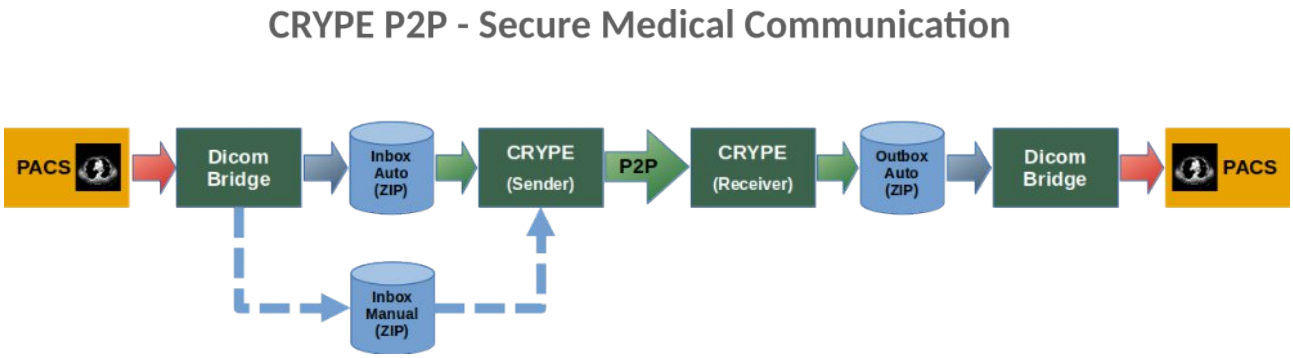
CRYPE DicomBridge User Manual

Overview

CRYPE DicomBridge is a software solution that integrates with the CRYPE app (www.crype.eu) to facilitate the secure transfer of medical imaging and report data via DICOM communication from and to Healthcare Professionals or even Patients. It receives DICOM data from any PACS (Picture Archiving and Communication System), creates ZIP files per patient and study, and stores them in designated directories.

The CRYPE app monitors these directories to process and forward the ZIP files based on embedded CRYPE ID(s) as receivers.

The software also supports sending DICOM data to a third-party PACS which is received by CRYPE and stored in a designated folder.



This manual is intended for IT administrators to install, configure, and manage **CRYPE DicomBridge** effectively.

1. System Requirements

To ensure proper operation of CRYPE DicomBridge, the following system requirements must be met:

- **Operating System**: Windows 10 or later (64-bit).
- **CPU**: x64 architecture (64-bit processor).
- **Storage**: Sufficient disk space for storing ZIP files, logs, and temporary data (minimum 100 GB recommended).
- **Network**: Stable and performing internet connection for CRYPE communication and local connection with PACS systems.
- **Permissions**: Administrator rights for installation and service setup.

2. Functionalities

CRYPE DicomBridge provides the following core functionalities:

2.1 DICOM Receiving

- **Process**: Receives medical images and report data via DICOM from a third party PACS.
  Note: For automatic forwarding by CRYPE, all received files should contain one or more CRYPE IDs in an available DICOM tag. For implementation details, please contact your PACS and RIS vendor.
- **ZIP Creation**: Groups received data by patient and study, creating a ZIP file per study.
- **Directory Sorting**:
  - If **one or multiple** CRYPE IDs (with prefix `CRID#`) are found in the configured DICOM tag, the ZIP file is stored in `Inbox_Auto` for automatic forwarding by the CRYPE app. The file name of ZIP file will include the receiver CRYPE ID(s).
  - If no CRYPE ID is present in the DICOM images, the ZIP file is stored in `Inbox_Manual` for manual forwarding via drag-and-drop in the CRYPE app.
  - If receiving or zipping of the DICOM data fails, the folder containing the received files is moved to `Inbox_Failed`.

