

# Tawasol's Decryption Interface

## Table of Contents

|                               |   |
|-------------------------------|---|
| 1. Introduction .....         | 2 |
| 2. Agent Login .....          | 2 |
| a. Login Interface.....       | 2 |
| b. Decryption Interface ..... | 4 |
| 3. Support Login .....        | 5 |
| a. Login Interface.....       | 5 |
| b. Decryption Interface ..... | 6 |

# 1. Introduction

Tawasol's decryption interface is designed to empower **agents** and **support teams** with the ability to securely decrypt content when necessary. This intuitive and user-friendly interface ensures that authorized personnel can access sensitive information while maintaining strict security protocols.

We have two user roles: **Agent** and **Support**, each with a specific key.

- **Agents** have only **Key Part 1**.
- **Support** must obtain **both key parts** before proceeding with decryption.

## Key Retrieval Process

- **Key Part 1:** The support receives this key from the agent.
- **Key Part 2:** The support must request this key by clicking the "**Send Key**" button. This sends a request to the **Branch Manager**.
- The **Branch Manager** will then send **Key Part 2** via email.

# 2. Agent Login

## a. Login Interface

The login interface allows agents to securely access the system using their credentials. The agent must enter a valid username and password, select the "Agent" role, and then click the "Login" button to proceed. This ensures secure authentication and controlled access to the decryption interface. A "**Cancel**" button is also available, allowing the agent to exit the login process if needed.



After submitting the login details, an OTP verification interface will appear. The agent must enter the OTP code sent to their registered mobile number. Without the correct OTP, access to the system will not be granted, ensuring an additional layer of security.

If the OTP has expired, a **"Resend OTP"** button is available. Clicking this button will trigger the system to send a new OTP to the agent's mobile number, ensuring they can complete the verification process securely.

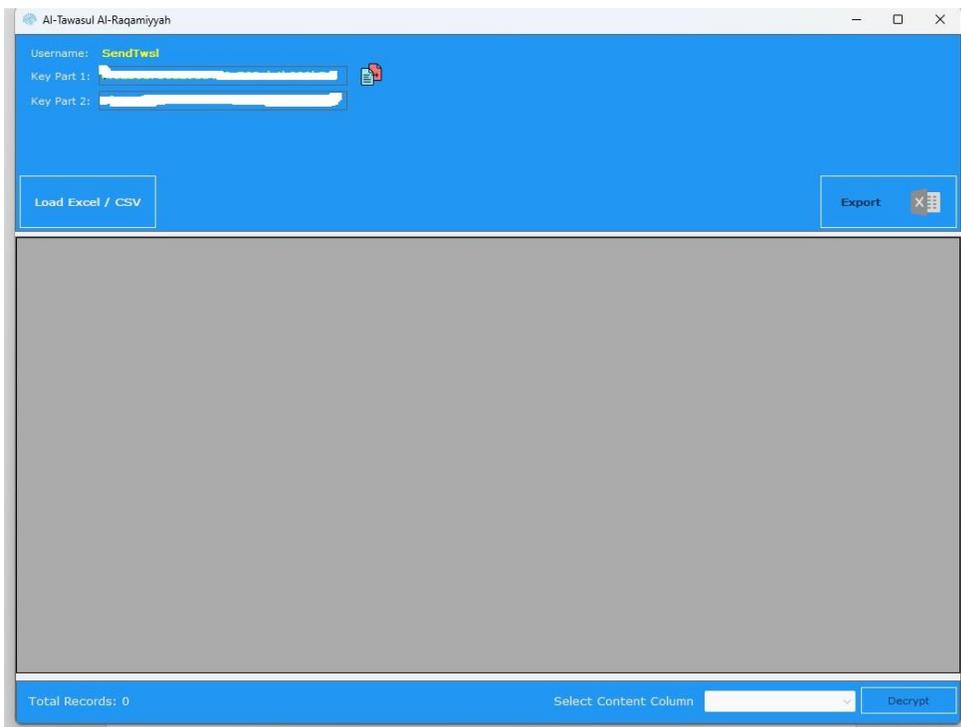


Once the agent successfully logs in and verifies the OTP, the decryption interface will appear. This interface allows the agent to access and decrypt authorized content based on their permissions, ensuring secure and efficient data handling.

