Ark Admin │ Functional Specifications

Issue 2.0

This document provides a comprehensive overview of the functional features and administrative capabilities available in Ark Admin, including configuration, user and device management, service integration, and system-level settings.

Contents

1. Status

The status page allows users to monitor and troubleshoot the system.

1.1. Overview

The overview page displays key server performance metrics to provide a real-time view of system health and usage:

- **CPU**: Current processor usage, helping identify performance bottlenecks or high-load conditions.
- **RAM**: Memory utilization, indicating how much system memory is in use versus available.
- **Activity**: The number of users currently connected to the system, API calls and background jobs in queue. Useful for tracking usage patterns and potential overloads.
- **Disk Usage**: Displays storage capacity and usage trends to prevent space-related issues.
- **Health check**: To verify that the system is configured with all the needed components and file accesses.
- **Content tally**: Counts on key content entities.

1.2. Worker

The worker tab allows users to manage background processing tasks and system maintenance routines.

1. **Queue**

   The Queue tab provides visibility and control over background jobs. Users can:

   - **View job details**: Including Job ID, Priority, Time Added (UTC), Job Type, Status, Reason for Status, Last Attempt (UTC), and Next Attempt (UTC).
   - **Monitor job status**: Identify jobs that are pending, running, postponed, or failed.
   - **Take action on jobs**: Retry failed jobs, delete unnecessary ones, or investigate postponed tasks.
   - **Track job lifecycle**: Understand when a job was last attempted and when it will be retried.

- **Pause execution:** Temporarily halt the execution of all background jobs.

2. **Maintenance**

   The Maintenance tab manages recurring system tasks. Users can:

   - **View scheduled maintenance tasks**: Including descriptions and execution intervals.
   - **Track execution history**: See when each task last ran and when it is scheduled to run next.
   - **Check task outcomes**: Review the result of the last execution (e.g., Successful, Failed) to ensure system health.
   - **Edit maintenance jobs**: Set or modify the execution interval (e.g., every 1 minute, 1 hour) and enable or disable a job.
   - **Pause execution**: Temporarily halt the execution of all background jobs.

1.3. Technical Logs

The Technical logs tab provides detailed records of system-level events and actions for troubleshooting purposes. Users can:

- **View log entries**: Each row represents a system event with details such as:
  - **Level**: Severity or type of the log (e.g., info, warning).
  - **UTC Time**: Timestamp of when the event occurred.
  - **Source**: Origin of the action (e.g., self, camera).
  - **Initiator**: User or system component that triggered the action.
  - **Action/Subaction**: The main operation and its subcategory (e.g., `pub_get_accounts`, `api_call_received`).
  - **Target/In target**: The object or entity affected by the action.
- **Filter and analyze logs**: Scan for specific actions, users, or timeframes to diagnose issues or verify system behavior.
  - Filter logs by **source**, **level**, **detection type**, **target type**, and more.
  - Choose specific **initiators** or set a **target ID** for focused log analysis.

- **Export/Import logs**: Export logs for external analysis or import logs for review.

1.4. Audit logs

The Audit Logs tab provides a searchable and filterable record of user and system actions for accountability and security auditing. Users can:

- **View Audit log entry details:**
  - **Time (UTC)**: Timestamp of when the action occurred.
  - **Initiator**: The user or system component that performed the action.
  - **Action/Subaction**: The type of operation and its specific context.
  - **Target:** The object that the entry concerns

- **Filter Audit logs by:**
  - **UTC Time**: Specify a starting timestamp to retrieve logs from a particular point in time.
  - **Account:** Filter logs to show actions involving a specific user account.
  - **Task:** Filter logs to show all activity related to a specific task, including task updates, exhibits, file views, and more.
  - **Advanced filtering**
    - **Key and Value**: Filter logs based on specific key-value pairs (e.g., `account_id`).
      - Selecting filter items from the log details will also automatically apply key-value filtering.
    - **Action (and Subaction)**: Narrow down logs by selecting specific actions (e.g., `account`, `decrypt`, `delete`) and their subactions.
- **Export audit logs:**
  - Export part (filtered and/or limited by timespan) of the audit log as a CSV file.

