Zapper Edge Managed File Transfer – User Manual (2025)

Welcome to **Zapper Edge Managed File Transfer (MFT)** – an Azure-native platform for secure, high-speed data exchange, governance and AI-driven automation. This manual is designed for administrators, auditors and end-users. It explains every section of the application outlines what each feature does based, and shows practical examples so you can get the most from the platform. The guide also includes contextual notes about managed file transfer best practices and common pain-points (for instance ensuring compliance and avoiding the pitfalls of commodity file sharing services).

Contents

Introduction

Zapper Edge Managed File Transfer (MFT) is a secure, cloud-native platform built on **Microsoft Azure**. It solves common file-transfer pain-points by offering:

- **Secure exchange** – data is protected in transit and at rest using HTTPS, TLS 1.2 and Azure storage encryption.
- **Compliance ready** – the product supports GDPR, HIPAA and SOC 2 compliance with soft-delete, audit logging and retention policies.
- **High-speed uploads** – large files are uploaded in parallel chunks using Azure's Blob SDK and configurable concurrency settings.

- **Role-based governance** – access to every feature (user management, file operations, AI agents, etc.) is controlled by a flexible permission system.
- **AI integration** – configurable AI agents can classify, transform or extract information from uploaded content via REST APIs.
- **Lifecycle automation** – policies move or archive data (Hot→Cool→Archive) or automatically delete stale files.

Zapper Edge differs from commodity file-sharing tools (like Dropbox or email attachments) because it gives enterprises full control over where their data lives (in their own Azure subscription), how long data persists, and who can access it. It is particularly useful for regulated industries that need to demonstrate chain-of-custody.

> **Tip:** If you're migrating from homegrown scripts or insecure FTP servers, Zapper Edge's architecture lets you onboard partners quickly without writing new code.

Getting started

System requirements

- A modern web browser (Chrome, Firefox or Edge) with JavaScript enabled.
- An internet connection.
- A Microsoft Entra ID (Azure AD) for single sign-on.

Authentication & single sign-on

When you open the application you're greeted by the **Login** page. Authentication is handled via Microsoft Azure AD and after successful authentication the user is redirected to the landing page and a session token is stored in the browser.

> **Example:** To log in with Microsoft, click "Sign in with Microsoft". You will be redirected to the Microsoft login page. After entering your credentials and completing any multi-factor authentication, you'll be returned to `landing page`.

Role selection and context

If your account has multiple roles across multiple organizations, the top navigation bar will include a **role selector**.

User management

The **Users** page (`/users`) is for managing user accounts and their roles. Important capabilities include:

Feature	Description
View users	A table lists users with their name, email, assigned roles, organizations and status. Columns can be sorted by name, role or organization.
Add user	A modal form lets administrators invite a new user by email and assign them a role and organization.
Edit user	Clicking the edit icon opens a modal where you can modify the user's name, assign additional roles or change their organization.
Enable/disable role	The table shows a toggle switch for each role assignment. Toggling it calls `to enable` or `/disable`. This is useful for temporarily suspending a user's access without deleting them.
Delete role	A delete icon prompts for confirmation before removing a user's role assignment.

Example workflow: As an Org Admin you need to onboard a new partner. Navigate to the Users page and click **Add User**. In the modal, enter the email, select the role "File Uploader" and choose your organization. After clicking **Create**, the user will receive an email to finish registration. Later, if the user's responsibilities change, you can click the edit icon and switch them to a different role or organization.

Roles & Permissions

Zapper Edge uses **role-based access control (RBAC)** to ensure users only see features they are permitted to use. There are two related pages:

Roles page

The **Roles** page (`/roles`) lists all defined roles and the associated access levels. Administrators can create new roles or edit existing ones. this component maintains a form where you enter the role name, description and select specific permission levels (e.g., Y = full access, R = read only, N = no access) for each permission.

