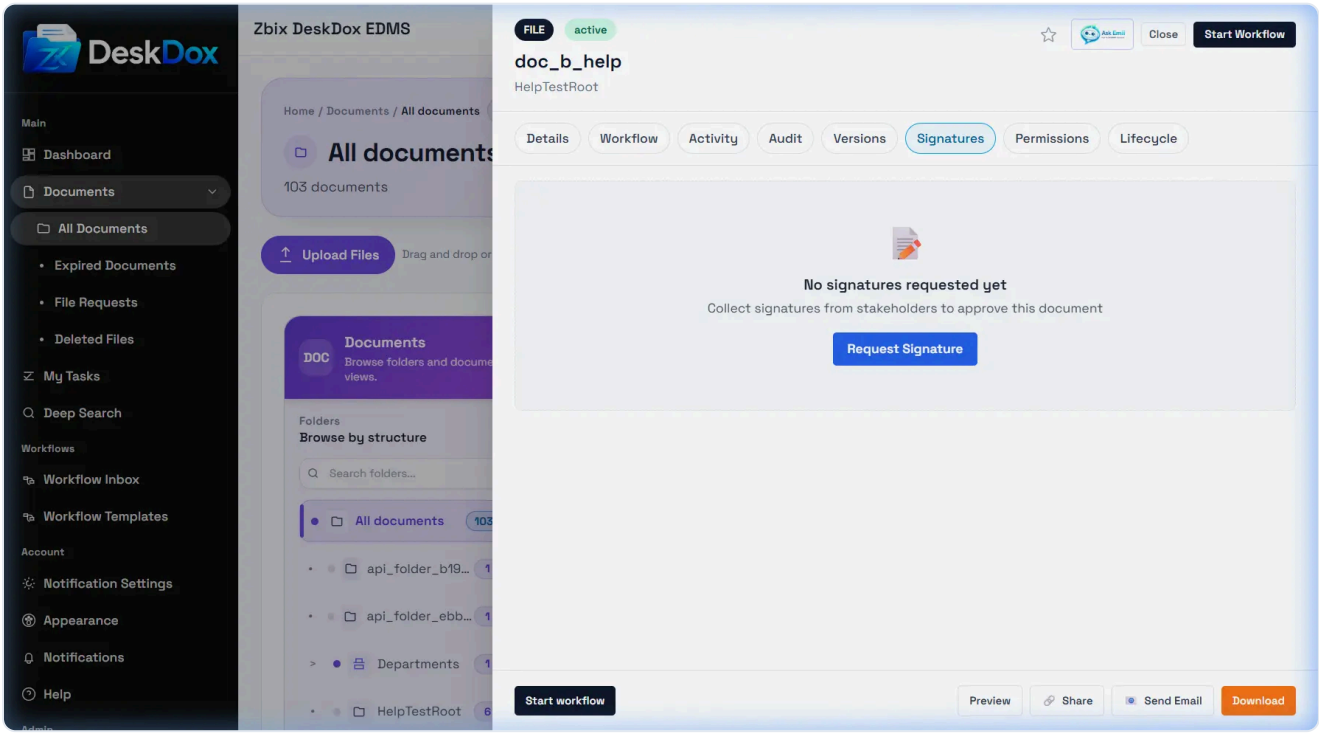

DeskDox
Zbix DeskDox EDMS
Main
Dashboard
Documents
All Documents
Expired Documents
File Requests
Deleted Files
My Tasks
Deep Search
Workflows
Workflow Inbox
Workflow Templates
Account
Notification Settings
Appearance
Notifications
Help
Home / Documents / All documents
All documents
103 documents
Upload Files
Drag and drop or
Documents
Browse folders and documents views.
Folders
Browse by structure
Search folders...
All documents
api_folder_b19...
api_folder_ebb...
Departments
HelpTestRoot
FILE
active
doc_b_help
HelpTestRoot
Close
Start Workflow
Details
Workflow
Activity
Audit
Versions
Signatures
Permissions
Lifecycle
Document details
System fields stay read-only. Business metadata can be edited separately.
Edit Metadata
FILENAME
doc_b_help
TYPE
-
FOLDER
HelpTestRoot
OWNER
help_user_b
UPLOADED
05/13/2026, 04:49 PM
UPDATED
05/13/2026, 04:49 PM
EXPIRY
-
STATUS
active
RETENTION / LIFECYCLE
Not configured
BUSINESS METADATA
Edit
Start workflow
Preview
Share
Send Email
Download

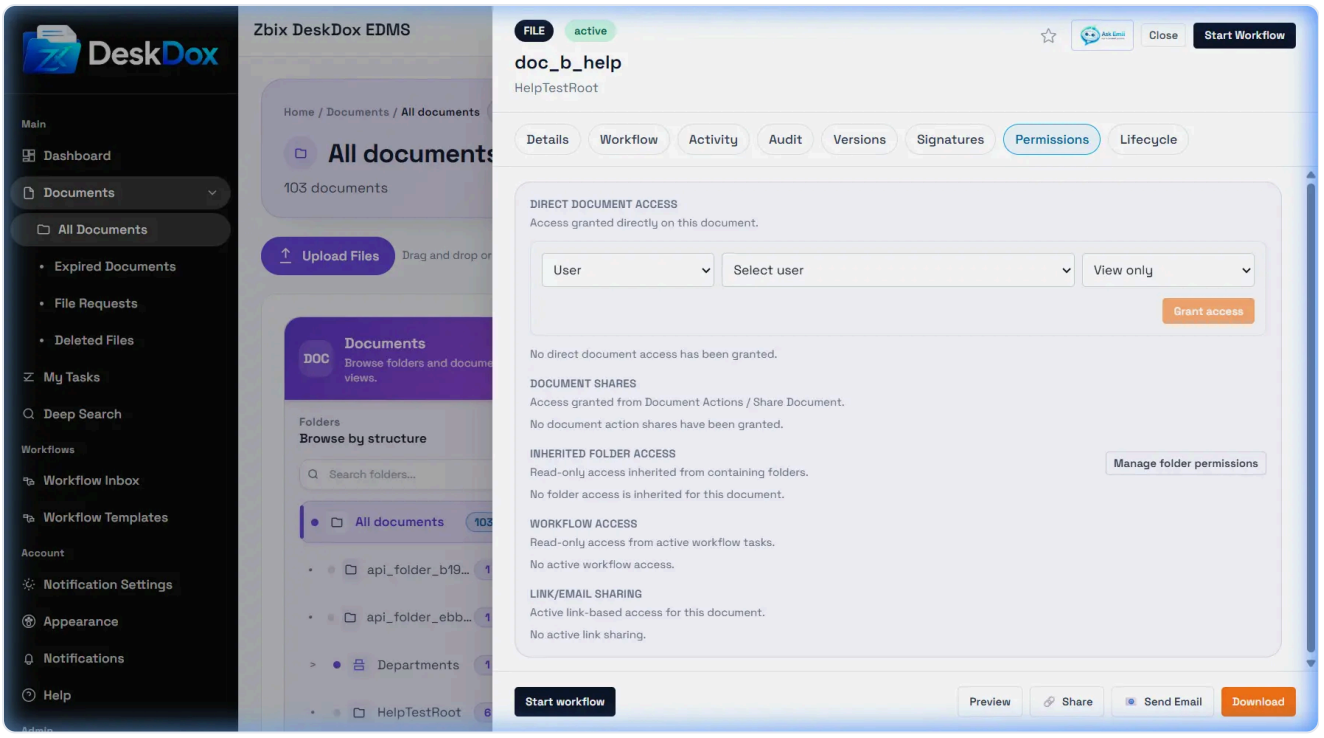

DeskDox
Zbix DeskDox EDMS
Main
Dashboard
Documents
All Documents
Expired Documents
File Requests
Deleted Files
My Tasks
Deep Search
Workflows
Workflow Inbox
Workflow Templates
Account
Notification Settings
Appearance
Notifications
Help
Home / Documents / All documents
All documents
103 documents
Upload Files
Drag and drop or
Documents
Browse folders and documents views.
Folders
Browse by structure
Search folders...
All documents
api_folder_b19...
api_folder_ebb...
Departments
HelpTestRoot
FILE
active
doc_b_help
HelpTestRoot
Close
Start Workflow
Details
Workflow
Activity
Audit
Versions
Signatures
Permissions
Lifecycle
No workflow is attached to this document.
Workflow Metadata
No metadata configured.
Start workflow
Preview
Share
Send Email
Download

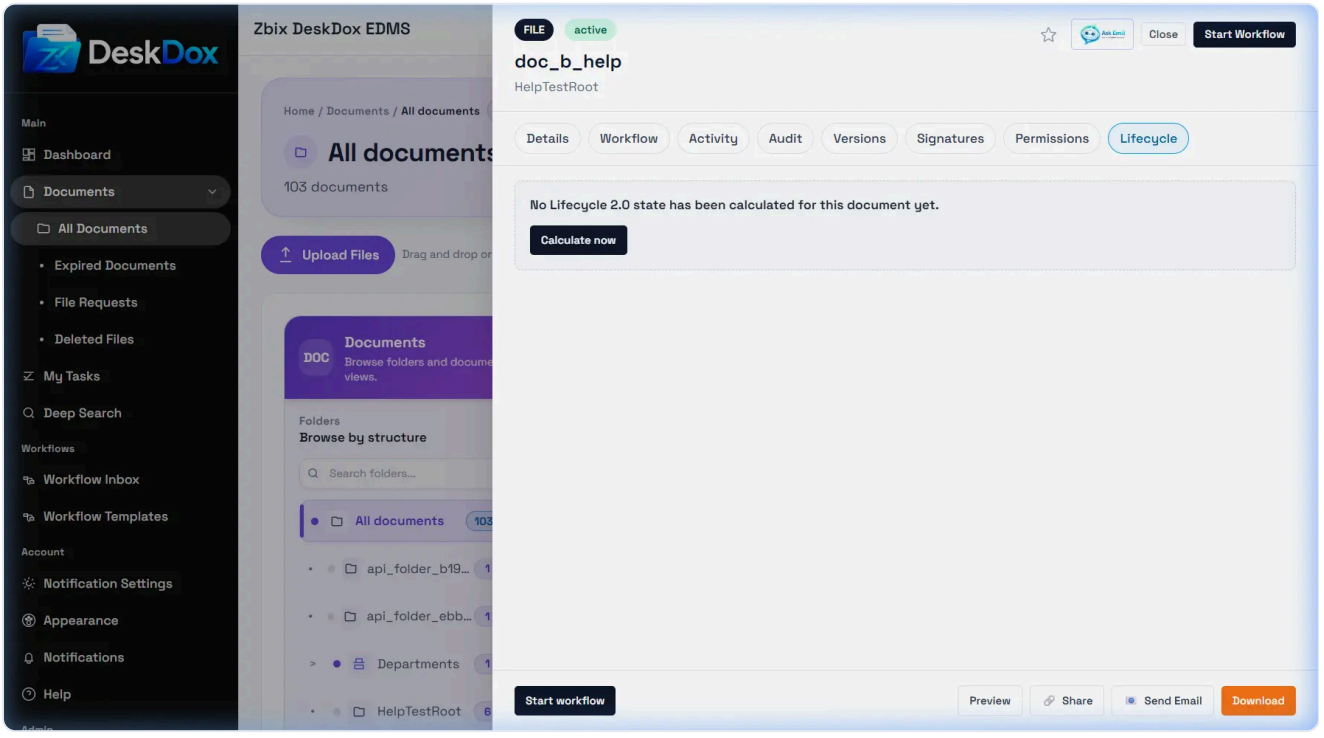

DeskDox
Zbix DeskDox EDMS
Main
Dashboard
Documents
All Documents
Expired Documents
File Requests
Deleted Files
My Tasks
Deep Search
Workflows
Workflow Inbox
Workflow Templates
Account
Notification Settings
Appearance
Notifications
Help
Home / Documents / All documents
All documents
103 documents
Upload Files
Drag and drop or
Documents
Browse folders and docume
views.
Folders
Browse by structure
Search folders...
All documents
api_folder_b19...
api_folder_ebb...
Departments
HelpTestRoot
FILE
active
doc_b_help
HelpTestRoot
Close
Start Workflow
Details
Workflow
Activity
Audit
Versions
Signatures
Permissions
Lifecycle
No activity recorded yet.
Start workflow
Preview
Share
Send Email
Download


DeskDox
Zbix DeskDox EDMS
Main
Dashboard
Documents
All Documents
Expired Documents
File Requests
Deleted Files
My Tasks
Deep Search
Workflows
Workflow Inbox
Workflow Templates
Account
Notification Settings
Appearance
Notifications
Help
Home / Documents / All documents
All documents
103 documents
Upload Files
Drag and drop or
Documents
Browse folders and docume
views.
Folders
Browse by structure
Search folders...
All documents
api_folder_b19...
api_folder_ebb...
Departments
HelpTestRoot
FILE
active
doc_b_help
HelpTestRoot
Close
Start Workflow
Details
Workflow
Activity
Audit
Versions
Signatures
Permissions
Lifecycle
Audit history
Export
All
Viewed
Downloaded
Workflow
Permissions
No audit history yet.
Start workflow
Preview
Share
Send Email
Download


DeskDox
Zbix DeskDox EDMS
Main
Dashboard
Documents
All Documents
Expired Documents
File Requests
Deleted Files
My Tasks
Deep Search
Workflows
Workflow Inbox
Workflow Templates
Account
Notification Settings
Appearance
Notifications
Help
Home / Documents / All documents
All documents
103 documents
Upload Files
Drag and drop or
Documents
Browse folders and documents views.
Folders
Browse by structure
Search folders...
All documents
api_folder_b19...
api_folder_ebb...
Departments
HelpTestRoot
FILE
active
doc_b_help
HelpTestRoot
Close
Start Workflow
Details
Workflow
Activity
Audit
Versions
Signatures
Permissions
Lifecycle
Version history
Current version controls preview and download for this document.
Upload New Version
No versions available.
Start workflow
Preview
Share
Send Email
Download


DeskDox
Zbix DeskDox EDMS
Main
Dashboard
Documents
All Documents
Expired Documents
File Requests
Deleted Files
My Tasks
Deep Search
Workflows
Workflow Inbox
Workflow Templates
Account
Notification Settings
Appearance
Notifications
Help
Home / Documents / All documents
All documents
103 documents
Upload Files
Drag and drop or
Documents
Browse folders and documents views.
Folders
Browse by structure
Search folders...
All documents
api_folder_b19...
api_folder_ebb...
Departments
HelpTestRoot
FILE
active
doc_b_help
HelpTestRoot
Close
Start Workflow
Details
Workflow
Activity
Audit
Versions
Signatures
Permissions
Lifecycle
No signatures requested yet
Collect signatures from stakeholders to approve this document
Request Signature
Start workflow
Preview
Share
Send Email
Download





Open the drawer

Click a document name in the table. The header shows document identity and badges such as status, workflow, lifecycle, or favorite/star when available. Use `Ask Emii` to ask about the selected document when Emii is enabled and your access permits it.

Tabs and footer actions

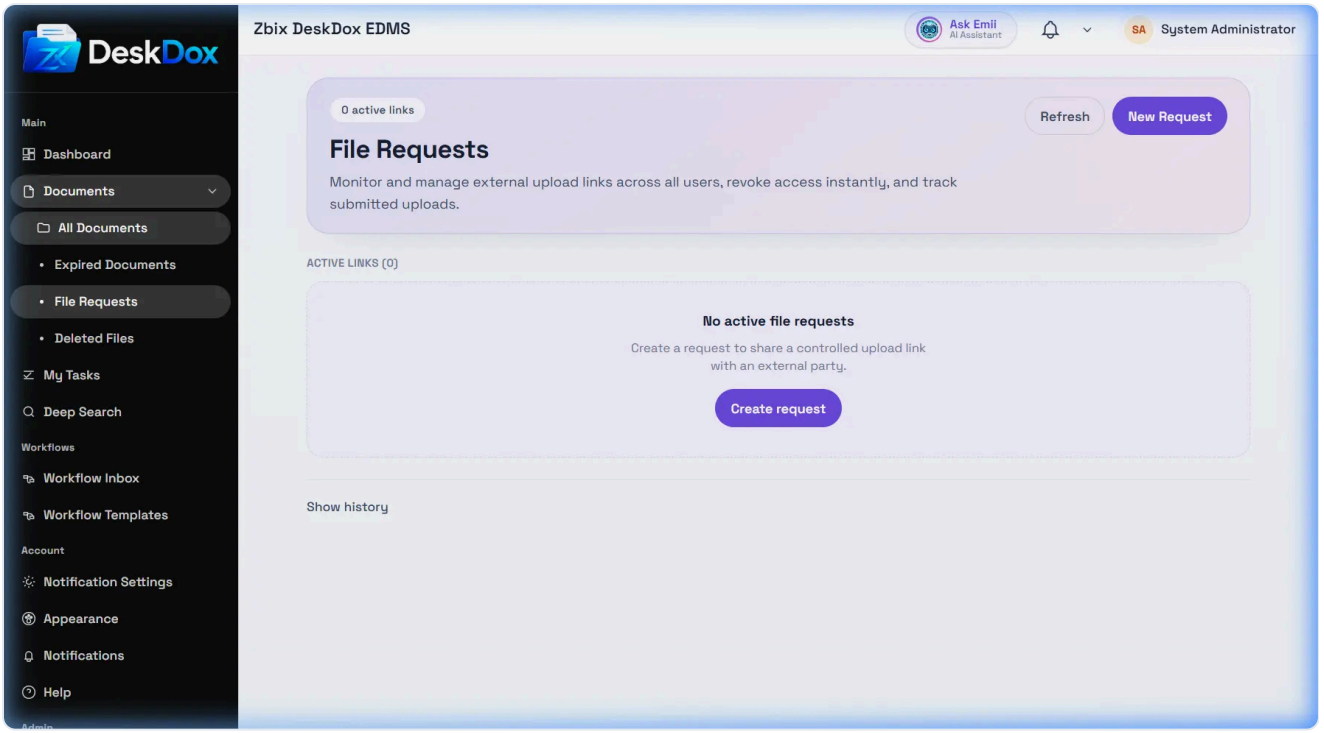
Tabs can include `Details`, `Workflow`, `Activity`, `Audit`, `Versions`, `Signatures`, `Permissions`, and `Lifecycle`. The footer can include `Start Workflow`, `Preview`, `Share`, `Email`, `Copy Link`, and `More actions`. Tabs and actions are permission-dependent, so a user may see details but not permissions, audit, lifecycle, email, share, or workflow controls.

Documents · 1 min read · Reviewed 2026-05-13

File Requests

What this helps you do

Use File Requests to collect documents from people outside your organization or from users who need a guided upload link.



Create and send a request

Open `Documents > File Requests`, click `Create Request`, enter the request details, and generate the request link. Send the link to the requester or external user using your approved communication channel.

Upload and tracking flow

The recipient opens the request link and uploads the requested files. Track submissions from the File Requests page and open request details or uploads when available. If expected files are missing, check whether the link expired, was revoked, was copied correctly, or failed during upload.

Security notes

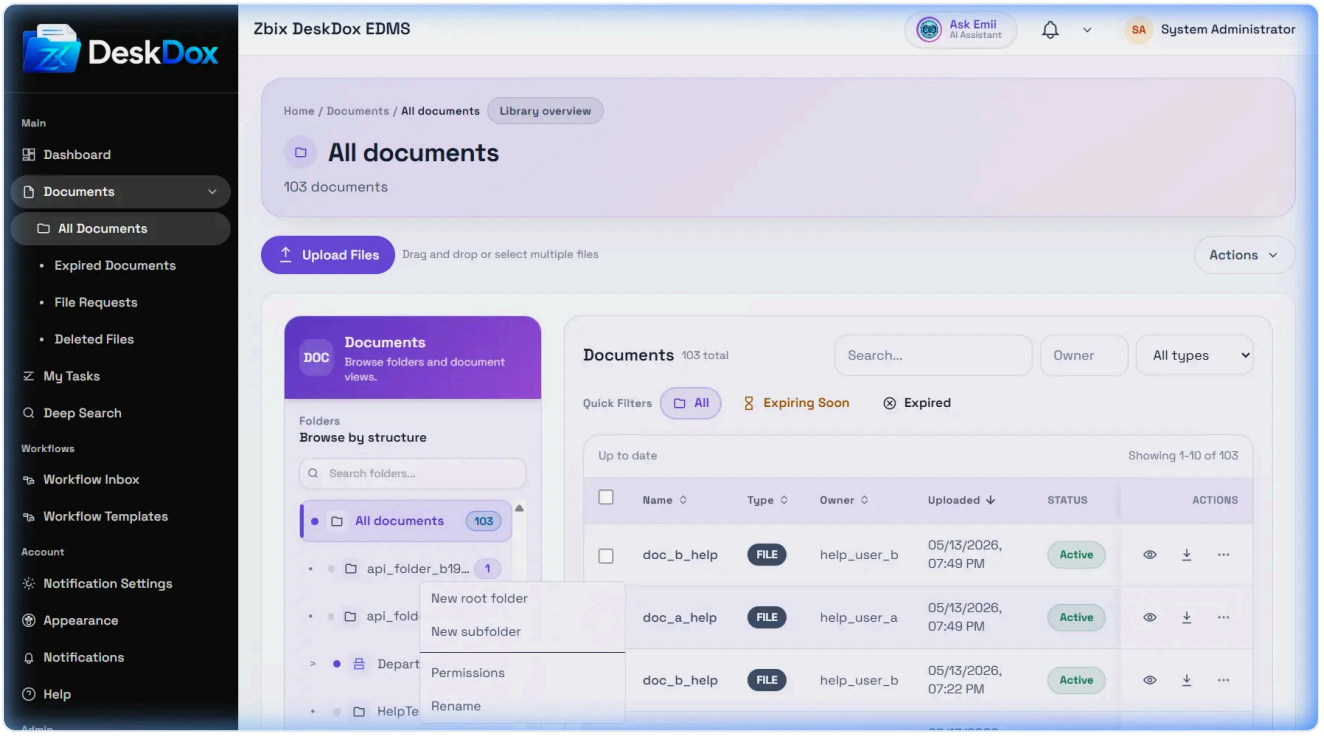
Use file requests for controlled external collection. Set expiry and destination folder carefully, and revoke links when collection is complete or the wrong recipient received the link.

Documents · 2 min read · Reviewed 2026-05-13

Folder Navigation and Actions

What this helps you do

Use the folder tree to move between root folders, department folders, and subfolders, and to create or manage folders when your permissions allow it.



Navigate folders

Root folders appear at the top of the tree. Expand a folder to reveal subfolders, then select a folder to show its documents in the table. A department folder may be visible only to users in that department or users granted folder access.

Folder actions

Use the folder context menu for the available folder actions: `New root folder`, `New subfolder`, `Permissions`, and `Rename`. Folder ownership and folder permission rules determine which actions appear. If an action is hidden, your role or folder-level access probably does not allow it.

Delete folder visibility

A Delete folder action may be hidden depending on the current license state. If your deployment exposes a Delete folder action, it may depend on license status, permissions, folder protection, and whether the folder is empty. Confirm with your administrator before deleting folders.

Missing folders

If a folder is not showing, clear folder search, refresh the page, and confirm you are in the correct department. Then ask an administrator to check folder ownership, department membership, inherited permissions, and whether the folder was renamed, moved, or deleted.

CHAPTER 4

Metadata and Versions

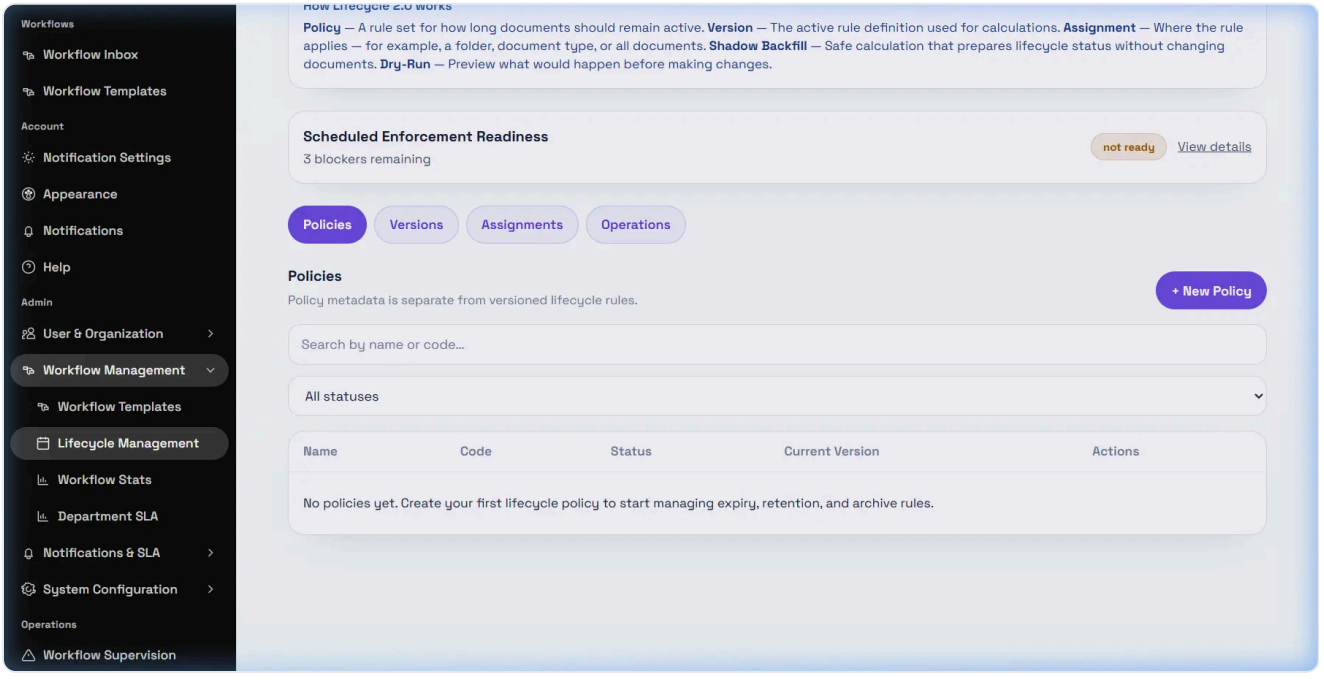
Metadata, versions, lifecycle policies, retention actions, and document governance.

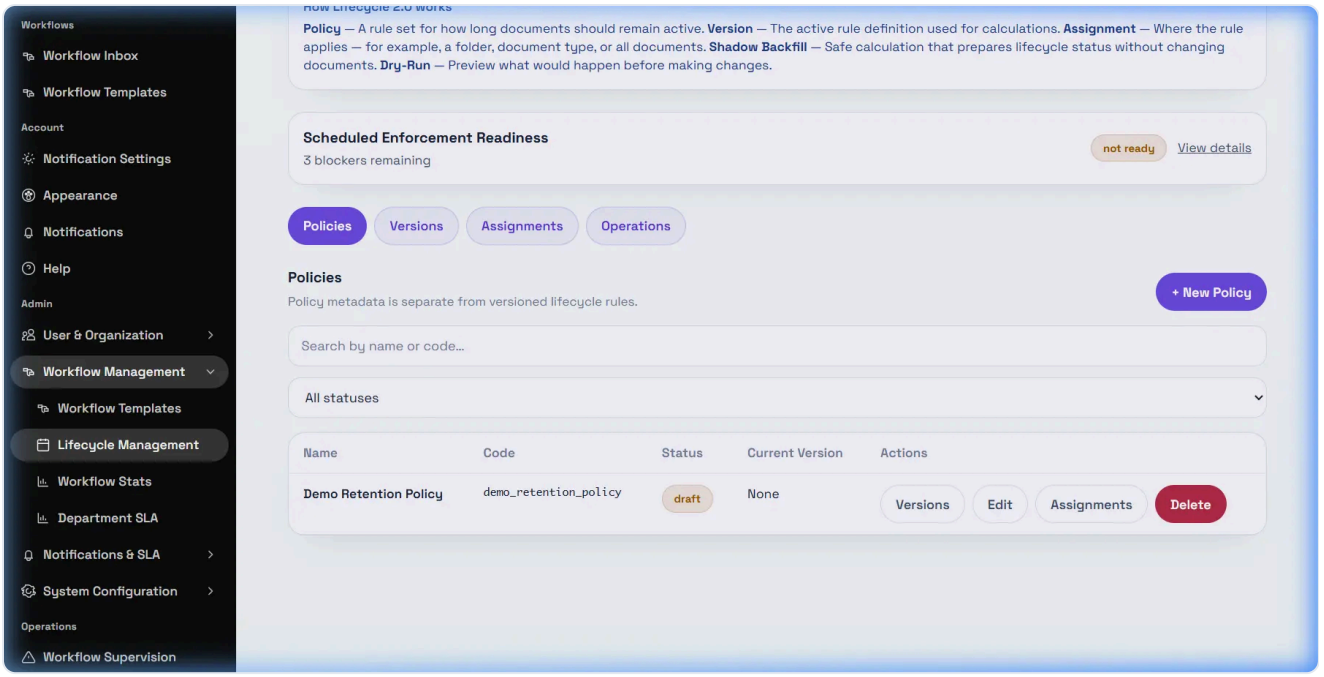
Metadata and Versions · 2 min read · Reviewed 2026-05-14

Lifecycle Management Overview

What this helps you do

Understand what Lifecycle Management does, how policies, versions, assignments, rules, and actions fit together, and where document users see lifecycle results.





Lifecycle Management is the admin area for document retention and expiry automation. A lifecycle policy is a container. A policy version holds the date source, rule settings, and on-expiry action. An assignment decides which documents the active version applies to. Enforcement is the step that applies an eligible action to matching documents.

Lifecycle is connected to Documents because recalculated lifecycle state can appear on a document, and configured actions can mark a document expired, archive its status, or move it to a target folder. Lifecycle is connected to Expired Documents because documents marked expired can appear there depending on permissions and filters.

Workflow-related behavior is available only as workflow template assignment scope and workflow metadata/date source support. Browser discovery also confirmed workflow-related metadata/date fields. Do not treat this as a true workflow approval, rejection, or completion event trigger unless your technical admin confirms a separate event integration.

Lifecycle Management is admin-only. Standard users may see lifecycle status on the Document Detail Drawer or Expired Documents when those screens and permissions are available.

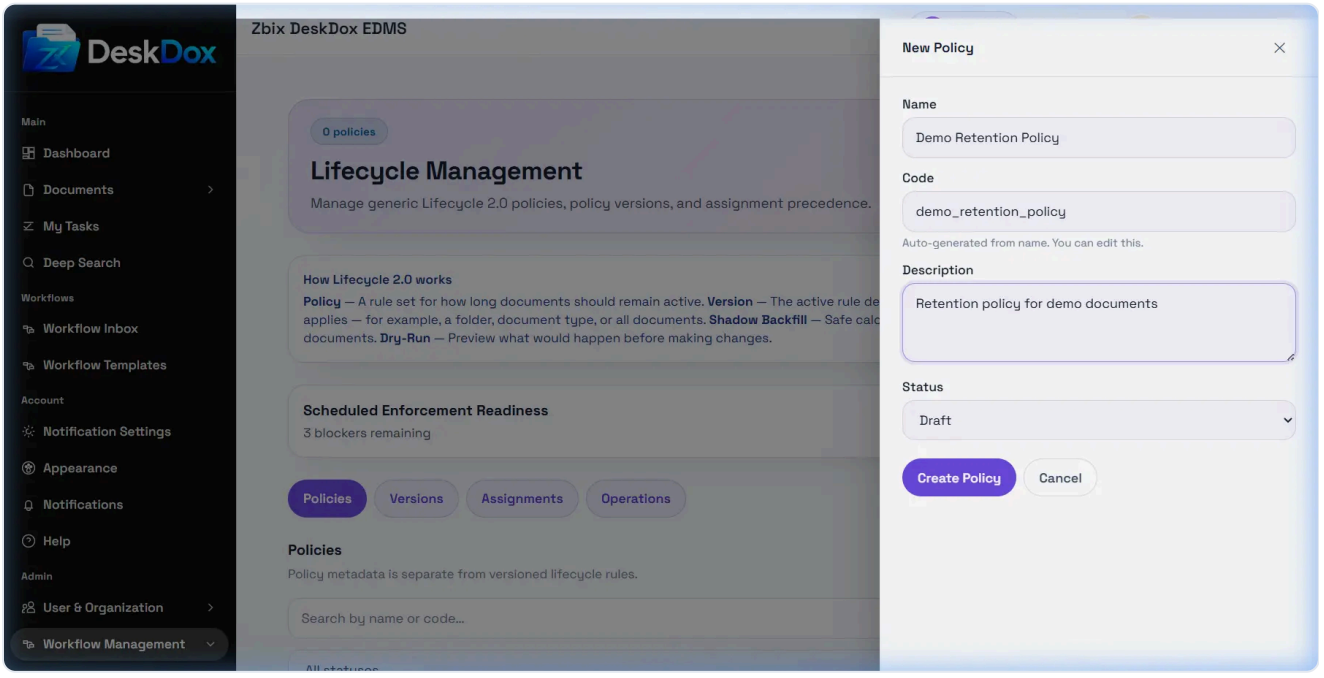
Safety note: Lifecycle does not delete documents. Supported Lifecycle 2.0 actions are none, mark_expired, move_to_folder, and archive. Archive is status-only; it does not delete storage or change permissions.

Metadata and Versions · 1 min read · Reviewed 2026-05-14

Create or Edit Lifecycle Policy

What this helps you do

Create or edit the basic lifecycle policy record before adding versions, rules, actions, and assignments.



Use + New Policy from the Policies tab when visible. The user list includes Basic Info fields for Name, Description, and Status. DeskDox also keeps a unique policy code, which the UI may auto-generate from the name.

Name is the field users and admins use to recognize the policy. Description should explain the business rule, such as finance retention or contract expiry. Status controls whether the policy is usable in the admin workflow, depending on configuration.

Validation errors can occur when required fields are missing or the policy code is already used. If Save fails, review the visible field errors, use a unique policy name/code, and confirm you have admin permission. Cancel closes the edit flow without applying unsaved changes.

Safe editing practice: avoid changing active governance policy details casually. For rule changes, create a draft version and activate it after review instead of trying to treat the policy name as the rule itself.

Metadata and Versions · 2 min read · Reviewed 2026-05-13

Edit Document Metadata

What this helps you do

Update the business fields that describe a document, such as category, reference number, expiry date, department, or workflow-related values.

System metadata and business metadata

System metadata is maintained by DeskDox and includes fields such as owner, uploaded date, updated date, status, folder, version, and audit timestamps. Business metadata is entered or edited by users and is used for search, workflow decisions, lifecycle policies, reporting, and compliance.

Edit metadata

Open the document, then use `Edit Metadata` or `Business Metadata Edit` if the action is visible. Update the fields that need correction and save the changes. Required fields must be completed before the update can be accepted; optional fields can be left blank unless your process requires them.

Where enabled, Emii can assist with metadata suggestions by reading the document content and proposing relevant values. Suggestions should be reviewed by the user before saving.

Validation and audit impact

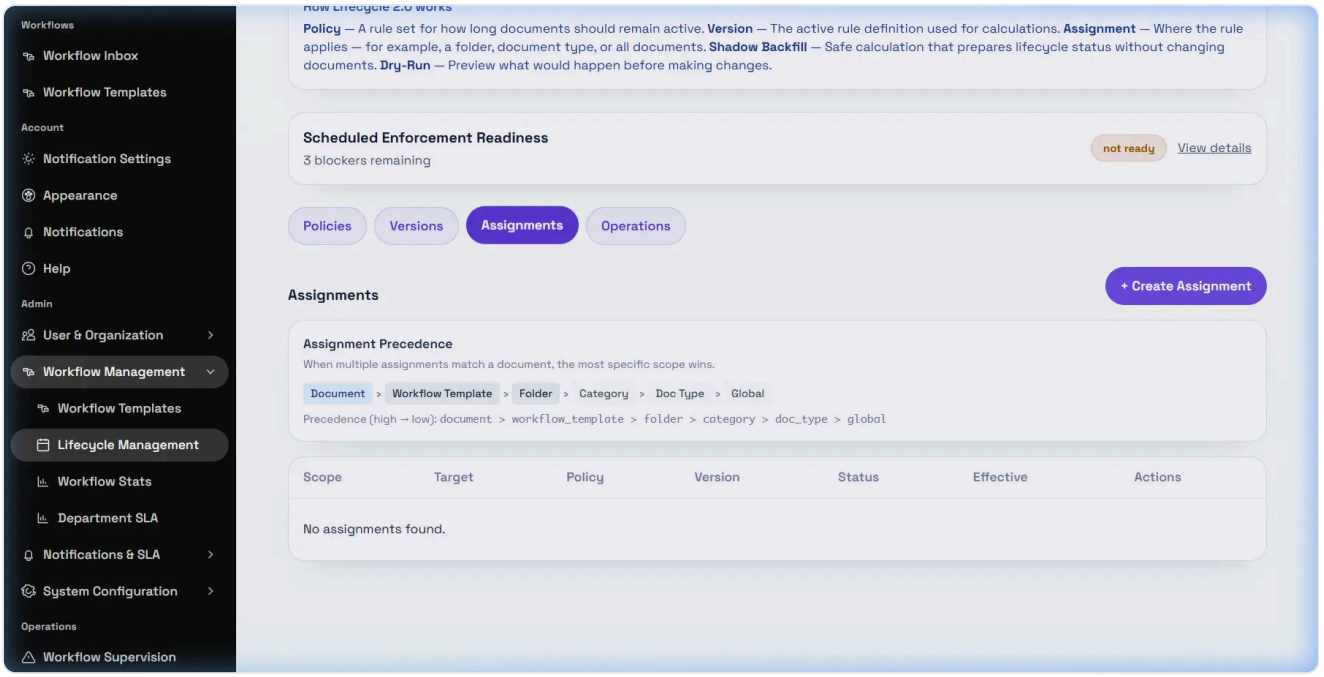
Metadata validation errors mean a required value is missing, has the wrong type, or does not match the expected format. Expiry metadata must be a valid date/value when lifecycle rules depend on it. After a successful save or update, the document details reflect the revised metadata. Metadata changes can affect workflow routing, lifecycle calculations, search results, and audit history. DeskDox records metadata edits for compliance.

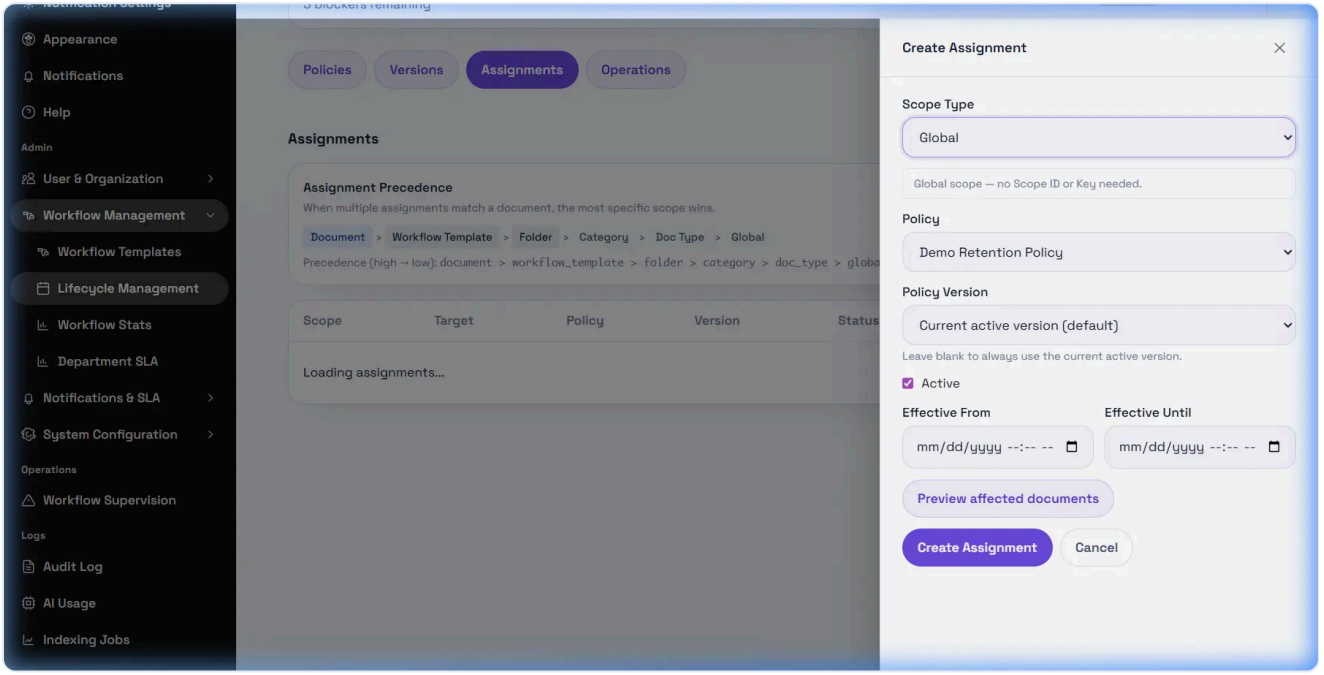
Metadata and Versions · 1 min read · Reviewed 2026-05-14

Lifecycle Assignments

What this helps you do

Assign lifecycle policies to the documents or scopes they should manage.





Assignments tell lifecycle where a policy applies. Supported scopes include global, folder, category, document type, workflow template, and individual document targets.

Global applies as a broad default. Folder applies to documents in a folder. Category and document type apply by document fields. Workflow template applies to documents with a workflow instance for that template. Document scope applies to a single document and is useful for exceptions.

Active assignments can be removed or deactivated when permissions allow. A removed/inactive assignment stops being selected for future resolution, but existing document lifecycle state may need recalculation or shadow backfill.

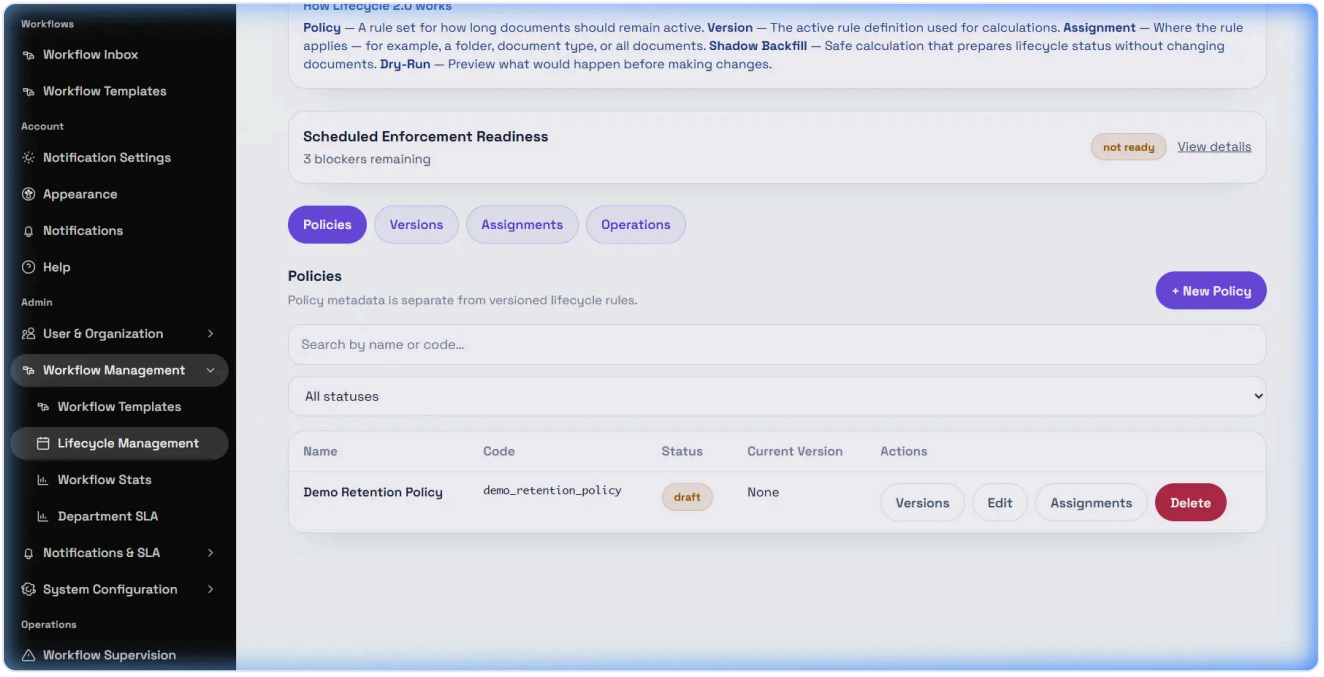
Supported precedence is document, workflow template, folder, category, doc type, then global. If an assignment does not apply, check active status, effective dates, selected target, active policy version, document fields, workflow instance, and resolver trace.

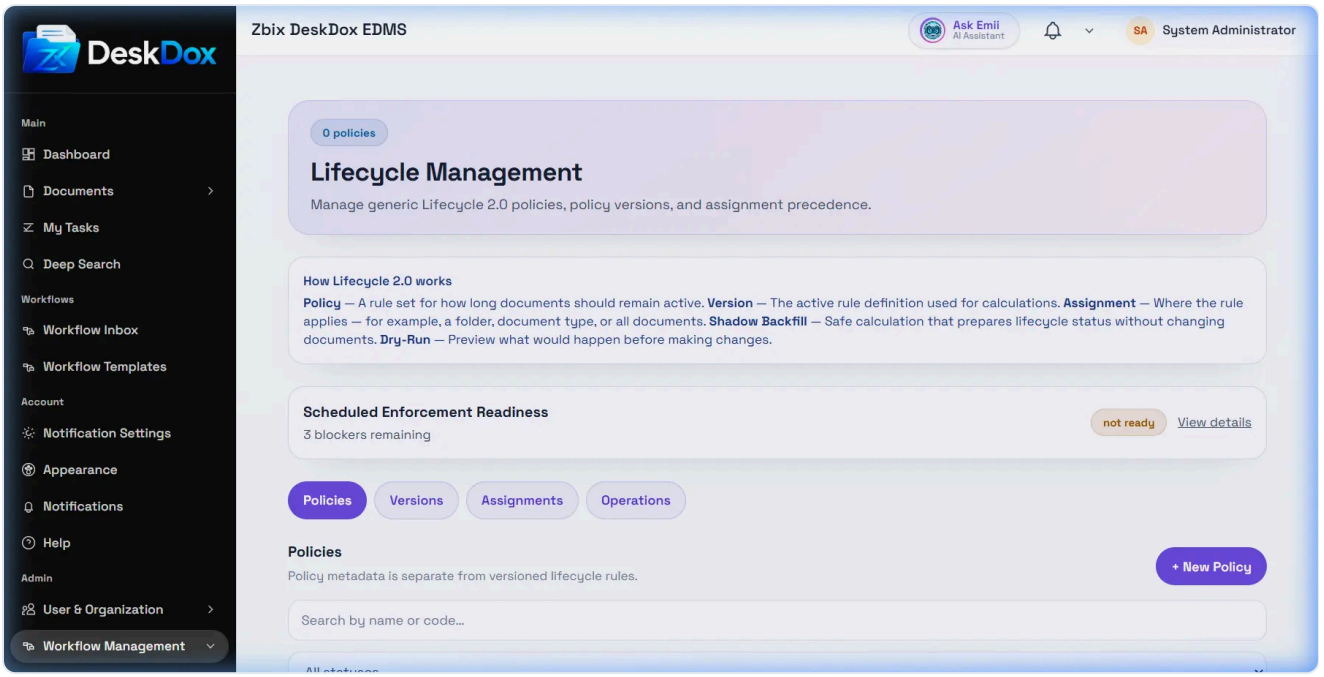
Metadata and Versions · 1 min read · Reviewed 2026-05-14

Lifecycle Policies List

What this helps you do

Find lifecycle policies, filter the list, understand status labels, and use row actions when your permissions allow them.





Open Admin > Lifecycle Management to view the Policies tab. The user list includes the list shows lifecycle policies and row actions such as Edit, Versions, and Assignments when available.

Use search to filter by policy name or code. Use the status filter to isolate Draft, Active, or Inactive policies when the filter is visible. If a policy seems missing, clear search text, reset the status filter, refresh, and confirm you are in the correct tenant or environment.

Policies can be active or inactive depending on configuration. A policy still needs an active version and an active assignment before it can match documents. The empty state appears when no policies are available or when filters leave no matching results.

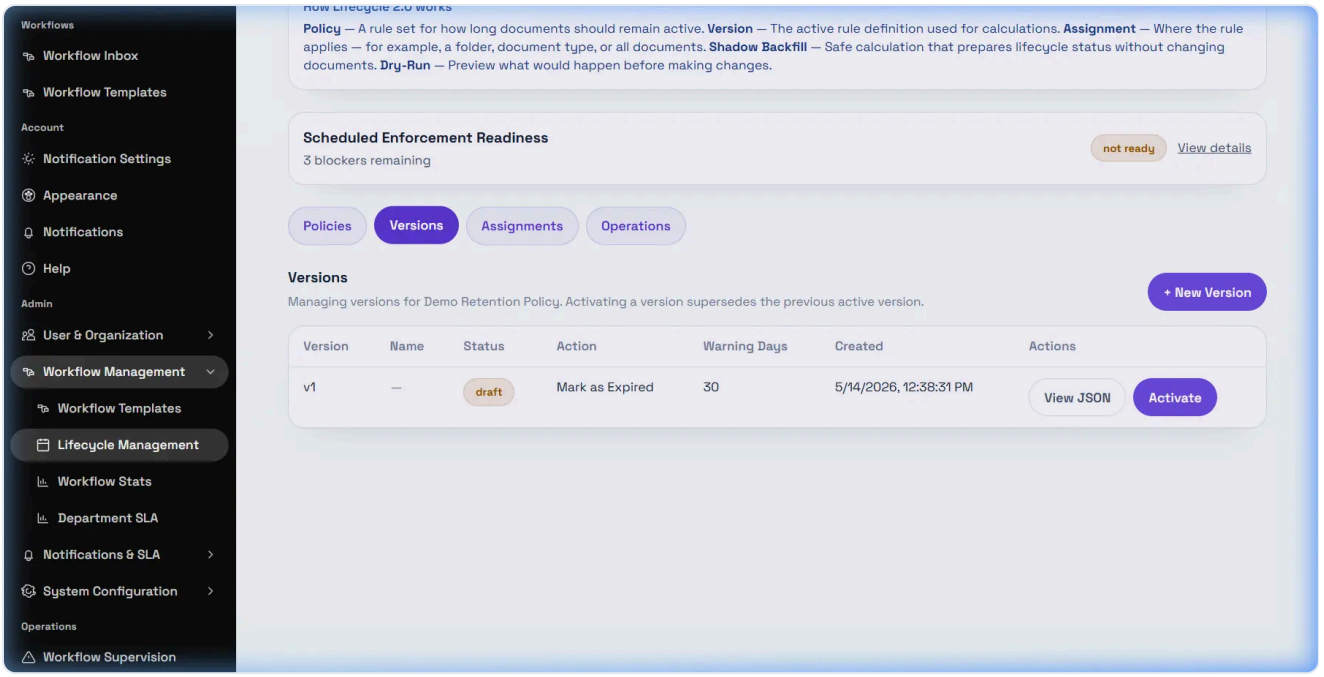
Policy list visibility is permission-dependent. If Lifecycle Management is not in the sidebar or row actions are missing, your account may not have lifecycle administration access.

Metadata and Versions · 1 min read · Reviewed 2026-05-14

Lifecycle Policy Versions

What this helps you do

Understand draft, active, and superseded lifecycle versions and what activation changes.



A policy version contains the actual lifecycle rule: date source, date field, warning/retention timing, and on-expiry action. The user list includes Draft, Active, and Superseded version states.

Draft versions let admins prepare rule changes without changing document management. Active is the version used for matching and enforcement. Superseded means the version used to be active but was replaced.

Each policy has one active version. Activating a new version sets it as the current version and supersedes the previous active version for that policy. Existing document lifecycle state may need recalculation or backfill before every affected document reflects the new active version.

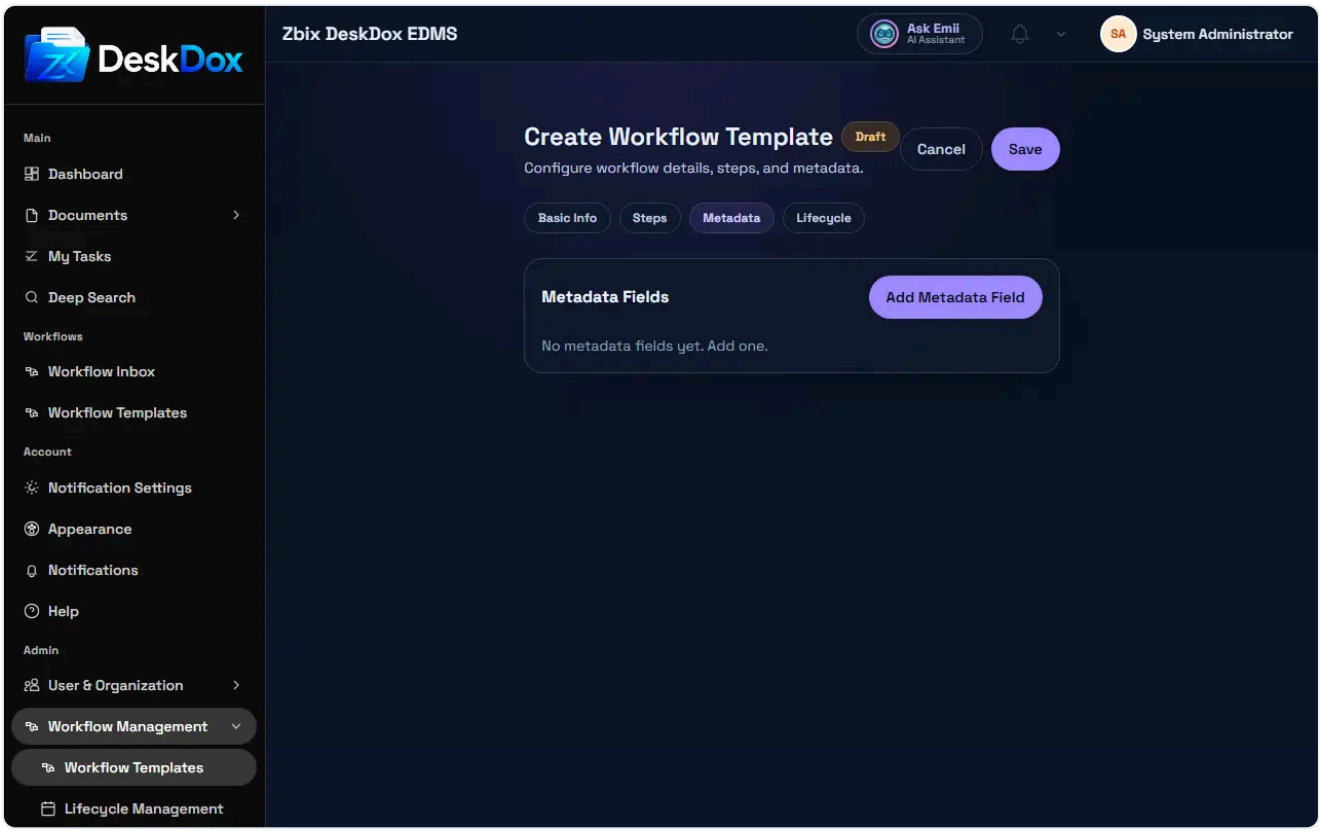
Safe versioning practice: create a draft, review date source and action settings, run dry-run after assignment, then activate only after the business owner approves the change.

Metadata and Versions · 2 min read · Reviewed 2026-05-14

Workflow Template Metadata

What this helps you do

Configure the fields a workflow template needs for validation, routing, and downstream document handling.



Metadata fields

The `Metadata` tab contains `Metadata Fields` and `Add Metadata Field`. Each field can include `Field Key`, `Label`, `Field Type`, `Required`, `Options (comma separated for select)`, `Default Value`, and `Help Text`.

Field types are `text`, `number`, `date`, `select`, `bool`, and `email`. Options are shown for `select` and `bool` fields.

Workflow metadata versus document metadata

Document metadata describes the document and can be used across search, lifecycle, audit, and reporting. Workflow metadata is defined by the workflow template and is collected or used because that workflow process needs it.

The two can overlap. For example, a workflow may require a business field that is also useful as document metadata, or use an `email` metadata field for `Metadata Email` assignee routing in workflow steps.

Missing metadata

A workflow may not start or may route incorrectly if a required field is missing, has the wrong type, lacks a valid option, or is needed for metadata-email routing. Required fields must pass validation before the

template or workflow can be used successfully. Expiry-related metadata may also affect lifecycle behavior if lifecycle policy uses workflow metadata as a date source.

Admins should keep field keys stable, use clear labels and help text, and test required fields before publishing a template.

Related Emii questions

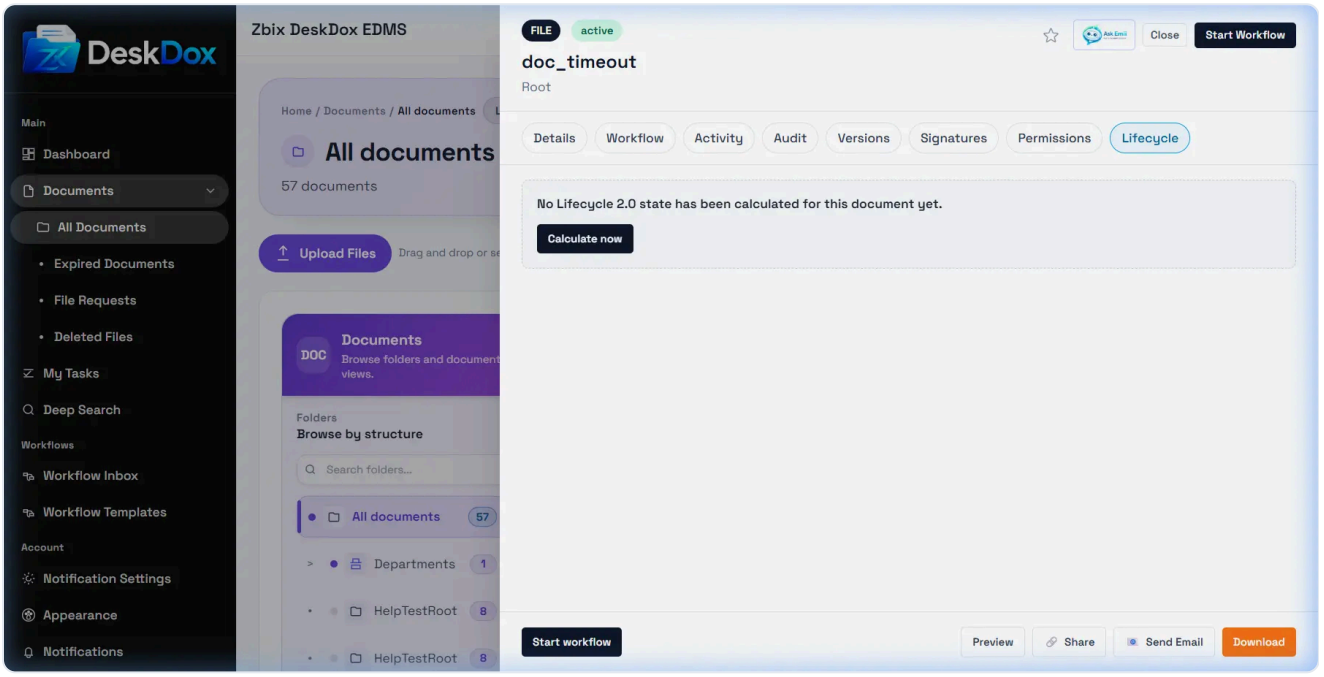
- "What is workflow metadata?"
- "Why does workflow say metadata is missing?"
- "How do metadata fields affect workflow routing?"

Metadata and Versions · 1 min read · Reviewed 2026-05-14

Document Lifecycle Tab

What this helps you do

Use the document Lifecycle tab to see lifecycle state, matched policy/version/assignment, and resolver trace when visible.



Open a document detail drawer and select Lifecycle when the tab is visible. The user list includes the tab can show lifecycle status, matched policy, matched version, matched assignment, resolver trace, and a Recalculate lifecycle action.

Lifecycle states can include managed, unmanaged, expiring, expired, retention active, archived, or calculation error depending on system state and UI wording. If no policy matched, check assignments, policy version activation, effective dates, document metadata, and permissions.

Resolver trace explains why a policy matched or why candidates were skipped. The resolver trace records the selected scope, skipped candidates, and candidates considered. Use it to diagnose wrong policy, wrong version, or assignment precedence.

Recalculate lifecycle is permission-dependent and normally requires administrator access. If the button is not visible, your role may not allow it or the feature may be hidden in that deployment.

Metadata and Versions · 2 min read · Reviewed 2026-05-13

Document Versions

What this helps you do

Use the Versions tab to see the current document version and previous versions kept for history, review, and compliance.

Version history

Open the Document Detail Drawer and select `Versions`. Version history shows the current version and, when available, earlier versions of the same document. The current version is the active version used for preview, download, workflow, and most document actions. Previous versions remain in the history when version retention is enabled.

Uploading a new version

Versions are created when a new file is uploaded as a revision of the existing document rather than as a separate document. If `Upload New Version` is available, use it when the same business document is being revised and the history should stay attached to the original record.

Version uploads and downloads are audit-relevant. If the button is hidden, your permission, the document state, or document policy may not allow version changes.

What users can do

Users may see version number, current or active status, upload details, file details, and available actions such as preview or download depending on permissions and configuration. Restore behavior should be used

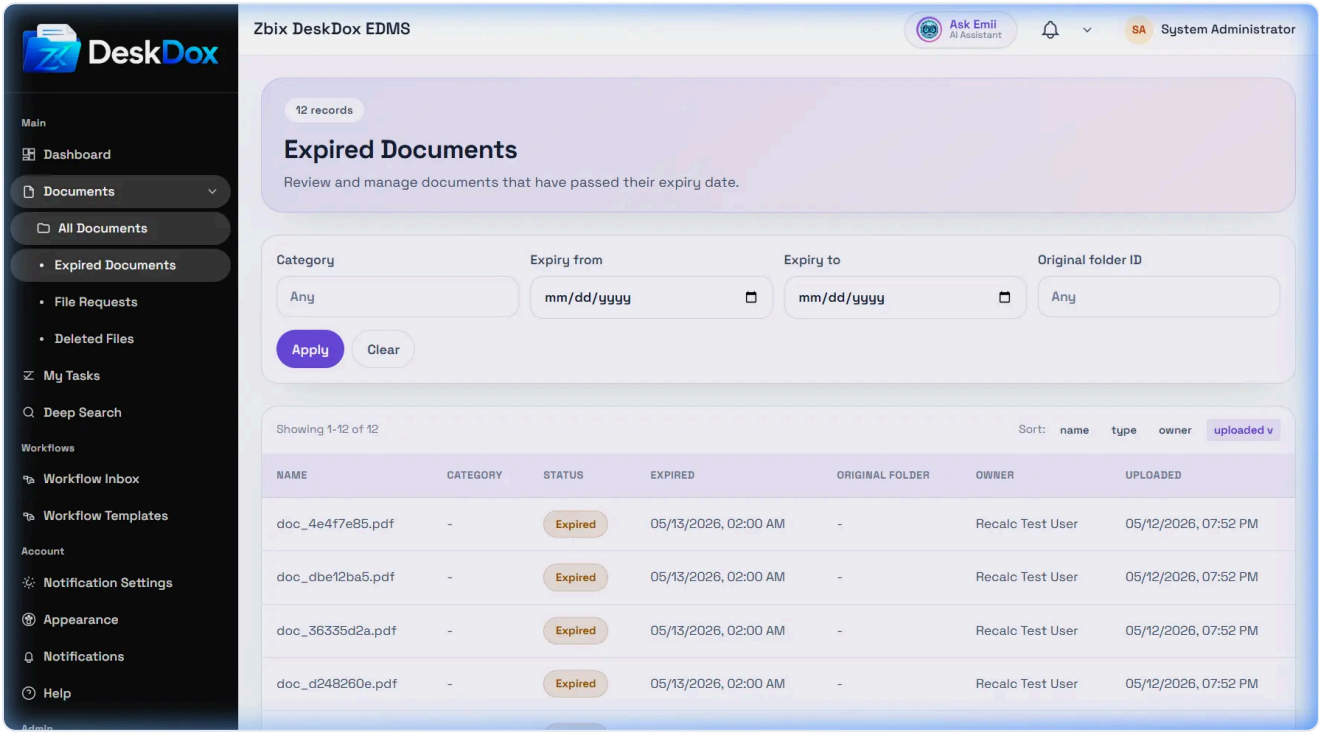
only when that action is visible and your role allows it.

Metadata and Versions · 1 min read · Reviewed 2026-05-13

Expired Documents

What this helps you do

Use the Expired Documents page to review documents marked expired by metadata, lifecycle calculation, or configured lifecycle actions.



Page contents

The page shows expired documents you are allowed to see. Columns can include `Name`, `Category`, `Status`, `Expired date/time`, `Original folder`, `Owner`, and `Uploaded`. The expired badge identifies documents whose lifecycle state is expired.

Actions and permissions

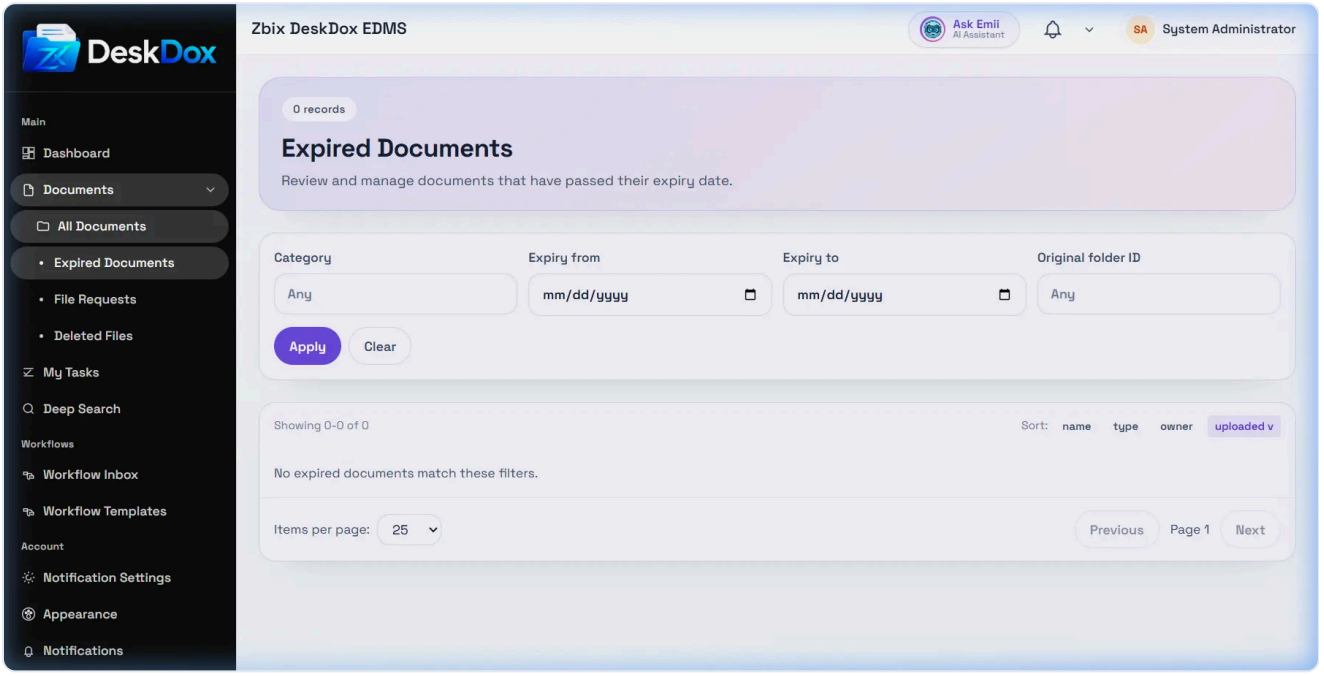
Available actions depend on role and document permission. Depending on configuration, you may be able to preview, open details, move, restore, or recalculate lifecycle. If a document moved to Expired Documents, check the Lifecycle tab for the matched policy and action.

Metadata and Versions · 1 min read · Reviewed 2026-05-14

Expired Documents and Lifecycle

What this helps you do

Understand how lifecycle-marked expiry relates to the Expired Documents view.



Expired Documents is the user-facing place to review documents that are expired and visible to your account. The user list includes the Expired Documents route and lifecycle relationship.

Documents can appear in Expired Documents when lifecycle or another process marks them expired, or when their expiry status/date is reflected by document fields and filters. Lifecycle actions can mark expired or move a document depending on the active policy version and enforcement.

The view may show an expired badge/status, expired date, and original folder context when available. Original folder is especially useful when a lifecycle action moved the document to another folder.