2. Tasks

The tasks page allows users to create and manage task templates, task, and externally shared content.

2.1. Templates

The Templates tab allows to manage task templates, which define the structure and metadata for creating standardised evidence tasks in the system.

Users can:

- **View and manage existing templates**: View a list of available templates, each labeled with a name and type (e.g., "ABE Interview", "Bike theft").
- **View template-specific logs**:
  - **Technical log**: View system-level events related to the template.
  - **Audit log**: Track user actions related to the template.
- **Create new templates**: Define new task templates with specific metadata fields, file upload options, and configuration settings. When creating a template, a user can:
  - Configure **retention**, **access control**, and **task access** rules.
  - Define **dynamic title templates** using field placeholders (e.g., `[case_number] [last_name]`).
  - Add **customisable fields** such as:
    Text, Number, File, Choice, Time, Entity, Layout, and Guide. The fields can be marked as required or left optional.
  - An **export key** can be added to each field to help map exported task data fields on to an external system if required.
- **Edit templates**: Make changes to an existing template.
- **Duplicate templates**: Create a copy of an existing template.
- **Discard templates**: Remove templates from active use (with the option to show discarded templates).
- **Download templates**: Export a template for backup or use in another system.
- **Import templates**: Upload existing templates from outside the system.

2.2. Tasks

The Tasks tab allows users to create and manage individual evidence records (referred to as **tasks**) created using templates.

Users can:

- **Browse and search tasks**: View a list of existing tasks with filters for quick navigation. Each task displays key metadata such as title, creation date, and update status.
- **See who has access:** On each task a summary of who can access it is available.
- **Create a task**:
  - Start a new task using a selected template.
  - Fill in required metadata fields and upload relevant evidence files.
  - Assign access permissions and retention settings as defined by the template.
- **View and edit task details**: Select a task to view its full metadata and files.
- **Attach and manage files**: Upload and view associated files such as video or audio recordings, with playback duration and preview.
- **Mark a task as complete**: indicate that all required information and evidence have been added and the task is finalized.
- **Manage task access:** Assign, Restrict, or Mark Task as Relevant for a user or group.

2.3. Shared Content

The Shared Content tab allows users to manage file sharing sessions that have been or are pending to be published to the Ark Sharing Portal. These sessions are used to securely share selected task files with external recipients.

Users can:

- **View sharing sessions**: Browse a list of sessions, including:
  - **Active** sessions that are already published and accessible.

    - **Pending** sessions that are not yet published and can still be edited.
- **Access session details**: View metadata such as:
    - Recipient name and email
    - Access URL and code (with options to open or copy)
    - Expiration date
    - Creator and creation date
- **Manage session settings**:
    - **Edit pending sessions** to update metadata (e.g., recipient info, expiration date).
    - **View logs**: Access technical and audit logs for tracking activity.
    - **Deactivate** active sessions to revoke access.
    - **Delete** sessions when no longer needed.
- **Review included files**: See which files are part of the session. Note: files themselves cannot be updated here—they must be managed directly in Ark.

3. Retention

3.1. Pending deletion

The Pending Deletion tab lists tasks that are approaching or have reached the end of their retention period according to to their incident type.

This tab ensures that data retention times are enforced consistently, while allowing users to create exceptions and extensions as needed.

Users can:

- **View tasks pending deletion**: See a list of tasks that are:
    - **Not expired**
    - **In grace period**
    - **In extension period**
    - **Expired** and in a grace or extension period.
    - **Overdue** for deletion based on their retention policy.

- **Review task metadata**: Each entry includes:
  - Task title and ID
  - Creator and creation date
  - Expiration date, grace period end, and retention policy
  - Incident type and retention rule (indicident type).
- **Filter tasks**
  - **By incident type**: Narrow down the list based on incident types.
  - **By deletion type** automatic vs. manual
- **Take action on tasks**:
  - **Extend** the retention period for selected tasks.
  - **Change** the incident type of tasks (and thereby their retention period).
  - **Delete** tasks that are no longer needed or have exceeded their retention and grace periods.