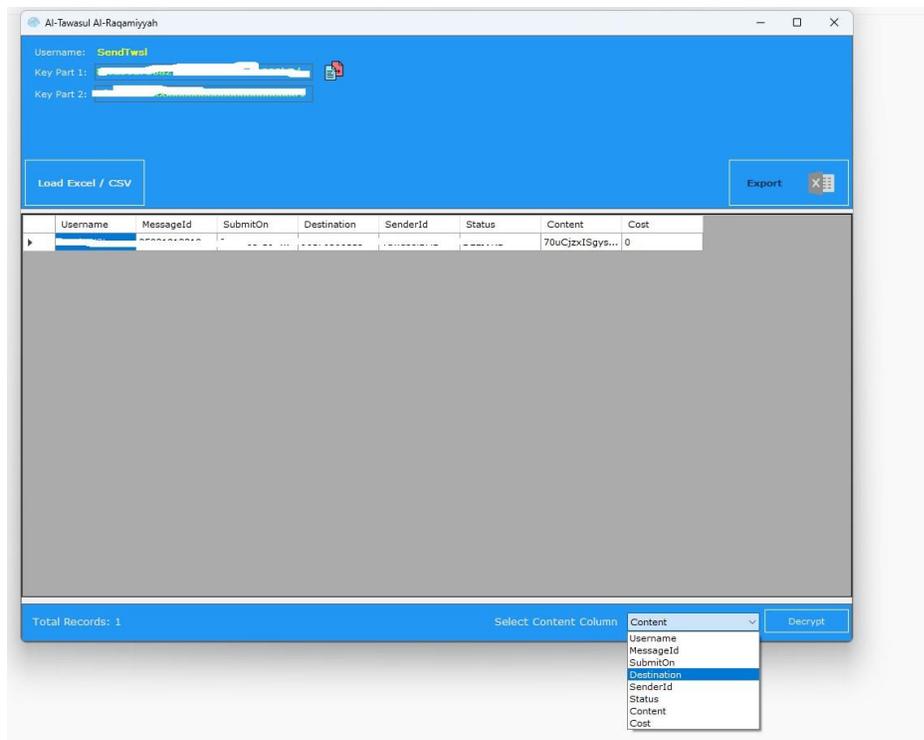
## b. Decryption Interface

The decryption interface allows the agent to securely decrypt content using **Key Part 1**. The agent can copy this **key Part 1** by clicking the copy icon. It will be used by support if requested.

**Key Part 2:** **Key Part 2** is partially masked and cannot be used by the agent. The Branch Manager will set **Key Part 2** by default.



To initiate the decryption process, the agent clicks the "Load Excel/CSV" button and selects a file. After the file is uploaded, a "Select Content" dropdown appears at the bottom of the interface, displaying available columns such as Username, Message ID, Submit On, Destination, Sender ID, Status, Content, and Cost. The agent must choose the specific encrypted content to decrypt before clicking the "Decrypt" button. The system will then process the selected columns and present the decrypted data in the table.



The "Export" button allows the agent to download the processed data as a CSV file. When clicked, the system generates a CSV file containing relevant information, such as decrypted content, status, message ID, and other selected columns. The file is then automatically downloaded, enabling the agent to save and share the data as needed. This feature ensures efficient data handling and easy access to exported records for further analysis or reporting.