Restore or reactivation behavior must be treated as permission- and configuration-dependent. Browser discovery saw Restore and Delete actions in the expired view, but Delete is not a supported Lifecycle 2.0

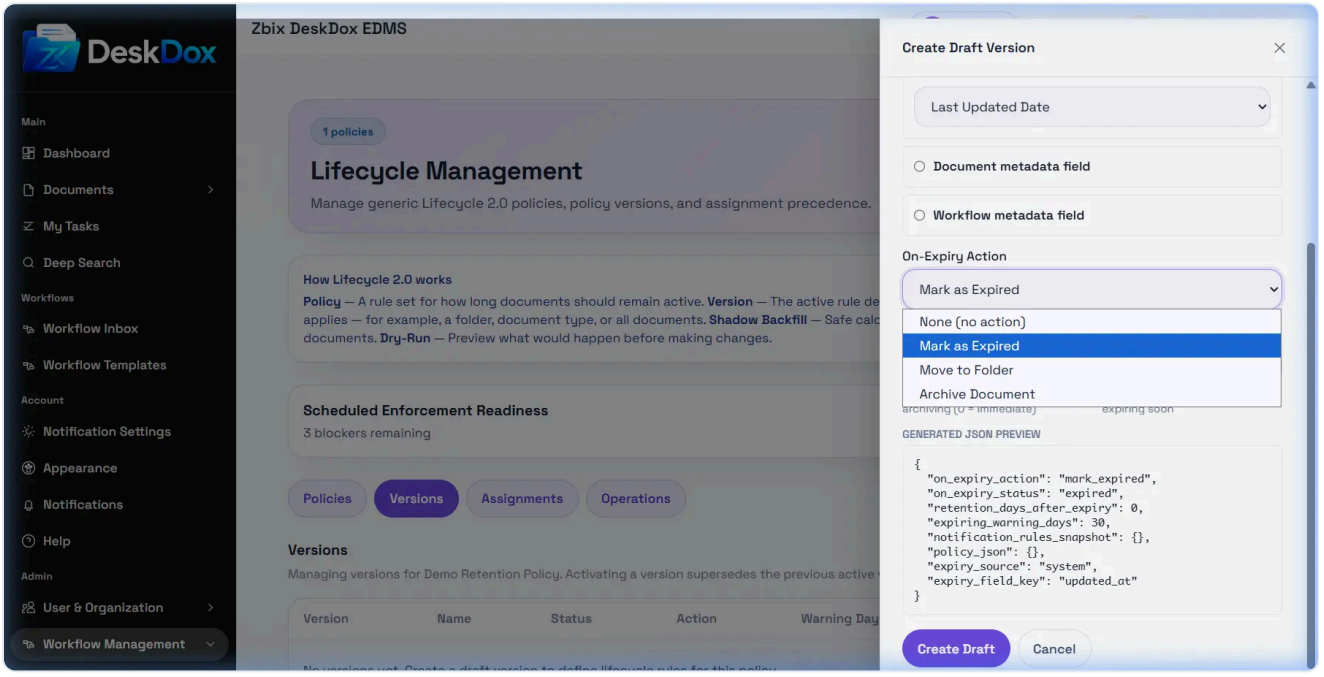
action and Lifecycle does not delete documents. Ask an admin before restoring records governed by retention policy.

Metadata and Versions · 1 min read · Reviewed 2026-05-14

Lifecycle Actions

What this helps you do

Understand the actions lifecycle can apply when a matched document becomes eligible.



The user list includes On-Expiry Action options including Mark as Expired, Move to Folder, Archive Document, and None/Do Nothing. Supported enforcement actions include leaving the document unchanged, marking it expired, moving it to a folder, or archiving it.

Move to Folder changes the document folder to a configured target folder. When this action is selected, the UI shows a target folder picker when visible. Enforcement fails or skips the action if the target folder is missing or deleted.

Mark as Expired sets the document expired timestamp when enforcement runs. Archive Document sets document status to archived. DeskDox includes archive is status-only today: it does not delete storage and does not change permissions.

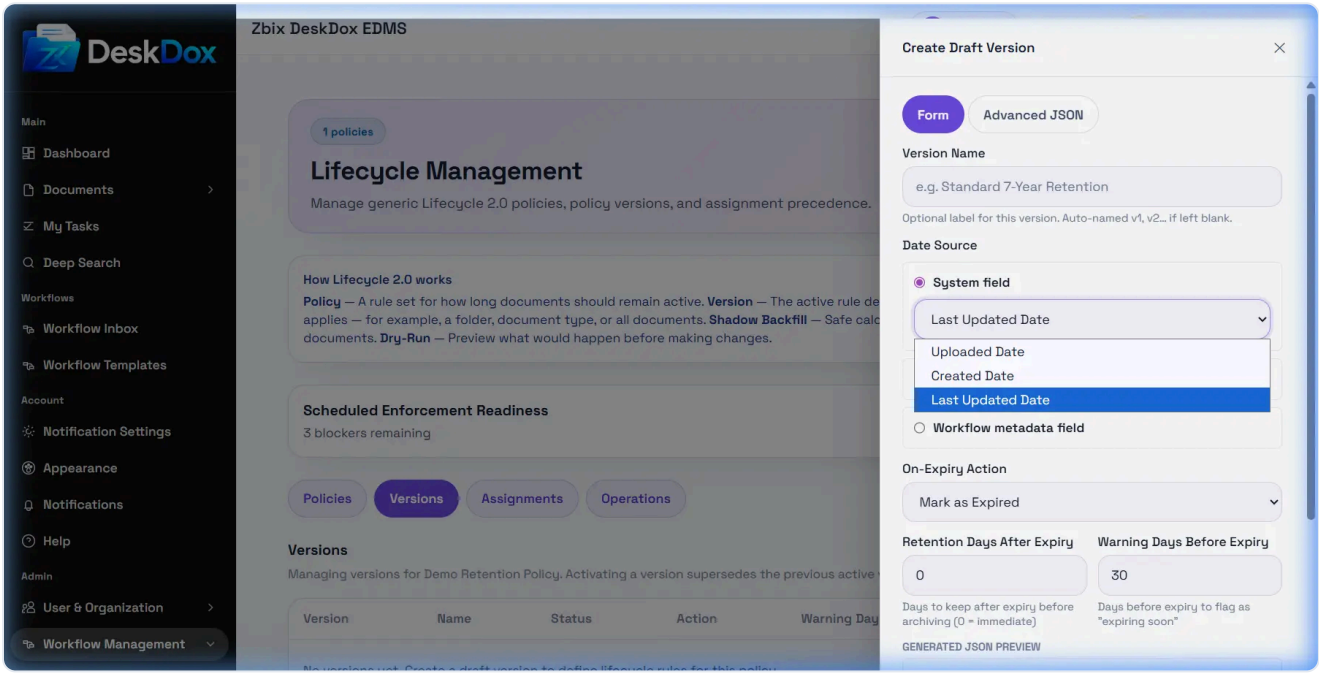
Notification behavior should be documented only if notification rules are configured in your deployment. Delete is not a supported Lifecycle 2.0 enforcement action. Lifecycle does not delete documents.

Metadata and Versions · 1 min read · Reviewed 2026-05-14

Lifecycle Date Sources

What this helps you do

Choose the date field lifecycle uses to calculate expiry and understand why missing dates block matching.



A lifecycle date source tells DeskDox which date to use for expiry calculation. Supported system fields include uploaded_at, created_at, updated_at, and last_modified_at. uploaded_at maps to the document created_at field.

Document metadata date sources read a metadata key on the document. Recognized standard aliases can fall back to document fields, including expiry_date, retention_until, updated_at, created_at, and uploaded_at. Custom metadata wins when a matching metadata row exists.

Workflow metadata date sources require a workflow template and a workflow metadata field. The document must have a workflow instance for that template and a stored metadata value for the field. This is a workflow-related metadata/date source, not a workflow approval-event trigger.

Expiry metadata may be required because lifecycle cannot calculate a due date when the selected date field is blank, invalid, or missing. Date parsing is available as ISO-style date/datetime parsing. Browser

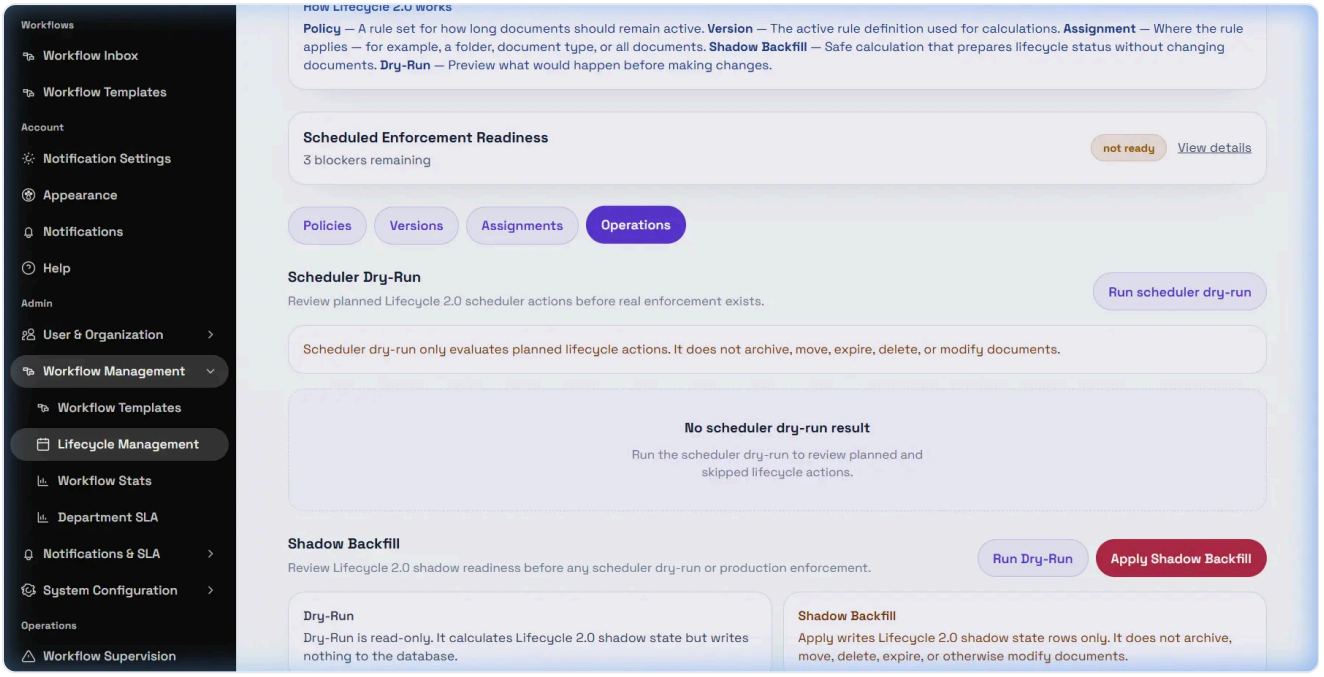
timezone handling was not confirmed; treat date boundary interpretation as pending confirmation in your deployment.

Metadata and Versions · 1 min read · Reviewed 2026-05-14

Lifecycle Enforcement and Dry-Run

What this helps you do

Use dry-run, shadow backfill, and guarded manual enforcement safely before changing production documents.



Dry-run previews planned and skipped lifecycle actions without changing documents. Use it before production enforcement to see due date, action type, trigger source, and skip reason.

Shadow Backfill can run as a dry run to report planned counts without changes. When applied, it creates or refreshes shadow document lifecycle state only; it does not move, archive, expire, or delete documents.

Manual enforcement is guarded by system configuration and explicit confirmation. The UI may require typed confirmation such as ENFORCE depending on the visible form. Keep production runs scoped to specific document IDs and limited allowed actions where possible.

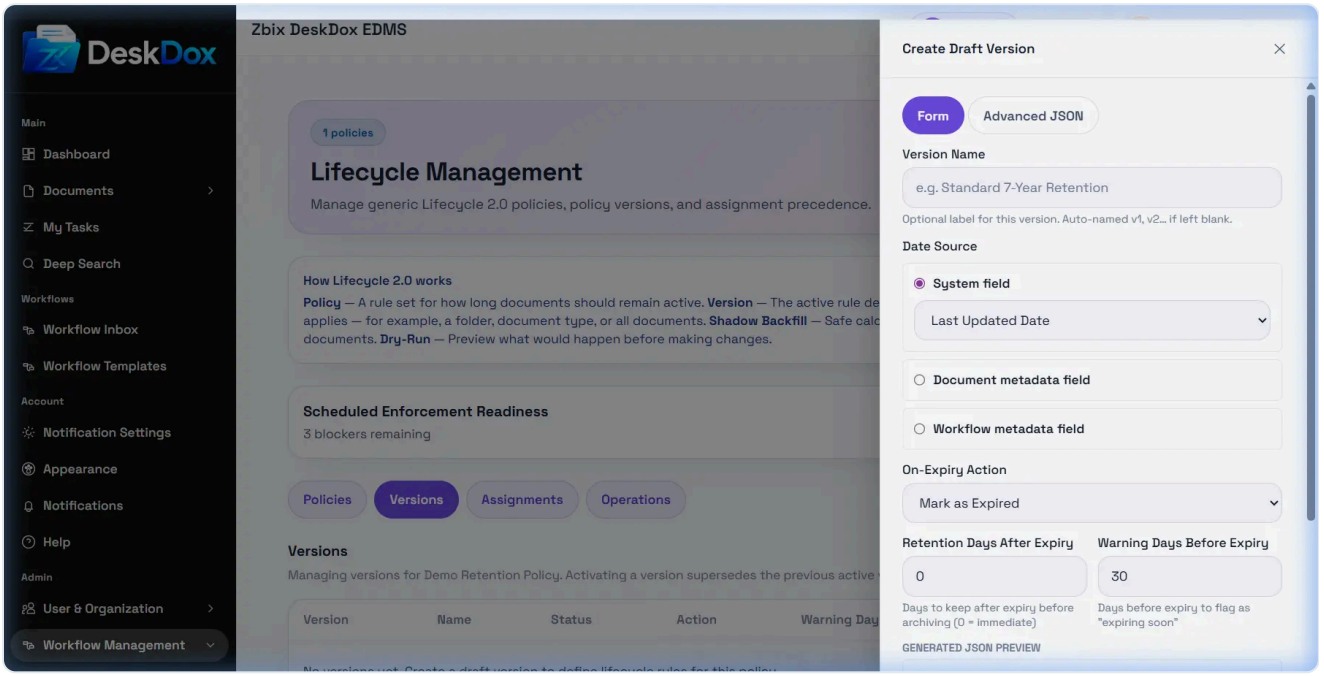
Observe-only or shadow mode should mean calculation/backfill without document-changing enforcement. Do not assume it applies actions. Review dry-run results, resolver trace, missing metadata, target folders, and action limits before running enforcement.

Metadata and Versions · 1 min read · Reviewed 2026-05-14

Lifecycle Rules and Triggers

What this helps you do

Configure lifecycle rule criteria and understand what can trigger lifecycle calculation or enforcement.



The rule builder configures date-based lifecycle behavior. Supported date source types are system fields, document metadata, legacy metadata aliases, and workflow metadata. The user list includes the rule builder and workflow-related metadata/date field selection.

Lifecycle rules are date-based. A document matches a policy through assignment scope first, then lifecycle calculates using the selected date source. Conditions and match details should be interpreted from the visible rule fields and resolver trace.

Do not describe workflow approval, rejection, or completion as a lifecycle event trigger unless a separate event integration is configured. Lifecycle supports workflow template assignment scope and workflow metadata date resolution, not automatic workflow-event triggers.

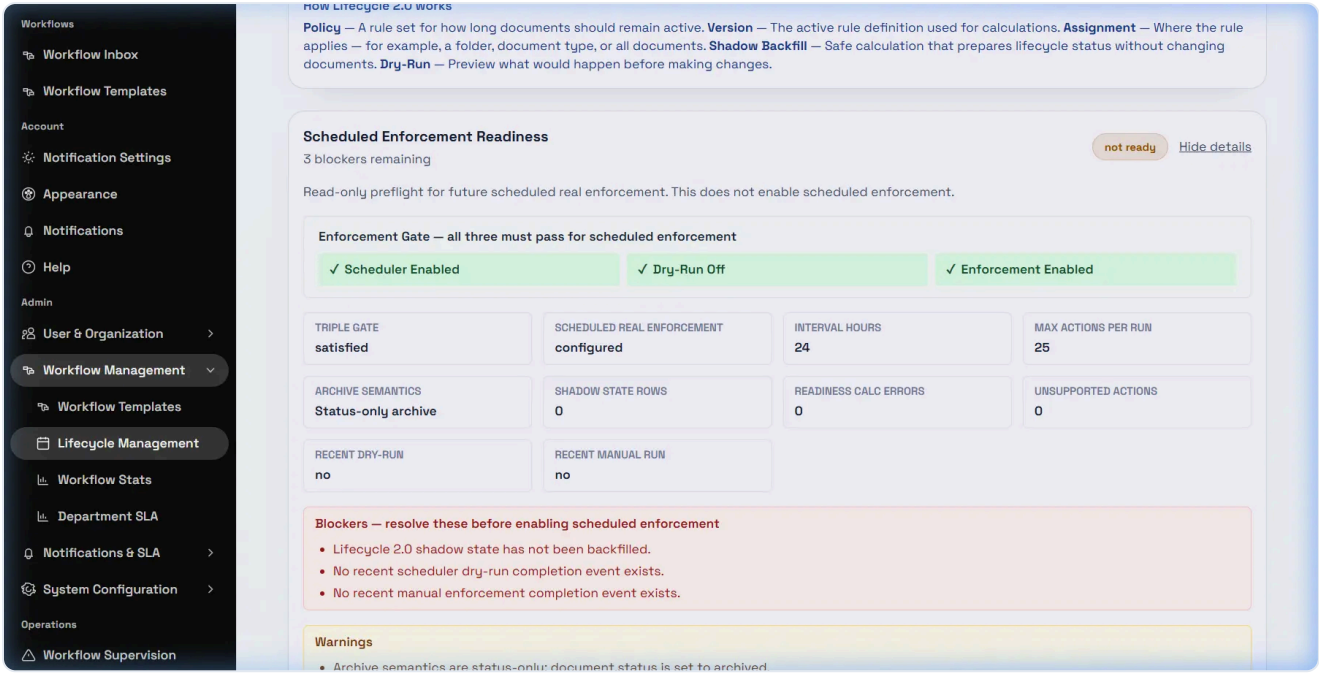
A document may not match because there is no active assignment, no active/current version, the assignment is outside its effective dates, the policy is deleted/inactive, the selected date is missing or invalid, or a higher-precedence assignment won. Assignment precedence is document, workflow template, folder, category, document type, then global.

Metadata and Versions · 1 min read · Reviewed 2026-05-14

Scheduled Lifecycle Enforcement Readiness

What this helps you do

Check whether scheduled lifecycle enforcement is configured and ready.



The readiness panel is a read-only operational check. It can show scheduled readiness status, blockers, warnings, and recent dry-run or manual enforcement signals.

Scheduled real enforcement requires backup scheduler and enforcement settings. The important readiness gates are scheduler enabled, scheduler dry-run disabled, and enforcement enabled. If any gate is missing, scheduled real enforcement should be treated as not ready.

If scheduled enforcement is not running, check readiness blockers, system service environment variables, worker/scheduler process health, recent dry-run events, calculation errors, unsupported actions, and max-actions-per-run settings.

Last-run status visibility depends on what the readiness card exposes in your environment. Treat exact scheduler timing and timezone as pending confirmation unless your admin has available the deployed scheduler configuration.

CHAPTER 5

Search and Retrieval

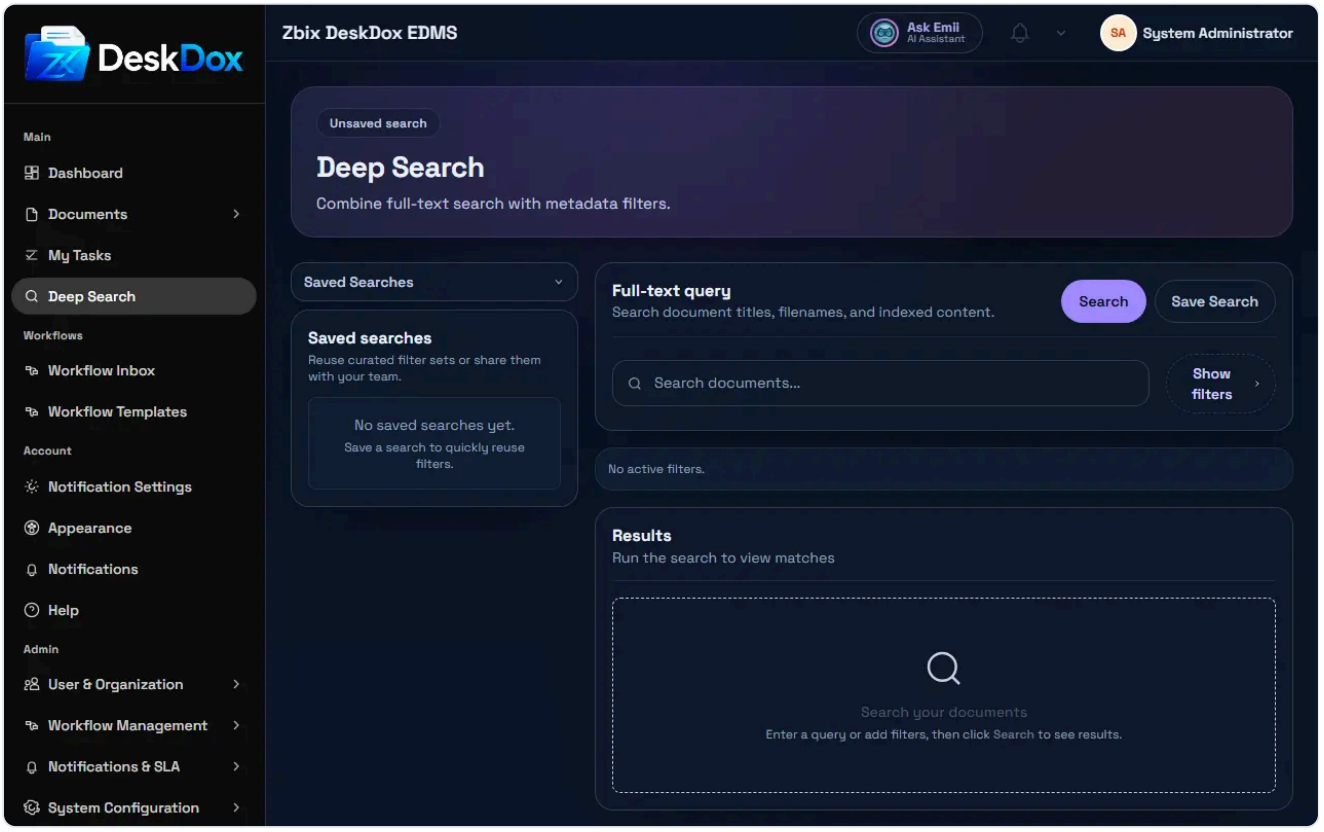
OCR search, deep search, search filters, and retrieval workflows.

Search and Retrieval · 2 min read · Reviewed 2026-05-13

How to Find a Document Using Search

Quick search

Open `Deep Search`, enter a keyword, and run the search. Keywords can include a document name, code, reference number, person, period, or a word from the document content when content indexing is available.



Metadata search

Use metadata fields when you know structured values such as category, department, reference number, date, status, owner, or other business fields. Metadata filters help narrow broad keyword searches to the exact document set you need.

Full-text and OCR search

DeskDox can search document content as well as metadata. Full-text and OCR-based word search can find words inside indexed files, including scanned content after OCR processing. Newly uploaded or scanned files may need indexing time before content words appear in results.

Filters and result refinement

Use status, category, metadata, and other visible filters to refine the result list. Start broad, then add filters one at a time so you can see which condition narrows the results.

Permission-aware results

Search results are filtered by your document, folder, role, and department permissions. If another user sees different results, confirm both users have the same access scope and that the same filters are selected.

If results are empty

- Check spelling and try fewer filters.
- Confirm document status (active vs expired/deleted context).
- Newly uploaded/scanned files may need indexing time.

Related reading

- How to Use Deep Search Filters
- User Manual: Search and Retrieval

Search and Retrieval · 1 min read · Reviewed 2026-05-13

How to Use Deep Search Filters

What this helps you do

Build precise searches with metadata filters, save reusable searches, and export results when allowed.

Steps

1. Open `Deep Search`.
2. Expand filters.

3. Add filter rows (field, operator, value).
4. Optionally set status/category criteria.
5. Run search.
6. Save search if you will reuse it.

Saved search actions

- `Save` : store current criteria.
- `Run` : apply a saved search.
- `Update` : overwrite criteria for an existing saved search.
- `Delete` : remove a saved search.

Export notes

- CSV export is role-dependent.
- Export only after confirming filters and result count.

Related reading

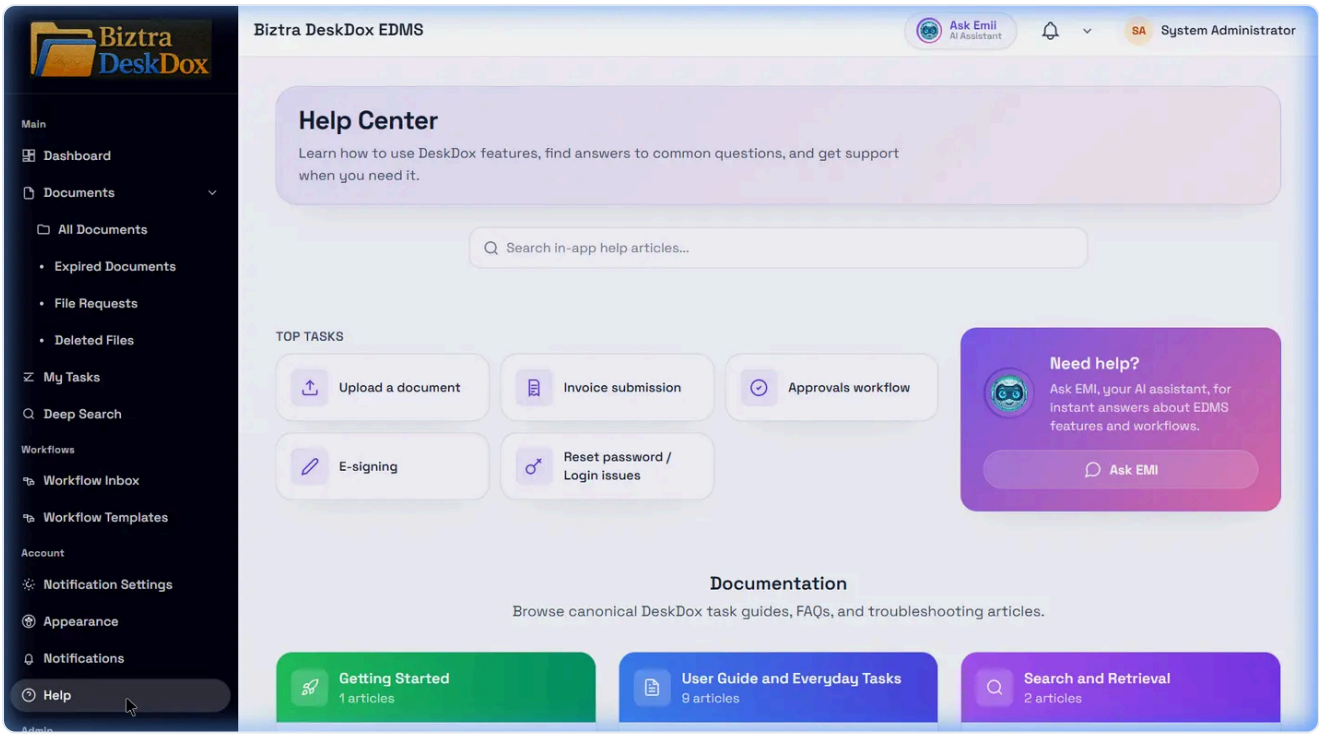
- How to Find a Document
- User Manual: Search and Retrieval

Search and Retrieval · 2 min read · Reviewed 2026-05-13

Search the Help Center

What this helps you do

Find DeskDox help articles, open the right article, and use Emii for source-based answers about DeskDox features.



Who can use it

All signed-in users with Help Center access can search articles. Emii availability depends on environment configuration and user access.

Required permissions

- Help Center route access.
- Emii access if asking the assistant.

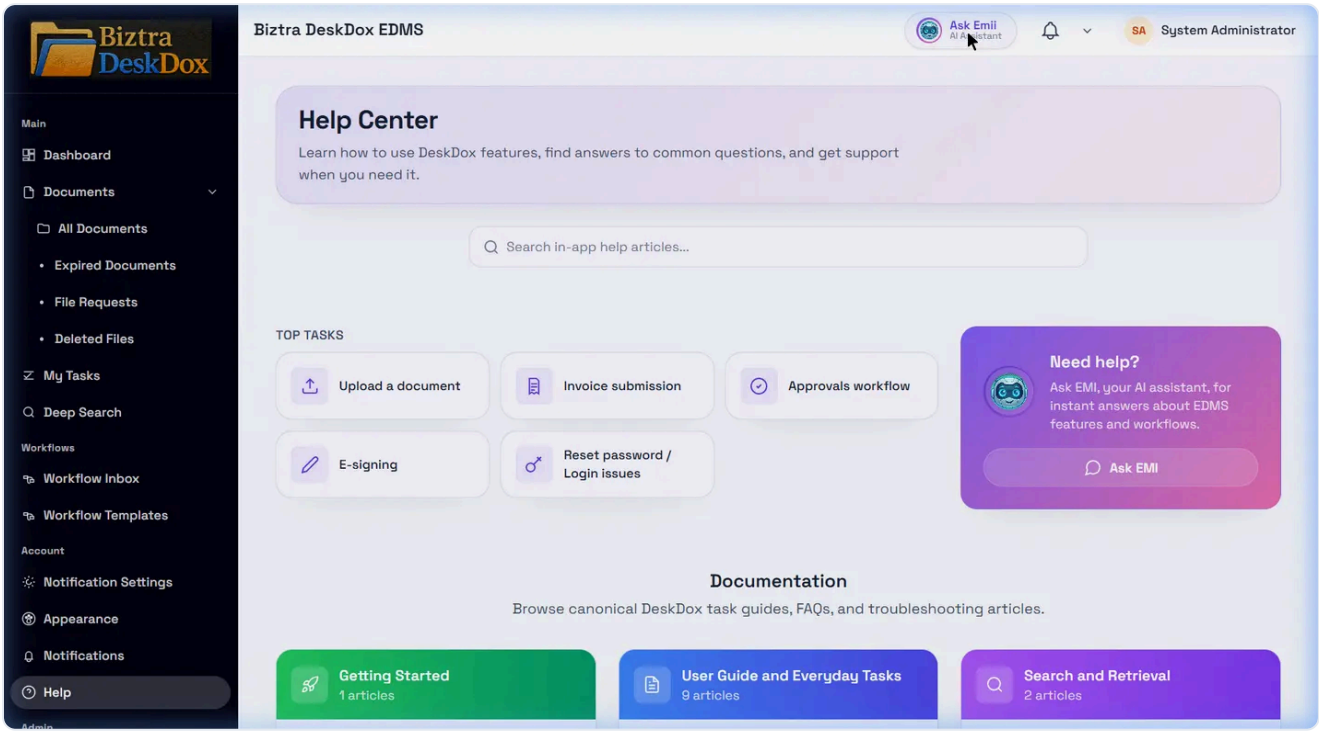
Search the Help Center

1. Open `Help Center`.
2. Type a feature, task, or problem in the search box.
3. Use practical keywords such as `upload`, `workflow`, `lifecycle`, `public link`, `department`, or `audit`.
4. Open the article that matches your task.

Open an article

Select an article from search results, top tasks, or categories. Articles include purpose, permissions, steps, troubleshooting, screenshots where available, and related Emii questions.

Ask Emii about DeskDox features



Ask how-to questions in normal language:

- "How do I upload a document with workflow?"
- "How do I create a user and assign a department?"
- "Why did lifecycle not move documents?"
- "Where can I view the document audit trail?"

Understand Emii source-based answers

For product and how-to questions, Emii should use Help Center articles first. When relevant help content exists, Emii should answer from that content and cite the source article or section. If no matching article exists, Emii should say the Help Center has no matching article yet instead of inventing product behavior.

Common mistakes

- Asking a document-content question in Help mode when you meant to search uploaded files.
- Asking a very broad question such as "help me" instead of naming a feature or task.
- Ignoring cited source articles when the answer includes them.
- Assuming Emii overrides permissions or policy.

Troubleshooting

If search returns no results, try fewer words or a product keyword. If Emii gives a generic answer, ask with the feature name and task. If Emii is unavailable, use the article search and contact support if needed.

Related Emii questions

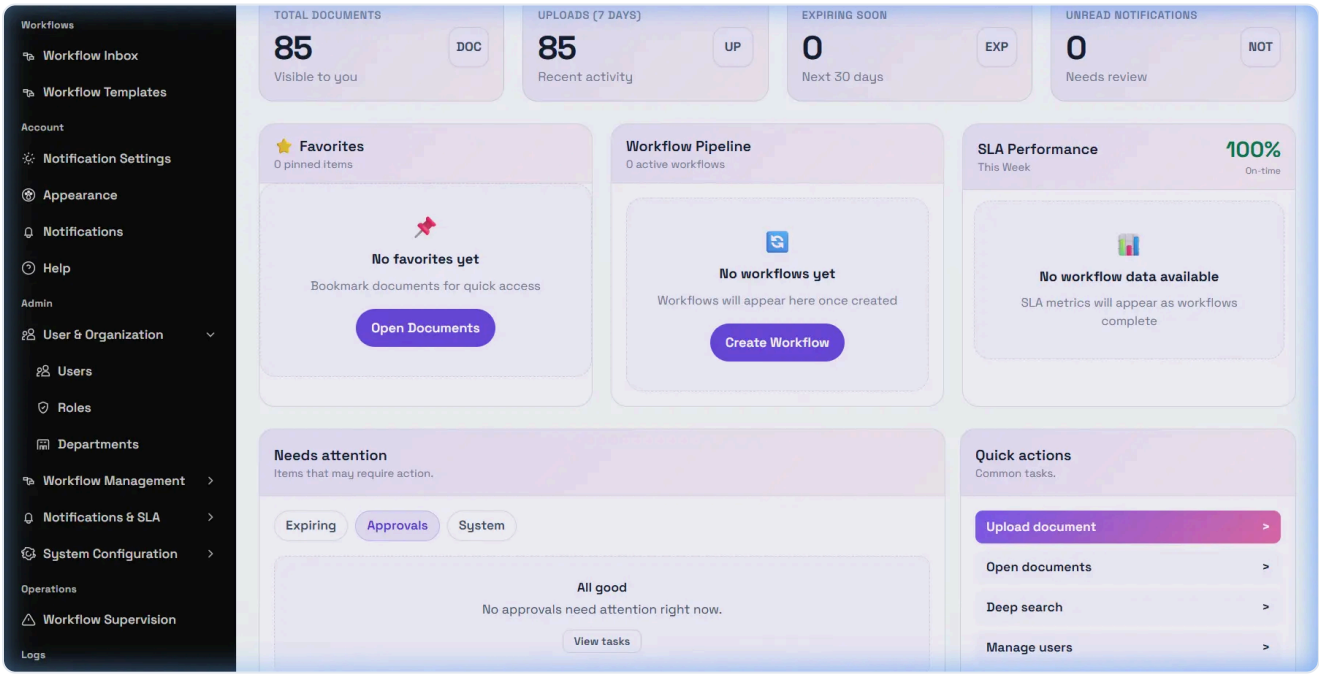
- "How do I search Help Center articles?"
- "Can Emii answer from Help Center sources?"
- "Why did Emii say no matching help article exists?"
- "How do I ask Emii about DeskDox features?"

Related reading

- How to Use Emii Effectively
- Common Issues and Quick Fixes
- Frequently Asked Questions

Search and Retrieval · 1 min read · Reviewed 2026-05-14

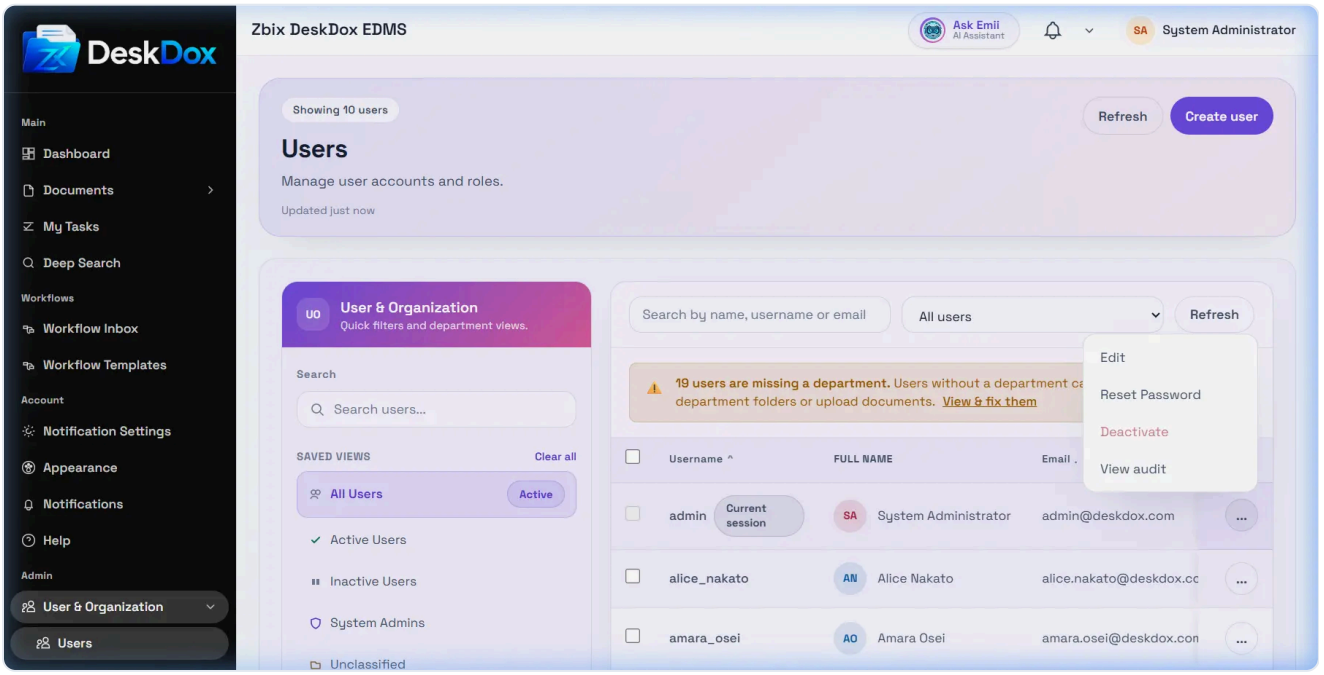
Users List and Search



Open `/app/admin/users` to manage user accounts when your account has admin user visibility. The page lists users with account details such as name, email, status, department, role information, and row actions

when available.

The DeskDox uses user search by username, email, or full name. Status filtering is available for active and inactive users. Status filters and row actions are available for managing active and inactive users.



Common actions can include `Edit`, `Reset Password`, `Deactivate`, `Activate`, and `View audit`, depending on your permissions and the user safety rules. An inactive user is a user whose account has been deactivated; they may be blocked from normal login or access until reactivated.

If you cannot see the Users page, ask an administrator to confirm your admin role and user-management permission. A visible page with no matching results usually means the current search, department filter, role filter, status filter, or pagination hides the user.

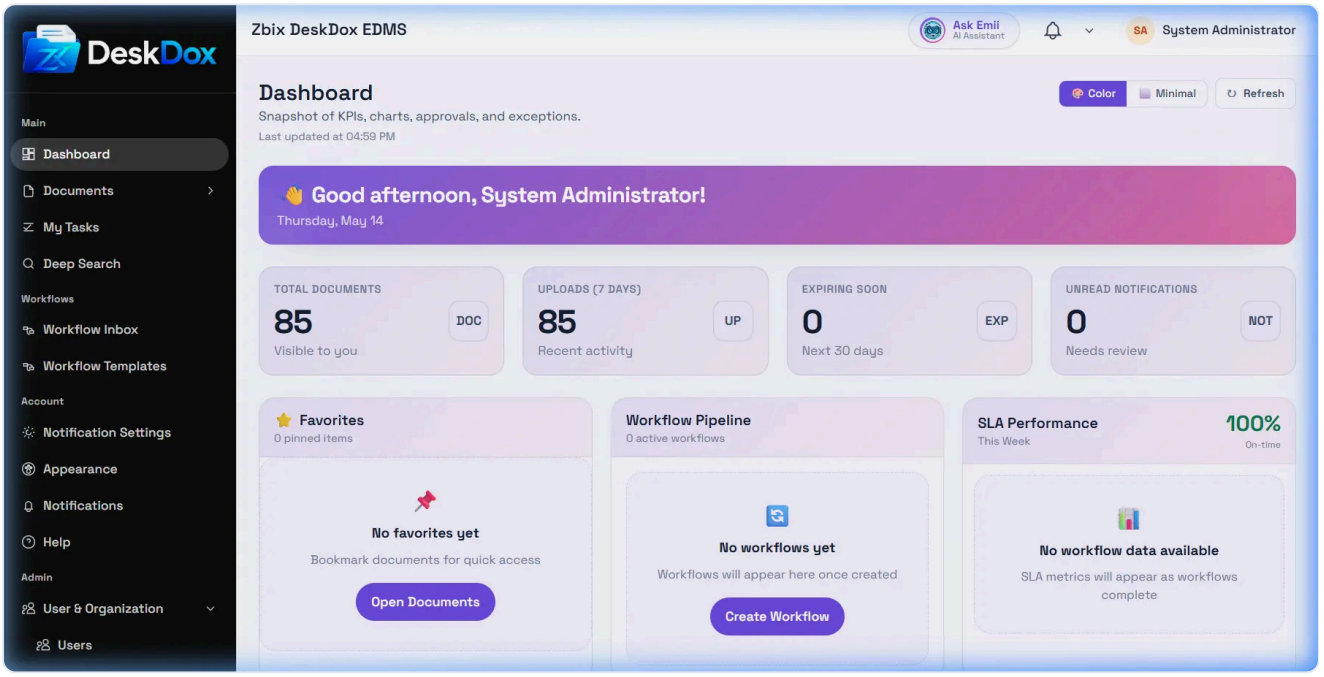
CHAPTER 6

Sharing and Access Control

Sharing, permissions, users, departments, roles, visibility, and audit access patterns.

Sharing and Access Control · 2 min read · Reviewed 2026-05-14

Access Control Overview



DeskDox access control is the set of user, role, department, permission, folder, document, and audit controls that decide what a signed-in person can see or do.

The browser-confirmed admin routes are `Users` at `/app/admin/users`, `Roles` at `/app/admin/roles`, role permissions at `/app/admin/roles/:id`, `Departments` at `/app/admin/departments`, and the security `Audit Log` at `/app/admin/system/settings/audit`.

Core concepts

`Users` are individual accounts. A user can be active or inactive, can belong to a department, and can have more than one role.

`Roles` are permission sets. DeskDox uses role-based access control, or RBAC, so a role can grant access to modules, screens, and actions. DeskDox includes built-in/protected role identities in `system service/app/services/role_identity.py` for `system_admin`, `edms_admin`, `edms_auditor`,

`edms_user`, `task_admin`, `workflow_admin`, `manager`, `approver`, and `department_head`. The same source also defines `demo_admin` as a demo administrator role and `admin` as a legacy compatibility role.

`Departments` group users by organization, branch, team, or unit. Department assignment matters because DeskDox uses department membership participates in folder access decisions, and the user creation UI requires a department for normal users.

`Permissions` control actions such as viewing, creating, editing, deleting, administering, managing workflow templates, viewing workflow statistics, and managing lifecycle policy where those permissions are implemented.

Admin permissions and document access are different

Admin access controls who can manage users, roles, departments, and system settings. Document and folder access controls which folders or documents a user can view, upload to, edit, share, or manage. A user can have a role that allows a module but still lack access to a specific folder or document.

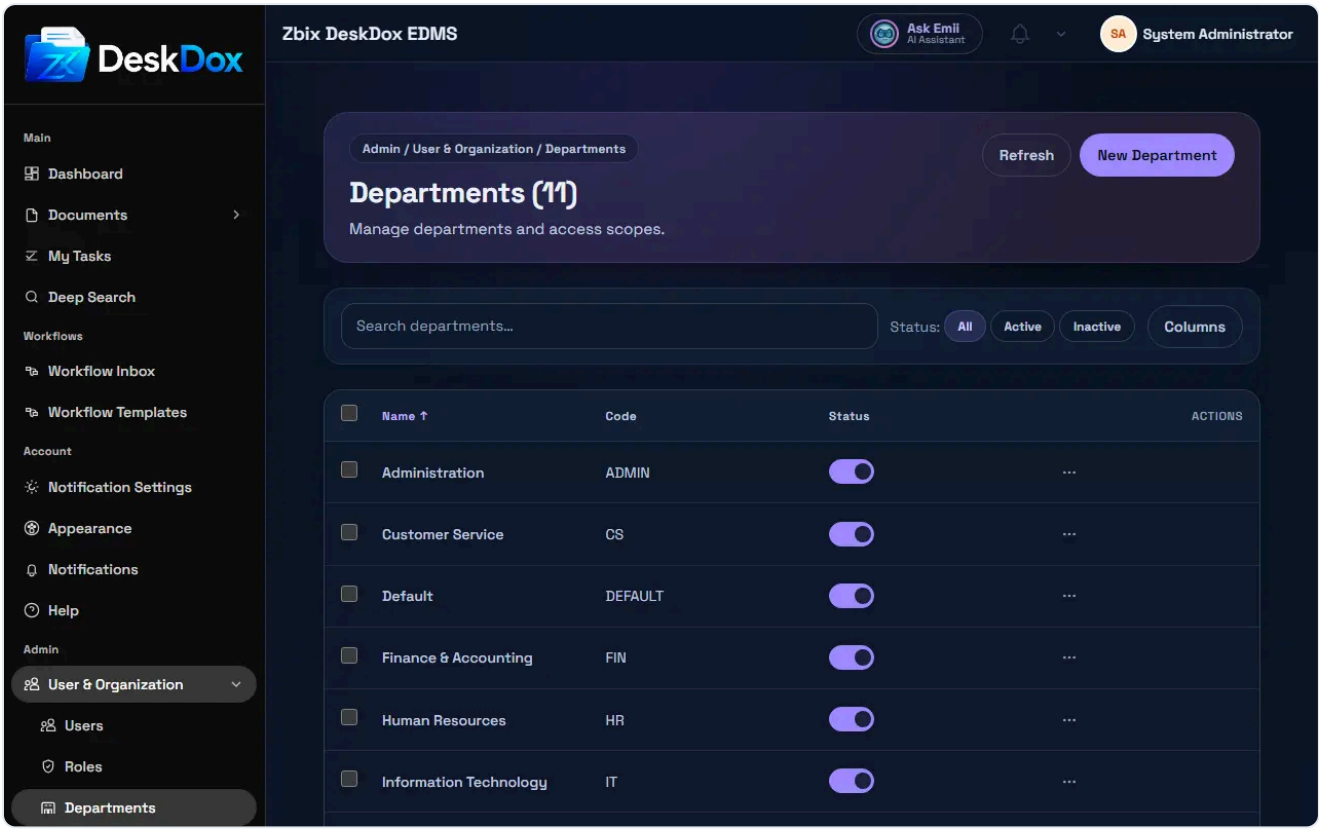
Why screens differ between users

DeskDox may hide menus, buttons, tabs, row actions, and admin pages when the current user lacks the needed role, permission, department scope, folder access, document access, workflow assignment, lifecycle permission, or license/configuration state. System service authorization should still enforce the final decision even if a UI action is visible.

Use least privilege: give the narrowest role and folder access that lets the user do their work. User, role, department, and permission administration is admin-only.

Sharing and Access Control · 1 min read · Reviewed 2026-05-14

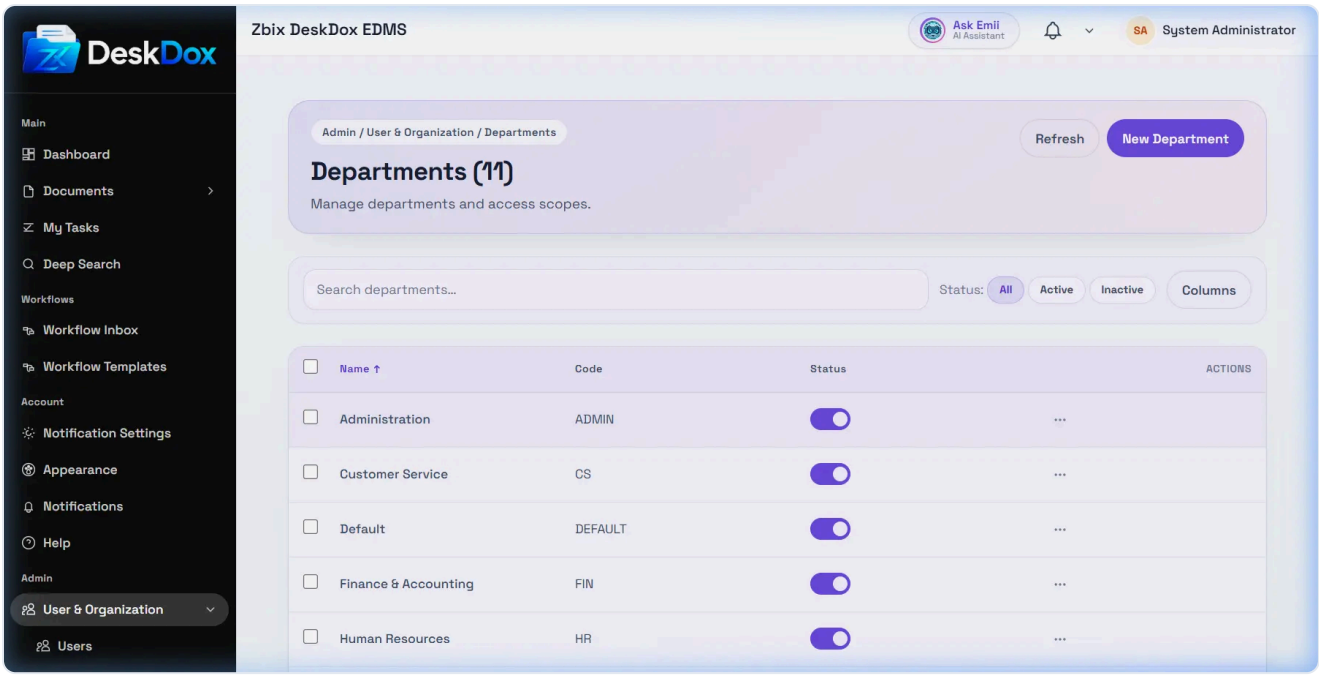
Departments Overview



A department is an organizational grouping such as a branch, team, or unit. DeskDox uses departments to organize users and to support access decisions.

DeskDox includes a user's `primary_department_id` participates in folder access checks. For normal users, department assignment is important because same-department fallback access can allow folder actions such as view, list, preview, download, and upload depending on folder ownership and access logic.

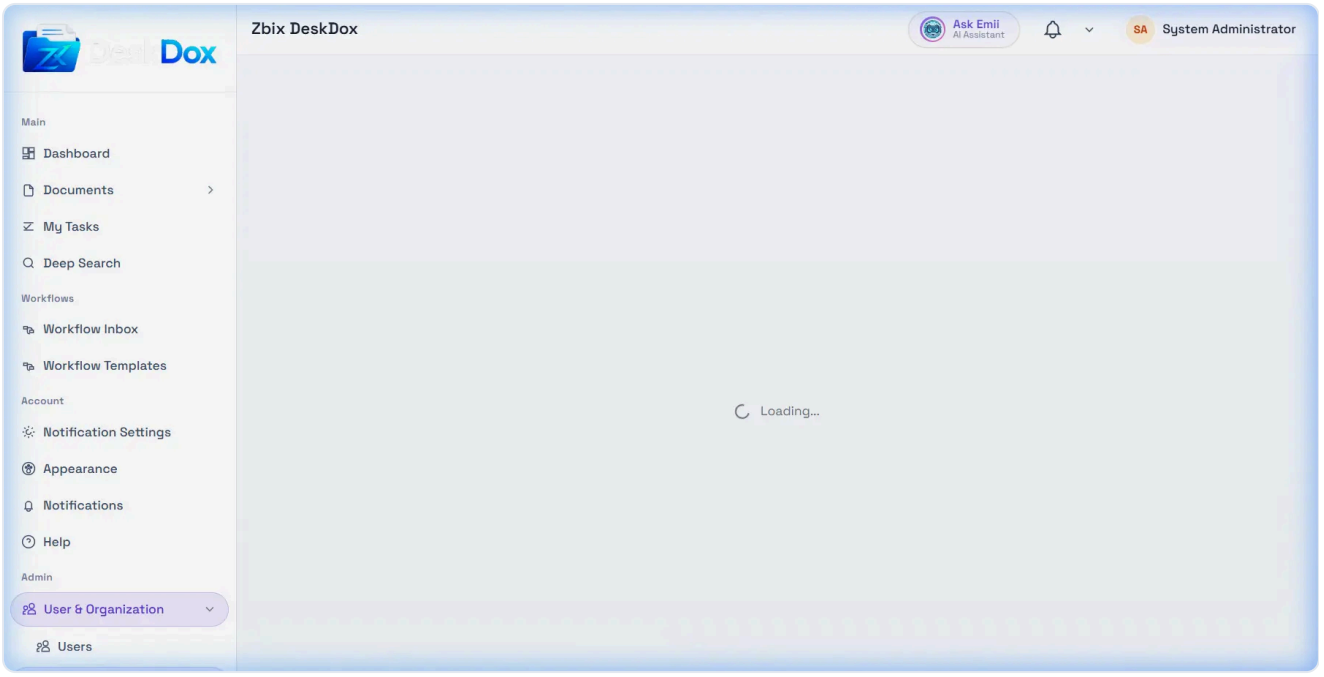
The user creation UI requires a department for normal users. DeskDox includes active non-`system_admin` users cannot be created without a department, and an active normal user cannot have the department removed during edit.



The user list includes department member viewing. The current user form has one primary department dropdown, so do not assume a user can belong to more than one primary department unless a separate feature is visible in your environment.

Sharing and Access Control · 1 min read · Reviewed 2026-05-14

Roles Overview



A role is a named access profile that can be assigned to users. DeskDox uses roles to grant administrative capabilities, workflow administration, lifecycle management, document-related capabilities, and other permissions where the permission is implemented.

DeskDox includes built-in/protected role identities in `system service/app/services/role_identity.py` for `system_admin`, `edms_admin`, `edms_auditor`, `edms_user`, `task_admin`, `workflow_admin`, `manager`, `approver`, and `department_head`. The same source also defines `demo_admin` as a demo administrator role and `admin` as a legacy compatibility role. Built-in, protected, and system roles are locked for metadata and permission assignment changes in the current custom-role lifecycle.

Custom roles can be created from `/app/admin/roles` by users with mutation permission. Custom role names must be lowercase machine names that start with a letter and use lowercase letters, numbers, and underscores.

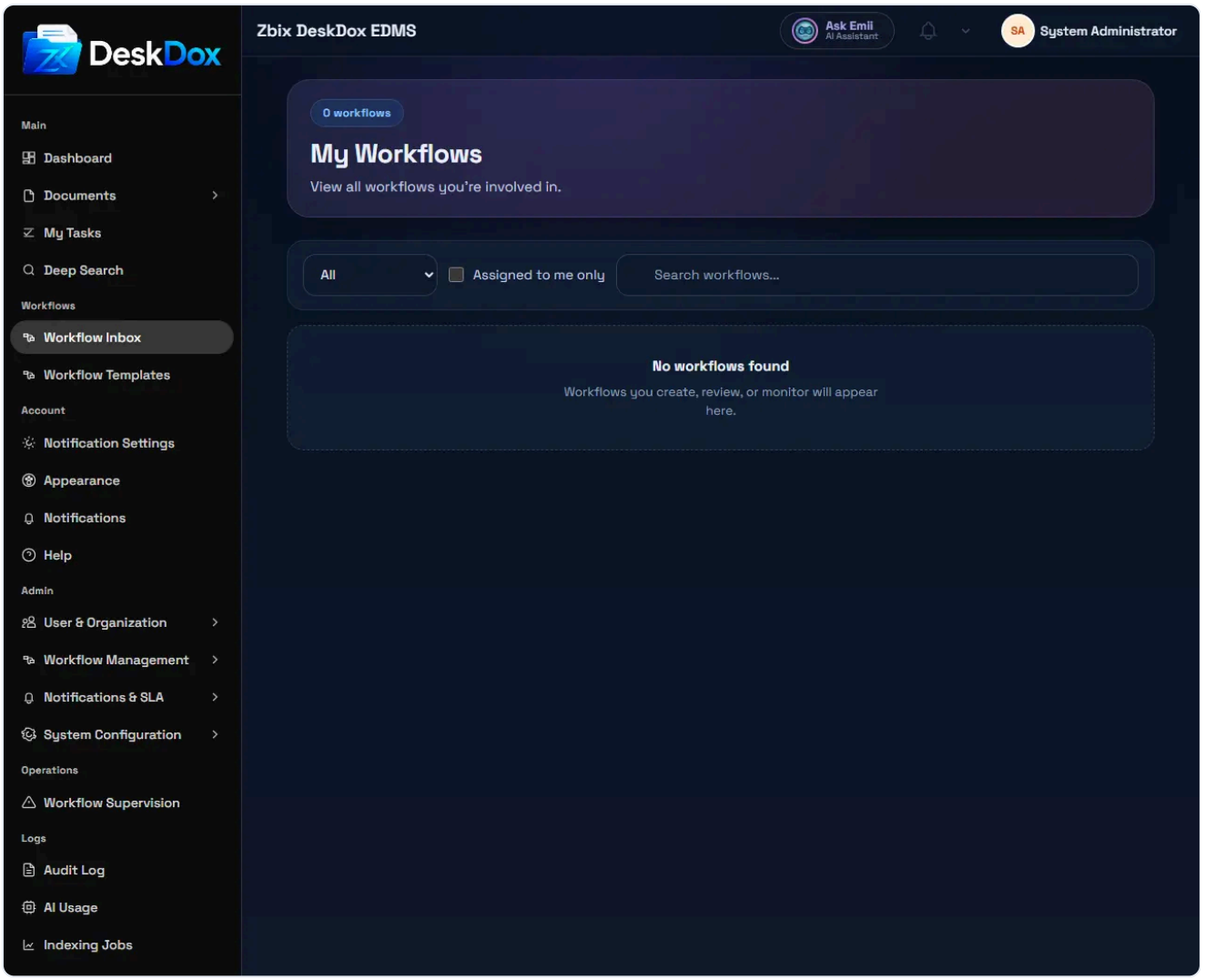
Roles affect access in two ways: they can make menus and buttons visible in the UI, and they can be checked by system service authorization. A role alone may not grant folder or document access; document and folder permissions, ownership, department membership, workflow assignment, and lifecycle configuration can still limit access.

Sharing and Access Control · 3 min read · Reviewed 2026-05-14

Workflow User Side Overview

What this helps you do

Understand where assigned workflow work appears, why workflow tasks differ between users, and how workflow connects to documents.



What user-side workflow is

User-side workflow is the part of DeskDox where reviewers, approvers, department members, and signers see work assigned to them. It is for acting on active workflow items, checking status, and reviewing documents that are moving through an approval or signing process.

Workflow tasks are different from admin workflow templates. A workflow template is the configured process that administrators create and manage. A workflow task is a live assignment created from a started workflow, usually tied to one document and one current step.

Where users see tasks

The user workflow area includes the task inbox, assigned tasks, pooled or department tasks, and task status. Use `My Tasks`, `Workflow Inbox`, or the visible workflow navigation entry to open work assigned to you or to a department you belong to.

Workflow tasks are related to documents. A task usually points back to the document being reviewed, signed, approved, rejected, or returned. The document may also show workflow information in the

Document Detail Drawer `Workflow` tab when the tab is visible and you have access.

Why users see different workflow tasks

Workflow visibility depends on assignment, role, department, permissions, and task status. A task may be assigned directly to a user, assigned to a role, or assigned to a department. Some users may only see tasks they can act on, while administrators or workflow managers may see broader workflow information depending on permissions.

Completed, cancelled, skipped, rejected, or already-actioned tasks may move out of an active list or appear only under completed/all filters when those filters are available.

Empty workflow pages

When no approval tasks exist, the empty state says: "You have no pending approval tasks. If a workflow you expected is unavailable, open the document workflow tab or contact an administrator."

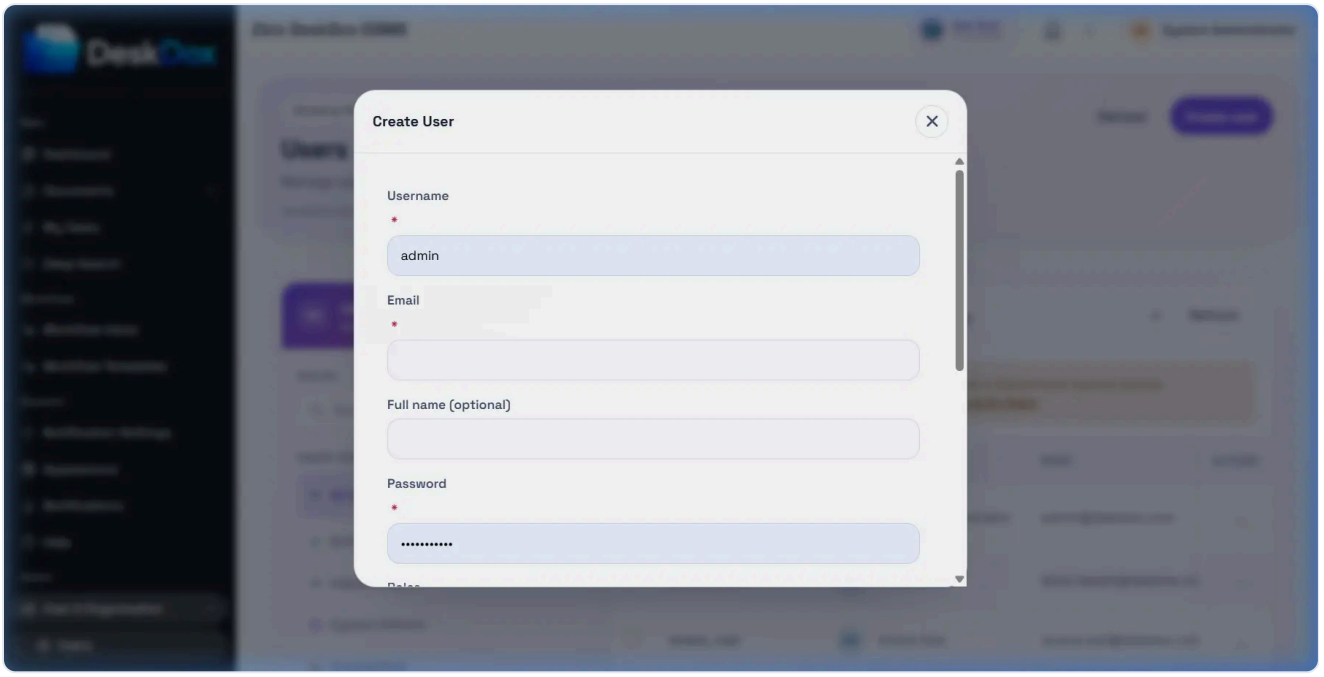
An empty page usually means there is no active task assigned to you. It can also mean the workflow has not started, the task belongs to another user/role/department, the workflow is completed or cancelled, or your role does not include the required workflow permission.

Related Emii questions

- "What is workflow used for?"
- "Where do I see my workflow tasks?"
- "Why can't I see a workflow task?"
- "Why are workflow tasks different for each user?"
- "Why is my workflow page empty?"

Sharing and Access Control · 1 min read · Reviewed 2026-05-14

Assign Roles to Users



Open `/app/admin/users`, create a user or edit an existing user, then use the `Roles` checkboxes. You can assign multiple roles to one user when the checkboxes are available.

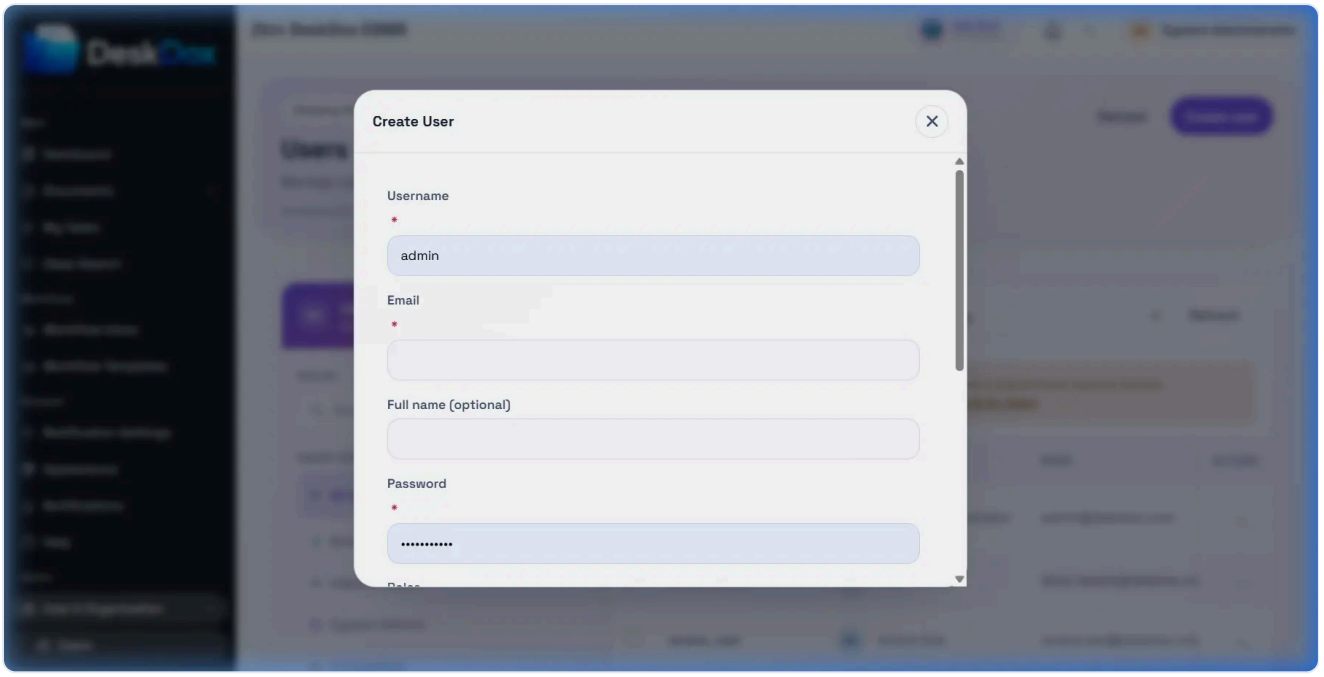
To add a role, check it and save. To remove a role, clear it and save. Bulk role changes are source-code supported through `Change roles` / `Apply roles`; bulk role update replaces the selected users' roles with the selected role set.

Role changes affect menus, buttons, admin screens, workflow access, lifecycle administration, and other permission checks only where the relevant role or permission is used. A role change may not grant folder or document access by itself.

If a role change does not appear to take effect, confirm the save succeeded, the user has the expected role names, the role has the expected permissions, the user has the needed department and folder/document access, and the user refreshed the page or signed in again if the current session still reflects older permissions.