- **CRYPE ID Handling**:
  - CRYPE IDs must be stored in every image in the configured DICOM tag with the prefix `CRID#` (e.g., `CRID#1234567890123456`).
    Note: You can use any DICOM text tag with sufficient space to store up to five CRYPE IDs (receivers). This DICOM tag is used solely to temporarily identify the CRYPE receivers. The **CRYPE IDs are automatically removed by the DicomBridge software and are not transmitted to the receiver,** ensuring that the existing DICOM content remains unchanged and intact.
  - Multiple CRYPE IDs can be concatenated (e.g., `CRID#1234567890123456CRID#9876543210987654`).
  - IDs must be at the end of the DICOM element's content.
  - After extraction, CRYPE ID(s) are removed from the DICOM data and appended to the ZIP filename (e.g., `PatientName_19900101_M_20230315_MR_StudyUID_CRID#1234567890123456.zip`).

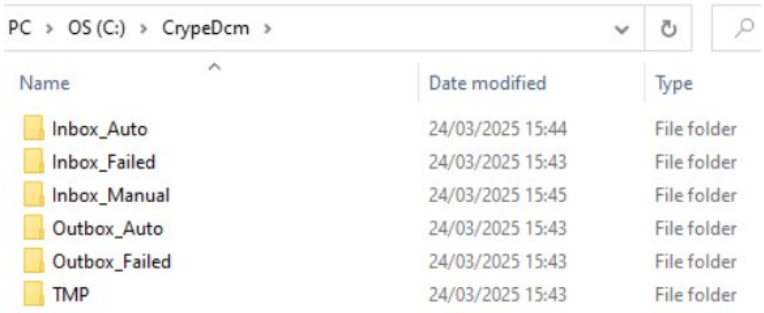
2.2 DICOM Sending

- **Process**: Monitors the `Outbox_Auto` directory for ZIP files containing DICOM data received from the CRYPE app.
- **Sending**: Extracts the received ZIP files and sends the DICOM data to a configured third-party PACS.
- **Error Handling**: If the transfer fails, the ZIP file is moved to `Outbox_Failed.`

2.3 Directory Structure

The software uses the following directories:

- **Inbox_Auto**: Stores ZIP files with CRYPE IDs for automatic forwarding.
- **Inbox_Manual**: Stores ZIP files without CRYPE IDs for manual forwarding.
- **Inbox_Failed**: Stores folders containing DICOM data, where receiving or zipping failed.
- **Outbox_Auto**: Stores ZIP files received from CRYPE for automatic sending to a PACS.
- **Outbox_Failed**: Stores ZIP files that failed to send to the third-party PACS.



2.4 Failed Data Management

- Both `Inbox_Failed` and `Outbox_Failed` directories are monitored by **CRYPE DicomBridge.**
- Files older than the configured retention period (set in "Keep failed (days)") are automatically deleted to prevent accumulation.

2.5 Logging

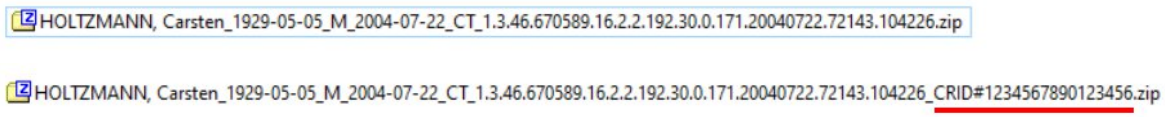
- All transactions (receiving, sending, errors) are logged in a logbook.
- The GUI displays the last 500 actions in the "Log Book" tab.

2.6 Windows Service

- The software can run as a background Windows service for continuous operation.
- Alternatively, it can run in the foreground with a GUI for configuration and monitoring.

2.7 File Naming Convention

- ZIP files received via DicomBridge are named as: `PatientName_PatientBirthDate_PatientGender_StudyDate_Modality_StudyUID.zip`
- If CRYPE ID(s) is/are present, they are appended before the file name extension in the format: `PatientName_PatientBirthDate_PatientGender_StudyDate_Modality_StudyUID_CRID#1234567890123456.zip`



3. Installation and Service Setup

3.1 Installation

1. **Download**: Obtain the `DicomBridge.zip` file from the official CRYPE website or provided distribution.
2. **Extract**: Extract the Zip file to a dedicated directory (e.g., `C:\Program Files\DicomBridge\`).
3. **Verify Requirements**: Ensure the system meets the requirements (Windows 10+, x64 CPU).