Example: Suppose you want a role that can only view activity logs and download files but cannot upload or delete. Create a role called **Compliance Auditor**, set File Management permissions to "download only", set Activity Logs to "view". Assign this role to the auditors; they'll see only the Activity Logs and File Management pages.

Roles & Permissions matrix

The **Roles & Permissions** matrix provides a tabbed interface for fine-tuning permissions across modules such as user management, role management, organizations, storage, files, activity logs and AI agents. Each row corresponds to a permission (e.g., "upload file",

“delete folder”) and each column represents a role. Administrators can enable or disable checkboxes to grant or revoke access.

> **Note:** Use the roles matrix when you need to grant granular capabilities (for example, allowing a user to upload files but not create folders). Remember to review permissions regularly to align with your organization’s least-privilege policy.

Organizations

Organizations represent business units, departments or external partners. On the **Organizations** page (`/organizations`), administrators can create, edit and delete organizations.

The UI shows each organization in a card with its name, description and creation date. A search box lets you quickly filter the list. Creating or editing an organization triggers toast notifications on success or error.

> **Example:** Your company acquires a new subsidiary. Navigate to Organizations, click **Add Organization**, enter the subsidiary’s name and description, and click **Create**. The new organization will now be available in the role selector and user assignments.

Storage accounts

The **Storage** page (`/storage`) manages Azure Storage accounts and SFTP enablement. Enterprises often struggle to provision secure storage for file exchange – Zapper Edge automates this process. Key features:

Feature	Description
List storage accounts	The page fetches storage accounts and displays them in a table. You can sort the list alphabetically using the sort button.
Create new account	Click **Add Storage** to open a form. You can choose to create a completely new Azure storage account (providing a unique name, location and container) or to use an existing account. This component shows step-by-step progress messages (validating, creating, configuring, finalizing) and updates a progress bar. Under the hood the server provisions the account and container and assigns the **required permission**.
Enable SFTP	After a storage account is created you may enable or disable SFTP for secure legacy integration. Selecting an account triggers a query and

Feature	Description
	displays the current status. A toggle enables or disables the SFTP endpoint.
Delete account	You can delete a storage account via the delete icon. The UI confirms the action and shows progress as the account is removed and cleaned up.

> **Example:** An Org Admin needs a storage account for the "Marketing" department. On the Storage page, click **Add Storage**, enter `marketingfiles` as the account name (lowercase letters and numbers only), choose `East US` as the location, specify a container (e.g., `campaigns`), select the Marketing organization and click **Create**. After a few minutes the progress indicator shows success, and the account appears in the list. You can now enable SFTP if required for partners using legacy clients.

File management

The **File Management** interface (`/file-management`) is the heart of Zapper Edge MFT. It allows you to upload and download files and folders, navigate directories and trigger AI processing. Major capabilities include:

Uploading files and folders

- **Drag-and-drop** upload: The interface listens for drag events; dropping files triggers the `uploadFiles` function.
- **Folder upload**: The page supports folder uploads by recursively reading directory entries and preserving folder structure.
- **Creating folders**: Pressing the folder icon opens a modal where you enter a folder name. The system calls `/api/storage/directories` to create it.
- **Deleting files/folders**: Selected items can be deleted by clicking the trash icon. The UI confirms before sending a `DELETE` request.
- **Download**: For files, clicking the download initiates download. For folders, the server uses an `archiver` library to compress the folder and returns a ZIP file.

AI agent actions

If your role has AI permissions, a drop-down appears above the file list allowing you to select an **AI agent**. After selecting files and clicking **Run**, each file is posted to the agent's API endpoint (`/api/ai-agents/{id}/run`). The UI displays a spinner next to running files and shows a toast when processing completes. This makes it easy to build workflows like OCR, document classification or virus scanning.

> **Example:** A compliance auditor needs to upload a 2 GB log file. On the File Management page, click **Upload Files** and select the file. You can then click the AI drop-down, choose your "PII Scanner" agent and run it on the file. When

processing finishes, a toast indicates whether the file contains sensitive information.