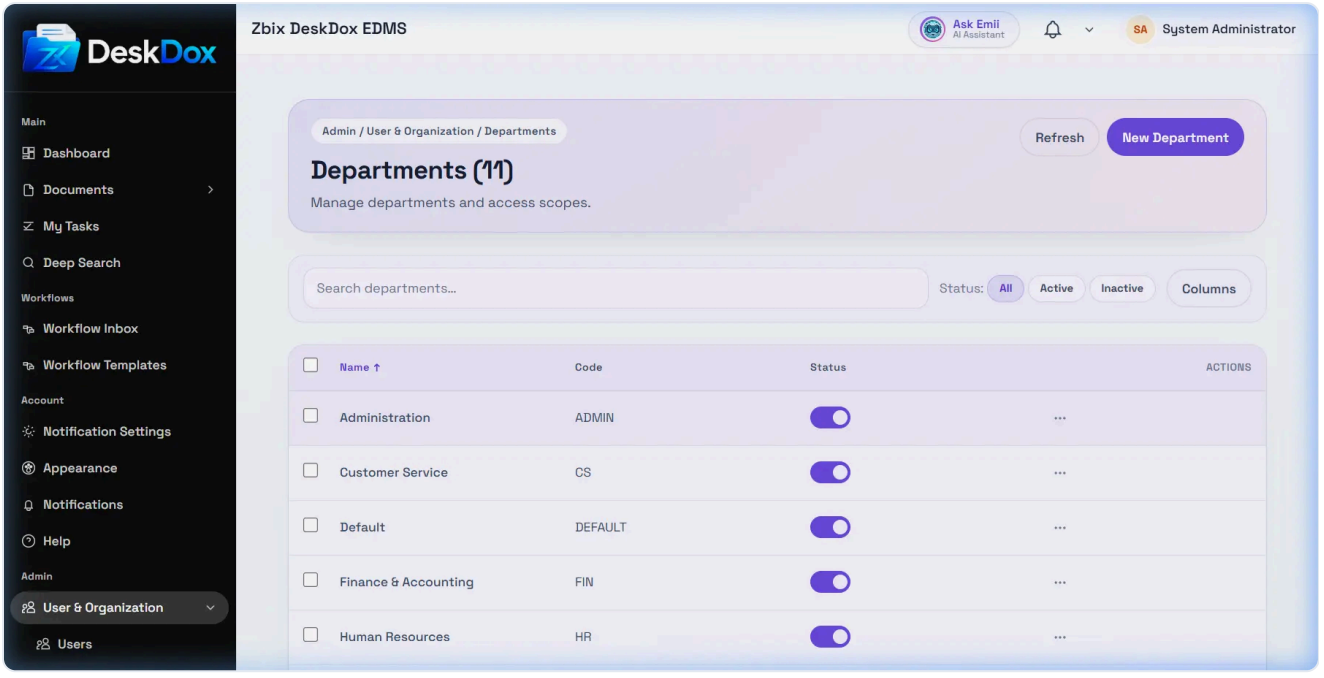
Sharing and Access Control · 1 min read · Reviewed 2026-05-14

Assign Users to Departments



Open `/app/admin/users`, create or edit a user, then choose the department from the `Department` dropdown. The browser-confirmed UI makes department mandatory for normal user creation.

DeskDox includes active non-`system_admin` users require a department at creation. DeskDox also blocks saving an active normal user with no department. A `system_admin` can be department-exempt.



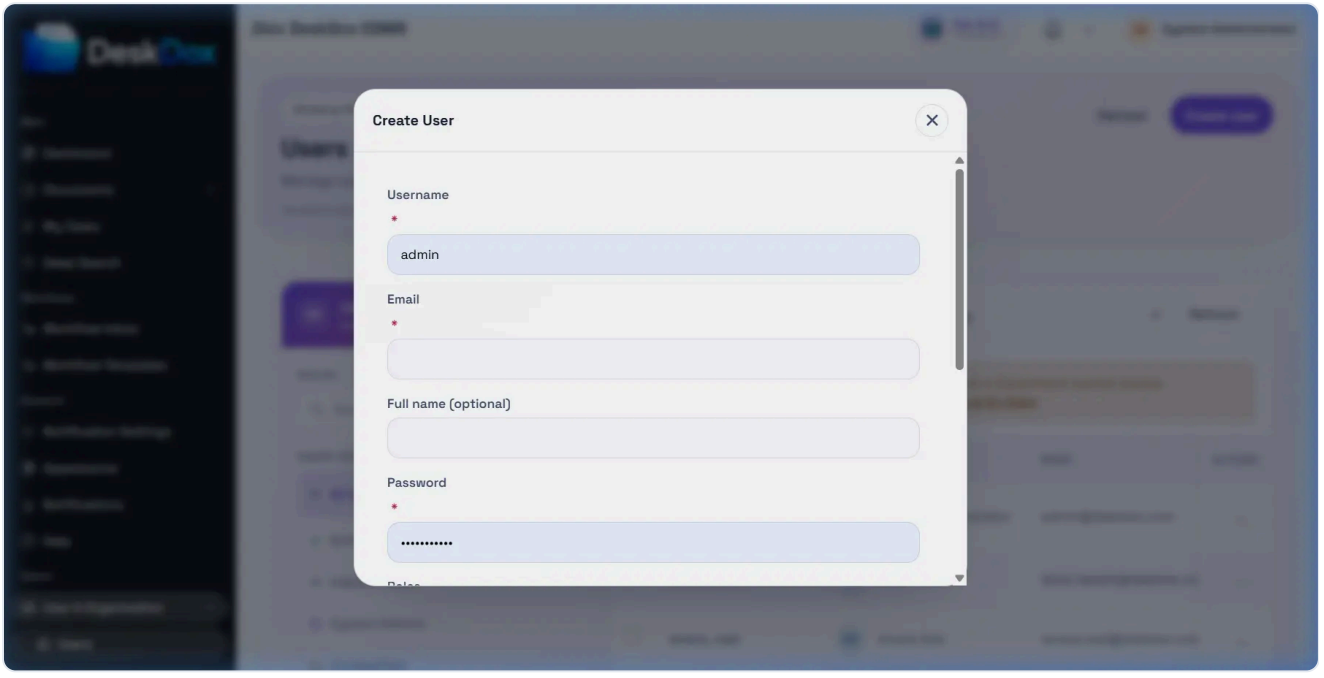
Changing a user's department can change what department-scoped folders or workflows they can access. DeskDox includes department membership participates in folder access logic, but exact folder results

depend on folder ownership, explicit folder permissions, document permissions, workflow assignment, and admin status.

If a new user has no folder access after creation, check that the selected department is active, the department owns or is granted access to the expected folders, the user's role allows the needed action, and the user is looking in the correct folder.

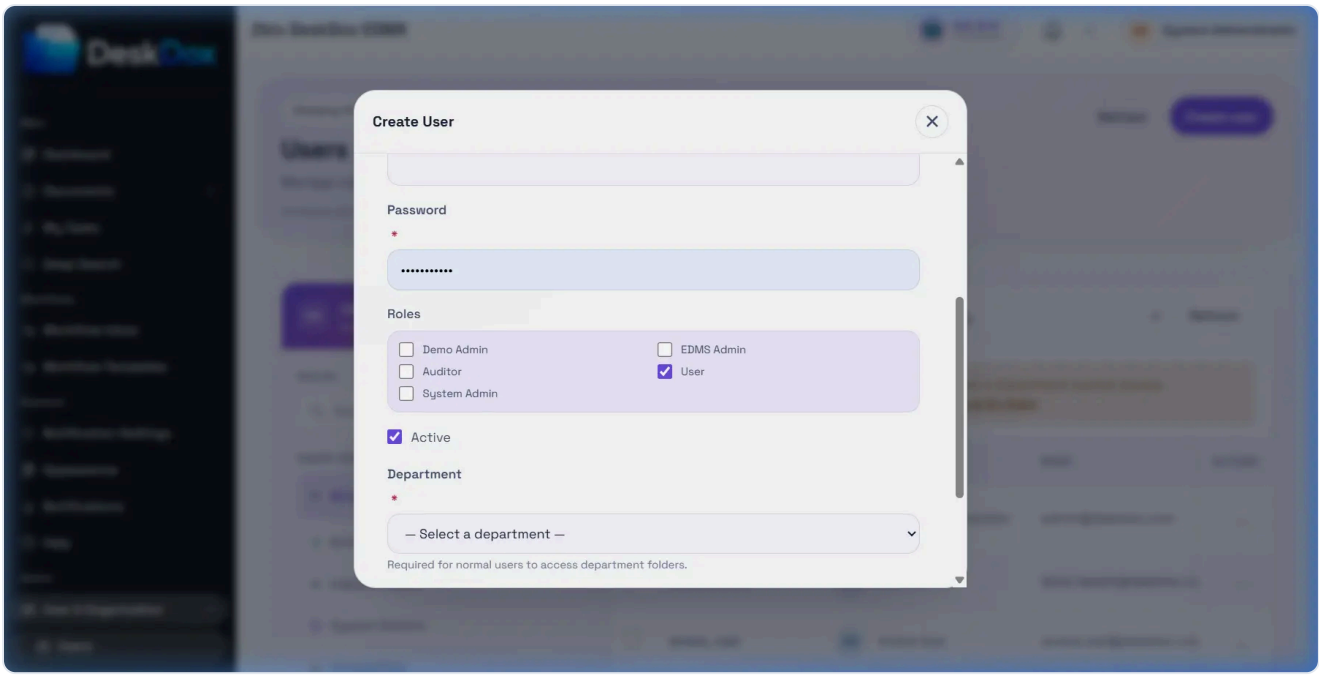
Sharing and Access Control · 2 min read · Reviewed 2026-05-14

Create or Edit a User

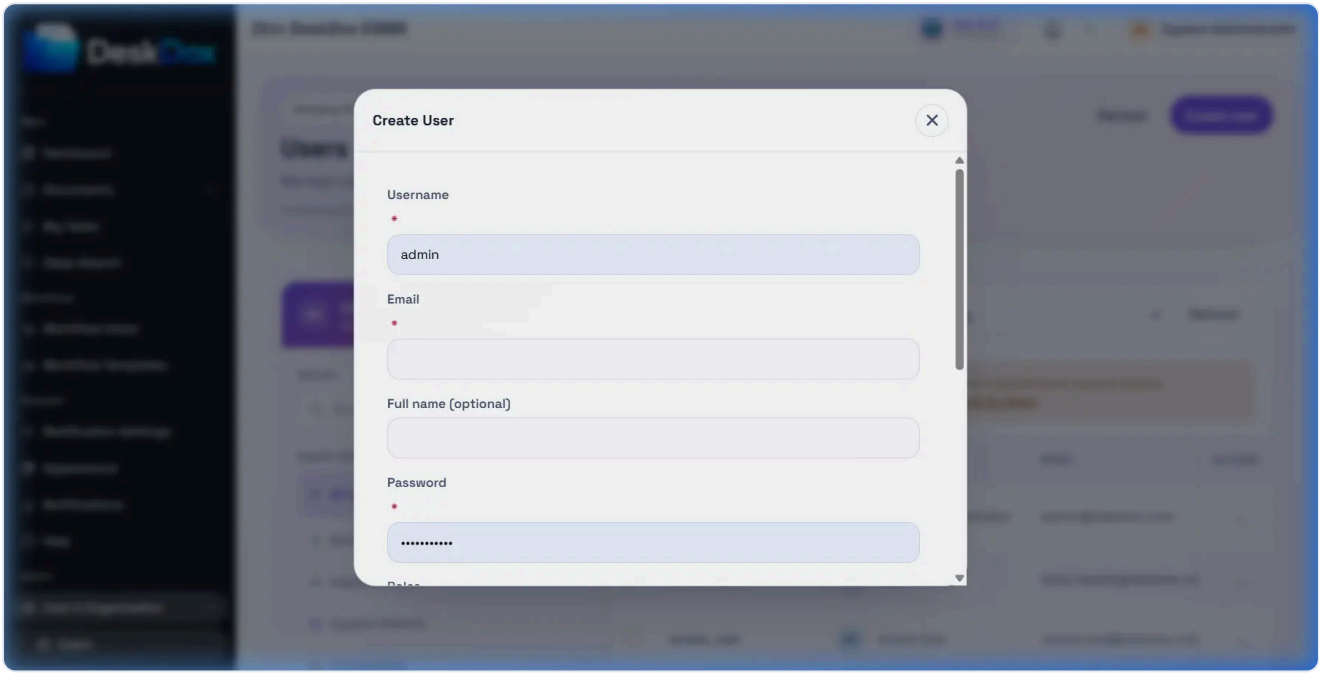


Open `/app/admin/users` and use `Create user` when it is visible. DeskDox includes that user creation is restricted to users with the required system administration or user-administration permission. Other admin users may be able to view or edit users depending on their user-admin permissions.

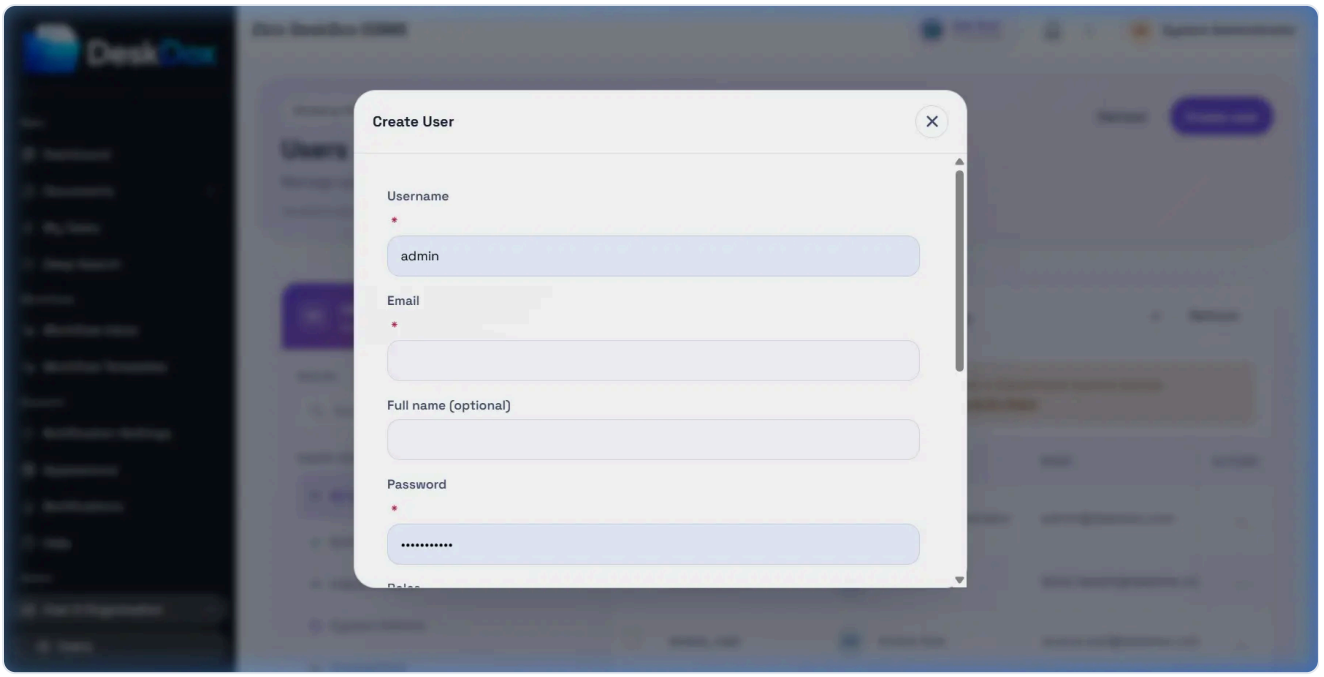
Required create fields in the UI include `Username`, `Email`, `Password`, roles, active status, and `Department` for normal users. DeskDox includes the system service also rejects creation of an active non-`system_admin` user without `primary_department_id`.



If `Create user` or `Save` fails, check required fields, email format, password length, duplicate username/email, selected role names, active status, and department assignment. The create form validates username, email, password, and department before sending the request.



Select the correct department from the department dropdown. The UI text says department is required for normal users to access department folders.

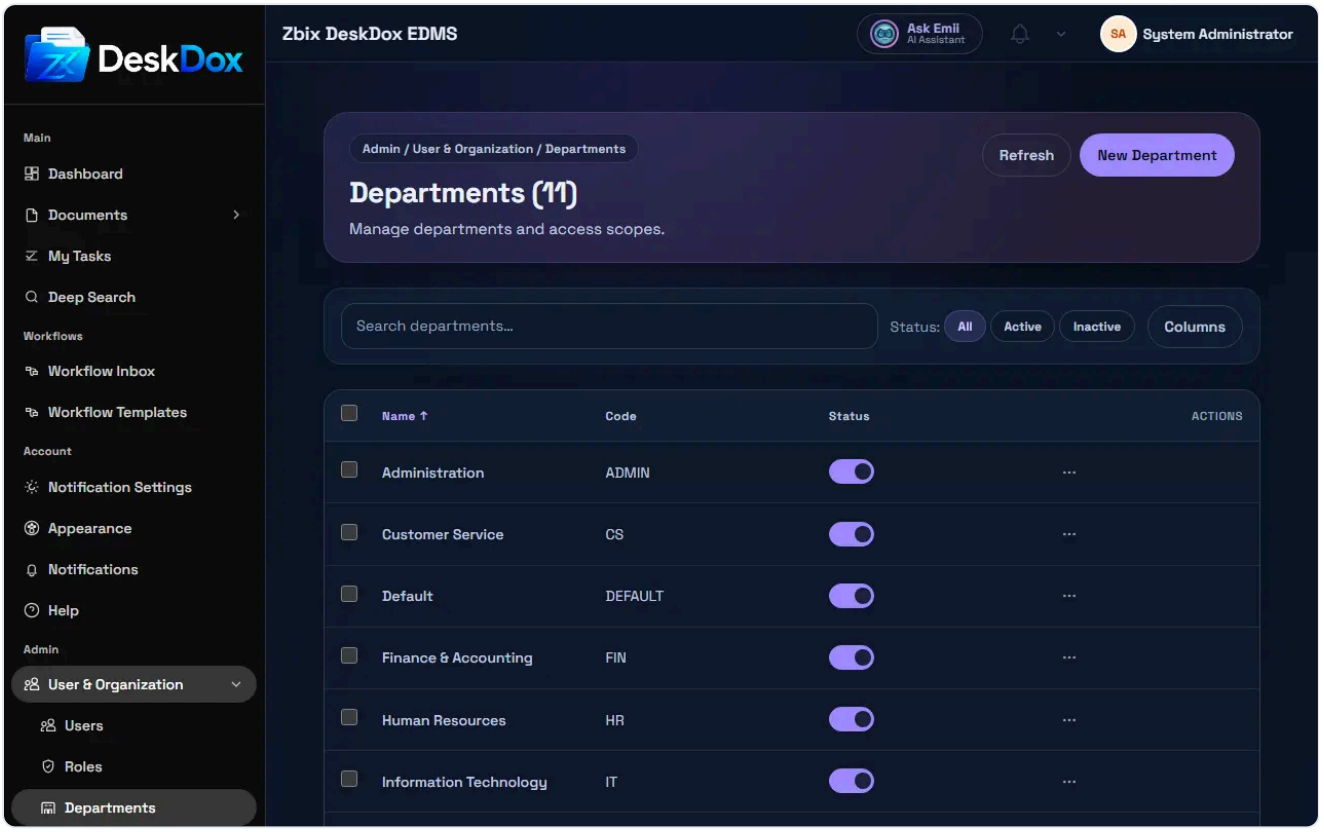


Roles are selected with checkboxes, so one user can have multiple roles. Use the least-privileged roles that cover the user's work.

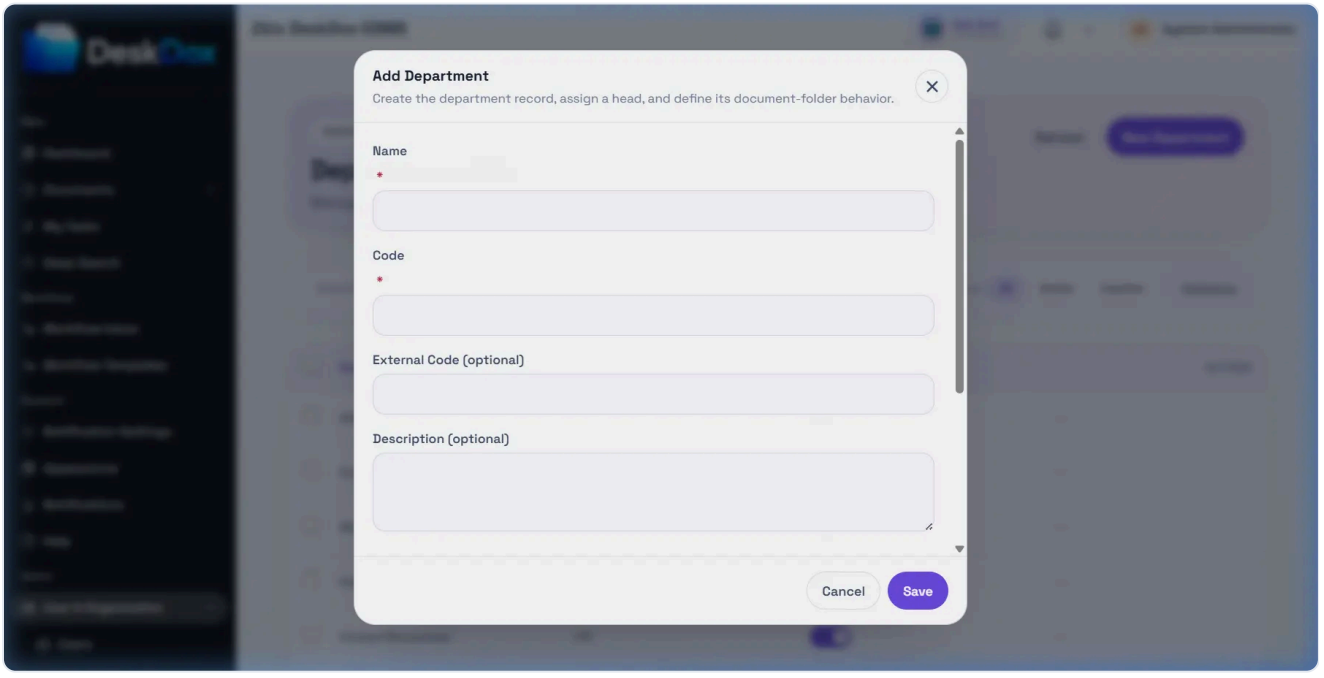
When editing a user, admins can change profile details, active status, roles, department, and manager when those controls are available. DeskDox includes an active normal user cannot have the department removed during save. Use `Cancel` to close without saving visible changes.

Sharing and Access Control · 1 min read · Reviewed 2026-05-14

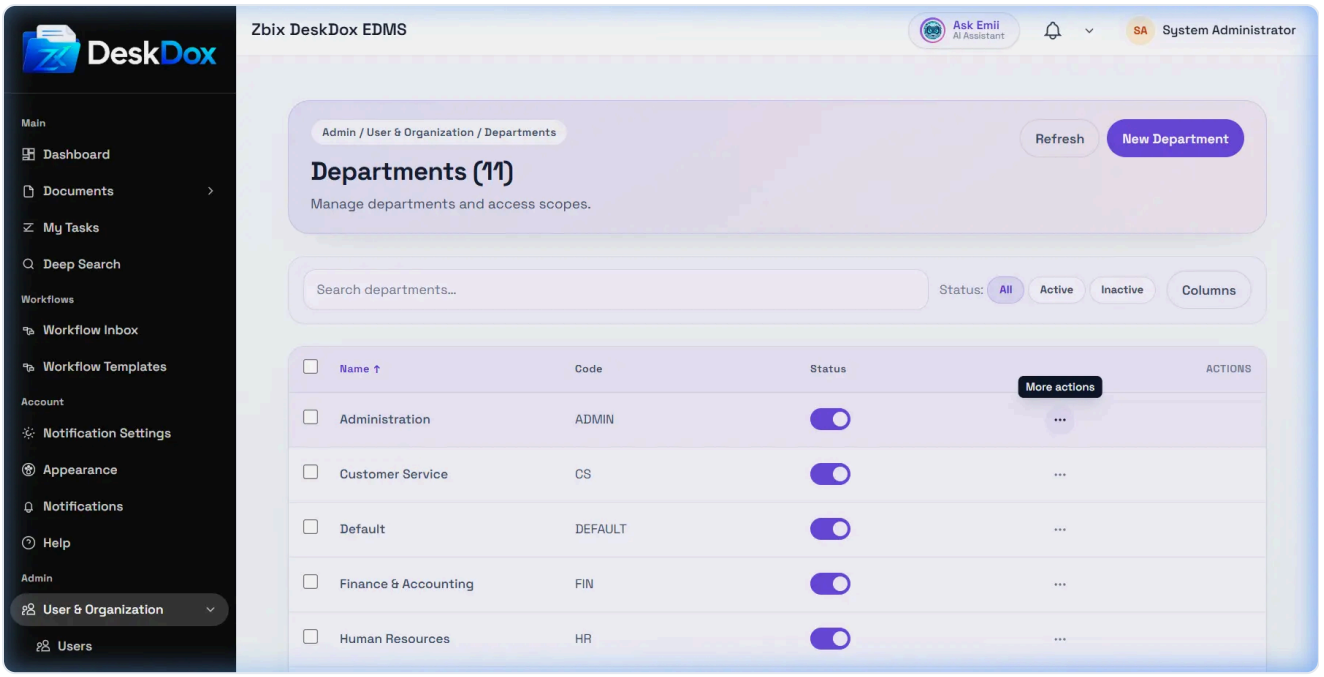
Departments List and Actions



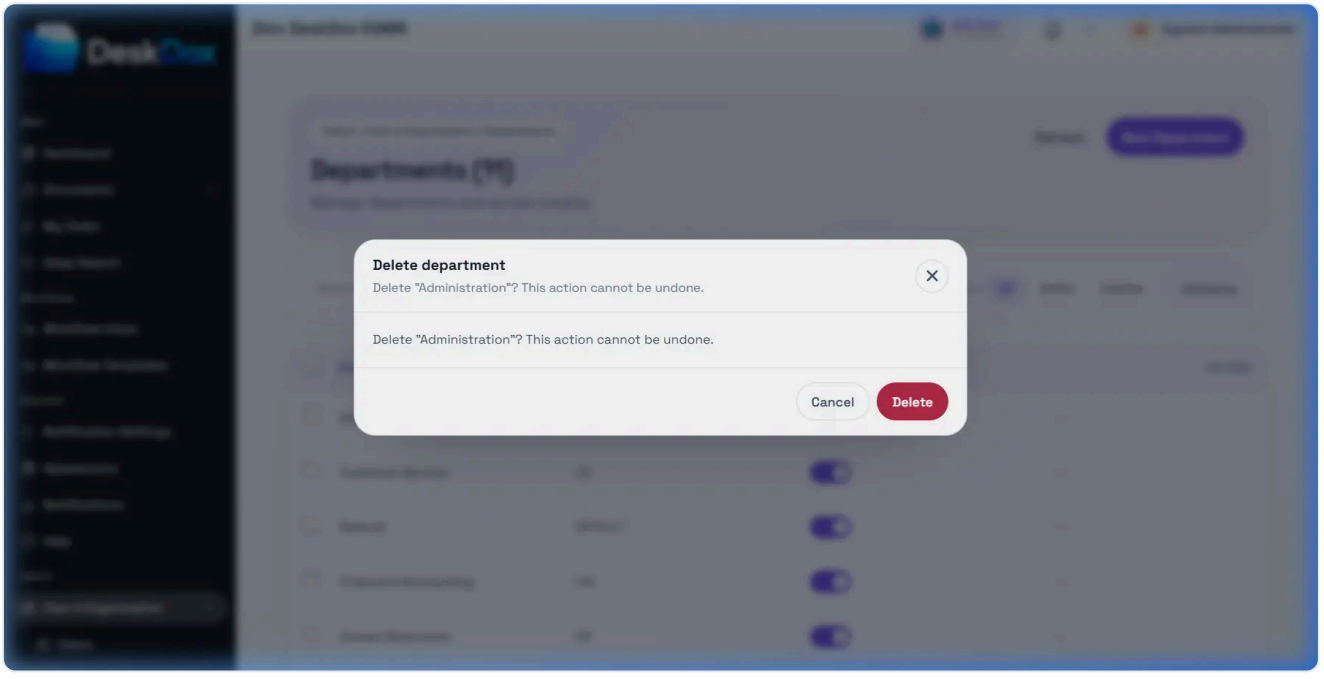
Open `/app/admin/departments` to view and manage departments. DeskDox includes search, active/inactive filtering, sorting, pagination, and admin-only access.



Use `Create Department` when visible to add a department. Depending on the form, fields can include name, code, external code, description, active status, folder options, and department head.



Use `Edit` to update department details. Use `Activate` or `Deactivate` to change status when available; DeskDox uses status updates.

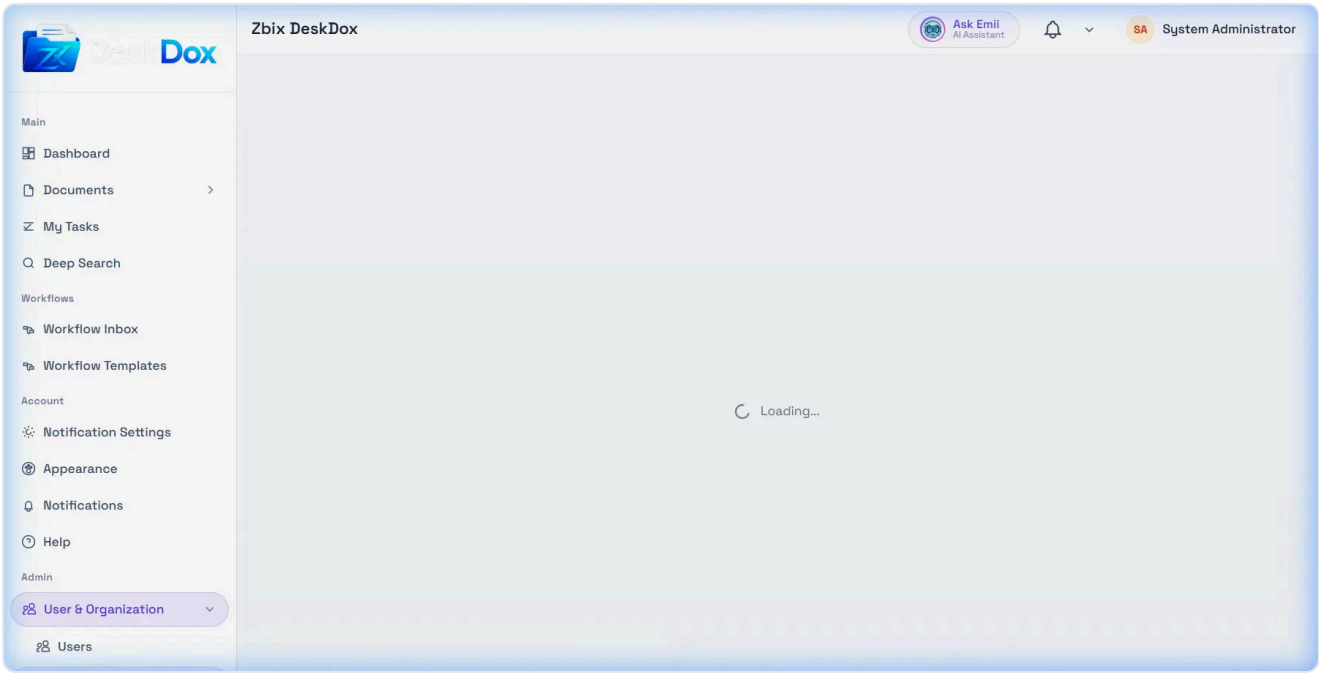


Use `Delete` only when the department is safe to remove. DeskDox includes department delete is blocked when users, folders, workflow steps, or workflow step templates still reference the department. If delete fails with "Department is in use", remove or reassign those references first.

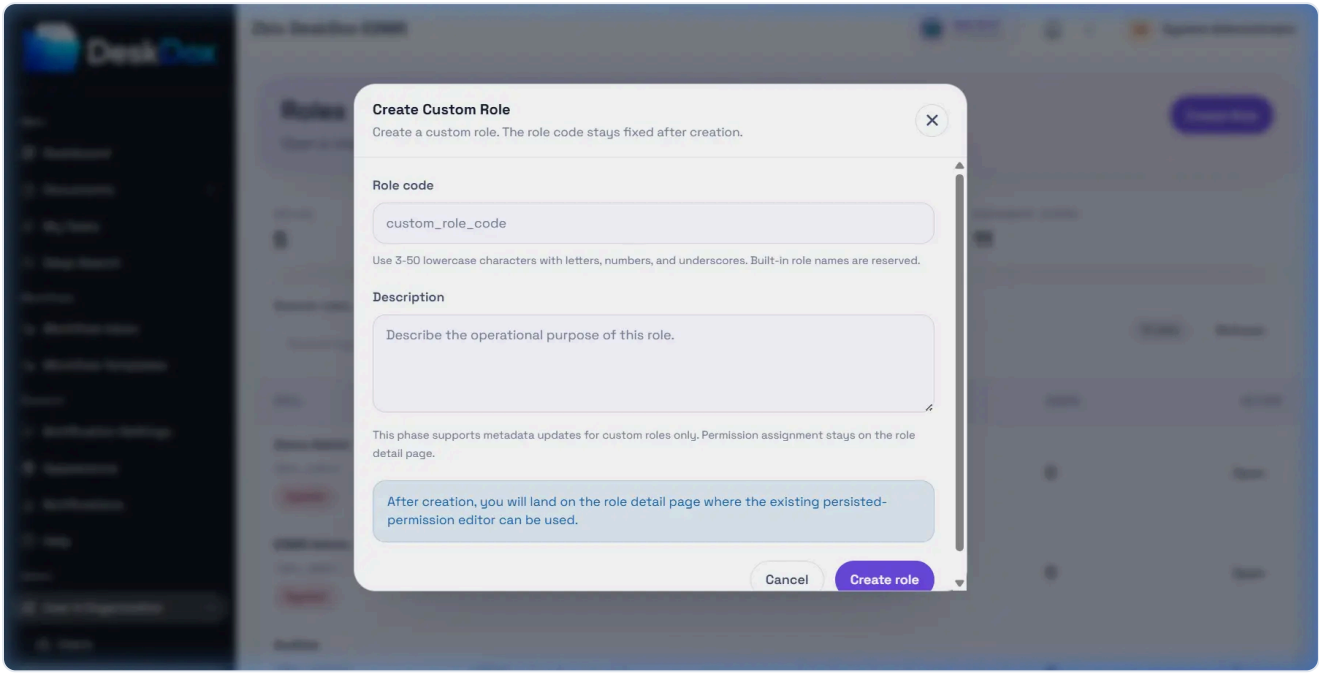
If you cannot see departments, ask an administrator to confirm your admin role. If the list is empty, create the first department before creating normal users who need department folder access.

Sharing and Access Control · 1 min read · Reviewed 2026-05-14

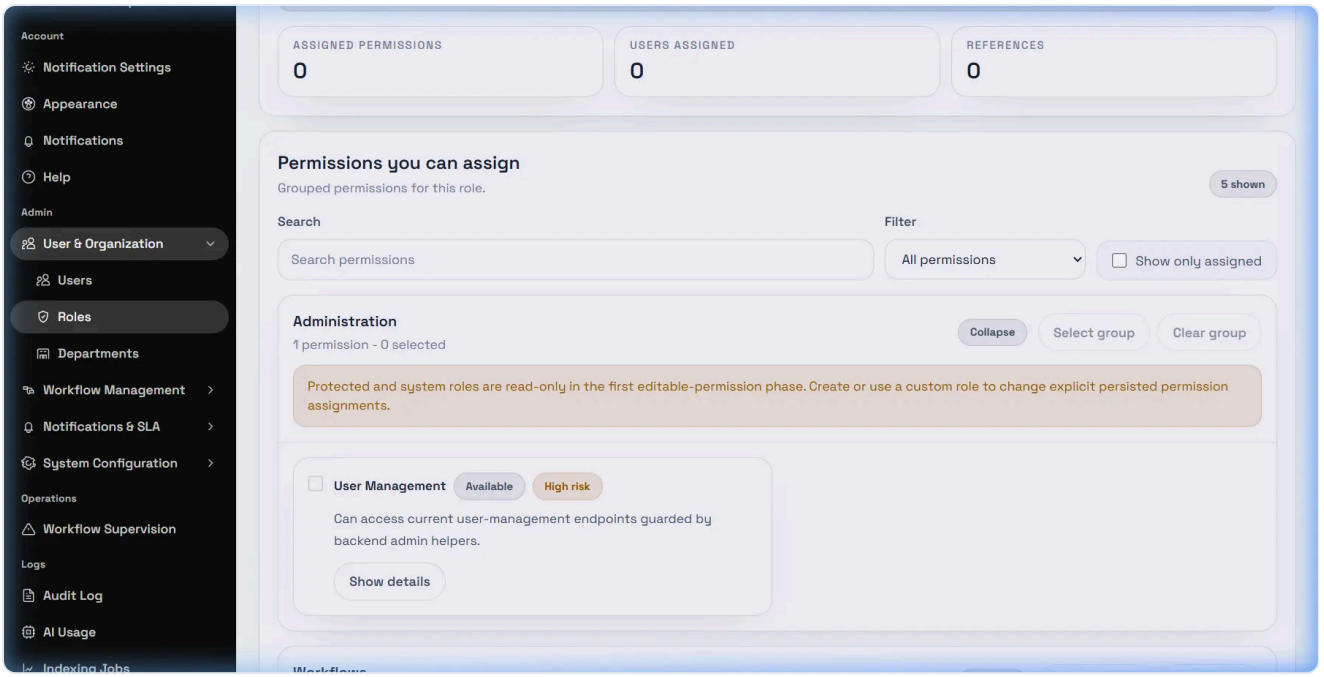
Roles List and Actions



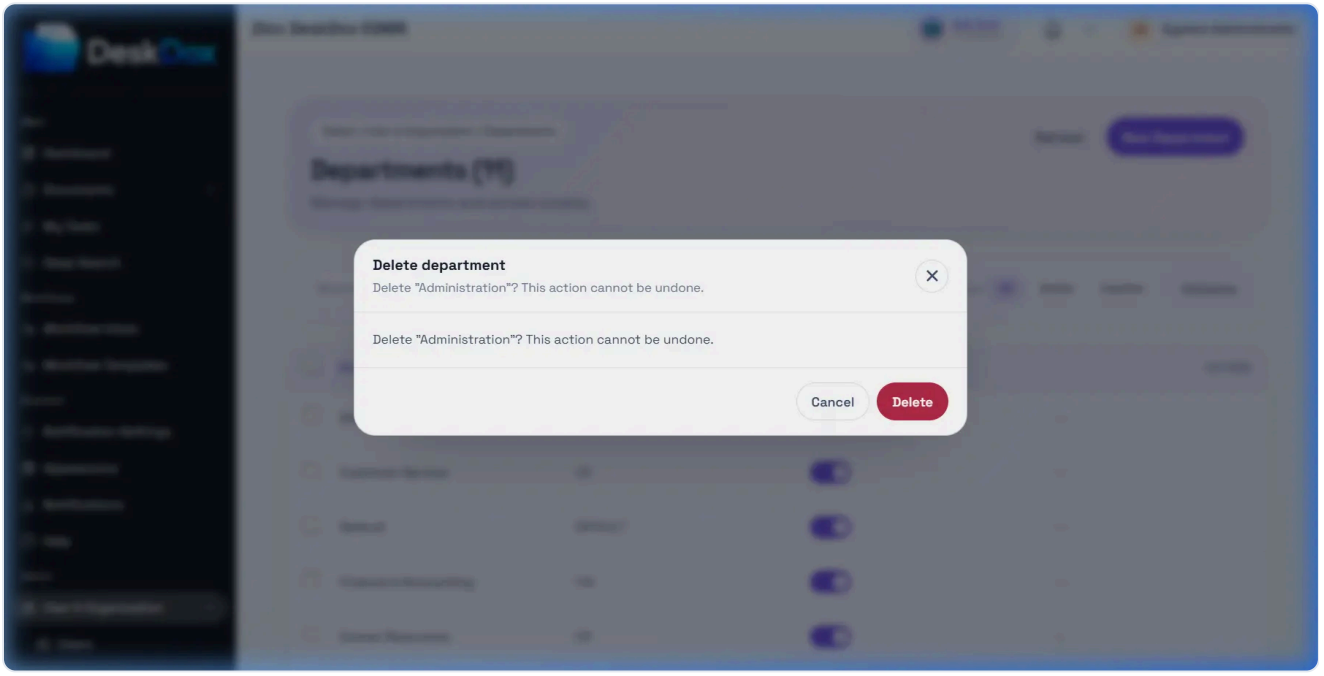
Open `/app/admin/roles` to view the role catalog. The list shows role name, description, assigned user count, and whether the role is custom, system, or protected.



Use `Create Role` to create a custom role when the action is visible. DeskDox includes custom role creation and validates that the role name is 3-50 characters, starts with a letter, and uses lowercase letters, numbers, and underscores. Reserved built-in role names cannot be reused.



Use `Open` to review a role. Use `Edit Details` when enabled to update custom role description. DeskDox includes built-in, protected, and system roles are immutable in the current custom-role lifecycle phase.



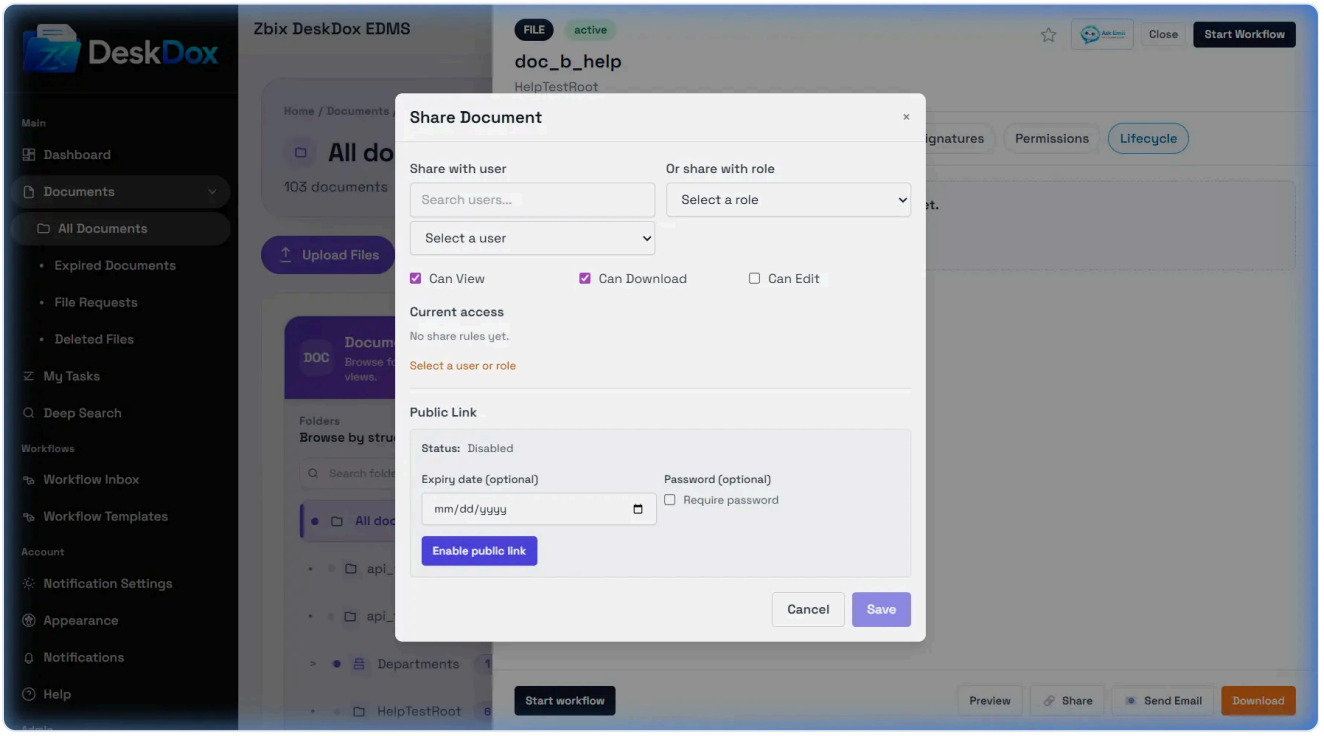
Destructive actions use confirmation prompts when they are available. Role delete or deactivate actions may be unavailable because roles can still be referenced by document shares and workflow assignee fields. Do not assume role delete is available unless the current UI exposes it in your environment.

Sharing and Access Control · 1 min read · Reviewed 2026-05-13

Share a Document

What this helps you do

Use internal sharing to give another DeskDox user access to a document without moving the document to another folder.



Share from a row or drawer

Open the row action menu and choose `Share`, or open the Document Detail Drawer and click `Share`. In the Share Document modal, select the user, choose the access level, and save.

`Can View` allows the user to see and preview the document. `Can Download` allows local download in addition to viewing. `Can Edit` allows permitted metadata or document edits where system policy allows it. Use the least access needed.

Current access and removal

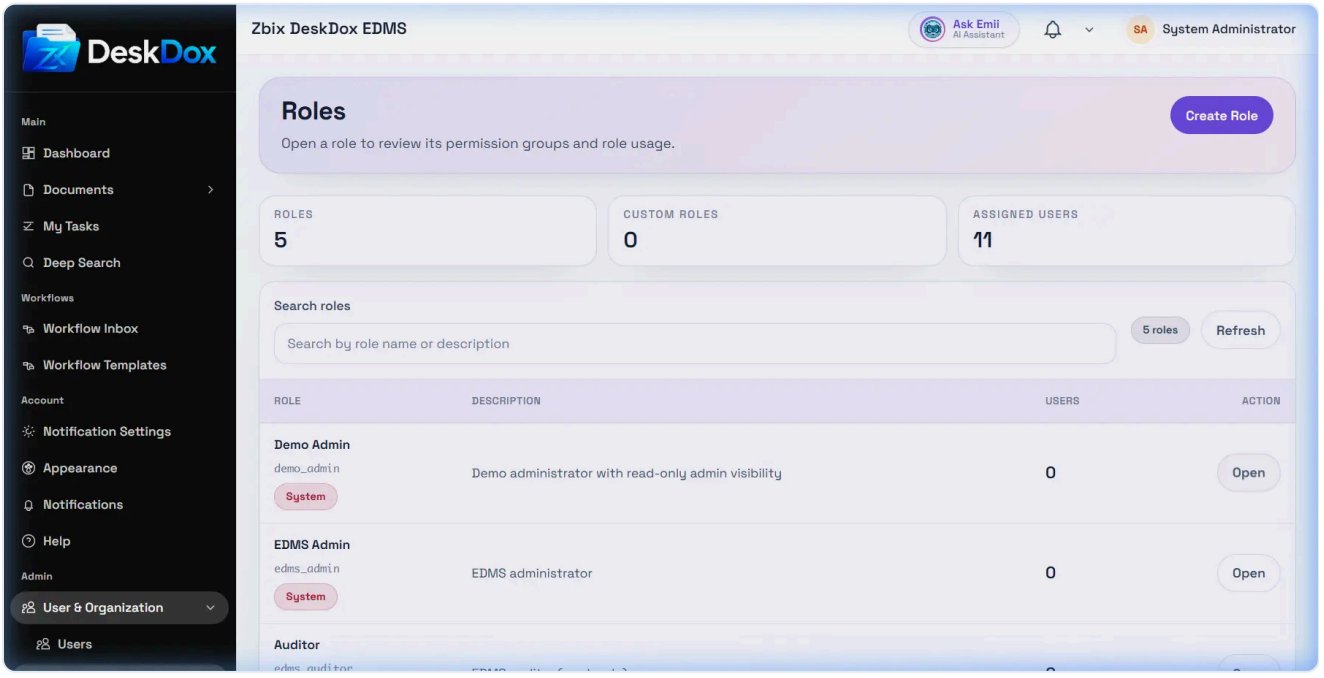
The Current Access list shows users who have direct access from sharing. Use `Remove` or `Revoke` if available to remove that direct share. A user may still see the document if they also have access through folder permission, ownership, workflow assignment, administrator rights, or another share.

Security and audit notes

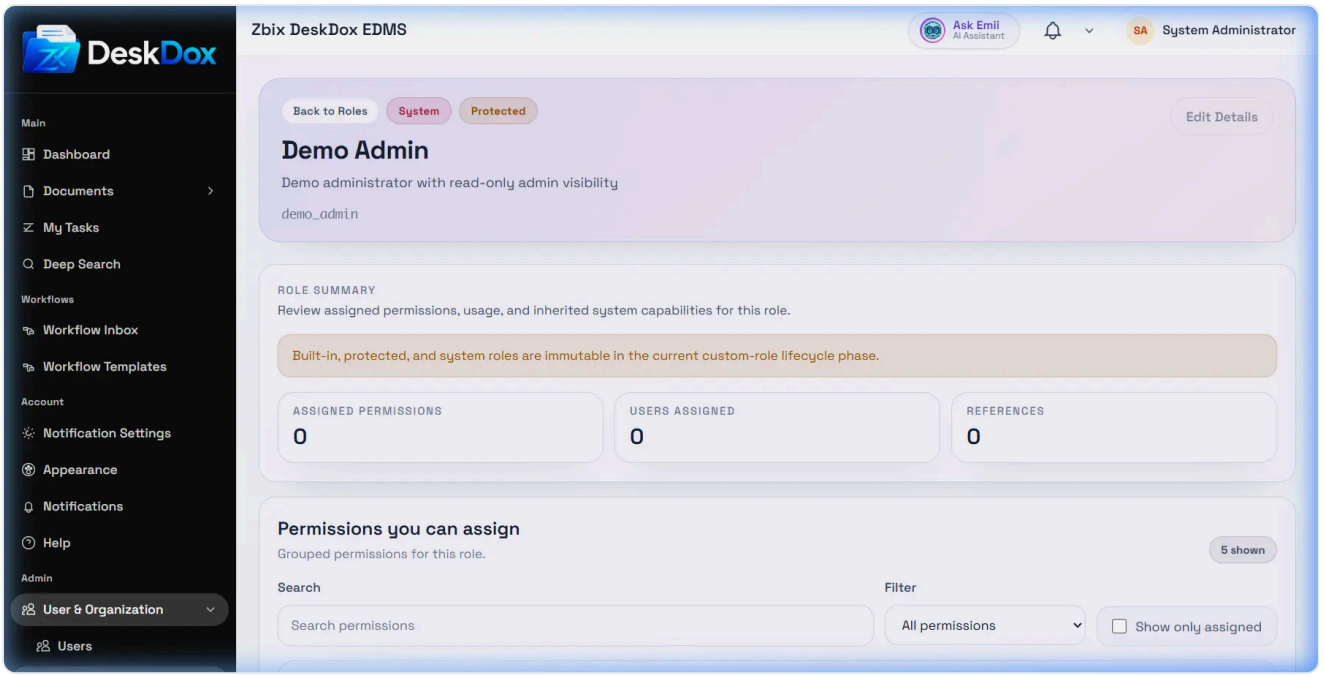
Internal sharing is different from a public link. Internal sharing requires the recipient to sign in and is the preferred option for organization users. Sharing and access changes are audit-relevant events.

Sharing and Access Control · 1 min read · Reviewed 2026-05-14

Role Permission Matrix



Open a role from `/app/admin/roles`, then use `/app/admin/roles/:id` to review and update permissions. The user list includes the permission matrix and DeskDox uses assignable permission groups, risk levels, selected permissions, and save confirmation for high-risk changes.



Permissions are grouped by functional area. Use `Search permissions`, `All permissions`, group filters, `High risk only`, `Currently assigned`, and `Show only assigned` to find permissions. Select or clear checkboxes, then use `Save changes` when it appears.

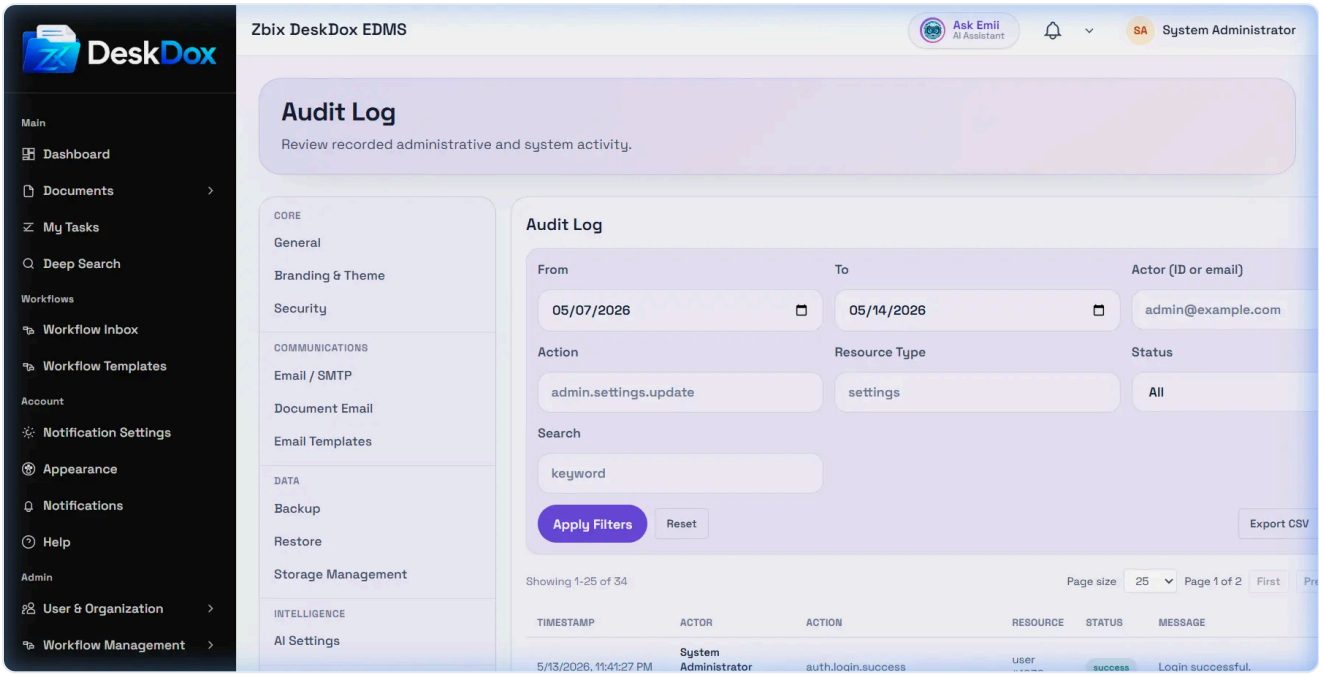
DeskDox includes workflow permissions including `workflow.template_management` and `workflow.stats_view`. Lifecycle policy management currently follows the workflow template management permission. Upload control may be affected by folder permission and document permissions, not only the role matrix; folder access also controls upload actions.

Treat user management, department management, role permissions, workflow administration, lifecycle policy management, delete, and admin permissions as high-risk. Apply least privilege and confirm affected users after saving.

UI visibility and system service authorization should both be enforced. If a role still cannot see a feature after permission changes, check whether the user actually has the role, whether the feature is license/configuration gated, whether the user needs a refreshed session, and whether folder/document/workflow/department scope also blocks the feature.

Sharing and Access Control · 1 min read · Reviewed 2026-05-14

Access Control Audit Log



Open `/app/admin/system/settings/audit` to review the security audit log when your account has permission. The user list includes the route and screenshot.

DeskDox includes user creation, protected user updates, bulk user status changes, bulk role changes, reset-related audit/notification behavior, and department deletion create audit or admin-action records. User-specific audit is also available from the user row action when visible.

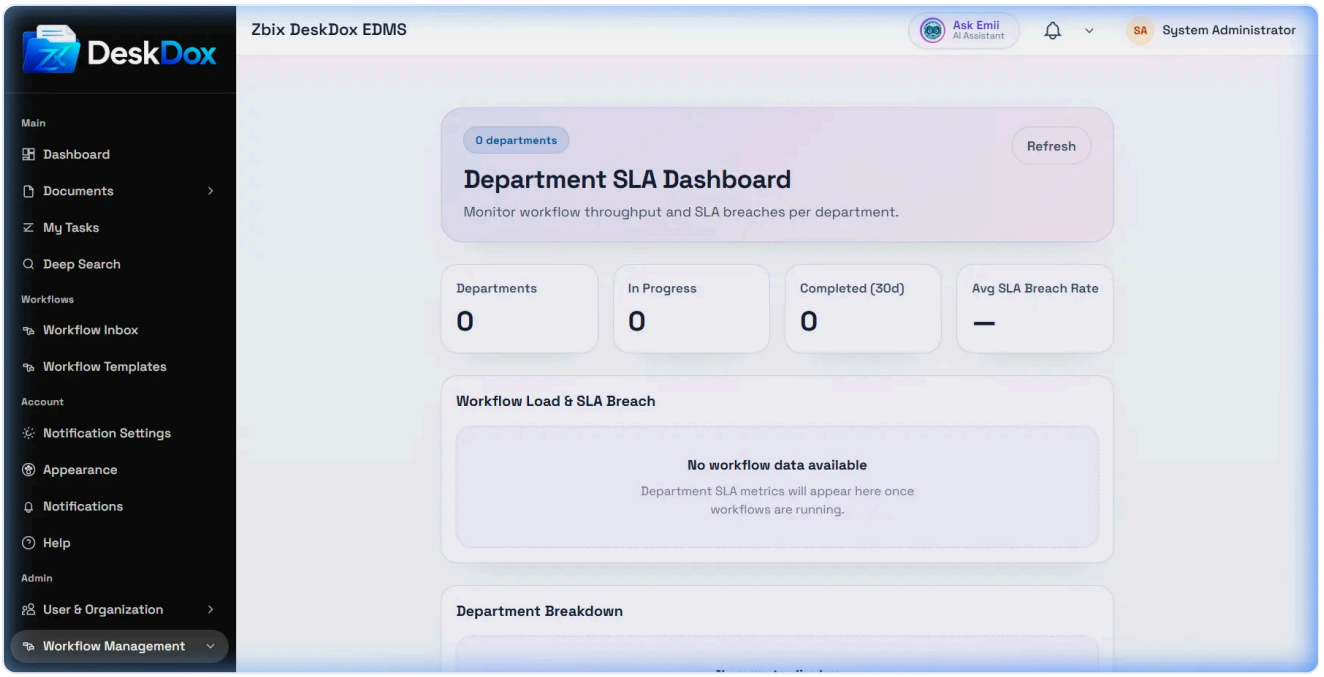
Role changes are partly source-code confirmed: custom role creation, role metadata updates, and role permission assignment updates use admin role endpoints and should be inspected through the security audit log if audit entries are present in your deployment. Do not assume every displayed field change appears unless the audit event is visible.

Admins can inspect who performed an action, what resource was affected, timestamps, and available metadata. If an expected event is missing, check the date range, filters, user-specific audit view, tenant/environment, and whether that exact action currently writes an audit event.

Sharing and Access Control · 1 min read · Reviewed 2026-05-14

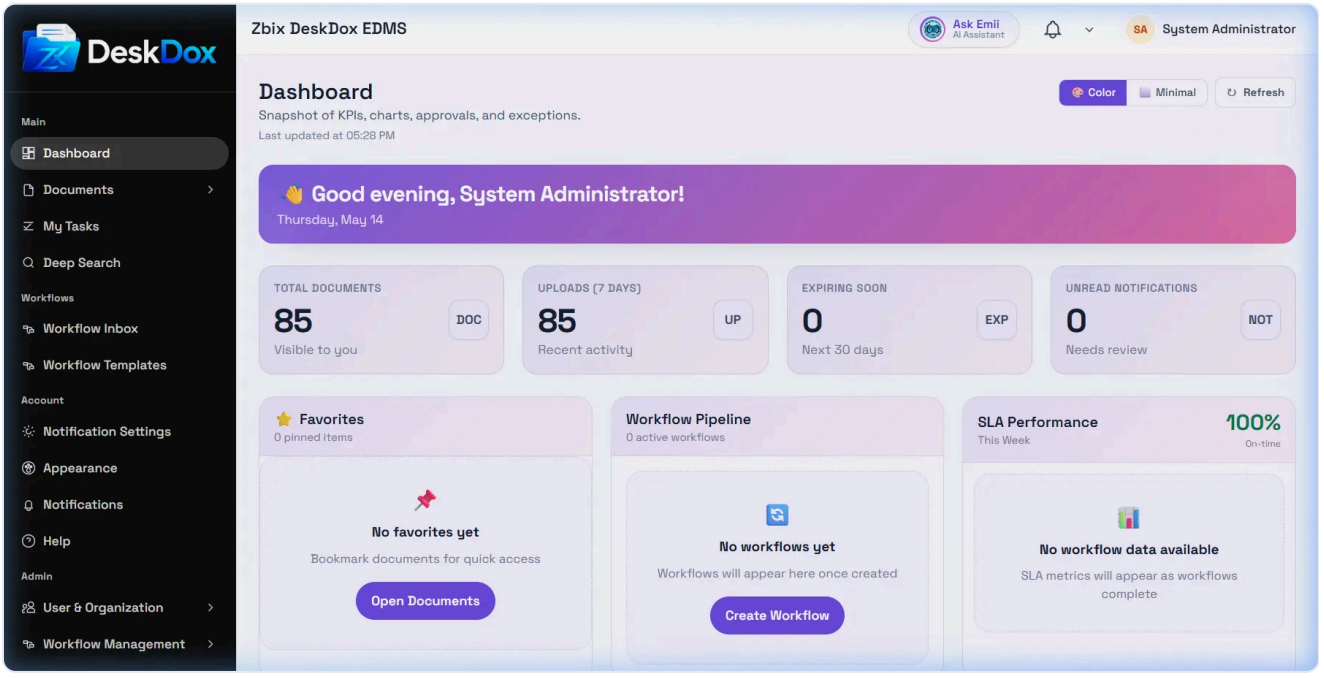
Department SLA Dashboard

Use `/app/admin/workflows/departments` to monitor department-level workflow throughput and SLA breach performance.



What the dashboard shows

DeskDox includes summary cards for `Departments`, `In Progress`, `Completed (30d)`, and `Avg SLA Breach Rate`. The chart is labeled `Workflow Load & SLA Breach`, and the table includes `Department`, `In Progress`, `Completed (30d)`, `Rejected (30d)`, `Avg Completion`, and `SLA Breach`.



An SLA breach means a workflow item missed the configured SLA target. The department dashboard groups those results by department and reporting window, so its values may differ from an individual task due date or a workflow template setting.

Empty or unexpected data

`No workflow data available` means department SLA metrics are not available for the current data set. Check whether workflows are running, departments are assigned, SLA settings exist on workflow steps, analytics have refreshed, and your role can view the dashboard.

Sharing and Access Control · 2 min read · Reviewed 2026-05-13

Manage Public Links

What this helps you do

Use a public or secure link when a document must be viewed outside normal internal DeskDox user access.

Public link controls

Open the document's sharing controls and check the public link status. If your permissions allow it, enable or disable the link, copy it, open it for verification, set or review expiry, rotate it when available, and configure a password when your tenant supports password-protected links.

Public link vs internal share

Internal sharing gives access to signed-in DeskDox users and is usually best for employees. A public link is intended for controlled external access and may work for recipients who do not have DeskDox accounts, depending on configuration.

What recipients may see

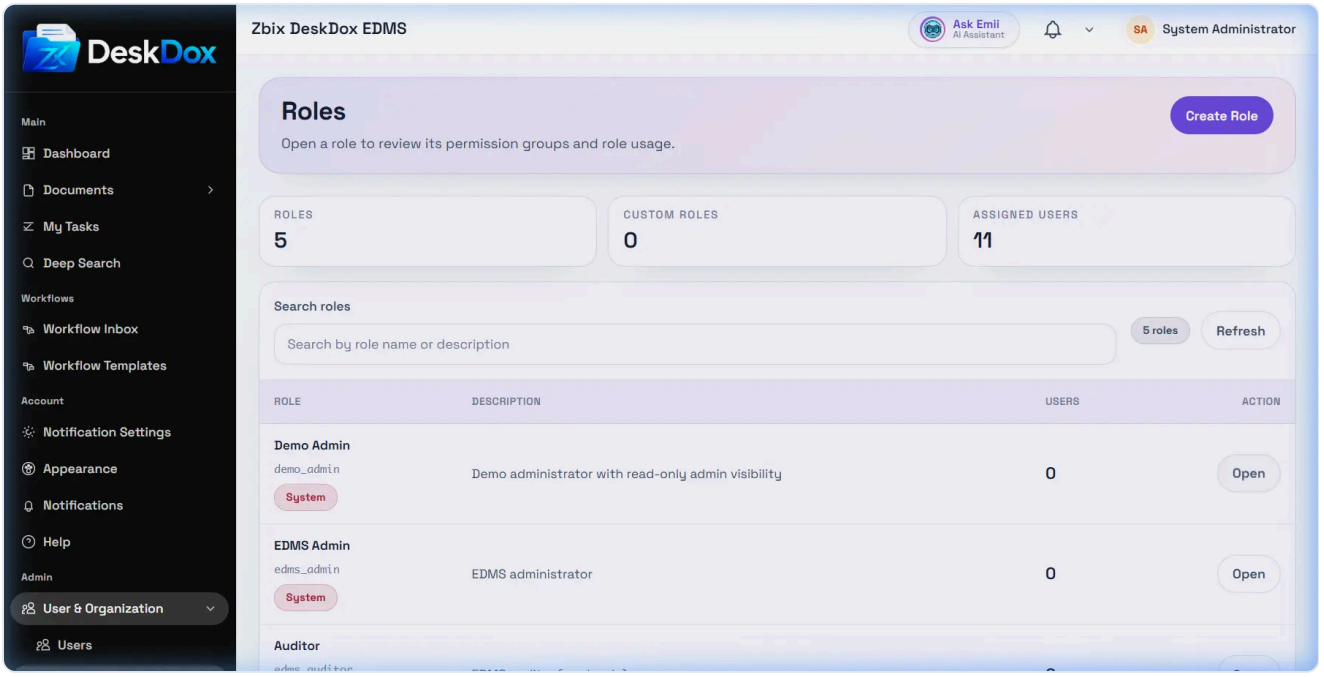
When a recipient opens a public link, the experience depends on tenant configuration. They may see a public document viewer, a download page, a password prompt, an expiry/error message, or a sign-in requirement. Test the link before sending sensitive or time-critical documents.

Security guidance

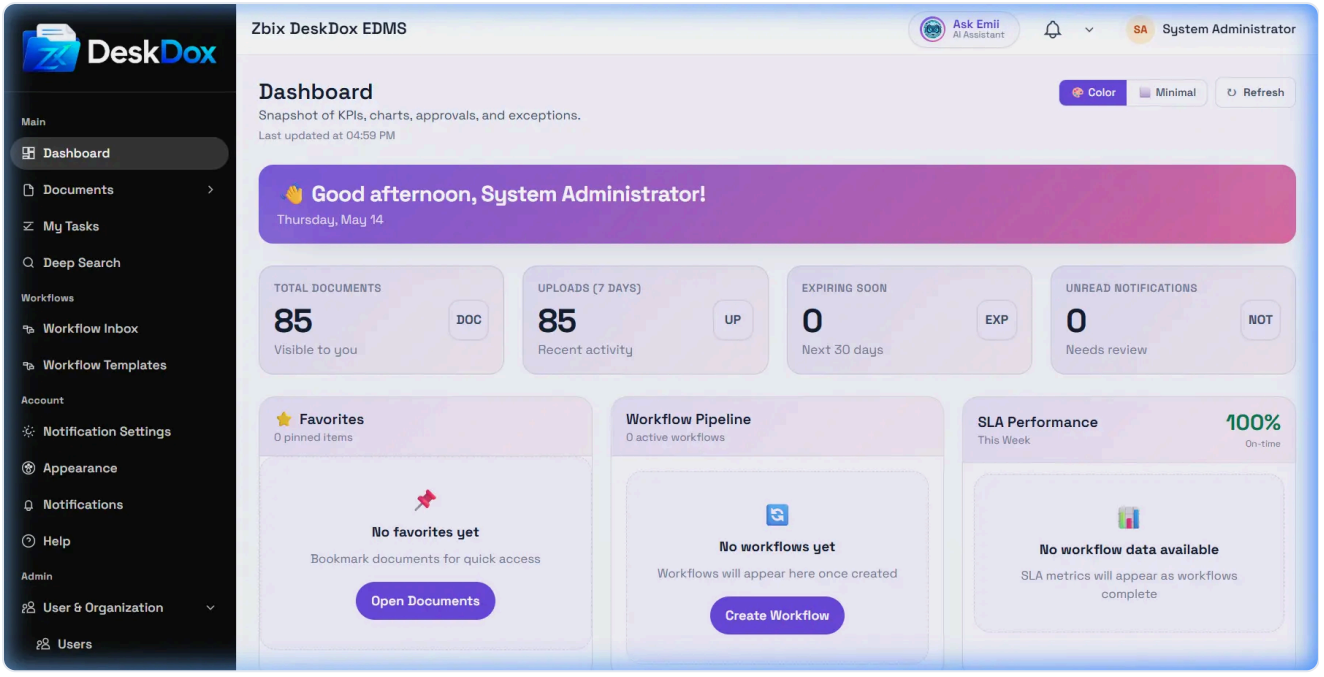
Use public links only when external access is necessary. Avoid public links for highly confidential documents unless your policy allows it and the link has expiry, password protection, and audit review. Disable or rotate a link if it was sent to the wrong recipient or should no longer work. Link events are audit-relevant.

Sharing and Access Control · 1 min read · Reviewed 2026-05-14

Permission-Based Visibility



DeskDox hides or disables menus, buttons, tabs, and row actions when your account lacks the required role, permission, department scope, folder access, document permission, workflow assignment, lifecycle permission, or feature configuration.