3.2 Running CRYPE DicomBridge

CRYPE DicomBridge can be run in two modes: as a Windows service (recommended for production) or in the foreground with a GUI (useful for initial setup and testing). Below are the steps for both approaches.

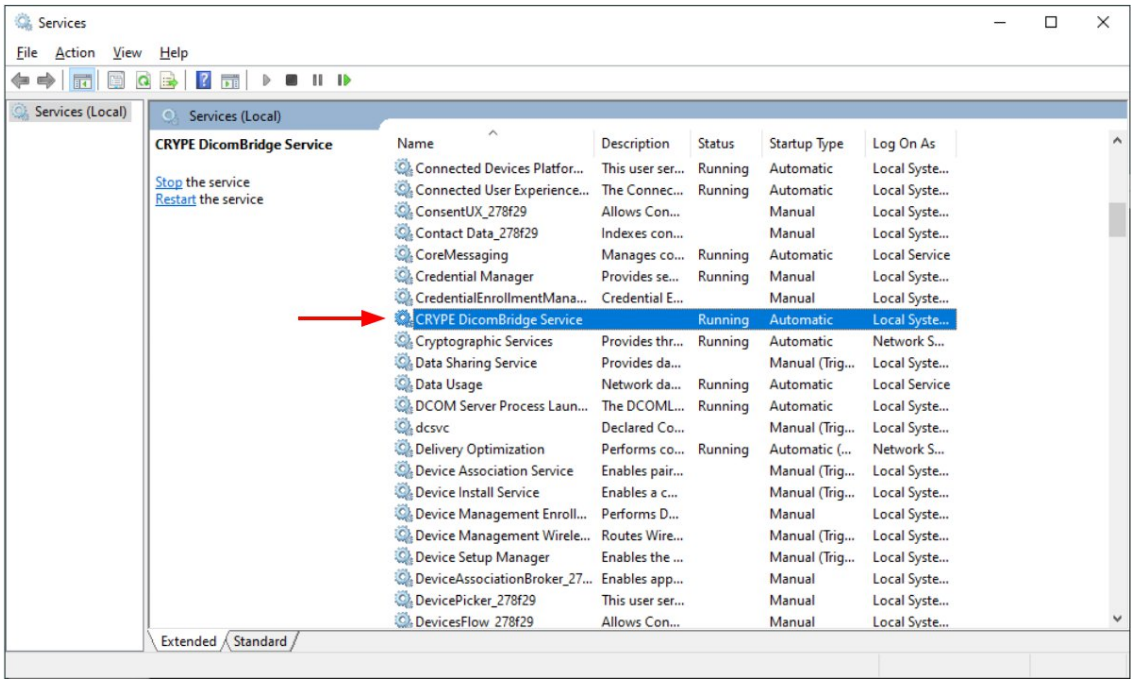
3.2.1 Installing as a Windows Service

Running **CRYPE DicomBridge** as a Windows service ensures it operates continuously in the background, even after a system reboot.

Steps to Install as a Service:

1. **Open Command Prompt with Administrator Rights**:
   - Press `Win + S`, type `cmd`, right-click on "Command Prompt," and select "Run as administrator."
2. **Navigate to the DicomBridge Directory**:
   - Use the cd command to switch to the directory containing DicomBridge.exe. For example:
   - `cd C:\Program Files\DicomBridge`

3. **Install the Service**:
   - Run the following command:
   - `DicomBridge.exe -i`
   - This installs **CRYPE DicomBridge** as a Windows service named "CRYPE DicomBridge Service."
4. **Verify Installation**:
   - Open the Services management console:
   - Press `Win + R`, type `services.msc`, and press Enter.
   - Look for "CRYPE DicomBridge Service" in the list.
   - Ensure the service is set to "Automatic" startup type and is running.