3.2. Deleted

The Deleted tab displays a list of tasks that have been deleted after reaching the end of their retention period based on their incident type.

Use this tab to verify that tasks are being deleted in accordance with organizational or legal data retention requirements.

Users can:

- **View deleted tasks**: See a historical list of tasks that were removed from the system
- **Review deletion metadata**:
  - Expiration date
  - Deletion method: Auto or manual
  - Deletion status
  - Task title and reference information
  - Creation date

3.3. Incident Types

The Incident types tab lets users define and manage task retention policies, referred to as *incident types* in the system. Each incident type represents a specific legal or organizational scenario that governs how long tasks are retained and when they are deleted.

Users can:

- **View incident types**: Browse a list of defined incident types with columns for:
  - Code
  - Title
  - Retention period
- **Create new incident types**: Use the **New Incident Type** form to define:
  - Code
  - Title
  - Details
  - Keywords (to facilitate searching)
  - Retention period (in any time unit, from minutes to years)
  - Grace period (as above)
  - Automatic deletion toggle
- **Edit or delete existing types**: Modify or remove incident types directly from the list
- **Import incident types**: Bulk import predefined incident types (such as the MOPI offence types) in CSV format

4. Users

4.1. Accounts

1. **User lookup:**

- Search by name or username.
- Filter users by region

2. **New account:**
    - **Username and password**: Setting up a new account requires setting a username and password with two or more characters.
    - **Region**: Select the region the user belongs to (city, county, office, etc.).
    - It is possible to set up new account connected with existing person in the registry or add an entirely new person or add an account as an anonymous user.
3. **Edit account: Change** username, password, RFID, PIN-code to operate the recording devices, Azure-ID, region and personal information (name, date of birth, email, etc.).
4. **Privileges:** Set privileges for creating exhibits in any tasks, edit task templates, edit users and groups, edit devices, log audit events on behalf of others, view and configure technical details, edit user interface translations, manage other users' shares, manage task retention and manage workflows in their region.
5. **Reset password:** Send link to account holder for resetting the password (with duration of validity).
6. **Technical Log:** View technical log for the specific user.
7. **Discard:** Deactivate a user account (with the possibility to reactivate it).
8. **Active Sessions:** View all active sessions of a user account in a list view.
    - Sign out of all active sessions
9. **Devices:** View device type, time added, last seen and description of device in list view.
    - View technical logs generated on the device.
10. **Group Membership:**
    - Add group memberships
    - View existing group memberships
    - Remove group memberships

4.2. Groups

- **New group:** Create name, identifier, description, region and automatic membership for the group
- **Set privileges to the groups:** Create exhibits in any task, edit task templates, edit users and groups, edit devices, log audit events on behalf of others, edit user interface translations, manage other users share, manage task retention, manage workflows
- View group memberships in list view
- Remove membership
- View audit log and technical log
- View discarded membership groups

4.3. User Analytics

The analytics dashboard provides a comprehensive view of user engagement and administrative configurations. It is designed to support monitoring, decision-making, and system optimisation.

Key Functionalities

- **Time-Based Filtering**: View metrics across multiple timeframes
- **User Segmentation**: Analyze activity by platform, role, or account type
- **Privilege Management**: Monitor and audit user access levels
- **Engagement Tracking**: Identify trends in user activity and productivity
- **Security & Compliance**: Track inactive users and privilege distribution
- **Granted Privileges:** Displays the distribution of user privileges across the system

Productivity Metrics

Tracks the volume of data or activity generated by users:

- **Metric**: Data usage or task volume (e.g., 64.2 MB in 24h, 220.1 GB ever)

- **Purpose**: Helps assess system load and user engagement over time

5. Recorders

The Devices Overview Page provides a centralised interface for managing all devices in the system. It supports viewing, organising, updating, and maintaining fixed and portable camera devices, as well as an overview of mobile devices running the Capture app.

Device Monitoring

- **Live View Toggle**: The system supports enabling or disabling continuous live updates of device and group data.

Logging and History

- **Technical Logs Access and Audit logs for devices**:
  - Each device and group has an associated history view.
  - Logs are filtered automatically based on the selected device or group.

5.1 Fixed/Portable Configuration

5.1.1 Devices

- **Device Group Management**
  - Search and filter device groups by operational status and region. Option to include discarded groups in the view.
  - **Create New Group**
    - Define a new group with a custom name, description, group type (e.g., “Room”), identifier, and assigned region.
  - **Schedule Updates**
    - Plan and assign firmware updates based on device type.
  - **Cancel Updates**
    - Revoke scheduled updates for selected devices or groups.
  - **Settings**

        - Access and configure system-wide group-specific settings.
    - **Device Groups**
        - View and manage group metadata including type, identifier, description, and associated devices.
        - Add or remove devices from groups, access technical and audit logs, manage software update schedules, and discard groups if needed.
        - Configure detailed settings for each group or individual device:
            - **Camera and Recording Settings**
                - Set resolution for AHD 1, AHD 2, and overview cameras.
                - Enable interview-specific recording features.
                - Configure Picture-in-Picture (PiP) location and recording.
                - Define streaming resolution and mode.
                - Set playback mode and volume.
                - Enable pre-recording audio cue (Ready-to-Record tone).
            - **Security and Access**
                - Choose login method (e.g., PIN, password).
                - Select keypad type for PIN entry.
                - Enable SSH for secure remote access.
                - Allow limited-access visitor mode.
                - Permit direct metadata entry.
                - Enforce mandatory metadata for interviews.
                - Display reminders before starting interviews.
            - **Storage and Media Handling**
                - Automatically delete footage after copying to external media (USB, DVD, SD card).
                - Encrypt media copies for secure handling.
                - Finalize DVDs after copying to ensure compatibility.
                - Enforce mandatory media export after recordings.

    - Disable use of external media ports if required.
- **Network and Connectivity**
    - Enable Bluetooth and WiFi automatically on startup.
    - Configure IP address, gateway, subnet mask, and DNS settings.
    - Choose between static IP or DHCP assignment.
    - Set local domain name.
    - Configure VPN access with domain and credentials.
    - Define proxy server settings.
    - Enable SMB file sharing over TCP/IP and configure share location and credentials.
- **Audio and Alerts**
    - Set duration and volume thresholds for low audio alarms.
    - Choose sound output device.
    - Enable notifications when interviews are bookmarked.
- **System and Interface**
    - Set device language.
    - Enable automatic screen saver.
    - Configure time zone.

5.1.2 Unassigned Devices

A list of recently added or self registered devices, not yet assigned to a group (room). Here you can:

- Add new devices manually, by specifying name, description, network address, type, model, identifier, and category.
- Assign devices to one or more existing groups.

5.1.3 Software Uploads

Here you can view a list of device firmware update packages available on the server. These will be available for scheduled device updates as mentioned earlier.

5.2. Capture

The purpose of this section is to monitor users running the Capture app on their mobile phones.

- Search for devices by phone model or name/username of the user.
- View device overview including:
  - Device type
  - Date added
  - Last seen timestamp
  - Description
  - Technical log
  - Audit log
  - QR code recovery options
- Display expired devices (offline for an extended time).

6. Settings

6.1. Client

1. Admin
   - Show
     - **Media:** Controls whether the media files are visible in Admin (to completely hide all photos, videos and audio recordings in the Admin tool).

2. Ark (Frontend)

   These settings configure user experience parameters for the Ark (Frontend) playback controls. They define default behavior for audio/video interaction, enabling more efficient media review and transcription workflows.

a. Playback

Set the playback globally.

2.1.1 Skip Backward Interval (seconds)

Defines the number of seconds the player jumps backward when the skip-back control is used.

- **Default**: 5 seconds
- **Range**: 1–3600 seconds

2.1.2 Skip Forward Interval (seconds)

Defines the number of seconds the player jumps forward when the skip-forward control is used.

- **Default**: 30 seconds
- **Range**: 1–3600 seconds

2.1.3 Slow Playback (%)

Determines the playback speed when users select "slow playback." Useful for detailed review or transcription.

- **Default**: 66% speed
- **Range**: 25–99%

2.1.4 Fast Playback (%)

Determines the playback speed when users select "fast playback," enabling quicker review of content.

- **Default**: 133% speed
- **Range**: 101–400%

b. Modules

The
Modules section in Ark Admin allows administrators to configure the availability and functionality of various features within the Ark platform. These settings control user access to specific tools and modules, enabling customized workflows based on operational needs.

- **Allow Task Creation**

  Enables users to create new tasks within the system. When enabled, users can define and initiate tasks related to transcription, media management, or other operational processes.

- **Allow Task Editing**

  Allows users to modify existing tasks. Useful for updating metadata, correcting details, or reassigning tasks.

- **Show Media Redaction Modul**

  Displays the media redaction interface, which allows users to redact sensitive audio/video content directly from the platform.

- **Allow Foot Pedal Control**

  Enables support for foot pedal devices, commonly used to control media playback hands-free—ideal for transcription workflows.

- **Show Room Recording Module**

  Makes the room recording functionality visible in the interface. This module is used to manage and monitor room-based recording setups.

- **Show Rooms Module**

  Displays the Rooms module, which provides access to physical or virtual room configurations and availability.

- **Show Share Module**

  Shows the sharing functionality within the platform, allowing users to share tasks, files, or transcripts with others via secure links or permissions.

- **Show Transcript Module**

  Reveals the transcript interface, enabling users to view, edit, and export transcriptions of audio/video content.

3. Capture

   The **App Settings** section in Ark Admin allows administrators to configure how the Ark mobile or desktop application behaves for end users. These settings influence performance, user interface, data usage, and media handling, enabling tailored experiences based on organizational policies and user needs.

   1. **Allow GPS-address Lookup**

      Enables the app to look ut its GPS position in Apple's/Google's API to retrieve and display address information for captured media or tasks.

2. **Auto Lock App**

   Automatically locks the app when not in use, requiring biometry/PIN-code to unlock it.

3. **Use Cellular Data for Uploads**

   Allows the app to use mobile data for uploading media files. Disable this to only upload via WiFi.

4. **Free Storage Required for Capture (MB)**

   Specifies the minimum amount of remaining free storage (in megabytes) required on the device to allow media capture.

   - **Range**: 0–9999 MB
   - **Default**: 70 MB

5. **Time to Keep Media Files on Device**

   Determines how long after upload to the server the media files are retained on the device before being automatically deleted.

   - **Range**: 0–99999 minutes
   - **Default**: 24 minutes

6. **Fast Playback (%)**

   Sets the speed for fast playback of media files, useful for reviewing content quickly.

   - **Range**: 101–400%
   - **Default**: 140%

7. **Skip Backward Interval (seconds)**

   Defines the time interval for skipping backward during media playback.

   - **Range**: 1–3600 seconds
   - **Default**: 5 seconds

8. **Skip Forward Interval (seconds)**

   Defines the time interval for skipping forward during media playback.

   - **Range**: 1–3600 seconds
   - **Default**: 30 seconds

9. **Slow Playback (%)**

   Sets the speed for slow playback of media files, useful for detailed review or transcription.

   - **Range**: 25–99%
   - **Default**: 60%

10. **Show Auto Lock Setting**

    Displays the auto lock configuration option in the app as a settings, allowing users to individually decide whether to enable this feature.

11. **Show Cellular Upload Setting**

    Displays the option to enable or disable cellular uploads in the app settings, allowing users to individually decide whether to enable this feature.

12. **Header on App Home Screen**

    Allows customisation of the header graphic displayed on the app's home screen.

13. **Organization Logo**

    The organization's logo used in the app interface, typically on the home screen or login page.

14. **Show Tab for Incomplete Tasks**

    Whether to show the tab for viewing a list of tasks that are not yet completed. If users should always create new tasks when capturing evidence, disabling this will simplify the user interface.

15. **App Opens on Template List**

    Whether the app should always open on the task template list. Useful if the users should mostly be creating new recordings from templates on the spot.

16. **Show Tab for Task Templates**

    Whether to show the tab with the list of available task templates. If users should never create new tasks, but only complete existing ones, this should be disabled.

17. **Recommend Update to Version**

Suggests that users update their app to a specific version. If the user is running an older version of the app, an update reminder will display when the user exits the app.

- **Value**: Version number (e.g., 23.2.1)
- **Note**: This is a recommendation, not a forced update.

4. **Color**

The **Color Settings** section in Ark Admin allows administrators to define the visual theme of the Ark application by specifying color values for various UI elements. Colors are defined using the **Hex AARRGGBB** format, where:

- **AA** = Alpha (transparency)
- **RR** = Red
- **GG** = Green
- **BB** = Blue

Default colours:

- **Disabled Buttons**

  Defines the background color of buttons when they are disabled or inactive.

  - **Value:** `FF999999` (Gray)

- **Enabled Buttons**

  Sets the background color for active or clickable buttons.

  - **Value:** `FF51A171` (Greenish)

- **Text/Icons in Buttons**

  Specifies the color of text and icons displayed within buttons.

  - **Value:** `FFFFFFFF` (White)

- **Background**

  Sets the primary background color of the application interface.

  - **Value:** `FF2B2B2B` (Dark Gray)

- **Card Background**

Defines the background color for cards or panels used throughout the UI.

  - **Value:** `FF353535` (Medium Dark Gray)
- **Text on Cards**

  Specifies the color of text displayed on cards.

  - **Value:** `FFFFFFFF` (White)
- **Form Field Background**

  Sets the background color for input fields and form elements.

  - **Value:** `FF2B2B2B` (Dark Gray)
- **Form Field Captions**

  Defines the color of labels or captions associated with form fields.

  - **Value:** `FFC2C2C2` (Light Gray)
- **Form Field Descriptions**

  Specifies the color of helper text or descriptions under form fields.

  - **Value:** `90FFFFFF` (Semi-transparent White)
- **Form Field Text**

  Sets the color of user-entered text in form fields.

  - **Value:** `FFFFFFFF` (White)
- **Form Background**

  Defines the background color for form containers.

  - **Value:** `FF2B2B2B` (Dark Gray)
- **Green**

  A general-purpose green color used for success indicators or highlights.

  - **Value:** `FF00CB8D` (Bright Green)
- **Text on Background**

  Specifies the color of text displayed on the main background.

  - **Value:** `E8FFFFFF` (Slightly Transparent White)

- **Red**

  A general-purpose red color used for errors or warnings.

  - **Value:** `FFF14B42` (Bright Red)

- **Yellow**

  A general-purpose yellow color used for alerts or highlights.

  - **Value:** `FFFFCB6B` (Warm Yellow)

5. **Davidhorn Device Metadata**

   The Device Metadata section in Ark Admin allows administrators to define and configure metadata fields that appear in the app interface. These fields are used for data entry, display, and export purposes. Each field includes settings for visibility, formatting, and export mapping, enabling structured and validated data collection.

Field Configuration Parameters (applies to each field):

- **Displayed Text**: The label shown to users in the app (max 30 characters).
- **Export Key**: The internal identifier used for exporting data (3–32 characters).
- **Format**: A regular expression pattern used to validate input (max 100 characters).
- **Help Text**: Optional guidance shown to users (max 30 characters).
- **Visible**: Determines whether the field is shown in the app.
- **Sequence**: The order in which the field appears (0–4).
- **Type**: The type of field (e.g., Displayed text).

Configured Fields:

1. **Occurrence Number**

   - **Export Key:** `CrimeId`
   - **Format:** `^[0-9a-zA-Z-_]{3,16}$`

- **Help Text**: `3-16 alphanumeric`
- **Visible**: Yes
- **Sequence**: 0
- **Type**: Displayed text

2. **Custody Number**
    - **Export Key**: `Custody_Number`
    - **Format**: `^[0-9a-zA-Z-_]{3,16}$`
    - **Help Text**: *(None specified)*
    - **Visible**: Yes
    - **Sequence**: 1
    - **Type**: Displayed text
3. **Interviewee Reference No.**
    - **Export Key**: `RecordingId`
    - **Format**: `^[0-9a-zA-Z-_]{3,16}$`
    - **Help Text**: *(None specified)*
    - **Visible**: Yes
    - **Sequence**: 3
    - **Type**: Displayed text
4. **Interviewee Name**
    - **Export Key**: `Interviewee`
    - **Format**: `^[0-9a-zA-Z-_]{3,16}$`
    - **Help Text**: `name`
    - **Visible**: Yes
    - **Sequence**: 2
    - **Type**: Displayed text
5. **Date of Birth**
    - **Export Key**: `IntervieweeBirthDate`

        - **Format**: `^([0-2]?[1-9]|[1-3][01])/(0?[1-9]|1[0-2])/\d{4}$`
        - **Help Text**: *(None specified)*
        - **Visible**: Yes
        - **Sequence**: 4
        - **Type**: Displayed text
    6. **Task ID**
        - **Export Key**: `Task_Id`
        - **Format**: `^[0-9a-zA-Z-]{36}$`
        - **Help Text**: *(None specified)*
        - **Visible**: Yes
        - **Sequence**: 0
        - **Type**: Displayed text
6. Organisation
7. Redaction Disclaimer
8. Share

6.2. Server

The server configuration page allows administrators to define core operational parameters for the server environment, including authentication, file handling, logging, and system behavior. These settings ensure secure access, consistent file naming, efficient resource usage, and appropriate logging levels for support and development.

Authentication and Session Management

- **Local Authentication**: Enables or disables user authentication directly on the server without relying on external identity providers.
- **Session Lifetime (minutes)**: Defines how long a user session remains active before automatic logout. Accepts values from 1 to 999,999 minutes.

Time and Regional Settings

- **Default Content Time Zone**: This is the default time zone for content created without a specified time zone (including content created before time zones were introduced). It applies whenever the client does not provide a time zone.

Storage and File Management

- **Upload Folder Space Usage (GB)**: Limits the maximum disk space allocated for uploaded files. Range: 0 to 999,999,999 GB.
- **Filename Template for Files from Fixed/Portable Recorder**: Defines structured naming for files from recording devices using metadata such as `{device_id}`, `{start_date}`, `{device_source}`, and part numbers.
- **Filename Template for Files from the Capture App**: Sets naming conventions for files captured via the app, incorporating task title, device name, time range, and versioning.
- **Filename Template for Files from Other Sources**: Customizes how filenames are generated for externally sourced files using placeholders like `{task_title}`, `{file_name}`, `{friendly_id}`, `{version}`, and `{extension}`.

Logging and Support Levels

- **Support Level Lifetime (days)**: How long support-level technical logs are retained. Range: 1 to 365 days.
- **Developer Level Lifetime (days)**: How long developer-level technical logs are retained. Range: 1 to 90 days.
- **Debug Level Lifetime (days)**: How long debug-level technical logs are retained. Range: 1 to 14 days.
- **Verbose Logging**: Enables detailed logging for troubleshooting and diagnostics.

Password Policy

- **Minimum Number of Characters**: Sets the minimum password length. Range: 1 to 99 characters.

- **Require a Mix of Upper and Lower Case**: Enforces use of both uppercase and lowercase letters in passwords.
- **Require at Least One Number**: Ensures passwords include numeric characters.
- **Require at Least One Special Character**: Enforces inclusion of symbols (e.g., !, @, #) for stronger passwords.

Report

- **Report Language**: Sets the default language for system-generated reports.

Share - Integration and API Access

- **Share Server API Key**: Provides a secure token for accessing the Share server's API.
- **Share Server URL**: Specifies the endpoint to reach the Share server API.

Worker - Performance and Processing

- **Number of Workers**: Defines how many concurrent worker threads or processes the server can use for executing background tasks (queue and maintenance). Range: 1 to 7.

6.3. Lists

The list page allows managing **custom lists (categories)** and their **translations** across all supported languages. These lists are commonly used as dynamic data sources for fields such as dropdown or choice fields in tasks and templates. It ensures that all list-based data used in the application is centrally managed, consistently translated, and easily maintained. It supports multilingual environments and improves the reusability and clarity of choice-based fields across the platform.

Define reusable option sets for task fields of type *choice* (e.g., a list of nationalities).

Manage task types or other categorical data used in templates and workflows.

Category Management

- **New Category**
  - Opens a popup to create a new list (category).
  - Requires a category name and at least one key.
  - Category names must consist of lowercase letters (a–z) only.
- **Edit Category**
  - Allows renaming an existing category.
  - Enforces the same character restrictions as above.
- **Category Structure**
  - Each category contains one or more **keys**.
  - Keys represent individual list items and support translations.

Key Management

- **New Key**
  - Adds a new item (key) to the selected category.
  - A key is automatically generated for each available language.
- **Edit Key**
  - Allows renaming the key.
  - Key names must also consist of lowercase letters (a–z) only.
- **Discard Key**
  - Deletes the key and all its associated translations.
- **Translation Status**
  - Each key displays a list of language codes.
  - Language codes appear in red if a translation is missing for that key.

Language Management

- **Add Language**
  - Opens a popup to select and add new languages to the system.
- **Discard Language**
  - Opens a popup to select and remove existing languages from the system.

6.4. Services

The services page provides an overview and management interface for configuring **external services** used by the system. Each service entry defines both the **connection details** and the **conditions under which the service should be used**.

Core Functions

- **New Service**
  - Opens a form to create a new service entry.
  - The *name* field is mandatory.
  - Additional configuration fields may include endpoint URLs, authentication tokens, and usage rules.
- **Show Discarded / Hide Discarded**
  - Toggles the visibility of services that have been discarded (soft-deleted).
  - Useful for reviewing or restoring previously removed services.

Service List Elements

Each service in the list includes visual indicators and action buttons:

- **Priority Icons**
  - Hovering over icons reveals the priority level of the service:

        - Maximum Priority
        - High Priority
        - No Priority
        - Low Priority
        - Minimum Priority
- **Edit**
    - Opens the service configuration for editing.
    - Allows updating service details such as name, priority, and connection settings.
- **History**
    - Opens the Technical Logs filtered by the selected service's ID.
    - Useful for auditing service usage and troubleshooting issues.
- **Discard / Restore**
    - Discards the service from active use.
    - A *Restore* button becomes available for discarded services, allowing reactivation.

Services provided

Status	Service Name
✓	Azure Blob
✓	Azure Email
✓	File conversion
✓	Decryption
✓	Indico Recorder integration
✓	NEC Connect integration
✓	Nice integration
✓	NICHE integration
✓	OIDC authentication
✓	Media redaction

Status	Service Name
✓	Report generator
✓	SMTP Email
✓	XML Export

6.5. Regions

The regions page enables the definition and management of **regions** within the system, establishing a hierarchical structure of **locations** that governs how **users, user groups, and devices** are organised and accessed across the ecosystem.

By configuring regions, administrators can:

- Create a structured geographic or organisational hierarchy (e.g., Country > State > City > Facility).
- Assign users, devices, and groups to specific regions to control visibility, access, and operational scope.
- Support region-based filtering, reporting, and policy enforcement across the platform.

This structure ensures consistent governance, simplifies large-scale deployments, and enhances control over distributed environments.

6.6. Translations

The translations page enables administrators and users with privilege “Edit user interface translations” to configure language support for **custom, undefined, or non-standard languages** within the system. It is designed to extend the platform’s multilingual capabilities beyond predefined language sets, allowing for tailored localisation and translation workflows.