Common examples:

- `Upload Files` can be hidden when your role or destination folder does not allow upload.
- `Admin` settings can be hidden when you are not an admin user.
- `Manage Access` can be hidden when you cannot manage permissions for that folder or document.
- `Workflow Templates` or workflow admin screens can be hidden when you lack workflow administration permission.
- `Lifecycle Management` can be hidden when lifecycle administration follows workflow/admin permission gates and your role does not satisfy them.
- `Edit` or `Delete` can be hidden or disabled because of role, folder/document permission, lifecycle state, workflow state, ownership, or safety rules.

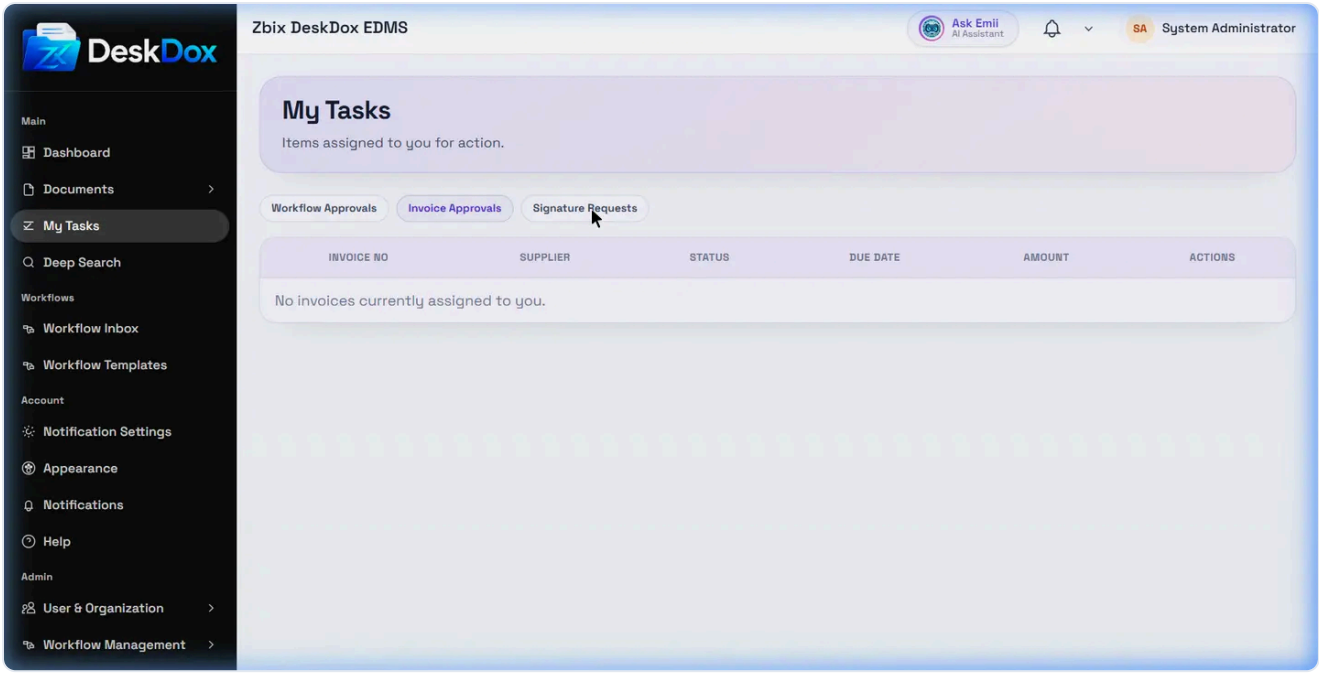
UI visibility is not the same as system service authorization. If an action appears but fails with forbidden or unauthorized, the system service rejected the operation. Ask an administrator to check your roles, role permission matrix, department, folder/document access, workflow assignment, and feature/license configuration.

Sharing and Access Control · 2 min read · Reviewed 2026-05-14

Signature Requests User Guide

What this helps you do

Find signature requests assigned to you and understand how signatures can relate to workflow tasks.



Signature Requests screen

The page shows `Signature Requests` as a tab on `My Tasks` at `/app/invoices/my-tasks?tab=signatures`. Use this tab to find pending signing work when the feature is enabled and visible to your account.

Signature requests are used when a document needs one or more users to sign. Signature statuses can include `pending`, `requested`, `in_progress`, and `completed`, and pending requests can show progress such as "1 of 2 signed" when visible.

Empty state

When no signature requests exist, the page explains that the screen shows a green checkmark and the text: "You have no pending signature requests".

Signing actions

The page can show a `Sign Now` button that opens a signature modal where users can draw, type, or upload a signature. Use signing actions only when they are visible and the request is assigned to you.

Signatures can also block workflow steps. The page can show the message "Signature required before you can complete this step." when a required signature has not been completed.

Relationship with document signatures

Signature requests are the task-side view for signing work. A document may also show signature information in its `Signatures` tab depending on document access, signature configuration, and permissions.

Why signature requests may not appear

A request may be missing because it is assigned to another signer, already completed, filtered out, not yet requested, linked to a document you cannot access, or hidden by configuration or permissions. Refresh the page after signing or after an administrator changes assignments.

Related Emii questions

- "Where can I see signature requests?"
- "Why can't I see a signature request?"
- "What does pending signature mean?"
- "How are signatures related to workflow?"

- "Why are signature requests empty?"

Sharing and Access Control · 2 min read · Reviewed 2026-05-13

Understanding Activity and Audit for Sharing

What this helps you do

Task guidance for tracking document sharing and access changes in the Activity and Audit logs.

Tracking Sharing Events

To ensure security and visibility, all changes related to document sharing and access are recorded in the system.

You can view these events in two places on the document screen:

1. **Activity Tab:** Look under **Activity → All** or filter specifically by **Activity → Permissions** to see access-related actions.
2. **Audit Tab:** This tab provides a formal, uneditable log of all compliance and security events.

Types of Logged Events

When users interact with document sharing features, the following events may be recorded:

- **Share granted (`document_share_granted`):** Logged when a user or role is newly granted access to the document.
- **Share changed (`document_share_changed`):** Logged when an existing user's access level (e.g., from View to Download) is updated.
- **Share revoked (`document_share_revoked`):** Logged when a user's or role's access is removed.
- **Email sent (`document_email_sent`):** Logged when the document or a secure link is delivered via the Send Email feature (if the email flow is implemented).
- **Public link created (`document_share_link_created`):** Logged when a public sharing link is first enabled.
- **Public link rotated (`document_share_link_rotated`):** Logged when a public link is rotated, invalidating the old link and creating a new one.
- **Public link revoked (`document_share_link_revoked`):** Logged when a public link is completely disabled.

By reviewing these logs, you can always see who was granted access, when it happened, and who authorized it.

Sharing and Access Control · 3 min read · Reviewed 2026-05-13

Understanding Document Permissions

What this helps you do

Task guidance for understanding how document permissions are structured and displayed.

Who can use it

Any user can use this article to understand visible access. Administrators, owners, and access managers can use it to diagnose why a document is visible or hidden.

Required permissions

You need document view access to inspect basic document details. Full permission breakdown may require owner, admin, or access-management permission.

Overview of Document Access

The **Document Permissions** tab provides a detailed breakdown of who can access a document and why. It is no longer a replica of the folder permissions, but instead specifically details document-level access.

The Permissions tab separates access into several categories:

1. Direct Document Access

This section displays users who have document-level access assigned to them.

- **View only:** The user can read the document.
- **Download:** The user can view and download the document.
- **Editor:** The user can edit the document metadata (if enabled and enforced by system policy).

2. Document Shares

When a document is shared using the **Share Document** action, those shares appear here. The system displays the real names of the users or roles (rather than showing "Unknown" or User IDs). These entries can be managed or revoked from the Share Document modal.

3. Inherited Folder Access

This section shows access that users have inherited from the folder containing the document.

- **Read-only view:** Inherited folder access is displayed as read-only in the document permissions panel.
- If access is inherited from a folder, you cannot revoke it here. You must manage it from the folder permissions instead.

4. Workflow Access

If the document is part of an active workflow, workflow-related access is displayed here.

- This section is read-only.
- To manage workflow access, you must use the workflow assignment or supervision tools, not the document permissions screen.

5. Link/Email Sharing

This section details access granted via links.

- Shows public links and secure email-link access.
- Public links can be enabled, disabled, copied, opened, or rotated.
- If a link is disabled or expires, it will immediately stop working.

Delete permission rule

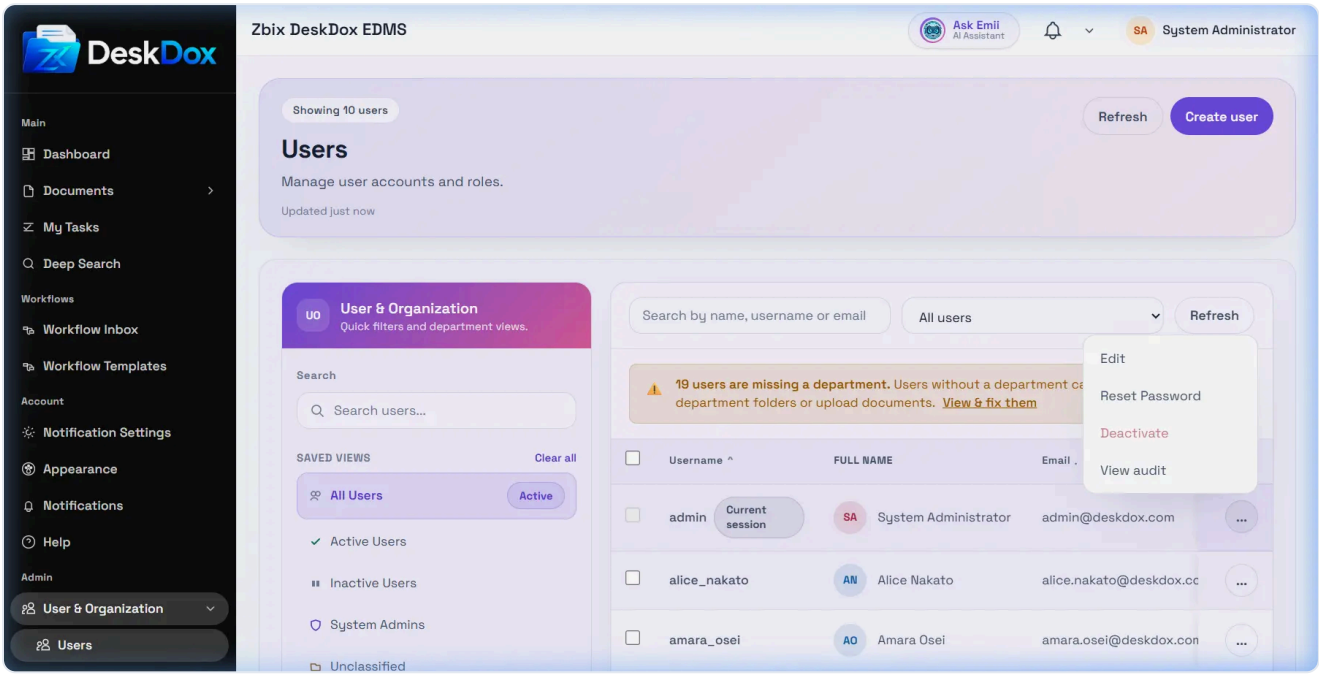
Edit access should not be treated as delete access. Delete should require explicit delete, owner, or administrator permission if DeskDox permission enforcement is configured correctly.

Related Emii questions

- "Why can this user see a document?"
- "Does edit access allow delete?"
- "What is inherited folder access?"
- "Why can't I remove an inherited permission?"

Sharing and Access Control · 2 min read · Reviewed 2026-05-14

User Status, Password, and Access Actions



User access actions are admin-only. On `/app/admin/users`, the user list includes row actions for `Deactivate` and `Reset Password`; DeskDox also supports active status updates and password reset.

Use `Deactivate` or clear `Active account` to make an account inactive. Use `Activate` or turn `Active account` back on to restore the account, subject to admin safety checks. DeskDox includes safety enforcement to avoid unsafe admin-account changes.

Use `Reset Password` to set a provided or generated temporary password. DeskDox includes DeskDox hashes the new password and enqueues a password reset email when the user has an email address and the email queue/service is configured. If email delivery is not configured or fails, the reset can still be saved while delivery may not occur.

DeskDox can queue an invitation email when a new user is created. Treat delivery as dependent on configured email templates, queue processing, SMTP settings, and app URL settings.

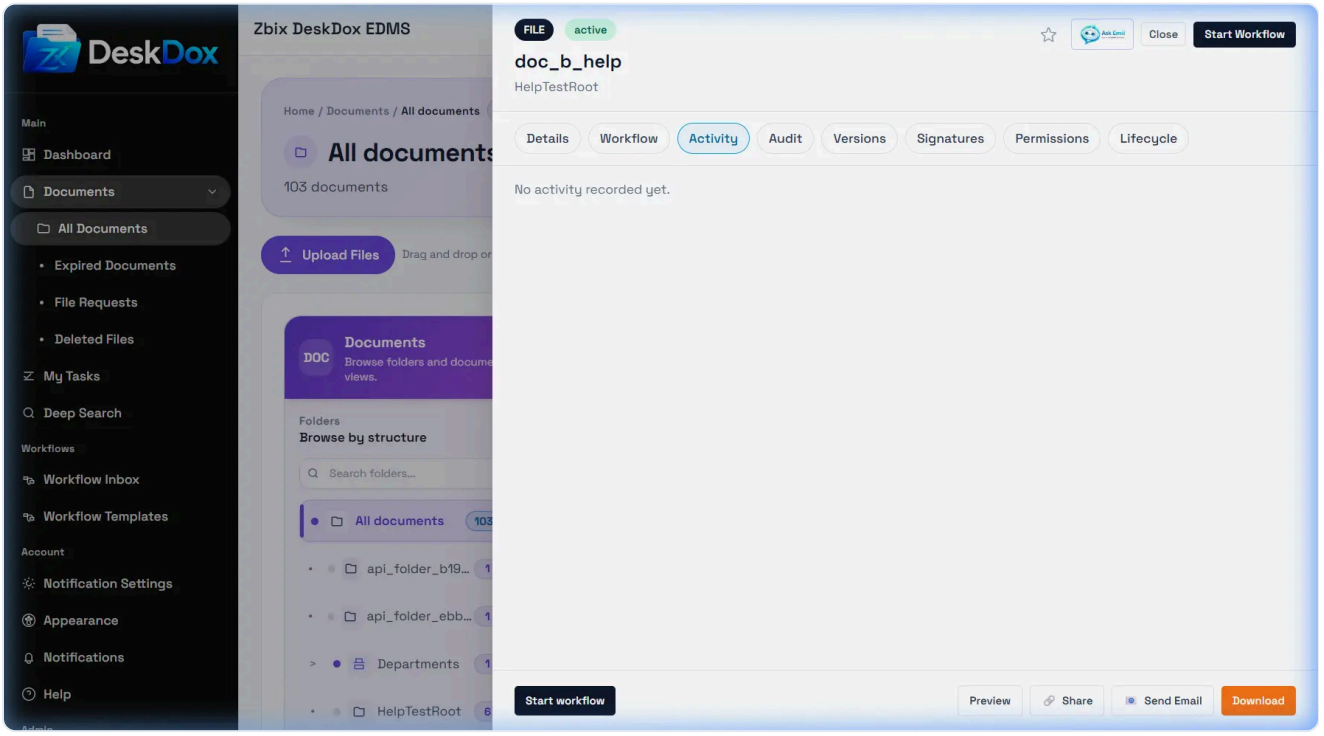
No lock/unlock UI was browser-confirmed for this module. If someone asks how to unlock a user, first check whether the account is inactive, the password is wrong, the user lacks a valid department, the email/reset message was not delivered, or the local login session is stale.

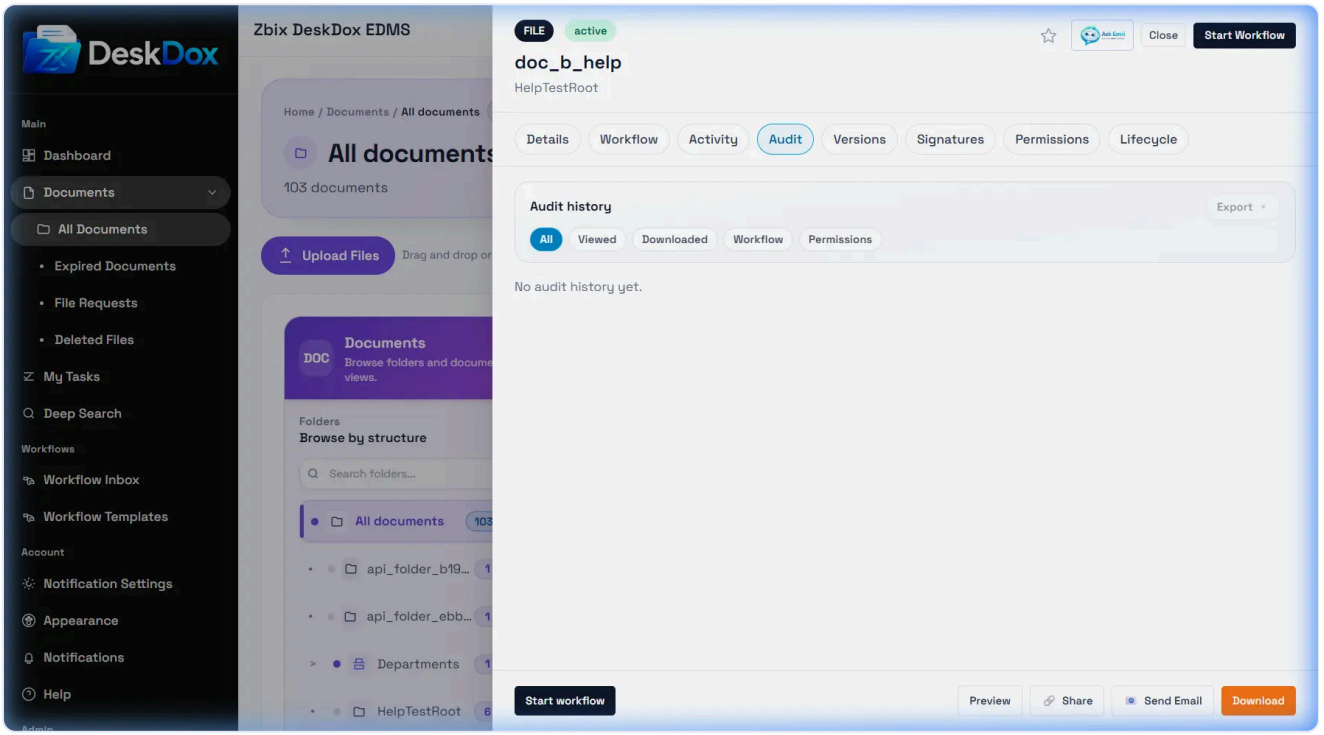
Sharing and Access Control · 1 min read · Reviewed 2026-05-13

View Document Activity and Audit Trail

What this helps you do

Use the Activity and Audit tabs to review document history, including views, downloads, workflow events, permission changes, sharing events, and other compliance-relevant actions.





Activity and Audit tabs

Open the Document Detail Drawer, then select `Activity` for a readable event stream or `Audit` for audit-focused records. Filters may include `All`, `Viewed`, `Downloaded`, `Workflow`, and `Permissions`. Use `Audit Export` when available to export audit history.

Access and compliance

Audit visibility depends on permission. Some users can see basic activity but not full audit records. Administrators, auditors, records staff, or document owners may have broader access depending on tenant policy. Use these tabs to confirm who viewed or downloaded a document, who shared it, and when workflow or permission changes occurred.

CHAPTER 7

Workflow Approvals

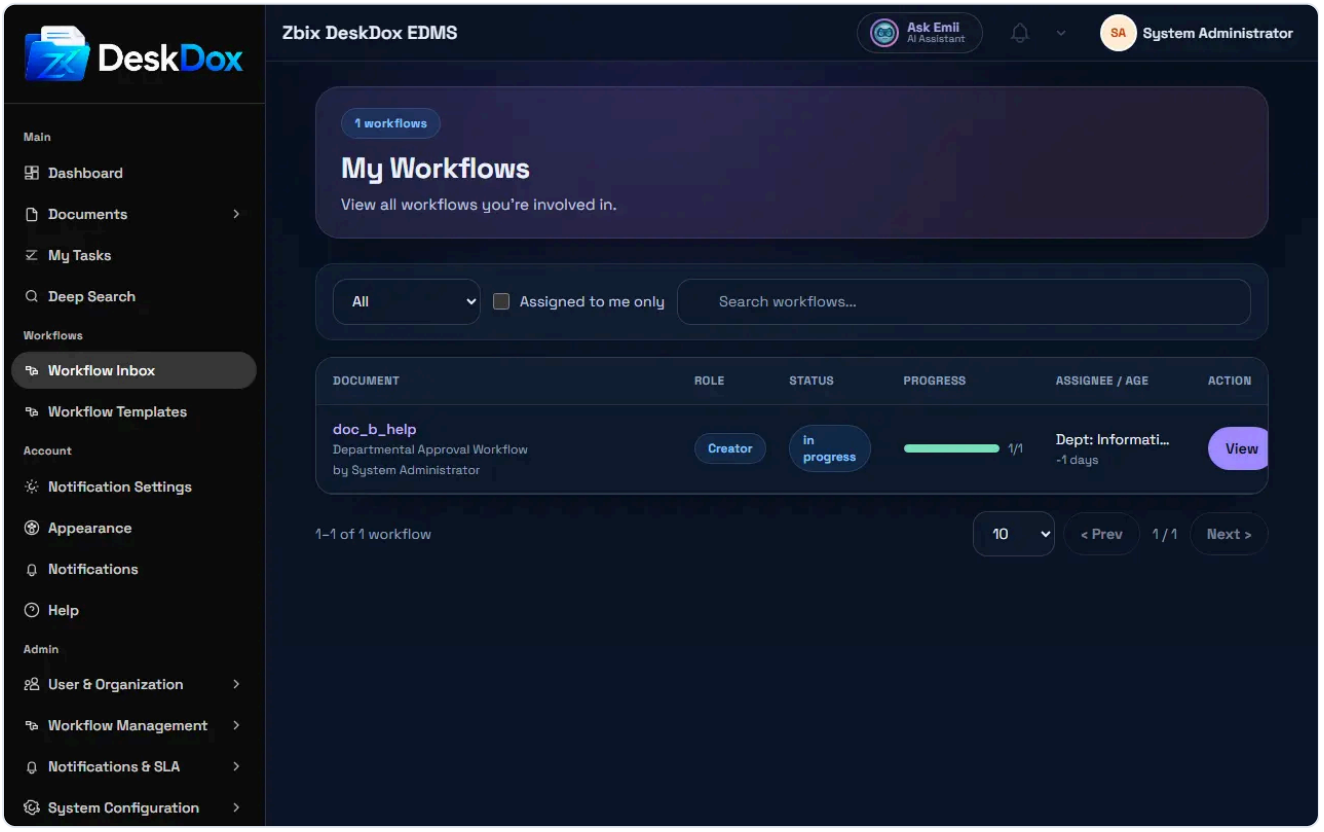
Approval routing, task inboxes, review decisions, signatures, and workflow participation.

Workflow Approvals · 3 min read · Reviewed 2026-05-13

How to Review an Approval Task

What this helps you do

Approve or reject a workflow task after reviewing the document, metadata, comments, and workflow history.



Who can use it

Assigned users, members of the assigned role or department, and workflow administrators can review tasks according to workflow configuration. When a workflow step is assigned to a department, eligible members of that department can see the pooled task. A user must claim the task before taking action, which helps prevent multiple users from acting on the same approval at the same time.

Required permissions

- View access to the linked document.
- Assignment to the current task or administrative workflow permission.
- Comment or decision permission for the workflow step.

Open your task

1. Open `My Tasks`.
2. Select the workflow task.
3. Review document, workflow context, due date, and activity.

If the task is pooled for a department, claim it first. After claiming, the available decision actions are shown according to the step configuration and your permissions.

Take action

1. Add decision comment.
2. Choose `Approve` or `Reject`.
3. If rejecting, include a clear reason (required).
4. Optionally upload a revised file where allowed.

View workflow status and history

Before acting, check prior comments, previous assignees, current step, due date, and any activity or audit records. This prevents approving a document that was already rejected, revised, or reassigned.

Claim and reassign notes

- If a task is role- or department-assigned, you may need to claim it first.
- Reassignment is role-controlled and may require reason logging.

Signature-related behavior

Some tasks cannot complete until required signatures are satisfied.

Common mistakes

- Approving without previewing the latest document version.
- Rejecting without a clear reason.
- Trying to act on a task assigned to a different user or role.

- Missing required signature steps before completion.

Troubleshooting

If action buttons are missing, confirm the task is assigned to you, the workflow is still active, and your user belongs to the required role or department. If the task disappeared, it may have been completed, reassigned, cancelled, or superseded by a newer workflow instance.

Related Emii questions

- "How do I approve a workflow task?"
- "Why can't I reject this task?"
- "Where can I see workflow history?"
- "Why is a workflow task assigned to my department?"

Related reading

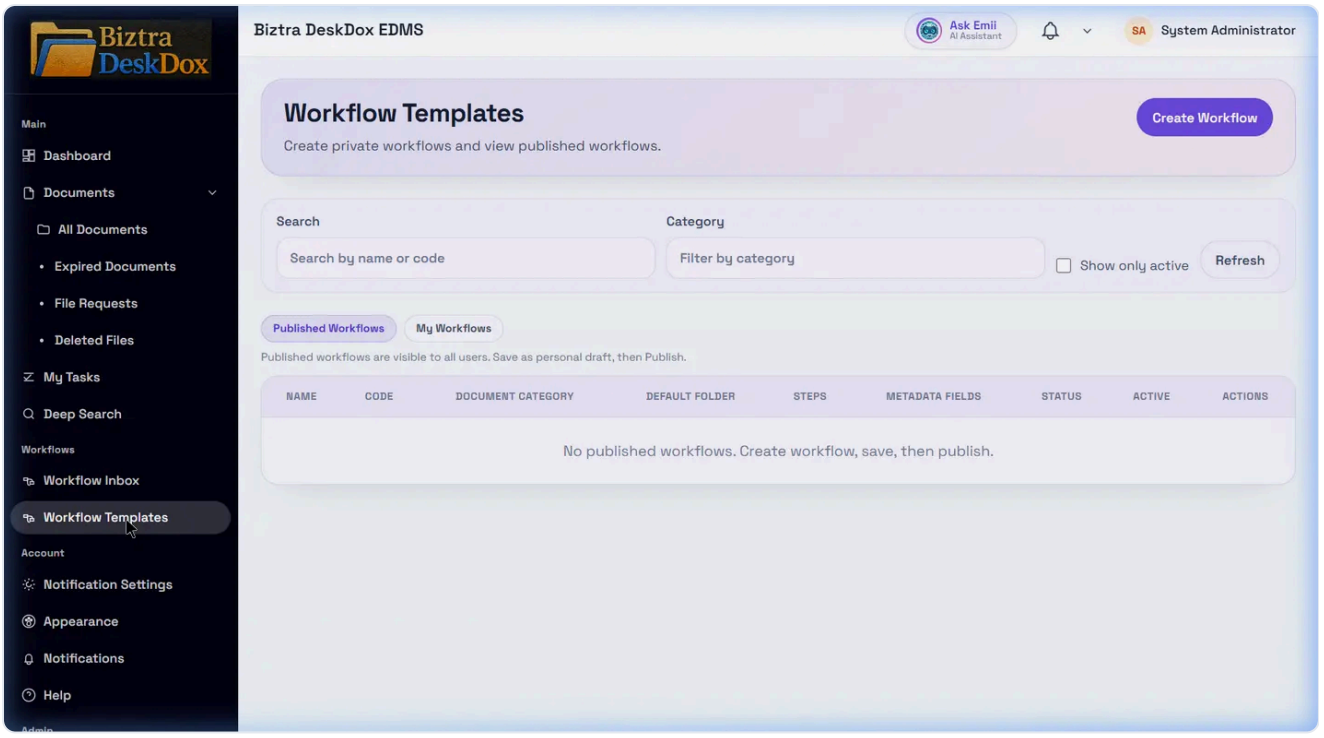
- How to Submit or Track a Workflow
- User Manual: Signatures and Collaboration

Workflow Approvals · 2 min read · Reviewed 2026-05-13

How to Submit or Track a Workflow

What this helps you do

Start a workflow from upload or document actions, track workflow status, and understand why workflow options may be missing.



Who can use it

Users with workflow access can submit documents into available templates and view workflow status. Approvers and task owners can act on assigned tasks.

Required permissions

- Document upload or document view access.
- Permission to start the selected workflow template.
- Task assignment, role assignment, or department assignment for approval actions.

Start a workflow

1. Open the document or upload a new document.
2. Choose the workflow template that matches the process.
3. Confirm required metadata is complete.
4. Submit or start the workflow.

Upload a document with workflow

1. Upload the document.
2. Select a workflow template (if required).
3. Complete required metadata.
4. Submit.

View workflow status

1. Open `Workflow Inbox`.
2. Filter by status or "assigned to me".
3. Open the linked document/workflow item.
4. Review current assignee and step progress.

Track workflow history

Open the document details or workflow item and review the activity, workflow, or audit sections. History helps confirm who submitted, approved, rejected, reassigned, or commented on a workflow.

If progress is blocked

- A prior step may still be pending.
- Signature may be required before completion.
- Task may be assigned to another user/role.

Troubleshoot missing workflow options

- No template appears: your role may not have access to the template.
- Template appears during upload but submit fails: required metadata may be missing.
- Task is not in `My Tasks`: it may be assigned to another user, role, or department.
- Approval buttons are hidden: you may be a viewer, not the assigned approver.

Related Emii questions

- "How do I start a workflow?"
- "Why can't I see workflow templates?"
- "How do I track workflow status?"
- "Why is my approval task missing?"

Related reading

- How to Review an Approval Task
- How to Upload a Document
- User Manual: Workflows, Tasks, and Approvals

Workflow Approvals · 2 min read · Reviewed 2026-05-14

Reviewing Workflow Tasks

What this helps you do

Review an assigned workflow task and understand when action buttons are available.

Open and review a task

Open a workflow task from `My Tasks` or `Workflow Inbox` when an `Open` action is visible. The task detail route is `/app/workflow/tasks/:stepId`, and the page title may use the workflow step name, such as an initial review step.

Before acting, review the linked document, document metadata, workflow step details, due date or SLA indicators when visible, and any activity or comments available in your task view.

Actions on a task

The walkthrough available that task detail can show a `Take Action` area with `Approve`, `Reject`, `Claim Task`, and `Sign Now` depending on assignment, step state, signature requirements, and permissions.

Use `Approve` only after confirming the document and metadata are acceptable. Use `Reject` when the document should not proceed. The page explains that rejection requires text in the `Decision Comment` field. `Upload revised file` and `Choose file` may be available when the workflow allows a revised version during review.

Return or request-changes behavior was not separately shown as a distinct button in the available screenshots. If a return/send-back option appears in your environment, follow your organization's workflow instructions and add a clear decision note.

Why action buttons may be hidden or disabled

Actions may be hidden or disabled when the task is assigned to the wrong user, role, or department; your account lacks workflow permission; the workflow has not started; the task is already completed, cancelled, skipped, or rejected; or a signature is required before completion.

The page can show the message "Signature required before you can complete this step." when signature requirements block completion.

After submitting a decision

After a decision is submitted, the workflow normally advances, stops, or records the outcome according to the configured process. The exact next state depends on the template, step rules, and whether required

signatures or revisions are still pending.

Related Emii questions

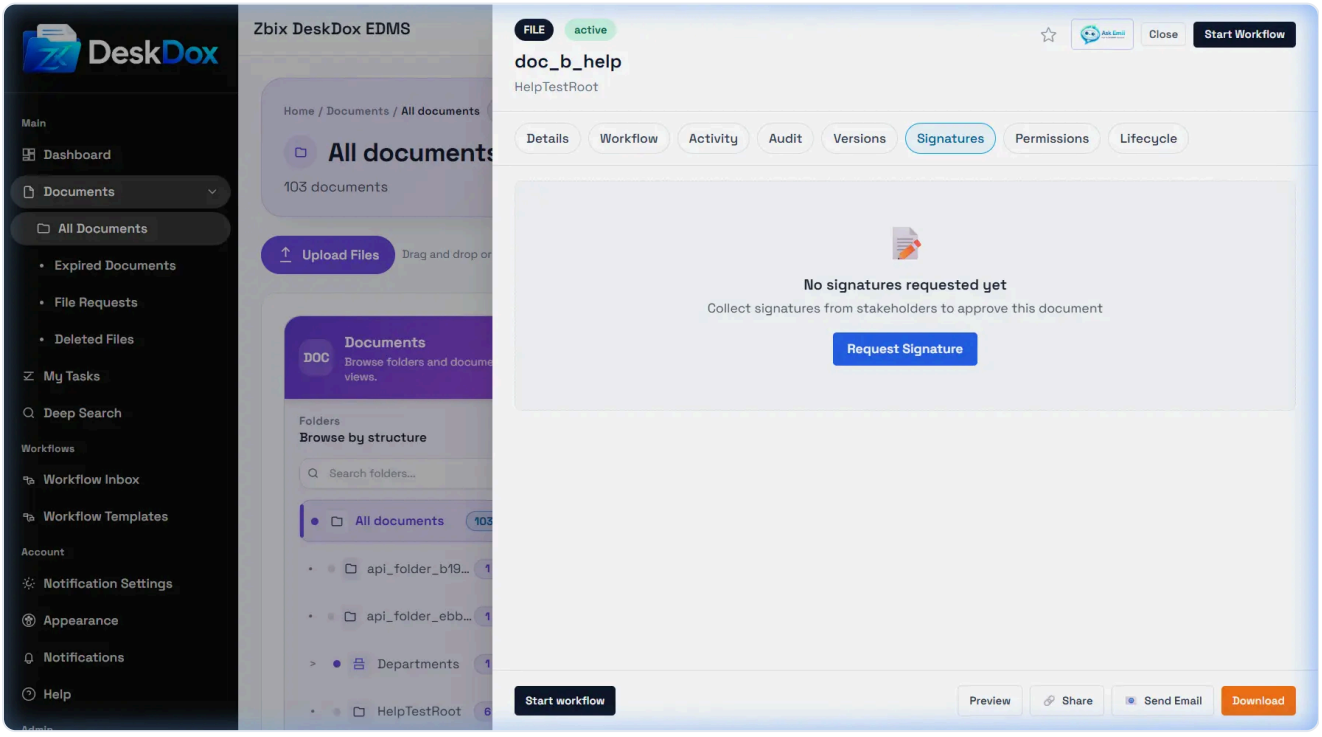
- "How do I review a workflow task?"
- "How do I approve a task?"
- "Why is the Approve button not visible?"
- "Do I need to add a comment when rejecting?"
- "What happens after I approve a workflow task?"

Workflow Approvals · 1 min read · Reviewed 2026-05-13

Document Signatures

What this helps you do

Use the Signatures tab to see signature requests and signing status connected to the selected document.



Signature requests

Signature requests are available for supported document types such as PDFs. If the signature action is unavailable, confirm that the document format is supported and that your role has the required permission.

Open the Document Detail Drawer and select `Signatures`. The tab can show signature requests, participants, statuses, and pending signatures when signature features are enabled. Related tasks may also appear in `My Tasks` or Signature Requests depending on deployment workflow.

Missing signature status

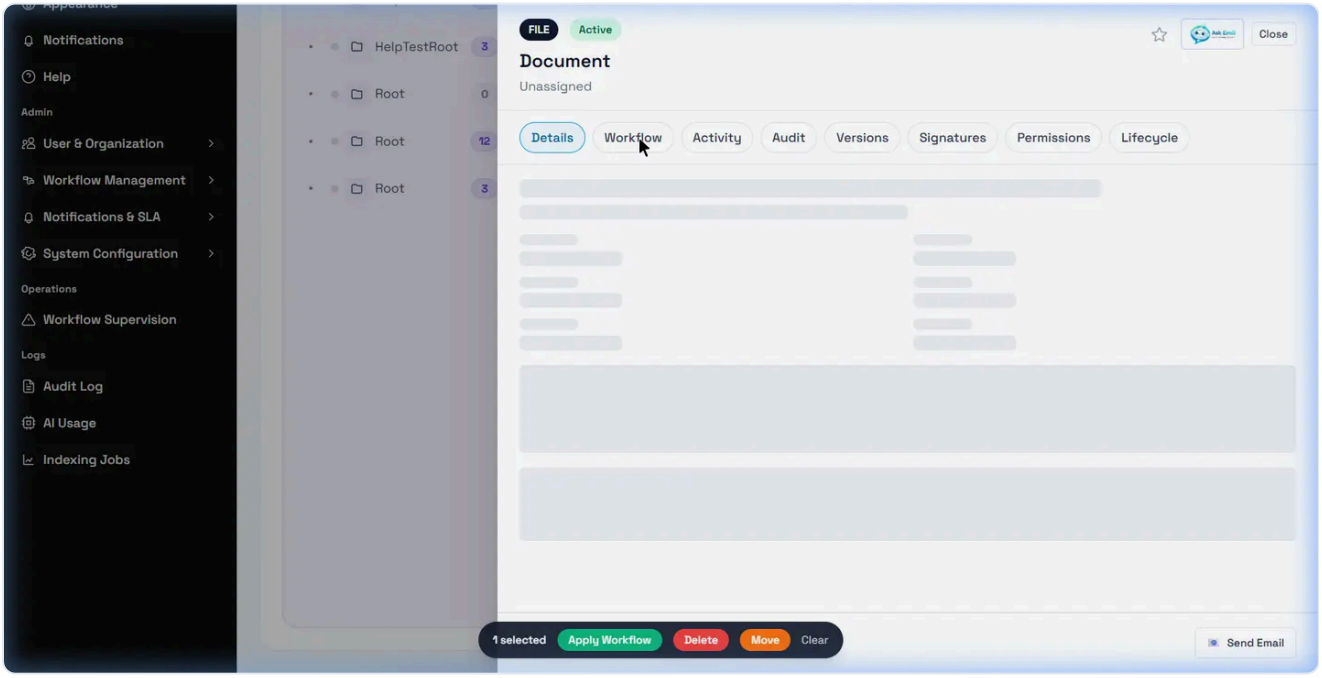
If signature status is not visible, check whether the document has a signature request, whether signatures are enabled, whether the file type is supported, and whether your role can view signature details. Some users may only see their own pending signing task.

Workflow Approvals · 2 min read · Reviewed 2026-05-14

Document Workflow Tab

What this helps you do

Use the Document Detail Drawer `Workflow` tab to check workflow status for a document.



Open workflow details from a document

Open a document, then select the `Workflow` tab in the Document Detail Drawer when it is visible. The route pattern is `/app/documents/:documentId?tab=workflow`.

The tab can show the active workflow status, workflow steps, and reviewer or approver assignment details when those fields are visible to your account. The page can show document workflow statuses such as `In Progress` and `Completed`.

Relationship with My Tasks and Workflow Inbox

`My Tasks` and `Workflow Inbox` show assigned work items. The document `Workflow` tab shows workflow context from the document side. If a task is missing from My Tasks, the empty-state guidance recommends opening the document workflow tab or contacting an administrator.

Workflow actions from the drawer

The document workflow area can show `Start Workflow` and `Apply Workflow` controls in the document workflow area. These controls are permission-dependent and may be intended for users allowed to start or apply workflows.

Approval, rejection, signing, or other task actions may be available from the document drawer only when visible and allowed by your configuration. If action buttons are not visible, open the assigned task from `My Tasks` or `Workflow Inbox`.

When no workflow is attached

If no workflow is attached to the document, the tab may show no active workflow or no steps. This can mean the workflow has not been started, no workflow template was applied, the workflow feature is not enabled, or your account cannot view workflow details for that document.

Related Emii questions

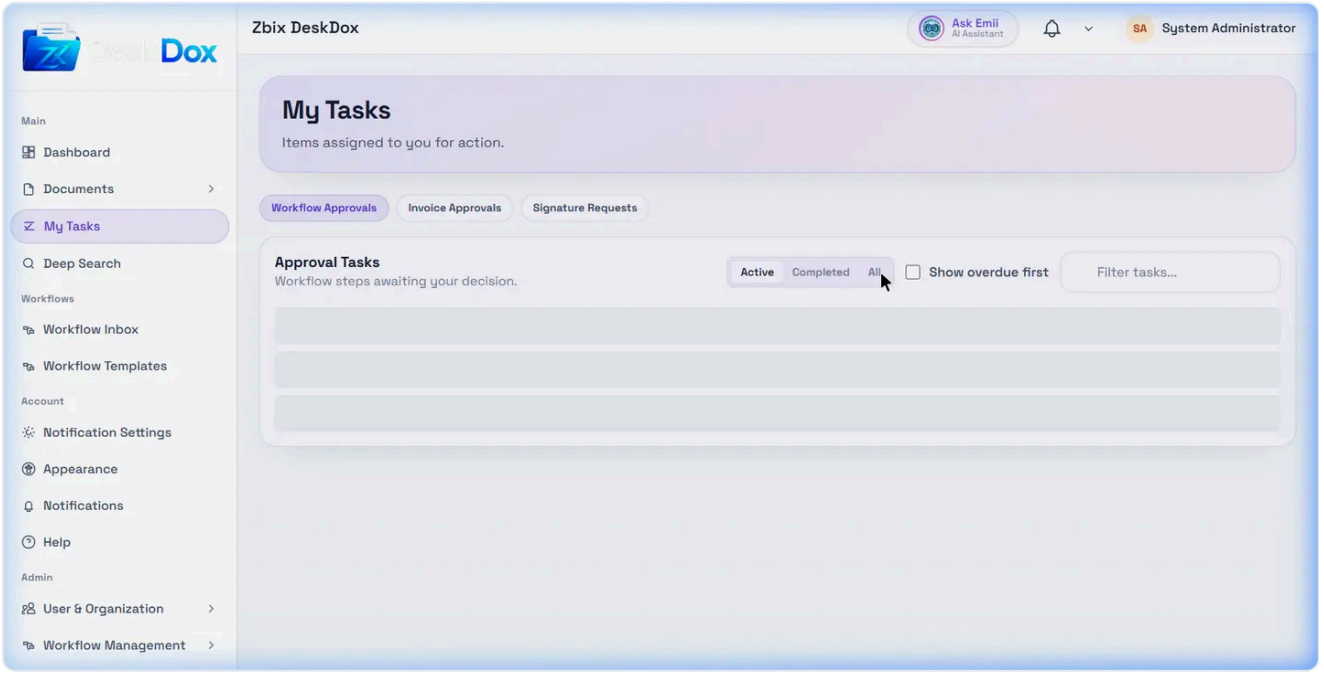
- "Where is the Workflow tab on a document?"
- "How do I see workflow status from a document?"
- "Why can't I see the Workflow tab?"
- "Can I approve a workflow from the document drawer?"
- "Why is there no workflow on this document?"

Workflow Approvals · 3 min read · Reviewed 2026-05-14

My Tasks and Workflow Inbox

What this helps you do

Find assigned workflow work, use visible task filters, and understand why a task may not appear.

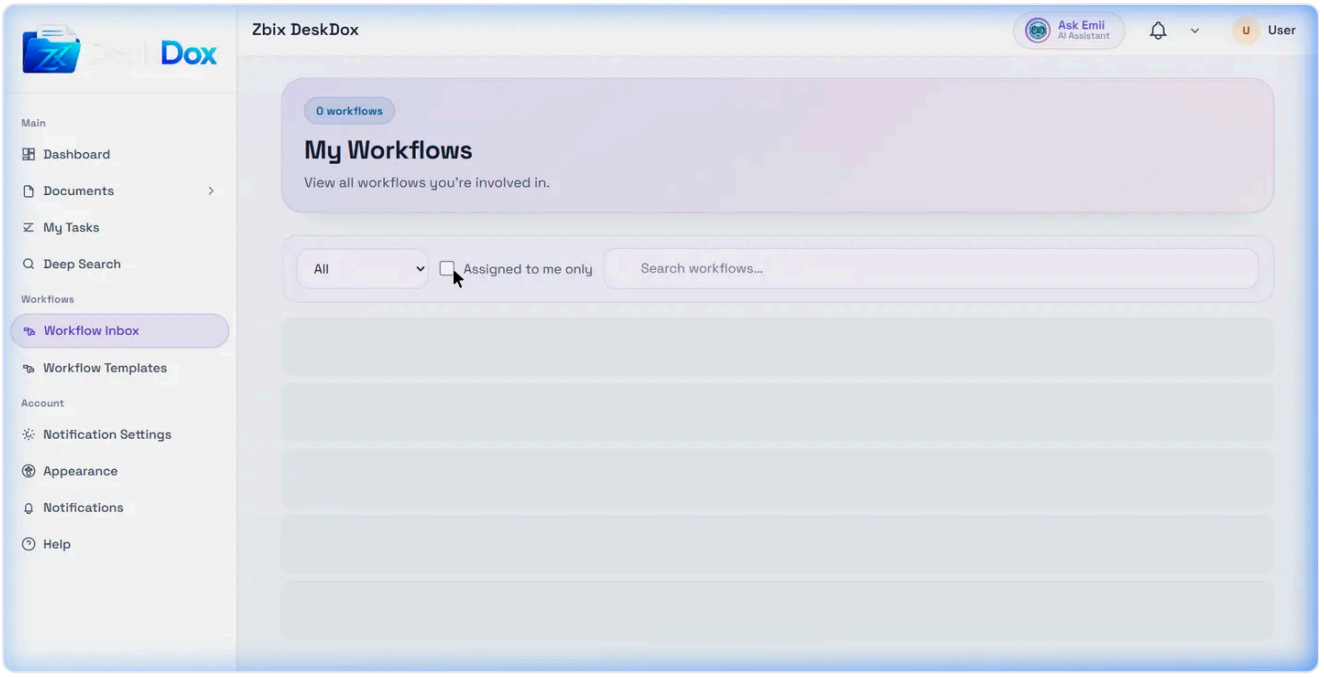


My Tasks

Open `My Tasks` from the main navigation. The available My Tasks screen showed tabs for `Workflow Approvals`, `Invoice Approvals`, and `Signature Requests`. Use `Workflow Approvals` for workflow review and approval assignments when that tab is visible.

The task list/table can show workflow items, status, deadline/SLA information, and actions depending on configuration and permissions. The walkthrough observed status and timing labels such as `pending`, `completed`, `Overdue`, `Due today`, and `SLA: X days`.

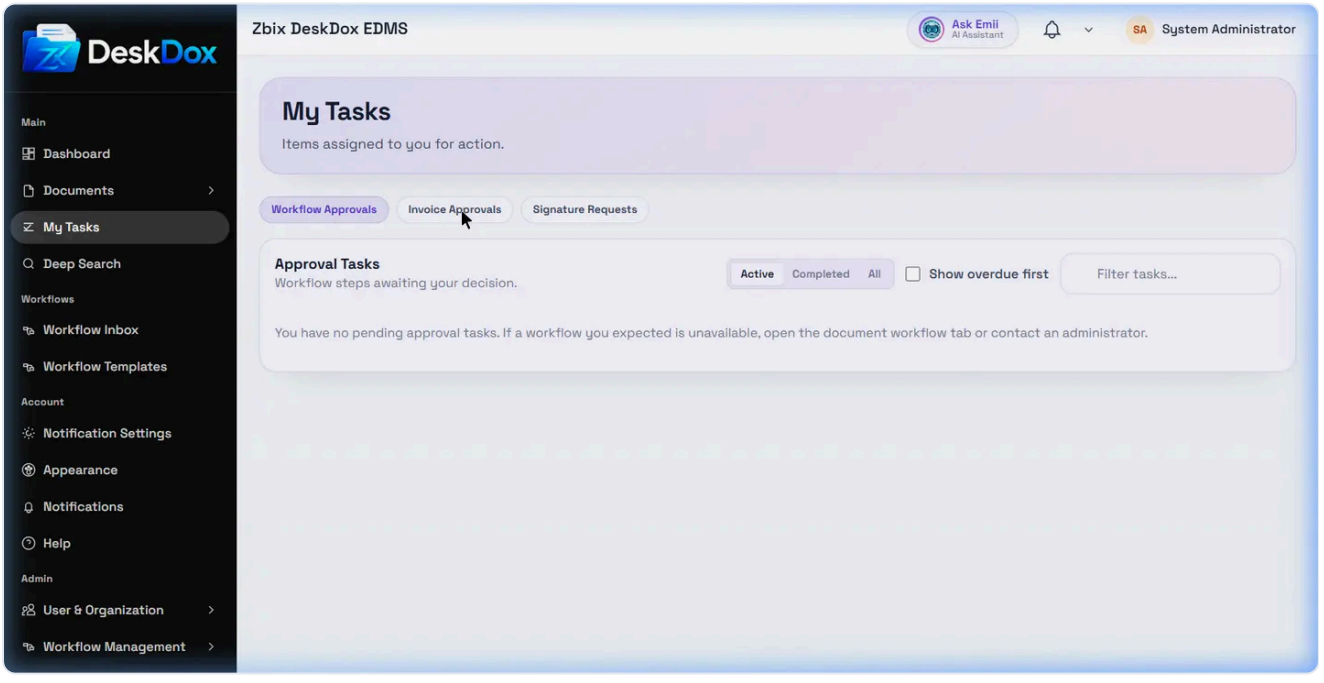
Workflow Inbox



`Workflow Inbox` was available at `/app/workflows/my-workflows` when visible in the Workflows area. It is another queue for workflows you are involved in, including assigned or visible workflow items depending on your role and permissions.

If `Open` is visible for a row, use it to open the task or related workflow item. Administrative actions such as `Reassign` or menu-based admin actions are permission-dependent.

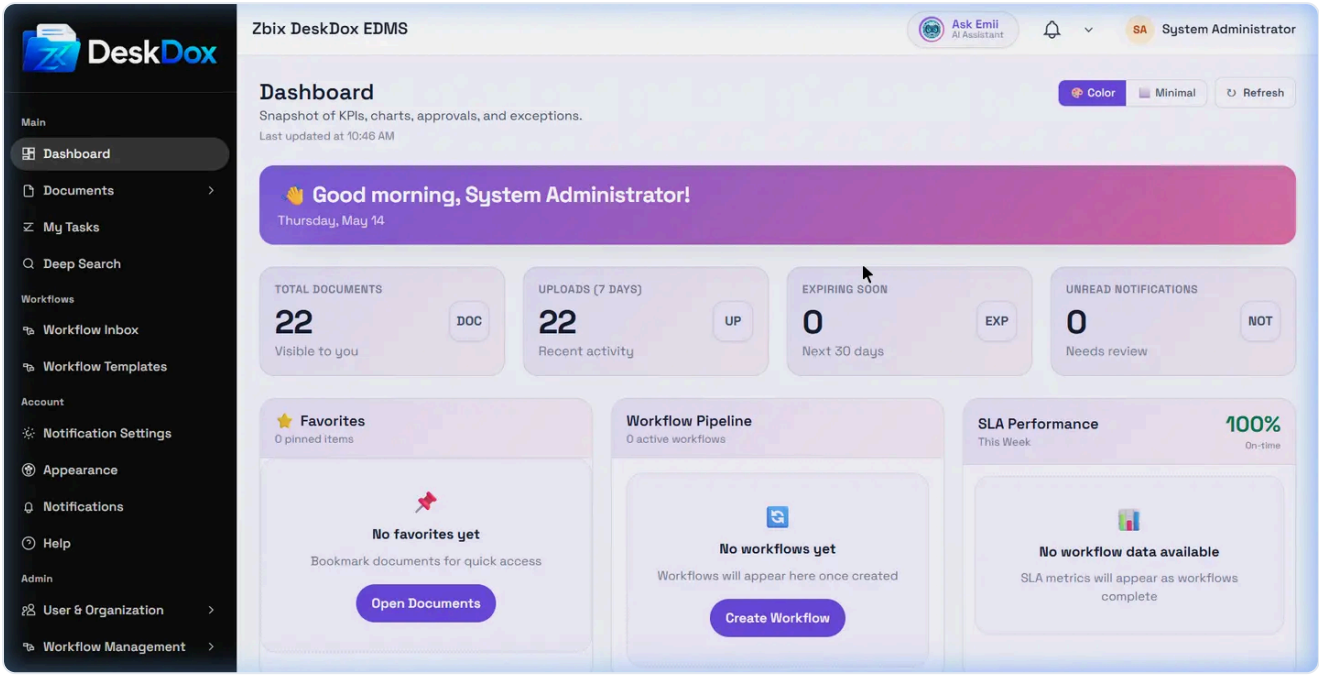
Filters and status tabs



The available workflow approval filters are `Active`, `Completed`, and `All`. Use them to switch between current tasks, completed tasks, and the broader task list when those filters are visible.

`Pending` means the task is waiting for the assigned user, role, or department to act. `Overdue` means the visible due date or SLA target has passed. SLA and due-date indicators may be hidden when no due date is configured or your view does not include that column.

Empty state



When no approval tasks exist, DeskDox displays: "You have no pending approval tasks. If a workflow you expected is unavailable, open the document workflow tab or contact an administrator."

Why tasks may not appear

A task may be missing because it is assigned to another user, role, or department; your account lacks the required permission; the workflow has not started; the task is already completed, cancelled, skipped, or rejected; a filter is hiding it; or the feature is not enabled in your environment.

After an administrator changes role, department, or permission assignments, refresh the page or sign in again before checking the list.

Related Emii questions

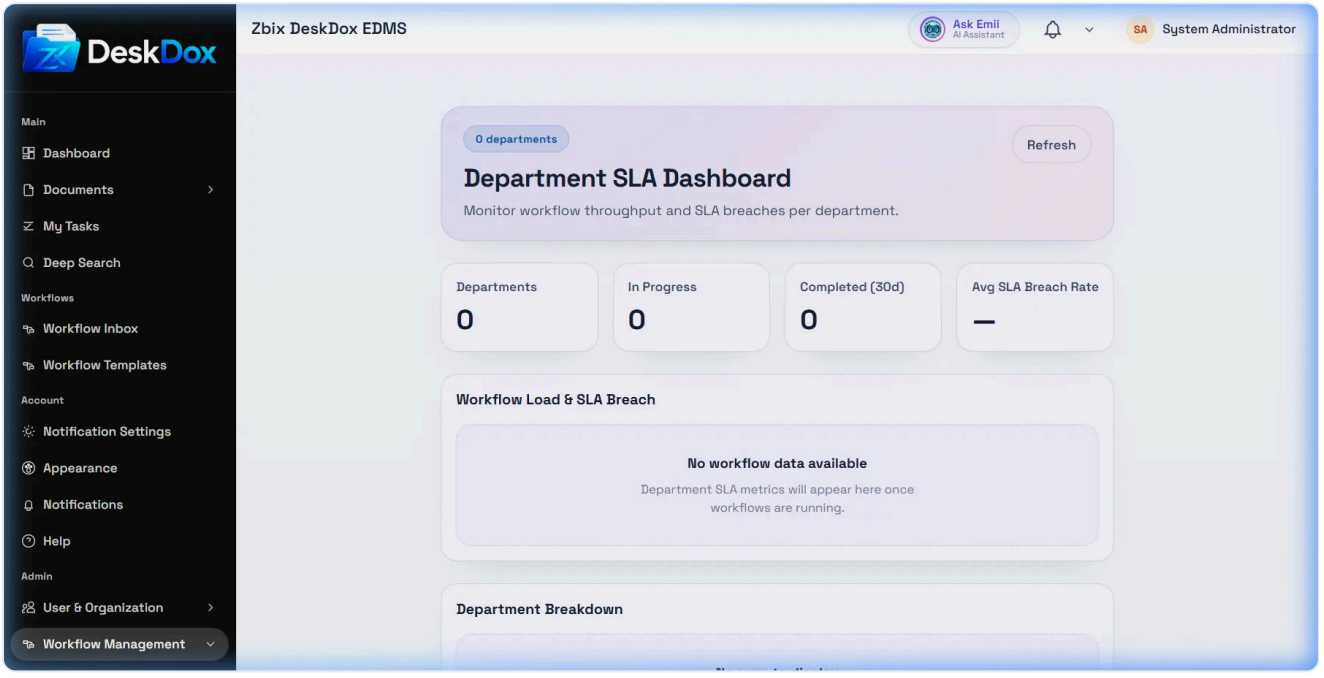
- "Where can I find my tasks?"
- "What is Workflow Inbox?"
- "Why is My Tasks empty?"

- "How do I filter workflow tasks?"
- "What does overdue workflow task mean?"

Workflow Approvals · 1 min read · Reviewed 2026-05-14

Overdue Tasks and SLA Breaches

Open your task inbox to review work assigned to you. Use `Show overdue first` when available to prioritize overdue work. Administrators can use the Department SLA dashboard to monitor department-level workload and SLA risk.



What overdue means

A task is overdue when its due date has passed. An SLA breach means the configured SLA target was missed. Due dates can be affected by workflow step SLA settings, business calendars, working hours, holidays, and escalation configuration.

The Department SLA dashboard can show department-level indicators such as active workload, overdue work, breached SLA counts, and escalation visibility when workflow activity and SLA configuration exist.

What to do

Open the overdue task, review the document or workflow context, and complete the assigned action if it is still assigned to you. If the task is assigned to another user, role, or department, you may not be able to act

on it. Admins should verify assignment, SLA configuration, calendar setup, escalation chain settings, and whether enough workflow activity exists for the SLA dashboard to show meaningful data.

Workflow Approvals · 2 min read · Reviewed 2026-05-14

Workflow Comments and Decision Notes

What this helps you do

Understand workflow comments and decision notes without assuming every workflow exposes the same fields.

Decision comments

The task detail view includes a `Decision Comment` field on task detail. It also available that rejecting a task requires text in that field. Approval comments or optional decision notes may be available depending on workflow configuration.

Comments may be unavailable when you do not have an active assigned task, the task is read-only, the workflow is completed or cancelled, or your permissions do not allow action on the current step.

Visibility and audit value

Workflow comments and decision notes help explain why a task was approved, rejected, returned, or changed. They are audit-relevant because they preserve review context for later users and administrators.

Who can see comments depends on role, workflow visibility, document access, and audit permissions. Users involved in the workflow or users with administrative workflow access may see more context than a standard viewer.

Document comments versus workflow notes

Some deployments may not show a separate document-comments interface in the workflow task view. If your environment shows both document comments and workflow decision notes, treat workflow decision notes as the reason attached to the workflow action, and document comments as collaboration notes on the document itself.

Related Emii questions

- "How do I add a workflow comment?"

- "Are workflow comments visible to other users?"
- "Do I need to give a reason when rejecting?"
- "Where can I see approval comments?"
- "Are workflow comments audited?"

Workflow Approvals · 2 min read · Reviewed 2026-05-14

Workflow History and Status

What this helps you do

Check workflow progress, understand common status labels, and know where approval history may appear.

Status and progress

Workflow status describes the overall workflow instance. Workflow instance statuses can include `pending`, `in_progress`, `completed`, and `cancelled`.

Workflow task or step status describes one step in the workflow. Workflow step statuses can include `pending`, `in_progress`, `completed`, `rejected`, `assigned`, `cancelled`, and `skipped`.

`Pending approval` means the current step is waiting for an assigned user, role, or department to act. `Rejected` means a reviewer rejected the task or workflow step according to the configured process. Returned/request-changes behavior may appear differently depending on the workflow configuration.

Where to check history

Task detail may show an `Activity` area with filters such as `All`, `Task`, `Versions`, and `Views`. That task-history screenshot is pending capture, so exact layout should be treated as configuration-dependent.

Users may also see workflow status and steps from the document's `Workflow` tab when visible. Document activity or audit areas may show related document events, while workflow history focuses on workflow steps, decisions, assignments, and task activity.

Who approved or rejected

When workflow history or activity is visible, it may show who approved, rejected, viewed, uploaded a revision, reassigned, or commented. Visibility depends on document access, workflow involvement, role, and audit permissions.

Why status may not update immediately

Status may appear stale if the page has not refreshed, another user just acted, background workflow processing is still running, or the task is filtered into another status tab. Refresh the page and check the document `Workflow` tab when visible.

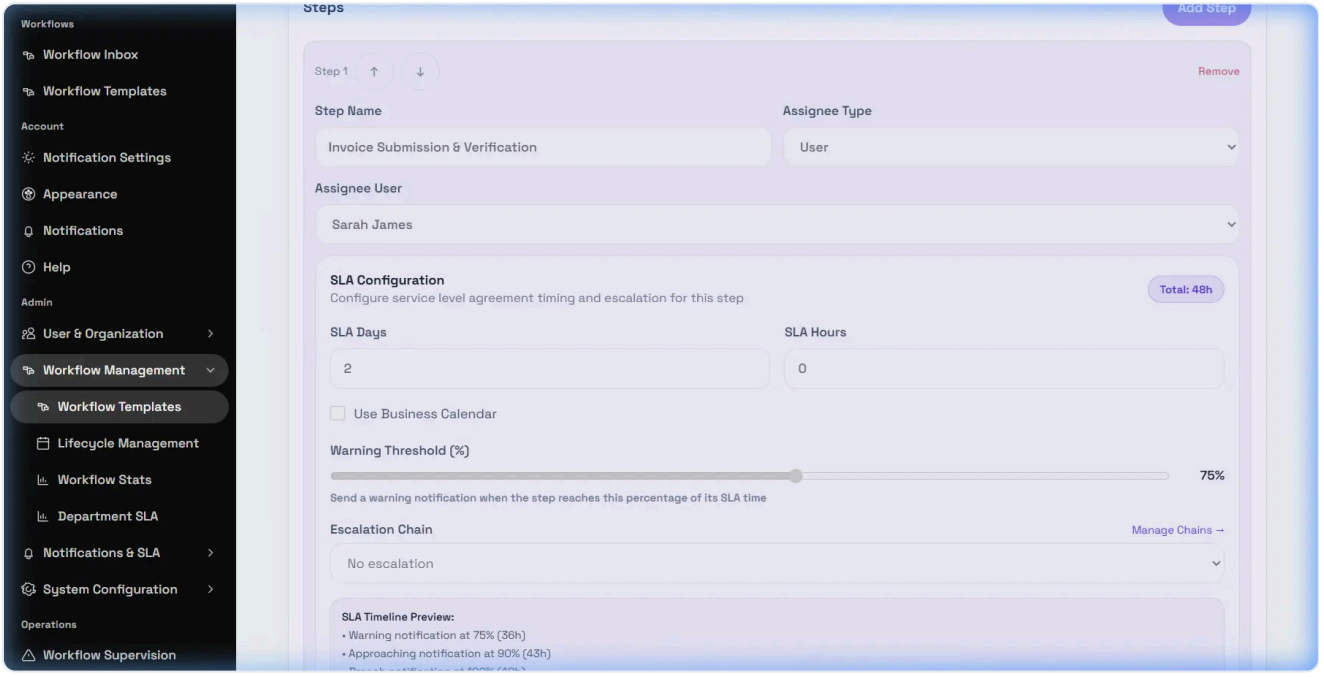
Related Emii questions

- "Where can I see workflow status?"
- "How do I know who approved a document?"
- "Where can I see workflow history?"
- "What does pending approval mean?"
- "Why is workflow status not updating?"

Workflow Approvals · 2 min read · Reviewed 2026-05-14

Workflow SLA and Due Dates

Workflow SLA is configured at the workflow template step level on `/app/admin/workflow-templates/:id`. This is an admin configuration area and may be hidden if your role cannot manage workflow templates or SLA policy.



Step-level SLA settings

The `SLA Configuration` panel includes `SLA Days`, `SLA Hours`, `Use Business Calendar`, `Calendar`, `Warning Threshold (%)`, and `Escalation Chain`. DeskDox calculates a total duration from days and hours. If a business calendar is selected, the UI labels the total as business hours and explains that weekends and holidays are excluded from SLA calculations.

The warning threshold slider is available from 50% to 95% in 5% steps, defaulting to 75% when unset. The step editor's SLA Configuration preview section is available to label warning notification, approaching notification, breach notification, and escalation timing. Exact delivery still depends on the configured notification, email, mobile, and escalation services.

Due dates and calendars

Task due dates are based on the step SLA, the task timing, and whether a business calendar is selected. If `Use Business Calendar` is enabled, DeskDox should calculate against the selected calendar's working days, working hours, and holidays. If it is off, due dates use elapsed time rather than the business calendar.

Safe rollout practices

Review SLA values before publishing or activating workflow templates. Existing workflows may continue using the template version they started with, so verify live workflow behavior after a template change. For production changes, confirm the business calendar, warning threshold, escalation chain, and notification preferences before relying on automated reminders.

CHAPTER 8

Workflow Administration

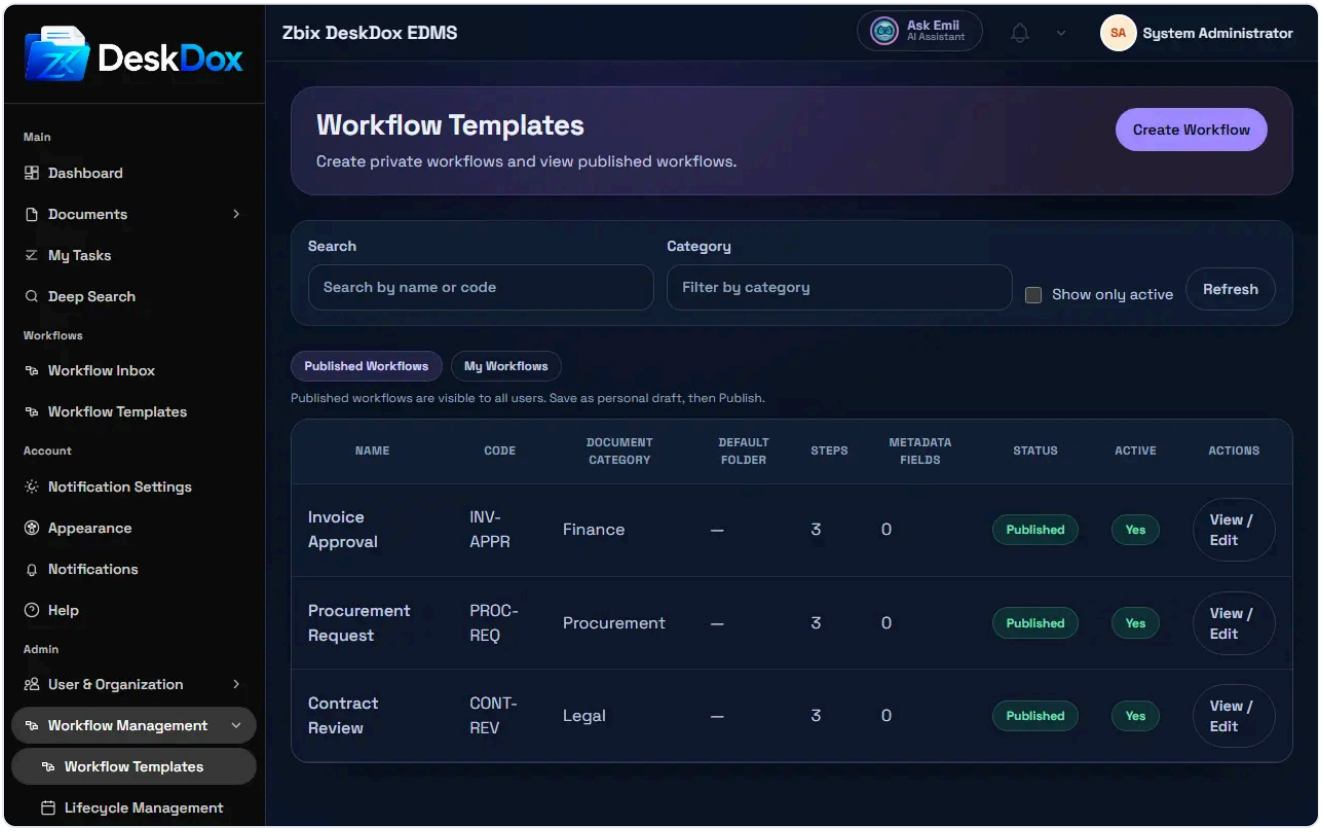
Workflow templates, supervision, SLA planning, escalation, and administrator controls.

Workflow Administration · 2 min read · Reviewed 2026-05-14

Workflow Admin Side Overview

What this helps you do

Understand the administrative workflow pages used to configure approval routing, monitor workflow performance, and supervise active or exceptional workflows.



What Workflow Admin is for

Workflow Admin is used to create and maintain workflow templates. A template defines how documents move through approval or review, including basic template information, steps, assignees, required metadata, default folder behavior, active status, and SLA settings when the SLA panel is available.

This is different from user workflow tasks. Admin workflow configuration controls the process. User-side workflow pages show live tasks created from that process, such as approvals, reviews, signatures, or assignments in `My Tasks` or `Workflow Inbox`.

Main admin areas

- `Workflow Templates` lists published and personal workflow templates.
- `Workflow Template Editor` creates or edits template details, steps, metadata, SLA settings, and status.
- `Workflow Stats` shows workflow totals, per-template performance, charts, and CSV export when the reporting feature is available.
- `Workflow Supervision` is an operational console for active tasks, exceptions, overdue items, reassignment, and ad-hoc step actions when permissions allow.
- `Department SLA` shows department-level workflow load and SLA breach metrics.

Permissions

Workflow Admin visibility depends on role, permissions, and configuration. Admin pages are commonly available to superusers, system admins, EDMS admins, workflow admins, or users with workflow administration capabilities.

Normal users may not see Workflow Admin because they can act on assigned tasks without having permission to create templates, publish templates, manage SLA policy, view admin statistics, or supervise other users' workflows.

How settings affect users

Workflow templates affect which approval templates are available during upload, where documents may be routed by default, who receives approval or review tasks, which metadata is required, and when a workflow is considered overdue. Published, active templates can be available to users; draft or inactive templates may be hidden from upload workflow selection depending on configuration.

Related Emii questions

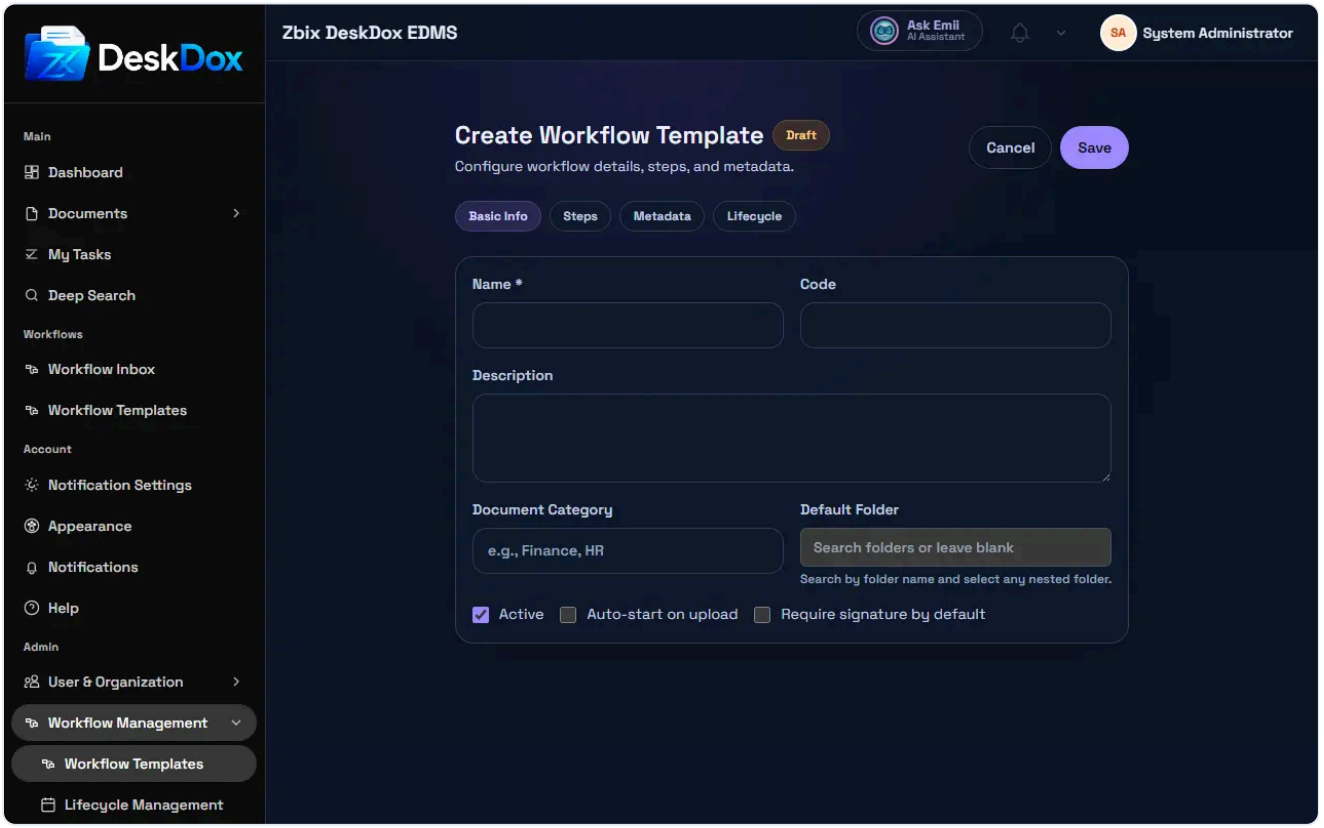
- "What is Workflow Admin used for?"
- "Why can't I see Workflow Admin?"
- "Which users can configure workflows?"
- "How do workflow templates affect document approvals?"

Workflow Administration · 2 min read · Reviewed 2026-05-14

Create or Edit a Workflow Template

What this helps you do

Open the workflow template editor, complete required fields, save changes, and understand why editing may be blocked.



Open the editor

From `Workflow Templates`, use `Create Workflow` when visible to create a new template. Use `View / Edit` from an existing row to open the edit route at `/app/admin/workflow-templates/:id`.

The editor title changes between `Create Workflow Template` and `Edit Workflow Template`. The layout is divided into sections or tabs such as `Basic Info`, `Steps`, and `Metadata`. Additional policy sections may appear when your role and license allow them.

Required fields

`Name *` and `Code` are required. The code can be auto-generated from the name on blur, but it is still validated on save. `Description`, `Document Category`, `Default Folder`, `Active`, `Auto-start on upload`, and `Require signature by default` are optional configuration fields.

Steps, metadata fields, SLA policy, and lifecycle settings are configured in their own tabs or panels when available.

Save, cancel, and validation

Use `Save` to create or update the template. Use `Cancel` to return to the list. Activation or publishing controls affect whether the template can be used for new workflows. Validation errors usually mean required fields are missing, the code is invalid or not unique, a step has incomplete assignment data, required metadata configuration is incomplete, or a restricted policy panel cannot be saved by the current user.

The editor can be read-only. Notices include `Read-only view. Click Edit to make changes.` and `Read-only: only owners of private drafts can edit.`

Permission requirements

Creating requires `canCreateWorkflowTemplate`. Publishing requires `canPublishWorkflowTemplate`. Editing a private draft may depend on ownership. Some panels, including SLA and lifecycle, are separately capability-gated.

Related Emii questions

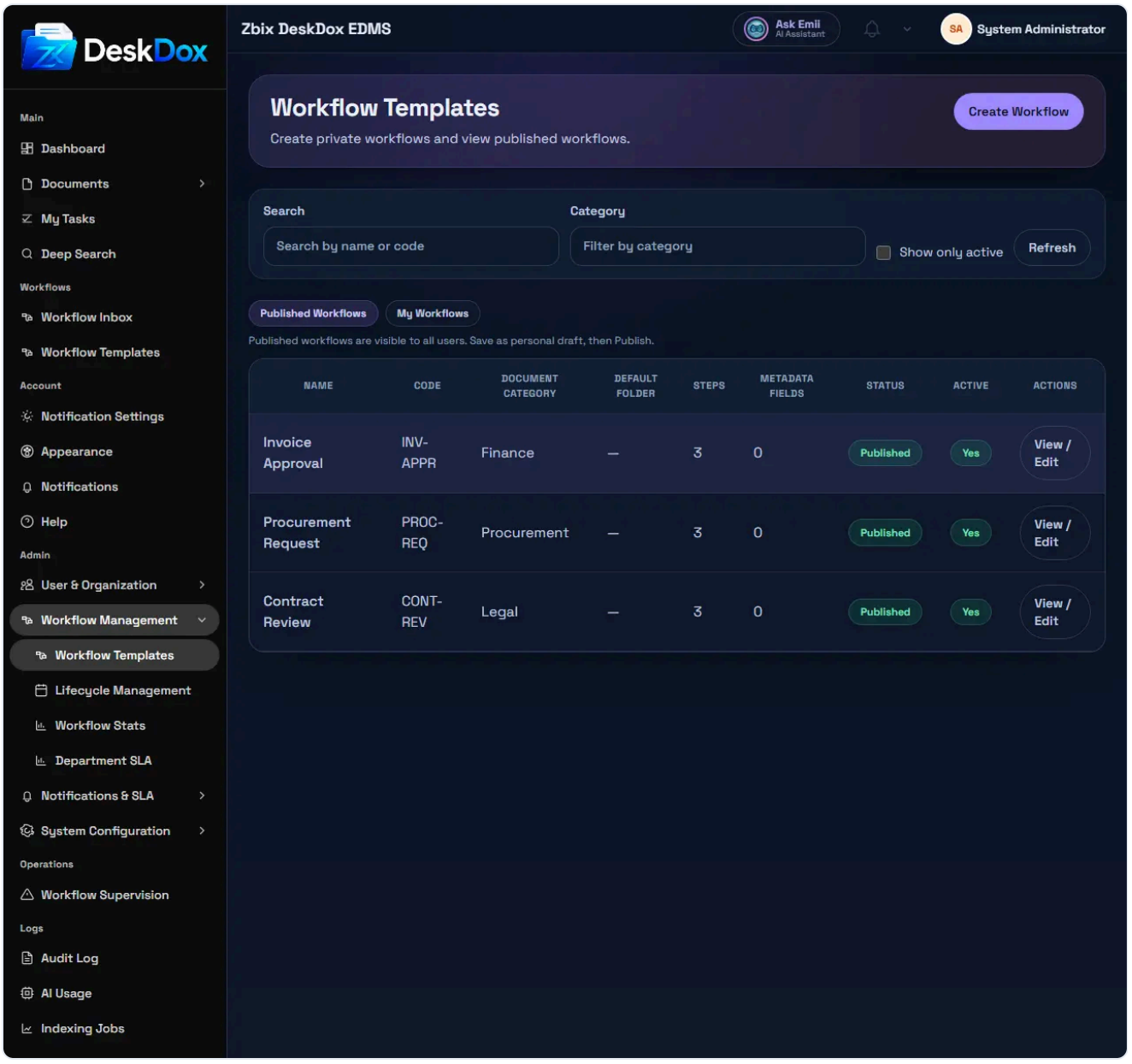
- "What fields are required in a workflow template?"
- "Why can't I save a workflow template?"
- "Who can edit workflow templates?"

Workflow Administration · 2 min read · Reviewed 2026-05-14

Workflow Templates List

What this helps you do

Find workflow templates, understand list filters and status badges, and open the editor when your permissions allow it.



List and tabs

Open `Workflow Templates` at `/app/admin/workflow-templates`. Tabs include `Published Workflows` and, when the user can publish workflow templates, `My Workflows`.

The table can include `Name`, `Code`, `Document Category`, `Default Folder`, `Steps`, `Metadata Fields`, `Status`, `Active`, and `Actions`.

Search, filters, and status

Use `Search` to filter by name or code. Use `Category` for document category filtering. Use `Show only active` to limit results to active templates, and `Refresh` to reload the list.

Status badges can show `Published` or `Draft`. Active badges can show `Yes` or `No`. An active template is enabled by its `Active` flag. A published and active template is the kind most likely to be available for starting workflows or upload selection, depending on configuration.

Create or edit templates

Use `Create Workflow` when visible to open the new template editor. The button is visible only when `canCreateWorkflowTemplate` is available.

Use `View / Edit` on a row to open the template editor. Editing may still be restricted by ownership, draft visibility, and workflow template permissions.

Templates can be reused by starting new workflows from the same published and active configuration. This helps keep repeated approval processes consistent.

Empty or hidden templates

Supported empty states include `No published workflows. Create workflow, save, then publish.`, `No published workflows available.`, and `No personal workflows found.`

If a template is not visible, check the selected tab, search text, category filter, `Show only active`, draft versus published status, active flag, ownership, and whether your account has workflow admin permissions.

Related Emii questions

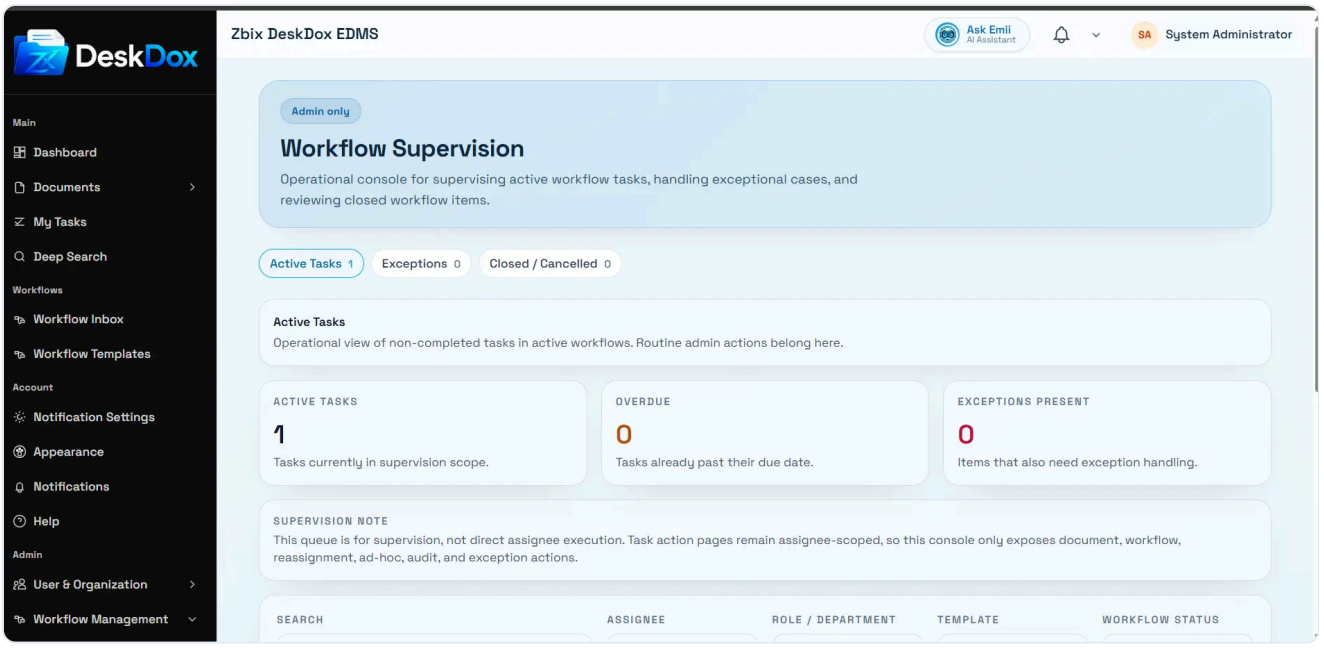
- "Where can I see workflow templates?"
- "How do I create a workflow template?"
- "Why can't I see a workflow template?"
- "What does active workflow template mean?"

Workflow Administration · 2 min read · Reviewed 2026-05-14

Workflow Supervision Console

What this helps you do

Monitor active workflow tasks, find overdue or stuck workflows, and use admin actions when permissions and policy allow them.



Purpose and tabs

`Workflow Supervision` is an operational admin console. Tabs are `Active Tasks`, `Exceptions`, and `Closed / Cancelled`.

The page includes a note that the queue is for supervision, not direct assignee execution. Use it to investigate workflow health before intervening.

Filters and lists

Filters include `Search`, `Assignee`, `Role/Department`, `Template`, `Workflow Status`, `Task Status`, `Due State`, `Exception State`, `Due From`, `Due To`, and `Clear Filters`.

The active task table can show task, document/workflow, step/assignment, status, due/age, flags, and actions. Flags may include exception, overdue, escalated, ad-hoc, `SLA breached`, or `Overdue`.

Admin actions

Actions include `Open`, `Reassign`, and `More` options such as Open Document, View Audit, `Add Step`, and Review Exception. Reassignment requires `New assignee` and `Reason`, and remains auditable. Ad-hoc step creation can include `Step name`, `Assignee`, `Due date`, and `Administrative note`.

Exception actions can include `Review`, `Restore`, `Resync`, and `Cancel` depending on suggested actions. Use these only after checking the document, current step, audit trail, assignee, metadata, and whether normal routing can resume.

Permissions

Workflow Supervision requires workflow task administration capability. Visibility is permission-based, so users without supervision rights may not see the page or may see a limited queue. If the page is empty, check filters, active versus closed tabs, workflow status, permissions, and whether the environment currently has active or exceptional workflows.

Related Emii questions

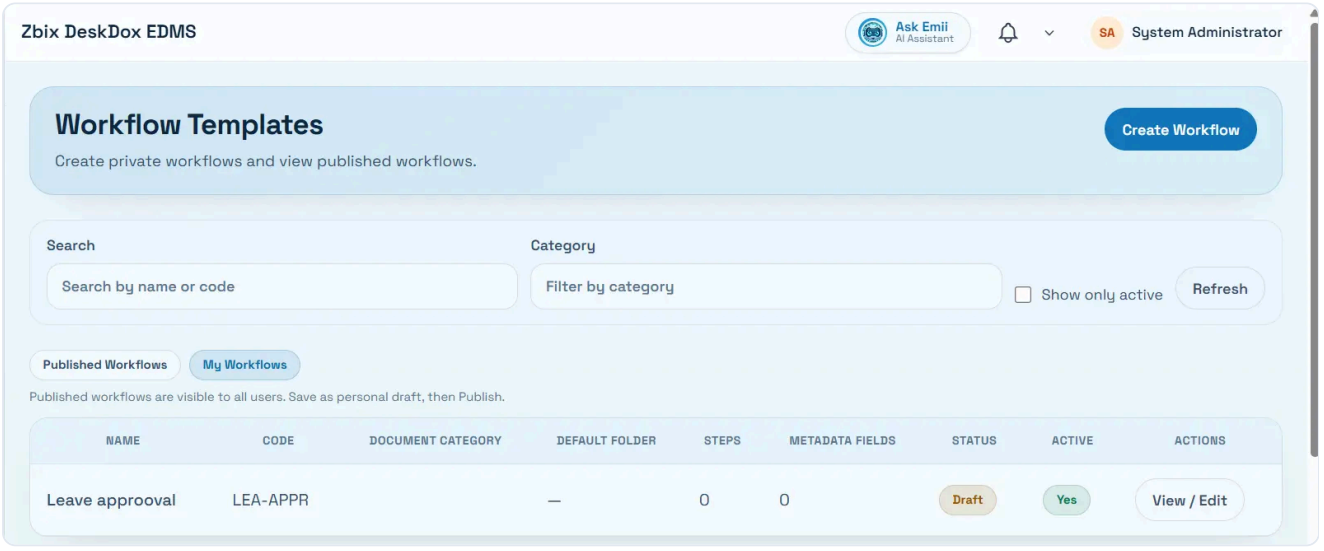
- "What is Workflow Supervision?"
- "Where can I see stuck workflows?"
- "Can an admin reassign or intervene in a workflow?"

Workflow Administration · 2 min read · Reviewed 2026-05-14

Workflow Template Activation and Status

What this helps you do

Understand the difference between draft/published status and active/inactive availability.



Draft, published, active, and inactive

The editor shows a status pill for `Published` or `Draft`. The list page also shows status and an active badge of `Yes` or `No`.

`Publish` changes a draft toward published status when the button is visible. The `Publish` action is visible only when `canPublishWorkflowTemplate` is available and the template is not already published.

`Active` controls whether the template is enabled. A template can be published but inactive. Inactive or draft templates may be visible to admins but should not be assumed to appear during upload or new workflow selection.

Upload availability

Upload workflow selection uses active published templates. If a template is not available during upload, check published status, active flag, user permissions, category or upload filters, and whether you are looking at the correct tenant or environment.

Safe activation practices

Before activating or publishing, check the name, code, default folder, required metadata, step order, assignees, SLA settings, and test-template status. Template changes may affect only new workflows depending on workflow versioning and how existing workflow instances were started.

Avoid editing an active template casually. If the change affects routing or compliance, document the change and confirm whether existing in-progress workflows should continue under their original configuration.

Related Emii questions

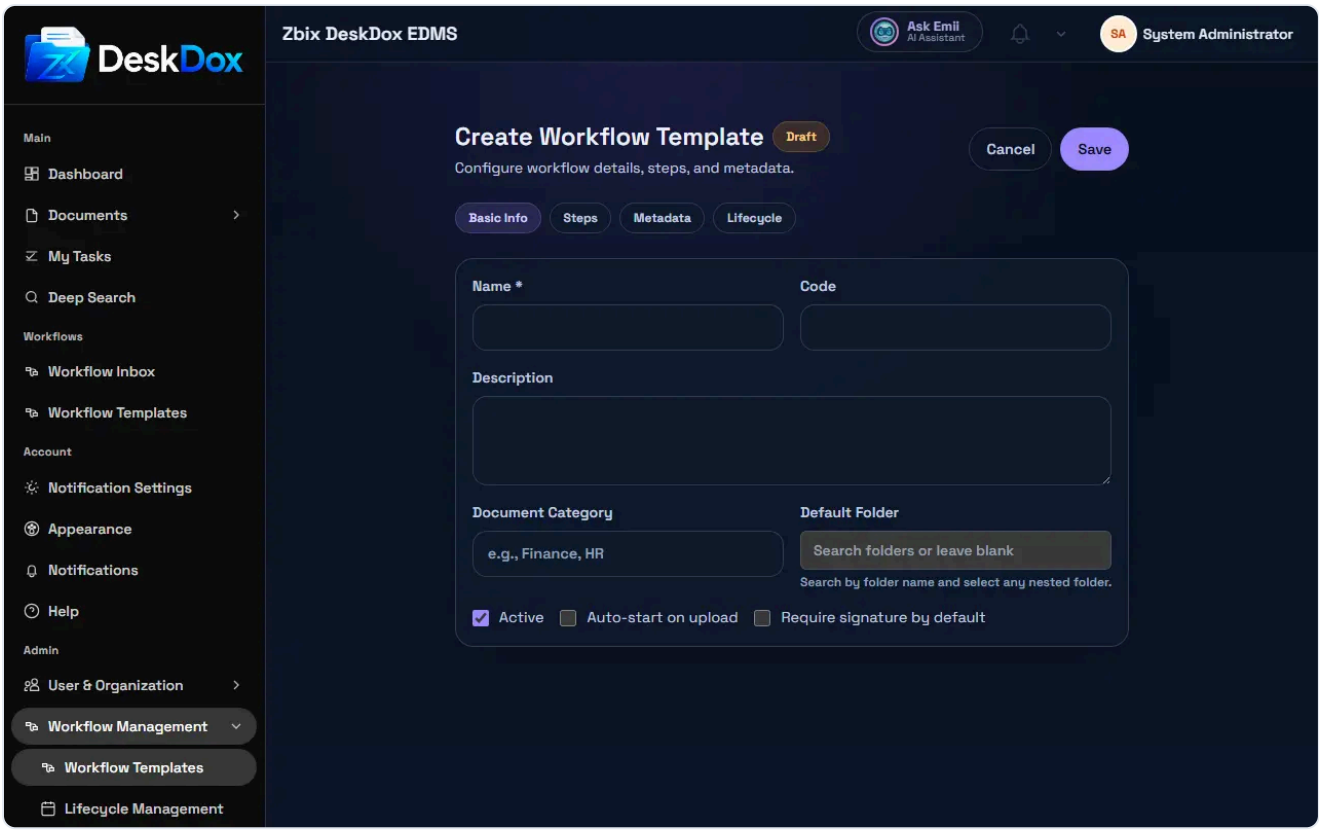
- "How do I activate a workflow template?"
- "Why is a workflow template not available during upload?"
- "Should I edit an active workflow template?"

Workflow Administration · 2 min read · Reviewed 2026-05-14

Workflow Template Basic Info

What this helps you do

Configure the core details that identify a workflow template and influence how it appears to users.



Basic fields

The `Basic Info` tab includes `Name *`, `Code`, `Description`, `Document Category`, `Default Folder`, `Active`, `Auto-start on upload`, and `Require signature by default`.

`Name *` is the user-facing template name. `Code` is a unique identifier and may be generated from the name, but it is validated on save. `Description` helps admins understand the purpose of the template. `Document Category` can be used to group or filter templates.

Ownership, department, or availability details may also appear depending on configuration. Use those values to keep template responsibility and access clear for administrators.

Default folder and upload availability

`Default Folder` sets a preferred destination folder for documents that use the template when that behavior is supported by the upload or workflow flow.

A workflow template may not be available during upload if it is draft, inactive, filtered out by category or configuration, hidden by permissions, or not published. Upload selection is based on active published templates.

Active status

`Active` controls the template's active flag. Inactive templates may remain visible to admins but should not be assumed to be selectable by normal users during upload.

Use inactive status for drafts, tests, or retired workflows when you do not want new workflows to start from that template.

Related Emii questions

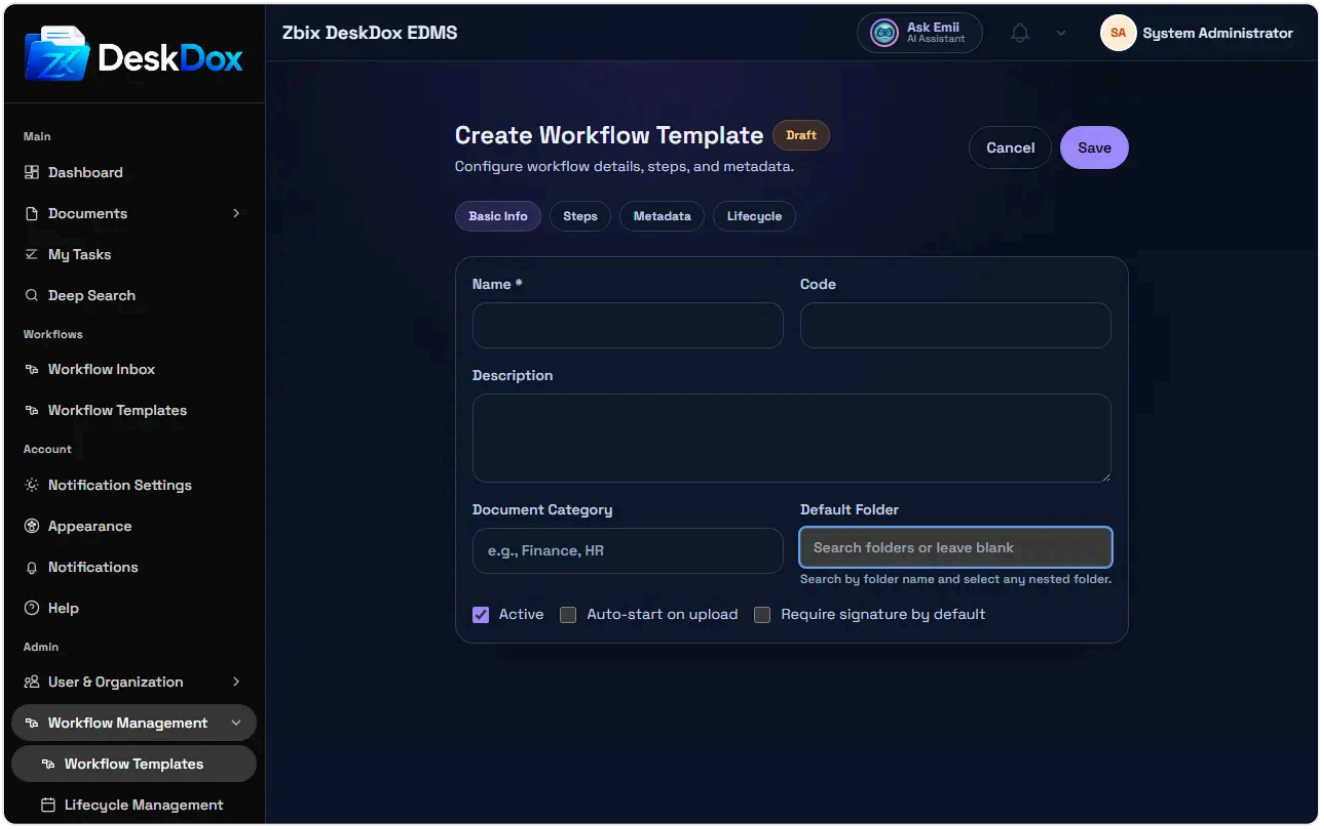
- "What does default folder mean in a workflow template?"
- "Why is a workflow template not available during upload?"
- "What happens if a template is inactive?"

Workflow Administration · 2 min read · Reviewed 2026-05-14

Workflow Template Default Folder Picker

What this helps you do

Select the default destination folder used by a workflow template when the configured flow supports it.



Searchable folder selection

`Default Folder` uses a searchable folder picker. It displays the full folder path and can be cleared.

Subfolders are searchable by name and can be selected when they are returned by the folder search. Do not assume only root folders are selectable.

Why a folder may not appear

A folder may be missing because the search text does not match it, the folder is outside the search scope, the user lacks permission to see or use it, the folder is inactive, or the folder is unavailable in the current configuration.

If only some folders are visible, compare folder permissions, department scope, and whether the folder is a root folder or subfolder. Ask an administrator to check folder availability if the folder exists and permissions look correct.

Upload relationship

The default folder can influence the destination used when documents start from the template, depending on upload configuration. If uploads still go elsewhere, check the upload folder selection, template active/published status, and whether your tenant uses the template default folder in that upload path.

Related Emii questions

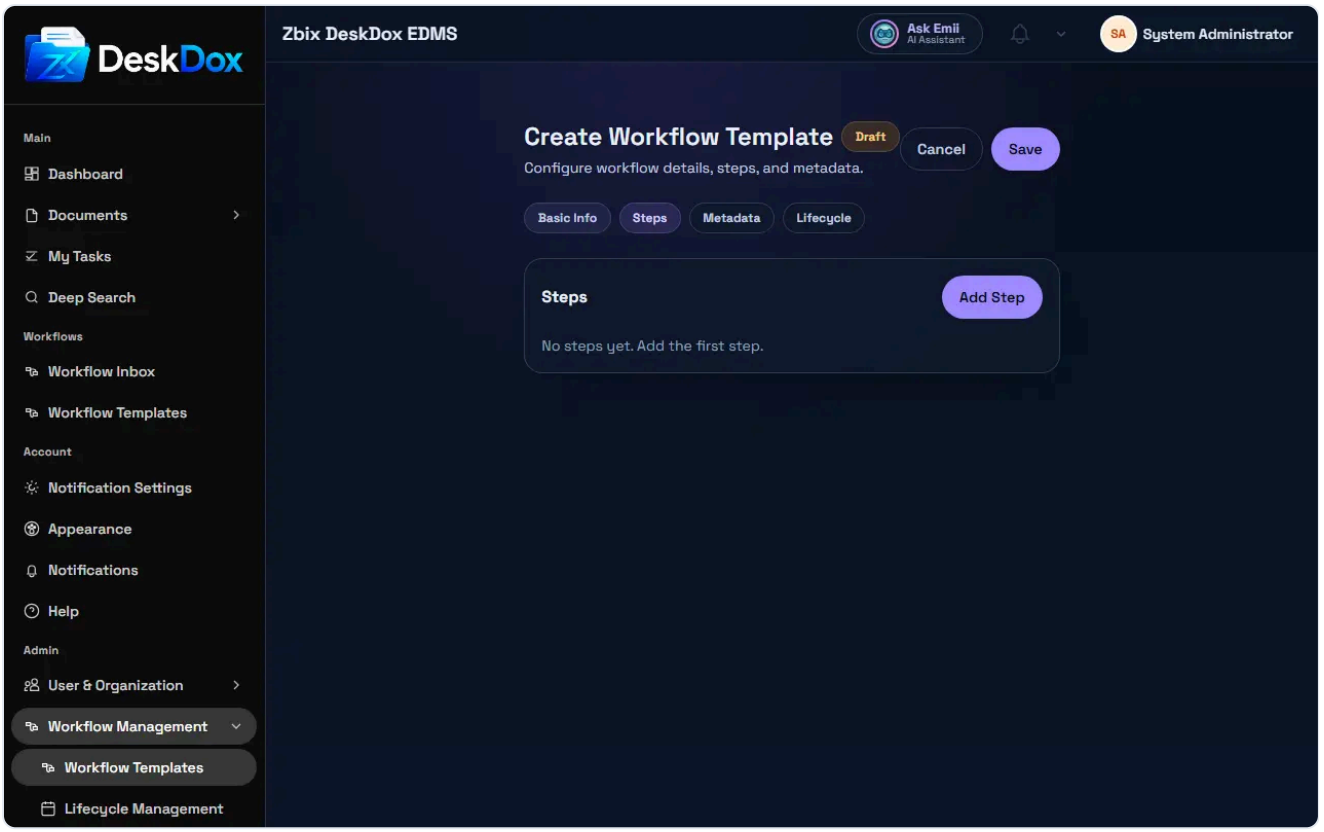
- "Can I select a subfolder as default folder?"
- "Why can't I find a folder in the picker?"
- "How does default folder affect uploads?"

Workflow Administration · 2 min read · Reviewed 2026-05-14

Workflow Template Steps and Routing

What this helps you do

Configure the approval or review stages that determine who receives workflow tasks, and how documents are routed through the approval path.



Step order

Use `Add Step` to add a step. Each step appears as `Step {N}` with `Step Name`, assignment fields, behavior toggles, and SLA settings when available. Steps can be reordered with the visible up and down controls and removed with `Remove`.

Assignee types and routing

Workflow routing is controlled by the assignee type on each step. Supported assignee types are `User`, `Role`, `Department`, `Department Head`, and `Metadata Email`.

- `Assignee User` selects a specific user.
- `Assignee Role` accepts a role value such as `edms_admin`.
- `Department` selects a department for department or department-head routing.
- `Metadata Email Field` selects from email-type metadata fields defined on the template.

Each step routes the workflow task to its assigned approver or reviewer in sequence. When a step is assigned to a department, eligible department members can see the pooled task and one user should claim it before acting.

Missing or wrong approver

If an approver is missing or a task goes to the wrong user, check the assignee type, selected user, role spelling, department membership, department head setup, metadata email value, required metadata, and whether the template version used by the live workflow matches the template you edited.

If no valid assignee is found, the workflow may fail to start, become stuck, or require admin supervision depending on system behavior and configuration.

Related Emii questions

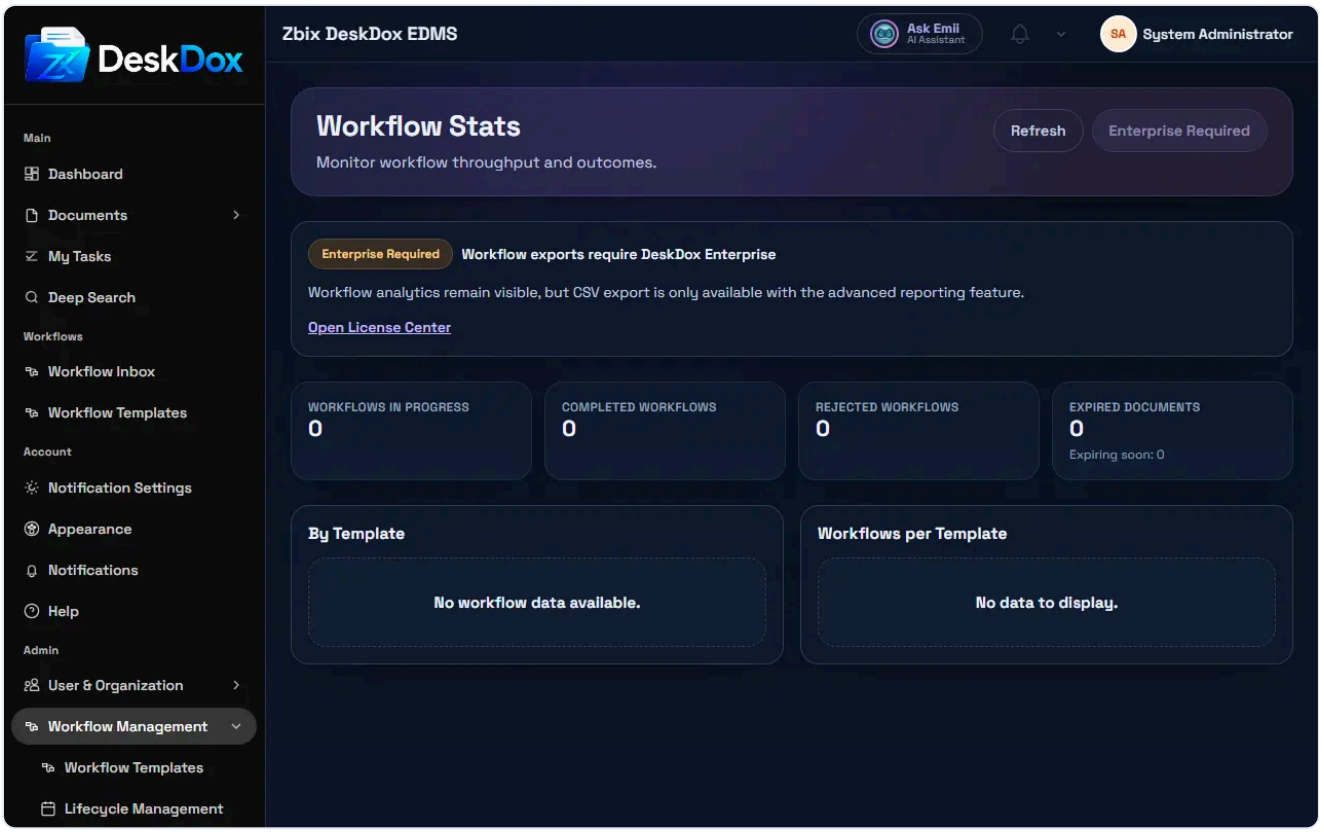
- "How do I add workflow steps?"
- "How do I assign approvers?"
- "Can I assign a workflow step to a department?"
- "What happens if no approver is found?"
- "How does workflow routing work?"

Workflow Administration · 2 min read · Reviewed 2026-05-14

Workflow Stats Dashboard

What this helps you do

Use the admin workflow reporting page to review workflow volume and outcomes.



What the page shows

`Workflow Stats` is an admin-only page. Controls include `Refresh` and `Export Workflows CSV`. Export can show `Enterprise Required` when the `advanced_reporting` license feature is not available.

The page includes summary cards for `Workflows In Progress`, `Completed Workflows`, `Rejected Workflows`, and `Expired Documents`, plus a `By Template` table with `Template Name`, `In Progress`, `Completed`, `Rejected`, and `Avg Completion`. It also shows a `Workflows per Template` bar chart.

Interpreting stats

Workflow Stats are administrative reporting totals. They can differ from `My Tasks` because `My Tasks` is user-assignment focused, while stats summarize workflow instances by status, template, and reporting rules.

Use stats to spot throughput, completion rates, rejected work, SLA or overdue indicators when visible, and templates with heavy activity. Use Workflow Supervision for live stuck or overdue tasks.

Export and refresh

Use `Refresh` to reload data. Use `Export Workflows CSV` only when available. If the page shows `Enterprise Required`, the export action depends on the Enterprise reporting license feature.

If stats do not update immediately, refresh and allow reporting jobs or reporting aggregation to complete. Confirm you are comparing the same date window, template scope, workflow status, and permission scope.

Related Emii questions

- "Where can I see workflow statistics?"
- "Why are workflow stats different from My Tasks?"
- "Can I export workflow statistics?"

CHAPTER 9

Emii AI

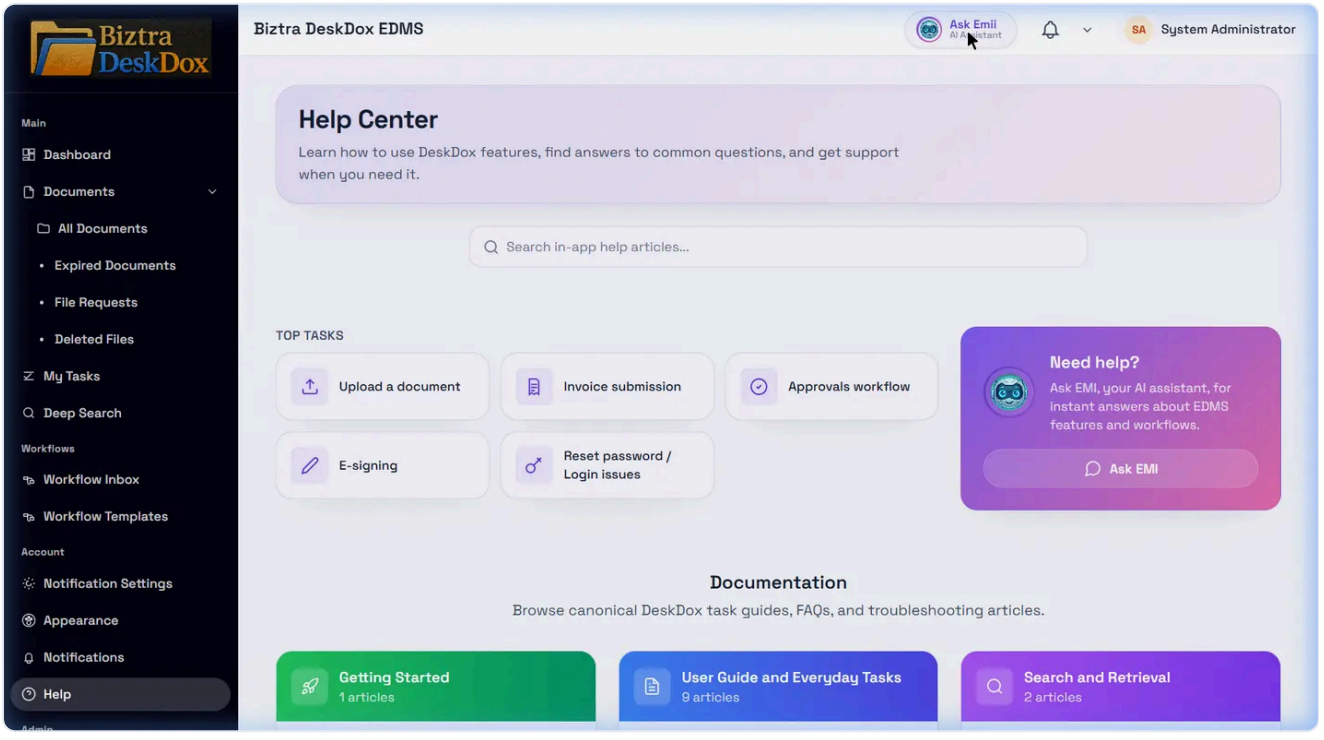
Emii AI entry points, effective use, and permission-aware assistance.

Emii AI · 2 min read · Reviewed 2026-05-13

How to Use Emii Effectively

What this helps you do

Ask Emii focused questions, understand when it uses Help Center articles, and verify source-based answers.



Who can use it

Users with Emii enabled in their environment can ask help or document questions. Available modes and scope may vary by deployment and permissions.

Required permissions

- Emii access.

- Document access when asking about uploaded documents.
- Help Center access when asking product how-to questions.

Where to open Emii

- Header `Ask Emii` button (if enabled)
- Help Center `Ask EMI` card
- Task-review Emii surfaces in workflow context

Ask Emii about DeskDox features

For product or how-to questions, ask about the DeskDox feature directly. Emii should search Help Center articles first for questions about uploading, sharing, workflow, lifecycle, users, departments, audit trail, Help Center, and permissions.

Best prompt pattern

Include:

- What you need ("summarize", "compare", "next action")
- Relevant context (document name/ID, workflow step)
- Scope request (single document vs broader help)

Good examples

- "Summarize the key obligations in this document."
- "What should I verify before approving this task?"
- "Why might my search return no results?"
- "How do I create a user and assign a department?"
- "Why did lifecycle not move documents?"

Safe use guidelines

- Verify citations or linked source context before making decisions.
- Use Emii as guidance, not policy override.
- Escalate uncertain or high-impact conclusions to a human approver/admin.

Understand source-based answers

When Emii answers a Help Center question, it should refer to the source article or section it used. If the Help Center has no matching article, Emii should say that clearly and avoid inventing DeskDox-specific steps.

Common mistakes

- Asking a document-content question when you meant to ask product help, or the reverse.
- Asking without enough feature context.
- Treating Emii guidance as approval authority.
- Ignoring citations or source article names.

Troubleshooting

If Emii cannot answer, rephrase with the module name and task. If it cites the wrong topic, open the Help Center article directly or try a more specific question. If Emii is not visible, ask an administrator whether it is enabled for your environment.

Related reading

- Search the Help Center
- User Manual: Using Emii
- Common Issues

CHAPTER 10

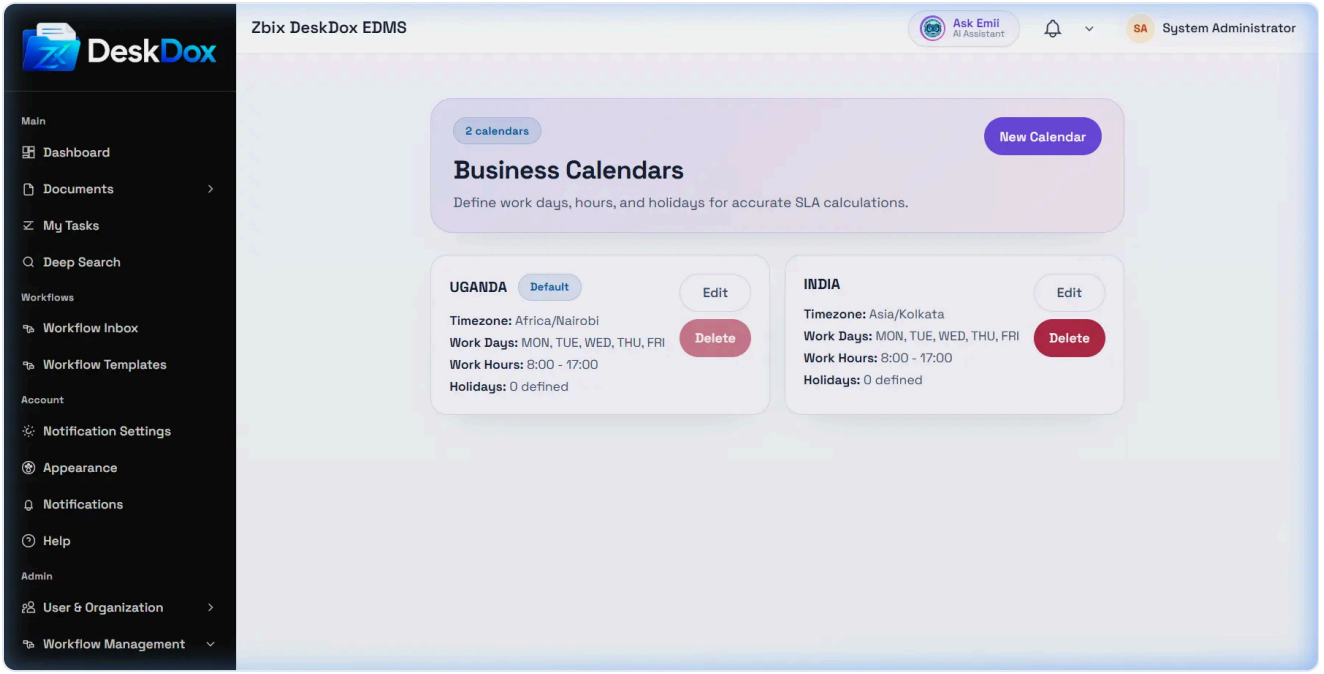
Administration and Operations

System settings, notifications, email, licensing, branding, and operating procedures.

Administration and Operations · 1 min read · Reviewed 2026-05-14

Business Calendars Overview

Business calendars define working days, working hours, timezone, and holidays used for SLA and due-date calculations. Manage them at `/app/admin/business-calendars`.



Why calendars matter

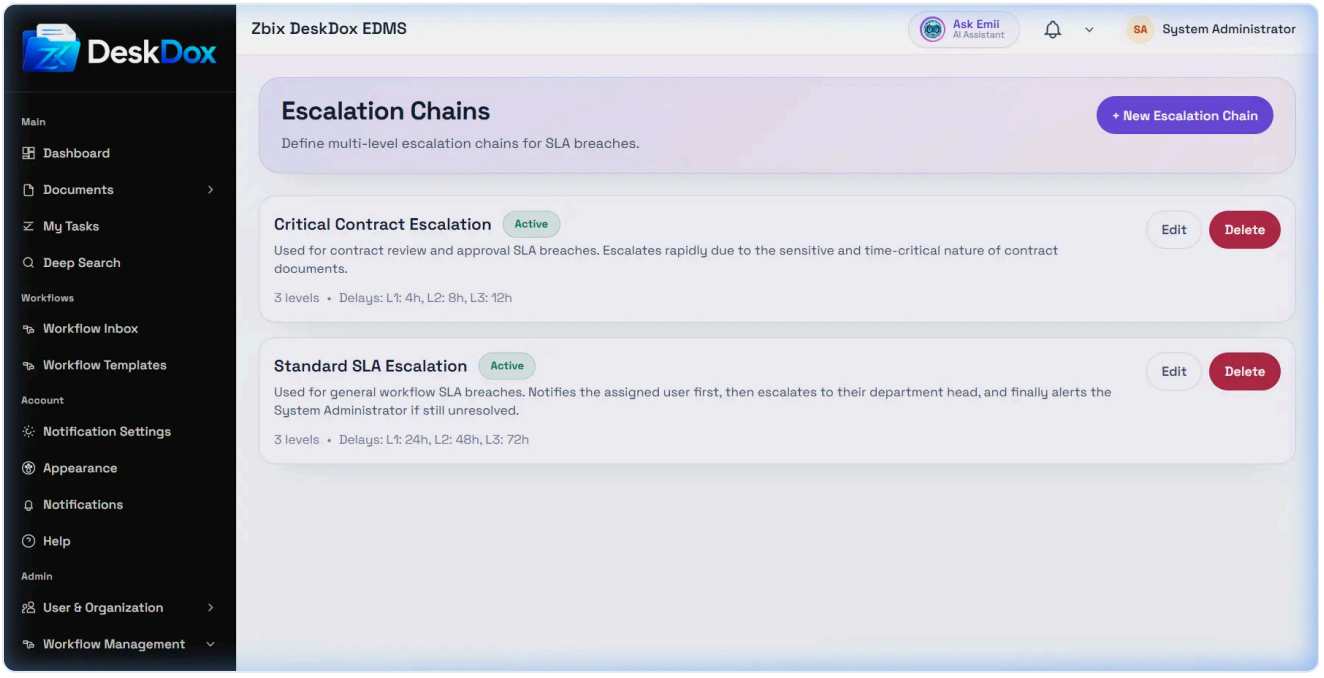
When a workflow step uses a business calendar, DeskDox can exclude non-working time such as weekends and configured holidays from SLA calculations. This helps avoid due dates that incorrectly count closed-office time.

Business calendar management is an admin feature. Standard users usually experience its effect through task due dates, overdue indicators, and SLA breach status rather than managing calendars directly.

Administration and Operations · 1 min read · Reviewed 2026-05-14

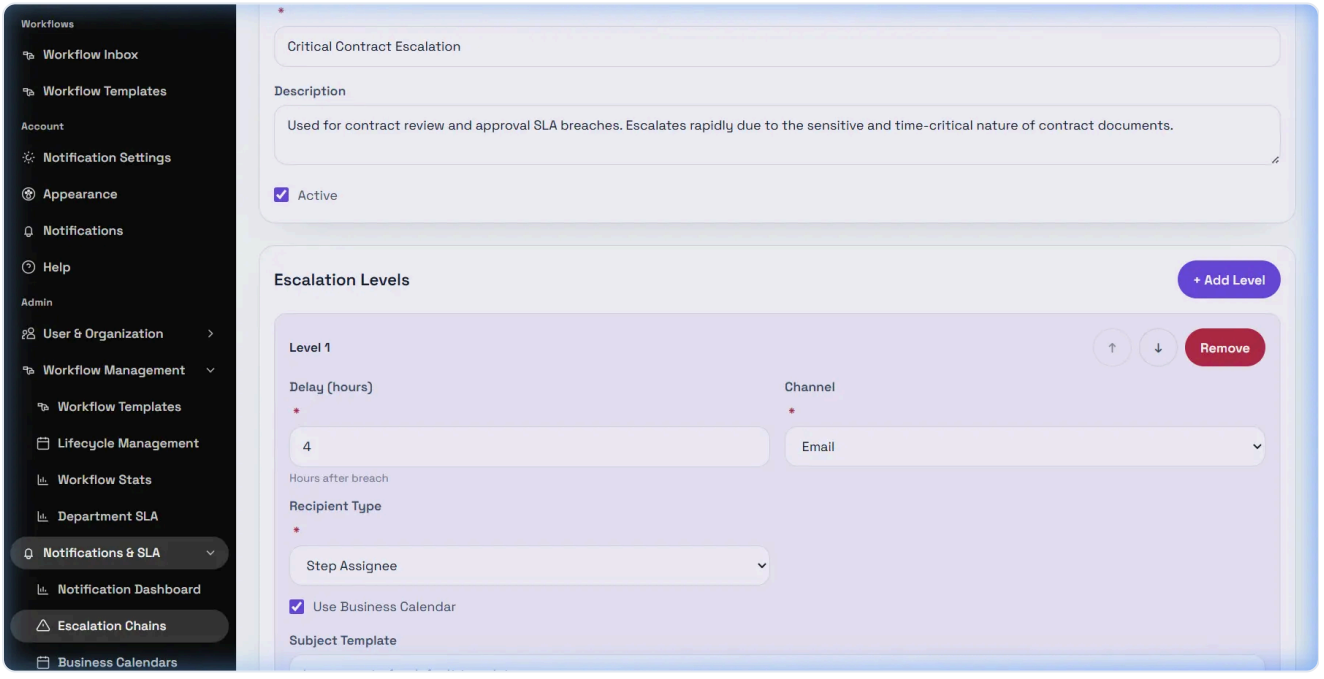
Escalation Chains Overview

Escalation chains are reusable sets of escalation levels for workflow steps that breach SLA. Manage them at `/app/admin/escalation-chains`.



How chains are used

Workflow admins create a chain once, then select it from a workflow template step's `Escalation Chain` field. When the step breaches its SLA, configured escalation levels can notify the selected recipients at defined intervals, depending on notification engine configuration.



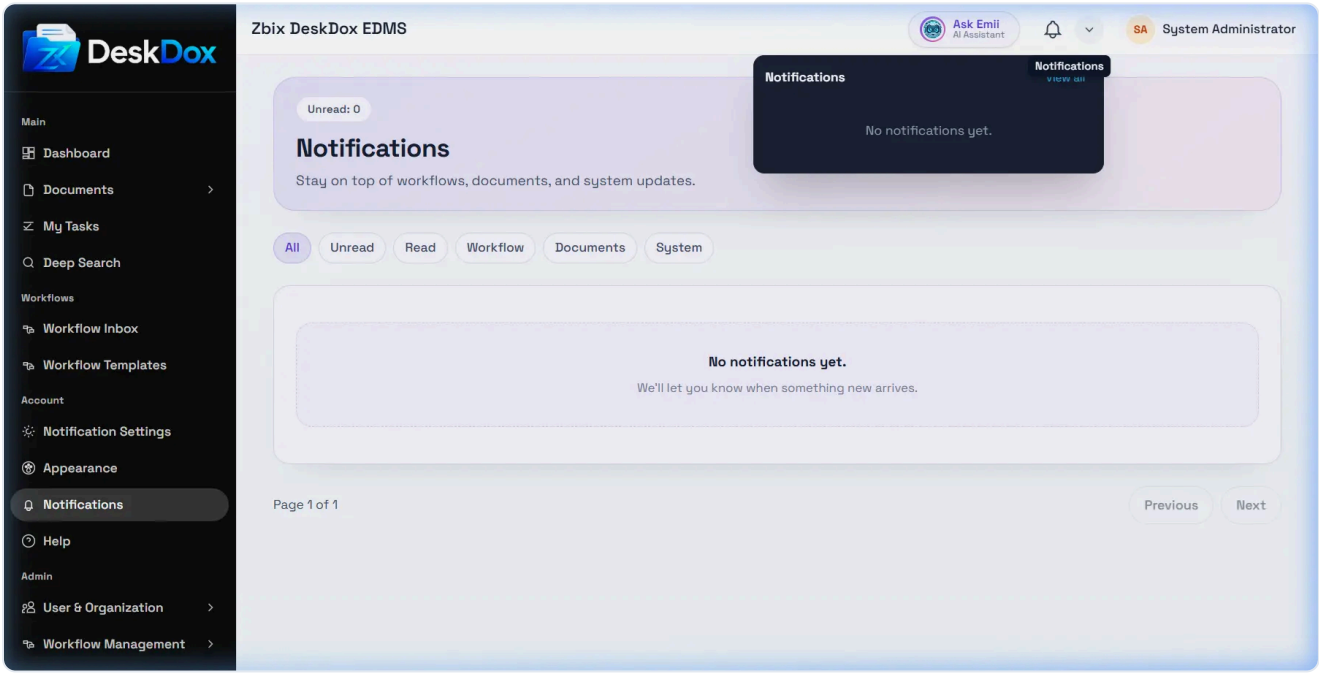
Permissions

Escalation chains are an admin feature. Standard users can see their own tasks and notifications, but they do not manage global escalation chains unless their role includes the required admin permissions.

Administration and Operations · 2 min read · Reviewed 2026-05-14

Notifications Overview

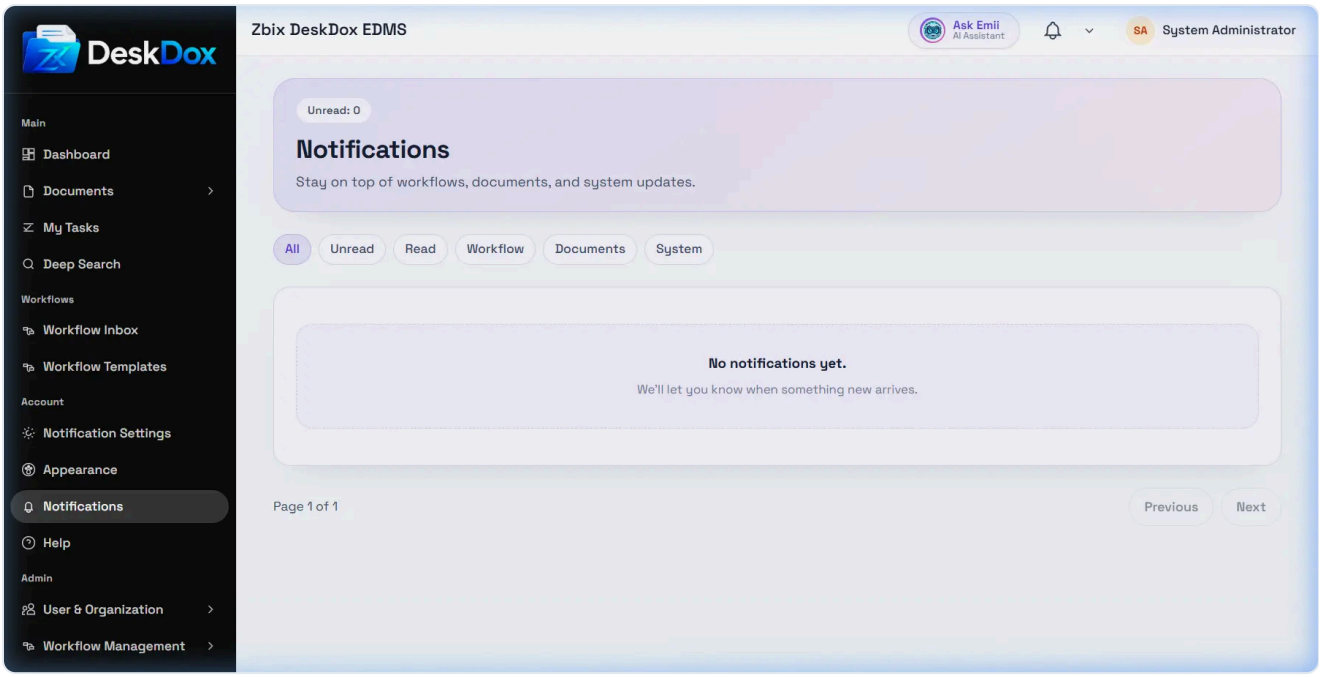
Notifications are DeskDox alerts for items that may need attention, such as workflow activity, document events, system events, reminders, and SLA-related workflow updates when those features are configured.



Where notifications appear

Use the topbar `Notifications` bell for quick access. The bell can show an unread count when unread notifications exist. The adjacent menu opens a dropdown with recent notification items, `View all`, and `Mark all as read` when there are unread items.

Use `/app/notifications` for the full notification center. In the environment the notification center had no active notifications, so the available screenshot shows the empty state rather than a populated history.



Relationship to workflow, SLA, and escalations

Notifications can be created by workflow assignments, document activity, system events, SLA warnings, SLA breaches, and escalation chains depending on configuration. Workflow SLA settings are configured on workflow template steps. Escalation chains can then define follow-up levels after a step breaches its SLA.

Notification delivery depends on the channel and configuration. In-app notifications are available in DeskDox. Email preferences are available, but actual email delivery depends on email service and queue configuration. Mobile or push delivery should be treated as configuration-dependent unless enabled in your deployment.

If notifications are missing

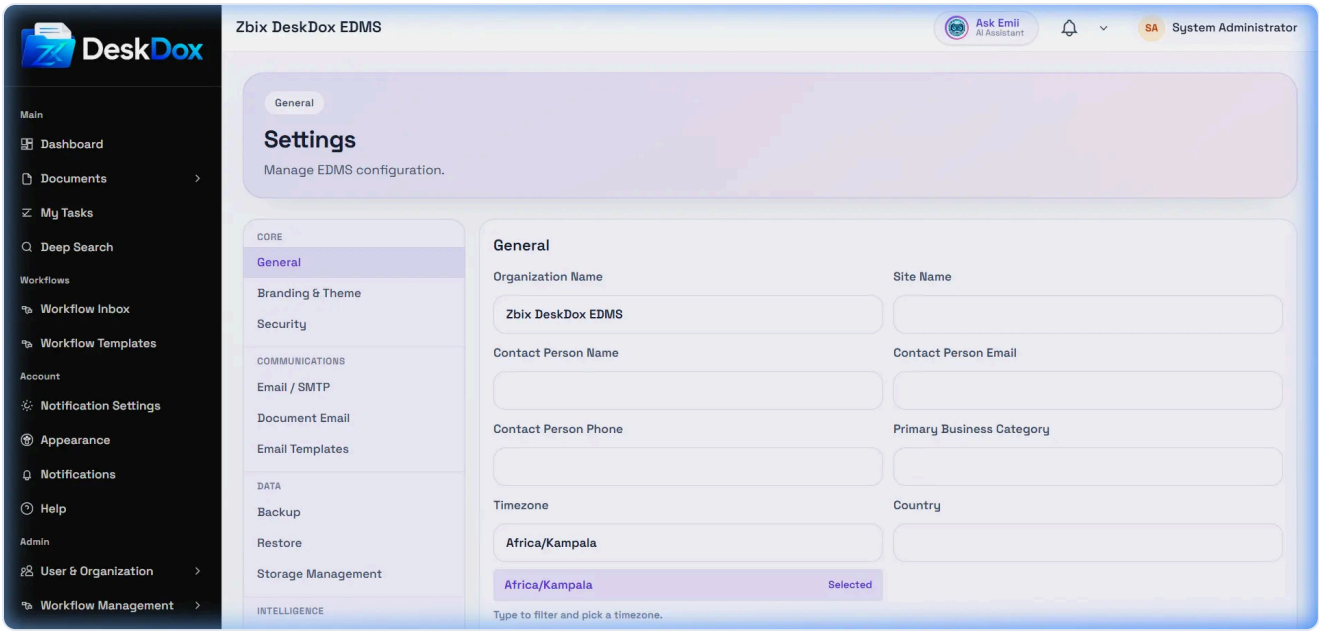
Check the notification center, your notification preferences, whether the event applies to your user or role, the linked document or workflow permissions, and whether the workflow/SLA/escalation feature is enabled. Administrators should also check email delivery configuration, notification rules, background jobs, and role or department assignment.

Administration and Operations · 1 min read · Reviewed 2026-05-14

System Settings Overview

System Settings is the administration area for deployment-wide DeskDox configuration. Open `/app/admin/system/settings/general` to start from General settings, then use the left settings menu for Branding & Theme, Security, Email / SMTP, Document Email, Email Templates, Backup, Restore, Storage

Management, and System Status. License Center and Audit Logs are separate admin routes at `/app/admin/license` and `/app/admin/audit-logs`.



Only administrator accounts can use these screens. DeskDox shows System Admins can access all listed sections. EDMS Admins can access settings sections except the backup, restore, and storage sections that are restricted to System Admins. If the page shows `You are not authorized to view this page`, your account does not have the required admin role.

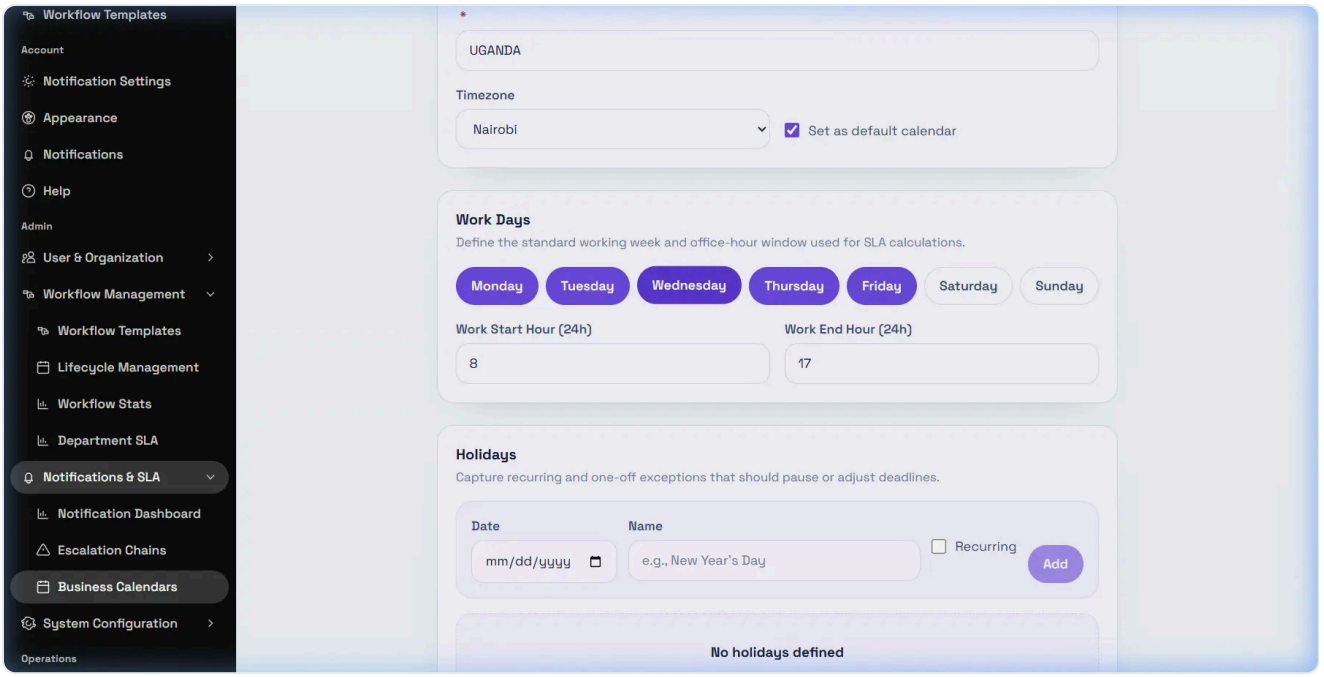
Configure high-impact settings carefully. Start with organization identity, branding, security policy, SMTP, document email, and backup readiness before relying on email notifications, secure links, scheduled backup, restore, or audit investigations.

Some values may be deployment-controlled instead of UI-controlled. If a setting is not visible, it may not be enabled for your role or environment. Public/Base URL behavior may depend on environment configuration and should not be treated as a visible admin setting unless it is shown in your installation.

Administration and Operations · 1 min read · Reviewed 2026-05-14

Create or Edit Business Calendar

Use `/app/admin/business-calendars` and select `New Calendar` or `Edit` to maintain a calendar for SLA timing.