3.2.2 Uninstalling the Windows Service

If you need to remove the service (e.g., for troubleshooting or reconfiguration):

1. **Open Command Prompt with Administrator Rights**:
   - Follow the same steps as above to open an elevated Command Prompt.
2. **Navigate to the DicomBridge Directory**:
   - Example:
   - `cd C:\Program Files\DicomBridge`
3. **Uninstall the Service**:
   - Run the following command:
   - `DicomBridge.exe -u`

4. **Verify Removal**:
   - Reopen `services.msc` and confirm that "CRYPE DicomBridge Service" is no longer listed.

3.2.3 Running in Foreground (GUI Mode)

For initial setup and for watching logs, you can run **CRYPE DicomBridge** in the foreground with its graphical user interface (GUI).

Steps to Run in Foreground:

1. **Navigate to the DicomBridge Directory**:
   - Open a Command Prompt or File Explorer and go to the directory containing DicomBridge.exe.
2. **Launch with GUI**:
   - Run the following command:
   - `DicomBridge.exe`
   - Alternatively, double-click DicomBridge.exe without parameters to launch the GUI directly.
3. **GUI Overview**:
   - The GUI opens with two tabs: "Log Book" (showing the last 500 actions) and "Settings" (for configuration).

3.2.4 Running as Test (Service Mode)

For testing, configuration, or manual operation, you can run **CRYPE DicomBridge** in service mode without installing as service.

Steps to Run in Service Mode:

1. **Navigate to the DicomBridge Directory**:
   - Open a Command Prompt and go to the directory containing DicomBridge.exe.
2. **Launch in Service Mode**:
   - Run the following command:
   - `DicomBridge.exe -s`
3. **Service Mode**:
   - DicomBridge runs in service mode in background. It can be stopped using the Task Manager.

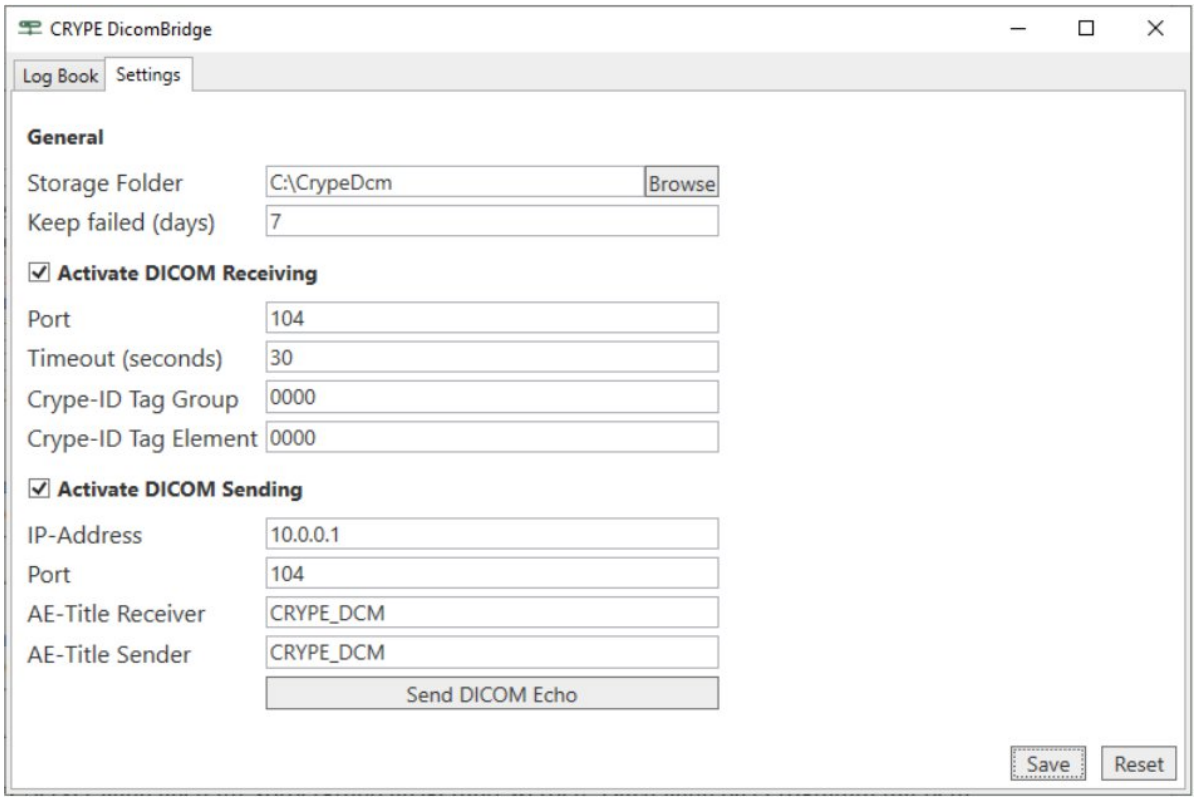
Note: Running in service mode is not recommended for production environments, as it does not auto-start after a reboot.

