TransferIQ Orchestrate
Quick start guide

Table Of Contents

Introduction

The TransferIQ Orchestrate App seamlessly integrates with MFT/B2Bi solutions, providing a customized digital experience for onboarding trading partners and setting up file routes through a self-service platform with robust administrative oversight. A configurable workflow orchestrates the onboarding and file routing processes, enhancing collaboration and progress visibility for business users, administrators, and approvers. This system significantly reduces the time and resources needed to onboard and exchange files with new partners and manage and update routing details for existing partners. Automation of administrator actions minimizes costly manual errors, boosting overall efficiency. The app implements role-based access control to govern user views and actions, ensuring security. Additionally, Orchestrate App integrates seamlessly with SAML-based SSO systems like Okta, facilitating easy user access, and ITSM systems like ServiceNow for creating and updating RITMs for official record-keeping.

Sign Up First Time Super Admin

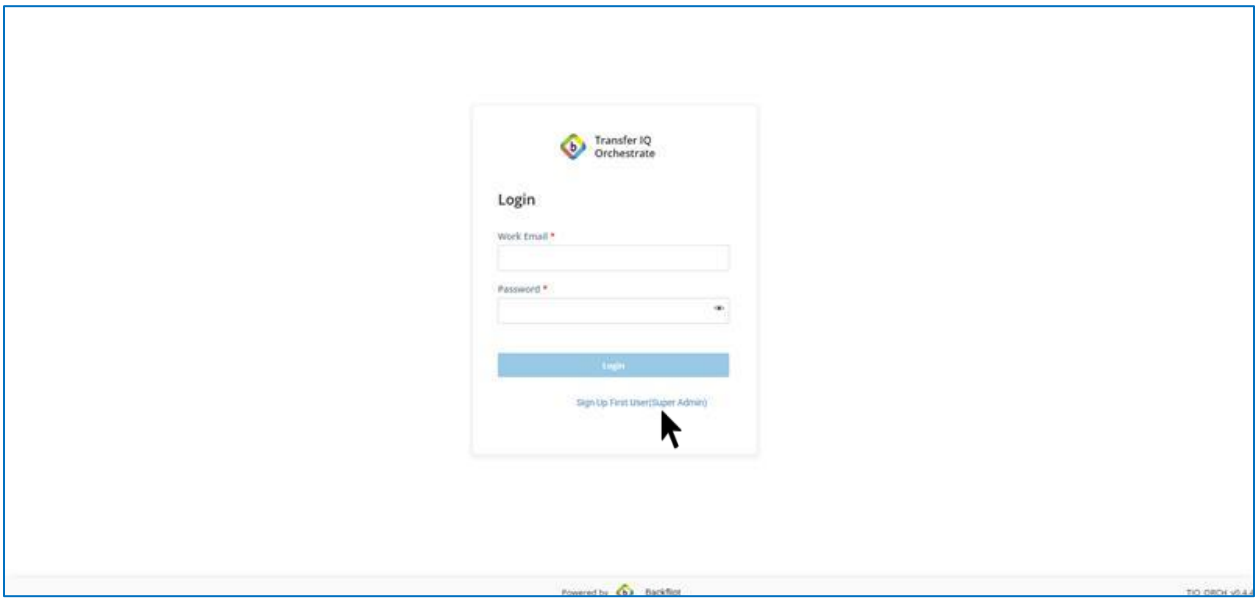
When the **Transfer IQ Orchestrate Application** is launched for the first time, the application does not contain any registered users. Since access to the application is restricted, it is necessary to add the **first user to start using the application**

To address this, the application automatically displays a screen prompting the registration of the initial user. This first user will be assigned **the Super Admin** role, allowing the user to configure settings, manage users, and perform other admin tasks.

This Super Admin account acts as the foundational user, enabling full access and control of the application

To sign up the first time Super Admin, follow the below steps

1. Click the **Sign Up First Super Admin** to begin the registration process for the first user, who will be assigned with role as **Super Admin**