Data protection

Zapper provides **soft delete** options that protect against accidental or malicious deletions. The **Data Protection** page (`/data-protection`) lets you enable or disable soft delete for both blobs and containers. Key elements:

- **Select storage account** – choose a storage account from the dropdown. The UI uses `useQuery` to fetch accounts from `/api/storage-accounts` and populates a `<Select>` component.
- **Blob soft delete** – check the box to enable soft delete for blobs. You can set the retention period (in days). When enabled, any deleted blob can be restored within the retention window.
- **Container soft delete** – similarly, enable soft delete for containers and specify retention days.
- **Status card** – after fetching the current configuration, the card displays whether blob and container soft delete are enabled and for how many days. Icons (check or alert) indicate success or warning.
- **Save settings** – clicking **Save** posts the configuration to the server. Toast messages indicate success or error.

Example: Suppose you want to ensure deleted files are recoverable for 14 days. On the Data Protection page select your storage account, enable **Enable Blob Soft Delete** and set the days to 14. Then click **Save**. If a user deletes a file, it will be recoverable via the Azure portal or API for two weeks.

Data lifecycle management

Over time, frequently accessed data becomes cold and can be stored on cheaper tiers. The **Data Lifecycle Management** page (`/data-lifecycle`) creates rules to automatically move blobs from Hot → Cool or from Cool → Archive after a specified number of days since the blob's last modified date. The component `data-lifecycle.tsx` leverages the same design as Data Protection. Its functionality includes:

Feature	Description
Select account & container	Choose a storage account; optionally select a specific container or choose **All containers**. Containers are fetched via `/api/storage-containers?accountName={name}`.
Enable rule	A checkbox toggles the lifecycle rule on or off.

Feature	Description
Transition type	A dropdown lets you choose `HotToCool` or `CoolToArchive`. This reflects Azure's storage tiers.
Days since last modified	Enter the number of days after the file's last modification when the transition should occur. For example, 30 days.
Fetch status	When an account or container is selected, the component calls to retrieve existing rules. The status is displayed along with rule name, transition type, number of days and enabled state.
Save	Clicking **Saves** new rule. The rule name is auto-generated with a timestamp (`zappermftlmruleYYYYMMDDHHmm`).

Example: To minimize storage costs, you decide that any file not modified in the last 90 days should move from the hot tier to the cool tier. On the Data Lifecycle Management page, select your storage account, set **Hot → Cool**, enter **90 days**, enable the rule, and click **Save**. Azure will automatically transition eligible blobs to the cool tier, saving money while retaining accessibility.

AI agents

AI Agents (`/ai-agents`) allow you to integrate external AI services such as document classification, OCR or virus scanning. This module manages a list of agents and uses a permissions query to determine whether the current user can view, add, edit or delete agents. The main capabilities are:

- **View agents** – A table lists each agent's name, API endpoint and associated organization. Rows include edit and delete icons if the user has those permissions.
- **Create agent** – Administrators can add a new agent by entering a name, the API endpoint (URL), an API key (if required) and selecting an organization.
- **Edit agent** – Clicking the edit icon opens a modal pre-populated with the agent's details..
- **Delete agent** – Clicking the trash icon prompts for confirmation and deletes it.

Once defined, AI agents appear in the File Management page's drop-down for processing files. This integration means you can route files through custom ML models or external services without leaving the platform.

Example: Your compliance department uses a third-party service that detects personally identifiable information (PII) in documents. On the AI Agents page, click **Add AI Agent**, enter `PIIScanner` as the name, paste the service's endpoint URL (e.g. `https://api.example.com/v1/scan`) and the API key, and choose your organization. After saving, the agent appears in the File Management page; you can now select a file and run the PII Scanner on it.