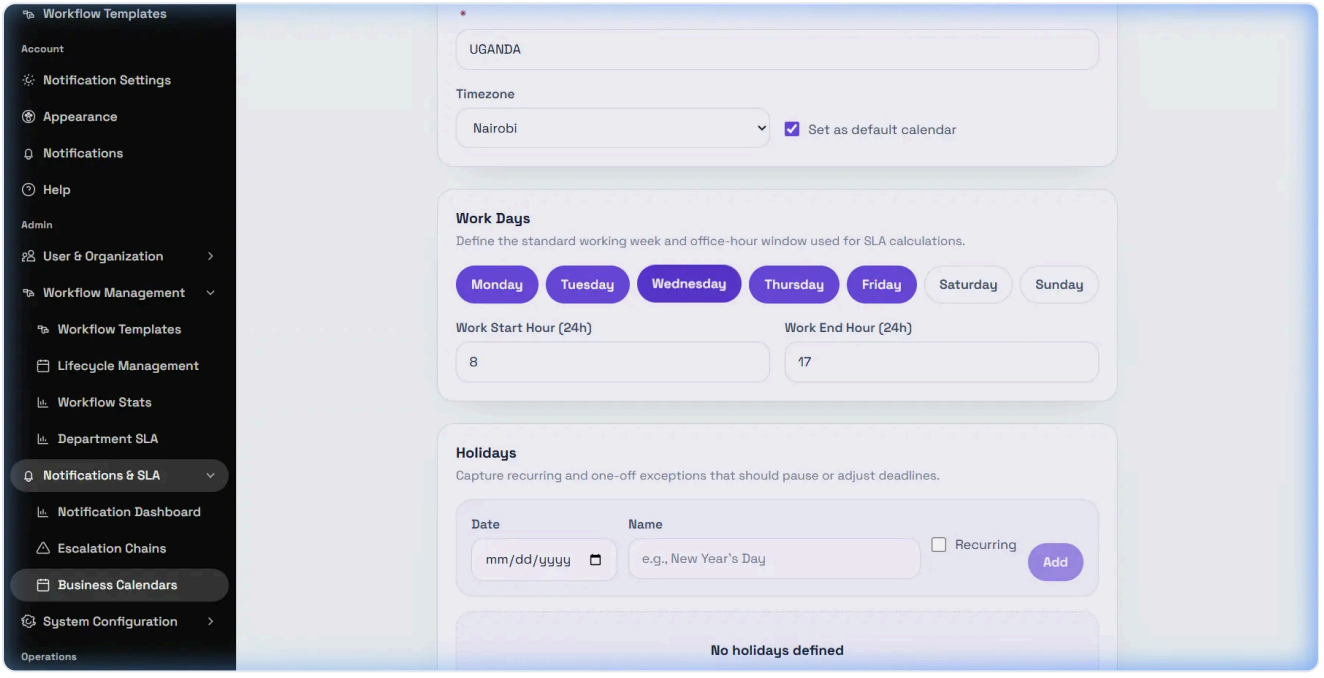


Calendar fields

DeskDox includes `Name`, `Timezone`, `Set as default calendar`, weekday buttons from Monday through Sunday, `Work Start Hour (24h)`, and `Work End Hour (24h)`. `Name` is required before `Save Calendar` is enabled.

Holidays

Use the Holidays section to add exception dates. Enter `Date`, optional `Name`, choose `Recurring` when the date repeats yearly, then select `Add`. Existing holiday rows can be removed with `Remove`.

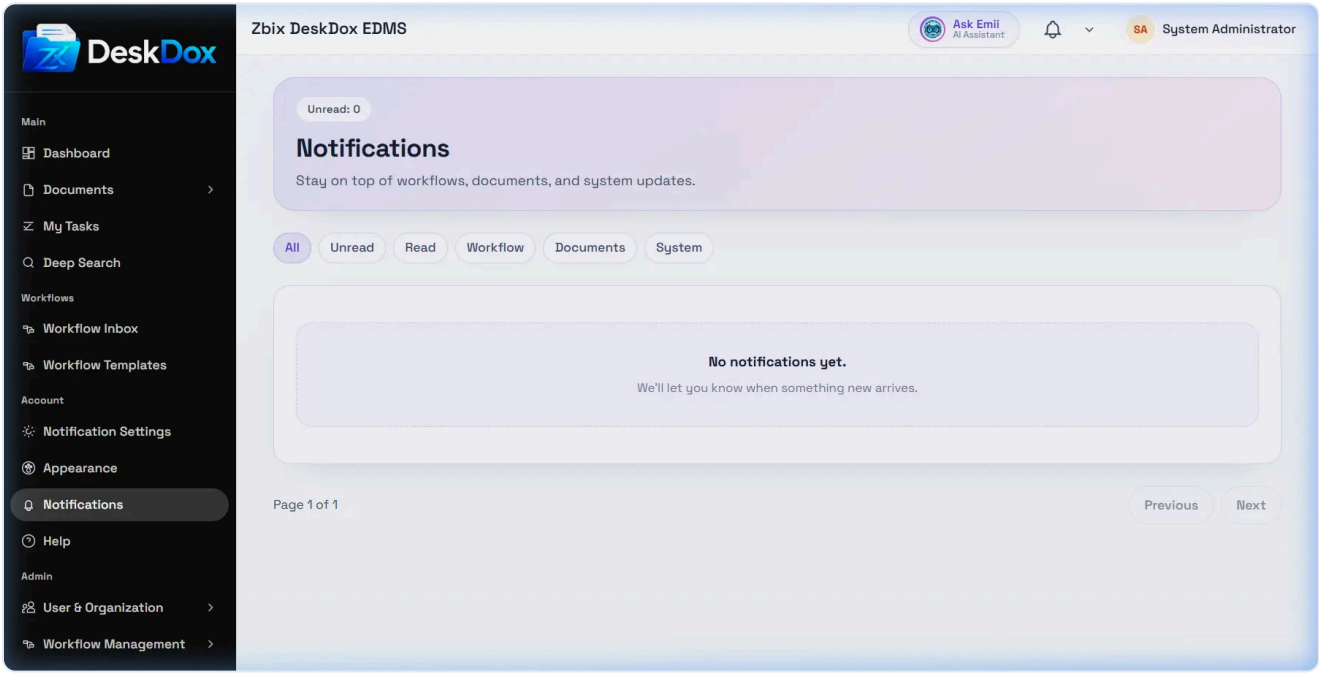


Use `Cancel` to close without saving. Use `Save Calendar` to persist the calendar.

Administration and Operations · 2 min read · Reviewed 2026-05-14

Notifications List and Actions

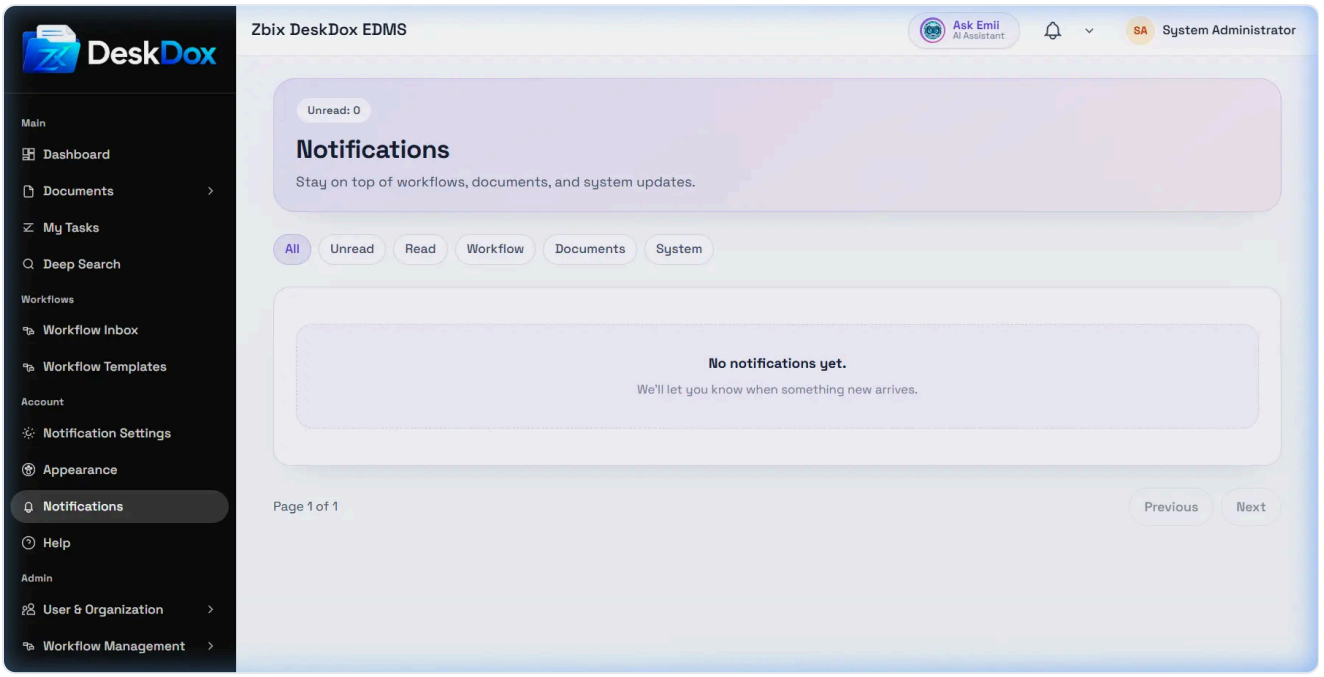
Open `/app/notifications` to view the notification center. The notification bell can also send you to this page with the `Unread` or `All` filter selected.



Filters and paging

DeskDox includes these notification center tabs: `All`, `Unread`, `Read`, `Workflow`, `Documents`, and `System`. The page shows 10 notifications per page and includes `Previous` and `Next` paging controls when more pages exist.

The `notifications-list.png` capture is identical to the empty-state image, so it is indexed as another notification center empty-state reference, not as proof of a populated notification history.



Read behavior

When you open an unread notification from the list, DeskDox marks that notification as read. If the notification points to a document, DeskDox opens the document route. If it points to a workflow, DeskDox opens the workflow route. Some notifications may not have a separate detail page.

`Mark all as read` appears when unread notifications exist. It can show success text such as `Marked 3 notifications as read` or `Nothing to mark as read` depending on the result.

Empty list troubleshooting

`No notifications yet.` means no matching notifications were returned for the current filter. `You're all caught up.` appears for an empty unread view. Check the selected filter, notification preferences, linked workflow or document permissions, and whether an event has actually occurred for your account.

Administration and Operations · 2 min read · Reviewed 2026-05-15

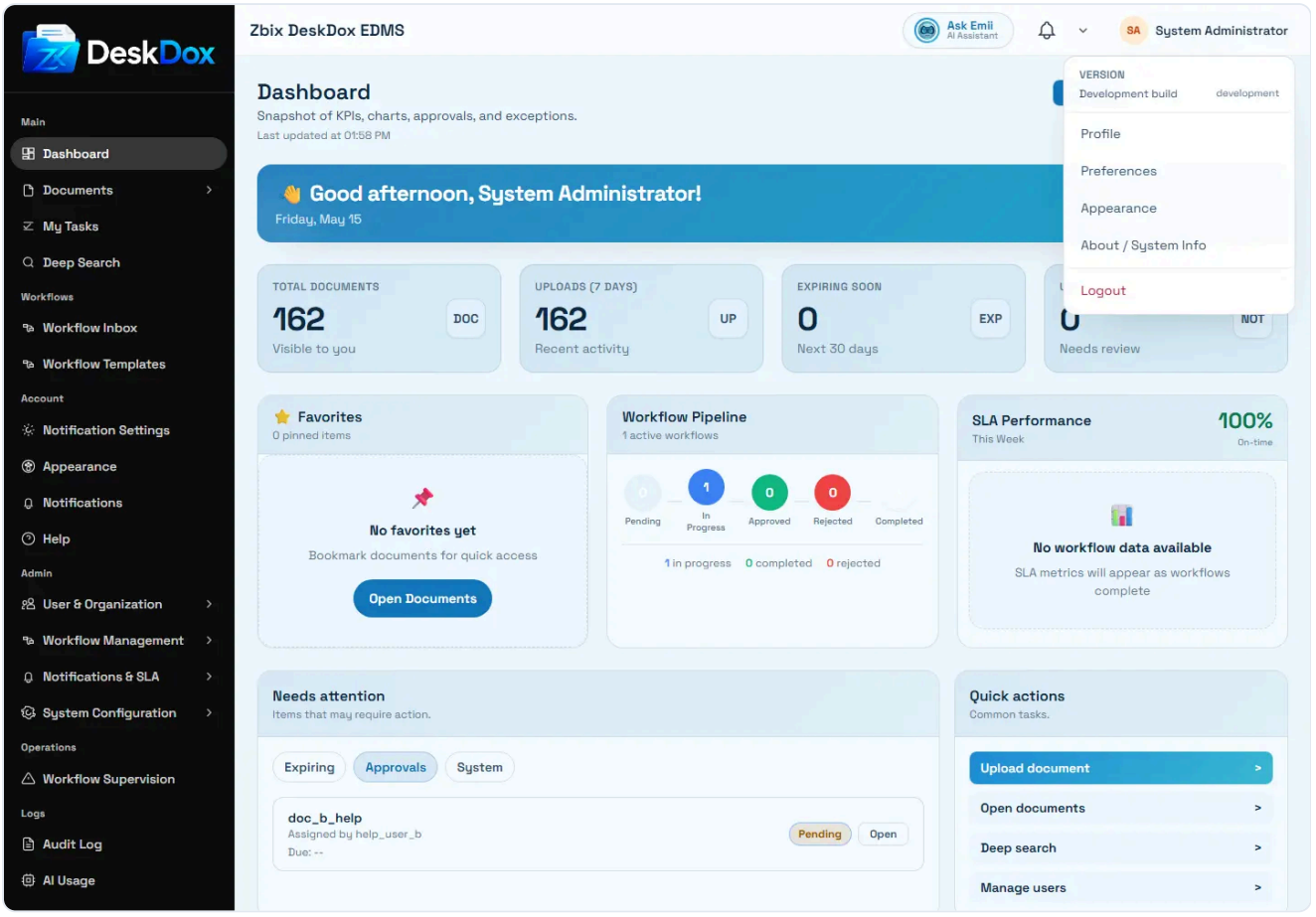
Profile and Account Menu

What this helps you do

Use the profile menu to open profile details, preferences, appearance settings, or log out.

Profile and account menu

Open the profile menu from the user initials or name in the topbar.



Menu options can include `Profile`, `Preferences`, `Appearance`, and `Logout`. Use `Profile` for profile details, password options, and account security controls. Use `Preferences` for notification preferences when available. Use `Appearance` for theme settings. Use `Logout` to sign out securely when you are finished.

Some administrator accounts may also see system information options. Exact menu options and placement may vary by screen size, permissions, and account configuration.

Profile page

The profile page showed fields including `Username` and `Email`, plus other profile details when visible. It also showed password fields labeled `Current`, `New`, and `Confirm`, with a `Change Password` action.

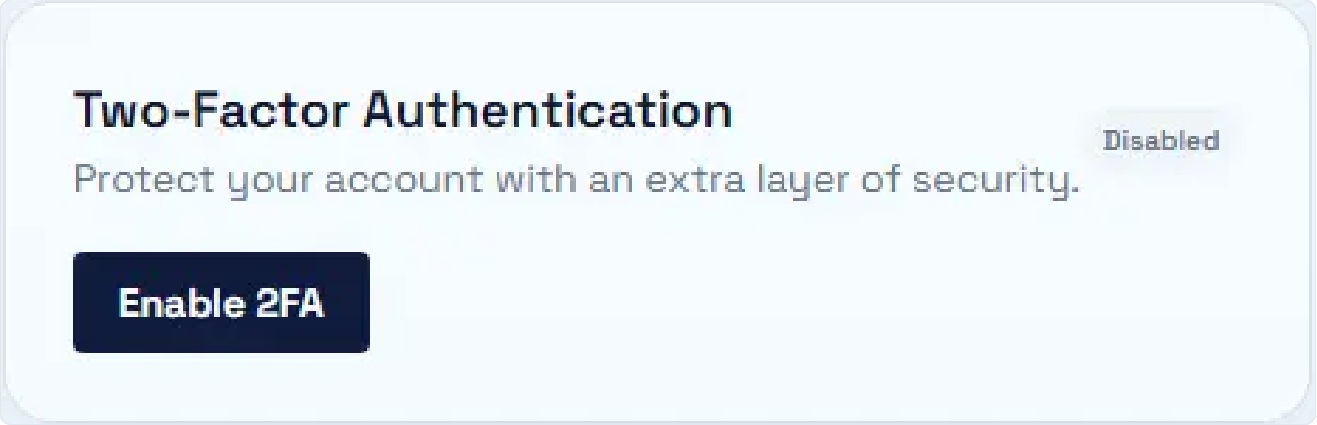
Use `Save` for editable profile details. Some fields may be admin-managed, identity-provider managed, or permission-controlled. If a field cannot be edited, ask an administrator whether that value is managed centrally.

Password and account details

Use `Change Password` only when the password form is visible and your account type allows local password changes. Role or department details may appear depending on configuration and permission.

Two-Factor Authentication

Two-Factor Authentication adds an extra verification step when signing in. If this option is available for your account, open the profile menu, go to `Profile`, and use the `Two-Factor Authentication` section.



The profile page can show whether 2FA is `Enabled` or `Disabled`. When 2FA is disabled, use `Enable 2FA` and follow the on-screen setup instructions. Setup may require scanning a QR code with an authenticator app, entering a 6-digit verification code, and storing backup codes safely if they are provided.

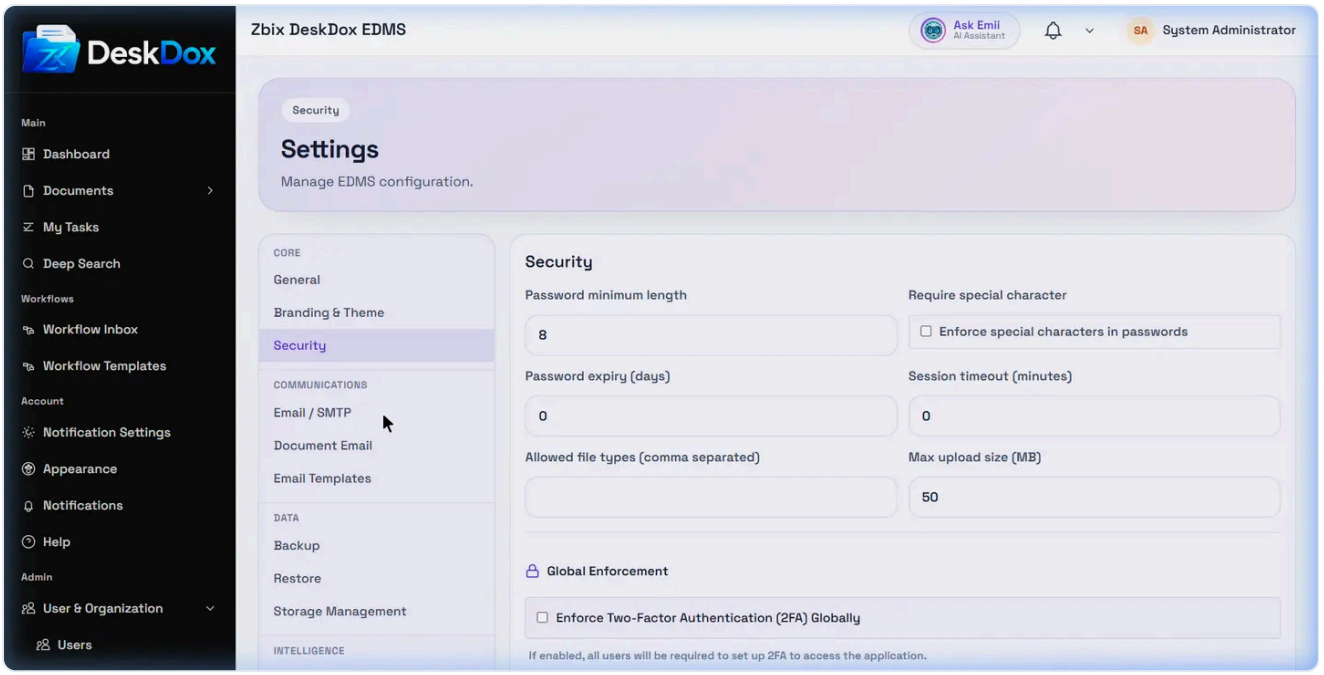
If 2FA is already enabled, the profile page may show a `Disable 2FA` option. Disabling 2FA may require your current password plus a one-time code or backup code.

Your organization may require 2FA based on its security policy. Availability and enforcement can depend on administrator configuration and your account permissions.

Administration and Operations · 1 min read · Reviewed 2026-05-14

Admin Security Settings

Open `/app/admin/system/settings/security` to configure deployment-level security settings.



DeskDox includes controls for Password minimum length, Require special character, Password expiry days, Session timeout minutes, Allowed file types, Max upload size in MB, and a global Enforce Two-Factor Authentication (2FA) toggle. The UI validates minimum password length, non-negative password expiry, and non-negative session timeout before saving.

Use conservative settings in production. Short sessions, stronger password rules, and global 2FA can improve security, but they can also affect every user. Communicate changes before enforcing them and confirm administrators can still sign in.

Security settings require admin access. If the page is not visible or says you are not authorized, ask a System Admin or EDMS Admin to review your role.

Administration and Operations · 1 min read · Reviewed 2026-05-14

Document Email Settings

Open `/app/admin/system/settings/document-email` to control document send-by-email behavior.

DeskDox includes a feature toggle, allowed send modes, maximum file attachment size in MB, default link expiry in hours, and maximum recipients across To and CC. The available send modes are `Send Link (Secure)` and `Send PDF Attachment` when enabled.

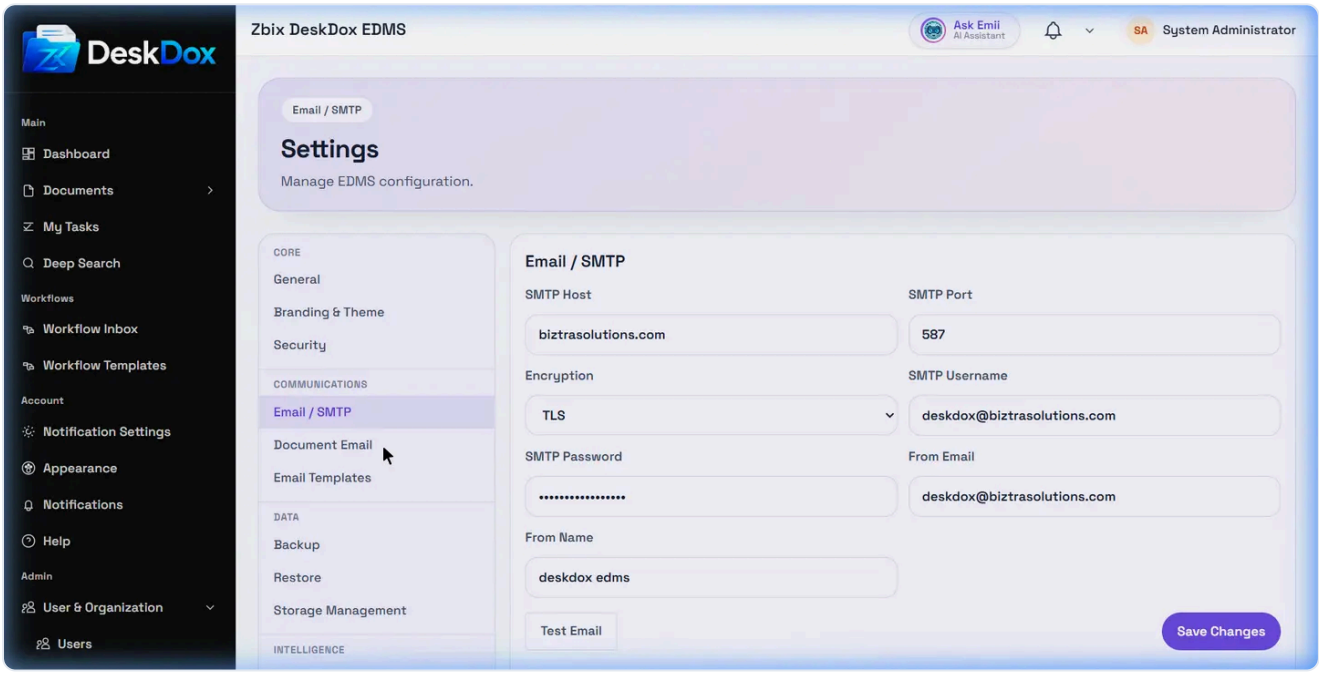
Document email depends on the general outbound email configuration. Enabling document email or allowing attachments does not guarantee delivery unless SMTP, network access, sender identity, and worker or synchronous send behavior are functioning.

Use the available document email settings to control how document messages are prepared and sent. If secure document links use the wrong host name, link generation may depend on deployment environment configuration.

Administration and Operations · 1 min read · Reviewed 2026-05-14

Email and SMTP Settings

Open `/app/admin/system/settings/smtp` to configure outbound email.



DeskDox includes SMTP Host, SMTP Port, Encryption, SMTP Username, SMTP Password, From Email, and From Name fields. The password field is secret input; do not paste real SMTP passwords, tokens, or keys into Help Center questions, screenshots, tickets, or chat.

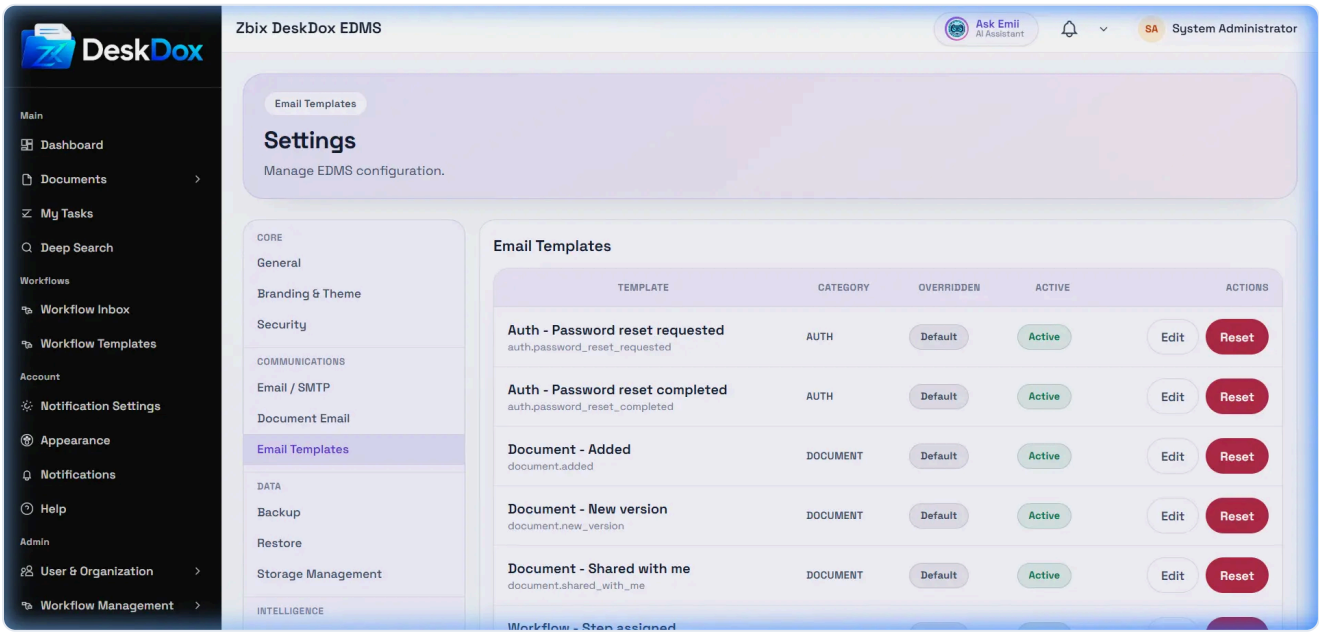
Use `Save Changes` to store SMTP settings. Use `Test Email` to open the Send Test Email dialog, enter a recipient address, and click `Send Test`. The test action submits the current SMTP settings to the system test process and reports success or failure.

A saved SMTP form does not prove email delivery works. Delivery still depends on a reachable mail server, accepted credentials, network/firewall rules, TLS or SSL compatibility, sender policy, and the recipient mail system. If email is not sending, run a test email, check the exact system service error, verify credentials outside DeskDox if permitted, and confirm the worker or synchronous send path is healthy.

Administration and Operations · 1 min read · Reviewed 2026-05-14

Email Template Settings

Open `/app/admin/system/settings/email-templates` to manage system email templates.



DeskDox includes a template table with Template, Category, Overridden, Active, and Actions columns. Use `Edit` to open the template editor, change the Subject and HTML Body, set whether the template is Active, and choose `Save changes`. Use `Reset` only when you intend to discard customizations and return to the system default.

Use the template variables shown in the template editor to insert document, workflow, recipient, or organization-specific values. Available variables may vary depending on the template type and system configuration.

Template changes affect message content, not delivery. SMTP configuration, sender policy, recipient address validity, and system service email processing must still be working.

Administration and Operations · 2 min read · Reviewed 2026-05-14

License Notices and Feature Access

What this helps you do

Understand conditional license notices and what to do when a feature is locked.

License notice visibility

License notices may appear in dashboard, topbar, account, or administration areas only when the license state requires attention. A license notice may appear only when the license state requires attention, such as inactive, expired, restricted, or reactivation-required states.

License notices may appear only when the license state requires attention, such as inactive, expired, restricted, or reactivation-required states.

Inactive or locked license

`License inactive` means the deployment may not currently have a valid active license state. A message such as `Deployment fingerprint changed beyond tolerance` means the deployment identity may have changed enough that reactivation is required.

Normal users should report the notice to an administrator or support team. Administrators or authorized support users should reactivate or repair the license through the approved license process.

Feature access and Emii

Some DeskDox features may depend on license, edition, configuration, or permissions. A locked feature does not always mean your account is broken.

Help Center articles and Emii Help / Guidance are separate from licensed document AI behavior. Help / Guidance should remain usable for Help Center questions when available. Document AI or document-RAG modes may still be blocked by AI license state, document permissions, or indexing configuration.

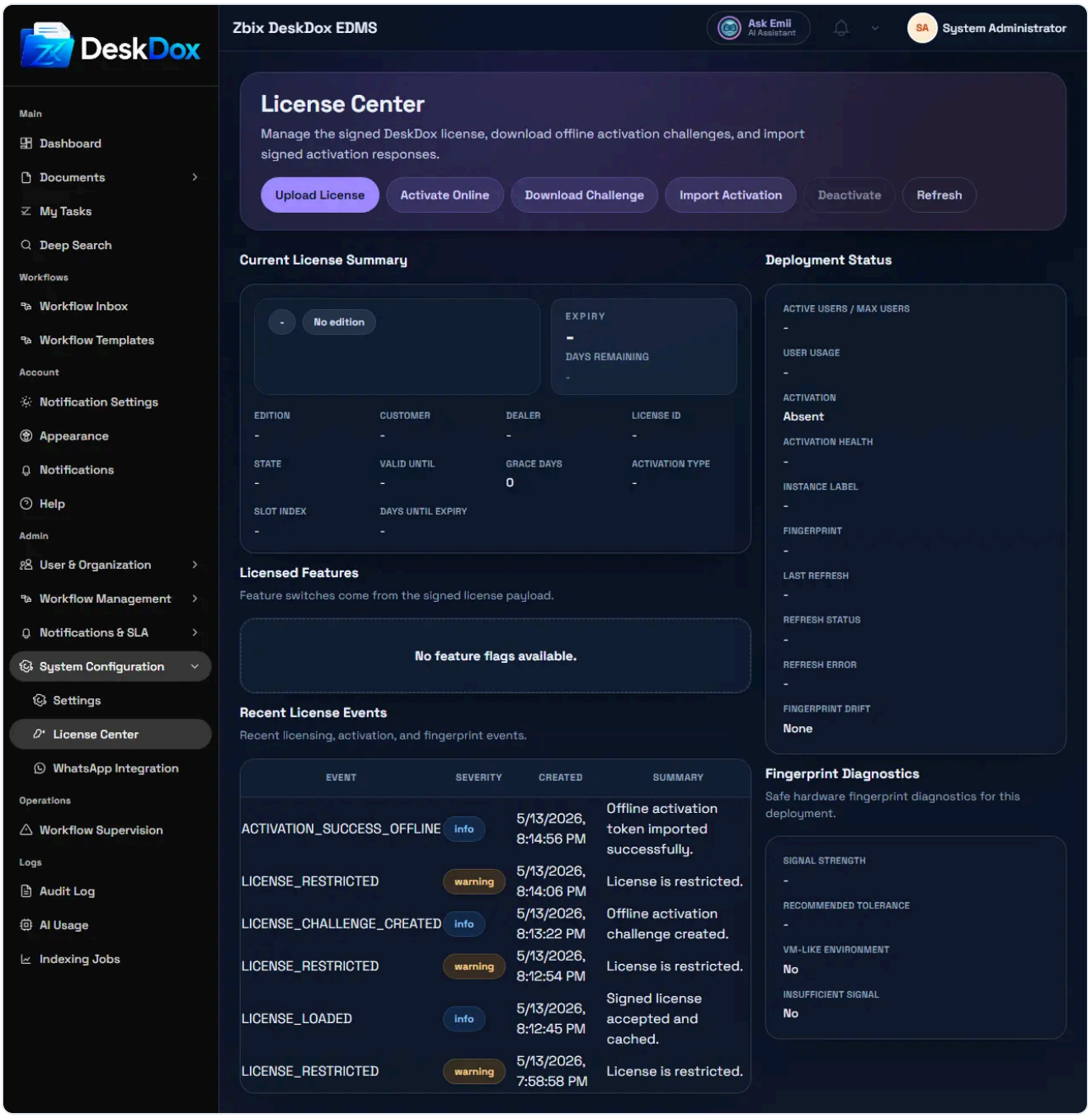
No banner on your dashboard

If there is no license banner on your Dashboard, the current UI state may not require one, your account may not see license notices, or the notice may appear only in administration screens. Do not assume the banner is always visible.

Administration and Operations · 1 min read · Reviewed 2026-05-14

License Status and Activation

Open `/app/admin/license` to review the License Center.



DeskDox licensing may be issued in different editions, such as Standard or Enterprise, depending on the customer agreement. The license screen shows the active edition and validity for the current installation. Feature availability may vary by edition and enabled modules.

The license screen displays the current license status, edition or tier, validity period, activation state, user limits when visible, and activation details available for your installation. Always read the current deployment values from the License Center.

DeskDox includes actions for `Upload License`, `Activate Online` or `Refresh Online Token`, `Download Challenge`, `Import Activation`, `Deactivate` when online activation is present, and `Refresh`. Offline activation means the deployment uses an offline challenge/response workflow instead of

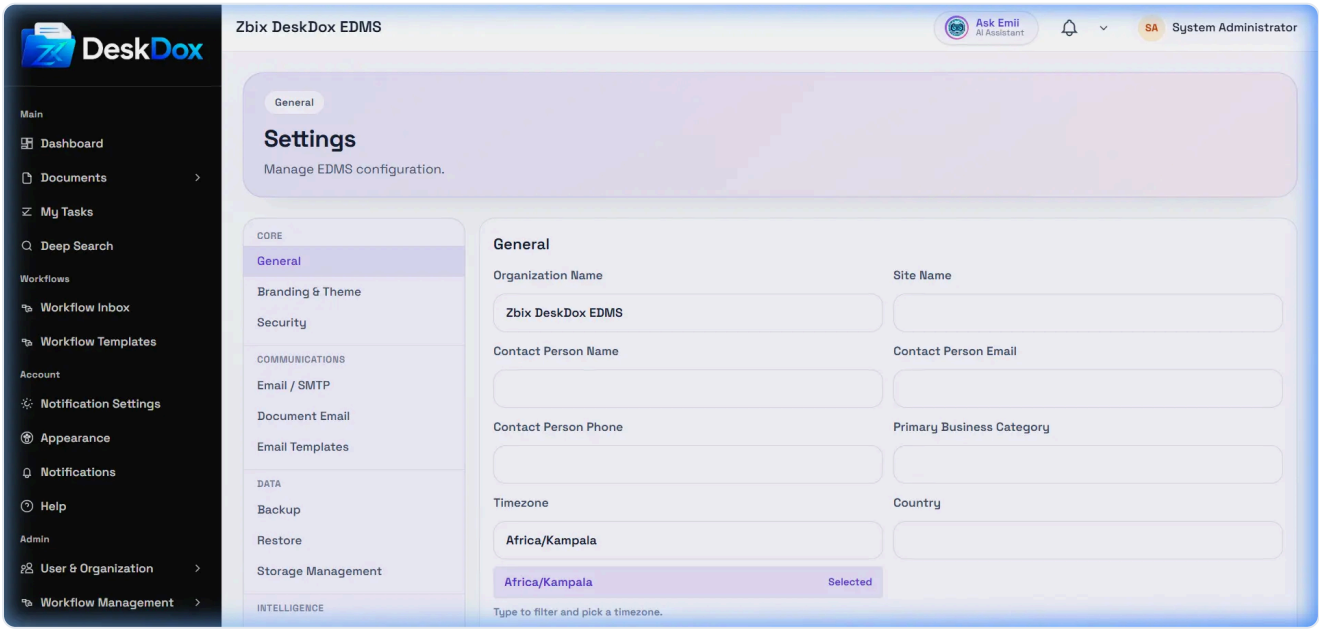
relying only on live online activation. Online and offline actions can fail if files, activation responses, fingerprints, or activation service responses are invalid.

If a feature is locked or disabled, check licensed features, overall license state, expiry or grace status, user limit status, and activation health.

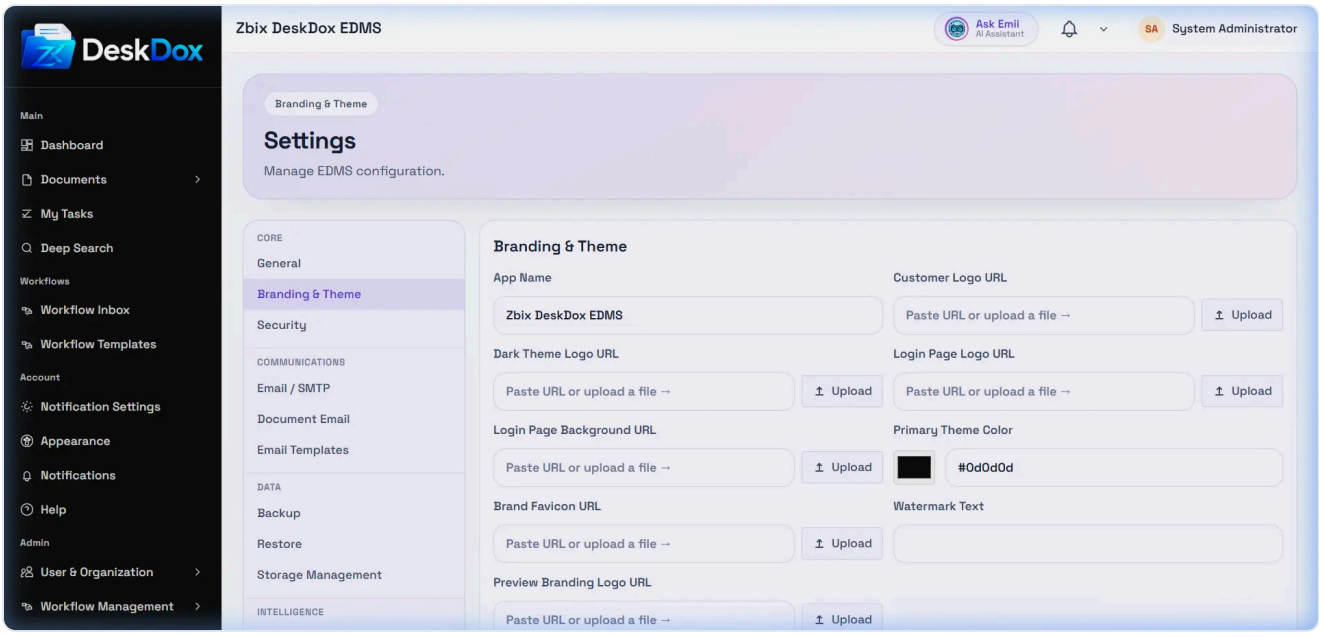
Administration and Operations · 1 min read · Reviewed 2026-05-14

Organization and Branding Settings

Use General settings at `/app/admin/system/settings/general` for organization identity fields. DeskDox includes fields for Organization Name, Site Name, Contact Person Name, Contact Person Email, Contact Person Phone, Primary Business Category, Timezone, Country, Support Email, and Support Phone. Use `Save Changes` to store updates.



Use Branding & Theme at `/app/admin/system/settings/branding` for visible product branding. DeskDox includes App Name, logo URL fields, uploaded branding assets, Primary Theme Color, Watermark Text, Preview Logo, and related login/logo image fields. Uploading an image stores an internal URL, and `Save Changes` applies the selected branding values.



Use the available organization and branding fields shown on this screen. If emails or document links use the wrong URL, check deployment environment configuration with your operations team rather than assuming it can be fixed from this screen.

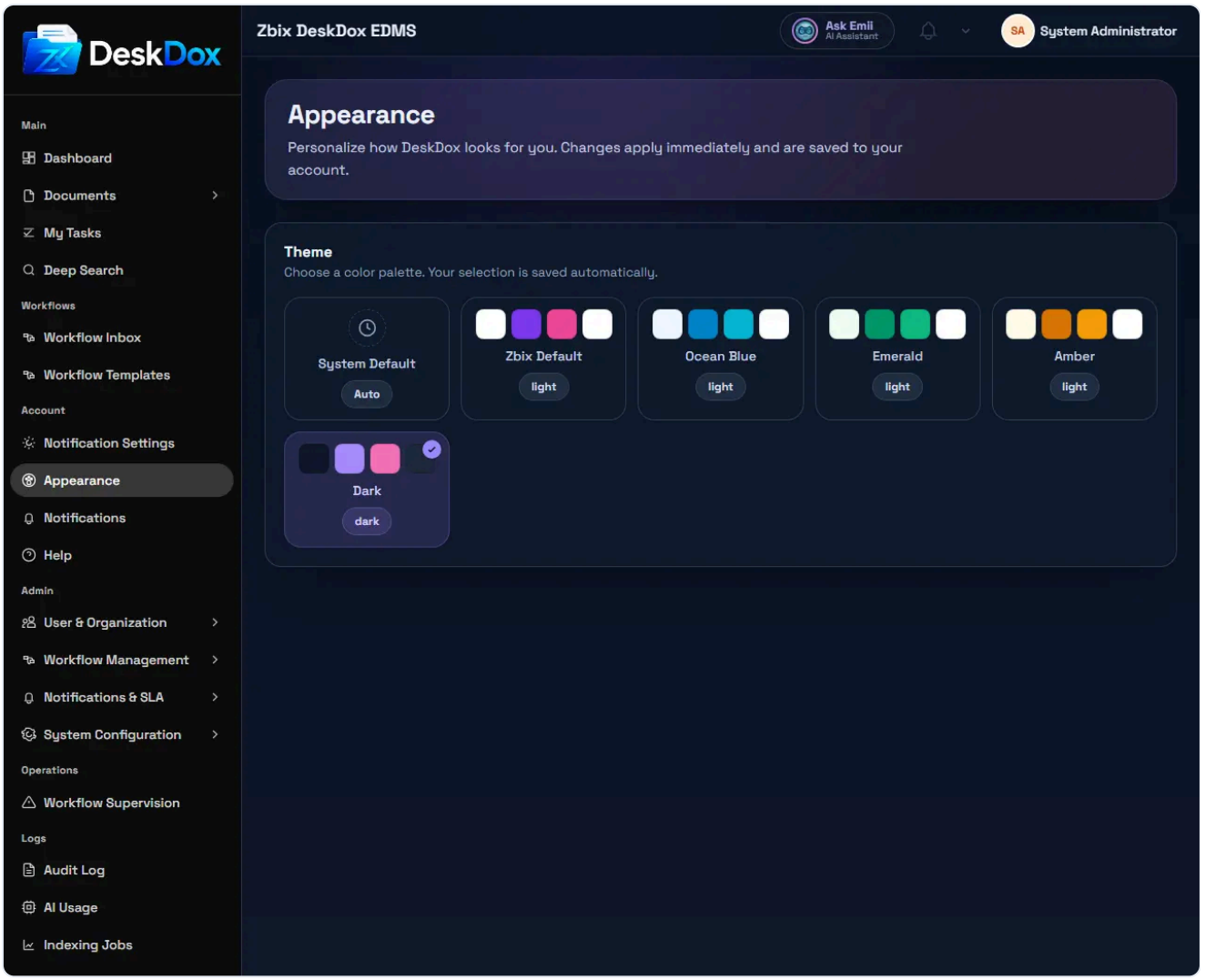
Access requires an administrator role. If General or Branding is hidden or blocked, verify the user role before changing deployment configuration.

Administration and Operations · 1 min read · Reviewed 2026-05-14

Appearance and Theme

What this helps you do

Change the DeskDox visual theme when appearance controls are available to your account.



Open appearance settings

Open the profile menu from the topbar, then choose `Appearance` when visible. The appearance page shows `Theme` controls.

Theme options

Appearance controls can include `Color`, `Minimal`, `System Default`, `Zbix Default`, `Ocean Blue`, `Emerald`, `Amber`, and `Dark`. Theme selections apply immediately.

Use `Dark` for dark mode. Use a light option such as `Minimal`, `Color`, `System Default`, or another visible light theme to return to light mode, depending on your configuration.

If the theme does not update

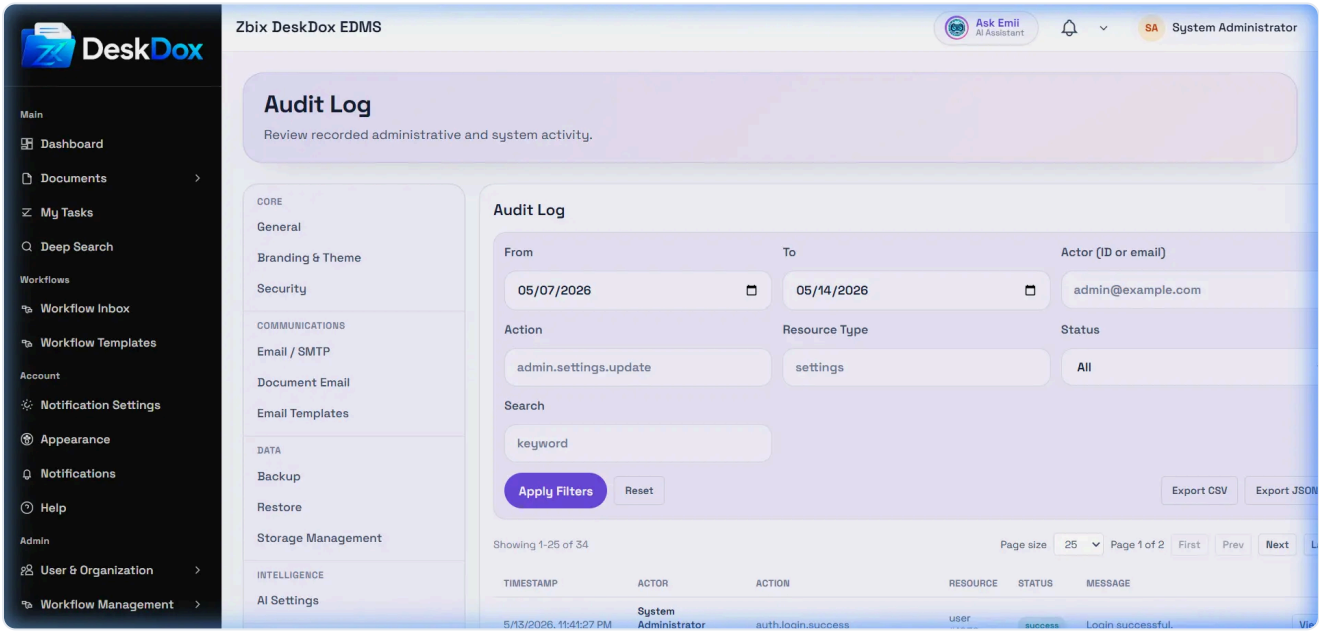
Refresh the browser tab, confirm the selected theme is still active, and clear browser cache if the old styling remains. If appearance settings are missing, ask an administrator whether theme controls are

enabled for your account. Per-user theme persistence should be treated as configuration-dependent unless your deployment confirms it.

Administration and Operations · 1 min read · Reviewed 2026-05-14

Audit Logs

Open `/app/admin/audit-logs` to review administrative and system audit events when your role allows it.



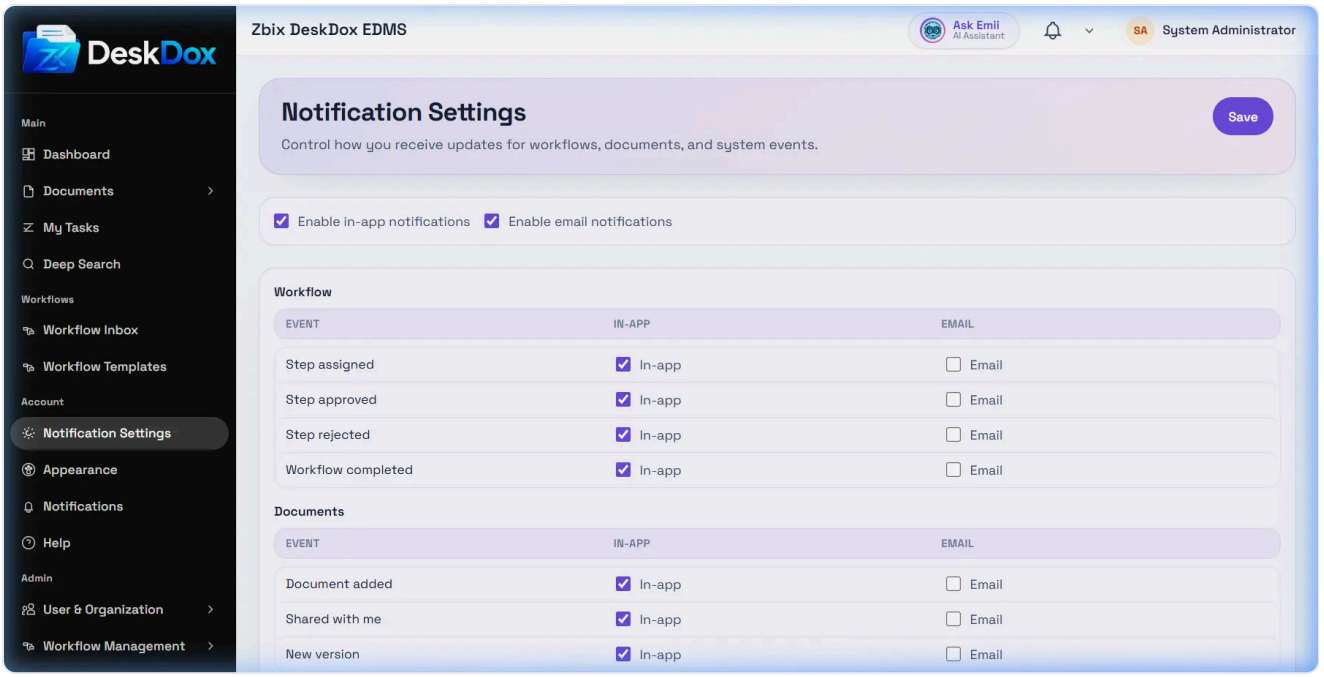
DeskDox includes filters for From, To, Actor, Action, Resource Type, Status, and Search. It also confirms `Apply`, `Reset`, `Export CSV`, `Export JSON`, pagination controls, and a `View` action that opens Audit Log Detail with Timestamp, Actor, Action, Status, Message, Before, After, and Metadata when available.

Audit logs can help answer who changed settings or what admin activity occurred, but do not claim every system action is audited unless the source confirms the specific event. Empty results can mean no matching events exist, filters are too narrow, retention removed older events, or the account lacks access.

Administration and Operations · 1 min read · Reviewed 2026-05-14

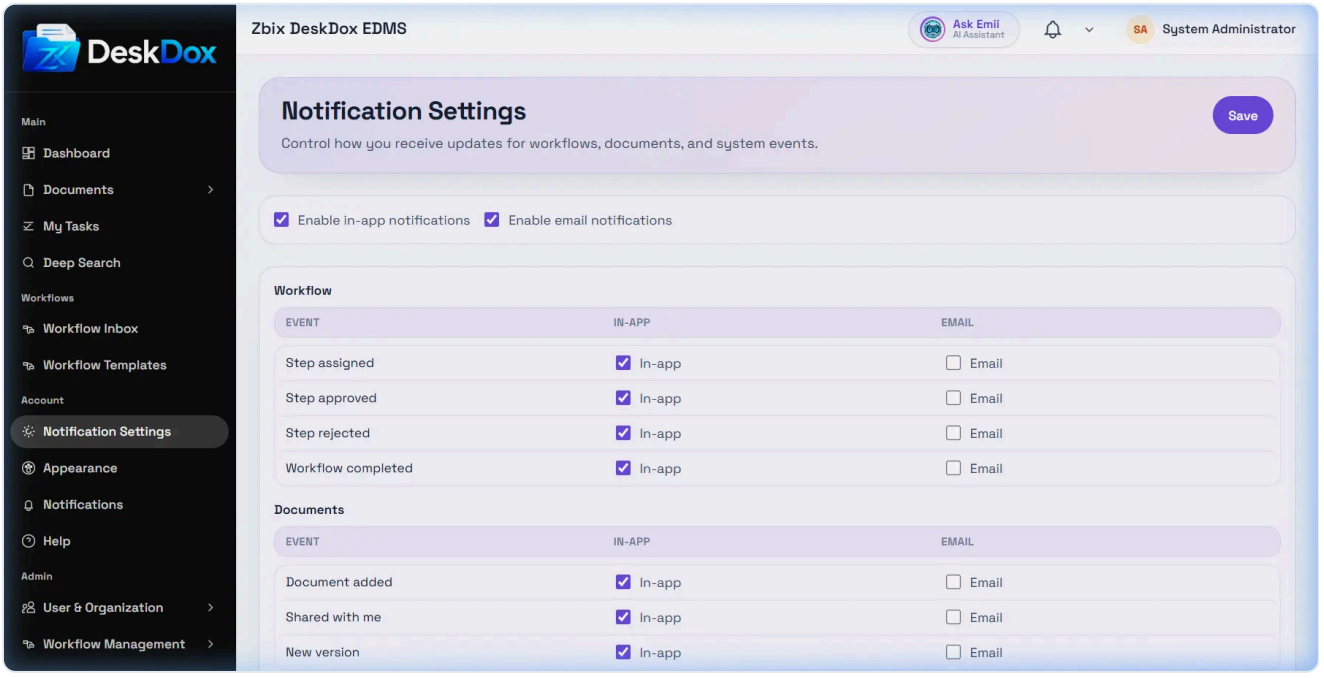
Email and Mobile Notification Delivery

Notification preferences can include email and, depending on the build or deployment, mobile notification options. Preferences control what you want to receive; they do not by themselves prove that delivery services are configured.



Email delivery

The current settings page source confirms `Enable email notifications` and per-event `Email` checkboxes. Actual email delivery depends on a valid user email address, email templates, SMTP or email service configuration, queue processing, and notification rules.



Mobile delivery

The browser capture showed a Mobile preference option, but current source reviewed for this module does not confirm working mobile push delivery. Do not assume push delivery works unless your deployment has

mobile notification implementation and configuration.

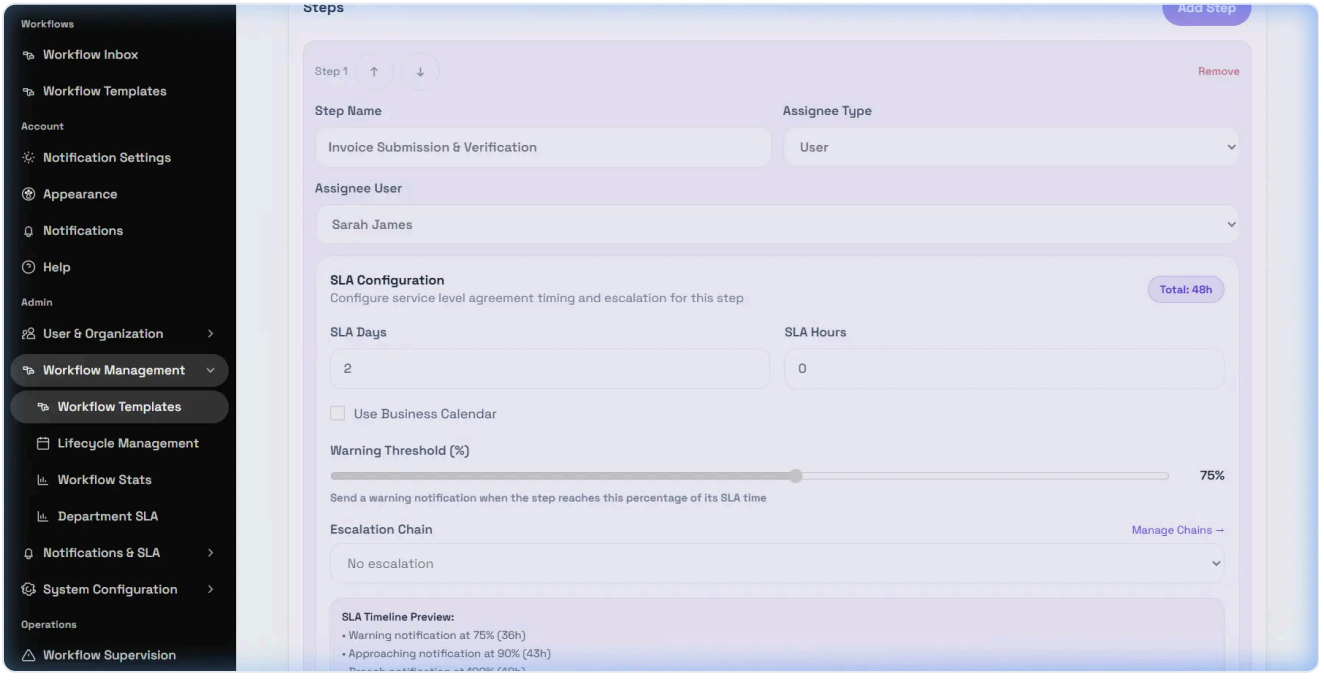
Troubleshooting

For missing email or mobile notifications, check the user's preferences, event eligibility, recipient assignment, channel availability, and service configuration. Admins should verify delivery logs or queues where available rather than assuming the notification was sent.

Administration and Operations · 1 min read · Reviewed 2026-05-14

Escalation Rules

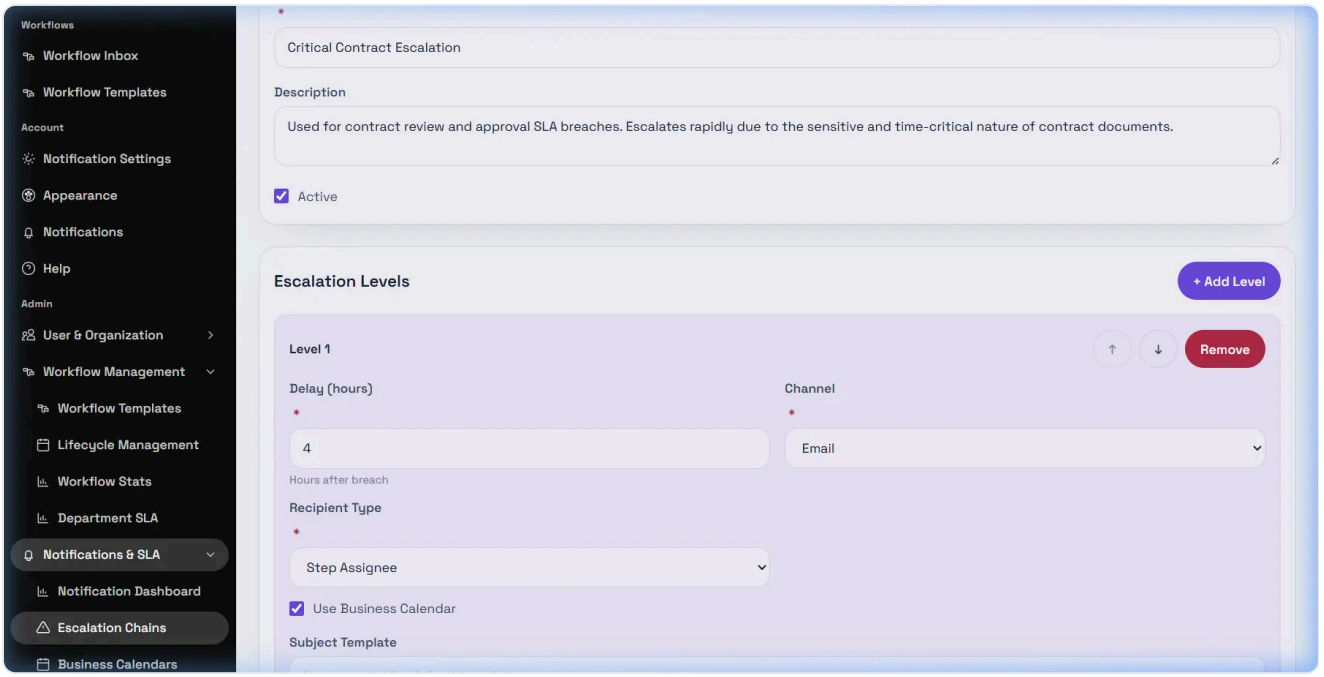
Escalation rules are the individual levels inside an escalation chain. Each level defines when to escalate, which channel to use, and who should receive the escalation.



Level fields

DeskDox includes the escalation editor fields `Delay (hours)`, `Channel`, `Recipient Type`, `Recipient Value`, `Use Business Calendar`, `Subject Template`, and `Body Template`. Recipient types include `Email Address`, `Role`, `Department Head`, `Step Assignee`, `Manager of Assignee`, and `Workflow Creator`.

For the first level, delay is measured in hours after breach. For later levels, delay is measured after the previous level. The editor supports `Email`, `In-App`, and `WhatsApp` channel labels, but actual delivery still depends on configured services and notification processing.



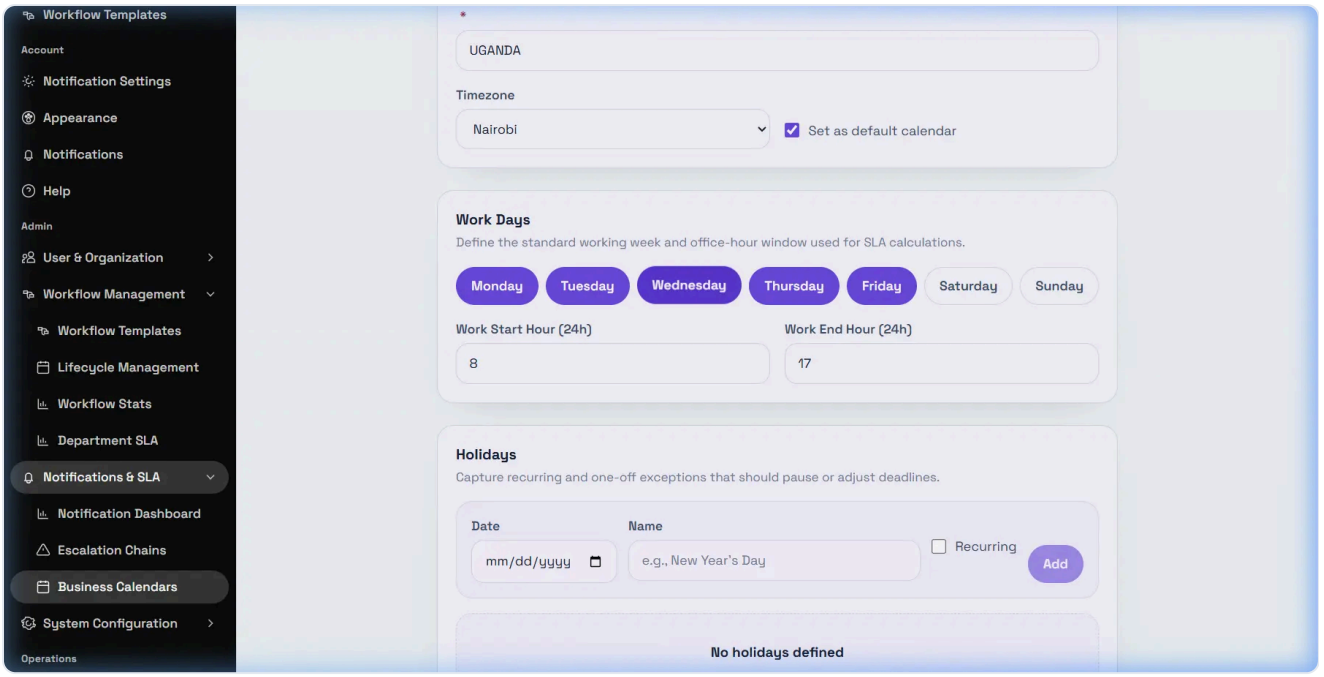
Troubleshooting

If an escalation does not happen, verify that the workflow step has an SLA, the selected escalation chain is active, the chain has at least one level, recipient fields are valid, the task actually breached, the business calendar is correct, and the configured channel can deliver in your environment.

Administration and Operations · 1 min read · Reviewed 2026-05-14

Holidays and Non-Working Days

Holidays and non-working days are calendar exceptions that can pause or adjust SLA due-date calculations when a workflow step uses a business calendar.



How to add a holiday

Open the business calendar, go to `Holidays`, select a `Date`, add a `Name` if useful, choose `Recurring` for holidays that repeat yearly, then select `Add`. Save the calendar after making changes.

Weekends or other non-working days are controlled by the Work Days selection in the same calendar. If Saturday or Sunday is selected as a work day, DeskDox may count that day for business-calendar SLA timing.

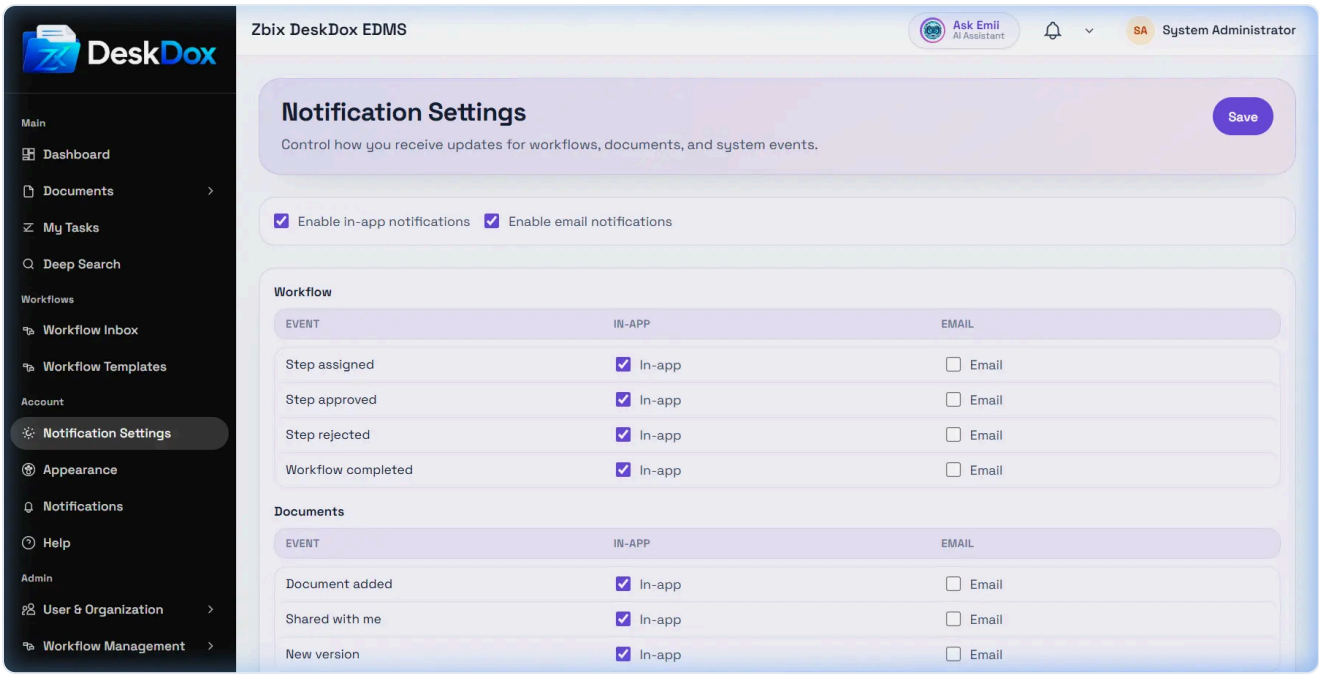
Troubleshooting wrong due dates

If a weekend or holiday was counted, check that the workflow step has `Use Business Calendar` enabled, the correct calendar is selected, the calendar's Work Days are correct, the holiday date exists, and the task started after the relevant template/calendar setup was applied.

`Administration and Operations · 1 min read · Reviewed 2026-05-14`

Notification Preferences

Use `/app/settings/notifications` to control how DeskDox sends notification updates for the event types visible to your account.



Available preferences

The current available settings include global `Enable in-app notifications` and `Enable email notifications` controls, plus per-event `In-app` and `Email` checkboxes. Visible event groups include Workflow, Documents, and System. System password reset events are treated as critical, and the screen warns if those events have no channel enabled.

The browser capture also showed a Mobile preference option. Treat mobile as a preference option only when it is visible in your environment. Actual mobile or push delivery is not available in this module and depends on deployment configuration.

Saving changes

Select the channels you want and use `Save`. The page can show `Notification settings updated.` after a successful save, `Unable to update settings. Please try again.` after a failed save, or `Unable to load notification settings.` if the settings request fails.

Delivery caveats

In-app notifications appear in DeskDox when events create notifications for you. Email delivery additionally depends on email address, SMTP or email service configuration, queue processing, and template/rule setup. Mobile delivery depends on whether your deployment implements and configures mobile push delivery.

CHAPTER 11

Deployment Manual

Infrastructure baseline, architecture, installation, security, backup, maintenance, and go-live readiness guidance.

Deployment Manual · 6 min read · Reviewed 2026-05-15

Infrastructure Baseline

DeskDox EDMS is deployed as a controlled enterprise document management platform. This Deployment Manual defines the infrastructure baseline used to plan, install, secure, validate, and operate DeskDox in customer-managed environments.

Purpose

This manual is written for infrastructure planning, deployment readiness review, architecture workshops, production preparation, and operational handover. It explains the expected platform, service topology, network exposure model, security baseline, storage and backup scope, and operational responsibilities for DeskDox deployments.

The manual is public Help Center documentation. It is not a commercial or formal completion document. Deployment teams can use it to prepare implementation notes and handover records, but final operational decisions remain part of the customer's normal governance process.

Primary Audience

Audience	Expected use of this guide
Enterprise IT and infrastructure teams	Confirm servers, storage, network, DNS, TLS, firewall, backup, and monitoring readiness.
Solution architects	Review logical architecture, deployment models, service boundaries, and sizing assumptions.
Deployment engineers	Plan installation, validate Compose/runtime configuration, and prepare deployment handover notes.
Security and risk teams	Review exposure boundaries, TLS, secrets, privileged access, backup handling, auditability, and hardening.
Operations and support teams	Establish monitoring, patching, backup review, escalation, and maintenance ownership.

Scope

This manual covers customer-managed deployments using repository-supported container deployment patterns:

- Linux Docker Compose production deployment using `docker-compose.prod.yml`.
- Windows offline installer deployment using `deploy-kit/compose/docker-compose.production.yml` and the deploy-kit PowerShell scripts.
- VPS or private-cloud single-server deployment where the customer controls the host, DNS, firewall, and backup destination.
- Conditional two-tier or three-tier readiness planning where components may be separated after solution review.

The manual does not present Kubernetes, managed database, multi-region, or active-active high availability as packaged deployment options. Those patterns require separate design validation and are treated as future-state or customer-specific architecture.

In Scope and Out of Scope

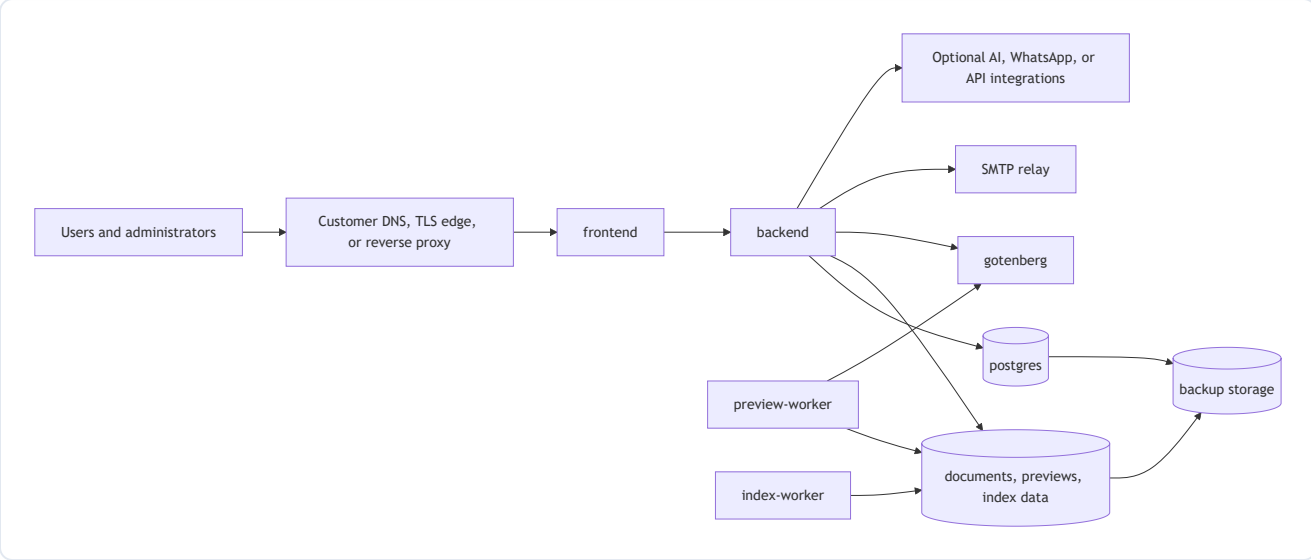
Area	Guidance
In scope	Infrastructure planning, deployment readiness, service topology, ports, storage, backup, restore validation, security hardening, and operational baseline.
Out of scope	Commercial terms, formal completion records, custom HA design, and customer-specific network diagrams.
Technical source of truth	Current repository Compose files, configuration templates, application settings, NGINX configuration, and deploy-kit scripts.
Deprecated assumptions	Redis and Celery are not part of the current production Compose service baseline and are not documented as required deployment services.

Deployment Assumptions

The current production baseline assumes:

- DeskDox runs as a Docker Compose application.
- PostgreSQL 16 is the primary database engine for production compose deployments.
- Uploaded documents, previews, search/index artifacts, licensing files, and backups are persisted on mounted filesystem paths.
- Gotenberg 8 provides document conversion for preview generation.
- Dedicated `preview-worker` and `index-worker` containers are present in the production compose paths.
- The frontend container serves the React application through NGINX and proxies `/api/` traffic to the backend.
- The database, converter, workers, and backend API remain internal unless a deployment-specific design explicitly requires otherwise.
- Linux is the preferred production baseline. Windows deployment is supported through the offline deploy-kit model with explicit operational boundaries.

Production Baseline at a Glance



Deployment Planning Areas

DeskDox deployment planning should cover the following areas before production use:

Area	Baseline guidance	Planning note
Controlled exposure	Users should reach only the approved web endpoint.	Internal ports must not be exposed publicly.
Persistent storage	Database, uploads, previews, index data, backups, and licensing state must survive container replacement.	Storage layout affects backup and restore design.
Workload-based sizing	CPU, RAM, database, and storage sizing must reflect real workload.	Concurrency, document volume, OCR, previews, retention, and RPO/RTO matter more than user count alone.
Recoverability	Backups must include the database and required file stores.	Production deployments should include restore validation before go-live.
Least privilege	Host, Docker, database, application admin, and service access should be restricted.	Shared admin access should be governed by the customer's privileged-access process.
Operational baseline	Monitoring, backup review, patching, escalation, and ownership should be documented.	Record open items in deployment handover notes.

Responsibility Model

Area	Customer responsibility	Implementation team responsibility
Host provisioning	Provide server, storage, OS baseline, DNS, firewall, and administrative access.	Validate that the host matches the selected deployment model and readiness checklist.
Network and TLS	Provide FQDN, certificate, reverse proxy or TLS termination approach, and firewall approvals.	Confirm DeskDox endpoint configuration and application URL alignment.
Secrets and credentials	Provide or approve secure handling of database, JWT, SMTP, WhatsApp, OpenAI/Emii, and backup keys.	Configure secrets according to the deployment package and avoid recording sensitive values in handover notes.
Backup location	Provide backup target, retention policy, off-host/off-site copy process, and restore owner.	Configure DeskDox backup paths and support initial backup or restore validation where in scope.
User and role readiness	Nominate administrators and define the initial access model.	Support initial admin setup and validation of RBAC-controlled access.
Monitoring and operations	Operate host monitoring, storage alerts, backup review, patching windows, and escalation.	Provide deployment handover notes and known support boundaries.

Support Boundary Statement

DeskDox support covers the application containers, DeskDox configuration, documented deployment scripts, application-level health validation, and product behavior. Customer or infrastructure-provider responsibilities include the host operating system, virtualization platform, Docker runtime installation, DNS, TLS certificate lifecycle, reverse proxy, firewall, storage subsystem, backup media, endpoint security tooling, external SMTP, WhatsApp, OpenAI/Azure/Ollama services, and organization-specific monitoring platforms.

Where an issue crosses these boundaries, joint troubleshooting may be required. Deployment handover notes should record the named customer owner for infrastructure, network, security, database/backup, and application administration.

Final Sizing Disclaimer

Sizing values in this manual are planning baselines. Final production sizing must be confirmed against the customer workload, document retention profile, preview/OCR percentage, workflow volume, search behavior, backup retention, and target RPO/RTO. Large document archives, high OCR usage, strict audit

retention, or short restore windows may require larger database, CPU, memory, and storage allocations than a user-count estimate alone suggests.

Deployment Manual · 6 min read · Reviewed 2026-05-15

Solution Architecture

DeskDox EDMS is delivered as a containerized application stack with clearly separated presentation, API, data, conversion, preview, indexing, and integration responsibilities.

Verified Production Services

The current production compose files define the following runtime services:

Service	Role	Repository evidence
`frontend`	NGINX-served React application and same-origin `/api/` reverse proxy to backend.	`docker-compose.prod.yml`, `deploy-kit/compose/docker-compose.production.yml`, `frontend/nginx.conf`
`backend`	FastAPI application, REST API, authentication, RBAC, workflows, document operations, settings, backup APIs, and startup orchestration.	Production Compose files and backend service entry point
`postgres`	PostgreSQL database for application state, metadata, users, roles, workflows, audit records, jobs, and settings.	Production Compose files
`gotenberg`	Document conversion service used for Office/PDF preview workflows.	Production Compose files
`preview-worker`	Dedicated worker process for preview generation jobs.	Production Compose files and preview worker entry point
`index-worker`	Dedicated worker process for OCR, search indexing, and retrieval/index artifacts.	Production Compose files and index worker entry point

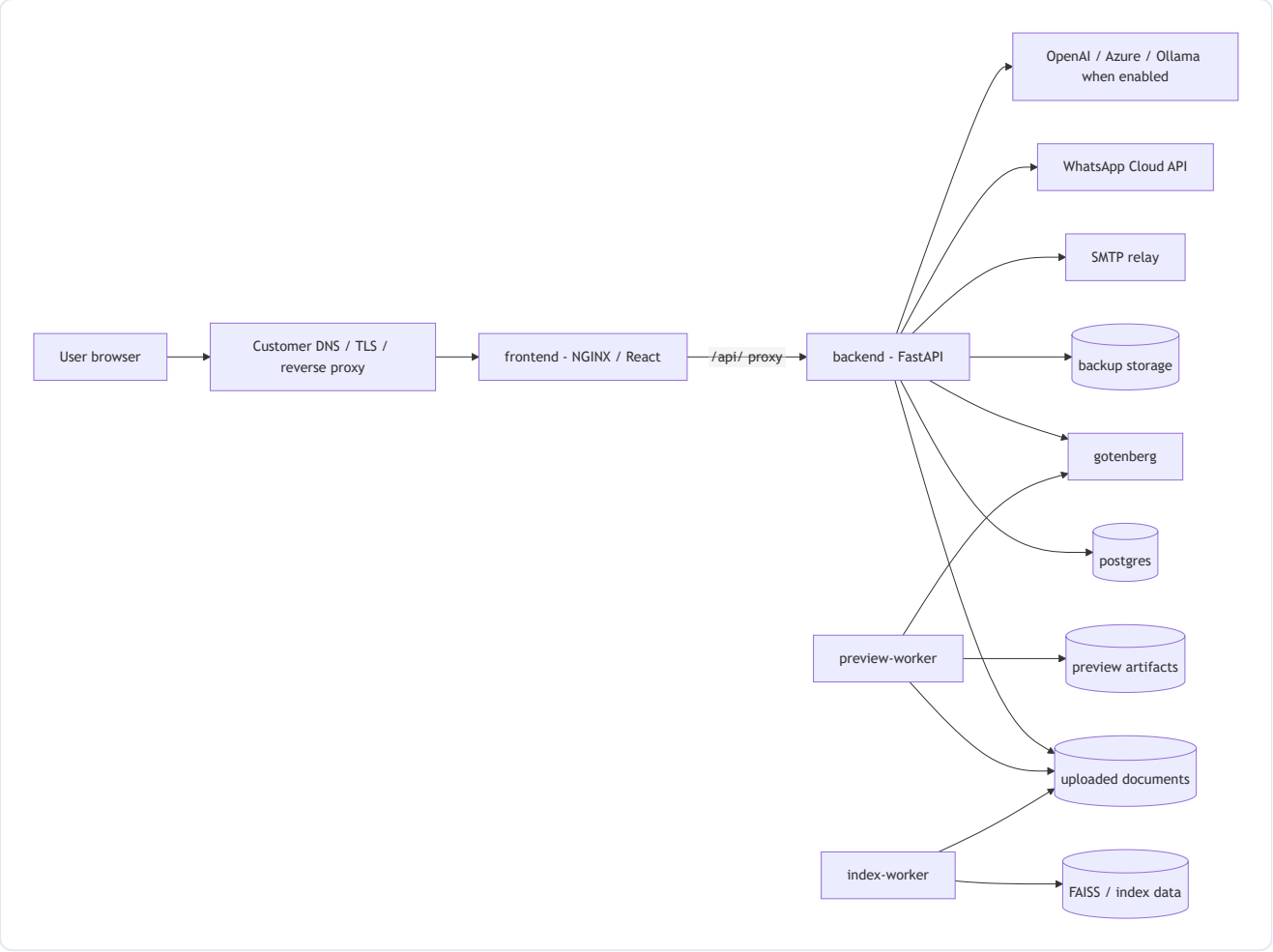
Redis and Celery are not deployed as services in the current production compose baseline. The application code contains optional `REDIS_URL` support for limited AI rate-limiting and WhatsApp state paths, but this is

not a required production service in the current packaged deployment. Celery is not part of the active production runtime topology.

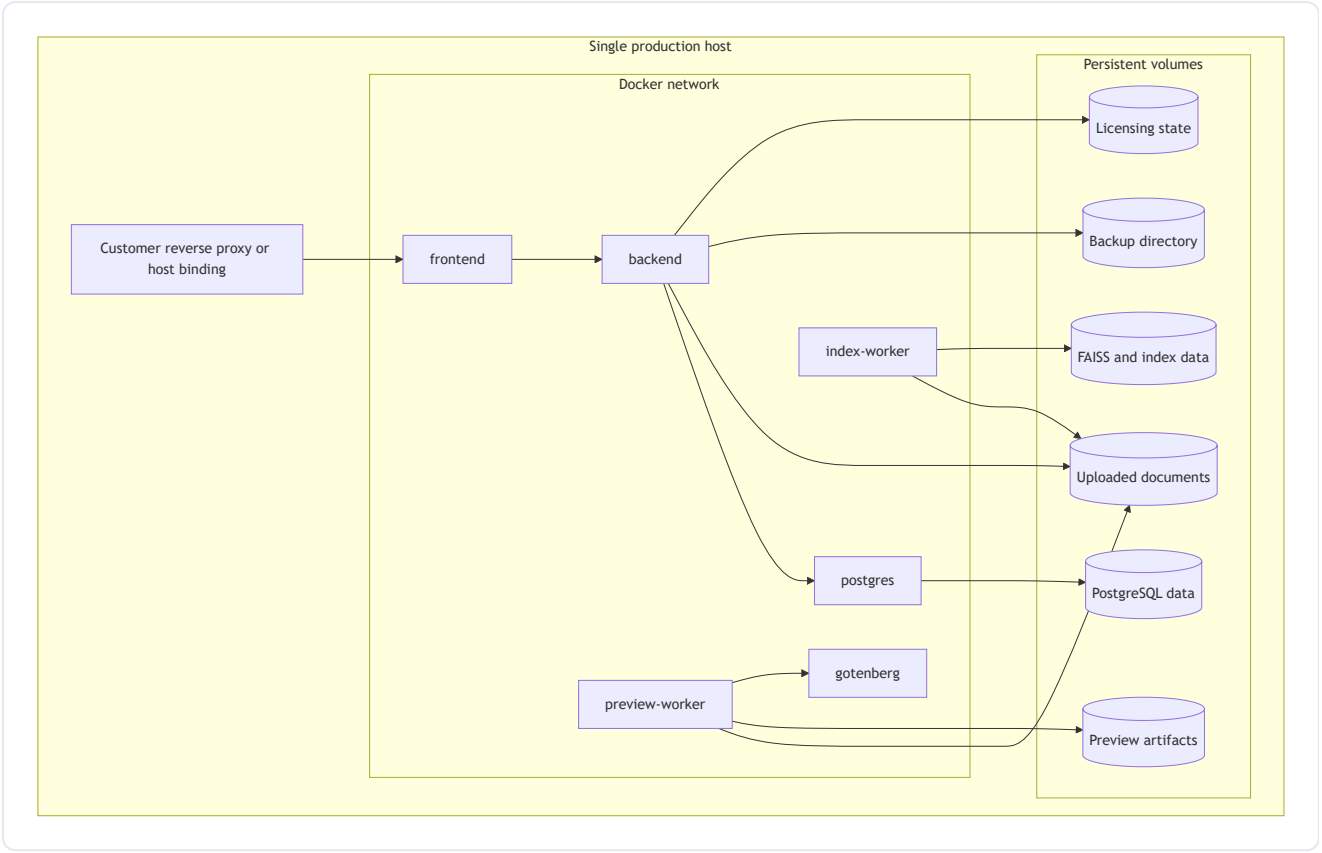
Logical Service Groups

Service group	DeskDox implementation	Planning note
Presentation layer	`frontend` container running NGINX and static React assets.	Public user access should terminate at HTTPS before reaching this layer.
Application/API layer	`backend` container running Uvicorn/FastAPI on port `8000` inside the stack.	Direct public exposure should be avoided unless a reviewed deployment model requires it.
PostgreSQL data layer	`postgres` service on internal port `5432`.	Must remain internal-only.
Document storage layer	Mounted filesystem paths for `/app/files` and related data directories.	Requires durable storage and backup coverage.
Preview/conversion layer	`gotenberg` service and `preview-worker`.	Converter must remain internal-only.
OCR/indexing/search layer	`index-worker`, Tesseract configuration, FAISS/index directories.	Sizing depends heavily on scanned documents and OCR percentage.
Integration layer	SMTP, WhatsApp Cloud API, OpenAI/Azure/Ollama, or local LLM endpoints when enabled.	Outbound access and secrets are customer-controlled.

Logical Architecture Diagram



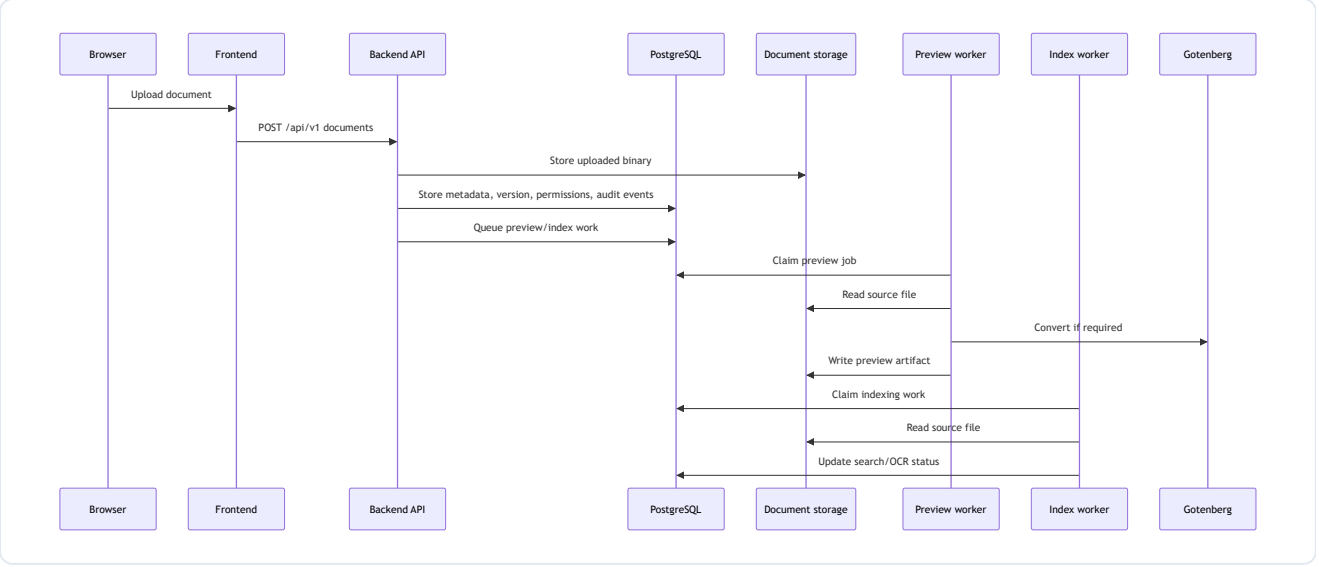
Single-Server Docker Compose Topology



Browser-to-Application Flow

1. The user accesses the approved public DeskDox URL.
2. DNS resolves the FQDN to the customer-controlled host or reverse proxy.
3. TLS is terminated at the customer-approved edge, reverse proxy, or equivalent network layer.
4. The request reaches the `frontend` service.
5. Static application assets are served by NGINX.
6. API requests under `/api/` are proxied by NGINX to the `backend` service on internal port `8000`.
7. The backend validates authentication, authorization, request limits, and business rules before reading or writing database and file storage.

Document Upload Flow



Preview Generation Flow

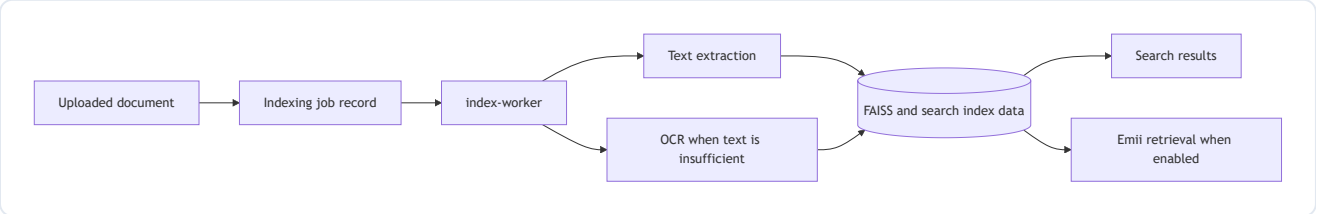
Preview generation is handled by the `preview-worker`. The worker reads source documents from mounted file storage, calls Gotenberg for supported conversion workflows, and writes preview artifacts to the preview data path. In the deploy-kit compose file, `CONVERTER_URL` is set to `http://gotenberg:3000`; in root production compose, Gotenberg is also the configured converter endpoint.

Preview workload is CPU and I/O sensitive. Office-document conversion can be materially heavier than simple PDF preview handling.

OCR, Indexing, and Search Flow

The `index-worker` handles indexing work. OCR is controlled by environment settings such as `OCR_ENABLED`, `TESSERACT_CMD`, `TESSERACT_LANG`, `OCR_MAX_PAGES`, and `OCR_MIN_TEXT_THRESHOLD`. Index and retrieval artifacts are stored under the configured FAISS/data directory, mounted in production as `/app/data/faiss`.

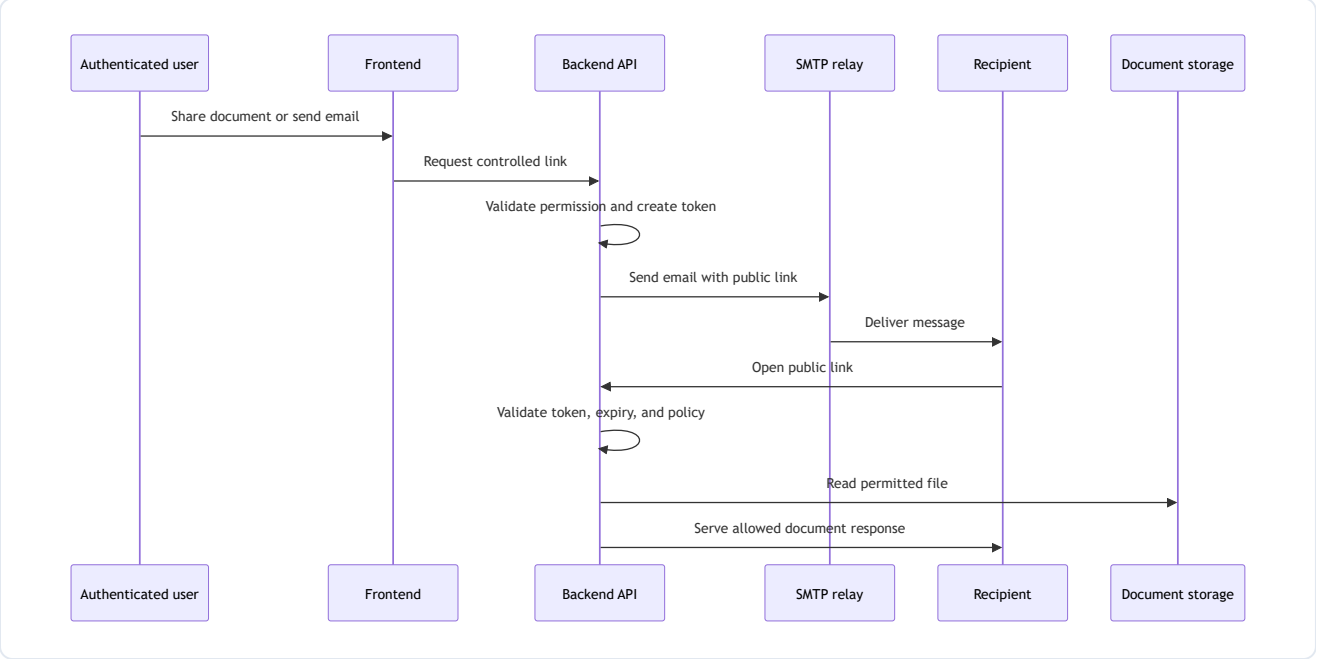
Sizing must account for the percentage of scanned documents, average page count, language coverage, OCR page limits, and expected search freshness.



Public Link and Email Flow

Document sharing, public document links, file requests, password reset, and notification emails depend on correct `FRONTEND_URL` or `PUBLIC_URL` configuration and SMTP readiness. The application embeds the public URL in outbound links, so production deployments must not use local-only URLs when `DEBUG=false`.

Outbound SMTP uses customer-provided settings. Email delivery quality, relay rate limits, mailbox reputation, and external spam controls remain customer or SMTP-provider responsibilities.



Backup Flow

Production backup coverage must include:

- PostgreSQL database dump or equivalent database backup.
- Uploaded document binaries.
- Preview artifacts where required for operational continuity.
- FAISS/search/index data where required to avoid reprocessing.
- Licensing data.
- Backup metadata and retention evidence.

The Windows deploy-kit `backup.ps1` script creates a database dump and copies `uploads`, `faiss`, and `previews` from `DATA_ROOT`. Application backup services are also configured through `BACKUP_ROOT` and `BACKUP_ENCRYPTION_KEY`. Restore handling should be validated against the selected deployment model before go-live.

Deployment Manual · 5 min read · Reviewed 2026-05-15

Installation Readiness

Installation readiness confirms that the customer environment, deployment package, security approvals, and operational owners are prepared before DeskDox is installed.

Readiness Principle

DeskDox installation should not begin until the infrastructure owner, network owner, security owner, application administrator, and deployment engineer have confirmed the target deployment model and the required access window. This reduces installation delay caused by missing DNS, firewall, storage, certificate, SMTP, license, or backup information.

Pre-Install Checklist

Area	Required confirmation
Deployment model	Linux Docker Compose, Windows offline installer, VPS/private cloud, or reviewed customer-specific model selected.
Host access	Administrative access available for the deployment engineer during the planned window.
Docker runtime	Docker Engine/Compose or Windows deploy-kit prerequisites available and tested.
Storage	Durable storage provisioned for database, uploads, previews, index data, backups, logs, and temporary processing.
DNS	FQDN selected and DNS administration available.
TLS	Certificate approach confirmed; certificate and private key handling defined where customer-managed.
Firewall	Inbound and outbound firewall decisions completed.
Secrets	Production secrets generated or secure generation procedure defined.
SMTP	SMTP relay details and test recipient available if email features are in scope.
Integrations	WhatsApp, OpenAI/Emii, Azure/OpenAI, Ollama, or other integration keys available if enabled.
Backup	Backup path, retention, off-host copy, restore owner, and restore validation approach defined.
License	DeskDox license key or activation process available.
Admin owner	Named customer administrator available for validation and handover.

Customer Information Required

Information	Required for	Notes
FQDN	Public endpoint, email links, public links, callbacks	Must match the production URL used in configuration.
TLS certificate	HTTPS access	Certificate chain and renewal process are customer responsibilities unless separately managed.
SMTP host, port, sender, username, password or token	Notifications, password reset, document email	Credentials must be handled as secrets.
Backup location	Backup and restore readiness	Prefer storage outside the primary application data path.
Admin contact	Initial validation and escalation	Must be available during installation and post-install validation.
License key or activation details	Product activation	Online activation settings are environment-specific.
Integration keys	WhatsApp, OpenAI/Emii, Azure, or external APIs	Only required if the feature is enabled.
DNS access	Public endpoint setup	Required for go-live unless preconfigured.
Firewall decisions	Inbound and outbound communication	Must include public endpoint, SMTP, WhatsApp/API, and AI endpoints where applicable.

Deployment Package Readiness

For Linux compose deployments, confirm:

- `docker-compose.prod.yml` is available.
- `.env.prod` has been created from `.env.prod.template`.
- Image tag policy is agreed through `IMAGE_TAG`.
- Persistent host paths under `/srv/edms/volumes/.` or approved equivalents are provisioned.
- Reverse proxy/TLS approach is defined if HTTPS is terminated outside the DeskDox frontend container.

For Windows offline installer deployments, confirm:

- The deploy-kit package is complete.
- `deploy-kit/config/.env` has been reviewed before first install.
- Offline image archives are available if the environment cannot pull from a registry.
- PowerShell execution policy and administrator access allow the deploy-kit scripts to run.
- The Windows service model and Docker runtime support boundary are accepted by the customer.

Image and Tag Readiness

Production deployments should use a deliberate image tag rather than an uncontrolled moving target. The deploy-kit template currently defines `IMAGE_TAG=v1.0.56`; the root production template uses `IMAGE_TAG=latest` as a placeholder to be pinned for the target release. The implementation team should confirm the release tag selected for the customer deployment and record it in the handover notes.

Offline Installer Readiness

Offline Windows deployment requires the deployment package to include all container images and scripts needed by the target host. The deployment engineer should validate that image archives load successfully before the installation window where possible. Internet access assumptions must be documented because offline environments may block activation, SMTP, WhatsApp, OpenAI/Emii, and update flows unless explicit allow-lists are approved.

Post-Install Validation Checklist

Validation area	Expected result
Login	Production admin can log in through the approved URL.
User access	At least one non-admin user can authenticate and access only permitted areas.
Upload	A test document uploads successfully and appears in the correct folder.
Preview	PDF and Office preview behavior is validated for representative file types.
OCR/search	Search returns expected results after index processing; scanned-document OCR is tested if in scope.
Workflow	A representative workflow can be started, actioned, and completed.
Email	SMTP test and at least one real notification or document email are delivered if email is in scope.
Backup	Initial backup completes and backup artifacts are visible in the configured location.
Restore review	Restore procedure is tested in a non-production environment or a deferred validation plan is recorded in handover notes.
Public URL	Email links, public document links, and frontend URL behavior use the production FQDN.
Audit logs	Login, upload, admin, and document events are visible in audit/history views where applicable.

Readiness Output

The readiness workshop should produce deployment handover notes containing:

- Target deployment model.
- Host, storage, DNS, TLS, and firewall decisions.
- Environment variables requiring customer-supplied values.
- Backup/restore expectations and RPO/RTO.
- Named operational owners.
- Support boundaries.
- Open items marked `To be confirmed` with owner and target date.

Deployment Manual · 6 min read · Reviewed 2026-05-15

Platform Requirements and Infrastructure Sizing

DeskDox sizing must be driven by workload, data growth, and recovery objectives. Named user count alone is not sufficient for production infrastructure planning.

Preferred Production Baseline

Linux is the preferred production baseline for DeskDox EDMS. The root production compose file uses Linux-style persistent paths under `/srv/edms/volumes/.`, loopback-bound internal service ports, and Docker Compose service health checks. This model is the primary baseline for enterprise production deployments, VPS deployments, private-cloud VMs, and customer-managed Linux hosts.

Windows deployment is available through the deploy-kit offline installer model and should be treated as a customer-specific or conditional deployment path. It is appropriate where the customer has a Windows operational standard, a controlled offline installation requirement, or a site-specific support agreement.

Runtime Requirements

Area	Requirement
Container runtime	Docker Engine with Docker Compose v2, or an approved equivalent runtime that supports the supplied Compose files.
Database	PostgreSQL 16 in the supplied production Compose baseline.
Frontend runtime	NGINX serving the built React application in the `frontend` container.
Backend runtime	Python/FastAPI application served by Uvicorn in the `backend` container.
Converter	Gotenberg 8 container for conversion and preview workflows.
Persistent paths	Database, uploads, previews, FAISS/index data, backups, and licensing paths must be durable.
Browser	DeskDox is intended for current enterprise-supported versions of Microsoft Edge, Google Chrome, Mozilla Firefox, and Safari. Internet Explorer is not supported.

Linux Considerations

For Linux production hosts:

- Provision persistent storage before installation.
- Restrict host access to approved administrators.
- Confirm Docker service startup after reboot.
- Review SELinux or AppArmor policy interactions with mounted paths and Docker access.
- Restrict file permissions on environment files and backup paths.
- Use a customer-approved reverse proxy or network edge for TLS when HTTPS is not terminated by upstream infrastructure.

SELinux/AppArmor behavior depends on the distribution and customer hardening profile. If enforced policies block Docker volume access, the customer security team must approve the required labeling or profile adjustment.

Windows Considerations

The Windows deploy-kit path uses:

- `deploy-kit/compose/docker-compose.production.yml`.
- `deploy-kit/config/.env` copied to `.env` on first install.
- `DATA_ROOT=C:/ProgramData/DeskDox` by default.
- `HTTP_PORT=8088` by default, with automatic port selection support in installer tooling.
- PowerShell scripts for install, start, stop, restart, health check, backup, restore, upgrade, reconfigure, and uninstall.

Antivirus and endpoint detection tooling should exclude the approved DeskDox data root, Docker storage paths, and temporary processing paths from destructive quarantine behavior. Exclusions must be approved by the customer security team; they should not disable monitoring, but they should prevent document, database, backup, and index files from being locked or modified during runtime operations.

Docker Desktop on Windows is not the preferred enterprise server baseline. Use of Docker Desktop in production must be explicitly accepted by the customer, including licensing, service startup, Windows update, resource allocation, and operational support implications. Where possible, Windows Server deployments should use the customer-approved container runtime model validated during implementation.

Service Account Expectations

DeskDox should be operated by named administrative users or approved service accounts. Service accounts should:

- Have only the host and Docker privileges required for the deployment model.

- Be controlled by the customer identity and privileged-access process.
- Be excluded from personal user offboarding risk.
- Have credential rotation and ownership documented in handover.

Sizing Inputs

Sizing must include the following inputs:

Sizing input	Planning impact
Concurrent users	Drives API, database, frontend, and session workload.
Document ingestion volume	Drives storage growth, indexing, preview jobs, and backup size.
Average file size	Drives upload limits, storage, backup windows, and network throughput.
OCR percentage	Drives CPU, memory, and index-worker workload.
Preview generation workload	Drives Gotenberg and preview-worker capacity.
Workflow volume	Drives database writes, notifications, task queues, and audit logs.
Audit retention	Drives database growth and reporting performance.
Backup retention	Drives backup storage and off-host copy requirements.
RPO/RTO expectations	Drive backup frequency, restore design, and standby infrastructure needs.

Planning Sizing Table

The following values are planning baselines only and must be validated against customer workload.

Profile	Application baseline	Database/storage baseline	Typical use case
Pilot / demo	2-4 vCPU, 4-8 GB RAM	100-200 GB usable, SSD-backed	Demonstrations, limited UAT, low document volume, short retention.
Small production	4 vCPU, 8-16 GB RAM	250-500 GB usable plus backup storage	Department deployment, moderate concurrent use, controlled OCR.
Medium production	8 vCPU, 16-32 GB RAM	1-2 TB usable plus backup/off-site retention	Multi-department production, regular OCR, workflow and audit growth.
Large production	12+ vCPU, 32+ GB RAM	2 TB+ usable, sized by retention and RPO/RTO	Enterprise or government deployment with high ingestion, long retention, stricter recovery targets.

For medium and large deployments, review whether the database, backup destination, or storage layer should be sized separately from the application host.

Application, Database, and Storage Split

Layer	Main sizing driver	Planning guidance
Application and workers	Concurrent users, OCR, previews, workflow activity	Scale CPU and memory for conversion and indexing peaks, not only login volume.
PostgreSQL	Metadata, workflow, audit, and job history growth	Use SSD-backed storage and include audit retention in database growth planning.
Document storage	Original files, previews, index data, backups, and logs	Size for retention, backup copies, off-host replication, and processing headroom.

Storage Sizing Method

Estimate production storage by adding:

- Original document repository size.
- Preview artifacts.
- Search, OCR, and FAISS/index data.
- PostgreSQL data and WAL/maintenance overhead.
- Backup retention footprint.
- Log retention.
- Temporary processing allowance.

- Growth reserve approved by the customer.

Storage category	Include in plan	Notes
Original documents	Yes	Primary document repository and highest recovery priority after the database.
Preview artifacts	Yes	May be regenerable, but rebuild time can affect operations.
FAISS/index data	Yes	Can be rebuilt in some cases, but OCR and indexing time must be planned.
Database	Yes	Use database-aware backup or dump procedures.
Backups	Yes	Store outside the primary application volume where possible.
Logs and temporary processing	Yes	Keep enough space for diagnostics, conversion, OCR, and backup activity.

Backup storage should normally be outside the primary application volume and replicated off-host or off-site according to the customer recovery policy.

Final Sizing Caveat

Final sizing is subject to validation. Deployment handover notes should state the expected workload, agreed sizing, growth assumptions, restore expectations, and the review date for capacity revalidation.

Deployment Manual · 5 min read · Reviewed 2026-05-15

Network, DNS, and Firewall

DeskDox should be exposed through a controlled public endpoint while database, conversion, worker, and internal application service ports remain private.

Public Endpoint Model

Production users should access DeskDox through a customer-approved FQDN, for example `https://deskdox.customer.example`. The FQDN must align with application URL configuration because outbound email links, public document links, password reset links, and integration callbacks depend on the configured public URL.

The recommended enterprise pattern is:

1. Customer DNS resolves the FQDN to the approved reverse proxy, load balancer, gateway, or host.
2. TLS terminates at the customer-approved edge or reverse proxy.
3. The reverse proxy forwards user traffic to the DeskDox frontend service.
4. The frontend NGINX proxy forwards `/api/` calls to the backend over the internal Docker network.

DNS Requirement

DNS must be confirmed before production validation. If the final FQDN is not available during installation, a temporary URL may be used only for implementation testing and must be replaced before go-live. Production must not retain local-only or temporary implementation hostnames in `FRONTEND_URL`, `PUBLIC_URL`, or allowed-origin settings.

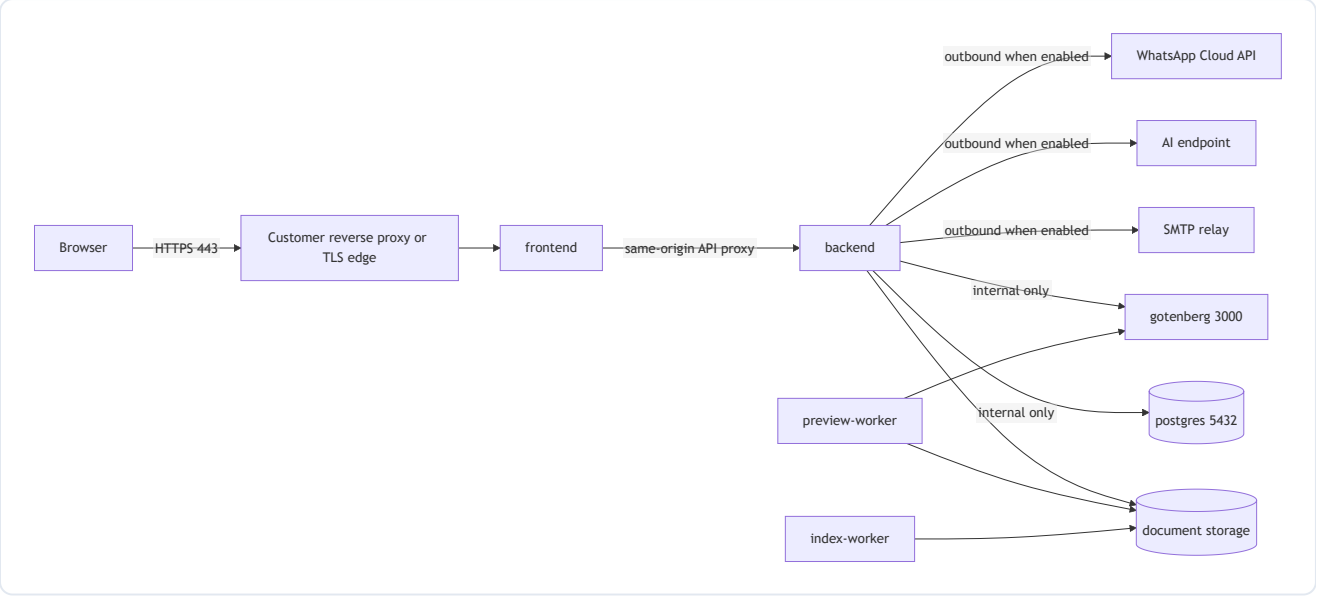
TLS Certificate Requirement

Production access should use HTTPS. The certificate may be managed by the customer reverse proxy, gateway, cloud load balancer, or another approved TLS termination point. Certificate issuance, renewal, private key custody, and HSTS policy are customer-controlled unless explicitly included in the implementation scope.

Exposure Rules

- PostgreSQL must remain internal-only.
- Gotenberg/converter must remain internal-only.
- Worker services must not expose public ports.
- Backend direct exposure should be avoided unless explicitly required by the deployment model and approved by architecture/security review.
- The public surface should be limited to HTTPS for the DeskDox web endpoint and only optional webhook endpoints required by enabled integrations.

Production Network Flow



Inbound User-Facing Ports

Port	Protocol	Destination	Purpose	Exposure guidance
`443`	HTTPS	Customer reverse proxy, gateway, or DeskDox endpoint	Primary production web access	Normal production access path.
`80`	HTTP	Customer edge or DeskDox frontend	Redirect to HTTPS or certificate validation	Optional; restrict or redirect according to customer policy.
`8080`	HTTP	`frontend` in root production Compose	Frontend HTTP binding	Bound to the loopback interface in `docker-compose.prod.yml`; use behind a reverse proxy.
`8088`	HTTP	`frontend` in Windows deploy-kit Compose	Default Windows install frontend port	Configurable through `HTTP_PORT`; review `HOST_BIND_IP` and host firewall before production use.

Internal-Only Service Ports

Port	Service	Used by	Exposure guidance
`8000`	`backend` API	`frontend` NGINX proxy and internal services	Internal only. Avoid direct public exposure unless a reviewed deployment model requires it.
`5432`	`postgres`	`backend`, workers, backup/restore processes	Internal only. Never expose PostgreSQL to the internet.
`3000`	`gotenberg`	`backend` and `preview-worker`	Internal only. Root production Compose binds it to loopback for host diagnostics.
N/A	`preview-worker`, `index-worker`	Internal job processing	No public ports. Workers communicate through database and mounted storage.

Outbound Integration Ports

Port	Destination	Purpose	Required when
`587`	SMTP relay	Email notifications and document email	Email is enabled and relay uses SMTP submission.
`465`	SMTP relay	Alternative SMTPS transport	The customer relay requires SMTPS.
`25`	SMTP relay	Customer-specific SMTP relay	The customer relay uses port 25.
`443`	WhatsApp Cloud API	WhatsApp integration	WhatsApp integration is enabled.
`443`	OpenAI, Azure OpenAI, or compatible AI endpoint	Emii, LLM, or embedding features	Cloud AI or external AI is enabled.
`11434`	Ollama endpoint	Local LLM integration	Ollama is enabled outside the container network.

SMTP, WhatsApp, OpenAI/Azure/OpenAI-compatible endpoints, and local/customer-hosted LLM endpoints are outbound dependencies only. The customer must approve outbound firewall rules, proxy settings, TLS inspection behavior, rate limits, and credential custody.

If Emii or cloud AI is disabled, outbound OpenAI/Azure access is not required. If WhatsApp is disabled, Meta WhatsApp Cloud API access is not required.

Internal-Only Services

The following services must not be reachable from the internet:

- `postgres`
- `gotenberg`
- `preview-worker`
- `index-worker`
- direct backend port `8000`, except through a reviewed and approved reverse proxy pattern
- Docker daemon or Docker socket

Network Readiness Checks

Before go-live:

- The production FQDN resolves correctly.
- HTTPS certificate is valid and trusted by customer browsers.
- Application links use the production FQDN.
- Public users cannot reach PostgreSQL, Gotenberg, workers, or Docker services.
- SMTP and enabled external integrations are tested from the deployed environment.
- Firewall decisions and the network owner are recorded in deployment handover notes.

Deployment Manual · 3 min read · Reviewed 2026-05-15

Linux Docker Compose Deployment

Linux Docker Compose is the preferred DeskDox production deployment model for customer-managed infrastructure.

Deployment Position

This model is fully supported by the repository production compose baseline. It is appropriate for dedicated Linux servers, enterprise VMs, VPS deployments, and private-cloud hosts where the customer can control storage, DNS, firewall, TLS, backup, and monitoring.

Production Compose Baseline

The root production compose file defines:

Service	Image / runtime	Persistent data
`postgres`	`postgres:16`	`/srv/edms/volumes/postgres:/var/lib/postgresql/data`
`gotenberg`	`gotenberg/gotenberg:8`	Stateless conversion service.
`backend`	`ghcr.io/dev-saifar/edms-backend:${IMAGE_TAG:-latest}`	Uploads, previews, FAISS, backups, licensing.
`preview-worker`	Same backend image	Uploads, previews, FAISS, backups, licensing.
`index-worker`	Same backend image	Uploads, previews, FAISS, backups, licensing.
`frontend`	`ghcr.io/dev-saifar/edms-frontend:${IMAGE_TAG:-latest}`	Static runtime container.

The backend startup command applies Alembic migrations before starting Uvicorn. This means deployment windows must allow for schema migration review and backup/rollback planning.

Host Preparation

The customer should provision:

- Linux server or VM with agreed CPU/RAM/storage sizing.
- Docker Engine and Docker Compose v2.
- Durable SSD-backed storage for `/srv/edms/volumes/.` or approved equivalent paths.
- Restricted administrative access.
- DNS and TLS endpoint strategy.
- Monitoring for CPU, memory, disk, Docker service state, and backup success.

Persistent Directories

The production compose baseline uses:

Host path	Container path	Purpose
`/srv/edms/volumes/postgres`	`/var/lib/postgresql/data`	PostgreSQL data.
`/srv/edms/volumes/uploads`	`/app/files`	Uploaded document binaries.
`/srv/edms/volumes/previews`	`/app/data/previews`	Preview artifacts.
`/srv/edms/volumes/faiss`	`/app/data/faiss`	Search, RAG, and index artifacts.
`/srv/edms/volumes/backups`	`/var/lib/deskdox/backups`	Backup output.
`/srv/edms/volumes/licensing`	`/var/lib/deskdox/licensing`	Licensing state.

These paths must be included in capacity planning and backup design.

Implementation Notes

Commands are provided here for deployment engineers and should be adapted to the customer's approved process.

```
cp .env.prod.template .env.prod
docker compose -f docker-compose.prod.yml--env-file .env.prod config
docker compose -f docker-compose.prod.yml--env-file .env.prod up -d
docker compose -f docker-compose.prod.yml--env-file .env.prod ps
```

Health validation should include the frontend endpoint, backend health API, container health status, and representative application smoke tests.

Linux Acceptance Criteria

Area	Expected result
Service startup	All six production services are running and healthy.
Persistence	Required host paths exist, are writable, and survive container replacement.
Public endpoint	Users access DeskDox through the approved FQDN and TLS endpoint.
Internal isolation	Database, converter, backend direct port, and workers are not publicly exposed.
Application validation	Login, upload, preview, search/OCR, workflow, email, backup, and audit tests pass.
Handover	Image tag, environment location, data paths, backup path, and support owners are documented.

Production Caveats

The Linux compose model is single-host by default. Two-tier, three-tier, and HA designs require separate design review for shared storage, database operations, worker concurrency, file locking, backup/restore, and network exposure.

Deployment Manual · 4 min read · Reviewed 2026-05-15

Windows Offline Installer Deployment

Windows deployment is supported through the DeskDox deploy-kit model and should be treated as a conditional, customer-specific deployment path rather than the preferred enterprise production baseline.

Deployment Position

Use the Windows offline installer model when:

- The customer requires Windows-based server operations.
- The environment is offline or registry access is restricted.
- The customer accepts the Docker runtime, service startup, Windows update, antivirus, and operational support boundaries.
- The implementation team has validated the deploy-kit package against the target host.

Linux remains the preferred production baseline where the customer has no Windows-specific requirement.

Deploy-Kit Components

Component	Purpose
`deploy-kit/compose/docker-compose.production.yml`	Production Compose definition for Windows deploy-kit deployments.
`deploy-kit/config/.env`	Configuration template copied to `.env` on first install.
`deploy-kit/scripts/install.ps1`	Installation and bootstrap entry point.
`deploy-kit/scripts/healthcheck.ps1`	Service and web endpoint validation.
`start.ps1`, `stop.ps1`, `restart.ps1`	Operational service control.
`backup.ps1`, `restore.ps1`	File/database backup and restore utilities.
`upgrade.ps1`	Upgrade helper for image/package updates.
`deploy-kit/tools/nssm.exe`	Windows service hosting support.

Windows Compose Baseline

The deploy-kit compose file defines `postgres`, `gotenberg`, `backend`, `preview-worker`, `index-worker`, and `frontend` on an internal Docker bridge network. The frontend publishes `${HOST_BIND_IP:-0.0.0.0}:${HTTP_PORT:-8088}:80`, which means network exposure depends on the configured bind IP and firewall rules.

The default deploy-kit configuration uses:

Setting	Default / template value	Planning implication
`DATA_ROOT`	`C:/ProgramData/DeskDox`	Primary persistent data location.
`HTTP_PORT`	`8088`	Default local/LAN HTTP access before TLS or reverse proxy.
`HOST_BIND_IP`	`0.0.0.0`	May expose to all host interfaces unless restricted by firewall or changed.
`IMAGE_TAG`	`v1.0.56` in current template	Must be confirmed for the target release.
`PUBLIC_URL` / `FRONTEND_URL`	Auto-generated on first install	Must be updated to the approved production URL where applicable.

Antivirus and Endpoint Security

Windows endpoint protection must be reviewed before production. The customer security team should approve exclusions or controlled-access rules for:

- `DATA_ROOT` and its subdirectories.
- PostgreSQL data files.
- Uploaded documents and preview artifacts.
- FAISS/index data.
- Backup output directories.
- Temporary processing paths used during conversion, OCR, backup, and restore.

The goal is to avoid file locks, quarantine, or partial backup corruption while maintaining security monitoring.

Support Boundaries

The implementation team can support DeskDox application configuration, deploy-kit scripts, container startup, application validation, and documented backup/restore workflows. The customer remains responsible for Windows patching, Docker runtime support, host hardening, antivirus policy, Windows service recovery behavior, storage reliability, firewall configuration, certificate lifecycle, and backup media.

Use of Docker Desktop for production should be reviewed carefully with the customer. Licensing, auto-start behavior, resource limits, Windows updates, and interactive-user dependencies must be assessed before production use.

Implementation Notes

Run deploy-kit scripts from an elevated PowerShell session according to the customer change window.

```
.\scripts\install.ps1
.\scripts\healthcheck.ps1
.\scripts\backup.ps1 -Tag "pre-go-live"
```

Restore is destructive and overwrites current database and runtime files. It should be tested outside production before go-live. If restore testing is deferred, record the decision and follow-up validation plan in deployment handover notes.

Windows Readiness Checks

Area	Expected result
Installation	Deploy-kit install completes without missing images, scripts, or privileges.
Service control	Windows service and Docker containers start after reboot.
Health check	`healthcheck.ps1` reports all required services operational.
Network	Bind IP, host firewall, and reverse proxy exposure match the reviewed design.
Data path	`DATA_ROOT` has capacity, permissions, backup coverage, and endpoint security handling.
Operations	Start, stop, restart, backup, restore, and upgrade ownership is documented.

Deployment Manual · 6 min read · Reviewed 2026-05-15

Appendix: Environment Variables and Directories

This appendix provides a deployment reference for services, directories, environment variables, ports, validation commands, and glossary terms. It is intended for implementation and handover use.

Service List

Service	Required	Purpose
`frontend`	Yes	NGINX-served React UI and `/api/` proxy.
`backend`	Yes	FastAPI application and main API runtime.
`postgres`	Yes	PostgreSQL database.
`gotenberg`	Yes	Document conversion for preview workflows.
`preview-worker`	Yes in production Compose paths	Preview job processing.
`index-worker`	Yes in production Compose paths	OCR, search indexing, and retrieval/index processing.

Directory List

Directory / path	Purpose	Production note
`/srv/edms/volumes/postgres`	Linux PostgreSQL data	Must be durable and backed up through a database-aware process.
`/srv/edms/volumes/uploads`	Linux uploaded documents	Must be included in backup and capacity planning.
`/srv/edms/volumes/previews`	Linux preview artifacts	Can be regenerated in some cases but should be protected for operational continuity.
`/srv/edms/volumes/faiss`	Linux search/RAG/index artifacts	Include in backup or plan reindex time.
`/srv/edms/volumes/backups`	Linux backup output	Prefer off-host/off-site copy.
`/srv/edms/volumes/licensing`	Linux licensing state	Must be preserved.
`C:/ProgramData/DeskDox`	Windows deploy-kit `DATA_ROOT`	Contains production data paths under the deploy-kit model.

Environment Variable Reference

Application and Public URL

Variable	Purpose	Production note
`IMAGE_TAG`	Container image version	Pin to the target release.
`DEBUG`	Runtime debug behavior	Production should be `false`.
`FRONTEND_URL` / `PUBLIC_URL`	Public application URL	Must be the real FQDN, not a local-only URL.
`ALLOWED_ORIGINS` / `CORS_ORIGINS`	Browser origin allow-list	Verify actual runtime behavior during validation.
`EDMS_AUTO_SEED`	Automatic seed behavior	Should be disabled for production (`0` or unset).

Database

Variable	Purpose	Production note
`POSTGRES_DB`	Database name	Present in production templates.
`POSTGRES_USER`	Database user	Use deployment-specific credentials.
`POSTGRES_PASSWORD`	Database password	Must be strong and secret.
`DATABASE_URL`	Backend database connection	Compose uses service host `postgres`.
`POSTGRES_CONTAINER_NAME`	Backup/restore container reference	Used by deploy-kit and backup tooling contexts.

Security and Authentication

Variable	Purpose	Production note
`JWT_SECRET_KEY`	Token signing secret	Must be unique, random, and protected.
`JWT_ALGORITHM`	Token signing algorithm	Template value is `HS256`.
`ACCESS_TOKEN_EXPIRE_MINUTES`	Session/token lifetime	Set according to customer security policy.

Email

Variable	Purpose	Production note
`SMTP_HOST`, `SMTP_PORT`	SMTP relay endpoint	Required when email is in scope.
`SMTP_USER`, `SMTP_PASSWORD`	SMTP credentials	Handle as secrets.
`EMAIL_FROM`	Default sender address	Should align with the customer email domain and relay policy.
`SMTP_SEND_TIMEOUT_SECONDS`	SMTP socket timeout	Default in backend example is `30` seconds.

Converter, Storage, and Workers

Variable	Purpose	Production note
`CONVERTER_URL`	Gotenberg endpoint	In Docker Compose, `http://gotenberg:3000`.
`CONVERTER_TIMEOUT_SECONDS`	Conversion timeout	Template default is `120`.
`OCR_ENABLED`	OCR enablement	Default production templates enable OCR.
`TESSERACT_CMD`	Tesseract executable path	Linux Compose sets `/usr/bin/tesseract`; Windows can auto-detect or configure.
`TESSERACT_LANG`	OCR language	Template default is `eng`.
`OCR_MAX_PAGES`	OCR page limit	Template default is `10`.
`INDEX_WORKER_ENABLED`	Index worker behavior	Dedicated worker container sets this to `true`.
`PREVIEW_WORKER_ENABLED`	Preview worker behavior	Dedicated worker container sets this to `true`.
`DATA_ROOT`	Windows deploy-kit data root	Default `C:/ProgramData/DeskDox`.
`HTTP_PORT`, `HOST_BIND_IP`	Windows frontend binding	Default `8088` and `0.0.0.0`; review exposure.

Backup and Licensing

Variable	Purpose	Production note
`BACKUP_ROOT`	Backup output path	Must have sufficient capacity and protection.
`BACKUP_ENCRYPTION_KEY`	Backup encryption key	Store separately from backup archives.
`BACKUP_WORKER_ENABLED`	Backup worker enablement	Template default is `true`.
`BACKUP_RETENTION_DAILY`, `BACKUP_RETENTION_WEEKLY`, `BACKUP_RETENTION_MONTHLY`	Retention controls in backend settings	Defaults in `config.py` are 7 daily, 4 weekly, and 12 monthly.
`LICENSE_DATA_DIR`	Licensing data path	Mounted in production Compose.

AI, Emii, WhatsApp, and Optional Redis URL

Variable	Purpose	Production note
`LLM_ENABLED`, `EMII_ENABLED`, `RAG_ENABLED`, `AI_EXTERNAL_ENABLED`	AI/Emii features	Confirm customer data handling and outbound access before enabling.
`OPENAI_API_KEY`, `OPENAI_BASE_URL`, `OPENAI_MODEL`	OpenAI-compatible AI integration	Required only for cloud AI features.
`AZURE_OPENAI_API_KEY`, `AZURE_OPENAI_ENDPOINT`, `AZURE_OPENAI_DEPLOYMENT`	Azure OpenAI integration	Required only for Azure OpenAI mode.
`OLLAMA_BASE_URL`, `OLLAMA_MODEL`	Local LLM integration	Required only for Ollama mode.
`WHATSAPP_PHONE_NUMBER_ID`, `WHATSAPP_ACCESS_TOKEN`, `WHATSAPP_APP_SECRET`, `WHATSAPP_VERIFY_TOKEN`	WhatsApp Cloud API	Required only when WhatsApp integration is enabled.
`REDIS_URL`	Optional AI/WhatsApp state or rate-limit backing	No Redis service is present in the current production Compose baseline.

Validation Commands

Use commands only in implementation or handover contexts.

```
docker compose -f docker-compose.prod.yml--env-file .env.prod config
docker compose -f docker-compose.prod.yml--env-file .env.prod ps
docker compose -f docker-compose.prod.yml--env-file .env.prod logs--tail 100 backend
```

```
.\deploy-kit\scripts\healthcheck.ps1
.\deploy-kit\scripts\backup.ps1 -Tag "validation"
```

Glossary

Term	Meaning
FQDN	Fully qualified domain name used as the production DeskDox URL.
RPO	Recovery Point Objective; maximum acceptable data loss measured in time.
RTO	Recovery Time Objective; maximum acceptable recovery duration.
Gotenberg	Conversion service used by DeskDox for preview workflows.
FAISS	Local vector/index artifact storage used by retrieval/search-related features.
OCR	Optical character recognition for scanned or image-based documents.
Deploy-kit	Windows-oriented deployment package containing Compose, configuration, scripts, and installer assets.

Deployment Manual · 4 min read · Reviewed 2026-05-15

Identity and Access Deployment

Identity and access deployment covers the first production administrators, role and department readiness, authentication policy, email-dependent account flows, and license activation. These decisions should be confirmed before the system is opened to business users.

Deployment Identity Decisions

Decision area	Required planning	Go-live impact
Initial administrators	Name the customer-owned administrators who will receive system access after installation.	Avoids shared or unmanaged production administration.
Role model	Confirm built-in roles, custom role requirements, and approval ownership for permission changes.	Determines which users can upload, approve, share, administer, and audit content.
Department model	Confirm initial departments and folder ownership expectations.	Affects folder visibility, workflow routing, and permission-based access.
Authentication policy	Confirm password policy, session policy, and MFA expectations.	Aligns DeskDox access behavior with customer security policy.
Email dependency	Confirm SMTP before relying on invitations, password reset links, notifications, and document email.	Prevents account and sharing workflows from failing after rollout.
License activation	Confirm online or offline activation process and owner.	Ensures licensed features are available before production users start.

Initial Administrator Access

Production administrator access should be issued to named customer owners. Shared credentials should be avoided. If a temporary implementation account is required during deployment, agree its expiry, ownership, and removal plan before go-live.

Record the following in the deployment handover notes:

- Named application administrators.
- Named infrastructure or Docker host administrators.
- Backup and restore owner.
- Security or audit owner.
- Support escalation owner.
- Any temporary access that must be disabled after handover.

RBAC and Department Readiness

DeskDox access is controlled through roles, permissions, departments, and document or folder-level access rules. Before go-live, administrators should confirm that the first set of users can perform only the actions

required for their responsibilities.

Access area	Validation example
Upload and edit permissions	A normal document user can upload where expected and cannot modify restricted administration settings.
Approval permissions	Approvers can open assigned tasks and cannot approve tasks outside their assignment.
Department visibility	Department users see the correct folders, documents, and workflow queues.
Administrative permissions	System administrators can open required settings while non-admin users cannot.
Audit visibility	Audit or compliance users can view required history without receiving unnecessary write access.

MFA and Password Policy

If MFA or stronger password rules are required by customer policy, enable and validate those controls before broad user onboarding. Confirm whether MFA is optional, administrator-only, or required for all users according to the customer's security policy.

Password reset and invitation flows depend on correct public URL and SMTP configuration. Validate email links after the production FQDN is configured so users receive links that open the intended DeskDox environment.

License Activation Planning

DeskDox licensing may use online or offline activation depending on the deployment package and customer environment. The deployment team should confirm:

- Who owns license activation.
- Whether internet access is available from the deployed environment.
- Whether offline challenge/response activation is required.
- Whether the license state must be preserved in backup and restore planning.
- Which licensed features must be validated before go-live.

Identity and Access Go-Live Checks

Before go-live:

- Named administrators can sign in.
- Temporary implementation access is removed or has a documented removal date.
- Required roles and departments are configured.
- Representative users have passed permission checks.
- MFA and password policy match the approved customer baseline.
- SMTP-dependent account and notification flows have been tested.
- License activation state is valid and feature access has been confirmed.

Deployment Manual · 5 min read · Reviewed 2026-05-15

Security and Hardening

DeskDox production security should be implemented as layered controls across the network, host, container runtime, application configuration, database, storage, backup, integrations, and operations.

Core Security Position

Do not expose database, converter, worker, Docker daemon, or internal service ports publicly. The public surface should be limited to the approved DeskDox web endpoint and only the integration endpoints explicitly required by the deployment model.

Layered Security Model

Layer	Baseline control
Network edge	FQDN, HTTPS/TLS, firewall restrictions, optional WAF or reverse proxy controls.
Host OS	Patched OS, restricted admin access, endpoint protection, time sync, disk monitoring.
Docker runtime	Approved runtime version, restricted Docker access, controlled Compose files, restart policies.
Application	`DEBUG=false`, correct public URL, rate limiting, RBAC, audit logging, maintenance controls.
Database	Internal-only network access, strong credentials, backup coverage, restricted admin access.
Storage	Durable paths, least-privilege filesystem permissions, antivirus/EDR compatibility, encryption where required.
Integrations	Least-privilege API keys, outbound allow-lists, credential rotation, vendor risk review.
Operations	Monitoring, log retention, patch cadence, backup review, escalation, change control.

TLS and HTTPS

Production DeskDox access should use HTTPS. HTTP should be redirected to HTTPS or restricted to internal health/implementation use. TLS certificate ownership, renewal, cipher policy, and HSTS configuration must follow the customer security standard.

Secrets Management

The following values must be treated as secrets:

- `JWT_SECRET_KEY`
- `POSTGRES_PASSWORD`
- `DATABASE_URL` when it contains credentials
- `BACKUP_ENCRYPTION_KEY`
- SMTP passwords or tokens
- WhatsApp access tokens and app secrets
- OpenAI/Azure/OpenAI-compatible API keys
- License or activation secrets where applicable

Environment files must be access-restricted. Secrets should not be pasted into tickets, screenshots, handover documents, or unsecured chat channels. Rotation procedures should be agreed for long-lived production deployments.

Database Isolation

PostgreSQL must remain internal-only. Remote database access, if required for DBA operations, must use a controlled administrative path such as VPN, bastion, restricted firewall rule, or approved database management plane. Public internet exposure of port `5432` is not acceptable.

Least Privilege Access

Least privilege applies to:

- Host administrators.
- Docker operators.
- DeskDox application administrators.
- Database administrators.
- Backup operators.
- Integration credential owners.

Application admin accounts should be named accounts where possible. Shared administrator accounts should be avoided or governed through a privileged-access process.

Auditability

Production readiness validation should confirm that representative login, document, sharing, admin, and workflow events are visible in audit/history views. Audit retention expectations must be reviewed because long retention windows affect database growth and reporting performance.

Admin Account Control

Initial administrator credentials must be rotated or transferred through an approved secure process after installation. Dormant, test, and implementation accounts should be disabled or removed before production handover.

Public Link Controls

Public document links, file requests, document email links, and password reset links depend on correct public URL configuration and token controls. Customers should review link expiry, recipient expectations, external access policy, and audit requirements before enabling public-facing document workflows.

Backup Encryption

Backups should be encrypted when handled by DeskDox backup tooling or stored outside protected infrastructure. The `BACKUP_ENCRYPTION_KEY` must be stored separately from the backup archive. Losing the key may make encrypted backups unrecoverable; exposing the key may compromise backup confidentiality.

Filesystem Permissions

Document storage, preview data, index data, backup paths, licensing files, and environment files should be restricted to the required service or administrator identities. On Windows, endpoint security exclusions must prevent file locking and quarantine without disabling monitoring. On Linux, SELinux/AppArmor policy interactions must be reviewed where enforcement is enabled.

Container Hardening

Production hardening should include:

- Use only approved image tags.
- Avoid uncontrolled `latest` usage unless deliberately used during a temporary implementation phase.
- Restrict Docker socket exposure to components that genuinely require it.
- Monitor container restarts and health status.
- Keep host Docker runtime patched.
- Prevent public access to Docker APIs.

Patching and Upgrade Cadence

Customer change management should define:

- OS patch window.
- Docker/runtime patch window.
- DeskDox application upgrade window.
- Backup taken before upgrades.
- Rollback or restore plan.
- Post-upgrade smoke test and handover note update.

Logging and Monitoring

Monitor application health, container state, CPU, RAM, disk, database availability, backup success, preview/index worker behavior, email failures, and integration errors. Logs should be retained according to customer policy and reviewed for sensitive data exposure.

Security Readiness Checks

Before go-live:

- HTTPS is active on the production URL.
- Placeholder secrets have been replaced.
- Internal service ports are not publicly reachable.
- Admin accounts are controlled.
- Backup encryption key handling is documented.
- Audit logging has been validated.
- Security owner and residual risk notes are recorded where applicable.

Deployment Manual · 4 min read · Reviewed 2026-05-15

Storage, Backup, and Disaster Recovery

DeskDox recoverability depends on coordinated backup of the database, document storage, generated artifacts, index data, licensing state, and operational configuration.

Storage Classes

Storage class	Examples / paths	Recovery importance
Database	PostgreSQL data directory or database dump	Critical system of record for metadata, users, roles, workflows, audit, settings, and jobs.
Uploaded documents	`/app/files`, Linux `/srv/edms/volumes/uploads`, Windows `DATA_ROOT/uploads`	Critical document repository.
Previews	`/app/data/previews`	Operational continuity; may be regenerable but can be expensive to rebuild.
OCR/index data	`/app/data/faiss`	Search, Emii, and retrieval performance; may be rebuildable but reprocessing time must be considered.
Backups	`/var/lib/deskdox/backups`, Windows `BACKUP_ROOT`	Must be protected and copied off-host or off-site.
Logs	Docker logs, host logs, reverse proxy logs	Required for operations, support, and audit investigation depending on policy.
Temporary processing	Converter, OCR, and backup temporary paths	Usually not retained; ensure sufficient capacity and endpoint security compatibility.
Licensing	`/var/lib/deskdox/licensing`	Required to preserve activation and licensing state.

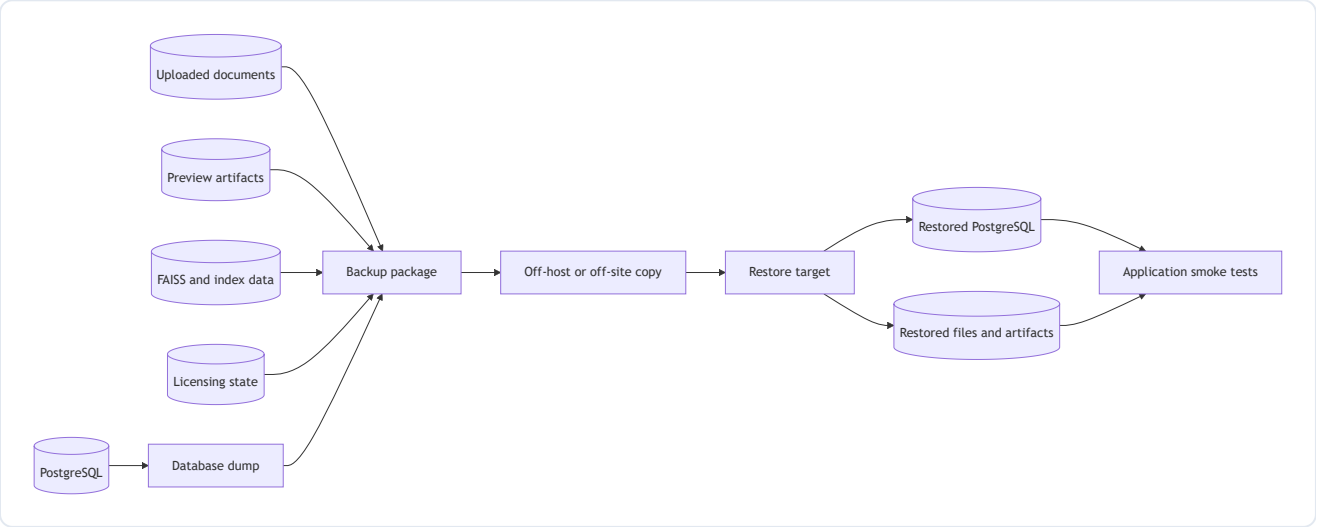
Backup Scope

Production backup planning should include:

- PostgreSQL database backup or dump.
- Uploaded document binaries.
- Preview artifacts where included in the continuity plan.
- FAISS/search/index artifacts where included in the continuity plan.
- Licensing directory.
- Environment/configuration record sufficient to rebuild the deployment.
- Backup metadata, timestamp, release tag, and restore notes.

The Windows deploy-kit `backup.ps1` script creates a `database.sql` dump and copies `uploads`, `faiss`, and `previews` from `DATA_ROOT` into a timestamped backup directory. Restore through `restore.ps1` recreates the target database and restores those file directories. This procedure is destructive and must be tested carefully.

Backup and Restore Flow



Backup Retention

Retention must be defined by the customer. The application configuration includes daily, weekly, and monthly retention settings, but the final retention policy must also account for storage cost, legal/regulatory retention, off-host copy, and restore testing.

Recommended planning questions:

- How many daily, weekly, and monthly recovery points are required?
- Is immutable or write-once storage required?
- How long must audit logs be retained?
- Must backups be encrypted at rest?
- Who verifies backup success?
- Who approves backup deletion?

Off-Host and Off-Site Copy

Backups stored only on the application host do not provide sufficient disaster recovery protection against host failure, ransomware, storage corruption, or site loss. Production deployments should copy backups to customer-approved off-host or off-site storage.

The off-host copy mechanism may be a customer backup platform, storage replication, object storage, network share, or enterprise backup agent. The customer owns the durability and access controls of that backup destination unless covered by a separate managed service arrangement.

Restore Testing

Restore testing must validate:

- Database restore.
- Document file restore.
- Preview/index artifact restore or accepted regeneration path.
- Licensing state.
- Application startup after restore.
- Login, upload, preview, search, workflow, email, and audit smoke tests.

Production deployments should include a restore validation exercise before go-live. If restore testing is deferred, the decision should be recorded in the deployment handover notes with the reason, owner, target validation date, and interim recovery approach.

DR Server Assumptions

A disaster recovery server is not automatically created by the current compose package. If the customer requires a standby environment, it must be designed separately and must include:

- Compatible DeskDox release/image tag.
- Compatible environment configuration.
- Restorable database target.
- Restorable document and artifact paths.
- DNS cutover or alternate access plan.
- License/activation handling.
- Backup access permissions.
- Defined RPO/RTO.

RPO/RTO Planning

Objective	Planning impact
RPO	Determines backup frequency, replication needs, and acceptable data loss.
RTO	Determines restore automation, standby readiness, database size limits, and staffing.
Retention	Determines backup storage capacity, off-site copy volume, and archive lifecycle.
Restore confidence	Requires scheduled restore validation and documented recovery procedures.

Backup and DR Readiness Checks

Before go-live:

- Backup location and retention are documented.
- Initial backup completes successfully.
- Backup includes required data classes.
- Backup encryption key handling is documented.
- Off-host/off-site copy is configured or the deferral is recorded in handover notes.
- Restore validation is completed or a follow-up validation plan is recorded.
- RPO/RTO are documented with operational owners.

Deployment Manual · 3 min read · Reviewed 2026-05-15

Operations and Maintenance

DeskDox production operation requires active monitoring, controlled patching, backup review, upgrade planning, and clear support ownership.

Monitoring Areas

Area	What to monitor
CPU	Sustained high usage, spikes during OCR, preview conversion, backups, or search indexing.
RAM	Container memory pressure, host memory exhaustion, database memory pressure.
Disk	Database volume, uploads, previews, FAISS/index data, backups, logs, and temporary processing capacity.
Docker containers	Running state, health status, restart count, failed pulls, image tag drift.
Database health	PostgreSQL readiness, connection failures, slow queries, storage growth, backup consistency.
Backup success	Schedule execution, archive presence, size trends, retention cleanup, off-host copy status.
Preview/index workers	Worker running state, queue growth, conversion failures, OCR errors, stale jobs.
Email failures	SMTP connectivity, authentication failures, bounced notifications, wrong public URL links.
Integrations	WhatsApp/API errors, OpenAI/Emii failures, rate limits, credential expiry.

Patch Management

Patch management should cover:

- Host operating system.
- Docker Engine and Compose.
- Reverse proxy or gateway.
- TLS certificate renewal.
- DeskDox images and deploy-kit package.
- Database maintenance and patching if using a separated database tier.

Patching should be performed during approved maintenance windows and preceded by a verified backup.

Upgrade Planning

DeskDox upgrades may include image updates and database migrations. The backend production startup command runs Alembic migrations before starting the API, so upgrade planning must account for:

- Release tag selection.
- Pre-upgrade backup.
- Review of release notes and migration impact.
- Maintenance window.
- Rollback or restore procedure.
- Post-upgrade smoke test.
- Handover note update after validation.

For Windows deploy-kit deployments, `upgrade.ps1` is the operational helper. For Linux compose deployments, image tag and compose update procedures must follow the customer change process.

Change Management

Production changes should be recorded for:

- Environment variable updates.
- Image tag changes.
- DNS/TLS changes.
- Firewall changes.
- Backup retention changes.
- SMTP/WhatsApp/AI integration changes.
- Storage expansion.
- Admin and service account changes.

Each change should include owner, approval, execution window, validation steps, and rollback plan.

Log Retention

Docker logging is configured with JSON file rotation in the compose files. The customer should define log retention for host logs, container logs, reverse proxy logs, application audit logs, and integration logs. Where regulatory audit retention is required, database growth must be included in sizing.

Support Handover

The handover package should record:

- Deployment model and host details.
- DeskDox image tag/release.

- Compose file and environment file locations.
- Persistent data paths.
- Public URL and TLS owner.
- Backup path, retention, encryption key custody, and off-host copy owner.
- Admin contacts and escalation path.
- Monitoring dashboards or alert owners.
- Known open items marked `To be confirmed`.
- Go-live readiness checklist.

Escalation Information

Escalation records should include:

- Customer infrastructure owner.
- Customer application administrator.
- Customer security/network owner.
- Database/backup owner where applicable.
- DeskDox implementation/support contact.
- Severity definitions and response expectations.
- Required diagnostic information for incidents.

Operational Readiness Record

Production handover notes should record:

- Infrastructure baseline.
- Security exposure model.
- Backup and restore posture.
- RPO/RTO.
- Monitoring and operational ownership.
- Known limitations or deferred validation items.
- Go-live validation results.

The record should include the named owner for each operational area and the date the handover notes were last updated.

Deployment Manual · 3 min read · Reviewed 2026-05-15

Deployment Validation and Troubleshooting

Deployment troubleshooting should begin with service health, configuration correctness, storage availability, and network reachability before investigating application-specific behavior.

Validation Sequence

Step	Expected result
Compose validation	Compose file renders successfully with the selected environment file.
Container status	`frontend`, `backend`, `postgres`, `gotenberg`, `preview-worker`, and `index-worker` are running.
Health checks	Frontend and backend health checks pass; PostgreSQL and Gotenberg are healthy.
Public URL	Production FQDN loads the application over HTTPS.
Login	Admin and non-admin accounts can authenticate.
Upload	Test files upload successfully.
Preview	Representative PDF and Office documents preview correctly.
OCR/search	Indexed documents can be found after worker processing.
Workflow	A representative workflow can be completed.
Email	SMTP test and live notification/document email work if enabled.
Backup	Manual or scheduled backup completes and writes to the configured location.
Restore review	Restore is tested or a deferred validation plan is recorded.

Common Issue Matrix

Symptom	Likely area	Initial checks
Frontend not reachable	DNS, TLS, firewall, frontend container	Confirm FQDN, certificate, port binding, reverse proxy target, frontend health.
Login page loads but API calls fail	NGINX proxy, backend, CORS/public URL	Confirm `/api/` proxy, backend health, `FRONTEND_URL`, allowed origins.
Backend unhealthy	Database, required env vars, migrations, startup settings	Check `DATABASE_URL`, `JWT_SECRET_KEY`, `CONVERTER_URL`, production guards, migration logs.
Database connection failure	PostgreSQL, credentials, network	Confirm postgres container health, credentials, `DATABASE_URL`, internal DNS name.
Previews fail	Gotenberg, preview worker, storage permissions	Confirm Gotenberg health, `CONVERTER_URL`, worker status, upload/preview paths.
OCR/search delayed	Index worker, Tesseract, workload	Confirm index worker running, `OCR_ENABLED`, `TESSERACT_CMD`, queue volume, CPU.
Email links use wrong URL	Public URL configuration	Confirm `FRONTEND_URL` or `PUBLIC_URL` and application settings.
SMTP fails	Relay, credentials, firewall, TLS policy	Confirm host, port, user/password, outbound firewall, relay allow-list, and test recipient.
Backup fails	Backup path, Docker access, permissions, encryption key	Confirm `BACKUP_ROOT`, available disk, key presence, write permissions, and deployment-specific backup method.
Restore fails	Backup integrity, destructive restore sequence, service state	Validate backup contents, database dump, data paths, restore procedure, and available disk.

Implementation Notes

Linux compose diagnostics:

```
docker compose -f docker-compose.prod.yml--env-file .env.prod ps
docker compose -f docker-compose.prod.yml--env-file .env.prod logs--tail 100 backend
docker compose -f docker-compose.prod.yml--env-file .env.prod logs--tail 100 preview-worker
docker compose -f docker-compose.prod.yml--env-file .env.prod logs--tail 100 index-worker
```

Windows deploy-kit diagnostics:

```
.\deploy-kit\scripts\healthcheck.ps1
docker compose -f .\deploy-kit\compose\docker-compose.production.yml--env-file .\deploy-kit\.env ps
```

Commands should be executed by authorized deployment or operations personnel.

Escalation Data

For support escalation, collect:

- Deployment model and OS.
- DeskDox image tag/release.
- Compose file path and sanitized environment summary.
- Container status and health.
- Relevant logs with secrets removed.
- Public URL and reverse proxy pattern.
- Recent change history.
- Backup/restore status if data recovery is involved.
- Exact user-facing error and timestamp.

Troubleshooting Boundary

DeskDox support can assist with application behavior, container configuration, documented deployment scripts, and product-level validation. Customer infrastructure teams own DNS, TLS, reverse proxy, firewall, host OS, Docker runtime installation, endpoint security policy, storage health, SMTP relay, external API availability, and enterprise monitoring platforms.

Deployment Manual · 4 min read · Reviewed 2026-05-15

Go-Live Readiness Checklist

Go-live readiness confirms that DeskDox has been deployed, secured, validated, backed up, and handed over according to the selected customer-managed deployment model. This article is a documentation checklist for operational readiness; it is not a formal completion certificate.

Readiness Checklist

Area	Expected result	Status
Infrastructure	Host, CPU, RAM, storage, Docker runtime, and persistent paths match the sizing baseline.	To be confirmed
Deployment model	Selected deployment model and support classification are documented.	To be confirmed
Services	`frontend`, `backend`, `postgres`, `gotenberg`, `preview-worker`, and `index-worker` are running.	To be confirmed
DNS/FQDN	Production FQDN resolves correctly.	To be confirmed
TLS	HTTPS certificate is valid and trusted.	To be confirmed
Firewall	Only the approved public endpoint is exposed; internal service ports are not public.	To be confirmed
Configuration	Production secrets, image tag, public URL, and required environment values are configured.	To be confirmed
Security	Admin account control, least privilege, auditability, and backup key custody are documented.	To be confirmed
Storage	Database, uploads, previews, FAISS/index data, backups, logs, and licensing paths are understood.	To be confirmed
Backup	Initial backup completes and backup location is documented.	To be confirmed
Restore	Restore validation is completed or a deferred validation plan is recorded.	To be confirmed
Functional smoke test	Login, upload, preview, OCR/search, workflow, email, public URL, and audit logs are validated as applicable.	To be confirmed
Operations	Monitoring, patching, backup review, escalation, and maintenance windows are assigned.	To be confirmed
Handover	Deployment notes, owners, open items, and support boundaries are documented.	To be confirmed

Functional Smoke Test

At minimum, production validation should include:

- Login with customer-approved admin account.
- Login with non-admin test account.
- Folder/document access check.
- Upload a representative PDF.
- Upload a representative Office document if Office preview is in scope.
- Confirm preview generation.
- Confirm OCR/search for a representative searchable or scanned document.
- Start and complete a representative workflow.
- Send or validate email notification if SMTP is in scope.
- Confirm public URL links use the production FQDN.
- Confirm audit/history entries for representative actions.
- Complete an initial backup.
- Review restore procedure and complete restore validation or record a deferred validation plan.

Restore Validation Deferral

Production deployments should include a restore validation exercise before go-live. If restore testing is deferred, deployment handover notes should state:

- Reason restore testing was deferred.
- Operational owner.
- Target date for first restore test.
- Interim recovery approach.

Restore validation should not be silently omitted.

Handover Roles

Role	Operational responsibility
Infrastructure owner	Host, storage, Docker/runtime, monitoring, and backup destination.
Network/security owner	DNS, TLS, firewall, endpoint security, and public exposure.
Application owner	Functional validation, admin ownership, user readiness, and go-live coordination.
DeskDox deployment engineer	Installation evidence, service validation, known issues, and handover completeness.
Operations/support owner	Escalation path, maintenance process, and ongoing monitoring readiness.

Handover Record

Deployment handover notes should include:

- Customer name and environment name.
- Deployment date.
- Release/image tag.
- Deployment model.
- Public URL.
- Data paths and backup path.
- Restore validation result or deferred validation plan.
- Open issues and mitigations.
- Named operational owners and dates.

CHAPTER 12

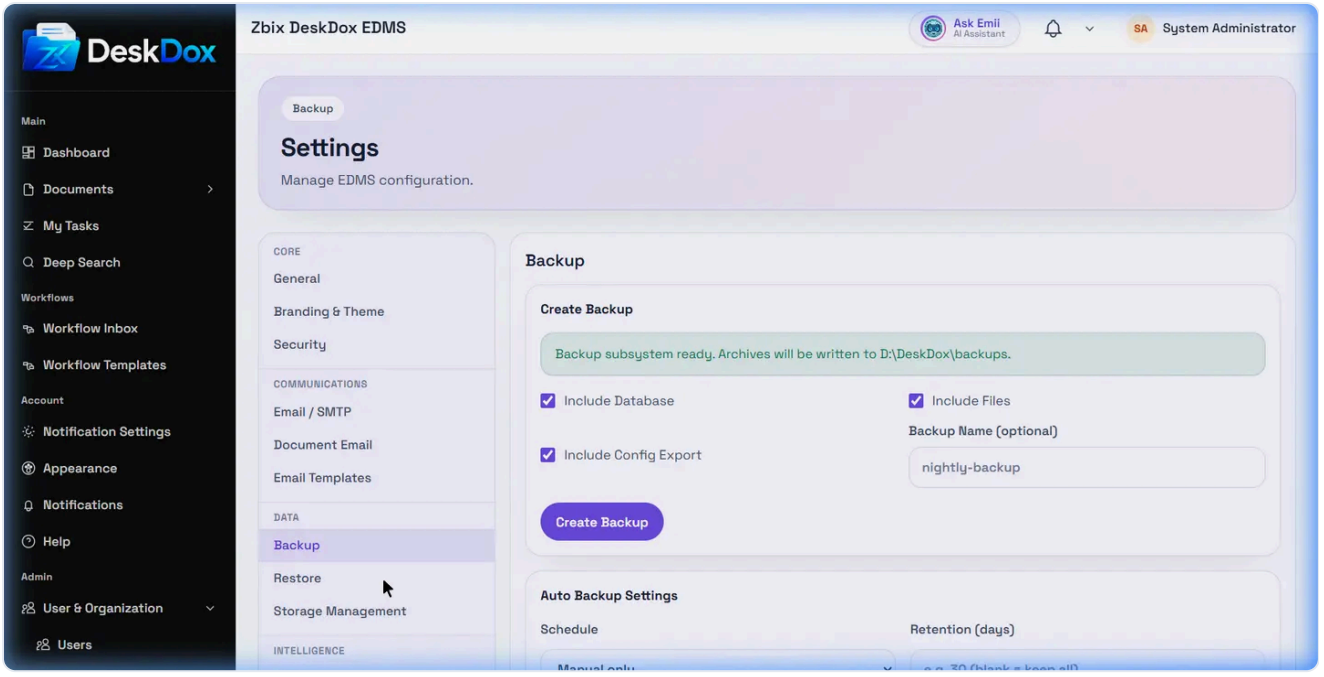
Backup, Restore, and System Health

Backups, restore, storage management, readiness checks, and platform health.

Backup, Restore, and System Health · 1 min read · Reviewed 2026-05-14

Backup Overview

Open `/app/admin/system/settings/backup` to review backup readiness and create backups.



DeskDox includes manual backups can include the database, files, and a config export. The Create Backup area shows whether the backup subsystem is ready and the effective backup root where archives are written.

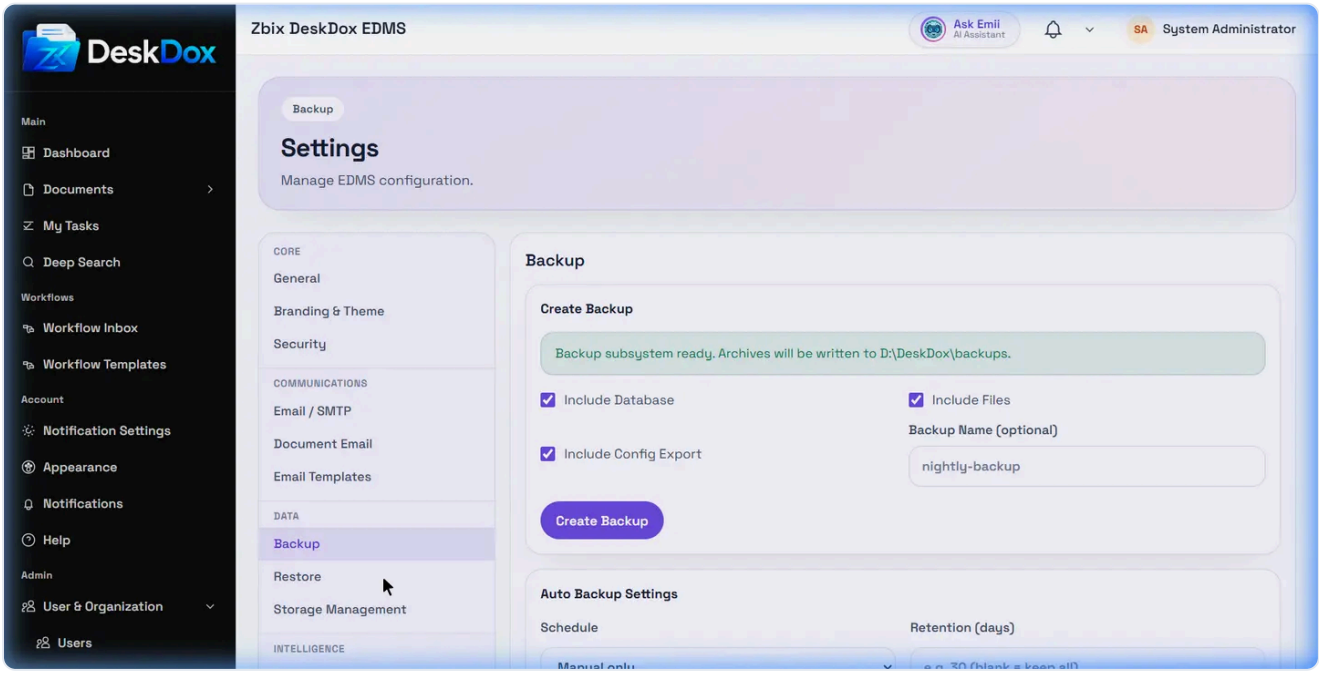
Backups are high-value operational artifacts. Store them in a protected location, control who can download them, and confirm backup and restore procedures outside peak production hours. Do not assume a backup is usable until validation or restore testing has been performed in an approved environment.

Backup, restore, and storage management are System Admin functions. EDMS Admins may see other settings sections but DeskDox keeps these Data sections out for non-System Admins.

Backup, Restore, and System Health · 1 min read · Reviewed 2026-05-14

Manual Backup and Download

To run a manual backup, open `/app/admin/system/settings/backup`, confirm the backup subsystem is ready, choose Include Database, Include Files, and/or Include Config Export, optionally enter a Backup Name, then select `Create Backup`.



DeskDox includes the backup list has Name, Created, Size, Includes, Status, Created By, and Actions columns. Completed backups can show actions for `Download`, `Verify`, `View Logs`, and `Delete`. Download and Verify are disabled until a backup status is completed.

If backup history is empty, the UI shows `No backups created yet.` The browser demo did not contain historical backups, so the screenshot does not prove what a populated production list looks like.

Treat downloaded backups as sensitive data. They may include database content, document files, and configuration export data depending on what was selected.

Backup, Restore, and System Health · 1 min read · Reviewed 2026-05-14

Restore from Backup

Open `/app/admin/system/settings/restore` to validate and start a restore.

DeskDox includes you can select an existing backup or upload a backup archive, then use `Validate Backup`. After validation, restore options include Restore Database, Restore Files, and Restore Config (sanitized).

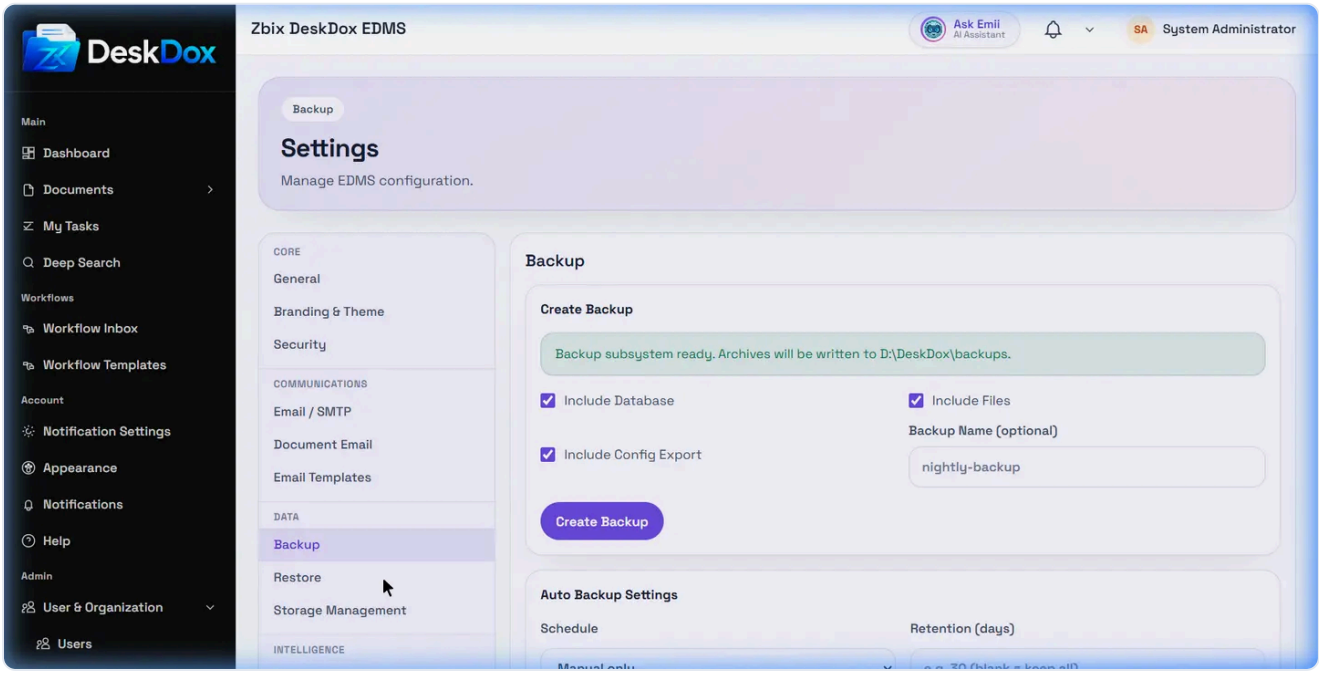
Restore is a high-risk System Admin operation because it can overwrite data. The UI requires the exact confirmation text `RESTORE DESKDOX` and an acknowledgement checkbox before `Start Restore` can run. If the button is disabled, check validation status, selected backup or upload token, the acknowledgement checkbox, and the exact confirmation string.

Only run restore after confirming the backup file, restore scope, and approval requirements.

Backup, Restore, and System Health · 1 min read · Reviewed 2026-05-14

Scheduled Backups and Readiness

The Backup page includes Auto Backup Settings. DeskDox includes Schedule options for Manual only, Daily at 2:00 AM, Weekly on Sunday at 2:00 AM, and Monthly on the 1st at 2:00 AM. It also confirms Retention days, Backup storage folder, `Browse`, `Reset`, and `Save Settings`.



Backup readiness means the system service believes the configured backup subsystem can write archives to the effective backup root. The UI can show a ready message, a readiness error, the effective backup root, last automatic backup, last automatic backup attempt, next scheduled run, scheduler unavailable errors, scheduler inactive warnings, and last automatic backup errors when the system service provides them.

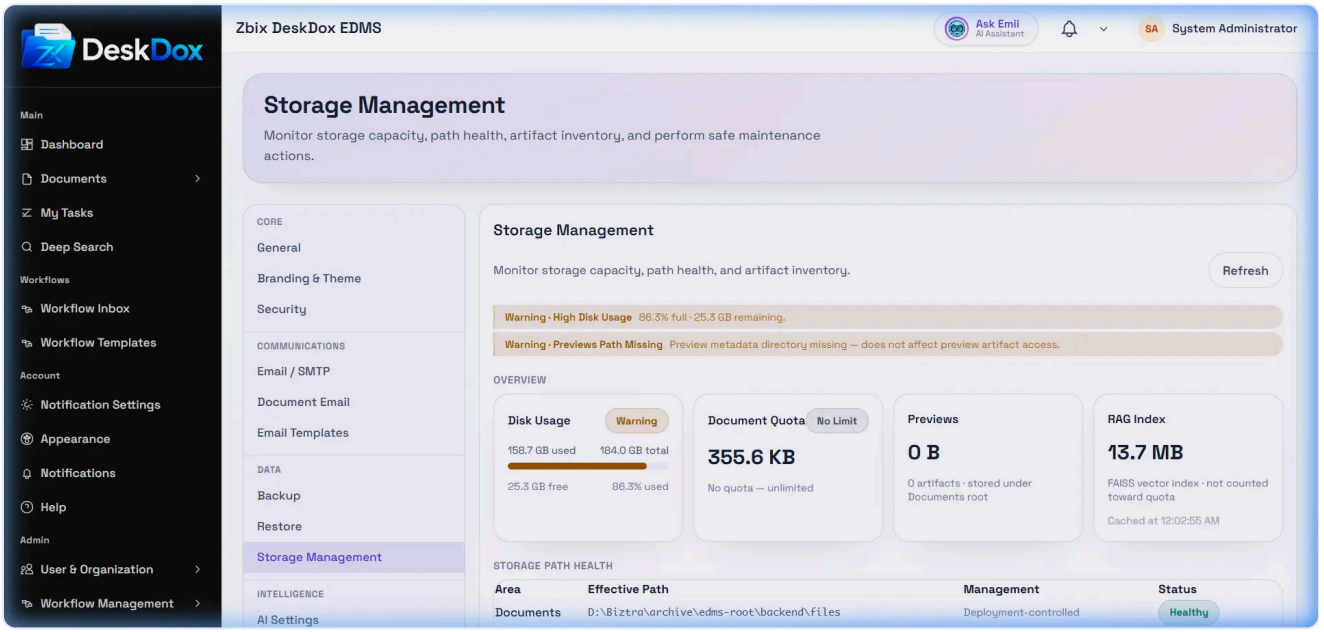
Do not claim scheduled backups are running just because a schedule is selected. Scheduled backups also depend on backup scheduler availability, active scheduler state, reachable storage, write permissions, and successful job execution. If `Manual only` is selected, automatic backups are not enabled.

Leaving the backup storage folder blank uses the default from the `BACKUP_ROOT` environment variable. Moving backup storage may require operations work and migration of existing archive files.

Backup, Restore, and System Health · 1 min read · Reviewed 2026-05-14

Storage Management

Open `/app/admin/system/settings/storage` to monitor storage capacity, path health, artifact inventory, and safe maintenance actions.



DeskDox includes overview cards for Disk Usage, Document Quota, Previews, and Search Index. It also confirms a Storage Path Health table for areas such as Documents, Previews, Search Index, and Backups, including effective path, management label, and status.

Storage warnings can mean disk usage is high, quota usage is high, a path is missing, a path is unreadable, or a path is not writable. If storage becomes full, uploads, previews, indexing, or backups may fail depending on which path is affected.

The Maintenance section includes `Clean Temp Files` for backup temporary files. The confirmation dialog uses `Delete Temp Files` and states that uploaded documents, preview artifacts, RAG/search index data, and completed backup archives are not affected. Only run cleanup when no backup job is in progress.

Backup, Restore, and System Health · 1 min read · Reviewed 2026-05-14

System Health and Status

Open `/app/admin/system/settings/status` to check health and build information.

DeskDox includes a summary status pill, product version, environment, uptime when provided, user interface service build details, application service build details, and additional health fields when system services return them. `Refresh` reloads health and version metadata. `Copy Version Info` copies a support-friendly summary of product, user interface service, application service, build tag, commit SHA, build date, environment, status, and uptime when available.

If the page shows `Unable to fetch system health`, check service connectivity, admin access, and service availability. A healthy user interface does not prove every worker or optional service is running unless that service is explicitly represented by the system health details.

CHAPTER 13

WhatsApp Integration

WhatsApp integration setup, readiness, and enabled-environment guidance.

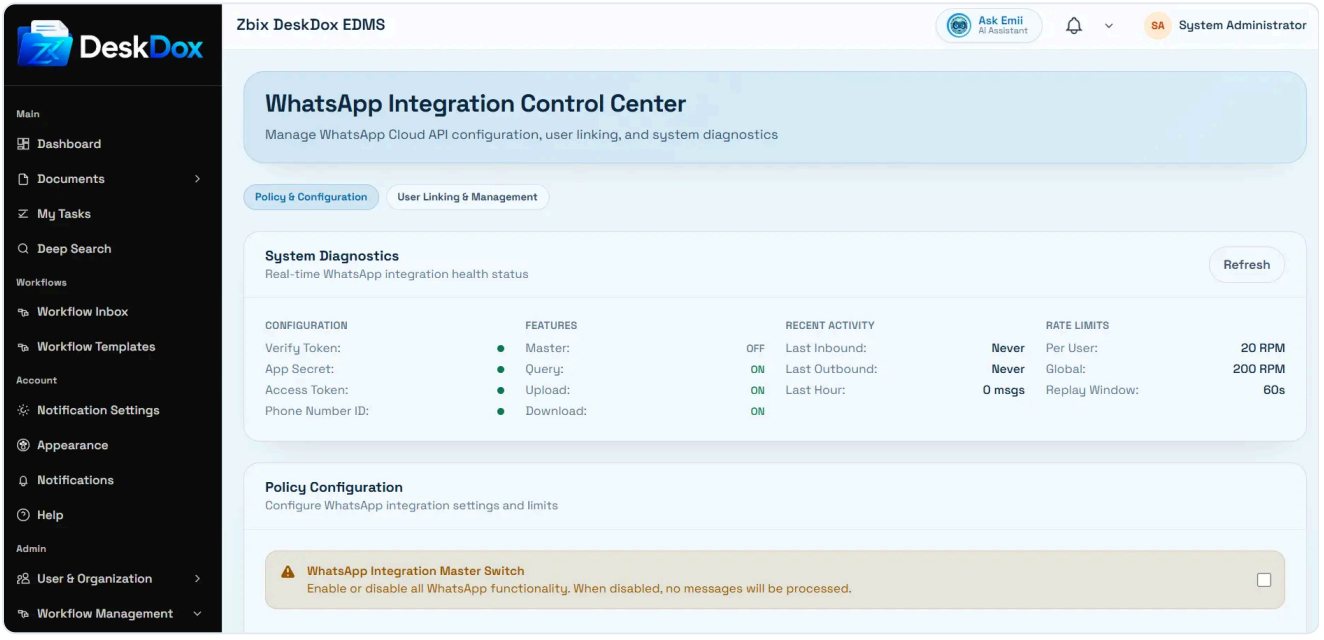
WhatsApp Integration · 1 min read · Reviewed 2026-05-13

How to Use WhatsApp Integration

Purpose

WhatsApp integration lets administrators configure WhatsApp-related communication options when the feature is enabled for the deployment.

WhatsApp integration is available only when the feature is enabled and configured for the deployment. Available options may vary by license edition and environment configuration.



Configure WhatsApp

Administrators can open the WhatsApp settings area when it is visible in the admin menu. The setup screen can include enablement controls, provider or connection settings, phone or sender details, webhook or callback values, and testing or save actions depending on the deployment.

Review every visible field before saving. Use any available test action to confirm the configuration after changes.

Troubleshooting

- WhatsApp settings missing: confirm the feature is enabled for your license and deployment.
- Save or test action unavailable: confirm your administrator role and required configuration values.
- Messages not available: confirm provider setup, deployment configuration, and any license or module requirements.

Related reading

- User Manual: Using WhatsApp with DeskDox

CHAPTER 14

Troubleshooting and FAQ

Common issues, FAQs, access problems, workflow troubleshooting, and support triage.

Troubleshooting and FAQ · 2 min read · Reviewed 2026-05-14

System Admin Troubleshooting

Use this article when an administration setting is blocked, unclear, or not behaving as expected.

If you cannot access system settings, confirm your role. System Admins can access all system settings sections. EDMS Admins can access many settings sections, but DeskDox keeps Backup, Restore, and Storage Management out for non-System Admins.

If backup is not ready, check the readiness message, effective backup root, path existence, and write permissions. If backup history is empty, the UI may simply have no completed backups yet. If scheduled backups are not running, check schedule frequency, scheduler availability, scheduler active state, storage path, retention settings, and last automatic backup error.

If restore is blocked, validate the backup first, select an existing backup or upload archive, choose restore options, acknowledge the overwrite warning, and type the exact confirmation string `RESTORE DESKDOX`. Run restore only during an approved maintenance window after validating the backup and confirming the overwrite warning.

If SMTP test fails or emails are not sending, check SMTP host, port, encryption, credentials, From Email, network access, mail server policy, and system error message. Do not expose passwords, API keys, tokens, or SMTP secrets in Help Center questions or support screenshots. If email links are wrong, check deployment Public/Base URL configuration with operations.

If a license warning appears, check license state, valid-until date, activation type, activation health, fingerprint drift, user limits, and licensed feature switches. Do not treat sample counts from screenshots as product limits.

If system status is unhealthy, refresh System Status, copy version info for support, and check service connectivity and service logs. If storage warning is shown, review Storage Management for disk usage, quota usage, path health, and temp cleanup status. If audit logs are missing, check filters, date range, permissions, and retention before assuming no activity occurred.

Contact support or your operations team when a setting depends on environment variables, filesystem mounts, mail infrastructure, activation service responses, or production restore procedures.

Troubleshooting and FAQ · 2 min read · Reviewed 2026-05-14

Workflow Admin Troubleshooting

What this helps you do

Work through common workflow admin configuration problems before escalating to a technical administrator or support.

Template not visible or unavailable during upload

Check the `Published Workflows` versus `My Workflows` tab, search text, category filter, `Show only active`, draft status, published status, `Active` flag, owner visibility, and workflow template permissions.

For upload selection, confirm the template is both published and active. Also check upload configuration, user permissions, document category behavior, and whether the user is in the expected tenant/environment.

Workflow not starting

Check that the document has a valid folder, required metadata is complete, required expiry or workflow metadata is present, the selected template is active and published, every step has a valid assignee, and the user has permission to start or apply the workflow.

If the workflow started before recent template changes, it may still use the earlier configuration.

Wrong or missing approver

Check the step assignee type: user, role, department, department head, or metadata email. Then verify selected users, role spelling, department membership, department head setup, metadata email field value, and whether the current template version is the one used by the live workflow.

Default folder not found

Search by folder name and check the full path. Subfolders can be returned by the picker when the folder search endpoint returns them. If the folder is still missing, check folder permissions, department scope, folder status, and the `/lifecycle/search/folders` search behavior with a technical admin.

SLA, stats, or supervision issues

If SLA does not update, check step SLA days/hours, business calendar, warning threshold, escalation chain, department assignment, and background reporting timing. If Workflow Stats do not update, use `Refresh` and confirm reporting jobs have run.

If Workflow Supervision is empty, clear filters, check `Active Tasks`, `Exceptions`, and `Closed / Cancelled`, confirm there are matching workflows, and verify the user has workflow task administration permission.

When to escalate

Contact a technical admin or support when permissions look correct but admin pages are hidden, folder search does not return known folders, workflow instances are stuck without a valid assignee, exception recovery is unclear, license-gated export is expected but unavailable, or background jobs are not updating SLA and stats.

Related Emii questions

- "Why is workflow not starting?"
- "Why is the wrong approver assigned?"
- "Why is SLA not updating?"
- "Who should fix workflow configuration issues?"

Troubleshooting and FAQ · 1 min read · Reviewed 2026-05-13

Frequently Asked Questions

Why can my colleague see actions I cannot?

DeskDox is role- and permission-based. Visibility and actions are not identical for all users.

Where did Advanced Search go?

Deep Search is now the primary search experience. Legacy advanced-search routes redirect to Deep Search.

Why is the Invoices tab missing?

Invoices can be feature-gated by deployment settings. In the current deployment configuration, invoices are disabled.

Why can I view but not edit/share a document?

Document and folder permissions can allow read-only access while blocking write/share actions.

Why am I asked for workflow selection during upload?

Some tenants enforce workflow on upload. Select a template or contact your admin.

Why is Emii not visible?

Emii can be disabled at environment level or hidden by deployment configuration.

Can I reset password from Forgot Password now?

UI exists, but system service reset flow can vary by deployment readiness. Follow your tenant support process if reset does not complete.

Where do I report product issues?

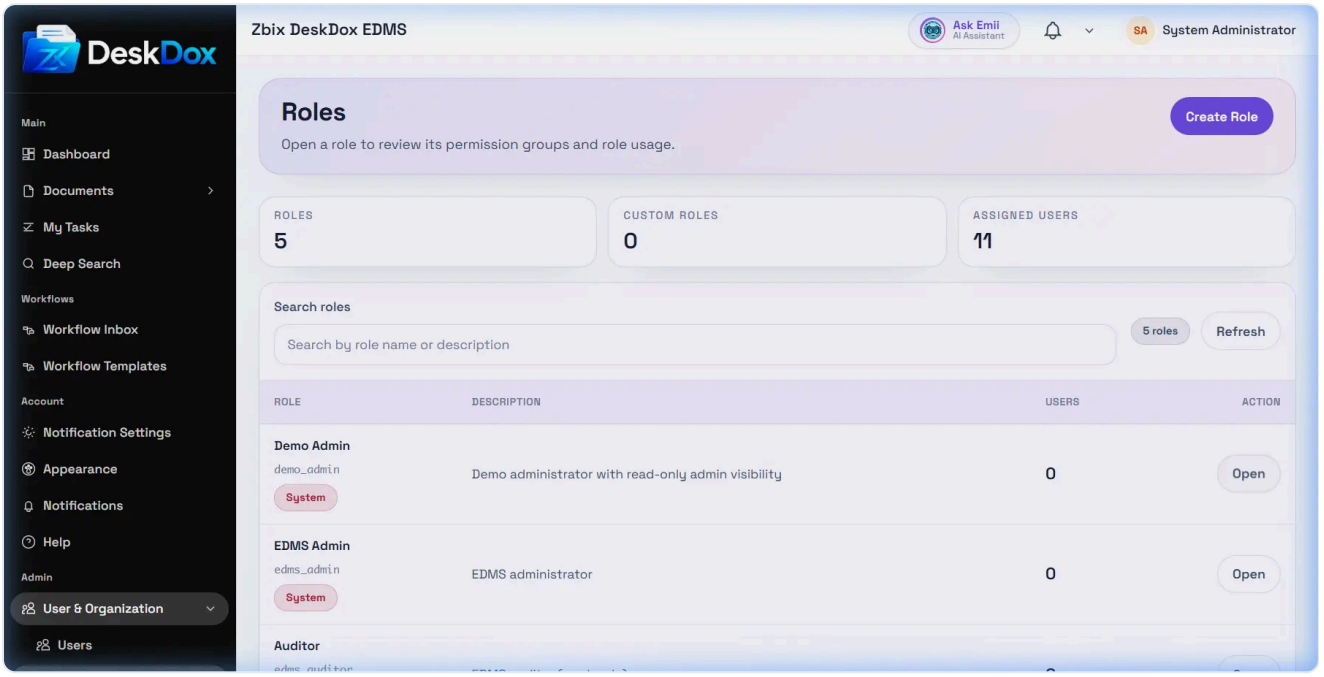
Use `Help→ Contact Support` to create a support ticket, then include reproducible steps and IDs.

Related reading

- Common Issues and Quick Fixes

Troubleshooting and FAQ · 2 min read · Reviewed 2026-05-14

Access Control Troubleshooting

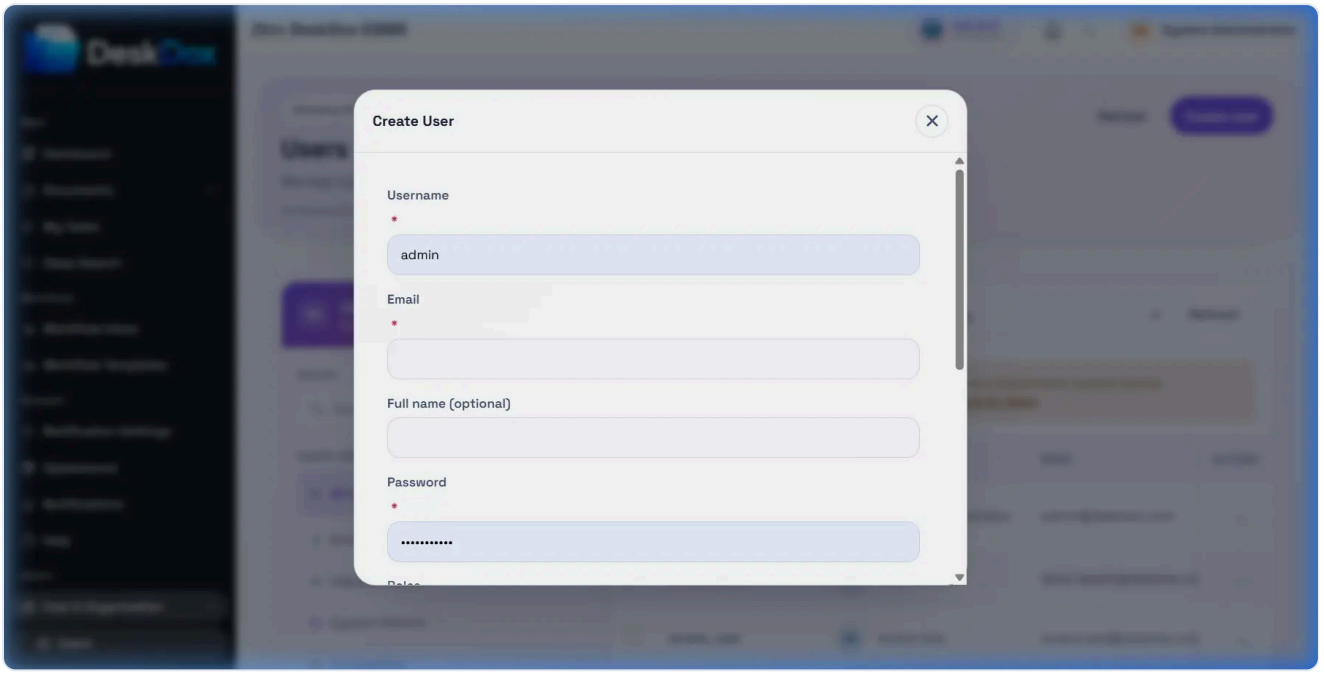


Use this checklist when access does not match expectations.

User cannot access DeskDox

Confirm the user is active, has the correct local username/email and password, is not using stale credentials, and has a department if they are an active normal user. Use `Reset Password` if needed. Invitation and reset emails depend on configured email service and queue processing.

User cannot see folders or documents



Check the user's department, folder ownership, explicit folder permissions, direct document permissions, document status, workflow assignment, and whether the document was moved, deleted, expired, or archived. A role alone may not grant folder visibility.

User cannot upload

Check that `Upload Files` is visible, the user has upload permission on the destination folder, the destination folder is selected, required metadata is complete, file rules allow the upload, and any workflow/lifecycle requirements are satisfied.

User cannot approve workflow

Check whether the active workflow task is assigned to the user, the user's role, or the user's department. Also check task status, document access, signature requirements, workflow permissions, and whether the task was already completed.

User cannot manage lifecycle

Check lifecycle admin visibility, workflow/admin permissions, role permission matrix entries, and whether the lifecycle feature is enabled and visible in the current deployment.

Role or permission changes are not working

Confirm the role was saved, the user has the role, the permission is in the correct group, the system allows the action, and department/folder/document scope also allows the action. Ask the user to refresh or sign in again if the screen still shows older permissions.

Troubleshooting and FAQ · 2 min read · Reviewed 2026-05-14

Access Denied and Permission Errors

A permission-denied page may appear when your account does not have access to the requested document, folder, workflow, or administration area.

`Unauthorized` usually means DeskDox could not accept the current authentication state. Sign in again, then retry.

`Forbidden`, `Not authorized`, or `Permission denied` usually means you are signed in but your role, department, folder permission, document permission, workflow assignment, lifecycle permission, or admin permission does not allow the action.

Try these first:

1. Refresh the page and retry from the current screen.
2. Confirm you are signed in as the expected user.
3. Check whether the item is in the expected folder and has not been moved, deleted, expired, or archived.
4. Ask an administrator to check your roles, department, role permissions, and folder/document access.
5. For workflow actions, confirm the task is assigned to you, your role, or your department and is still active.
6. For lifecycle/admin actions, confirm the admin menu and role permissions are assigned.

Contact an administrator or support when the error persists after the permission and department checks. Do not assume SSO, Active Directory, Entra ID, or external identity sync is involved unless your deployment explicitly uses and documents that feature.

Troubleshooting and FAQ · 1 min read · Reviewed 2026-05-13

Common Issues and Quick Fixes

I cannot upload a document

Check:

1. Folder selected.
2. Required workflow selected (if enforced).
3. Required metadata complete.
4. You have upload permission in that folder.

I cannot approve/reject a task

Check:

1. Task is currently assigned to you.
2. Task is active/current step.
3. Task does not require claim first.
4. Signature prerequisites are complete.

Search returns no results

Check:

1. Remove extra filters and retry.
2. Confirm spelling/identifier.
3. Verify document is not in deleted/expired context only.
4. Wait for indexing on newly uploaded or scanned files.

I do not see expected menu options

Check:

1. Your role and permissions.
2. Tenant feature availability.
3. Whether the module is intentionally gated in current release.

Notifications are missing

Check:

1. Global notification toggles are enabled.
2. Event-level channels are enabled.
3. Email channel is available for your tenant.

Related reading

- Frequently Asked Questions

- User Manual: Help, Support, and Troubleshooting

Troubleshooting and FAQ · 2 min read · Reviewed 2026-05-14

Lifecycle Troubleshooting

What this helps you do

Work through common lifecycle setup, matching, dry-run, enforcement, scheduler, and permission issues.

If a policy is not applying, confirm the policy exists, is not deleted, has one active/current version, and has an active assignment within its effective dates. Then recalculate the document lifecycle state or run shadow backfill depending on the scope.

If a document did not match a rule, check assignment target, precedence, document folder/category/doc type, workflow template instance when using workflow scope, and whether the resolver trace selected a different assignment.

If the wrong version is active, open Versions and confirm the intended version is Active. Only one version can be active per policy; activating a new version supersedes the old one.

If the date source is missing, check the selected system field, document metadata key, or workflow metadata field. For workflow metadata, the document needs a matching workflow instance and stored metadata value. Invalid date values must be corrected to an ISO-style date or datetime.

If an action did not run, use dry-run first. Check lifecycle state, due date, skipped reason, unsupported action, calculation errors, missing target folder, manual enforcement enabled, confirm=true, allowed actions, and max action limits.

If scheduled enforcement is not running, check readiness blockers, scheduler enabled, scheduler dry-run setting, enforcement enabled, system service worker health, recent dry-run/manual enforcement events, and environment configuration.

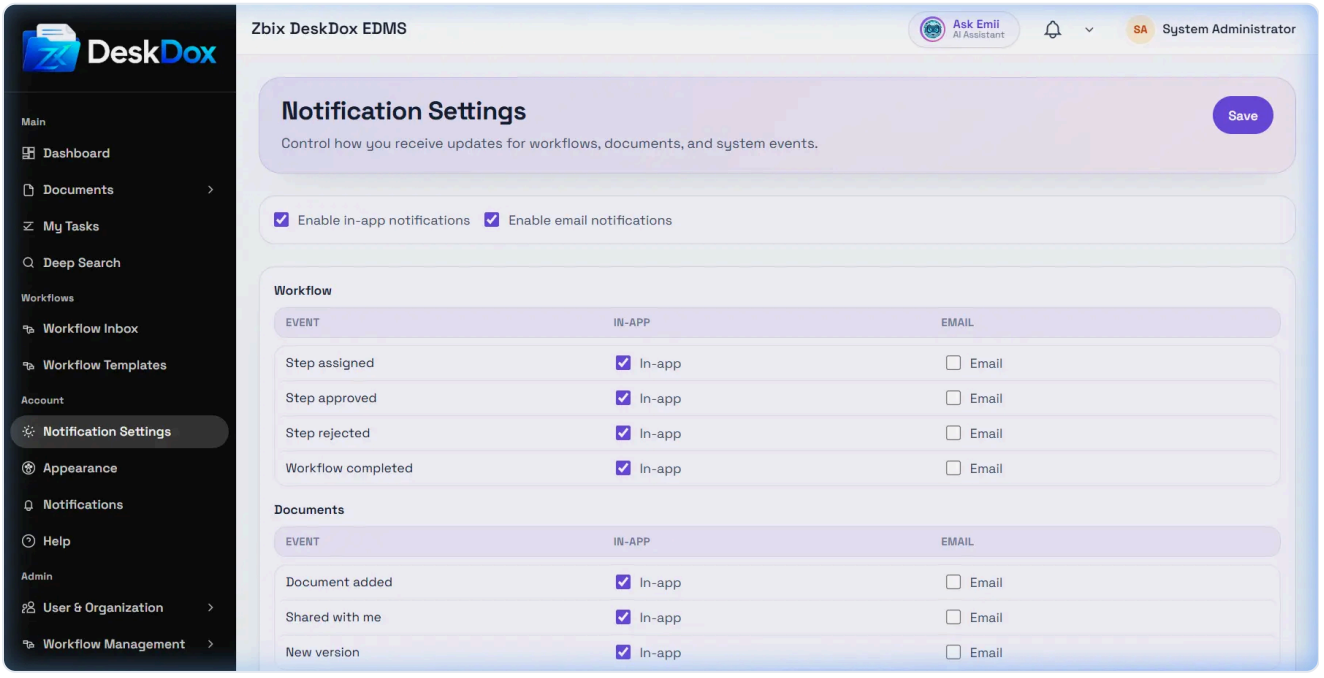
If resolver trace is confusing, read the selected scope first, then the skipped candidates. Precedence is document, workflow template, folder, category, doc type, global.

Contact an administrator or support when permissions look correct but admin pages are hidden, a policy cannot be saved, workflow metadata cannot be resolved, scheduled readiness is blocked by system service configuration, or enforcement results conflict with dry-run evidence.

Troubleshooting and FAQ · 2 min read · Reviewed 2026-05-14

Notification and SLA Troubleshooting

Use this checklist when notifications, due dates, escalations, calendars, dashboard metrics, or overdue task views do not match expectations.

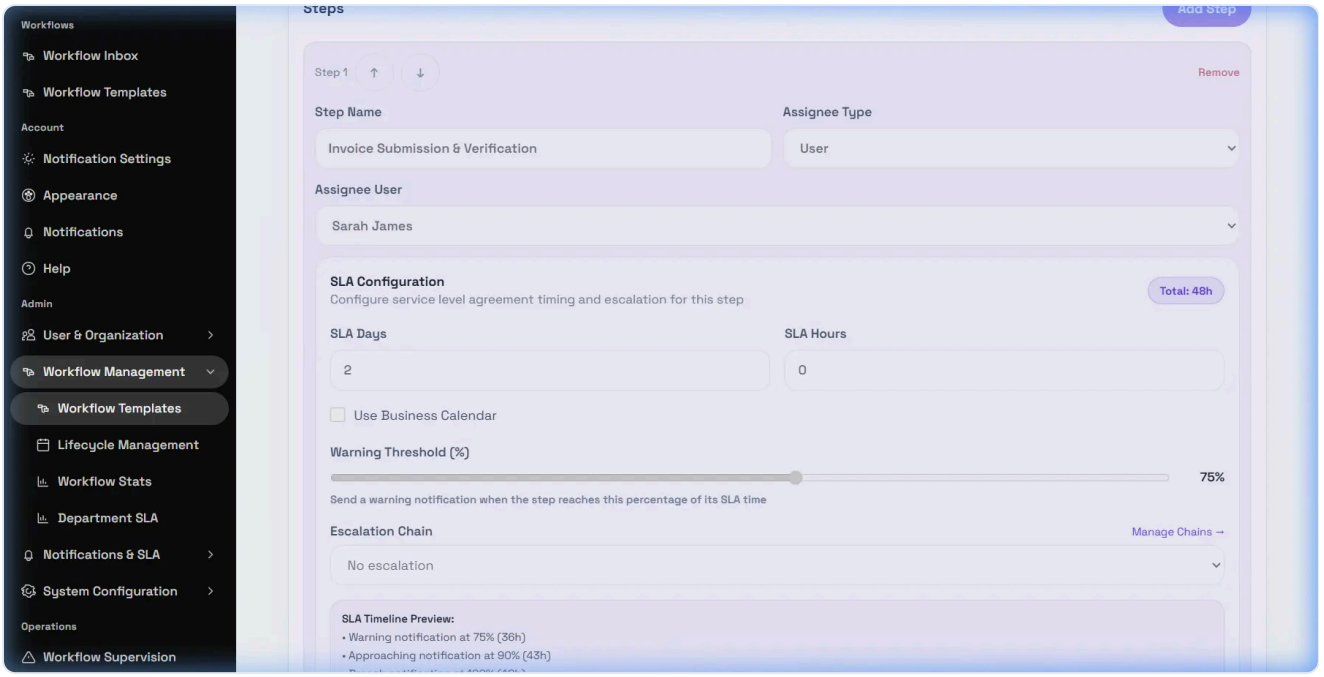


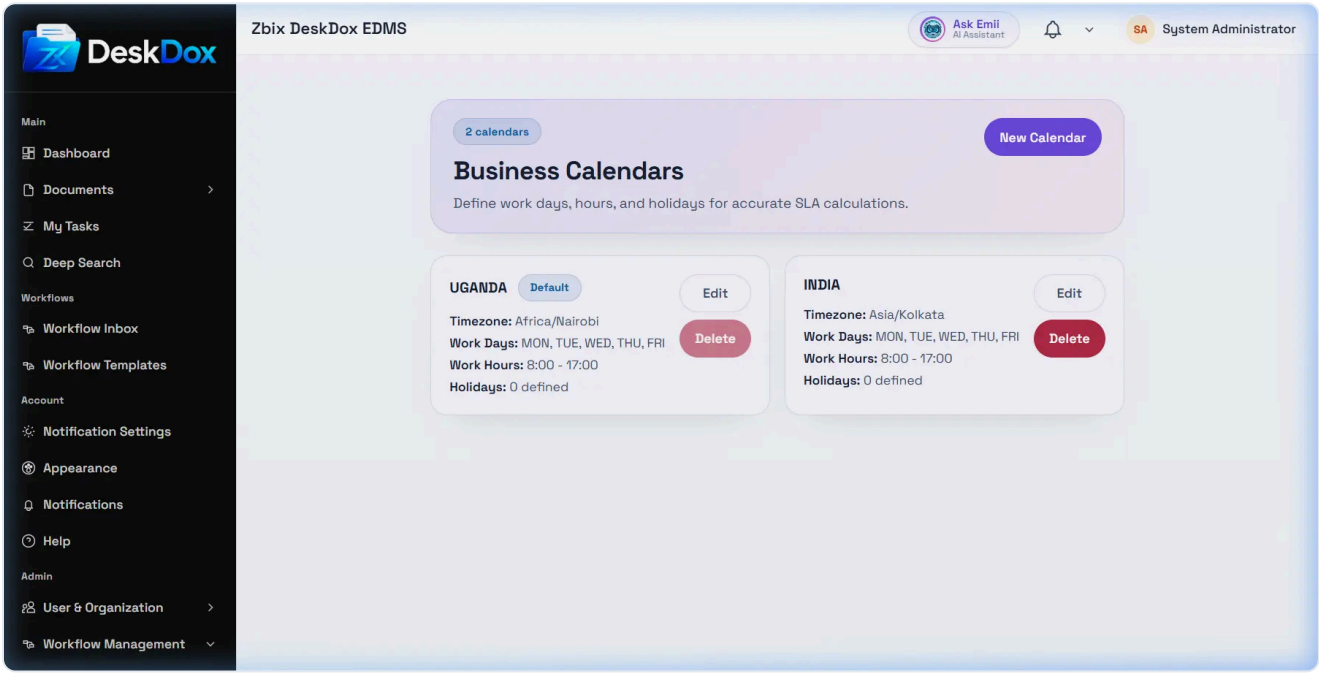
Notifications missing

Check whether the notification exists under `/app/notifications`, whether the selected filter hides it, whether your notification preferences enable the channel, and whether the event applies to your user, role, department, document, or workflow assignment. Email and mobile delivery also require service configuration.

Wrong SLA due date

Check the workflow template step's `SLA Days`, `SLA Hours`, `Use Business Calendar`, selected `Calendar`, and `Warning Threshold (%)`. If the due date counted a weekend or holiday, verify the business calendar Work Days and holiday entries.





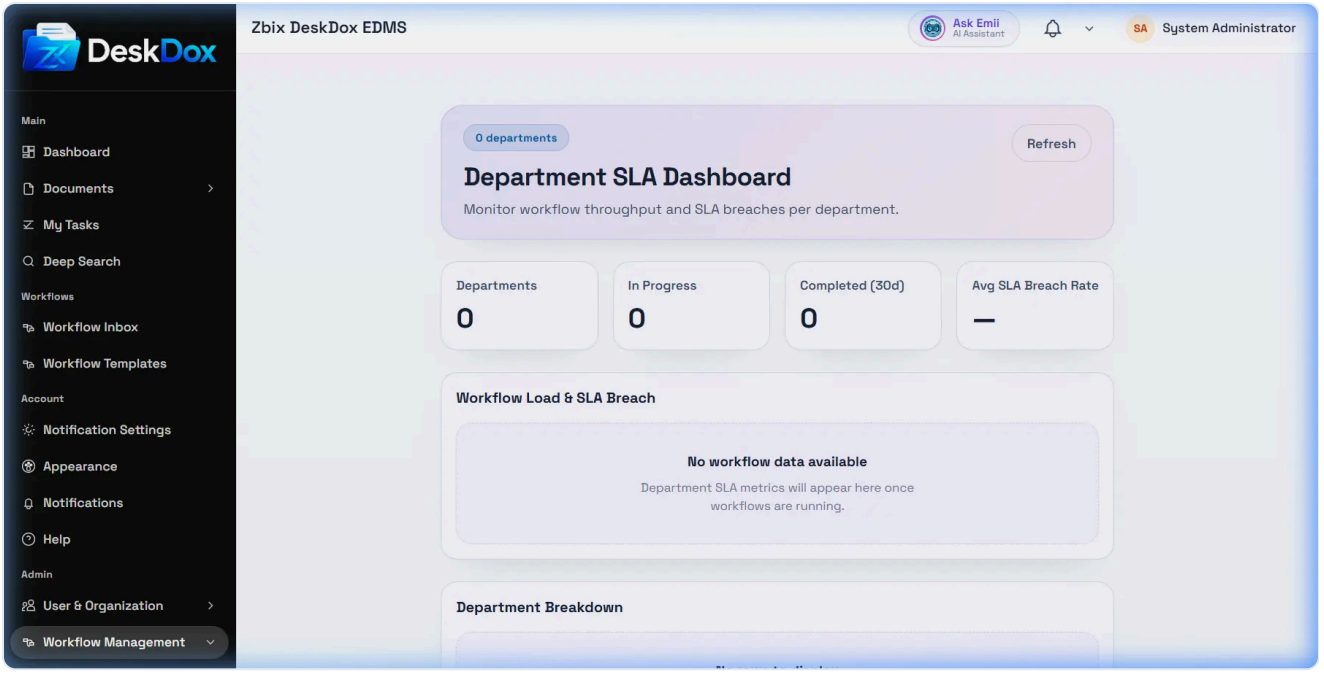
Escalation not firing

Verify that the task breached SLA, the workflow step has an escalation chain selected, the chain is active, levels exist, recipients are valid, and the selected channel is configured. Do not assume email, mobile, WhatsApp, audit events, or scheduled job behavior unless confirmed in your deployment.

Dashboard or overdue task data missing

For the department SLA dashboard, confirm workflows are running, departments are assigned, SLA data exists, and analytics have refreshed. For overdue tasks, check assignment, permissions, task status, filters,

and `Show overdue first`.



Troubleshooting and FAQ · 2 min read · Reviewed 2026-05-13

Troubleshooting Document Sharing

What this helps you do

Task guidance for diagnosing and resolving common issues with document sharing, public links, and permissions.

Common Issues and Solutions

User Cannot See a Shared Document

- **Check Access Level:** Ensure the user has been granted "Can View" or higher access.
- **Refresh Required:** Ask the user to refresh their browser or check their "Shared with Me" view.
- **Name shows as "Unknown":** The system resolves real user names. If a user name shows as "Unknown," this indicates an issue with the user account or active status. This should not happen for active users; please contact your administrator or support team.

User Still Has Access After Their Share Was Revoked

If you removed a user from the "Document Shares" section but they can still access the document, check the following:

- **Inherited Folder Access:** The user may have access to the parent folder. Folder access cannot be revoked from the document screen.
- **Workflow Access:** The user may be part of an active workflow that grants them temporary access to review or approve the document.
- **Admin Access:** The user may be a system administrator or have a global role that grants access to all documents.

Public Link Does Not Open

- **Link Disabled:** Check if the public link has been toggled off. Disabled links immediately stop working.
- **Link Expired:** Check if the public link had an expiry date that has already passed. Expired links are no longer valid.
- **Link Rotated:** If the link was rotated, the old URL will no longer work. You must provide the user with the newly generated URL.

Email Link Opens a 404 Error

If a recipient clicks a secure link from an email and receives a 404 (Not Found) error:

- **Check Public URL:** Ensure the system's public URL configuration is correct.
- **Check Web App Route:** The web app route for secure links must be properly mapped.
- **Check Email Configuration:** Confirm with an administrator that the email configuration is fully active and correct.

If you encounter persistent issues that you cannot resolve using this guide, please contact your system administrator.

Troubleshooting and FAQ · 2 min read · Reviewed 2026-05-13

Why Can't I See the Permissions Tab?

What this helps you do

Task guidance for understanding why the Permissions tab might be hidden or read-only.

Accessing Document Permissions

Document sharing and access management are capability-driven. Depending on your role and permissions, you may not see the **Permissions** tab or be able to edit access rights.

View or Download Only Users

If your access to a document is limited to "View only" or "Download", you do not have permission to manage who else can see the document. As a result, the Permissions tab is hidden from your view.

Editors

If you are an Editor for a document, you can edit the document's metadata (such as its title or tags, if allowed by policy). However, being an Editor does not automatically make you an access manager. Depending on the system policy, Editors or owners may see a limited summary of permissions, but they cannot grant or revoke access.

Administrators and Access Managers

Only system administrators and designated access managers have the full capability to view, grant, change, and revoke document access. If you need to share a document but lack the permissions to do so, please contact your administrator.

Folder Inherited Access

If you are viewing the Permissions tab and notice that some users or roles cannot be removed, it is likely because their access is inherited from the parent folder.

- Inherited access is read-only on the document screen.
- To change or revoke folder inherited access, a user with access management rights must change the permissions on the folder itself.

Troubleshooting and FAQ · 3 min read · Reviewed 2026-05-14

Workflow Task Troubleshooting

What this helps you do

Work through common workflow task, approval, signature, and permission issues before contacting an administrator.

Task not visible or My Tasks empty

Check `My Tasks`, `Workflow Inbox`, and the document `Workflow` tab when visible. Confirm you are using the right filter such as `Active`, `Completed`, or `All`.

A task may not appear because it is assigned to another user, role, or department; your account is missing workflow permissions; the workflow has not started; the task was already completed, cancelled, rejected,

or skipped; the workflow feature is disabled; or the task belongs to a document you cannot access.

Action button missing or disabled

If `Approve`, `Reject`, `Claim Task`, or `Sign Now` is missing, check whether the current step is assigned to you, your role, or your department. Also check whether the workflow is still active and the task status is `pending` or `in_progress`.

The page can show action blocking for wrong user, missing permissions, workflow not started, task already completed, and required signature. Signature-blocked tasks can show: "Signature required before you can complete this step."

Unable to approve or reject

Review the document and metadata first. If rejection is available, the page explains that `Decision Comment` text is required. If approval or rejection still fails, refresh the page and confirm the task was not completed by someone else.

Workflow stuck or status not updating

Refresh the page, check another status filter, and open the document `Workflow` tab when visible. The next workflow step may be waiting for another user, role, department, required signature, revised file, or required metadata.

Document or metadata problems

If the linked document cannot be opened from a task, check document permission, folder access, ownership, sharing, workflow involvement, and whether the document was moved, deleted, expired, or archived.

If workflow says metadata is missing, complete required document or workflow metadata when you have edit permission. If you cannot edit the field, ask an administrator or document owner to update it.

Browser and session checks

Refresh the browser, clear active filters, sign out and sign in again after permission changes, and try a clean browser session if the page appears stale. Avoid taking action from an old task tab after another user may have already completed the task.

When to contact an administrator

Contact an administrator when the task is assigned to the wrong user, department, or role; your role needs workflow permissions; a workflow was never started; the workflow template configuration looks wrong; metadata is locked; or a signature request is missing for the expected signer.

Related Emii questions

- "Why can't I see my workflow task?"
- "Why can't I approve a task?"
- "Why is the workflow action button missing?"
- "Why is my workflow stuck?"
- "Who should I contact for workflow issues?"