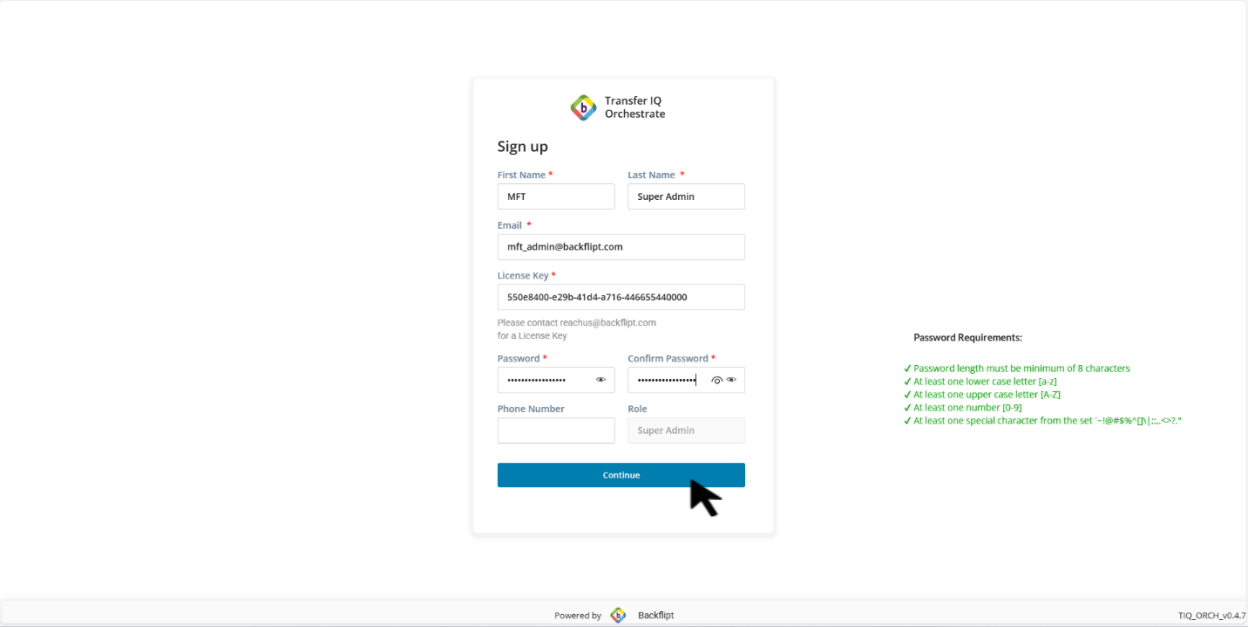


2. Once the button is clicked a signup form will be displayed with the following fields
    a. **First Name** – The first name of the Super Admin.
    b. **Last Name** – The last name of the Super Admin.
    c. **Email Address** – A valid email to be used for login and communication.
    d. **License Key** – Only users with a valid license key can register and access the application. The Backflipt team will provide the license key offline to users

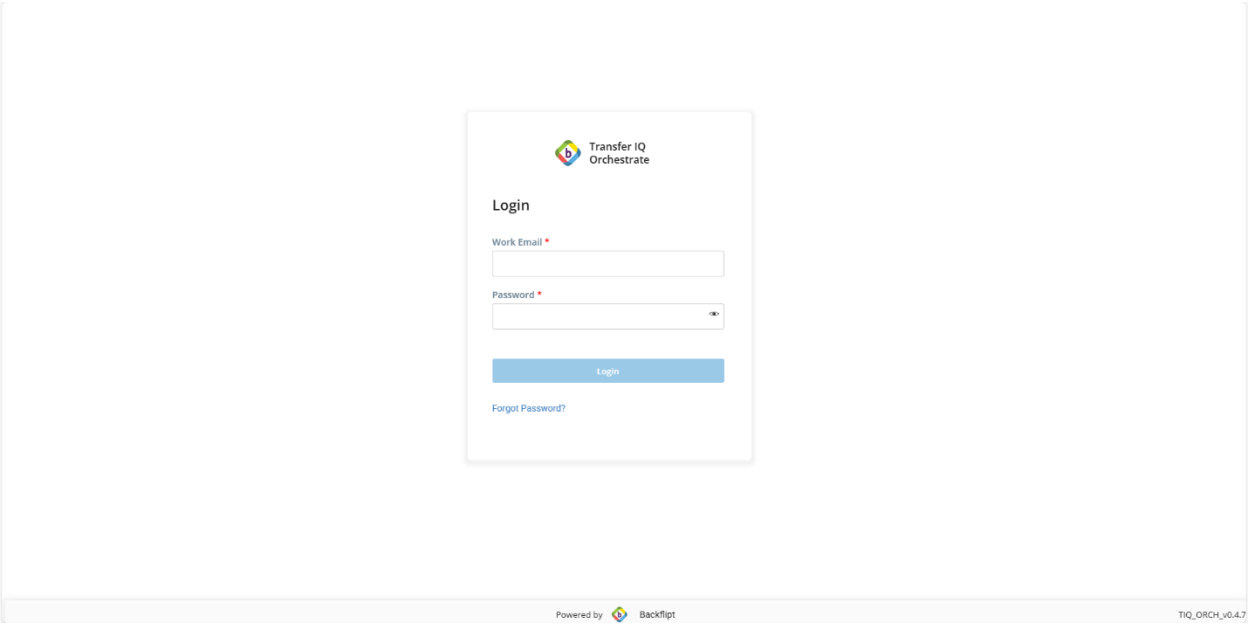
signing up for the first time. This key will then be used by the admin to log in to the application.

e. **Password** – A secure password for account access.
f. **Confirm Password** – Re-enter the password to confirm accuracy.
g. **Phone Number** – A valid phone number for verification or support.