Activity logs

The **Activity Logs** page (`/activity-logs`) provides a comprehensive audit trail of user actions. Accurate logging is vital for compliance and forensic investigations. Features include:

- **Search** – Use the search box to filter logs by user name, email, action or resource.
- **Filters** – Drop-downs allow you to filter by action (e.g., UPLOAD_FILE, DELETE_USER), category (e.g., AUTH, FILE_MANAGEMENT) and user (email address).
- **Sorting** – Click column headers to sort by action time, action name, user name, category or resource. The default sort places the most recent events at the top.
- **Pagination** – The component paginates results (20 per page). You can navigate between pages using the page controls at the bottom.
- **Icons & badges** – Each action displays an icon representing the type of activity (e.g., upload, delete, login) and a colored badge for the category. This visual aid helps identify patterns quickly.

Example: As a security officer investigating a potential breach, you can filter the logs to show only **DELETE_FILE** actions and search for the specific file name. Sorting by action time will reveal who deleted the file and when. Clicking the export button (if available) lets you download the logs for further analysis.

Examples & workflows

This section walks through typical workflows to demonstrate how the features come together.

Onboard a new department

1. **Create an organization** – Go to **Organizations** and add a new unit (e.g., `Sales`), including a description.
2. **Create a storage account** – Navigate to **Storage**, click **Add Storage**, choose a name like `salesfiles`, pick a region, specify a container and select the Sales organization.
3. **Define roles** – On **Roles**, create two roles: *Sales Manager* (granted file upload/download permissions) and *Sales Viewer* (read-only access). Use the permission matrix to fine-tune rights.
4. **Add users** – On **Users**, add the Sales team members and assign them to the appropriate role and organization.

5. **Set up retention** – On **Retention Policy**, ensure that sales documents are kept for 1 year. On **Data Lifecycle**, configure a rule to move files older than 180 days to the cool tier.

Use an AI agent for document classification

1. **Create an AI agent** – On **AI Agents**, click **Add AI Agent**, specify `DocClassifier` as the name, set the API endpoint to your classification service, provide an API key and assign it to the appropriate organization.
2. **Upload files** – On **File Management**, upload a batch of PDF invoices.
3. **Run the AI agent** – Select the uploaded invoices, choose **DocClassifier** from the drop-down and click **Run**. The UI will show each file's status (pending, running, completed). Once done, the service might return labels (e.g., invoice type) or metadata which you can use in downstream workflows.
4. **Review results** – Depending on your integration, results could be written back to the file metadata or to an external system. Use the Activity Logs to audit the AI processing.

Investigate a suspicious deletion

1. **Enable soft delete** – Ensure Data Protection is configured with blob soft delete enabled for an appropriate number of days.
2. **Filter logs** – In **Activity Logs**, search for the filename or user. Filter by the **DELETE_FILE** action to see who deleted the file and at what time.
3. **Restore data** – Because soft delete is enabled, the file can be recovered via Azure's blob restore tools or through Zapper Edge's recovery interface (if available).
4. **Adjust permissions** – If the deletion was unauthorized, modify the user's role in **Users** or adjust role permissions in **Roles & Permissions**.

Troubleshooting & FAQs

I can't upload files.

- Verify that your role includes the `uploadFile` or `uploadFolder` permission in the Roles matrix. Without this, the Upload button is disabled.
- Check that a storage account is selected in the role selector and that you have at least one container configured.
- Large uploads may fail if your network connection is unstable. Try uploading a smaller file or reduce the upload concurrency in the server configuration.

I can't see a page or menu item.

- Pages only appear if your role has the corresponding `view` permission. For example, the **AI Agents** menu item is shown if `permission` is true for your role.

- If you just changed a role, log out and back in or refresh the page to load the new permissions.

Soft delete status says "error".

- The Data Protection page displays an error if the API call fails. Ensure the storage account exists and that managed identity has the `Storage Blob Data Owner` or `Contributor` role. Check the server logs for more details.

Can I integrate with other storage providers (e.g., AWS S3)?

- The current implementation is Azure-centric. However, Zapper Edge's architecture can be extended to support other clouds. Contact the product team for roadmap details.