4. Configuration

CRYPE DicomBridge is configured via its GUI, accessible by launching the application in foreground mode. The "Settings" tab allows you to customize directories, DICOM communication parameters, and error handling.

4.1 Accessing the Settings

1. **Launch the GUI**:
   - Double-click DicomBridge.exe.
2. **Navigate to the Settings Tab**:
   - In the GUI, click the "Settings" tab to view the configuration options.



4.2 Configuration Options

The settings are divided into three sections: General, DICOM Receiving, and DICOM Sending. Below is a detailed explanation of each option:

4.2.1 General Settings

- **Storage Folder**:
  - **Description**: Specifies the root directory where all data (inbox, outbox, logs) is stored.
  - **Default**: C:\CrypeDcm
  - **Action**: Click "Browse" to select a different directory. Ensure the path has sufficient disk space and write permissions.

- **Keep failed (days)**:
  - **Description**: Number of days to retain files in Inbox_Failed and Outbox_Failed before automatic deletion.
  - **Default**: 7 days
  - **Range**: 1–365 days
  - **Purpose**: Prevents accumulation of failed files, keeping the system clean.

4.2.2 DICOM Receiving Settings

- **Activate DICOM Receiving**:
  - **Description**: Enables/disables the receiving of DICOM data from a PACS.
  - **Default**: Enabled (checked)

- **Port**:
  - **Description**: The port on which the DicomBridge listens for incoming DICOM data.
  - **Default**: 104
  - **Range**: 1–65535
  - **Note**: Ensure this port is open in the firewall and not in use by other applications.

- **Timeout (seconds)**:
  - **Description**: Time to wait (in seconds) for additional DICOM data before zipping a study.
  - **Default**: 30 seconds
  - **Range**: 1–3600 seconds
  - **Purpose**: Ensures studies are not split unnecessarily due to network delays.

- **Crype-ID Tag Group**:
  - **Description**: Hexadecimal group number of the DICOM tag containing the CRYPE ID.
  - **Default**: 0000
  - **Format**: Four hexadecimal digits (e.g., 0010)

- **Crype-ID Tag Element**:
  - **Description**: Hexadecimal element number of the DICOM tag containing the CRYPE ID.
  - **Default**: 0000
  - **Format**: Four hexadecimal digits (e.g., 0020)
    In general you can use existing DICOM tags with content or you can use DICOM tags which are normally not used:
    (0010,2201) Patient Species Description
    (0010,2292) Patient Breed Description
    (0010,1040) Patient's Address

- **Note**: The CRYPE ID must be stored with the prefix `CRID#` (e.g., `CRID#1234567890123456`) at the end of the tag's content.