### 3. Support Login

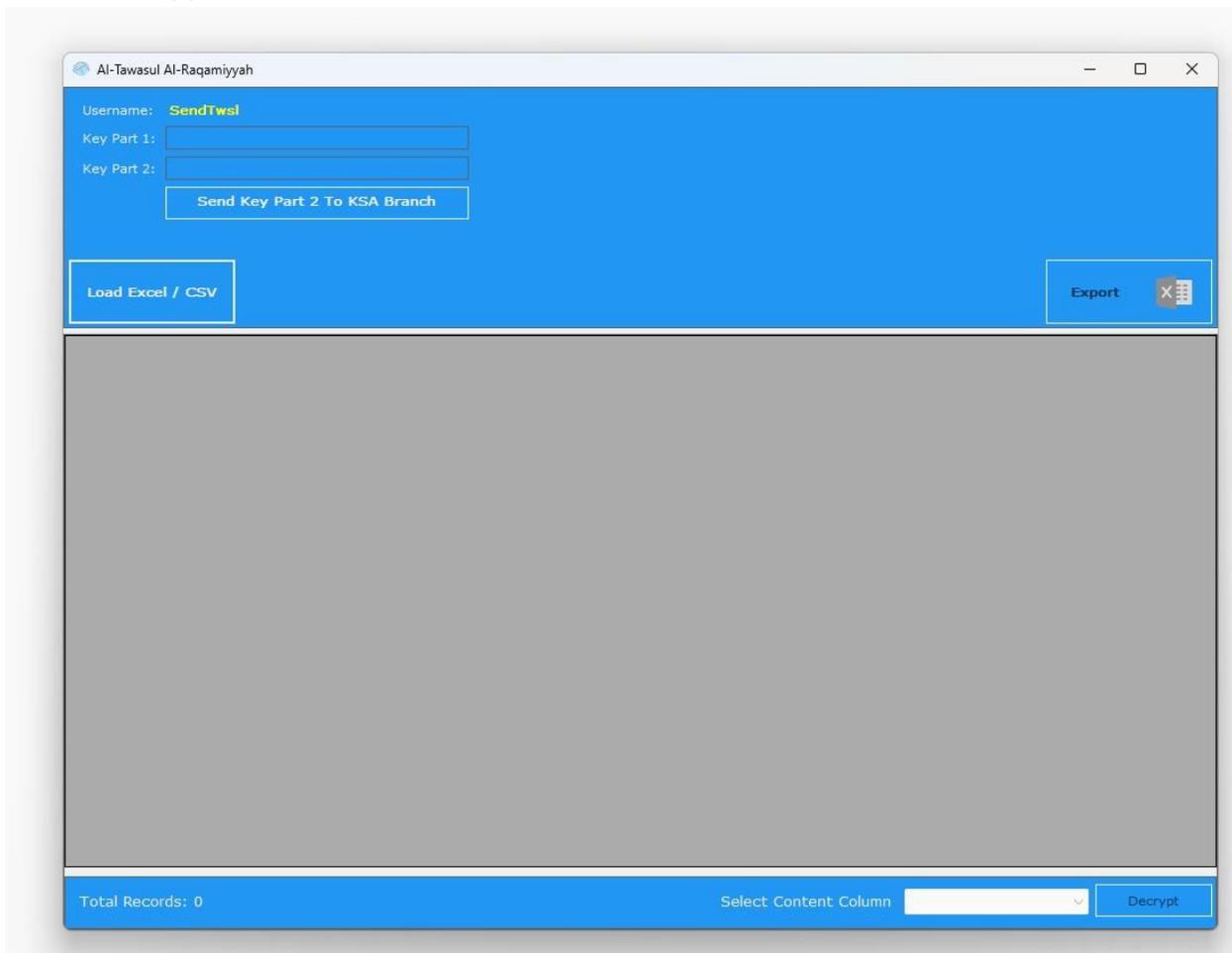
#### a. Login Interface

The support selects the **Support** role and enters only their **username**, as they do not have access to a password. They then click "**Login**" to proceed, or click "**Cancel**" to exit the login process.

After submitting the login, Decryption Interface will appear.



## b. Decryption Interface



The support must:

- **Request Key Part 1** from the **agent**.
- **Request Key Part 2** by clicking the **"Send Key"** button, which sends a request to the **Branch Manager**.

The **Branch Manager** will then send **Key Part 2** via email.

Once both key parts are obtained, the **support** clicks the **"Load Excel/CSV"** button and selects a file. After the file is uploaded, a **"Select Content"** dropdown appears at the bottom of the interface, listing available columns such as **Username, Message ID, Submit On, Destination, Sender ID, Status, Content, and Cost**.

The support selects the specific **content** to decrypt and clicks the **"Decrypt"** button. The system will then process the selected columns and proceed with the decryption.

The **"Export "** button allows the agent to download the processed data as a CSV file. When clicked, the system generates a CSV file containing relevant information, such as decrypted content, status, message ID, and other selected columns. The file is then automatically downloaded, enabling the agent to save and share the data as needed. This feature ensures efficient data handling and easy access to exported records for further analysis or reporting.