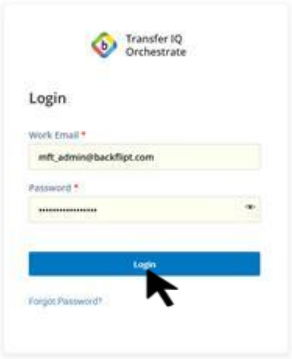
3. Click the **Continue** button to complete the registration process



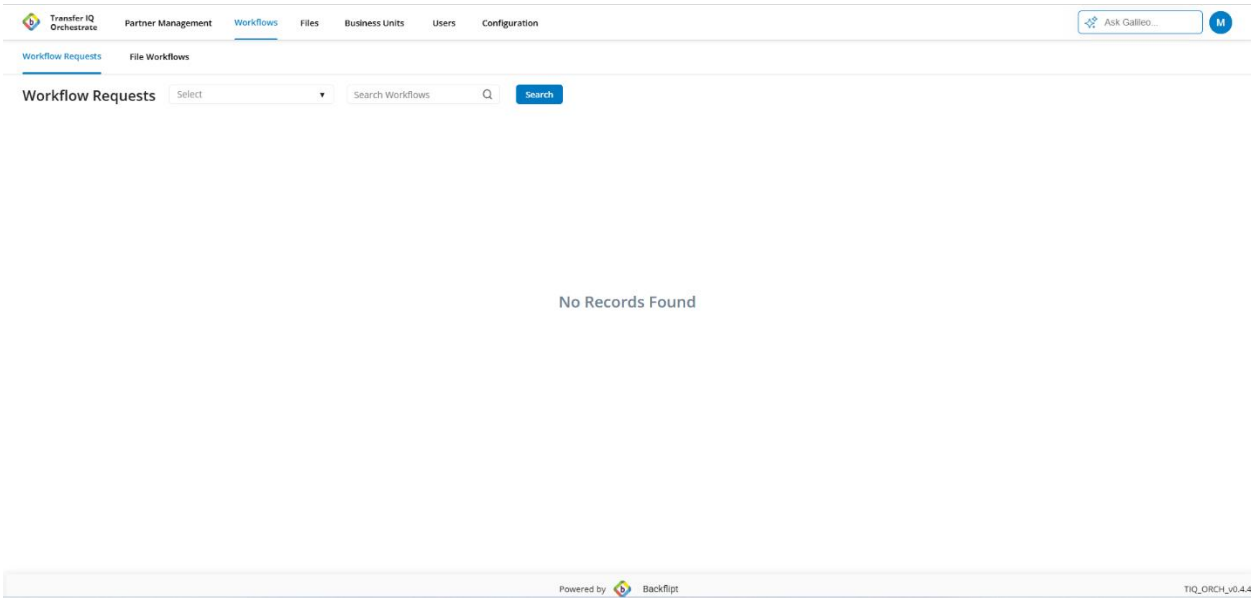
4. After the Super Admin is successfully registered, the application redirects to the following **Login page**.



5. Enter the email and password and click the login button to login to the application



6. Once login is successful, super admin is redirected to the application Workflows>Workflow Requests



Configuration

When the user clicks on the **Configuration** tab, they are redirected by default to the **SFTP Servers** section.

The **Configuration** tab contains the following subsections:

- SFTP Servers
- MFT Settings

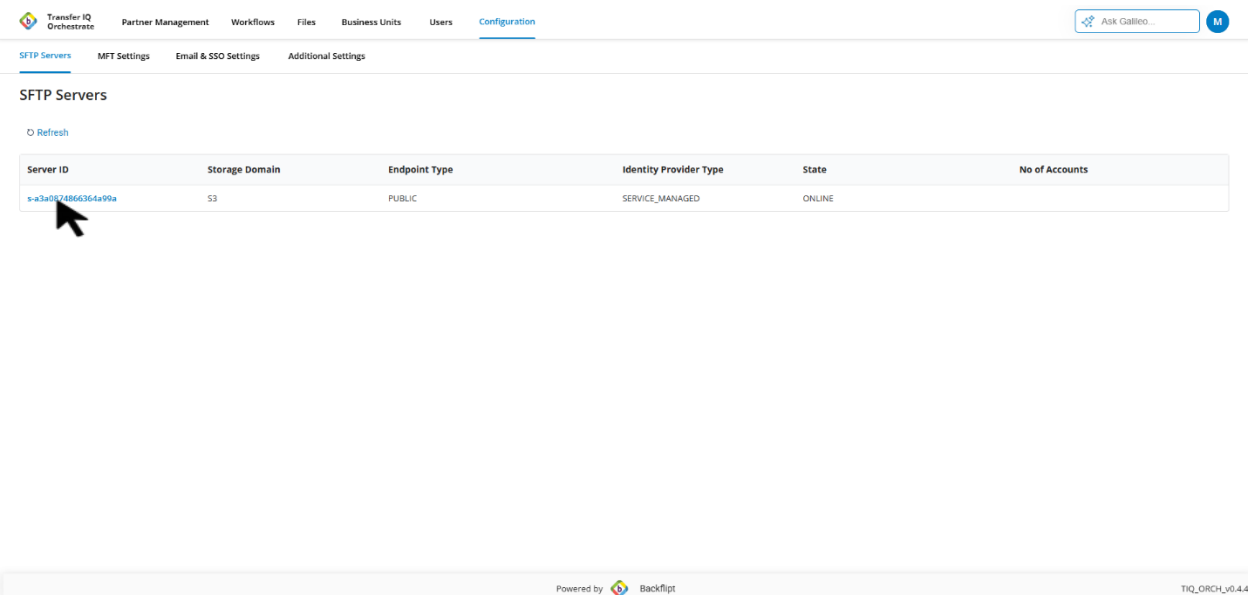
SFTP Servers

When the user clicks on Configuration tab navigates to the SFTP Servers.

The **SFTP Servers** section displays a list of available SFTP servers configured for the company. Each server entry provides the following details:

- **Server ID:** A unique identifier for the SFTP server. This is clickable and navigates the user to the server details page.
- **Storage Domain:** Indicates the storage type used, e.g., **S3**.
- **Endpoint Type:** Specifies the server's endpoint type, e.g., **Public**.
- **Identity Provider Type:** Displays the identity provider type, e.g., **SERVICE_MANAGED**.
- **State:** Shows the current server status, e.g., **Online**.
- **No of Accounts:** Displays the number of accounts created for this server (empty if no accounts are created yet).

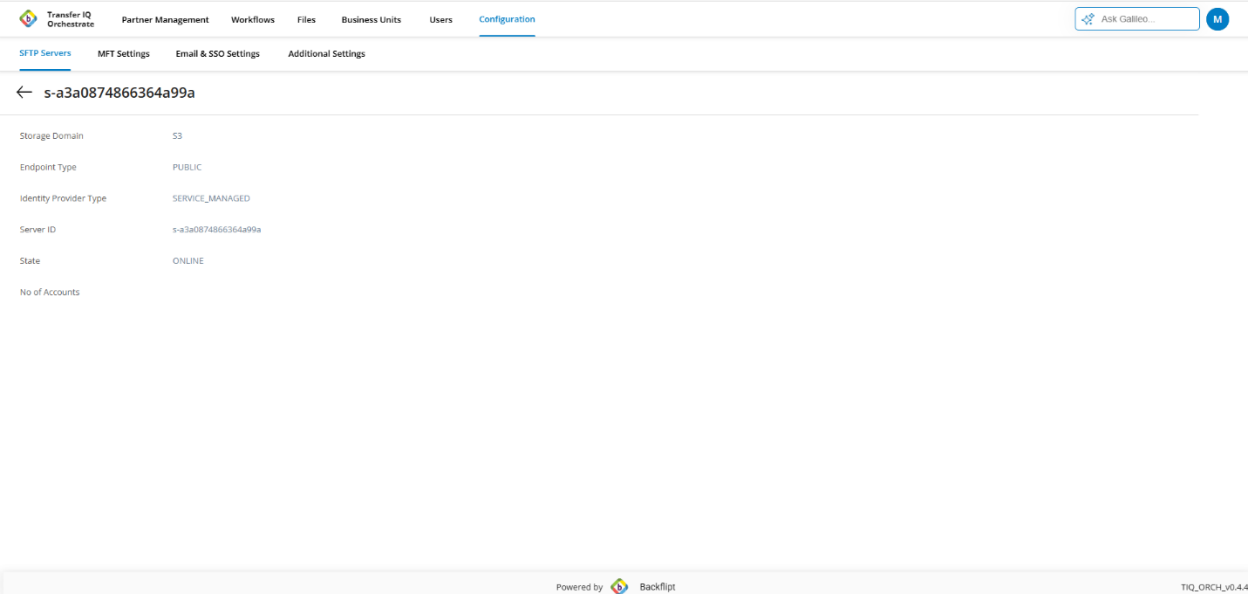
Users can click on the **Server ID** to view more detailed information about that server.



The user can also click on the server, which navigates to the server page.

When a user clicks on a **Server ID** from the SFTP Servers list, they are navigated to the server details page. This page displays detailed information about the selected server, including:

- Storage Domain
- Endpoint Type
- Identity Provider Type
- Server ID
- Status
- No of Accounts



This view provides a quick summary of all key server properties for better visibility and troubleshooting.

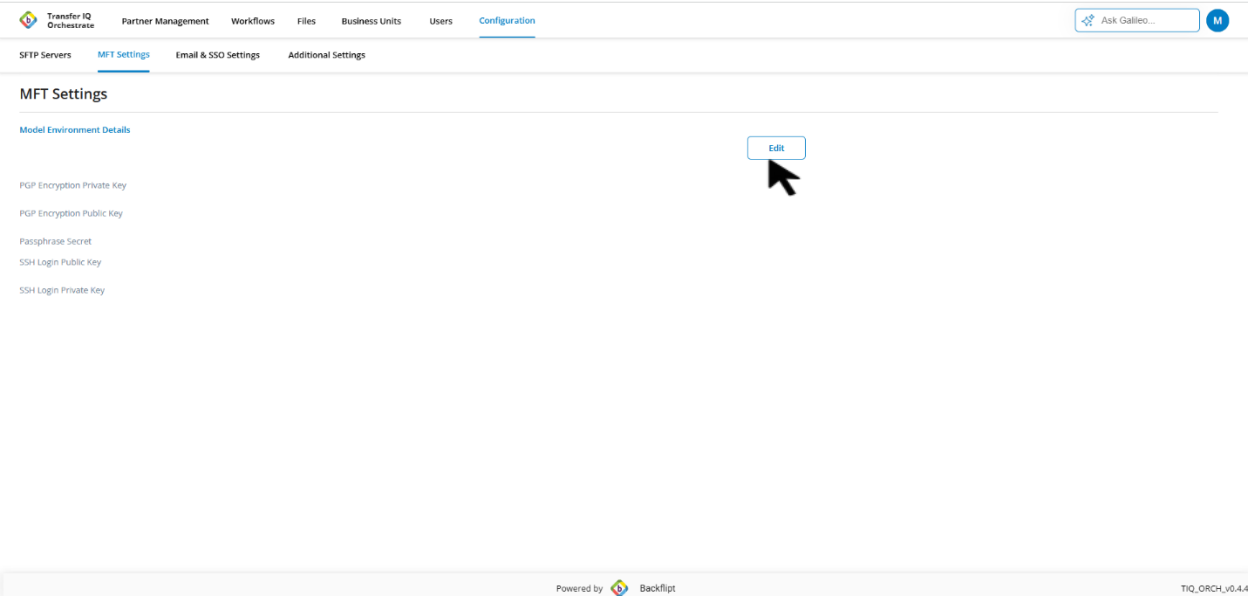
MFT Settings

Click on MFT Settings to navigate to the MFT Settings section in the Configuration tab.

By default, the page shows an empty state with the following fields:

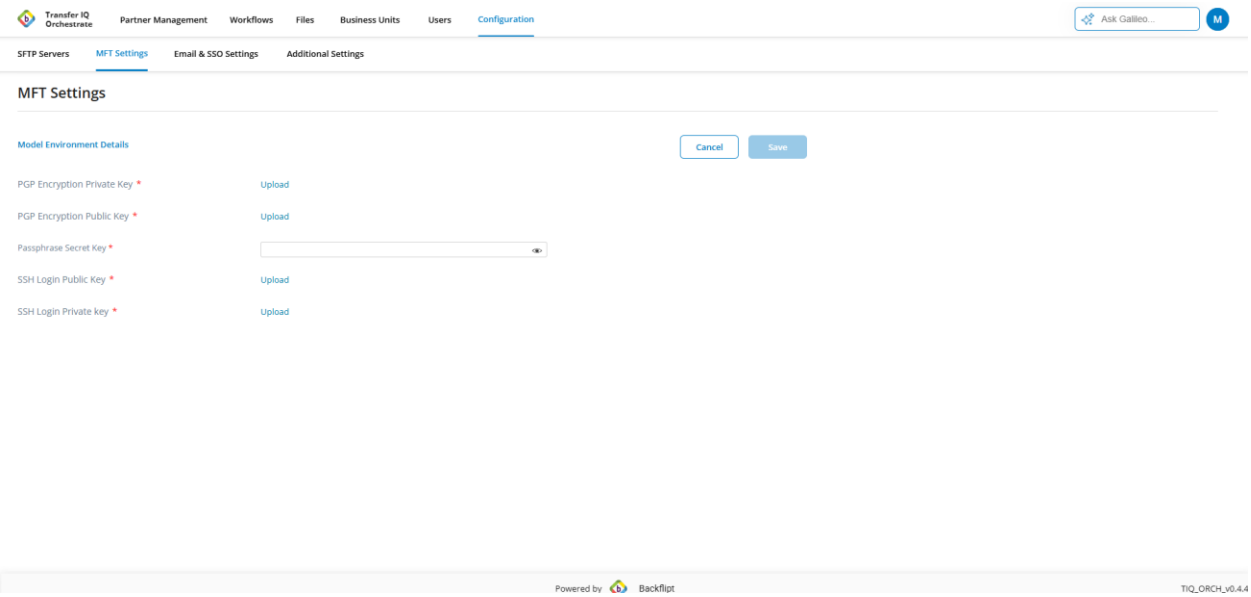
It includes the following fields:

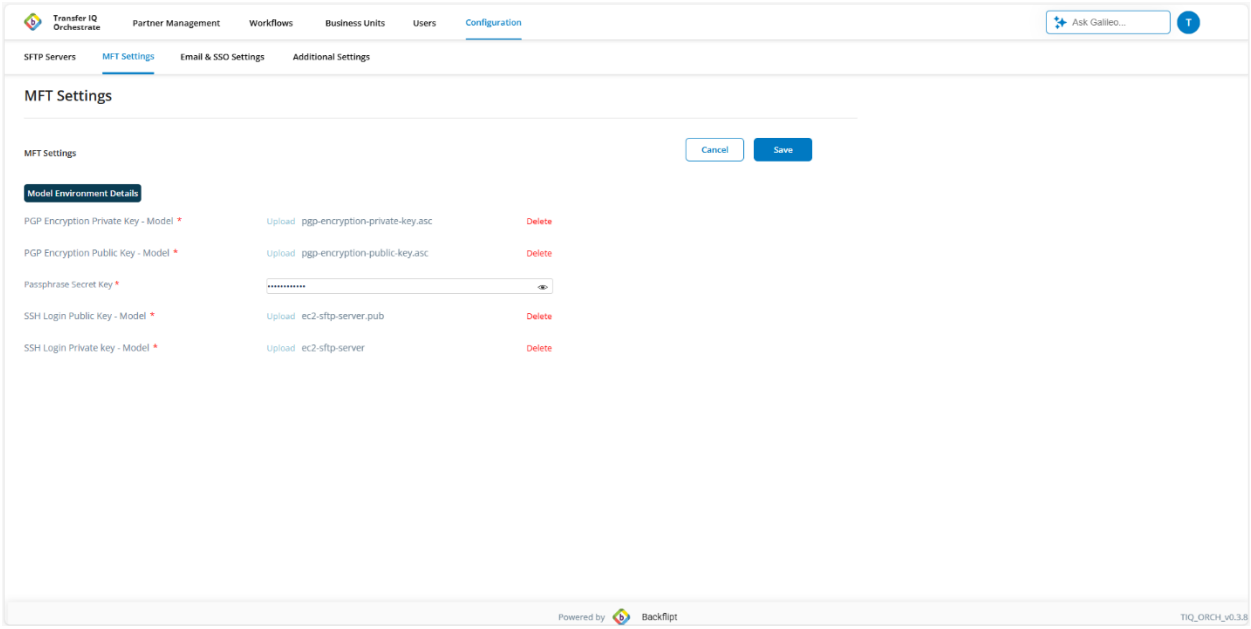
- PGP Encryption Private Key
- PGP Encryption Public Key
- Passphrase Secret Key
- SSH Login Public Key
- SSH Login Private Key



At the top-right, an **Edit** button is available.

When the user clicks **Edit**, they can configure and upload valid certificates or keys for each of the above fields.





Upon clicking on Save, the provided details by the user will be saved.

PGP Encryption Public Key:
This is a **publicly shared key** used for file encryption.

- When a partner needs to send files to the company, the company provides this public key in the *Account Creation Successful* email.
- The partner uses this public key to encrypt files on their end, ensuring that the files can only be decrypted by the company.
- Since it is a public key, it is safe to share with external partners.

PGP Encryption Private Key:
This is the **private key** that corresponds to the public key above.

- The company keeps this key secure and never shares it.
- When encrypted files are received from a partner, the company uses this private key to decrypt and access the file contents.
- The private key, together with the passphrase (if configured), ensures that only authorized company users can decrypt the data.

Passphrase Secret Key:
This acts as an **additional security layer** for the PGP private key.

- The passphrase must be entered whenever the private key is used for decryption.

- This prevents unauthorized use of the private key, even if someone gains access to the key file.
- It ensures end-to-end data confidentiality by adding another authentication step.

SSH Login Public Key:
This is the **public part of the SSH key pair** used for server authentication.

- The company shares this public key with the partner in the *Account Creation Successful* email.
- The partner adds this public key to their server's authorized keys list.
- Once configured, it allows the company to log in securely to the partner's server without using a password.

SSH Login Private Key:
This is the **private part of the SSH key pair**, which must be kept secure by the company.

- The company uses this private key to authenticate itself when logging in to the partner's server.
- Together with the public key stored on the partner's server, it enables a secure, password-less SSH connection.
- The private key should never be shared or exposed, as it grants direct access to the partner's server.

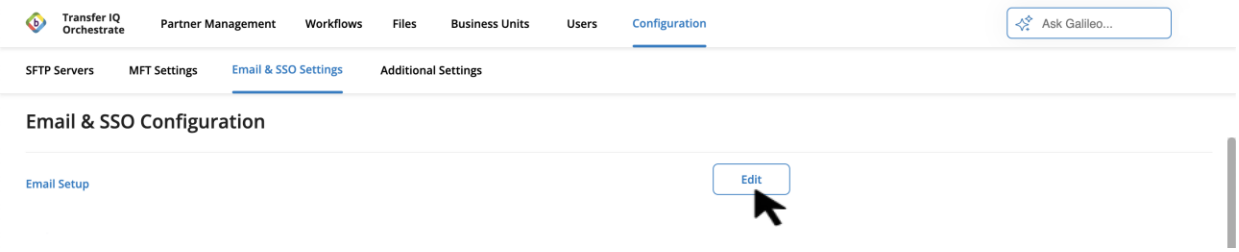
Email and SSO Settings

Click on Configuration > Email and SSO Settings to view and edit the email and SSO settings

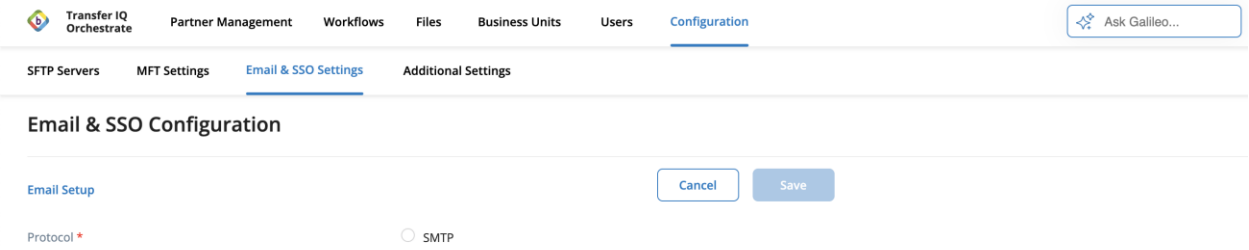
Email Setup

The **Email Setup** section is used to configure how the application sends emails.

Click the Edit button to edit the email setup

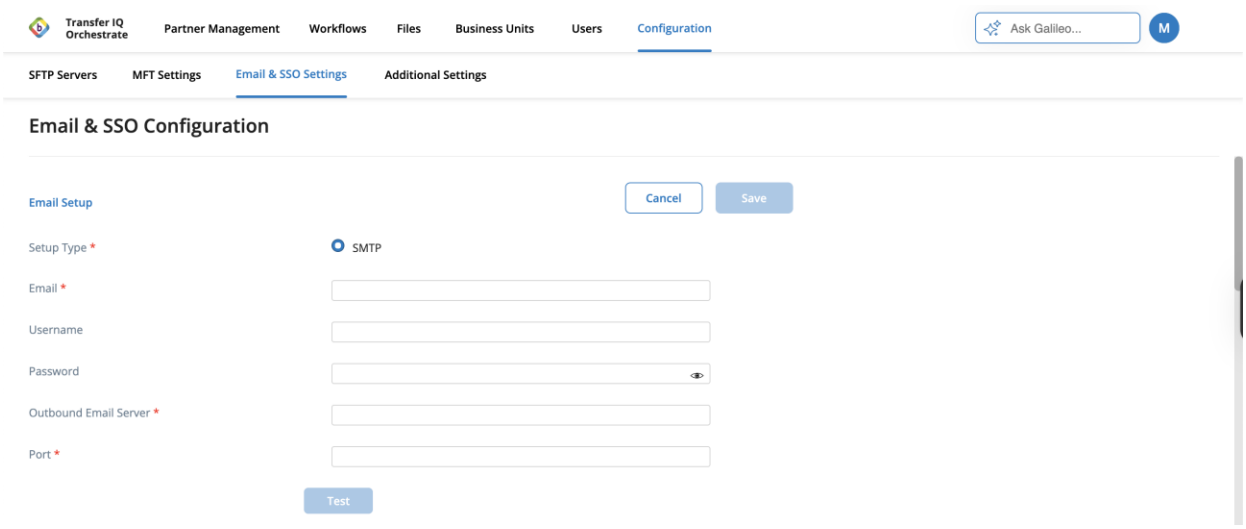


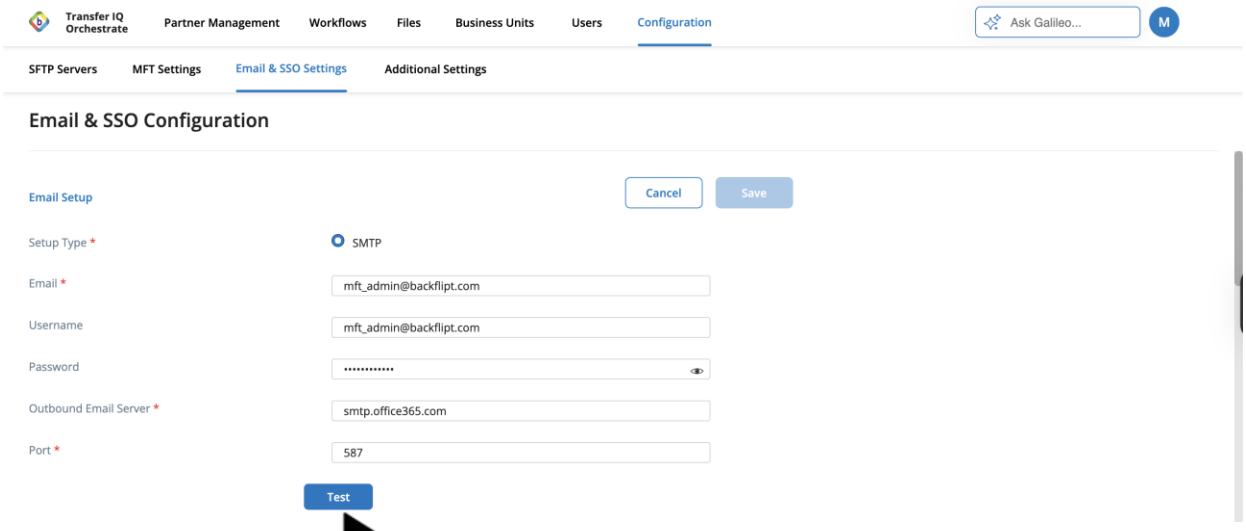
The application supports SMTP (Simple Mail Transfer Protocol) for sending emails, which requires specifying the appropriate email server and credentials.



This section contains the below fields

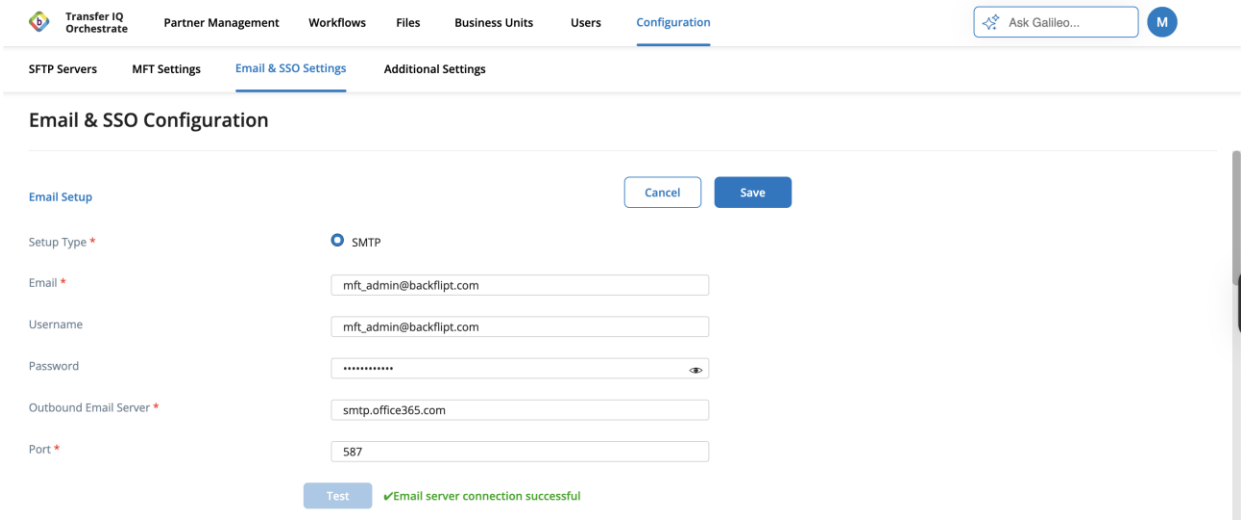
1. **Setup Type -** Specifies the method used to send emails. Transfer IQ Orchestrate application supports **SMTP**, which is a standard protocol for sending email messages between servers.
2. **Email -** The email address that will appear as the sender of system-generated emails.
3. **Username-** The username used to authenticate with the email server.
4. **Password-** The password associated with the email account or application-specific password. This is used to authenticate the application with the SMTP server.
5. **Outbound Email Server -** The address of the SMTP server through which emails will be sent. This is provided by the email service (e.g., Office 365)
6. **Port -** The port number used to connect to the SMTP server. (Example: 587)



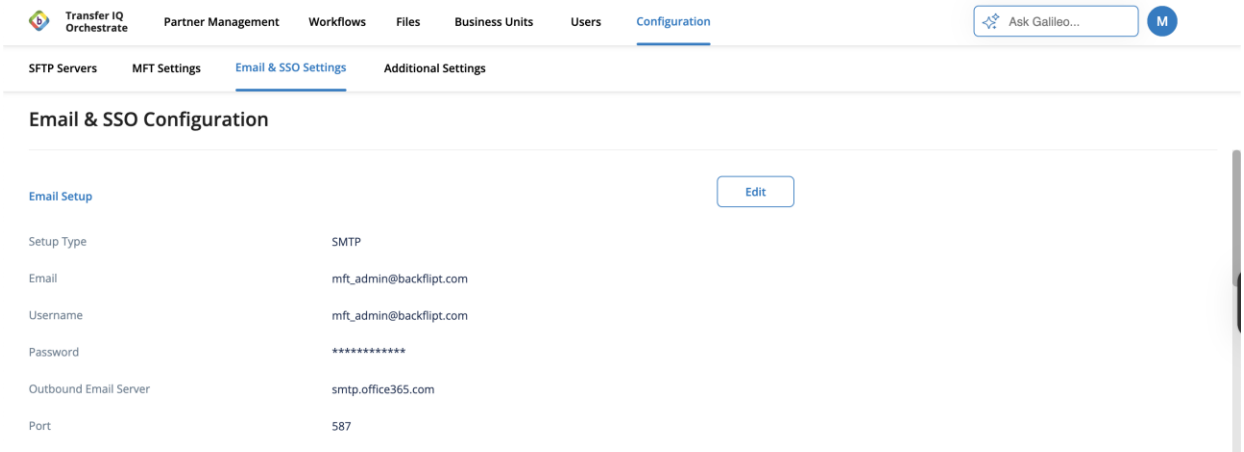


Once the Super Admin has entered all the SMTP details, Super Admin clicks the **"Test"** button to verify the connection. If the connection is successful, a confirmation message

will be displayed indicating that the email server has been successfully connected.



After a successful test, click the **"Save"** button to save the details. Once saved, the details will appear in **view mode** within the **Email Setup** section



The Application is now ready to onboard business users and partners and create a workflow to initiate the use of the TransferIQ MFT Solution.