4.2.3 DICOM Sending Settings

- **Activate DICOM Sending**:
  - **Description**: Enables/disables sending DICOM data to a third-party PACS.
  - **Default**: Disabled (unchecked)

- **IP-Address**:
  - **Description**: IP address of the target PACS for sending DICOM data.
  - **Default**: Empty
  - **Format**: IPv4 address (e.g., 192.168.1.100)

- **Port**:
  - **Description**: Port on the target PACS for DICOM communication.
  - **Default**: 104
  - **Range**: 1–65535

- **AE-Title Receiver**:
  - **Description**: Application Entity (AE) Title of the receiving PACS.
  - **Default**: CRYPE_DCM
  - **Format**: Up to 16 characters, no spaces

- **AE-Title Sender**:
  - **Description**: AE Title used by **CRYPE DicomBridge** when sending data.
  - **Default**: CRYPE_DCM
  - **Format**: Up to 16 characters, no spaces

4.2.4 Testing Connectivity

- **Send DICOM Echo**:
  - **Description**: Sends a DICOM Echo (C-ECHO) to the configured PACS to verify connectivity.
  - **Action**: Click the "Send DICOM Echo" button. A success or failure message will appear.

4.3 Saving and Applying Changes

- **Save**: Click the "Save" button to store the settings. The changes are written to the configuration file.
- **Reset**: Click the "Reset" button to revert to the last saved settings.

- **Restart Service**: After saving changes, restart the Windows service to apply them:
  1. Open `services.msc`.
  2. Find "CRYPE DicomBridge Service."
  3. Right-click and select "Restart."

5. Directory Structure and Workflow

CRYPE DicomBridge uses a structured directory system to manage incoming and outgoing DICOM data. All directories are created under the configured "Storage Folder."

5.1 Directory Overview

- **Inbox_Auto**: Contains ZIP files with CRYPE IDs, automatically processed by the CRYPE app.
- **Inbox_Manual**: Contains ZIP files without CRYPE IDs, requiring manual forwarding via drag-and-drop in the CRYPE app.
- **Inbox_Failed**: Contains folders of DICOM data, where receiving or zipping failed.
- **Outbox_Auto**: Contains ZIP files received from the CRYPE app, that will be automatically send to the configured PACS.
- **Outbox_Failed**: Contains ZIP files that failed to send to the PACS.

5.2 File Naming Convention

- **Received ZIP Files**:
  `PatientName_PatientBirthDate_PatientGender_StudyDate_Modality_StudyUID.zip`
  Example:
  `JohnDoe_19900101_M_20230315_MR_1.2.840.113619.2.55.3.20230315.zip`
- **With CRYPE IDs**:
  CRYPE IDs are appended before the extension:
  `PatientName_PatientBirthDate_PatientGender_StudyDate_Modality_StudyUID_CRID#1234567890123456.zip`

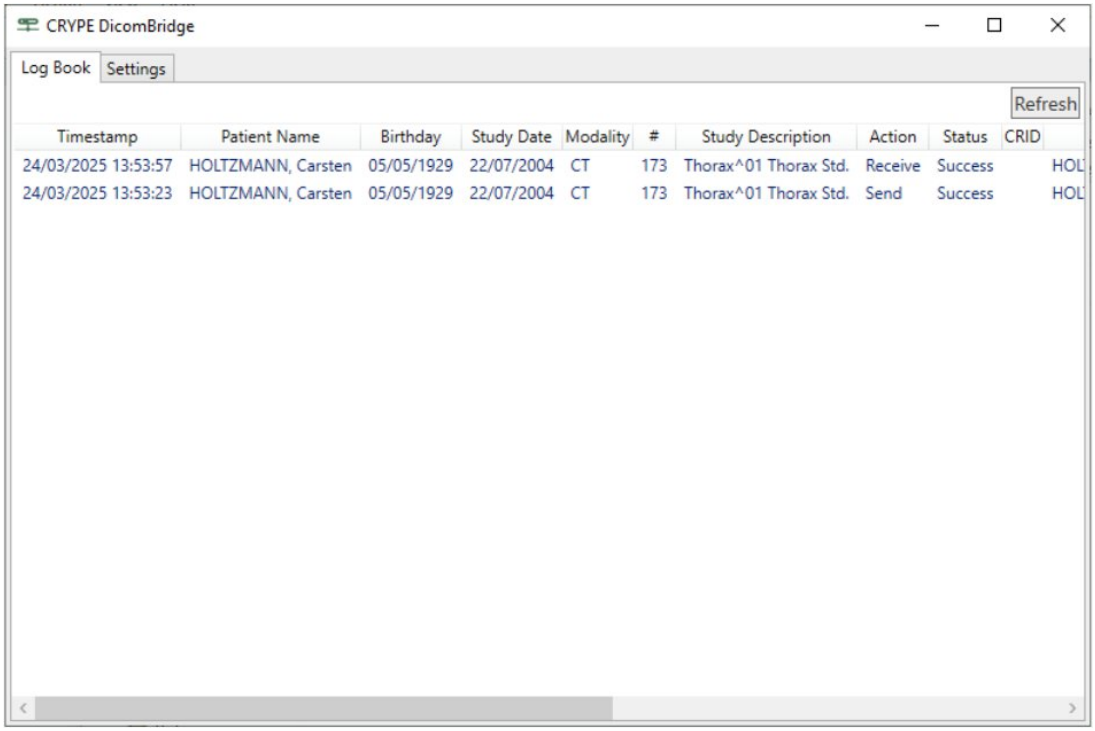
5.3 Workflow

1. **Receiving**:
   - DICOM data is received from a PACS.
   - Data is grouped by study and zipped.
   - If a CRYPE ID is found, the ZIP file goes to `Inbox_Auto`; otherwise, to `Inbox_Manual`.
   - Failed receptions go to `Inbox_Failed`.

2. **Sending**:
   - The CRYPE app places ZIP files in `Outbox_Auto`.
   - DicomBridge sends the DICOM data to the configured PACS.
   - Failed sends are moved to `Outbox_Failed.`
3. **Cleanup**:
   - Files in `Inbox_Failed` and `Outbox_Failed` are deleted after the "Keep failed (days)" period.

6. Logging and Monitoring

- **Logbook**: The "Log Book" tab in the GUI displays the last 500 actions (e.g., received files, sent files, errors).
- **Log Storage**: Logs are stored in the "Storage Folder" for reference.
- **Monitoring Failed Files**: Regularly check `Inbox_Failed` and `Outbox_Failed` for issues, though automatic cleanup reduces manual effort.



7. Troubleshooting

- **Service Not Starting**:
- Verify the service is installed (`services.msc`).
- Check the logbook for errors.
- Ensure the "Storage Folder" path is accessible and writable.
- **DICOM Communication Fails**:
- Use the "Send DICOM Echo" button to test connectivity.
- Confirm the IP address, port, and AE titles match the target PACS.
- Check firewall settings for the configured ports.
- **Files in Failed Directories**:
- Review the logbook for error details.
- Verify DICOM data integrity or PACS availability.
- **CRYPE IDs Not Detected**:
    - Ensure the correct DICOM tag (Group and Element) is configured.
    - Confirm the CRYPE ID format (`CRID#1234567890123456`) in the DICOM tag.

8. Best Practices

- **Run as Service**: Always use the Windows service mode for production to ensure continuous operation.
- **Backup Storage Folder**: Regularly back up the "Storage Folder" to prevent data loss.
- **Monitor Disk Space**: Ensure sufficient disk space in the "Storage Folder" to handle incoming and outgoing ZIP files.
- **Test Configuration**: After changing settings, use "Send DICOM Echo" to verify connectivity before restarting the service.
- **Secure Ports**: Configure firewall rules to allow traffic only on the specified DICOM ports (e.g., 104).

9. Support

For additional assistance, contact CRYPE support via:

- **Website**: www.crype.eu
- **C-mail**: