



# **TransferIQ Orchestrate**

## **Quick start guide**



## Table Of Contents

Introduction.....	2
Sign Up First Time Super Admin.....	2
Configuration.....	5
Servers.....	6
SFTP Protocol.....	6
AS2 Protocol.....	8
SFTP & AS2 Protocol.....	10
MFT Settings .....	10
SFTP Protocol.....	11
Key Rotation for SFTP .....	14
Company PGP Key Rotation.....	14
Company SSH Key Rotation.....	21
Custom Step Configuration: .....	29
AS2 Protocol.....	35
Key Rotation for AS2.....	46
Company Message Encryption Certificates Rotation .....	46
Company Message Signing Certificates Rotation.....	52
SFTP & AS2 Protocol.....	58
Email and SSO Settings .....	58
Email Setup.....	59
Email Templates .....	62
Transfer IQ Orchestrate SSO Setup .....	65
External Services.....	69
Support .....	80
Backflift Standard Support Model .....	80



# 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 manages and updates 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.

Transfer IQ Orchestrate supports multiple file transfer protocols, including **SFTP** and **AS2**.

1. If only SFTP Protocol is deployed, the application will display the information associated with SFTP. This includes the SFTP server configuration details along with the PGP encryption keys and SSH keys used for secure access
2. If only AS2 Protocol is deployed, the application will display exclusively the information associated with AS2. This includes the AS2 server details as well as the certificates used for AS2 communication
3. When both AS2 and SFTP protocols are deployed, the application will display the information for both. This includes all AS2-related details such as server configuration and certificates used for AS2 communication as well as SFTP-specific details, including the SFTP server configuration and the encryption and SSH keys used for secure access.



# Sign Up First Time Super Admin

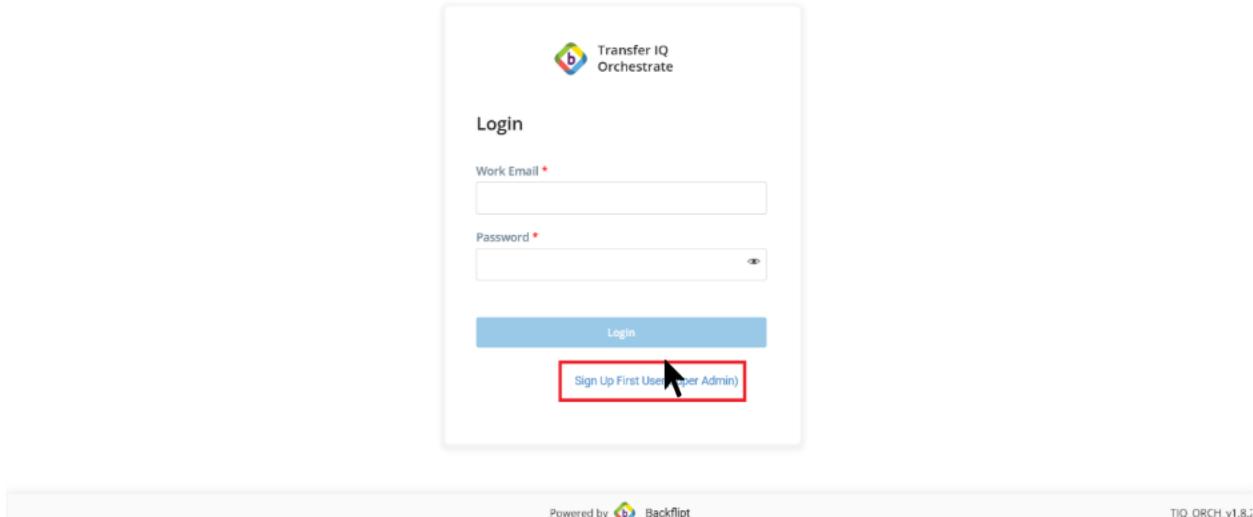
When the **Transfer IQ Orchestrate Application** is launched for the first time, the application does not contain any registered users. Since access to the application is restricted, it is necessary to add the **first user to start using the application**

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**



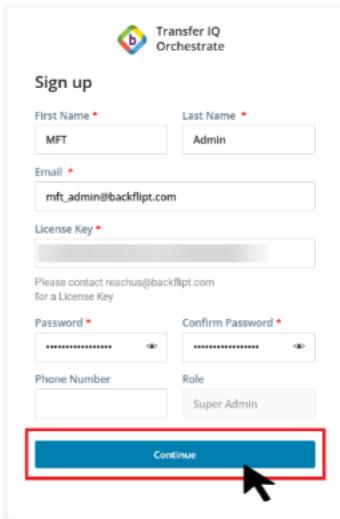
2. Once the button is clicked a signup form will be displayed with the following fields
  - a. **First Name** – The first name of the Super Admin.
  - b. **Last Name** – The last name of the Super Admin.
  - c. **Email Address** – A valid email to be used for login and communication.
  - d. **License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

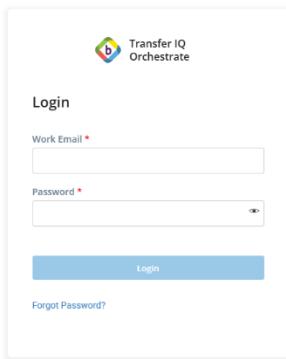
- e. **Password** – A secure password for account access.
- f. **Confirm Password** – Re-enter the password to confirm accuracy.
- g. **Phone Number** – A valid phone number for verification or support.

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



The screenshot shows the 'Sign up' page for Transfer IQ Orchestrate. The page has fields for First Name (MFT), Last Name (Admin), Email (mft\_admin@backflipt.com), License Key (redacted), Password and Confirm Password (both redacted), Phone Number (redacted), and Role (Super Admin). To the right of the form is a 'Password Requirements' section with the following text:  
✓ Password length must be minimum of 8 characters  
✓ At least one lower case letter [a-z]  
✓ At least one upper case letter [A-Z]  
✓ At least one number [0-9]  
✓ At least one special character from the set '!@#\$%^&|~<>?.'  
A red box highlights the 'Continue' button at the bottom of the form, and a cursor is shown hovering over it.

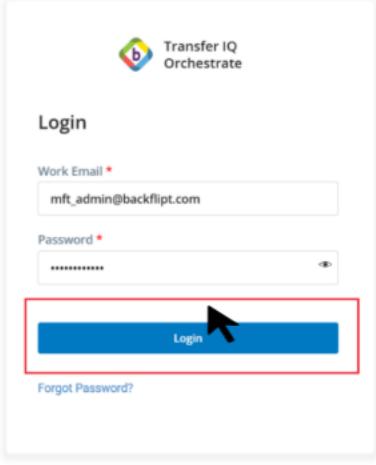
4. After the Super Admin is successfully registered, the application redirects to the following **Login page**.



The screenshot shows the 'Login' page for Transfer IQ Orchestrate. It has fields for Work Email and Password, and a 'Login' button. Below the button is a 'Forgot Password?' link. A red box highlights the 'Login' button, and a cursor is shown hovering over it.

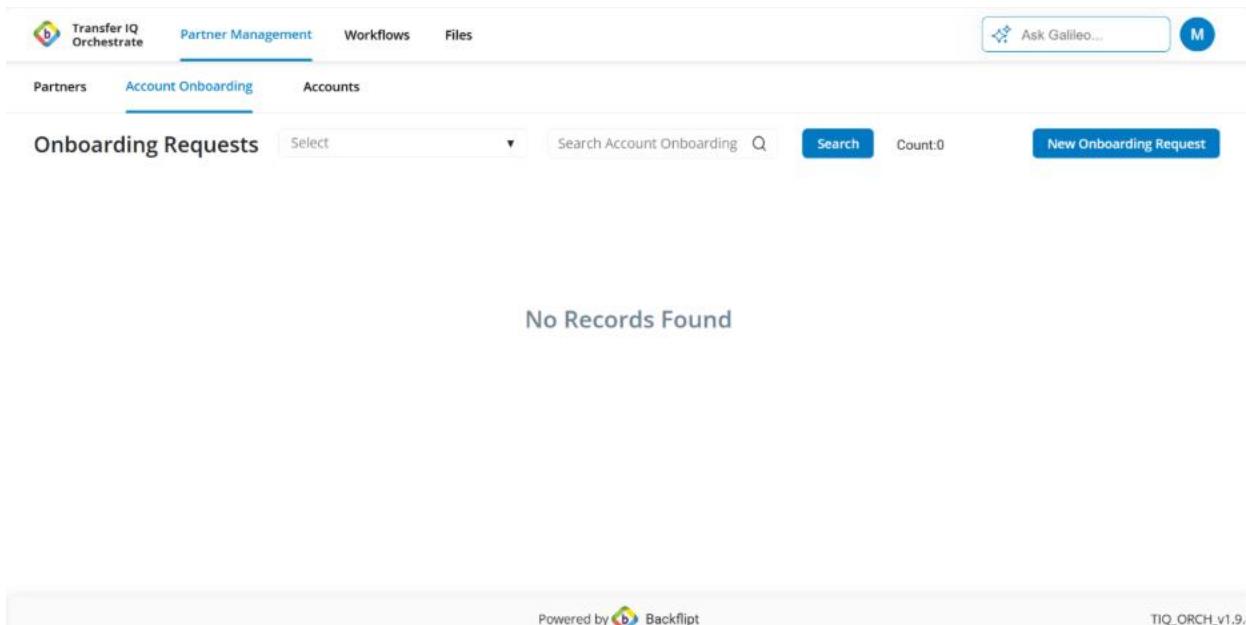


5. Enter the email and password and click the login button to login to the application



The image shows the Transfer IQ Orchestrate login page. At the top is the Transfer IQ Orchestrate logo. Below it is the word "Login". There are two input fields: "Work Email \*" containing "mft\_admin@backflift.com" and "Password \*". A red box highlights the "Login" button, which has a mouse cursor pointing to it. Below the button is a "Forgot Password?" link. At the bottom of the page is a "Powered by Backflift" footer.

6. Once login is successful, super admin is redirected to the application Partner Management > Account Onboarding



The image shows the Transfer IQ Orchestrate Partner Management > Account Onboarding page. The top navigation bar includes "Transfer IQ Orchestrate", "Partner Management" (which is the active tab), "Workflows", and "Files". On the right, there are "Ask Galileo..." and "M" buttons. The main content area has tabs for "Partners", "Account Onboarding" (which is active), and "Accounts". Below these is a search bar with "Onboarding Requests" and "Select" dropdowns, a search button, and a "Count:0" indicator. A "New Onboarding Request" button is also present. The center of the page displays the message "No Records Found". At the bottom is a "Powered by Backflift" footer.



# Configuration

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

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

- Servers
- MFT Settings
- Email & SSO Settings

## Servers

When the user clicks on Configuration tab navigates to the Servers (**AWS Transfer Family Servers**) which displays the details of the servers deployed in a table format

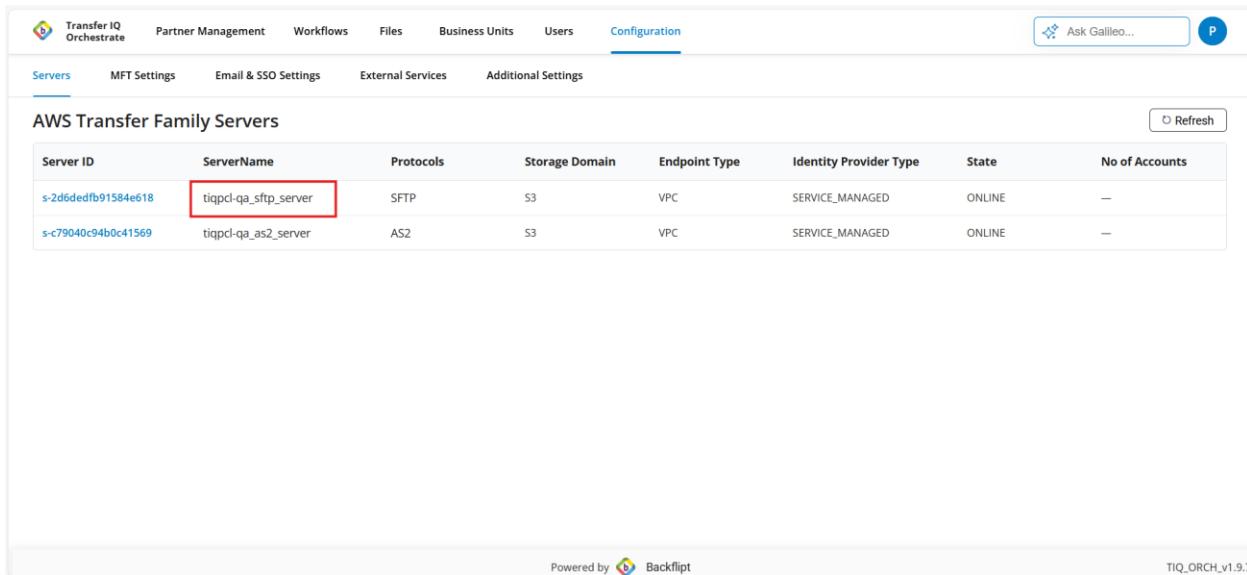
## SFTP Protocol

When only SFTP is deployed, The **AWS Transfer Family Server** section displays the SFTP server configured for the company with the following details

- a) **Server ID:** A unique identifier for the SFTP server. This is clickable and navigates the user to the server details page.
- b) **Server Name:** Name of the Server deployed, e.g. sftp\_server
- c) **Protocol:** SFTP
- d) **Storage Domain:** Indicates the storage type used, e.g., S3.
- e) **Endpoint Type:** Specifies the server's endpoint type, e.g., VPC.
- f) **Identity Provider Type:** Displays the identity provider type, e.g., SERVICE\_MANAGED.
- g) **State:** Shows the current server status, e.g., Online.
- h) **No of Accounts:** Displays the Number of accounts created for this server (blank (\_) if no accounts are created yet).

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





The screenshot shows the Transfer IQ Orchestrate interface with the 'Configuration' tab selected. Under 'Configuration', the 'Servers' tab is active. The page displays a table of 'AWS Transfer Family Servers' with the following data:

Server ID	ServerName	Protocols	Storage Domain	Endpoint Type	Identity Provider Type	State	No of Accounts
s-2d6dedfb91584e618	tiqpcl-qa_sftp_server	SFTP	S3	VPC	SERVICE_MANAGED	ONLINE	—
s-c79040c94b0c41569	tiqpcl-qa_as2_server	AS2	S3	VPC	SERVICE_MANAGED	ONLINE	—

At the bottom, it says 'Powered by  Backflip' and 'TIQ\_ORCH\_v1.9.7'.

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:

- Server Name
- Protocol
- Storage Domain
- Endpoint Type
- Identity Provider Type
- Server ID
- State
- No of Accounts



Transfer IQ Orchestrate

Partner Management Workflows Files Business Units Users Configuration

Ask Galileo... M

Servers MFT Settings Email & SSO Settings Additional Settings

← s-8c2c299cf79e4f58a

ServerName	tiqqapcl-qa_sftp_server
Protocols	SFTP
Storage Domain	S3
Endpoint Type	VPC
Identity Provider Type	SERVICE_MANAGED
Server ID	s-8c2c299cf79e4f58a
State	ONLINE
No of Accounts	—

Powered by Backflift

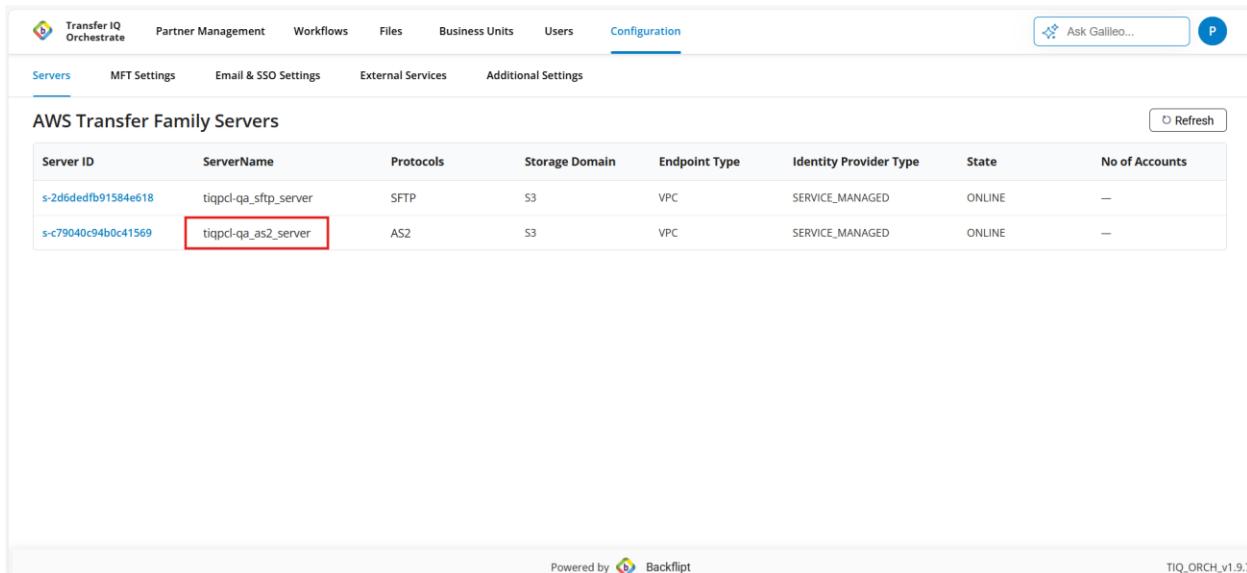
TIQ\_ORCH\_v1.9.4

## AS2 Protocol

When only AS2 is deployed, The AWS Transfer Family Server section displays the AS2 server configured for the company with the following details

- Server ID:** A unique identifier for the AS2 server. This is clickable and navigates the user to the server details page.
- Server Name:** Name of the Server deployed, e.g. as2\_server
- Protocol:** AS2
- Storage Domain:** Indicates the storage type used, e.g., **S3**.
- Endpoint Type:** Specifies the server's endpoint type, e.g., **VPC**.
- 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 as blank (—)





The screenshot shows the Transfer IQ Orchestrate web interface. The top navigation bar includes links for Transfer IQ Orchestrate, Partner Management, Workflows, Files, Business Units, Users, and Configuration. The Configuration tab is selected, and the Servers sub-tab is also selected. The main content area displays a table titled "AWS Transfer Family Servers" with the following data:

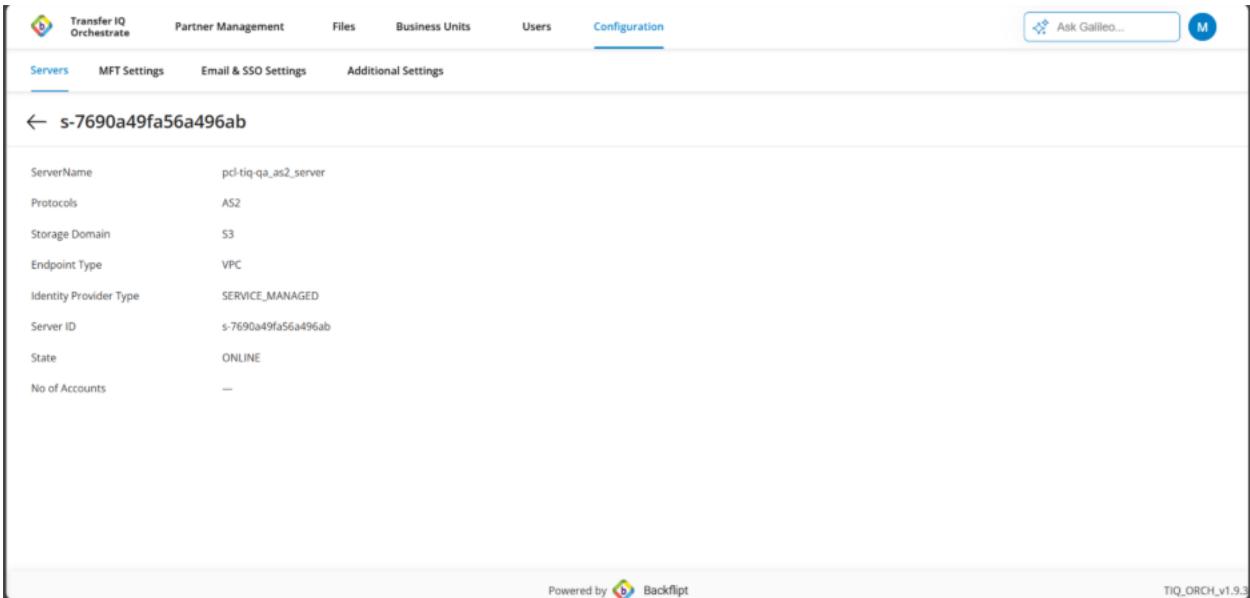
Server ID	ServerName	Protocols	Storage Domain	Endpoint Type	Identity Provider Type	State	No of Accounts
s-2d6dedfb91584e618	tiqpcl-qa_sftp_server	SFTP	S3	VPC	SERVICE_MANAGED	ONLINE	—
s-c79040c94b0c41569	tiqpcl-qa_as2_server	AS2	S3	VPC	SERVICE_MANAGED	ONLINE	—

At the bottom of the interface, it says "Powered by  Backflip" and "TIQ\_ORCH\_v1.9.7".

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

- Server Name
- Protocol
- Storage Domain
- Endpoint Type
- Identity Provider Type
- Server ID
- State
- No of Accounts





The screenshot shows the 'Configuration' tab selected in the top navigation bar. Under the 'Servers' tab, a server with ID 's-7690a49fa56a496ab' is selected. The page displays the following server details:

Setting	Value
ServerName	pcl-tiq-qa_as2_server
Protocols	AS2
Storage Domain	S3
Endpoint Type	VPC
Identity Provider Type	SERVICE_MANAGED
Server ID	s-7690a49fa56a496ab
State	ONLINE
No of Accounts	—

At the bottom, it says 'Powered by  Backflipt' and 'TIQ\_ORCH\_v1.9.3'.

## SFTP & AS2 Protocol

When both **SFTP** and **AS2** are deployed, the AWS Transfer Family Servers section lists both servers in a single table. Selecting either server's ID opens its details page, which shows the same set of server information described above.



## MFT Settings

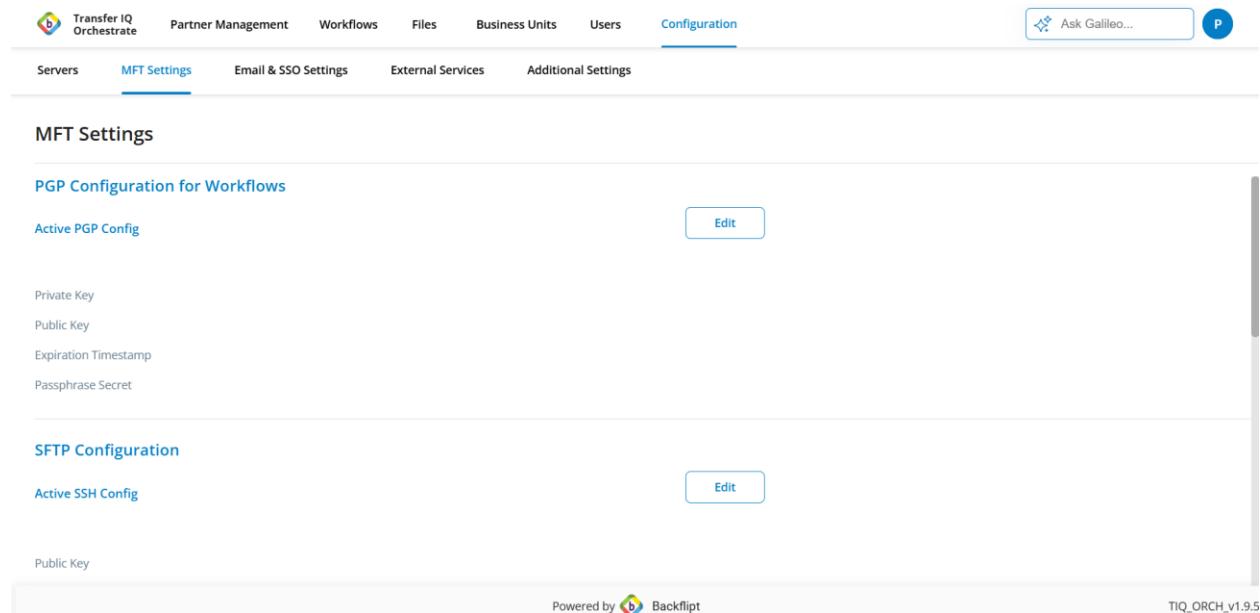
### SFTP Protocol

**When only the SFTP protocol is deployed**, clicking on *MFT Settings* in the Configuration tab will navigate to the MFT Settings section, where only the PGP Config and SFTP Config are displayed. The SFTP Config contains the SSH keys required for logging into the SFTP server

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

It includes the following sections:

- a. PGP Configuration
- b. SFTP Configuration



The screenshot shows the 'MFT Settings' page in the Transfer IQ Orchestrate interface. The top navigation bar includes 'Transfer IQ Orchestrate', 'Partner Management', 'Workflows', 'Files', 'Business Units', 'Users', and 'Configuration'. The 'Configuration' tab is active. Below it, a sub-navigation bar shows 'Servers', 'MFT Settings' (selected), 'Email & SSO Settings', 'External Services', and 'Additional Settings'. The main content area is titled 'MFT Settings' and contains two sections: 'PGP Configuration for Workflows' and 'SFTP Configuration'. The 'PGP Configuration for Workflows' section has a sub-section 'Active PGP Config' with an 'Edit' button. The 'SFTP Configuration' section has a sub-section 'Active SSH Config' with an 'Edit' button. At the bottom, there is a 'Powered by Backflift' logo and the text 'TIQ\_ORCH\_v1.9.5'.

### Uploading PGP Keys:

1. Navigate to the PGP Config to upload PGP keys
2. At the top right, an **Edit** button is available in the PGP Config Section
3. When the user clicks **Edit**, they can upload valid PGP keys



**MFT Settings**

**PGP Configuration for Workflows**

Active PGP Config

Private Key \*

Public Key \*

Expiration Timestamp

Passphrase Secret Key \*

**SFTP Configuration**

Active SSH Config

Powered by Backflipt TIQ\_ORCH\_v1.9.5

**MFT Settings**

**PGP Configuration for Workflows**

Active PGP Config

Private Key \*

Public Key \*

Expiration Timestamp

Passphrase Secret Key \*

**SFTP Configuration**

Active SSH Config

Powered by Backflipt TIQ\_ORCH\_v1.9.5

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

## PGP Configuration

### PGP Encryption Public Key:

This is a **publicly shared key** used for file encryption.

1. When a partner needs to send files to the company, the company provides this public key in the *Account Creation Successful* email.



2. The partner uses this public key to encrypt files on their end, ensuring that the files can only be decrypted by the company.
3. 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.

1. The company keeps this key secure and never shares it.
2. When encrypted files are received from a partner, the company uses this private key to decrypt and access the file's contents.
3. 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.

1. The passphrase must be entered whenever the private key is used for decryption.
2. This prevents unauthorized use of the private key, even if someone gains access to the key file.
3. It ensures end-to-end data confidentiality by adding another authentication step.

## **SFTP Configuration**

1. Navigate to the SFTP Config to upload SSH keys
2. At the top right, an **Edit** button is available in the SFTP Config Section
3. When the user clicks **Edit**, Super Admin can upload valid SSH keys

Below are the Fields Available in SFTP Config Section

### **SSH Login Public Key:**

This is the **public part of the SSH key pair** used for server authentication.

1. The company shares this public key with the partner in the *Account Creation Successful* email.
2. The partner adds this public key to their server's authorized keys list.
3. Once configured, it allows the company to log in securely to the partner 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.

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

### **Key Rotation for SFTP**

Key rotation in MFT for SFTP is the process of periodically replacing old SSH and PGP keys with new ones to maintain secure authentication, encryption, and uninterrupted file transfers.

### **Company Keys Rotation**

When a company decides to migrate or rotate keys in an MFT system, the company replaces their old SSH and/or PGP keys with new ones. The process begins by generating a new key pair. For SSH, this ensures secure server login, and for PGP, it ensures continued file encryption and decryption.

After generating the new keys, the company shares the **new public keys** with all required partners—SSH public keys are added to the partner's SFTP server for authentication, and PGP public keys are shared so partners can encrypt files using the new key. Then, the company updates the application with the **new private keys** so the system can authenticate (SSH) and decrypt incoming files (PGP).

### **Company PGP Key Rotation**

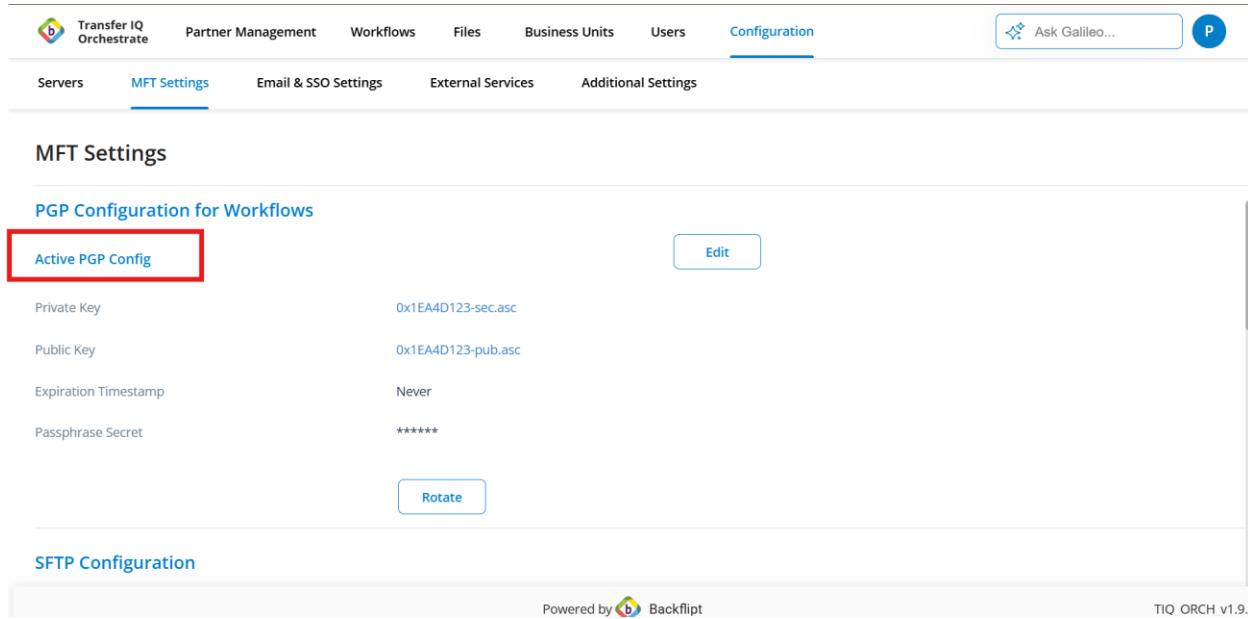
The process involves three distinct phases: **Before Rotation**, **During Rotation**, and **Deprecation**

Before rotation, only the **Active PGP Keys** section is visible, displaying the currently in-use keys.



## 1. Before Rotation

At this stage, the system continues to rely solely on the active keys for all ongoing file transfers and workflow executions.



The screenshot shows the 'MFT Settings' page in the Transfer IQ Orchestrator. The 'Active PGP Config' section is highlighted with a red box. The configuration table includes:

Setting	Value
Private Key	0x1EA4D123-sec.asc
Public Key	0x1EA4D123-pub.asc
Expiration Timestamp	Never
Passphrase Secret	*****

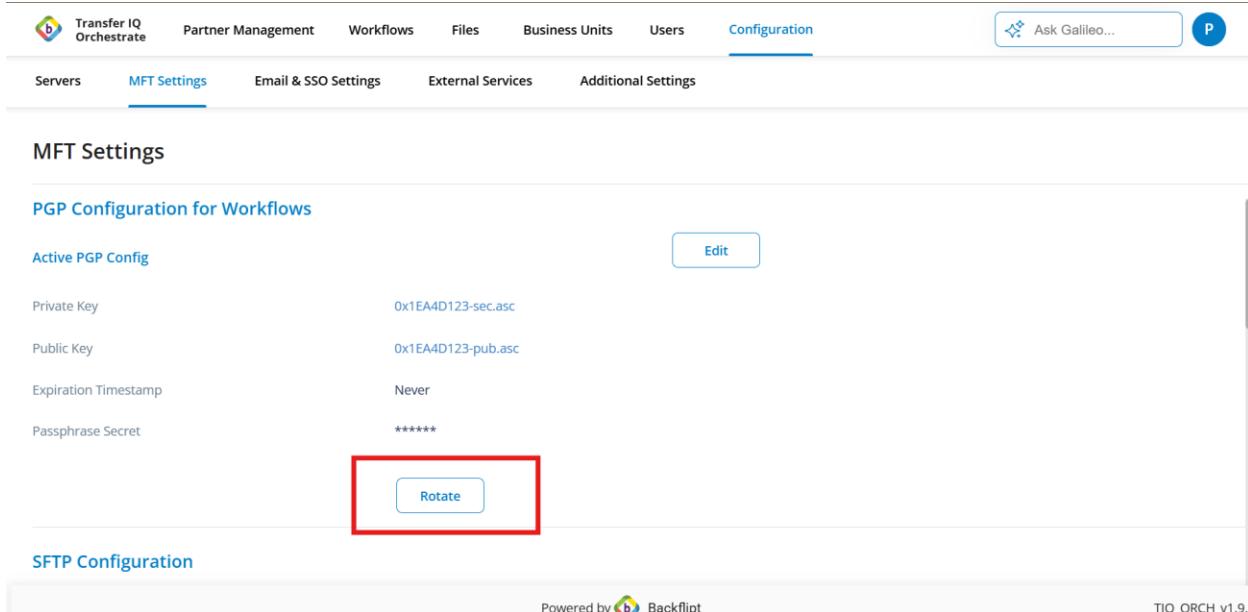
Below the table is a 'Rotate' button. The page also includes sections for 'PGP Configuration for Workflows' and 'SFTP Configuration'.

## 2. During Rotation

To begin the rotation process

1. Navigate to **MFT Settings > Active PGP Keys**.
2. Click the **Rotate** button located next to the *Active PGP Keys* section





Transfer IQ Orchestrator

Partner Management Workflows Files Business Units Users Configuration

Ask Galileo... P

Servers MFT Settings Email & SSO Settings External Services Additional Settings

## MFT Settings

### PGP Configuration for Workflows

Active PGP Config

Edit

Private Key	0x1EA4D123-sec.asc
Public Key	0x1EA4D123-pub.asc
Expiration Timestamp	Never
Passphrase Secret	*****

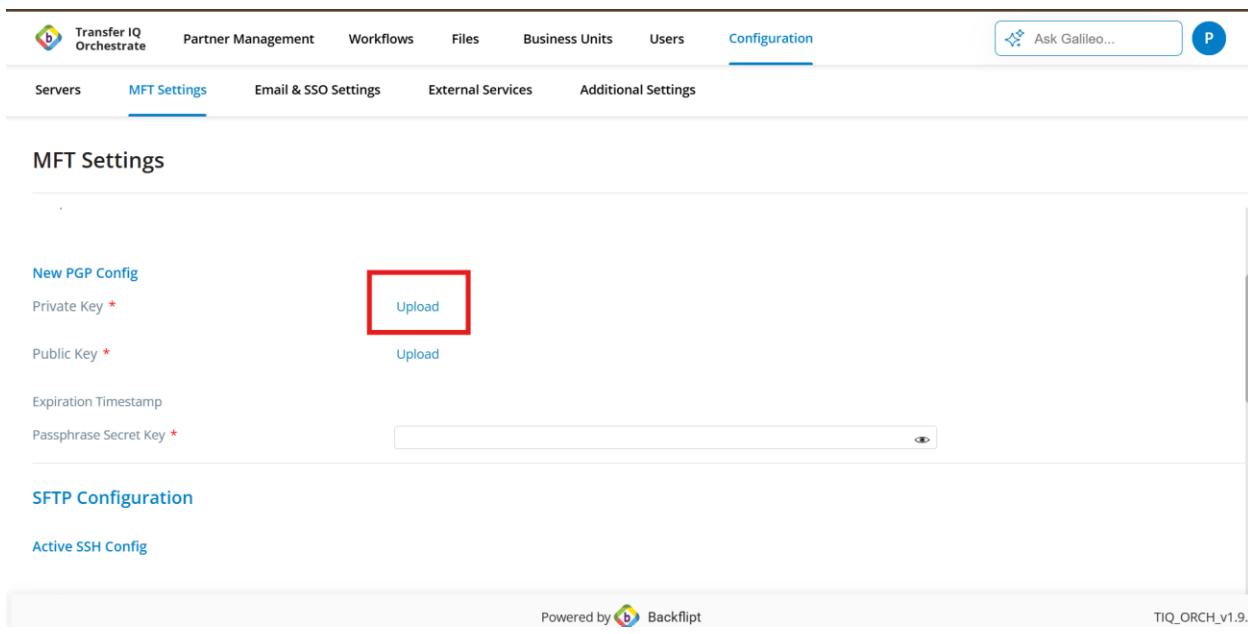
**Rotate**

### SFTP Configuration

Powered by  Backflift

TIQ\_ORCH\_v1.9.5

3. This action displays an additional section labeled **New PGP Keys**, which includes fields for uploading both **public** and **private** PGP keys along with the corresponding **passphrase**.
4. To upload the new keys, click the **Upload** button under the **New PGP Keys** section.



Transfer IQ Orchestrator

Partner Management Workflows Files Business Units Users Configuration

Ask Galileo... P

Servers MFT Settings Email & SSO Settings External Services Additional Settings

## MFT Settings

### New PGP Config

Private Key *	<b>Upload</b>
Public Key *	Upload
Expiration Timestamp	
Passphrase Secret Key *	<input type="text"/>

### SFTP Configuration

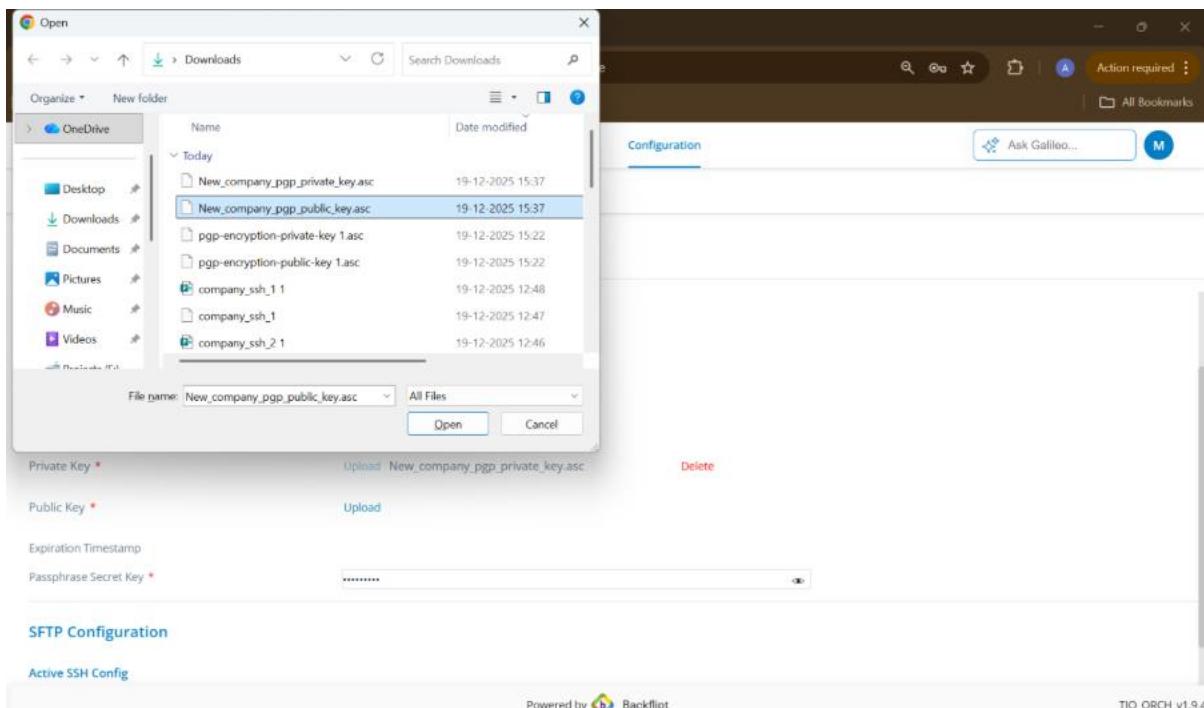
### Active SSH Config

Powered by  Backflift

TIQ\_ORCH\_v1.9.5

5. In the file selection dialog, choose a valid PGP key file.





- Once the file is uploaded successfully, the newly uploaded keys are displayed in the **MFT Settings** tab under the **New PGP Keys** section with an expiration timestamp.

**New PGP Config**

Private Key \*

Public Key \*

Expiration Timestamp

Passphrase Secret Key \*

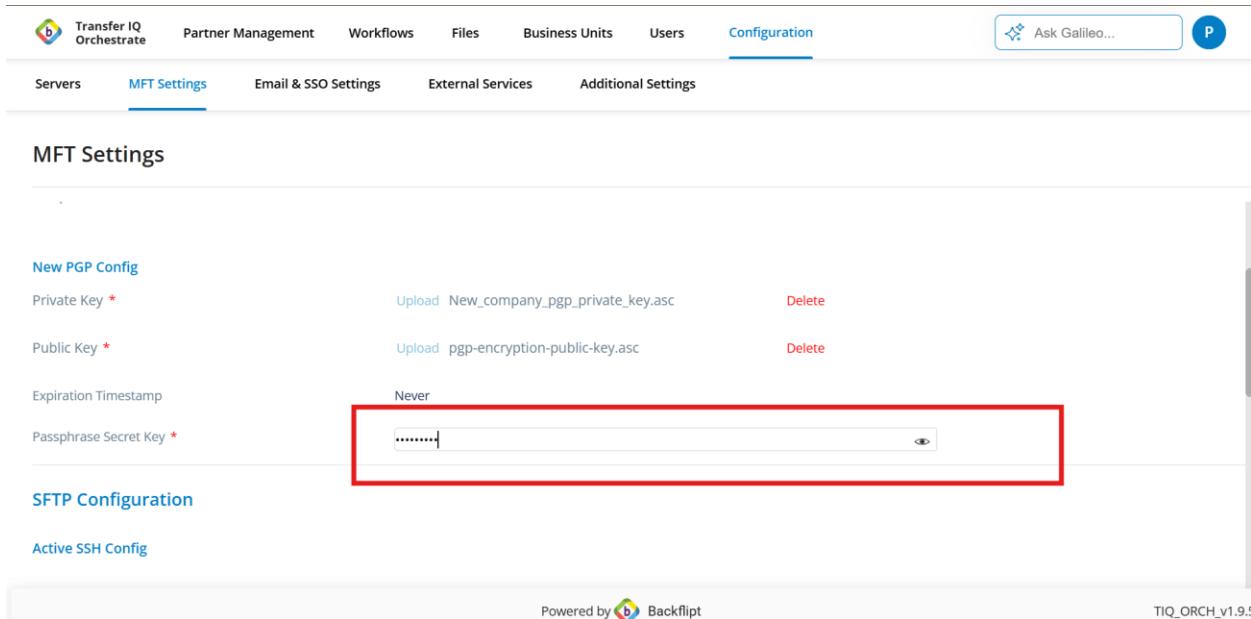
**SFTP Configuration**

**Active SSH Config**

Powered by Backflip TIQ\_ORCH\_v1.9.5

- Enter a valid passphrase in the Passphrase Secret Key Field





New PGP Config

Private Key \*

Upload New\_company\_pgp\_private\_key.asc Delete

Public Key \*

Upload pgp-encryption-public-key.asc Delete

Expiration Timestamp

Never

Passphrase Secret Key \*

.....|

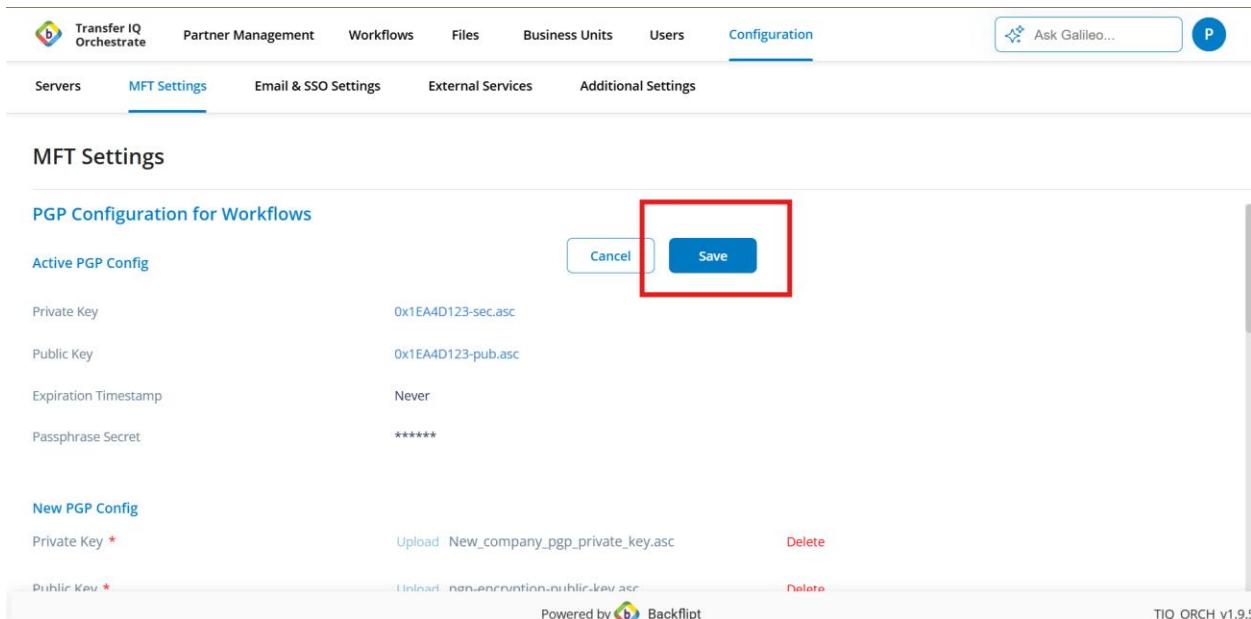
SFTP Configuration

Active SSH Config

Powered by  Backflip

TIQ\_ORCH\_v1.9.5

8. Click **Save**. Once saved, all uploaded keys and their passphrases will be displayed under the **New PGP Config** section in *View* mode. The previously active (old) keys will be shown with a **Deprecate** button.



Transfer IQ Orchestrator Partner Management Workflows Files Business Units Users Configuration

Ask Galileo... P

Servers MFT Settings Email & SSO Settings External Services Additional Settings

MFT Settings

PGP Configuration for Workflows

Active PGP Config

Cancel Save

Private Key 0x1EA4D123-sec.asc

Public Key 0x1EA4D123-pub.asc

Expiration Timestamp Never

Passphrase Secret \*\*\*\*\*

New PGP Config

Private Key \*

Upload New\_company\_pgp\_private\_key.asc Delete

Public Key \*

Upload pgp-encryption-public-key.asc Delete

Powered by  Backflip

TIQ\_ORCH\_v1.9.5



## File Transfer Behavior During Rotation

1. During PGP key rotation, if a partner sends an encrypted file and the workflow configuration includes a PGP decrypt step
2. The decryption step uses a fallback mechanism to ensure successful decryption.
3. The system first attempts to decrypt the file using the **new PGP private key**.
4. If decryption with the New Private key fails because the partner continues to use the old key, decryption is then automatically attempted using the previously active (old) PGP key.
5. This approach enables seamless file processing during the transition period, accommodating partners who have not yet switched to the new key.

This alternating validation process — where the system switches between new and old keys — is referred to as the **ping-pong mechanism**.

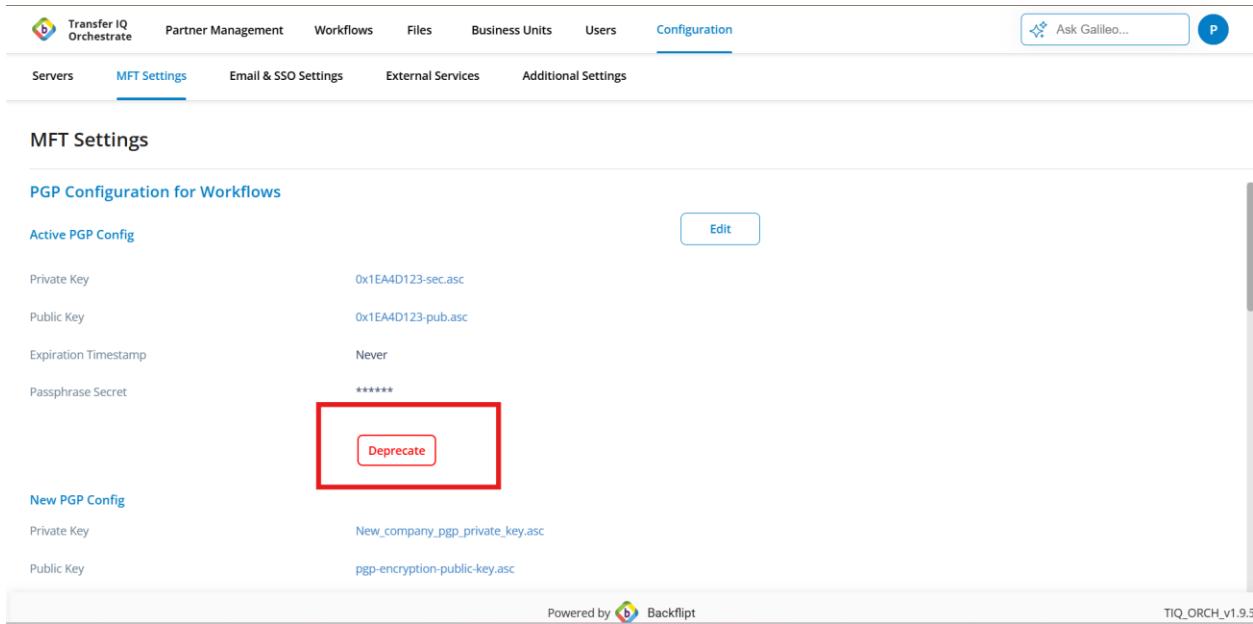
## PGP Key Deprecation

Deprecating a PGP key means disabling the old PGP key, so it can no longer encrypt or decrypt files, ensuring that only the newly rotated PGP key is used for secure file transfers.

### Deprecating PGP Keys

1. Navigate to the **Active PGP Keys** section in the MFT Settings tab.
2. Click the **Deprecate** button next to the old active **PGP** key.





Transfer IQ Orchestrate

Partner Management Workflows Files Business Units Users Configuration

Ask Galileo... P

Servers MFT Settings Email & SSO Settings External Services Additional Settings

## MFT Settings

### PGP Configuration for Workflows

Active PGP Config

Private Key: 0x1EA4D123-sec.asc  
Public Key: 0x1EA4D123-pub.asc  
Expiration Timestamp: Never  
Passphrase Secret: \*\*\*\*\*

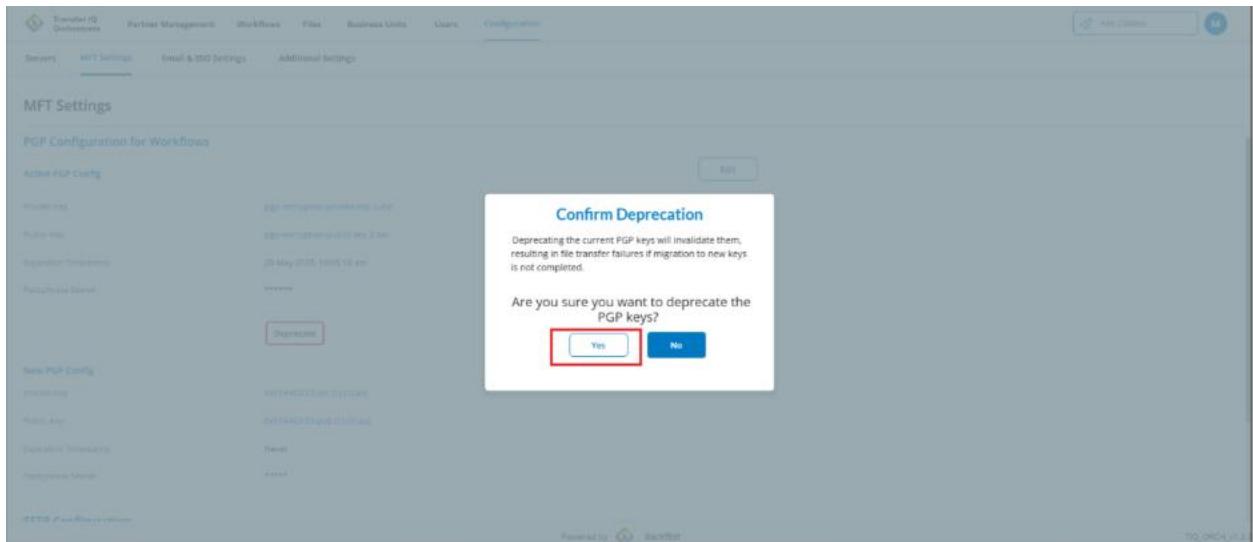
New PGP Config

Private Key: New\_company\_pgp\_private\_key.asc  
Public Key: pgp-encryption-public-key.asc

Powered by  Backflipt

TIQ\_ORCH\_v1.9.5

3. A **popup** is displayed asking for confirmation to deprecate the selected key.
4. Confirm the action by clicking the **Yes button** in the popup. The system marks the key as **deprecated**, indicating it is no longer active for encrypting or decrypting new files.



Transfer IQ Orchestrate

Partner Management Workflows Files Business Units Users Configuration

Ask Galileo... M

Servers MFT Settings Email & SSO Settings Additional Settings

## MFT Settings

### PGP Configuration for Workflows

Active PGP Config

Private Key: pgp-encryption-public-key.asc  
Public Key: pgp-encryption-public-key (key 2 sec)  
Expiration Timestamp: 29 May 2016, 10:05:18 am  
Passphrase Secret: \*\*\*\*\*

New PGP Config

Private Key: New\_company\_pgp\_private\_key.asc  
Public Key: 0x1EA4D123-pub.asc  
Expiration Timestamp: Never  
Passphrase Secret: \*\*\*\*\*

Powered by  Backflipt

TIQ\_ORCH\_v1.9.5

5. The deprecated key is **removed completely** from the application.



## File Transfer Behavior During Deprecation

1. Once a PGP key is **deprecated**, it is **removed from the system** and will **no longer be used** for decrypting any files.
2. Files encrypted with the **new PGP key** continue to be decrypted using the new key.
3. Any file encrypted with the old, deprecated key will **fail to decrypt**, ensuring only the current active key is used.

## Company SSH Key Rotation

SSH key rotation ensures secure and continuous connectivity between MFT and partner servers using SFTP connectors. The process involves three distinct phases: **Before Rotation**, **During Rotation**, and **Deprecation**.

### 1. Before Rotation

Before initiating the key rotation process, only the **active set of SSH keys** currently in use are visible under the *MFT Settings > Active SSH Keys* section.

These keys represent the ones actively used for establishing secure SFTP connections with partner servers.



Expiration Timestamp: Never

Passphrase Secret: \*\*\*\*\*

Rotate

Active SSH Config

Public Key: company\_ssh\_1 1.pub

Private Key: company\_ssh\_1

Rotate

Powered by Backflift

TIQ\_ORCH\_v1.9.5

At this stage, the system continues to rely solely on the active keys for all ongoing file transfers and workflow executions.

## 2. During Rotation

1. Navigate to **MFT Settings > Active SSH Keys**.
2. Click the **Rotate** button next to the *Active SSH Keys* section.

Expiration Timestamp: Never

Passphrase Secret: \*\*\*\*\*

Rotate

Active SSH Config

Public Key: company\_ssh\_1 1.pub

Private Key: company\_ssh\_1

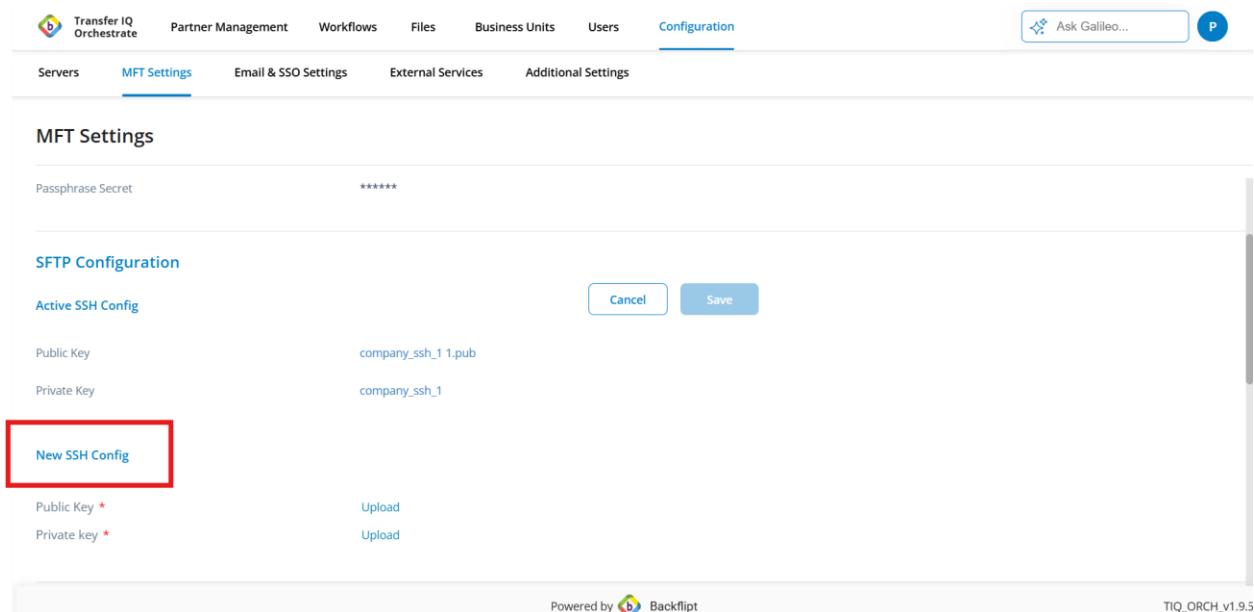
Rotate

Powered by Backflift

TIQ\_ORCH\_v1.9.5

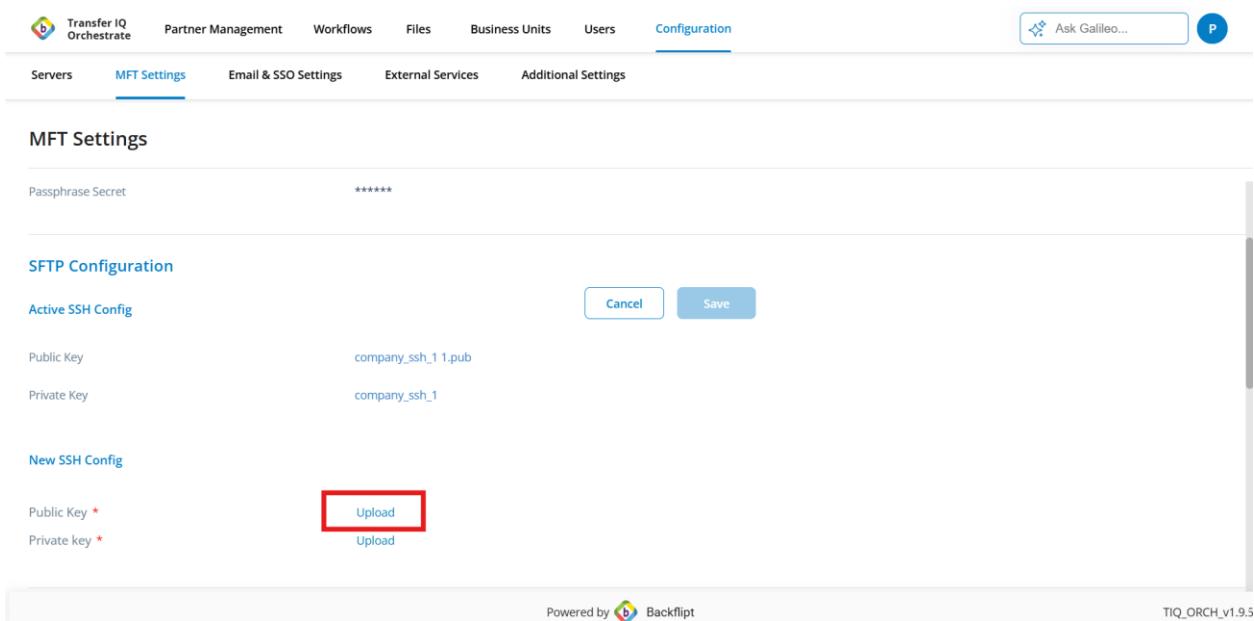


This action reveals a new section labeled **New SSH Keys**, which allows you to upload the **public** and **private** SSH keys for the new key pair.



The screenshot shows the 'MFT Settings' page under the 'Configuration' tab. The 'Active SSH Config' section is visible, showing a public key named 'company\_ssh\_1 1.pub' and a private key named 'company\_ssh\_1'. A red box highlights the 'New SSH Config' section. Under 'New SSH Config', there are fields for 'Public Key \*' and 'Private key \*', each with an 'Upload' button. The 'Save' button is located in the top right of the 'Active SSH Config' section. The page is powered by Backflip and version TIQ\_ORCH\_v1.9.5.

3. Under the **New SSH Keys** section, click **Upload** and select a valid SSH key file.



The screenshot shows the 'MFT Settings' page under the 'Configuration' tab. The 'Active SSH Config' section is visible, showing a public key named 'company\_ssh\_1 1.pub' and a private key named 'company\_ssh\_1'. A red box highlights the 'Upload' button next to the 'Public Key \*' field in the 'New SSH Config' section. The 'Save' button is located in the top right of the 'Active SSH Config' section. The page is powered by Backflip and version TIQ\_ORCH\_v1.9.5.

4. Select and open a file from the file selection dialog box



File name: **New\_company\_ssh\_public\_key**

Public Key: ec2-sftp-server 1 1.pub

Private Key: ec2-sftp-server 1

New SSH Config

Public Key \*  ec2-sftp-server 1 1.pub

Private key \*  ec2-sftp-server 1

Powered by Backflift

TIQ\_ORCH\_v1.9.4

File name: **New\_company\_ssh\_private\_key**

Public Key: ec2-sftp-server 1 1.pub

Private Key: ec2-sftp-server 1

New SSH Config

Public Key \*  New\_company\_ssh\_public\_key.pub

Private key \*

Powered by Backflift

TIQ\_ORCH v1.9.4

- Once uploaded successfully, both **Active SSH Keys** and **New SSH Keys** will be displayed in the *MFT Settings* tab.



MFT Settings

Passphrase Secret \*\*\*\*\*

**SFTP Configuration**

Active SSH Config

Cancel Save

Public Key company\_ssh\_1 1.pub

Private Key company\_ssh\_1

New SSH Config

Public Key \* Upload New\_company\_ssh\_public\_key.pub Delete

Private key \* Upload New\_company\_ssh\_private\_key Delete

Powered by Backflip TIQ\_ORCH\_v1.9.5

## 6. Click the Save button to save the new SSH Keys

MFT Settings

Passphrase Secret \*\*\*\*\*

**SFTP Configuration**

Active SSH Config

Cancel Save

Public Key company\_ssh\_1 1.pub

Private Key company\_ssh\_1

New SSH Config

Public Key \* Upload New\_company\_ssh\_public\_key.pub Delete

Private key \* Upload New\_company\_ssh\_private\_key Delete

Powered by Backflip TIQ\_ORCH\_v1.9.5

- Once saved, all uploaded keys and their passphrases will be displayed under the **New SSH Config** section in **View mode**. The previously active (old) keys will be shown with a **Deprecate** button.



The screenshot shows the 'MFT Settings' page in the Transfer IQ Orchestrate interface. The 'New SSH Config' section is highlighted with a red box. It contains two key pairs: 'New SSH Config' (highlighted) and the 'Active SSH Config' (which is being deprecated). The 'Active SSH Config' section shows 'company\_ssh\_1 1.pub' and 'company\_ssh\_1'. A 'Deprecate' button is present in the 'Active SSH Config' section. The interface includes a 'Rotate' button, an 'Edit' button, and a 'Ask Galileo...' button.

## File Transfer Behavior During Rotation

When SSH key rotation is initiated, the system determines which key to use for establishing the SFTP connection through a validation mechanism:

1. The system first attempts to establish the SFTP connection using the **new SSH key** uploaded under *MFT Settings*.
2. If the connection is **successful**, the corresponding connector's SSH private key is automatically updated with the **new key**, and all future connections will continue to use this new key.
3. If the connection **fails** with the new key, the system retries using the **existing (old) key**.
4. If the connection is **successful** with the old key, the connector continues using the old SSH key.
  - a. For **subsequent connection attempts**, the system will **prioritize the key that was last successful** (in this case, the old key) before trying the other key again.

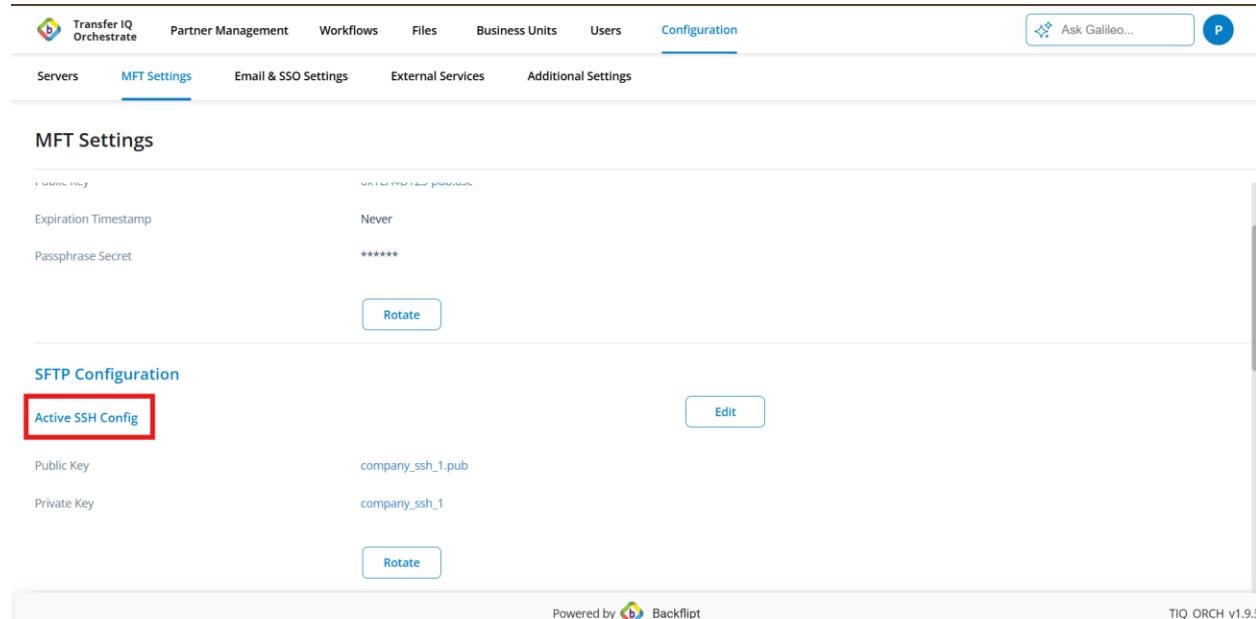
This alternating validation process — where the system switches between new and old keys based on connection success — is referred to as the **ping-pong mechanism**.

## 3. Deprecation (post-rotation)



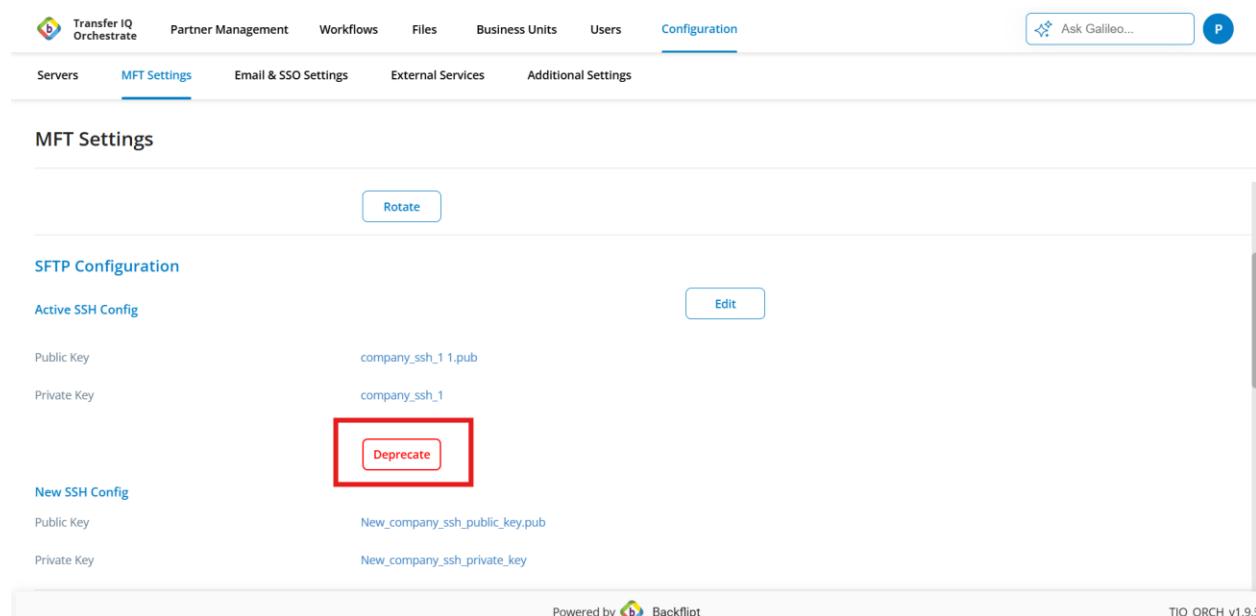
Once the new SSH keys are validated and successfully in use, the **old keys are deprecated**.

1. Navigate to the **Active SSH Keys** section in the *MFT Settings* tab.



The screenshot shows the 'MFT Settings' tab selected in the navigation bar. Under 'SFTP Configuration', the 'Active SSH Config' section is highlighted with a red box. It displays two key pairs: 'Public Key' (company\_ssh\_1.pub) and 'Private Key' (company\_ssh\_1). A 'Rotate' button is located below the keys. An 'Edit' button is also present. The page footer indicates 'Powered by Backflift' and 'TIQ ORCH v1.9.5'.

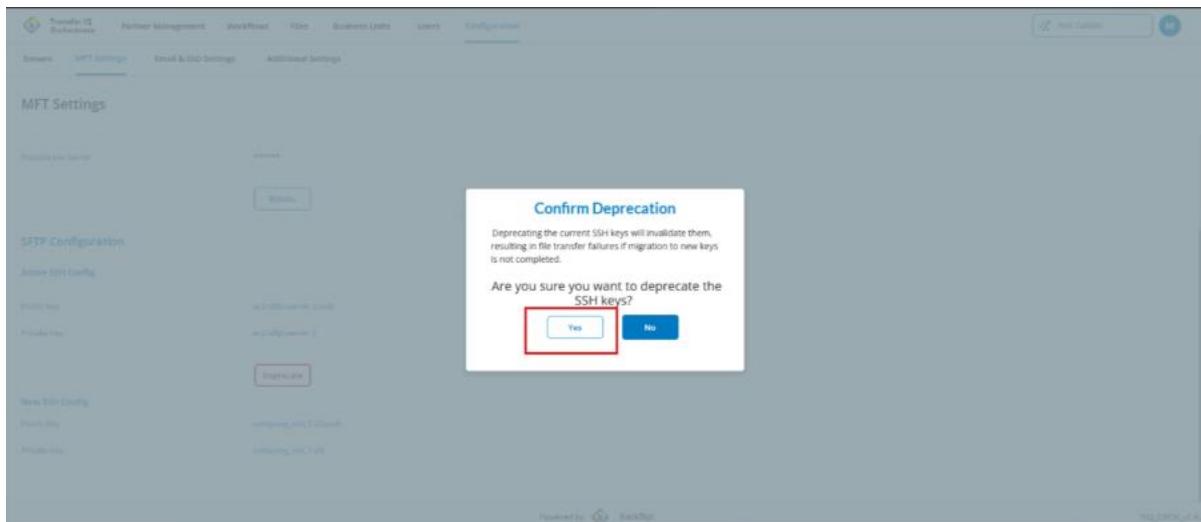
2. Click the **Deprecate** button next to the old active SSH key.



The screenshot shows the 'MFT Settings' tab selected. The 'Active SSH Config' section is visible, showing the same key pairs as the previous screenshot. A red box highlights the 'Deprecate' button next to the 'Private Key' entry. The page footer indicates 'Powered by Backflift' and 'TIQ\_ORCH\_v1.9.5'.

3. A confirmation popup is displayed. Click **Yes** to confirm the deprecation of the selected key.





4. The system marks the key as deprecated, indicating it is no longer active for establishing SFTP connections.
5. The deprecated key is removed completely from the application.

**MFT Settings**

Expiration Timestamp: Never

Passphrase Secret: \*\*\*\*\*

**SFTP Configuration**

**Active SSH Config**

Public Key: New\_company\_ssh\_public\_key.pub

Private Key: New\_company\_ssh\_private\_key

Once the new SSH keys are validated and successfully in use, the old keys are deprecated. At this stage:

- The **Active SSH Keys** section in *MFT Settings* is updated to show only the newly active keys.



- All subsequent file transfers and SFTP connections use the rotated (new) SSH keys exclusively.

This ensures a smooth transition with no disruption to ongoing transfers while maintaining enhanced security.

## Custom Step Configuration:

### Configuring Authentication Token in MFT Settings Tab:

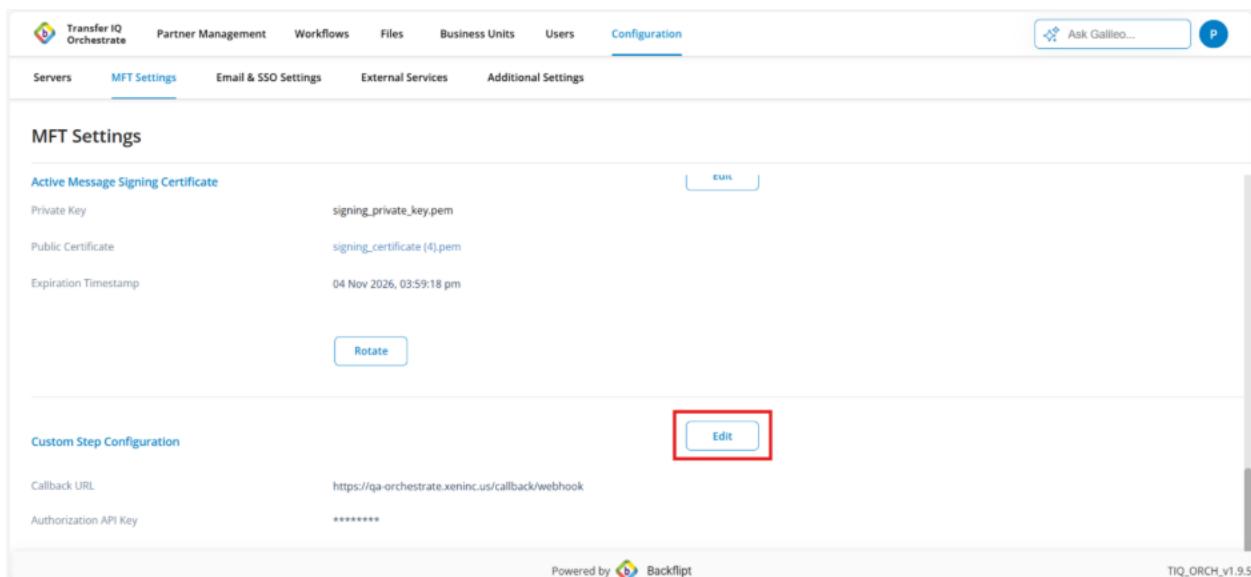
The callback URL and authentication key, which the company uses to receive responses from the external service, will be specified in the Custom step Configuration section of the MFT settings tab

This section consists of two input fields:

- Callback URL – This field is pre-populated with a default value when the Orchestrate application is deployed.
- Authentication Token – The company provides the authentication token in this field.

To configure customs step configuration, follow the below steps

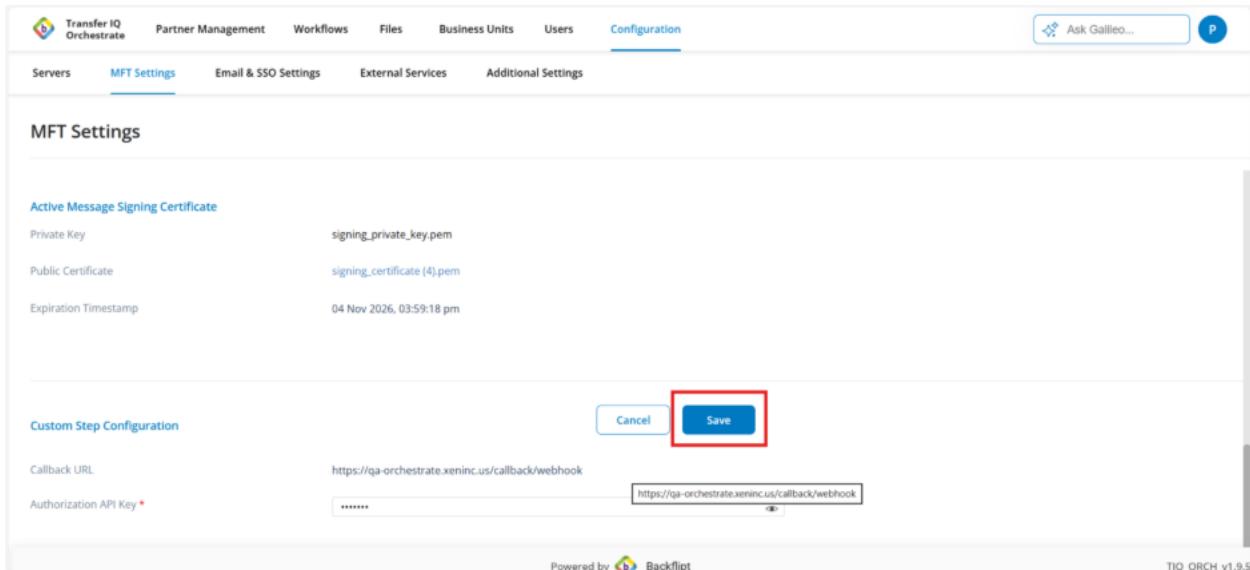
1. Navigate to Configuration > MFT Settings
2. Navigate to Custom Step Configuration in MFT Settings Tab
3. Click edit to enter the authentication token



The screenshot shows the 'MFT Settings' tab selected in the navigation bar. The 'Custom Step Configuration' section is visible, containing fields for 'Callback URL' (set to <https://qa-orchestrate.xeninc.us/callback/webhook>) and 'Authorization API Key' (set to '\*\*\*\*\*'). A red box highlights the 'Edit' button in this section.

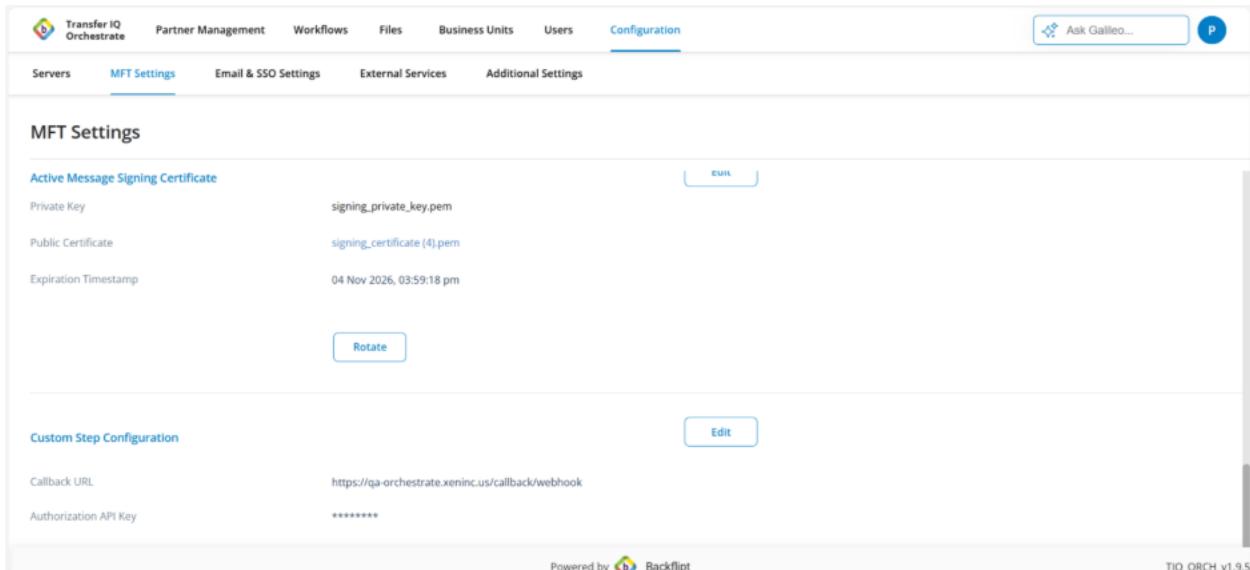


#### 4. Provide the authentication token and Click save



The screenshot shows the 'MFT Settings' page in the Transfer IQ Orchestrator interface. The 'Configuration' tab is selected. Under 'MFT Settings', there is a section for 'Active Message Signing Certificate' with fields for 'Private Key' (value: 'signing\_private\_key.pem'), 'Public Certificate' (value: 'signing\_certificate (4).pem'), and 'Expiration Timestamp' (value: '04 Nov 2026, 03:59:18 pm'). Below this is a 'Custom Step Configuration' section with 'Callback URL' (value: 'https://qa-orchestrate.xeninc.us/callback/webhook') and 'Authorization API Key' (value: '\*\*\*\*\*'). At the bottom right of this section is a 'Save' button, which is highlighted with a red box. Other buttons in the section are 'Cancel' and 'Edit'.

Once the details are saved, the details will be displayed in the **View** mode, with the authentication token masked.



The screenshot shows the 'MFT Settings' page in the Transfer IQ Orchestrator interface, but in 'View' mode. The layout is identical to the 'Edit' mode screenshot above, but the 'Authorization API Key' field now contains '\*\*\*\*\*' instead of the original value, indicating it is masked. The 'Save' button is also present but is not highlighted.

### Configuring Callback Time:

- When an external service is invoked, it may return either a **success** or **failure** response based on how the request is processed.

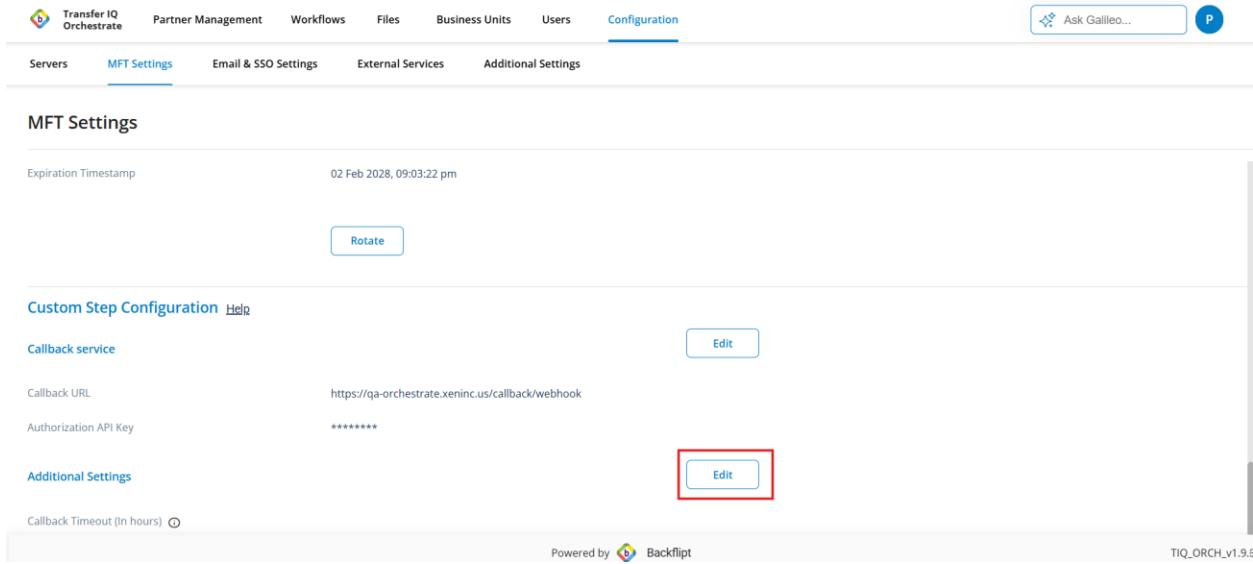


- If no response is received from the external service, the workflow transitions into a **suspended** state.
- In the suspended state, workflow execution is **paused**, and no further steps are processed until a response is received or manual action is taken.
- While suspended, the workflow status is displayed as “**Waiting for Response**” in the **Track tab**.
- The application waits for a callback from the external service based on the **callback time** configured in the **Additional Settings** section of the custom step configuration.
- The **Additional Settings** section allows configuration of the callback time in **hours**.
- When the workflow enters the suspended state, the record is **displayed immediately** in the Track tab with the status “**Waiting for Response.**”
- The system continues to wait for the external service response for the duration specified in the callback time in hours.
- Once the configured callback time is reached, the Track tab displays the available actions:
  - **Retry**
  - **Continue to Next Step**
  - **Terminate Workflow** (mark as failure)
- These actions allow **admins** to manually decide how the suspended workflow should proceed.

#### To configure the callback time, follow the below steps

1. Navigate to Configuration > MFT Settings > Custom Step Configuration
2. Navigate to Additional Settings Sections in Custom Step Configuration
3. Click the Edit button





Transfer IQ Orchestrate

Partner Management Workflows Files Business Units Users Configuration

Ask Galileo... P

Servers MFT Settings Email & SSO Settings External Services Additional Settings

### MFT Settings

Expiration Timestamp 02 Feb 2028, 09:03:22 pm

Rotate

Custom Step Configuration Help

Callback service

Callback URL https://qa-orchestrate.xeninc.us/callback/webhook

Authorization API Key \*\*\*\*\*

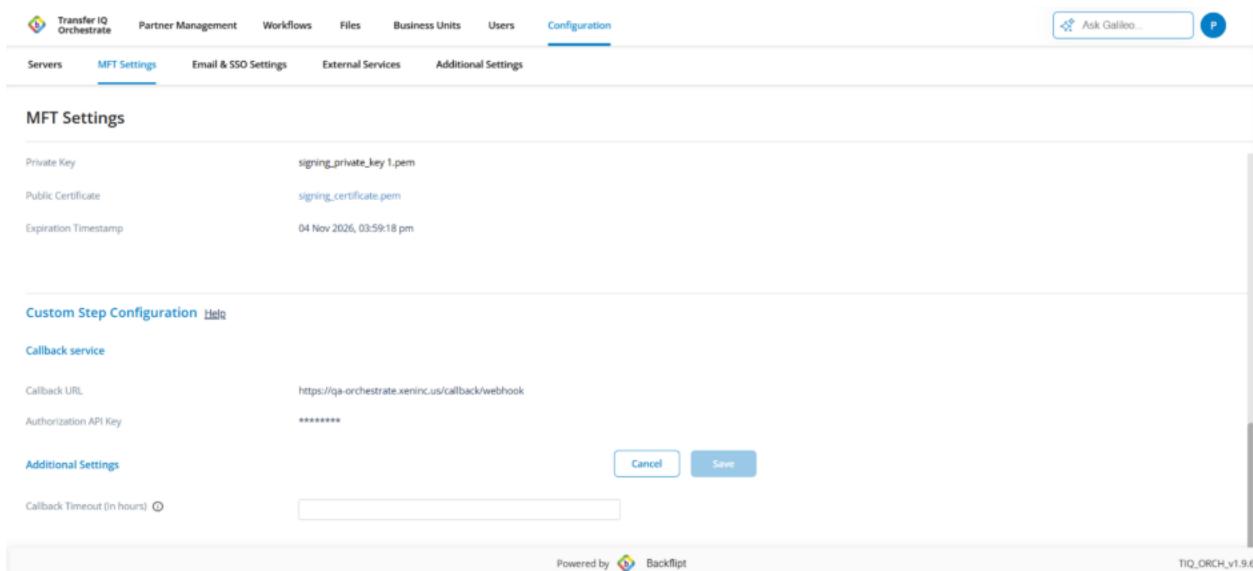
Additional Settings

Callback Timeout (in hours)

Powered by Backflip

TIQ\_ORCH\_v1.9.5

#### 4. Configure the Callback Time in hours



Transfer IQ Orchestrate

Partner Management Workflows Files Business Units Users Configuration

Ask Galileo... P

Servers MFT Settings Email & SSO Settings External Services Additional Settings

### MFT Settings

Private Key signing\_private\_key1.pem

Public Certificate signing\_certificate.pem

Expiration Timestamp 04 Nov 2026, 03:59:18 pm

Custom Step Configuration Help

Callback service

Callback URL https://qa-orchestrate.xeninc.us/callback/webhook

Authorization API Key \*\*\*\*\*

Additional Settings

Callback Timeout (in hours)

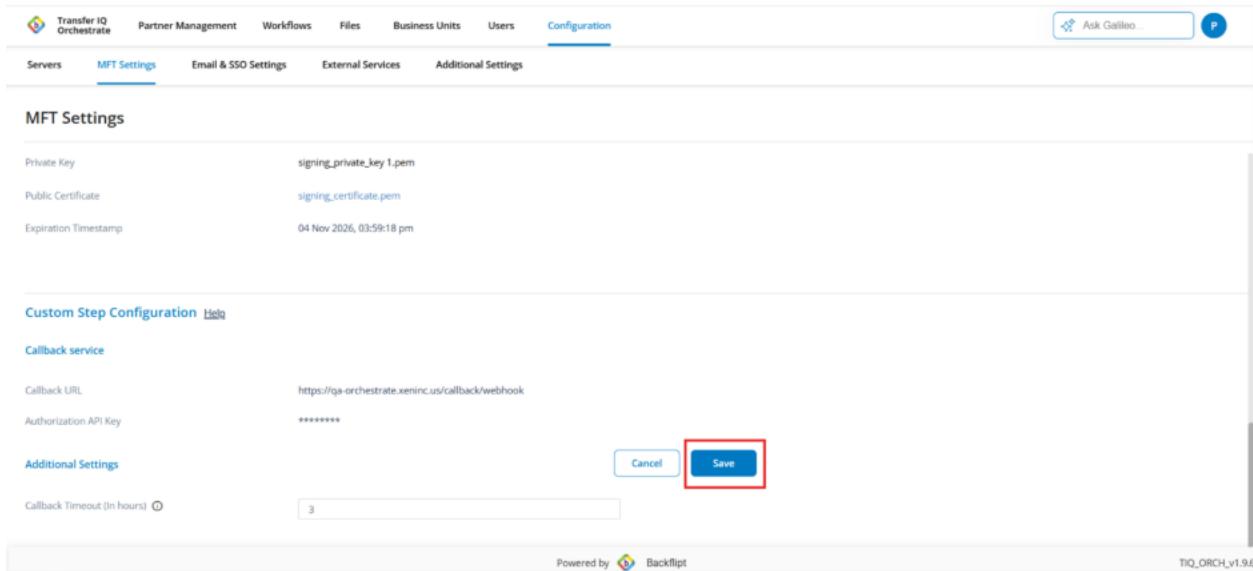
Cancel Save

Powered by Backflip

TIQ\_ORCH\_v1.9.6

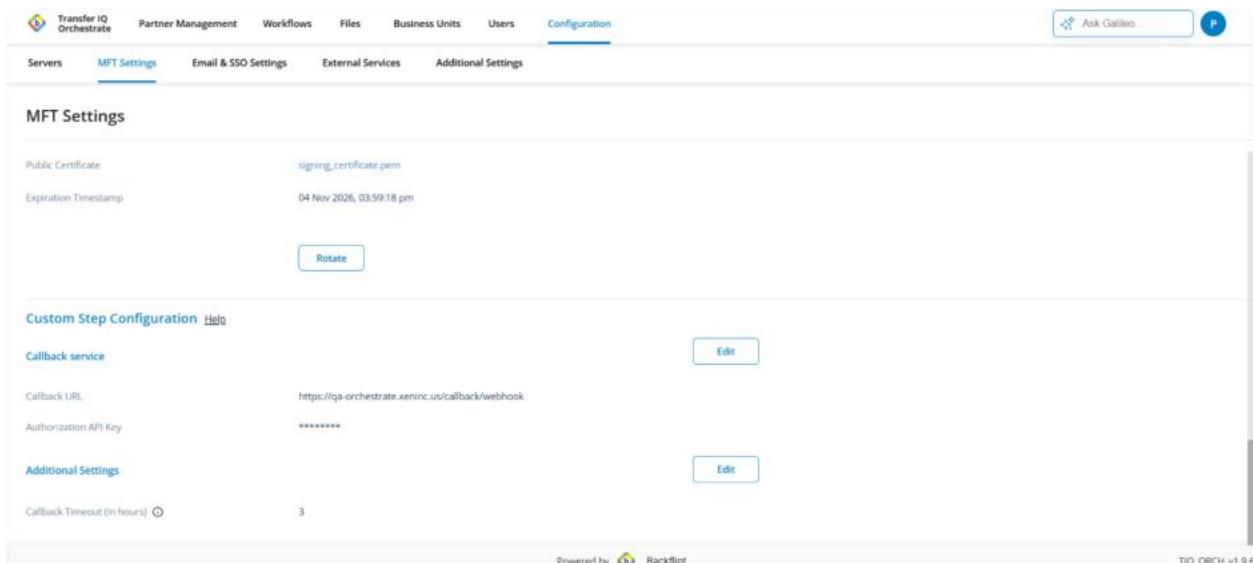
#### 5. Once configured, Click the Save





The screenshot shows the 'MFT Settings' page in the Transfer IQ Orchestrate interface. The 'Save' button is highlighted with a red box. Other visible elements include the 'Callback service' section with a 'Callback URL' of <https://qa-orchestrate.xeninc.us/callback/webhook> and an 'Authorization API Key' of '\*\*\*\*\*'. The 'Additional Settings' section shows a 'Callback Timeout (in hours)' of 3. The 'Save' button is located in the 'Custom Step Configuration' section.

## 6. Once saved the callback time will be displayed in view mode



The screenshot shows the 'MFT Settings' page in the Transfer IQ Orchestrate interface. The 'Edit' button for the 'Callback service' is highlighted with a red box. Other visible elements include the 'Callback service' section with a 'Callback URL' of <https://qa-orchestrate.xeninc.us/callback/webhook> and an 'Authorization API Key' of '\*\*\*\*\*'. The 'Additional Settings' section shows a 'Callback Timeout (in hours)' of 3. The 'Edit' button is located in the 'Custom Step Configuration' section.

**Note:** If the callback time is not configured, it will default to 2 hours.

## Callback API Help:

- Clicking the Help link in the Custom Step Configuration opens the Callback API Details popup.



- The purpose of this popup is to explain how the external service should notify the platform about the execution status of a request.
- It details the HTTP method and endpoint URL that the external service must use to send the callback.
- It describes the required headers, including the Authorization token, which is the same token specified in the Custom Step Configuration. This token authenticates the callback request.
- The popup also explains key request parameters used to communicate the execution status and link the callback with the original workflow request.
- This ensures the external service sends properly formatted and authenticated callback responses to the orchestrate



The screenshot shows the Xerion Platform Configuration interface. In the top navigation bar, the 'Configuration' tab is selected. Below it, the 'MFT Settings' section is active. A modal window titled 'Callback API Details' is open, containing the following details:

**Description**  
The Callback API is used by the external service to notify the platform about the execution status of a request. Once processing is completed (success or failure), the external service must invoke this API with the execution details.

**Request Details**

- HTTP Method: POST
- Endpoint: https://ga-orchestrate.xerion.us/callback/webhook

**Headers**

- Content-Type: application/json
- Authorization: Bearer <token>

**Request Body**  
The request body must be sent in JSON format and contain the execution status details.

```
{
  "status": "success" | "failure",
  "message": "Process completed successfully",
  "execution_id": "1234567890abcdef1234567890abcdef"
}
```

**Request Parameters Explanation**

Field Name	Description
token	Bearer token used for authenticating the callback request. It must be passed in the Authorization header.
status	Indicates the execution status. Possible values include SUCCESS, FAILED.
message	Human-readable message describing the execution result or failure reason.
execution_id	Unique identifier of the execution generated during the initial request. Used to correlate the callback with the original request.

## AS2 Protocol

When only the **AS2 protocol is deployed**, clicking on *MFT Settings* in the Configuration tab will navigate to the MFT Settings section, where only the Message Encryption Certificates and Message Signing Certificates are present as certificates.

By default, the page shows an empty state with the following fields in AS2 Server Configuration:

It includes the following sections:

1. Local Profile
2. Active Message Encryption Certificates
3. Active Message Signing Certificates



The screenshot shows the 'MFT Settings' section of the Transfer IQ Orchestrator interface. The 'Local Profile' tab is selected. A 'Create' button is visible. The configuration fields for a local profile include 'Profile Name' and 'AS2 ID'. Below these, there are sections for 'Active Message Encryption Certificate' and 'Active Message Signing Certificate', each with an 'Edit' button. The bottom of the page includes a 'Powered by Backflip' footer and a version number 'TIO\_ORCH\_v1.9.5'.

## Local Profile:

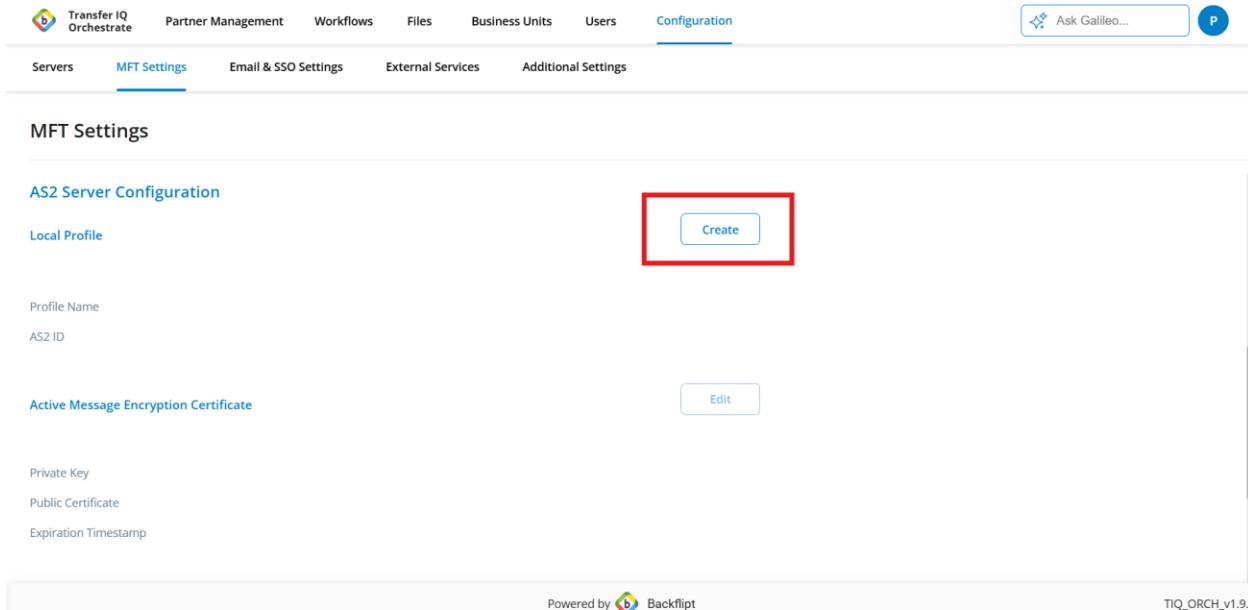
The **Local Profile** defines the company's identity for AS2 communication. It includes the following fields:

- **Profile Name**
- **AS2 ID**

### Creating the Local Profile

1. Navigate to **Configuration** → **MFT Settings** → **Local Profile**.
2. The page appears blank when no profile is configured.
3. Click Create





Transfer IQ Orchestrator

Partner Management Workflows Files Business Units Users Configuration

Servers MFT Settings Email & SSO Settings External Services Additional Settings

## MFT Settings

### AS2 Server Configuration

Local Profile

Create

Profile Name

AS2 ID

Active Message Encryption Certificate

Edit

Private Key

Public Certificate

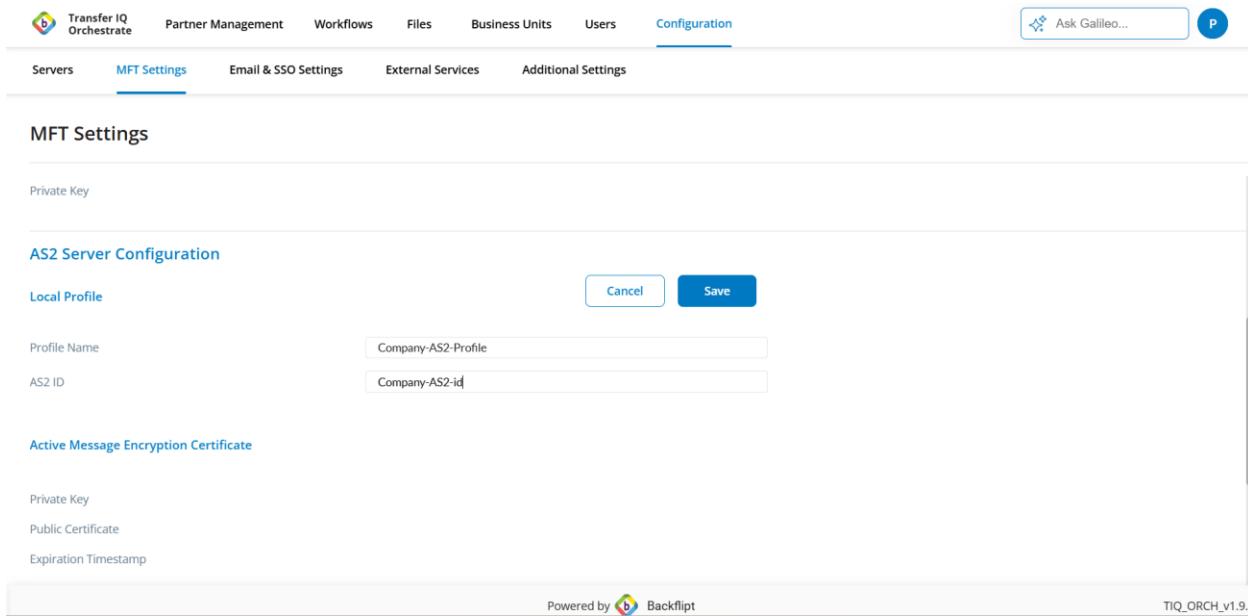
Expiration Timestamp

Powered by Backflip

TIQ\_ORCH\_v1.9.5

4. Enter the following details:

- Profile Name
- AS2 ID



Transfer IQ Orchestrator

Partner Management Workflows Files Business Units Users Configuration

Servers MFT Settings Email & SSO Settings External Services Additional Settings

## MFT Settings

### AS2 Server Configuration

Local Profile

Cancel Save

Profile Name: Company-AS2-Profile

AS2 ID: Company-AS2-id

Active Message Encryption Certificate

Private Key

Public Certificate

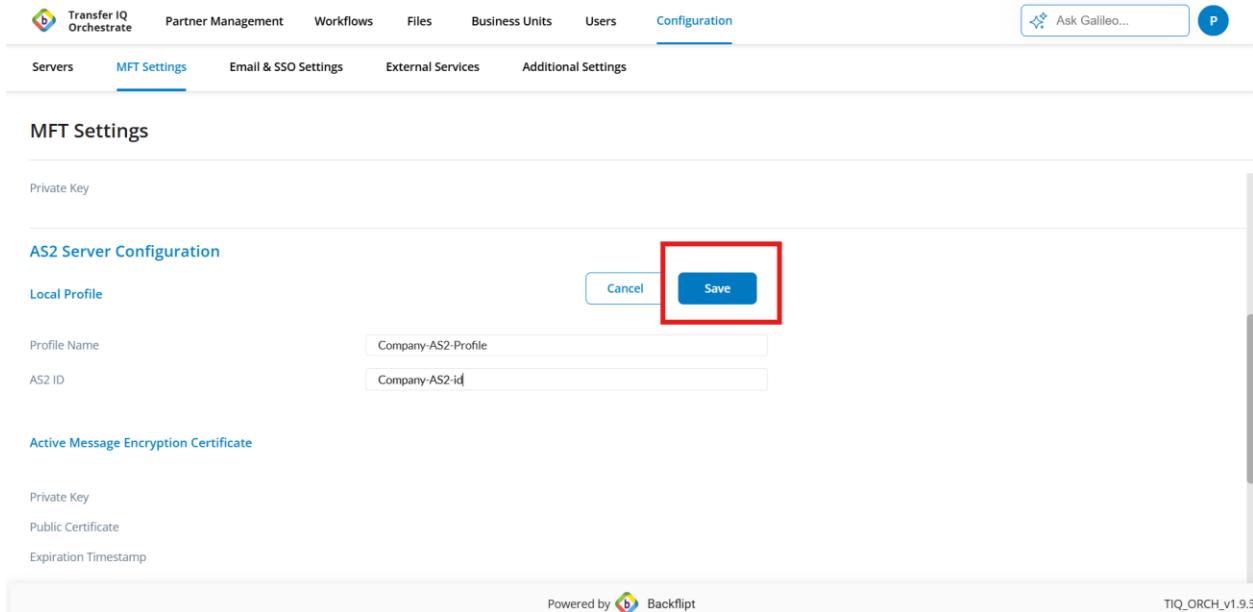
Expiration Timestamp

Powered by Backflip

TIQ\_ORCH\_v1.9.5

5. Click **Save**.





Transfer IQ Orchestrate

Partner Management Workflows Files Business Units Users Configuration

Servers MFT Settings Email & SSO Settings External Services Additional Settings

### MFT Settings

Private Key

#### AS2 Server Configuration

Local Profile

Profile Name: Company-AS2-Profile

AS2 ID: Company-AS2-id

Save

Cancel

#### Active Message Encryption Certificate

Private Key

Public Certificate

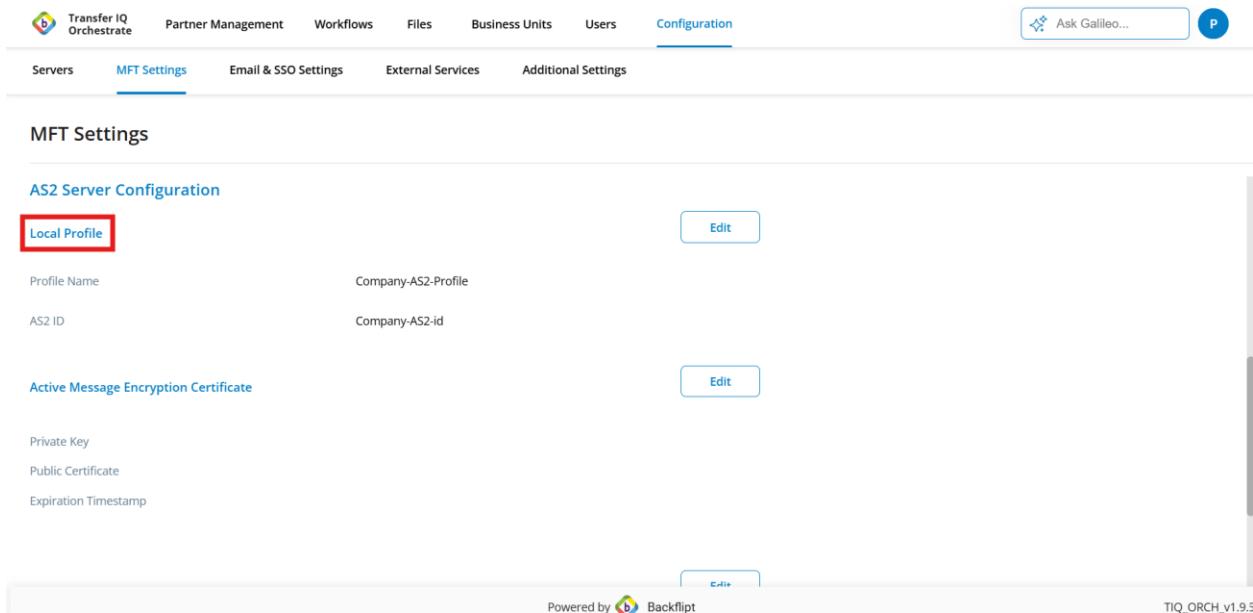
Expiration Timestamp

Powered by  Backflipt

TIQ\_ORCH\_v1.9.5

## Outcome:

1. The Local Profile is created in the application.



Transfer IQ Orchestrate

Partner Management Workflows Files Business Units Users Configuration

Servers MFT Settings Email & SSO Settings External Services Additional Settings

### MFT Settings

#### AS2 Server Configuration

Local Profile

Profile Name: Company-AS2-Profile

AS2 ID: Company-AS2-id

Edit

#### Active Message Encryption Certificate

Private Key

Public Certificate

Expiration Timestamp

Edit

Powered by  Backflipt

TIQ\_ORCH\_v1.9.5

2. The same profile is automatically created under **AWS Transfer Family → Servers** to maintain consistency between the application and AWS.



3. After creation, the **AS2 ID becomes locked and cannot be modified**.
4. A Local Profile **must be created before** configuring AS2 Agreements, as it represents the company during all AS2 exchanges.
5. The AS2 ID must be **unique**, as trading partners use this value to identify your company.

## Message Encryption Certificates

1. Navigate to the Message Encryption Certificates to upload Message Encryption Certificates
2. At the top right, an Edit button is available in the Message Encryption Certificates Section
3. When the user clicks **Edit**, Super Admin can upload valid Certificates by clicking the upload button.

MFT Settings

Active Message Encryption Certificate

Private Key

Public Certificate

Expiration Timestamp

Edit

4. This section contains of the below certificates:
  - a. Message Encryption Public Certificate
  - b. Message Encryption Private Key



## MFT Settings

Active Message Encryption Certificate

Private Key \*  Upload

Public Certificate \*  Upload

[Cancel](#) [Save](#)

Transfer IQ  
Orchestrator

Partner Management Workflows Files Business Units Users Configuration

Ask Galileo... [P](#)

Servers [MFT Settings](#) Email & SSO Settings External Services Additional Settings

## MFT Settings

Active Message Encryption Certificate

Private Key \*  Upload: encryption\_private\_key.pem [Delete](#)

Public Certificate \*  Upload: encryption\_certificate (2).pem [Delete](#)

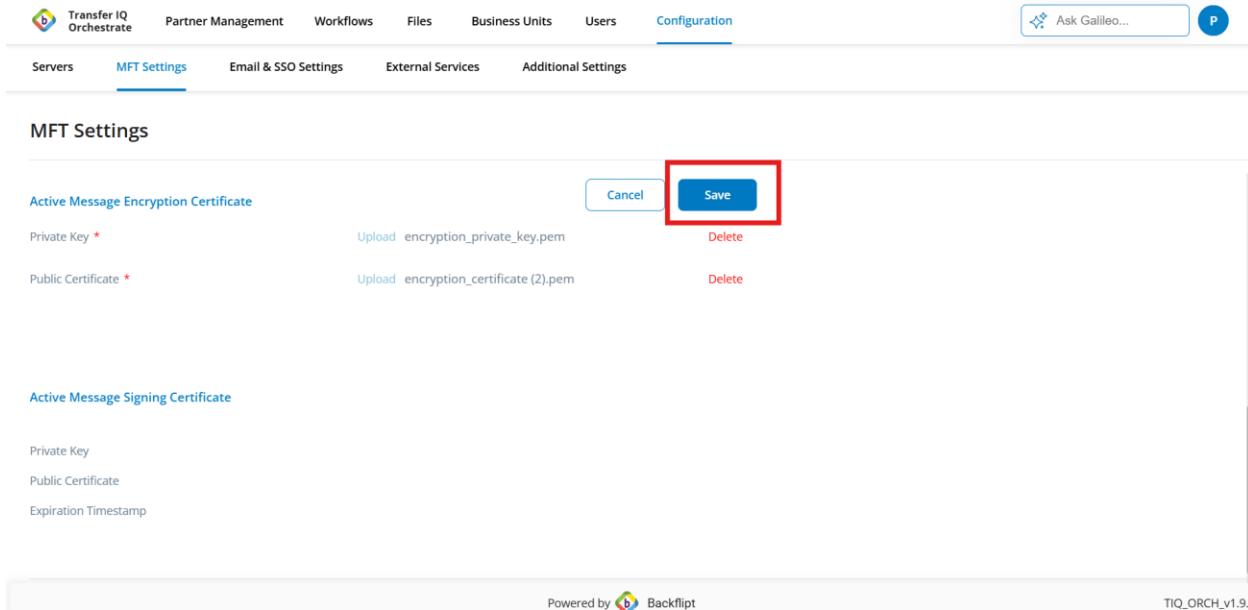
Active Message Signing Certificate

Private Key  
Public Certificate  
Expiration Timestamp

Powered by  Backflift TIQ\_ORCH\_v1.9.5

5. Click Save





Transfer IQ Orchestrate

Partner Management Workflows Files Business Units Users Configuration

Ask Galileo... P

Servers MFT Settings Email & SSO Settings External Services Additional Settings

### MFT Settings

Active Message Encryption Certificate

Private Key \* Upload encryption\_private\_key.pem Cancel Save Delete

Public Certificate \* Upload encryption\_certificate (2).pem Delete

Active Message Signing Certificate

Private Key

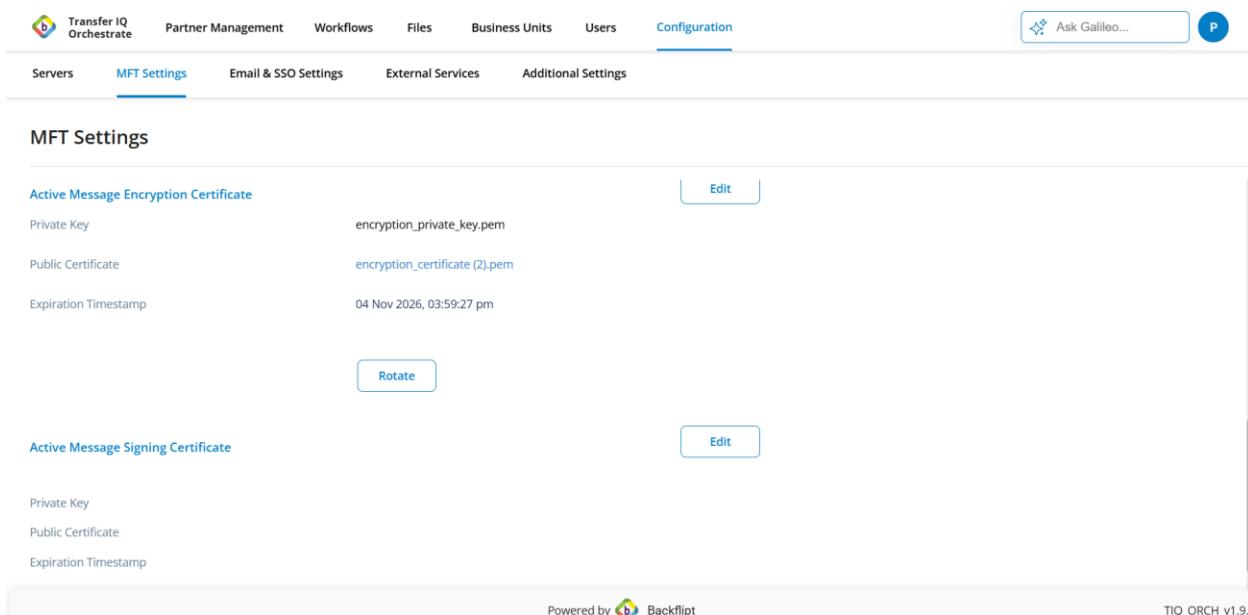
Public Certificate

Expiration Timestamp

Powered by Backflift

TIQ\_ORCH\_v1.9.5

6. Once the save button is clicked both the public and private encryption certificates will be merged into a single certificate and attached to the Local Profile



Transfer IQ Orchestrate

Partner Management Workflows Files Business Units Users Configuration

Ask Galileo... P

Servers MFT Settings Email & SSO Settings External Services Additional Settings

### MFT Settings

Active Message Encryption Certificate

Private Key encryption\_private\_key.pem Edit

Public Certificate encryption\_certificate (2).pem

Expiration Timestamp 04 Nov 2026, 03:59:27 pm

Rotate

Active Message Signing Certificate

Private Key

Public Certificate

Expiration Timestamp

Powered by Backflift

TIQ\_ORCH\_v1.9.5



Profile description

Name: Company-AS2-Profile AS2 ID: Company-AS2-Id

Profile type: LOCAL

Setup automated notifications for certificate(s) approaching expiry: To configure automated notifications when your certificate is approaching expiry, you can set a custom alarm in Amazon CloudWatch on the metric "Days to Expiry". Manage AS2 Certificates

Certificates (1) Info

Find resources

Name	Description	Certificate...	Usage	Status	Active date	Inactive d...	Certificate ID
-	CERTIFICATE...	ENCRYPTION	ACTIVE	2025-10-30	2028-02-02	cert-97ac5769cb3f...	

Tags (4)

Import certificate

Manage tags

## Message Encryption Public Certificate

1. This is the public part of the certificate used to **encrypt AS2 messages**.
2. When a partner needs to send AS2 files to the company, the company provides this **encryption public certificate** to the partner.
3. The partner uses this certificate to **encrypt the AS2 message** before sending it. Once encrypted, the message cannot be viewed or read by anyone else on the network.
4. Since it is a **public key**, it is safe to share with external partners. Its only purpose is to allow partners to encrypt messages that **only the company can decrypt**.

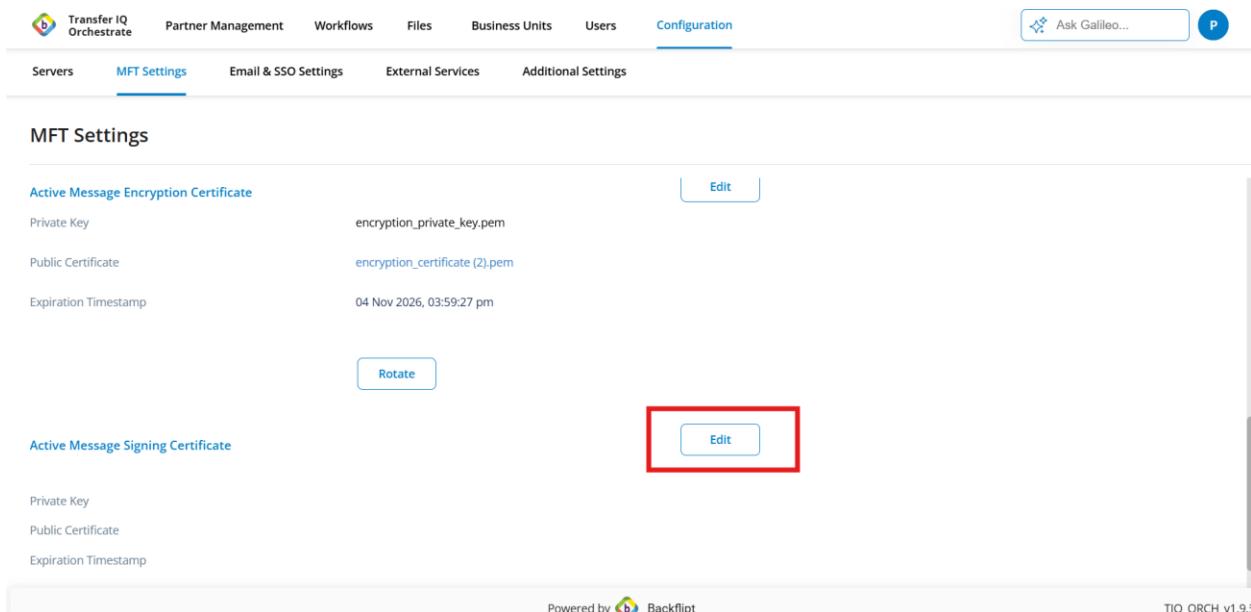
## Message Encryption Private Key:

1. This is the private key that matches the public encryption certificate.
2. The company keeps this key **secure and confidential** and never shares it.
3. When the company receives an encrypted AS2 message from a partner, the company uses this **private key** to decrypt the message and read its contents.



## Message Signing Certificates:

1. Navigate to the Message Signing Certificates section to upload Message Signing Certificates
2. At the top right, an Edit button is available in the Message Signing Certificates Section
3. When the user clicks **Edit**, Super Admin can upload valid Certificates by clicking the upload button



The screenshot shows the 'MFT Settings' section of the Transfer IQ Orchestrate interface. At the top, there are tabs for 'Servers', 'MFT Settings' (which is active and highlighted in blue), 'Email & SSO Settings', 'External Services', and 'Additional Settings'. Below the tabs, the 'MFT Settings' section is titled 'Active Message Encryption Certificate'. It displays the following information:

- Private Key: encryption\_private\_key.pem
- Public Certificate: encryption\_certificate (2).pem
- Expiration Timestamp: 04 Nov 2026, 03:59:27 pm

Below this section is a 'Rotate' button. Further down, there is another section titled 'Active Message Signing Certificate' with the following information:

- Private Key
- Public Certificate
- Expiration Timestamp

At the bottom of the page, there is a 'Powered by' logo for Backflift and the text 'TIQ ORCH v1.9.5'.

4. This section contains of the below certificates:
  - a. Message Signing Public Certificate
  - b. Message Signing Private Key



**MFT Settings**

**Active Message Encryption Certificate**

Private Key	encryption_private_key.pem
Public Certificate	encryption_certificate (2).pem
Expiration Timestamp	04 Nov 2026, 03:59:27 pm

**Active Message Signing Certificate**

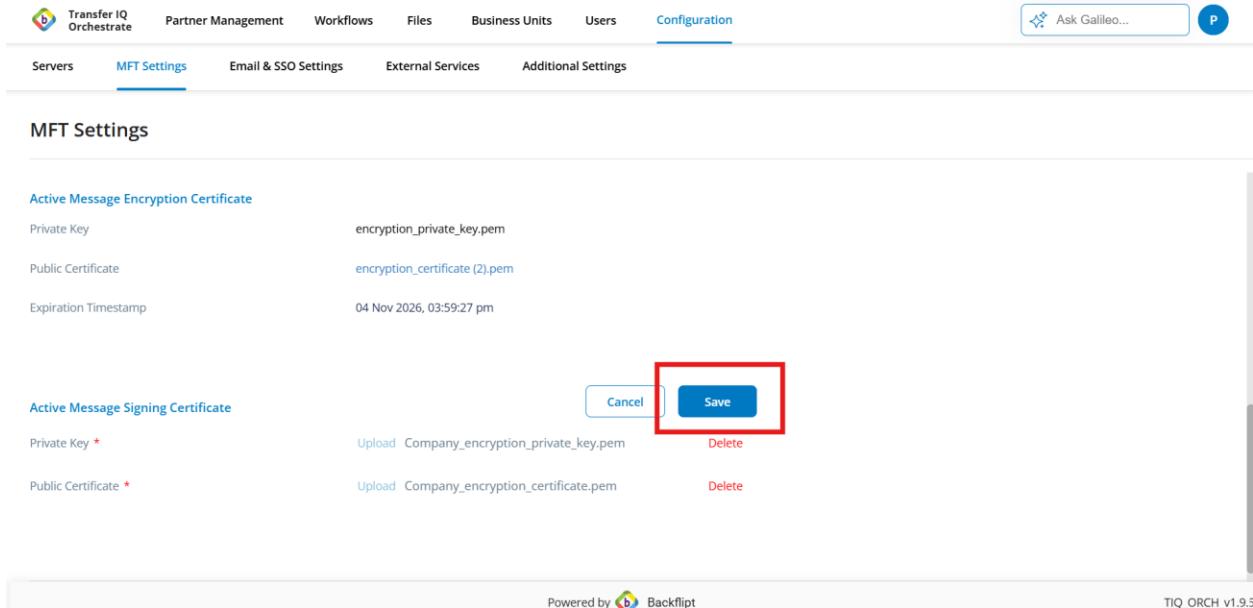
Private Key *	Upload
Public Certificate *	Upload

Powered by  Backflip

TIQ\_ORCH\_v1.9.5

5. Click Save





Transfer IQ Orchestrate

Partner Management Workflows Files Business Units Users Configuration

Servers MFT Settings Email & SSO Settings External Services Additional Settings

### MFT Settings

**Active Message Encryption Certificate**

Private Key	encryption_private_key.pem
Public Certificate	encryption_certificate (2).pem
Expiration Timestamp	04 Nov 2026, 03:59:27 pm

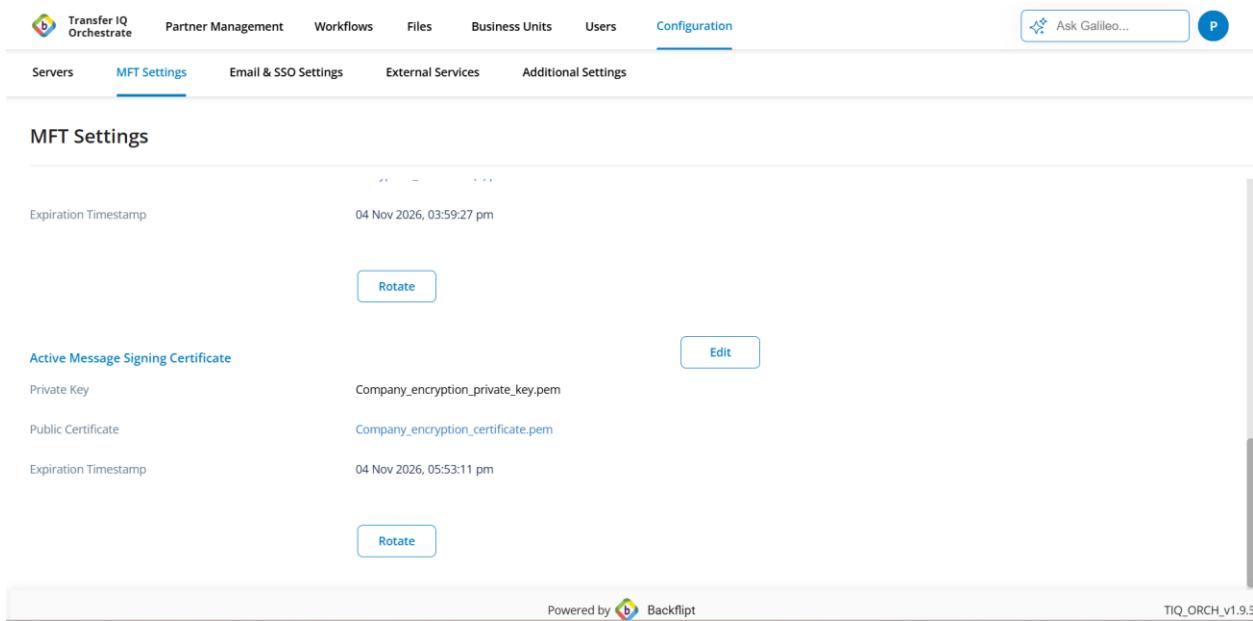
**Active Message Signing Certificate**

Private Key *	Upload Company_encryption_private_key.pem	Cancel	Save	Delete
Public Certificate *	Upload Company_encryption_certificate.pem	Cancel	Save	Delete

Powered by  Backflipt

TIQ\_ORCH\_v1.9.5

6. Once the save button is clicked both the public and private signing certificates will be merged into a single certificate and attached to the Local Profile



Transfer IQ Orchestrate

Partner Management Workflows Files Business Units Users Configuration

Servers MFT Settings Email & SSO Settings External Services Additional Settings

### MFT Settings

Expiration Timestamp 04 Nov 2026, 03:59:27 pm

**Active Message Signing Certificate**

Private Key	Company_encryption_private_key.pem	Rotate
Public Certificate	Company_encryption_certificate.pem	Edit
Expiration Timestamp	04 Nov 2026, 05:53:11 pm	Rotate

Powered by  Backflipt

TIQ\_ORCH\_v1.9.5

## Message Signing Private Key:

1. This private key is used by the company to **digitally sign outgoing AS2 messages**.
2. When the company sends a file to a partner, it uses this private key to create a **digital signature**. This signature proves two things:



- a. The file genuinely came from the company.
- b. The file was not altered during transmission.
3. This private signing key must be kept secure and should never be shared.

#### **Message Signing Public Certificate:**

1. This is the public part of the signing certificate.
2. The company shares this public signing certificate with its partners so they can **verify the digital signature** for incoming messages from the company.
3. When the partner receives a signed AS2 message, partners use this public key to confirm that:
  - a. The message was really sent by the company.
  - b. The message was not changed or tampered with on the way.
4. Since it is a **public certificate**, it is safe to share with external partners.

## **Key Rotation for AS2**

Key rotation in MFT for AS2 is the process of periodically replacing old Encryption & Signing Certificates of Company.

## **Company Message Encryption Certificates Rotation**

Before rotation, only the **Active Encryption Certificates** section is visible, displaying the currently in-use Certificates.

The process involves three distinct phases: **Before Rotation**, **During Rotation**, and **Deprecation**



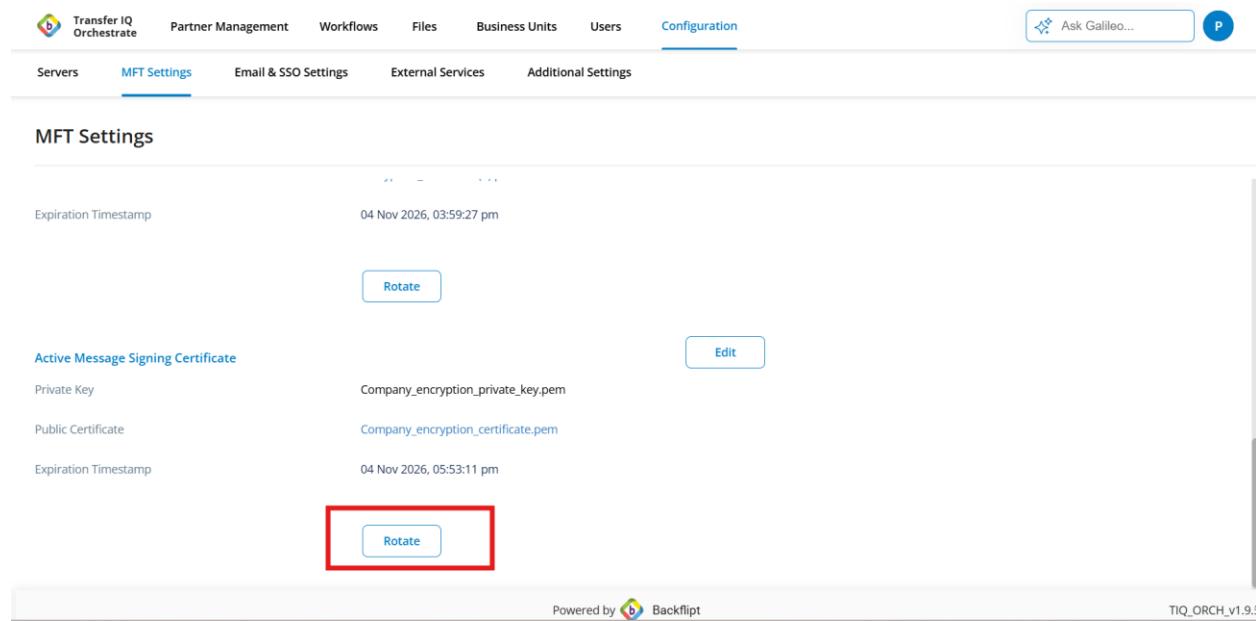
## Before Rotation:

1. Only **one encryption certificate** is present in the **MFT Settings** tab.
2. A **single certificate pair** (public + private key) is attached to the **Enterprise Local Profile**.
3. **Decryption is successful only when** the partner profile on the partner server contains **the same public certificate** corresponding to the private key used for decryption.
4. When the partner uses this certificate for encryption and sends the file, decryption completes successfully.

## During Rotation

To begin the rotation process

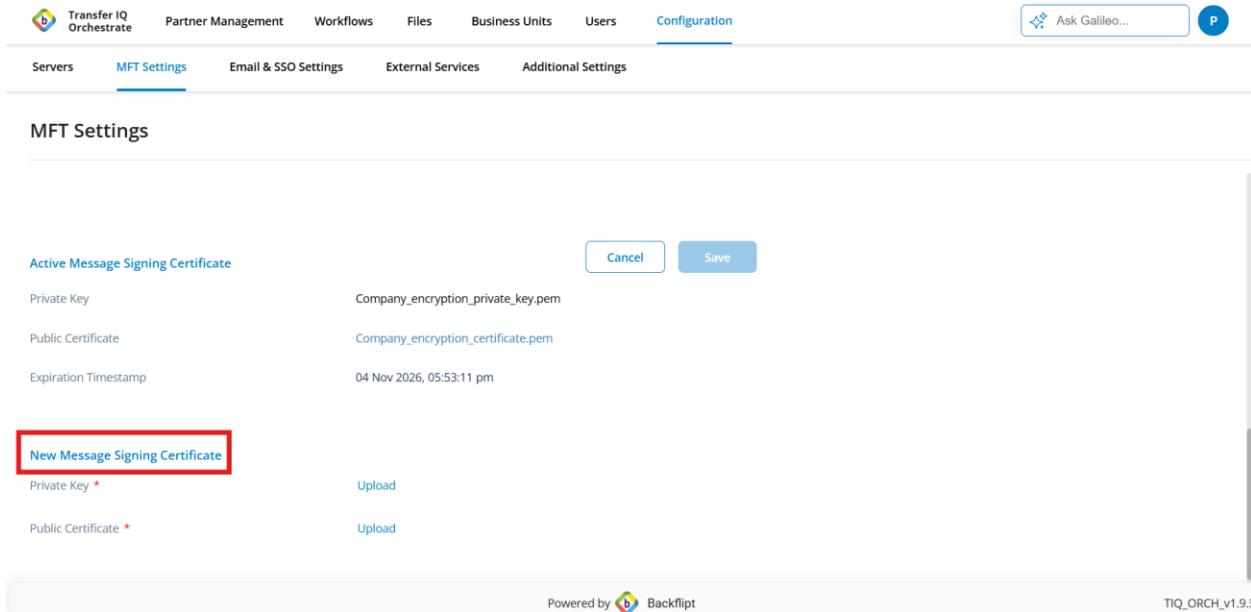
1. Navigate to **MFT Settings > Active Message Encryption Certificate**
2. Click the **Rotate** button located next to the **Active Message Encryption Certificate**



The screenshot shows the 'MFT Settings' tab selected in the navigation bar. The 'Active Message Encryption Certificate' section is displayed, showing a private key and a public certificate. Below this, a new section labeled 'New Message Encryption Certificate' is shown, with a 'Rotate' button highlighted by a red box. The page is powered by Backflip.

3. This action displays an additional section labeled **New Message Encryption Certificate** which includes fields for uploading both **public** and **private** Encryption Certificates.





Active Message Signing Certificate

Private Key: Company\_encryption\_private\_key.pem

Public Certificate: Company\_encryption\_certificate.pem

Expiration Timestamp: 04 Nov 2026, 05:53:11 pm

New Message Signing Certificate

Private Key \*: Upload

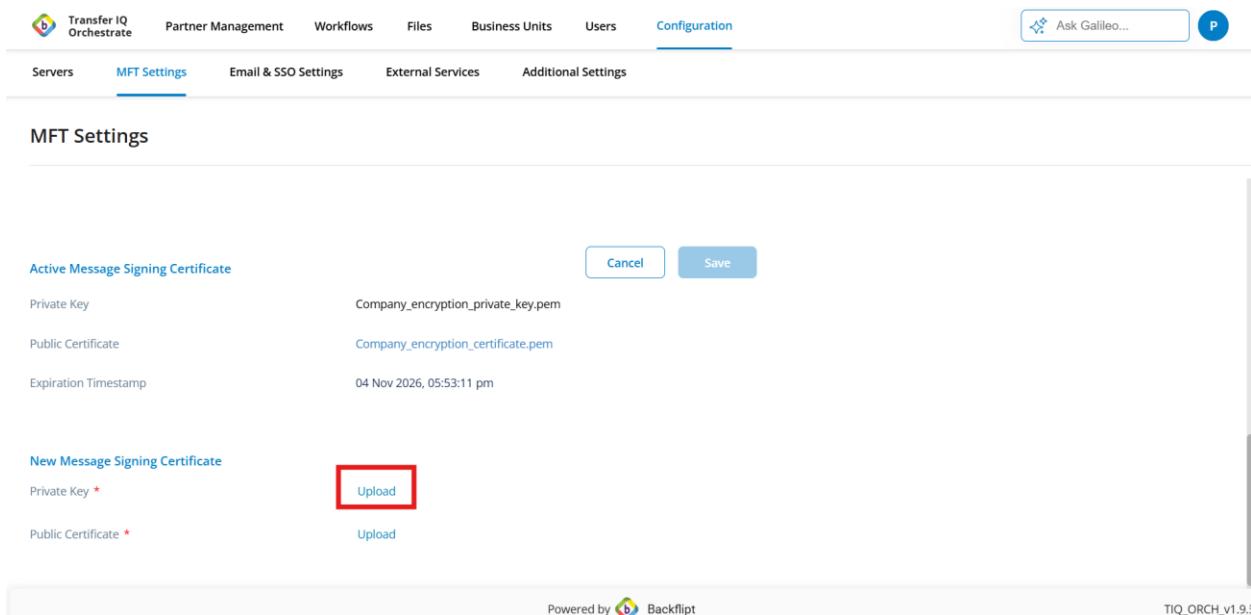
Public Certificate \*: Upload

Cancel Save

Powered by  Backflip

TIQ\_ORCH\_v1.9.5

4. To upload the **New Message Encryption Certificate**, click the **Upload** button under the **New Message Encryption Certificate** section.



Active Message Signing Certificate

Private Key: Company\_encryption\_private\_key.pem

Public Certificate: Company\_encryption\_certificate.pem

Expiration Timestamp: 04 Nov 2026, 05:53:11 pm

New Message Signing Certificate

Private Key \*: Upload

Public Certificate \*: Upload

Cancel Save

Powered by  Backflip

TIQ\_ORCH\_v1.9.5

5. In the file selection dialog, choose a valid Certificate file.
6. Once the file is uploaded successfully, the newly uploaded keys are displayed in the **MFT Settings** tab under the **New Message Encryption Certificates** section



Active Message Signing Certificate

Private Key: Company\_encryption\_private\_key.pem

Public Certificate: Company\_encryption\_certificate.pem

Expiration Timestamp: 04 Nov 2026, 05:53:11 pm

Cancel Save

New Message Signing Certificate

Private Key \*: Upload New\_encryption\_private\_key (1).pem Delete

Public Certificate \*: Upload New\_encryption\_certificate.pem Delete

Powered by Backflift TIQ\_ORCH\_v1.9.5

7. Click **Save**. Once saved, all uploaded certificates will be displayed under the **New Message Encryption Certificate** section in *View* mode. The previously active (old) certificates will be shown with a **Deprecate** button.

Active Message Signing Certificate

Private Key: Company\_encryption\_private\_key.pem

Public Certificate: Company\_encryption\_certificate.pem

Expiration Timestamp: 04 Nov 2026, 05:53:11 pm

Cancel Save

New Message Signing Certificate

Private Key \*: Upload New\_encryption\_private\_key (1).pem Delete

Public Certificate \*: Upload New\_encryption\_certificate.pem Delete

Powered by Backflift TIQ\_ORCH\_v1.9.5

## File Transfer Behavior During Rotation

1. **Two encryption certificates** (old and new) are visible in the **MFT Settings** tab.
2. After rotation, the **new certificate pair** is added to the **Enterprise Local Profile** **along with the old certificate pair**



3. **Decryption succeeds** if the partner profile on the partner server contains:
  - a. **either** the old certificate,
  - b. **or** the new certificate,
  - c. **or both certificates.**
4. If the file is encrypted using any of the certificates available on the partner server, the system can decrypt it successfully using the corresponding private key.

## Message Encryption Certificates Deprecation

Deprecating a Certificate means disabling the old Certificate, so it can no longer encrypt or decrypt files, ensuring that only the newly rotated Encryption Certificate is used for secure file transfers.

### Deprecating Message Encryption Certificates

1. Navigate to the **Active Message Encryption Certificates** section in the MFT Settings tab.
2. Click the **Deprecate** button next to the old active **Message Encryption Certificates**

The screenshot shows the Transfer IQ Orchestrate interface with the following details:

**MFT Settings**

**Active Message Signing Certificate**

- Private Key: Company\_encryption\_private\_key.pem
- Public Certificate: Company\_encryption\_certificate.pem
- Expiration Timestamp: 04 Nov 2026, 05:53:11 pm

**Deprecate** (button highlighted with a red box)

**New Message Signing Certificate**

- Private Key: New\_encryption\_private\_key(1).pem
- Public Certificate: New\_encryption\_certificate.pem
- Expiration Timestamp: 04 Nov 2026, 03:59:27 pm

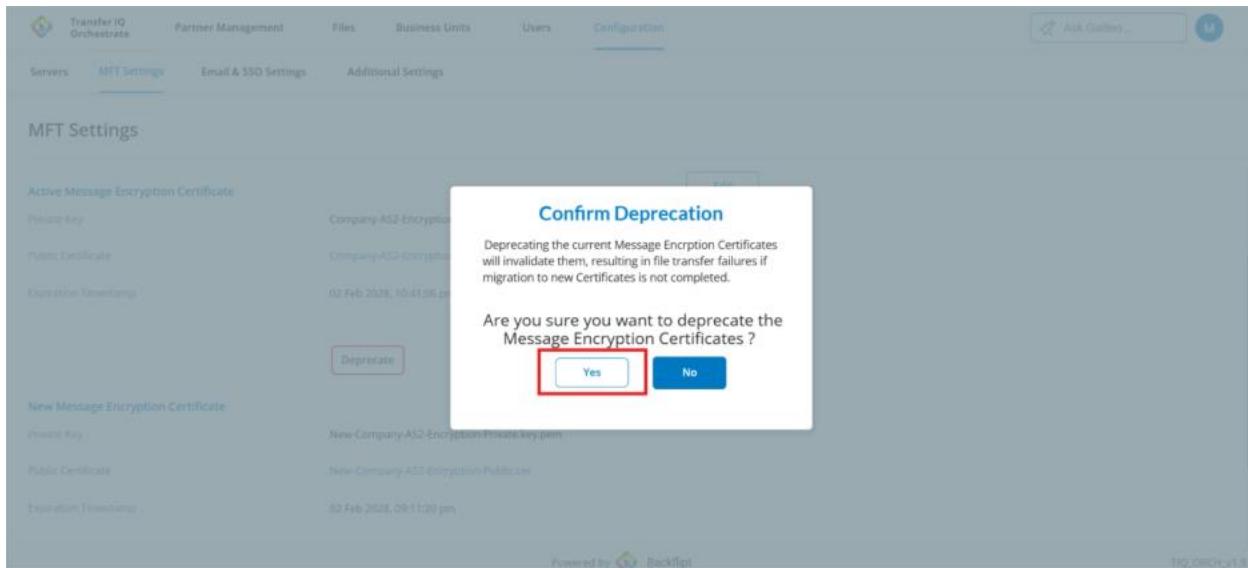
Powered by Backflift

TIQ\_ORCH\_v1.9.5

3. A **popup** is displayed asking for confirmation to deprecate the selected key.



4. Confirm the action by clicking the **Yes button** in the popup. The system marks the key as **deprecated**, indicating it is no longer active for encrypting or decrypting new files.



5. The deprecated certificate is **removed completely** from the application.

The screenshot shows the 'MFT Settings' tab in the Transfer IQ Orchestrator interface. The 'Active Message Signing Certificate' section is visible, showing a public certificate named 'encryption\_certificate (2).pem' with an expiration timestamp of '04 Nov 2026, 03:59:27 pm'. A 'Rotate' button is present. Below this, the 'Active Message Encryption Certificate' section is shown, listing a private key and a public certificate, both with the same expiration timestamp. A 'Rotate' button is also present here. The 'Edit' button for the signing certificate is highlighted with a red box.

## File Transfer Behavior During Deprecation

1. Only the **new encryption certificate set** remains in the **MFT Settings** tab.



2. The **Enterprise Local Profile** holds **only the new certificate pair**, and the deprecated (old) certificate set is removed.
3. **Decryption is successful only if** the partner profile on the partner server contains the **newly rotated public certificate** and sends the encrypted file using this updated key.

## Company Message Signing Certificates Rotation

Before rotation, only the **Active Signing Certificates** section is visible, displaying the currently in-use Certificates.

The process involves three distinct phases: **Before Rotation**, **During Rotation**, and **Deprecation**

### Before Rotation:

1. Only **one certificate** is present in the **MFT Settings** tab.
2. A **single certificate pair** (public + private key) is attached to the **Enterprise Local Profile**.
3. **All outbound signing** is performed using the active private key.
4. As long as the partner uses the **public key that corresponds to this private key**, the partner can **successfully verify the digital signature**.

### During Rotation

To begin the rotation process

1. Navigate to **MFT Settings > Active Message Signing Certificate**
2. Click the **Rotate** button located next to the **Active Message Signing Certificate**



Expiration Timestamp: 04 Nov 2026, 03:59:27 pm

Active Message Signing Certificate

Private Key: New\_encryption\_private\_key (1).pem

Public Certificate: New\_encryption\_certificate.pem

Expiration Timestamp: 04 Nov 2026, 03:59:27 pm

Powered by Backflip

TIQ\_ORCH\_v1.9.5

3. This action displays an additional section labeled **New Message Signing Certificate** which includes fields for uploading both **public** and **private** Signing Certificates
4. To upload the **New Message Signing Certificate**, click the **Upload** button under the **New Message Signing Certificate** section

Active Message Signing Certificate

Private Key: New\_encryption\_private\_key (1).pem

Public Certificate: New\_encryption\_certificate.pem

Expiration Timestamp: 04 Nov 2026, 03:59:27 pm

New Message Signing Certificate

Private Key \*  Cancel Save

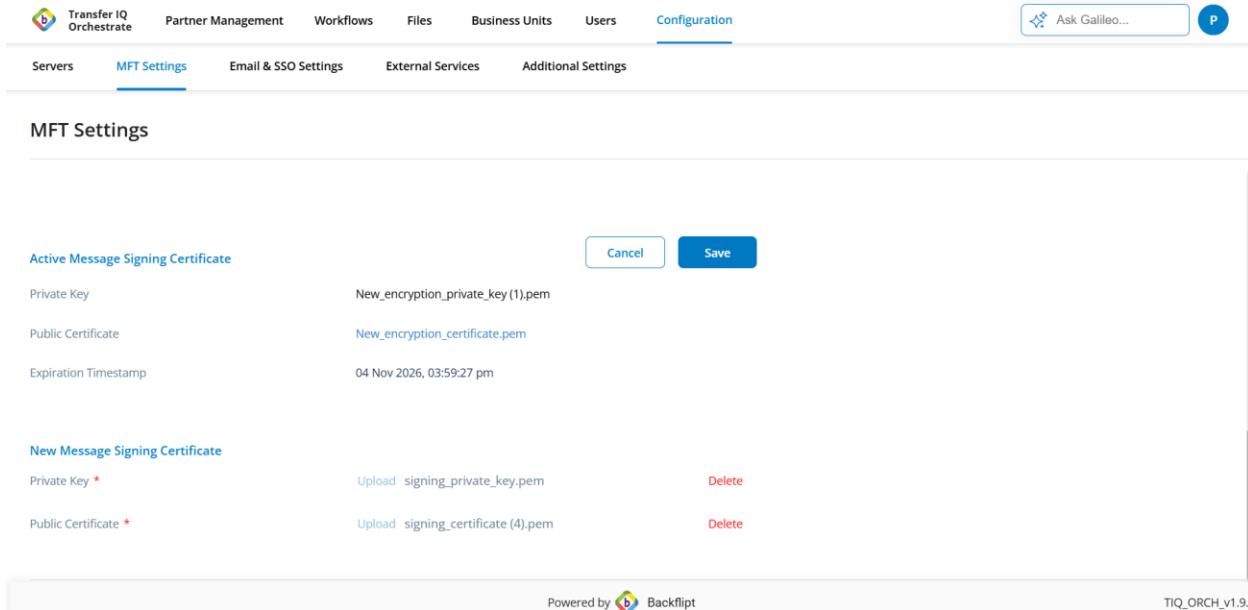
Public Certificate \*

Powered by Backflip

TIQ\_ORCH\_v1.9.5

5. In the file selection dialog, choose a valid Signing Certificate.
6. Once the file is uploaded successfully, the newly uploaded keys are displayed in the **MFT Settings** tab under the **New Message Signing Certificates** section





Transfer IQ Orchestrate

Partner Management Workflows Files Business Units Users Configuration

Ask Galileo... P

Servers MFT Settings Email & SSO Settings External Services Additional Settings

### MFT Settings

**Active Message Signing Certificate**

Private Key: New\_encryption\_private\_key (1).pem

Public Certificate: New\_encryption\_certificate.pem

Expiration Timestamp: 04 Nov 2026, 03:59:27 pm

**New Message Signing Certificate**

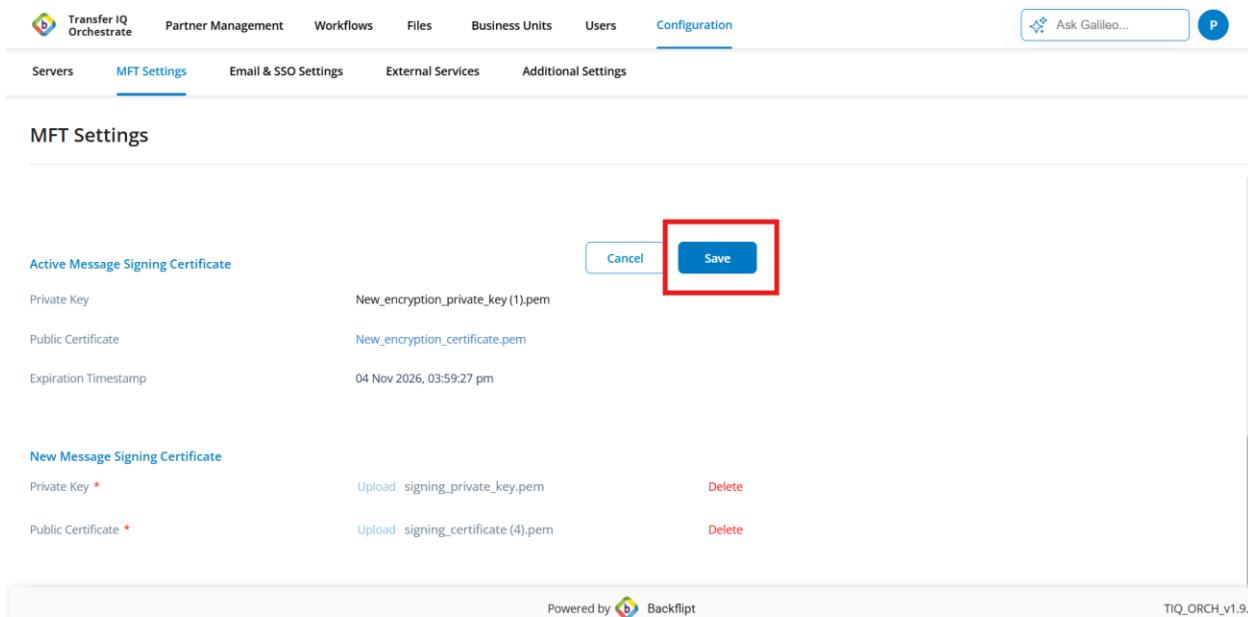
Private Key \*: Upload signing\_private\_key.pem Delete

Public Certificate \*: Upload signing\_certificate (4).pem Delete

Powered by  Backflift

TIQ\_ORCH\_v1.9.5

## 7. Click **Save**.



Transfer IQ Orchestrate

Partner Management Workflows Files Business Units Users Configuration

Ask Galileo... P

Servers MFT Settings Email & SSO Settings External Services Additional Settings

### MFT Settings

**Active Message Signing Certificate**

Private Key: New\_encryption\_private\_key (1).pem

Public Certificate: New\_encryption\_certificate.pem

Expiration Timestamp: 04 Nov 2026, 03:59:27 pm

**New Message Signing Certificate**

Private Key \*: Upload signing\_private\_key.pem Delete

Public Certificate \*: Upload signing\_certificate (4).pem Delete

Powered by  Backflift

TIQ\_ORCH\_v1.9.5

8. Once saved, all uploaded keys and their passphrases will be displayed under the **New Message Signing Certificate** section in *View* mode with an expiration timestamp.
9. The previously active (old) certificates will be shown with a **Deprecate** button.



## File Transfer Behavior During Rotation

1. **Two certificates** are visible in the **MFT Settings** tab.
2. Once the certificates are rotated, the **new certificate pair** is also attached to the **Enterprise Local Profile**, along with the old one.
3. Out of the two available certificates, **the certificate with the later expiration date (with more validity) is** used for signing outgoing messages from enterprise to partner.
4. If the partner contains the certificate that has more validity (either newly rotated certificate or old existing certificate) then the signature verification is becoming successful

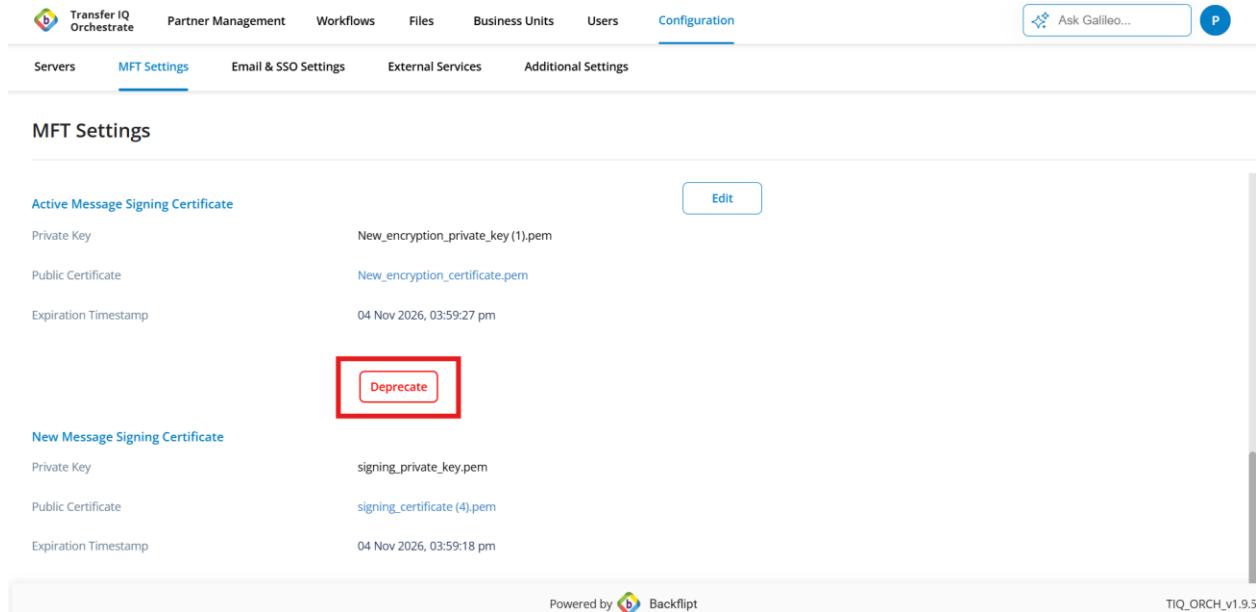
## Message Signing Certificates Deprecation

Deprecating a Certificate means disabling the old Certificate, so it can no longer be used for signing outgoing messages, ensuring that only the newly rotated Signing Certificate is used.

## Deprecating Message Signing Certificates

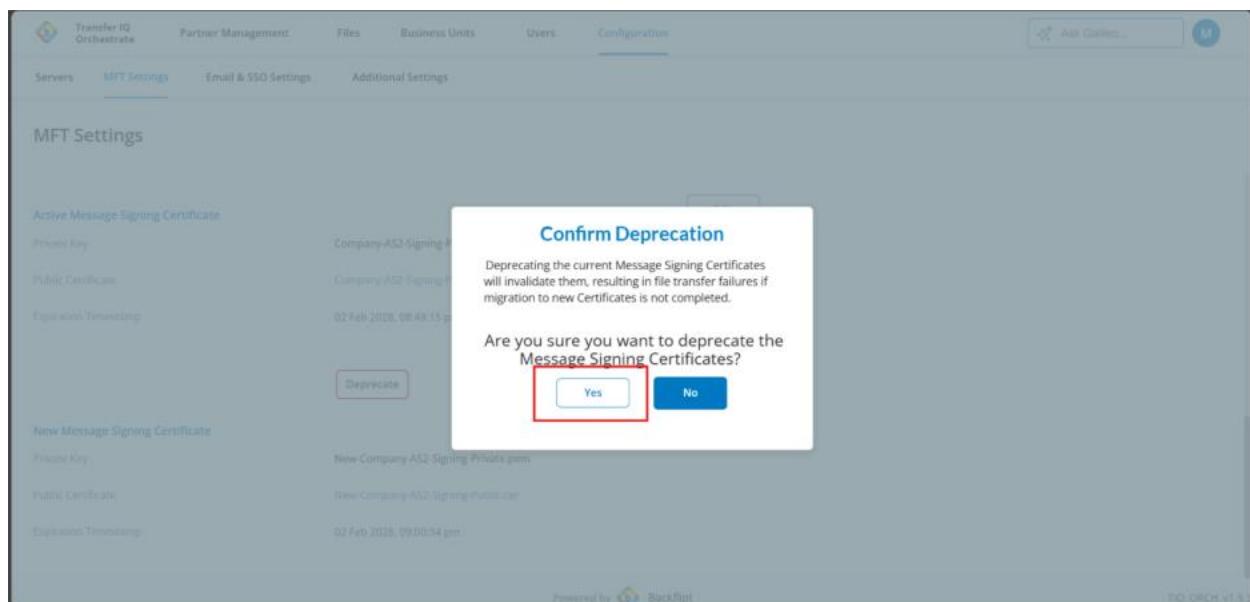


1. Navigate to the **Active Message Signing Certificates** section in the MFT Settings tab.
2. Click the **Deprecate** button next to the old active **Message Signing Certificates**



The screenshot shows the 'MFT Settings' page in Transfer IQ Orchestrate. The 'Configuration' tab is selected. Under 'MFT Settings', the 'Active Message Signing Certificate' section is displayed. It shows a table with three rows: 'Private Key' (value: 'New\_encryption\_private\_key (1).pem'), 'Public Certificate' (value: 'New\_encryption\_certificate.pem'), and 'Expiration Timestamp' (value: '04 Nov 2026, 03:59:27 pm'). Below this is a 'Deprecate' button, which is highlighted with a red box. The next section, 'New Message Signing Certificate', shows a table with three rows: 'Private Key' (value: 'signing\_private\_key.pem'), 'Public Certificate' (value: 'signing\_certificate (4).pem'), and 'Expiration Timestamp' (value: '04 Nov 2026, 03:59:18 pm'). At the bottom of the page, it says 'Powered by Backflift' and 'TIQ\_ORCH\_v1.9.5'.

3. A **popup** is displayed asking for confirmation to deprecate the selected certificate
4. Confirm the action by clicking the **Yes button** in the popup. The system marks the key as **deprecated**, indicating it is no longer active for encrypting or decrypting new files



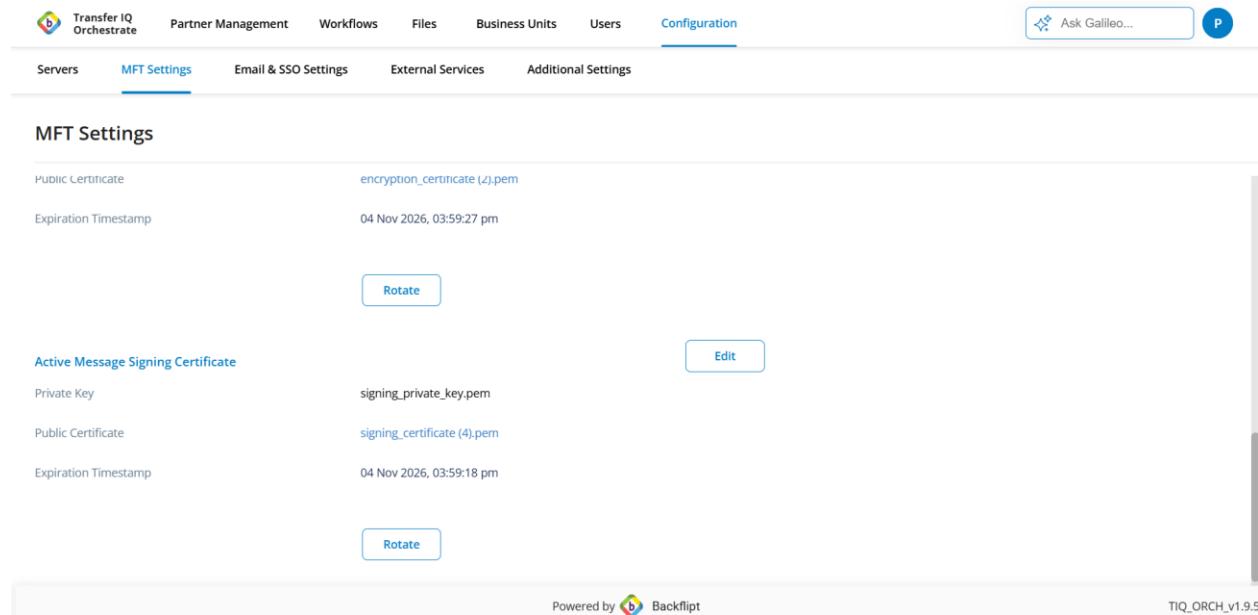
The screenshot shows the 'MFT Settings' page with a 'Confirm Deprecation' dialog box in the foreground. The dialog box has a title 'Confirm Deprecation' and a message: 'Deprecating the current Message Signing Certificates will invalidate them, resulting in file transfer failures if migration to new Certificates is not completed.' Below the message is a question: 'Are you sure you want to deprecate the Message Signing Certificates?' with 'Yes' and 'No' buttons. The 'Yes' button is highlighted with a red box. The background shows the 'Active Message Signing Certificate' section with the same data as the previous screenshot.

5. The deprecated key is **removed completely** from the application



# File Transfer Behavior During Deprecation

1. Only the **new certificate set** remains in the **MFT Settings** tab



Transfer IQ Orchestrate

Partner Management Workflows Files Business Units Users Configuration

Ask Galileo... P

Servers MFT Settings Email & SSO Settings External Services Additional Settings

**MFT Settings**

Public Certificate: encryption\_certificate (2).pem

Expiration Timestamp: 04 Nov 2026, 03:59:27 pm

**Rotate**

Active Message Signing Certificate

Private Key: signing\_private\_key.pem

Public Certificate: signing\_certificate (4).pem

Expiration Timestamp: 04 Nov 2026, 03:59:18 pm

**Rotate**

Powered by Backflipt

TIQ\_ORCH\_v1.9.5

2. The **Enterprise Local Profile** contains **only the new certificate pair**, and the deprecated certificate set is removed.
3. All outbound signing is now performed **using the new private key**.
4. If the partner uses the **public key that matches this new private key**, they will continue to **successfully verify** signature.

## SFTP & AS2 Protocol

When both SFTP and AS2 protocol are deployed, clicking on MFT Settings in the Configuration tab will navigate to the MFT Settings section, where Certificates related to both SFTP and AS2 will be displayed. Certificates used for SFTP and AS2 are discussed above.



## Email and SSO Settings

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

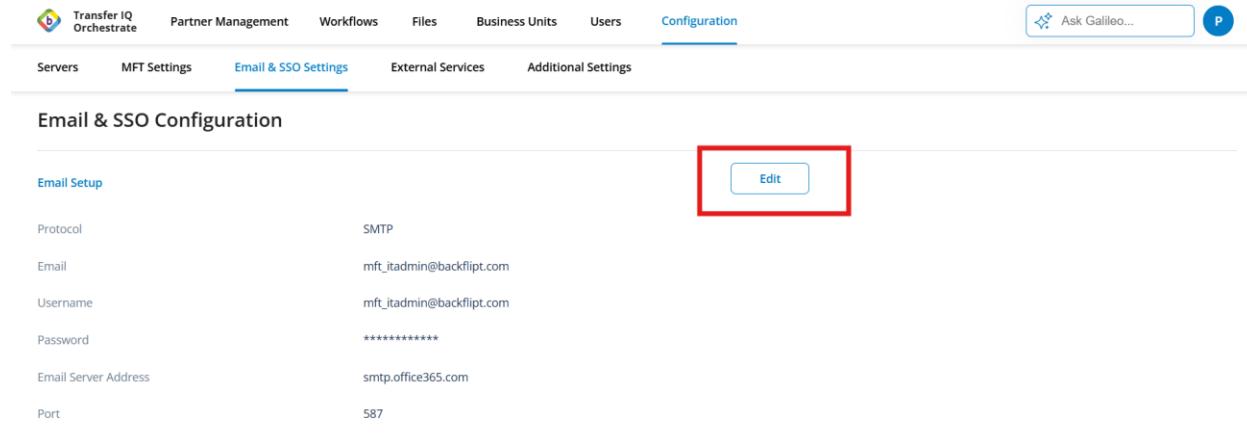
Email and SSO Settings consists of three sub sections

1. Email Setup
2. Email Templates
3. 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 screenshot shows the application's navigation bar with 'Transfer IQ Orchestrate' and various menu items like Partner Management, Workflows, Files, Business Units, Users, and Configuration. Under Configuration, 'Email & SSO Settings' is selected. The main content area is titled 'Email & SSO Configuration' and contains a table for 'Email Setup' with fields for Protocol (SMTP), Email (mft\_itadmin@backflift.com), Username (mft\_itadmin@backflift.com), Password (redacted), Email Server Address (smtp.office365.com), and Port (587). An 'Edit' button is located to the right of the table, and it is highlighted with a red box.

Email Setup	
Protocol	SMTP
Email	mft_itadmin@backflift.com
Username	mft_itadmin@backflift.com
Password	*****
Email Server Address	smtp.office365.com
Port	587

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



Transfer IQ Orchestrate

Partner Management Workflows Files Business Units Users Configuration

Ask Galileo... P

Servers MFT Settings Email & SSO Settings External Services Additional Settings

### Email & SSO Configuration

#### Email Setup

Protocol \*

SMTP

Email \*

mft\_itadmin@backflift.com

Username

mft\_itadmin@backflift.com

Password

.....

Email Server Address \*

smtp.office365.com

Port \*

587

Cancel Save Test

This section contains the below fields

- 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.
- Email** - The email address that will appear as the sender of system-generated emails.
- Username** - The username used to authenticate with the email server.
- Password** - The password associated with the email account or application-specific password. This is used to authenticate the application with the SMTP server.
- 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.)
- Port** - The port number used to connect to the SMTP server. (Example: 587)

Transfer IQ Orchestrate

Partner Management Workflows Files Business Units Users Configuration

Ask Galileo... P

Servers MFT Settings Email & SSO Settings External Services Additional Settings

### Email & SSO Configuration

#### Email Setup

Protocol \*

SMTP

Email \*

mft\_itadmin@backflift.com

Username

mft\_itadmin@backflift.com

Password

.....

Email Server Address \*

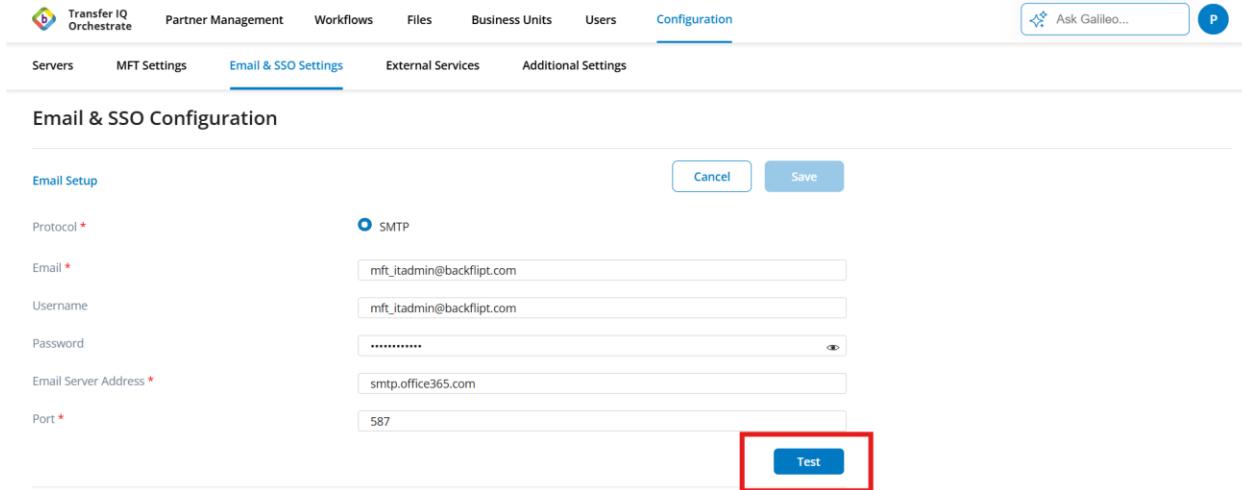
smtp.office365.com

Port \*

587

Cancel Save Test





Transfer IQ Orchestrate

Partner Management Workflows Files Business Units Users Configuration

Ask Galileo... P

Servers MFT Settings Email & SSO Settings External Services Additional Settings

### Email & SSO Configuration

#### Email Setup

Protocol \*  SMTP

Email \*

Username

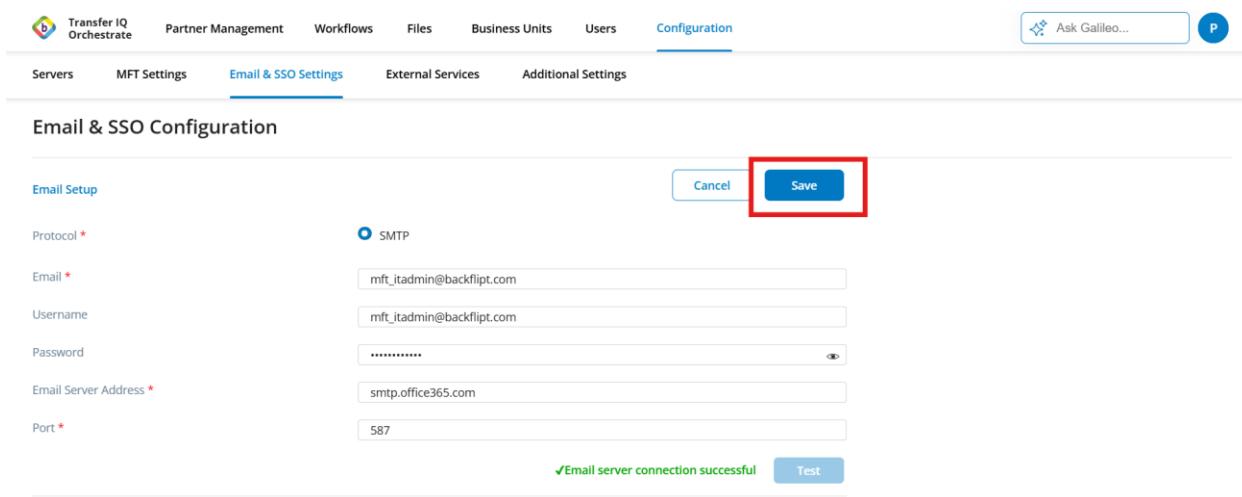
Password

Email Server Address \*

Port \*

**Test**

Once the Super Admin has entered all the SMTP details, Super Admin click 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.



Transfer IQ Orchestrate

Partner Management Workflows Files Business Units Users Configuration

Ask Galileo... P

Servers MFT Settings Email & SSO Settings External Services Additional Settings

### Email & SSO Configuration

#### Email Setup

Protocol \*  SMTP

Email \*

Username

Password

Email Server Address \*

Port \*

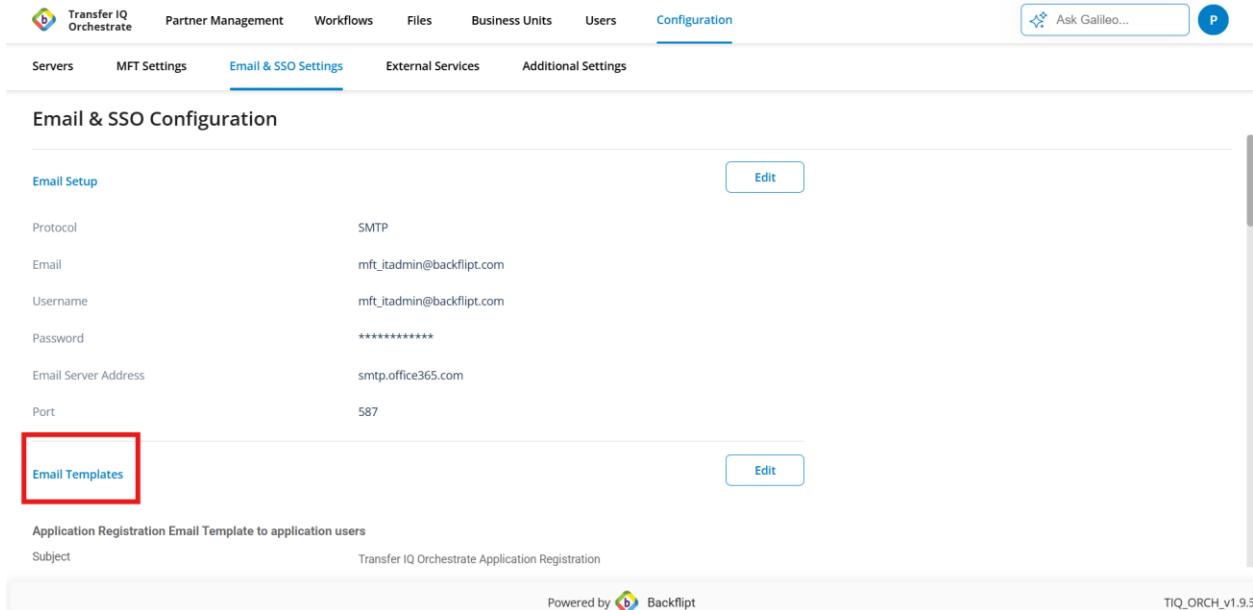
**Save**

✓Email server connection successful

**Test**

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





Transfer IQ Orchestrate Configuration

Email & SSO Configuration

Email Setup

Protocol: SMTP

Email: mft\_itadmin@backflift.com

Username: mft\_itadmin@backflift.com

Password: \*\*\*\*

Email Server Address: smtp.office365.com

Port: 587

**Email Templates**

Application Registration Email Template to application users

Subject: Transfer IQ Orchestrate Application Registration

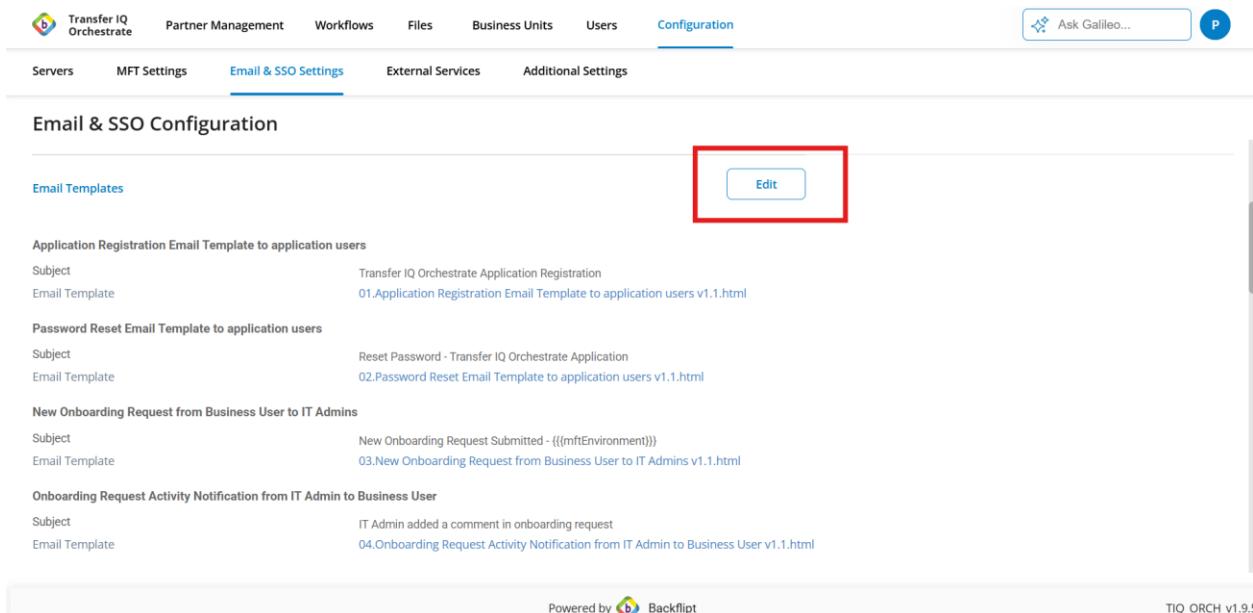
Powered by  Backflift

TIQ\_ORCH\_v1.9.5

## Email Templates

Upon the first login of the **First Super Admin**, a set of default **Email Templates** is automatically populated in the email templates section. These templates define the content and subject lines for various system-generated emails such as user invitations, password resets, and notifications etc.

Click the edit button to make changes to the existing templates



Transfer IQ Orchestrate Configuration

Email & SSO Configuration

Email Templates

**Edit**

Application Registration Email Template to application users

Subject: Transfer IQ Orchestrate Application Registration

Email Template: 01.Application Registration Email Template to application users v1.1.html

Password Reset Email Template to application users

Subject: Reset Password - Transfer IQ Orchestrate Application

Email Template: 02.Password Reset Email Template to application users v1.1.html

New Onboarding Request from Business User to IT Admins

Subject: New Onboarding Request Submitted - {{{mftEnvironment}}}

Email Template: 03.New Onboarding Request from Business User to IT Admins v1.1.html

Onboarding Request Activity Notification from IT Admin to Business User

Subject: IT Admin added a comment in onboarding request

Email Template: 04.Onboarding Request Activity Notification from IT Admin to Business User v1.1.html

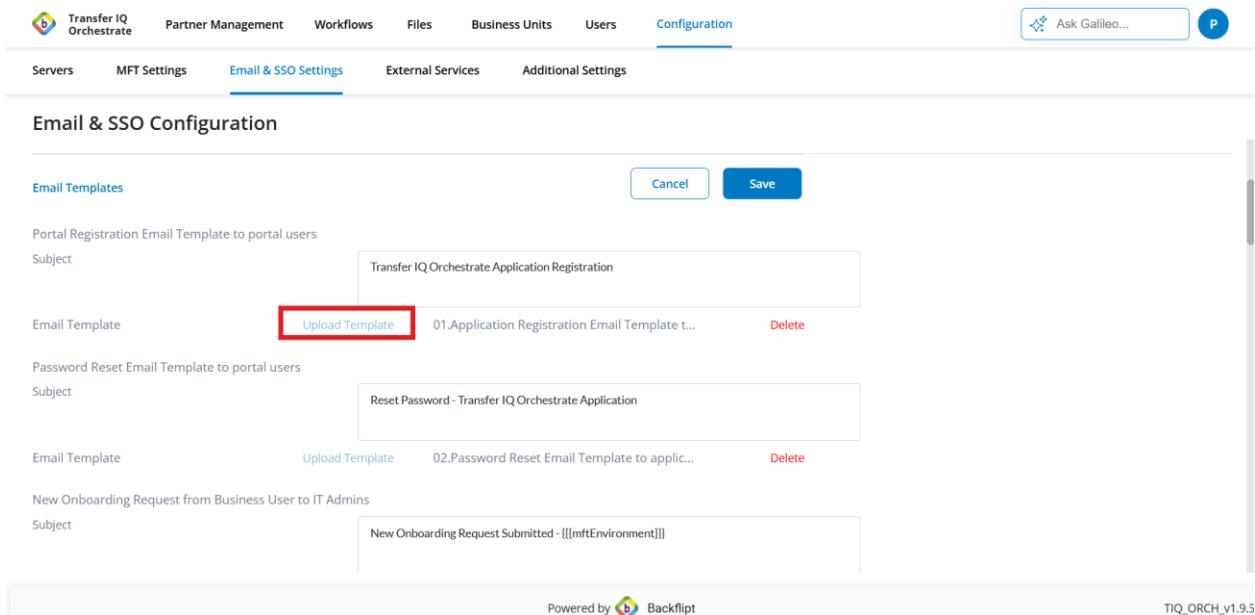
Powered by  Backflift

TIQ\_ORCH\_v1.9.5

Each email template includes the following elements:



1. **Upload Button** - Allows the Super Admin to upload a custom email template file, replacing the default content if desired.



Portal Registration Email Template to portal users

Subject: Transfer IQ Orchestrate Application Registration

Email Template: 01.Application Registration Email Template t... [Delete](#)

Upload Template

Password Reset Email Template to portal users

Subject: Reset Password - Transfer IQ Orchestrate Application

Email Template: 02.Password Reset Email Template to applic... [Delete](#)

Upload Template

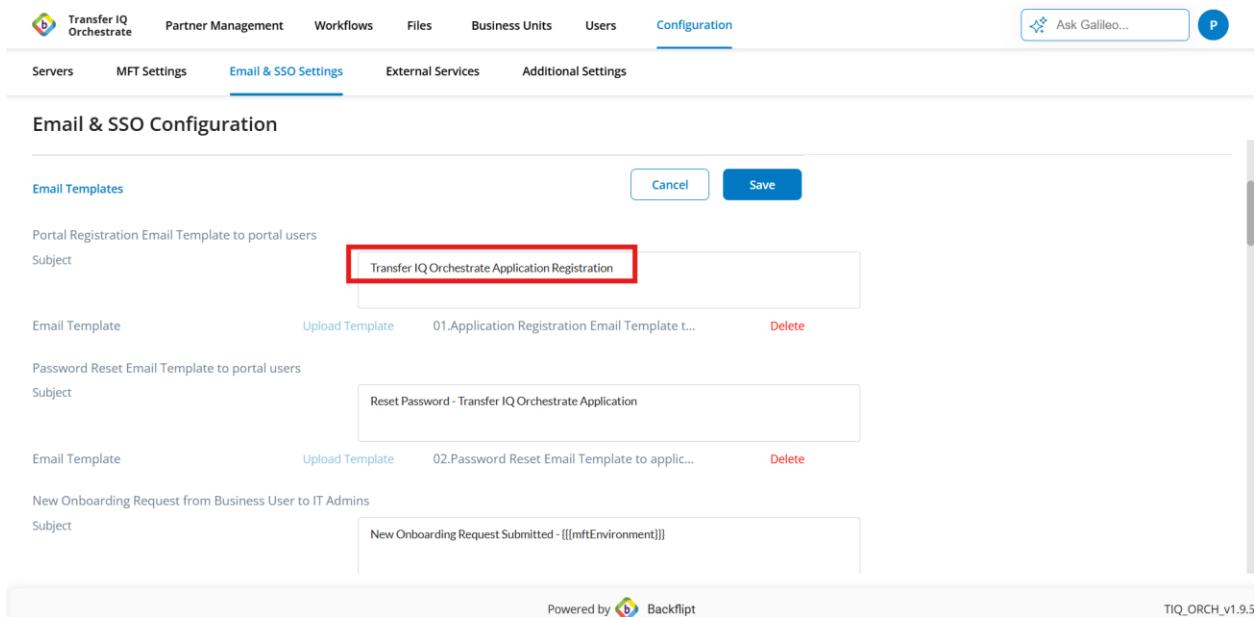
New Onboarding Request from Business User to IT Admins

Subject: New Onboarding Request Submitted - {{{mftEnvironment}}}

Powered by  Backflip

TIQ\_ORCH\_v1.9.5

2. **Subject** - Displays the default subject line of the email, which can be edited.



Portal Registration Email Template to portal users

Subject: Transfer IQ Orchestrate Application Registration

Email Template: 01.Application Registration Email Template t... [Delete](#)

Upload Template

Password Reset Email Template to portal users

Subject: Reset Password - Transfer IQ Orchestrate Application

Email Template: 02.Password Reset Email Template to applic... [Delete](#)

Upload Template

New Onboarding Request from Business User to IT Admins

Subject: New Onboarding Request Submitted - {{{mftEnvironment}}}

Powered by  Backflip

TIQ\_ORCH\_v1.9.5

3. **Delete Button** - Removes the previously uploaded template and helps to upload a new template.



Transfer IQ Orchestrate

Partner Management Workflows Files Business Units Users Configuration

Ask Galileo... P

Servers MFT Settings Email & SSO Settings External Services Additional Settings

Email & SSO Configuration

Email Templates Cancel Save

Portal Registration Email Template to portal users

Subject Transfer IQ Orchestrate Application Registration

Email Template Upload Template 01.Application Registration Email Template t... Delete

Password Reset Email Template to portal users

Subject Reset Password - Transfer IQ Orchestrate Application

Email Template Upload Template 02.Password Reset Email Template to applic... Delete

New Onboarding Request from Business User to IT Admins

Subject New Onboarding Request Submitted - [[[mftEnvironment]]]

Powered by  Backflipt

TIQ\_ORCH\_v1.9.5

The Email Templates section contains the following templates

- Application Registration Email Template to application users
- Password Reset Email Template to application users
- New Onboarding Request from Business User to Admins
- Onboarding Request Activity Notification from Business User to Admin
- Onboarding Request Activity Notification from Admin to Business User
- Account Creation notification to Business User
- Onboarding completed notification to Business User
- New Workflow Request Notification to Admins
- Workflow Request Activity Notification from Admin to Business User
- Workflow Request Activity Notification from Business User to Admin
- New Workflow Request Completion Template
- Account Creation notification to Distribution List
- Application Login Email Template to application users
- New Workflow Request Outcome on Success
- New Workflow Request Outcome on Failure
- Workflow Completion

After uploading all the templates, click the **"Save"** button to save the details. Once saved, the details will appear in **view mode** within the **Email Templates** section



Transfer IQ Orchestrate    Partner Management    Workflows    Files    Business Units    Users    Configuration

Ask Galileo...    P

Servers    MFT Settings    **Email & SSO Settings**    External Services    Additional Settings

## Email & SSO Configuration

**Workflow Completion**

Subject	New Workflow Creation Successfull
Email Template	Workflow completed notification to Business User.html

**AS2 Successful File Transfer**

Subject	AS2 File Transfer Success Notification
Email Template	success_as2.2.html

**AS2 File Transfer Failure**

Subject	AS2 File Transfer Failure Notification
Email Template	failure_as2.2.html

**Transfer IQ Orchestrate SSO Setup**

Enable SSO    [Edit](#)

Powered by  Backflipt    TIQ\_ORCH\_v1.9.5



## Transfer IQ Orchestrate SSO Setup

**Single Sign-On (SSO)** is a user authentication method that allows users to log in once and access multiple applications or systems without needing to log in again for each one.

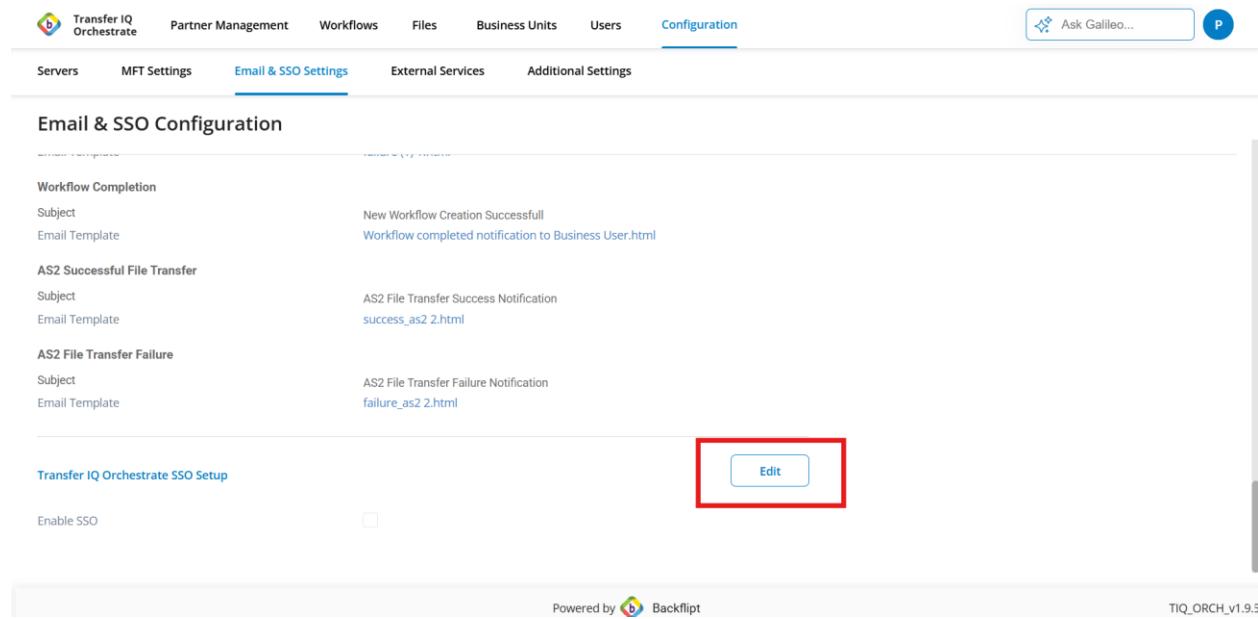
Instead of managing separate usernames and passwords for each application, users log in through a central **Identity Provider (IdP)** like **AWS IAM Identity Center**.

Super admin can enable and disable SSO by editing and simply checking and unchecking the checkbox

### User Access Requirement with SSO :

- When **SSO is enabled**, the user must be created in **IAM Identity Center** and assigned to the application.
- The **Transfer Family (TransferIQ) application must be created in the same AWS region as the IAM Identity Center**.
- Only after these prerequisites are met, the **business user (B-User)** can log in through the **AWS Access Portal URL** and upload files.

**Note:** When **SSO is disabled**, **IAM Identity Center is not required**. Users can access the application without Identity Center configuration.



The screenshot shows the Transfer IQ Orchestrate configuration interface. The top navigation bar includes 'Transfer IQ Orchestrate', 'Partner Management', 'Workflows', 'Files', 'Business Units', 'Users', 'Configuration' (which is underlined), 'Ask Galileo...', and a profile icon. Below the navigation is a sub-menu with 'Servers', 'MFT Settings', 'Email & SSO Settings' (which is underlined), 'External Services', and 'Additional Settings'. The main content area is titled 'Email & SSO Configuration'. It contains sections for 'Workflow Completion', 'AS2 Successful File Transfer', 'AS2 File Transfer Failure', and 'Transfer IQ Orchestrate SSO Setup'. The 'Transfer IQ Orchestrate SSO Setup' section has a 'Enable SSO' checkbox, which is highlighted with a red box. At the bottom, there is an 'Edit' button inside a red box, and the footer includes 'Powered by Backflift' and 'TIQ\_ORCH\_v1.9.5'.



The SSO Section when enabled consists of the below fields

## SSO Configuration Fields – Mandatory and Required Fields

- **IdP Service** - The Identity Provider used for SSO. (e.g., **IAM Identity Center**)
- **Entity ID** - This is the **Issuer URL** that uniquely identifies the IAM Identity Center.
- **Sign-in Page URL** - This is the AWS SAML Assertion Consumer Service (ACS) URL from IAM Identity Center, where users are redirected to log in when SSO is enabled
- **Whitelist URL** - Allowed redirect domains after successful SSO login. (Example: <https://d-9067cad15b.awsapps.com>)
- **IdP X.509 Certificate** - The Super Admin uploads the Base64-encoded X.509 certificate provided in the IAM Identity Center SAML metadata file, which is used to validate SAML responses from AWS

## SSO Logout Configuration (Optional)

- **Single Logout URL** - This is the URL where users are redirected to log out from the Identity Provider when they sign out of the application. It helps ensure that the user is logged out from all connected applications in a single action.
- **Logout Public Certificate** - A public certificate used to verify the logout requests sent by the Identity Provider. This certificate can be uploaded to secure the logout process.
- **Logout Private Key** - A private key used by the application to sign logout requests sent to the Identity Provider. Uploading this key enhances security during the logout process.



Transfer IQ Orchestrate

Partner Management

Files

Business Units

Users

Configuration

Ask Galileo...

Servers

MFT Settings

Email & SSO Settings

Additional Settings

Email & SSO Configuration

Transfer IQ Orchestrate SSO Setup

Enable SSO

IdP Service \*

Entity ID (Identity Provider Issuer) \*

Sign-in Page URL \*

Whitelist URL \*

The whitelist URLs must be separated by (,).

IdP X.509 Certificate \*

Upload

Single Logout URL

Logout Public Certificate

Logout Private Key

Powered by Backflipt

TIQ\_ORCH\_v1.9.4

After providing all the details, click the "Save" button to save the details.

Transfer IQ Orchestrate

Partner Management

Workflows

Files

Business Units

Users

Configuration

Ask Galileo...

Servers

MFT Settings

Email & SSO Settings

External Services

Additional Settings

Email & SSO Configuration

Transfer IQ Orchestrate SSO Setup

Enable SSO

IdP Service \*

IAM Identity Center

Entity ID (Identity Provider Issuer) \*

https://identitycenter.amazonaws.com/ssoins-7223a69792407606

Sign-in Page URL \*

https://portal.sso.us-east-1.amazonaws.com/saml/assertion/MTkyODY4MTc4NzczX2I

Whitelist URL \*

https://d-9067cad15b.awssapps.com

The whitelist URLs must be separated by (,).

IdP X.509 Certificate \*

Upload AWS\_SSO\_for\_Custom SAML 2.0 application\_certificate (4).pem

Single Logout URL

Powered by Backflipt

TIQ\_ORCH\_v1.9.5

Once saved, the details will appear in view mode within the Transfer IQ Orchestrate SSO Setup section



Transfer IQ Orchestrate SSO Setup

Enable SSO	<input checked="" type="checkbox"/>
IdP Service	IAM Identity Center
Entity ID (Identity Provider Issuer)	<a href="https://identitycenter.amazonaws.com/ssoins-7223a69792407606">https://identitycenter.amazonaws.com/ssoins-7223a69792407606</a>
Sign-in Page URL	<a href="https://portal.sso.us-east-1.amazonaws.com/saml/assertion/MTIyODY4MTc4NzczX2lucy1hMGM2N2UzMjlkMDMxMzc5">https://portal.sso.us-east-1.amazonaws.com/saml/assertion/MTIyODY4MTc4NzczX2lucy1hMGM2N2UzMjlkMDMxMzc5</a>
Whitelist URL	<a href="https://d-9067cad15b.awssapps.com">https://d-9067cad15b.awssapps.com</a>
IdP X.509 Certificate	<a href="#">AWS_SSO_for_Custom SAML 2.0 application_certificate (4).perm</a>
Single Logout URL	
Logout Public Certificate	
Logout Private Key	

Powered by  Backflip

TIQ\_ORCH\_v1.9.5

## External Services

External Services can be created and configured within the External Services Section of the Configuration tab of orchestrate application. Once an External Service is created, it can be associated with a custom workflow step. When a workflow that includes this custom step is triggered, the configured External Service is called.

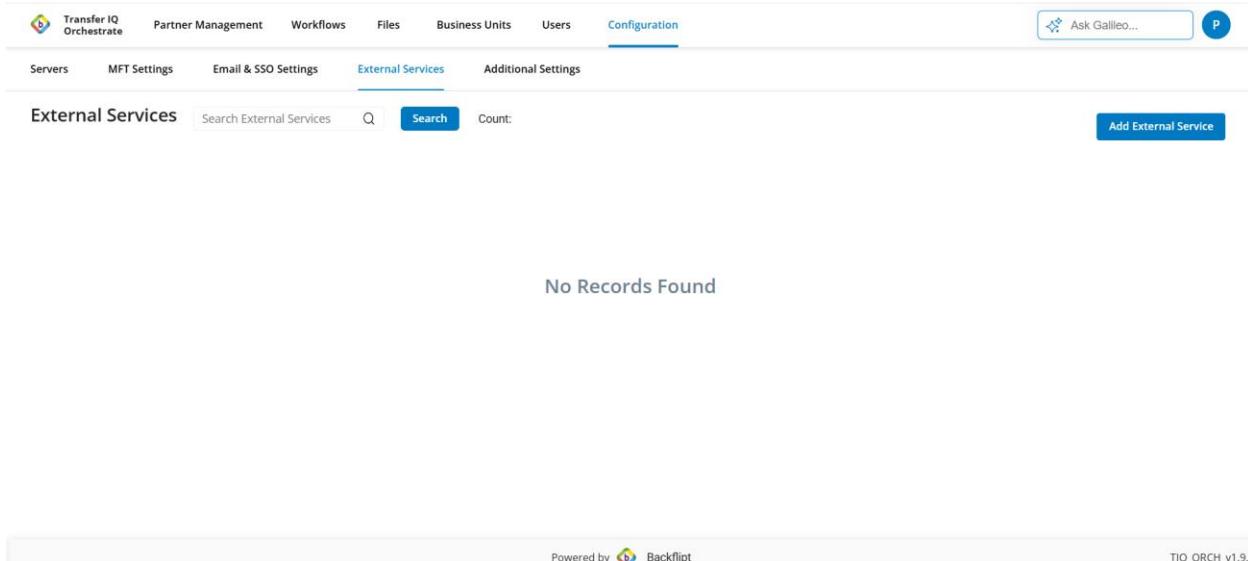
Orchestrate application supports the creation of multiple External Services, and each service can be reused across different workflows.

### Creating an External Service:

To create an external service:

1. Navigate to Configuration > External Services (if there are no external services created yet No Records Found Text will be displayed)





Transfer IQ Orchestrate

Partner Management Workflows Files Business Units Users Configuration

Ask Galileo... P

Servers MFT Settings Email & SSO Settings External Services Additional Settings

External Services Search External Services Q Search Count: 0

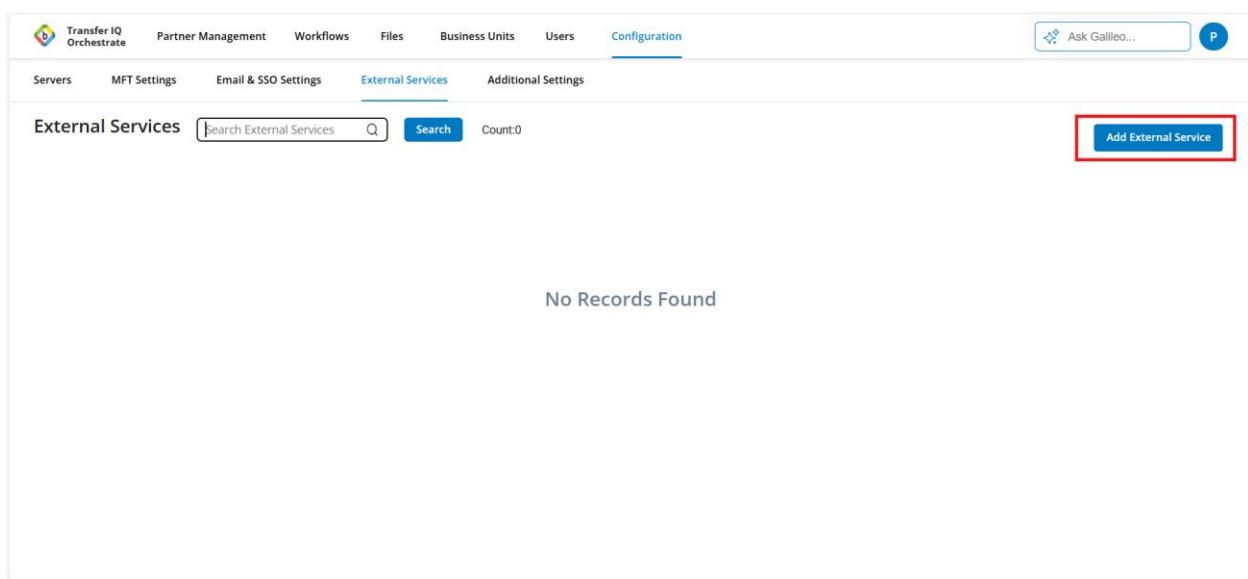
Add External Service

No Records Found

Powered by Backflipt

TIQ\_ORCH\_v1.9.7

## 2. Click on Add External Service



Transfer IQ Orchestrate

Partner Management Workflows Files Business Units Users Configuration

Ask Galileo... P

Servers MFT Settings Email & SSO Settings External Services Additional Settings

External Services Search External Services Q Search Count: 0

Add External Service

No Records Found

## 3. Once the **Add External Service** button is clicked, the **Add External Service** form is displayed with the following fields and buttons:



The screenshot shows the 'Add External Service' configuration page in Transfer IQ Orchestrate. The page has a header with tabs: Servers, MFT Settings, Email & SSO Settings, **External Services** (which is selected), and Additional Settings. Below the tabs, there are fields for Service Name, Service Description, Server Endpoint, Server Health Check Endpoint, Retry on Failure, Authentication Type, and Request Headers. A 'Test' button is located next to the Server Endpoint field. At the bottom right, there are 'Cancel' and 'Create' buttons.

- a. **Service Name \* (Mandatory)** - This field is used to enter a unique name for the external service. The service name is required and helps identify the external service when configuring and selecting it in workflow custom steps.
- b. **Service Description** - This optional field allows the user to provide a detailed description of the external service. It can be used to explain the purpose, functionality, or any important notes related to the service.
- c. **Server Endpoint \* (Mandatory)** - This field specifies the primary endpoint (URL) of the external service. This endpoint is invoked when the workflow executes the custom step that uses this external service. A valid and reachable URL must be provided.
- d. **Server Health Check Endpoint (Optional)** - This field is used to configure a health check endpoint for the external service. The system can call this endpoint to verify whether the external service is up and running.
- e. **Retry on Failure (Checkbox)** - Retry for a custom step execution is determined by the following two conditions:
  - i. **External service not reachable**
    1. If the external service is not reachable, the system automatically retries the custom step execution regardless of whether the **Retry on Failure** option is enabled or disabled.
  - ii. **Failure response from external service**
    1. If the external service returns a failure response, retry attempts are made **only if the Retry on Failure** option is enabled.
    2. When enabled, the system retries the execution up to **three times** at intervals of **5, 10, and 15 minutes**.



3. If the option is disabled, no retry attempts are performed.

f. **Authentication Type\* (Mandatory Dropdown)** - This dropdown allows the user to select the authentication mechanism required to access the external service. Selecting an authentication type is mandatory. Based on the selected option, additional authentication-related fields may be displayed for configuration. Below are the three types of authentication types that are supported by the orchestrate application

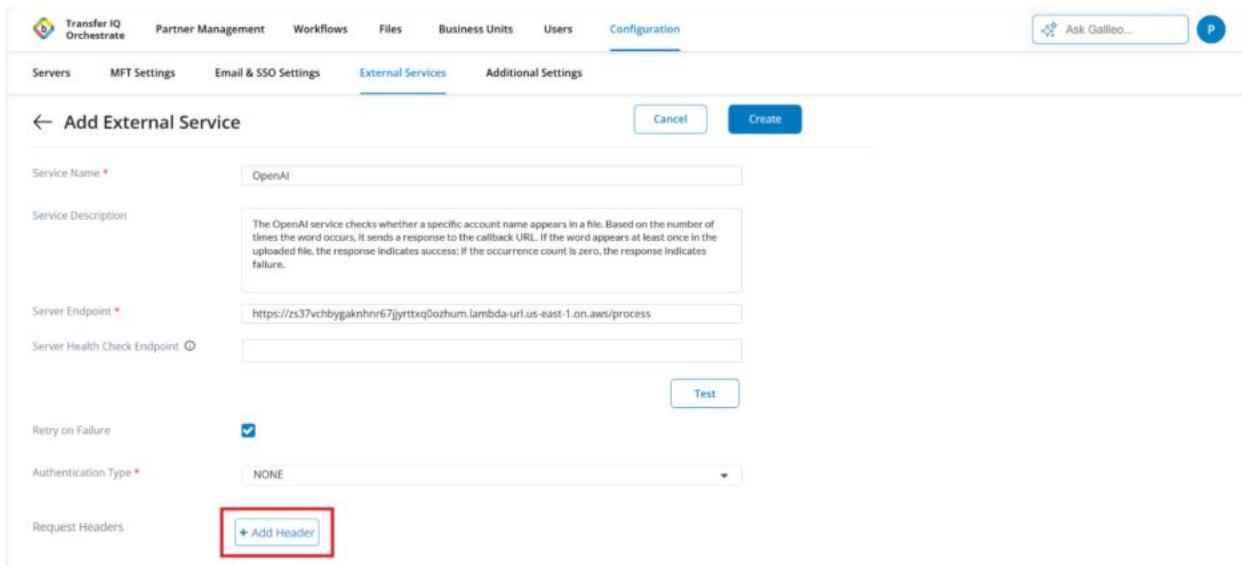
- i. **None** - This option indicates that no authentication is required to access the external service. When selected, the request is sent without any authentication credentials.
- ii. **Basic** - This option enables Basic Authentication, where a username and password are required. When **Basic** is selected, additional fields are displayed to capture the username and password.



iii. **API Key** - This option enables authentication using an API key. When API Key is selected, additional fields are displayed to enter the API key details, such as the header key and value.

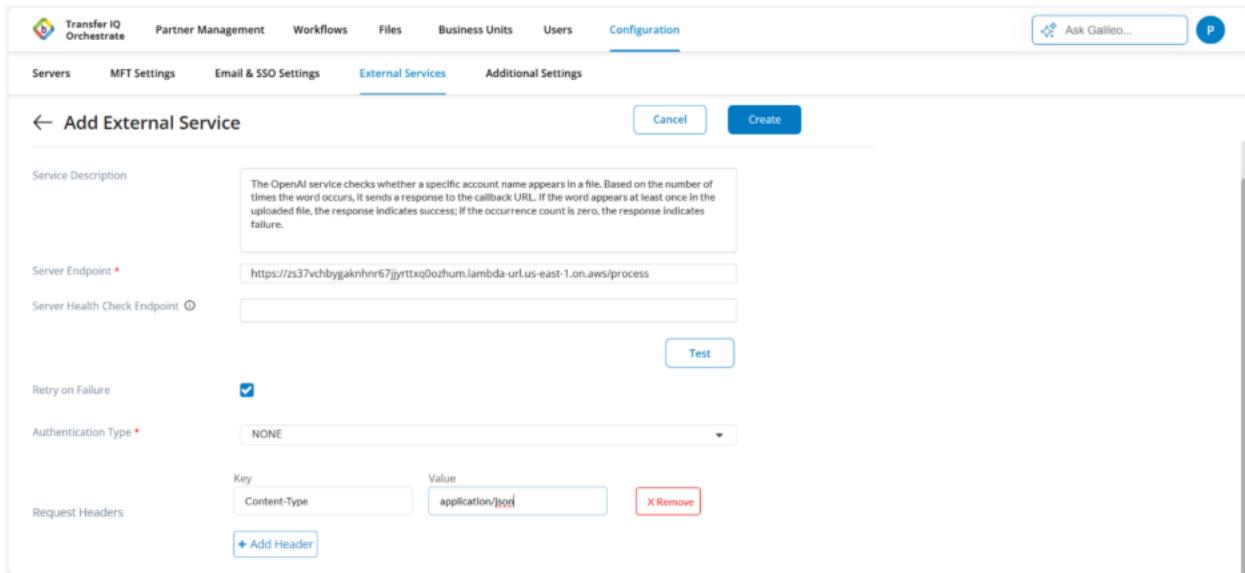
#### 4. Request Headers

- This section allows users to define custom HTTP request headers that will be included when invoking the external service.
- Click the add header button



The screenshot shows the 'Add External Service' configuration page. The 'External Services' tab is active. The 'Request Headers' section contains an 'Add Header' button, which is highlighted with a red box. Other fields in this section include 'Service Name' (OpenAI), 'Service Description' (a detailed text box), 'Server Endpoint' (a URL), 'Server Health Check Endpoint' (an empty field), 'Test' button, 'Retry on Failure' (checked), 'Authentication Type' (set to 'NONE'), and a dropdown menu.

- Clicking the **Add Header** button displays two input fields—**Key** and **Value**—along with a **Remove** button. This enables administrators to add one or more key-value header pairs and remove any existing headers as needed
- Request headers are commonly used to pass authorization tokens, Content type information, or other required metadata to the external service.
- Multiple Headers can be added by clicking the **Add Header** button multiple times



Transfer IQ Orchestrate

Partner Management Workflows Files Business Units Users Configuration

Servers MFT Settings Email & SSO Settings External Services **External Services** Additional Settings

← Add External Service

Service Description: The OpenAI service checks whether a specific account name appears in a file. Based on the number of times the word occurs, it sends a response to the callback URL. If the word appears at least once in the uploaded file, the response indicates success; if the occurrence count is zero, the response indicates failure.

Server Endpoint:

Server Health Check Endpoint:

Test

Retry on Failure:

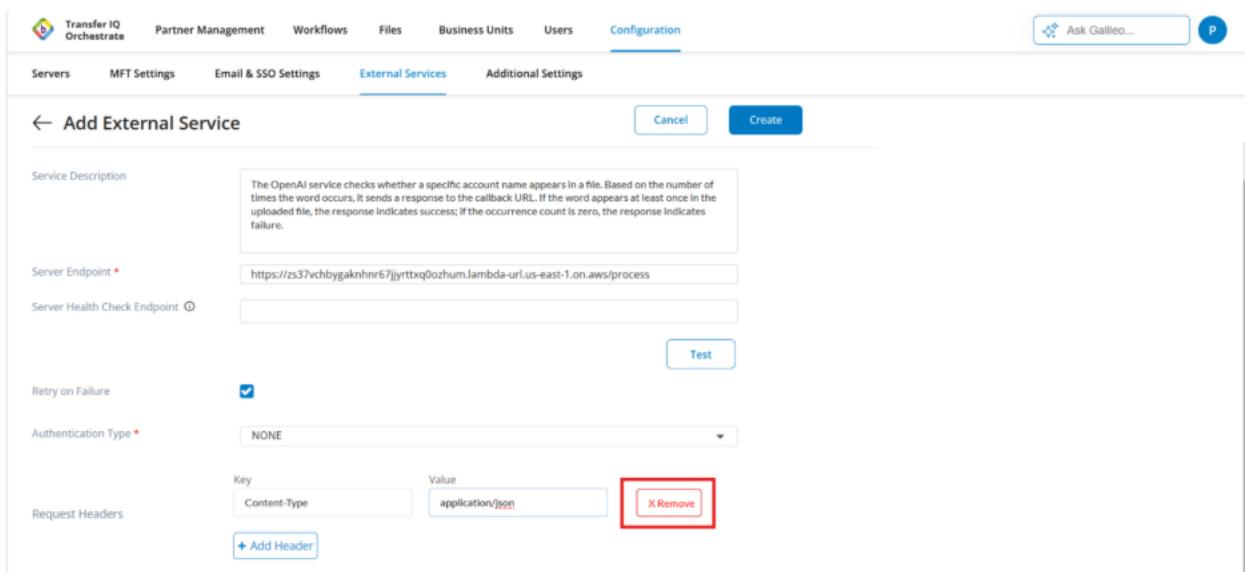
Authentication Type:

Request Headers:

Key	Value	Action
Content-Type	application/json	X Remove

+ Add Header

f. Clicking the remove button will remove the added header



Transfer IQ Orchestrate

Partner Management Workflows Files Business Units Users Configuration

Servers MFT Settings Email & SSO Settings External Services **External Services** Additional Settings

← Add External Service

Service Description: The OpenAI service checks whether a specific account name appears in a file. Based on the number of times the word occurs, it sends a response to the callback URL. If the word appears at least once in the uploaded file, the response indicates success; if the occurrence count is zero, the response indicates failure.

Server Endpoint:

Server Health Check Endpoint:

Test

Retry on Failure:

Authentication Type:

Request Headers:

Key	Value	Action
Content-Type	application/json	X Remove

+ Add Header



The screenshot shows the Transfer IQ Orchestrate configuration interface. The top navigation bar includes 'Transfer IQ Orchestrate', 'Partner Management', 'Workflows', 'Files', 'Business Units', 'Users', and 'Configuration'. The 'Configuration' tab is selected. Below it, the 'External Services' tab is active. A sub-form titled 'Add External Service' is displayed, with a 'Service Name' field containing 'OpenAI'. The 'Server Endpoint' field contains the URL 'https://zs37vchbygaknhr67jjyrttxq0zuhm.lambda-url.us-east-1.on.aws/process'. A 'Test' button is located below the endpoint field. Other fields include 'Service Description' (with a detailed description of the OpenAI service), 'Server Health Check Endpoint' (empty), 'Retry on Failure' (checked), 'Authentication Type' (set to 'NONE'), and 'Request Headers' (with a '+ Add Header' button). A 'Cancel' and 'Create' button are at the top right of the sub-form.

5. **Test External Service** - The **Test** button is used to validate the connectivity and availability of the configured external service before saving the configuration. When clicked, the system sends a request to the **Server Health Check Endpoint** (or the primary server endpoint if a health check endpoint is not configured) to verify that the external service is reachable and responding as expected. This functionality helps ensure that the provided endpoint details are correct and that the external service is operational.

- Based on the outcome of the test, the system displays appropriate messages to inform the user of the result:
- If the endpoint is reachable and responds successfully, a success message is displayed indicating that the connection to the external service was successful. If the endpoint is unreachable, returns an error response, or does not respond within the expected time, a failure message is displayed.



6. Once entering all the required data, click the Create button to create an External Service

7. Once Created the created service will be displayed in External Services Table View



External Service Name	External Service ID	External Service URL	Retry on Failure	Authentication Type	Actions
OpenAI	00001	https://qa-mock-server.xeninc.us/p...	No	NONE	

## Update External Service:

Once an external service is created, its configuration can be updated. All details entered during creation can be edited and saved. There are two ways to update an external service:

1. Click the **Edit** icon next to the external service in the view table.
2. By navigating to the external service's detail view and clicking the **Edit** button.

### Option 1: Edit from the View Table

1. Navigate to **Configuration > External Services**.
2. Search for the required external service.
3. Click the **Edit** icon next to the external service in the view table.

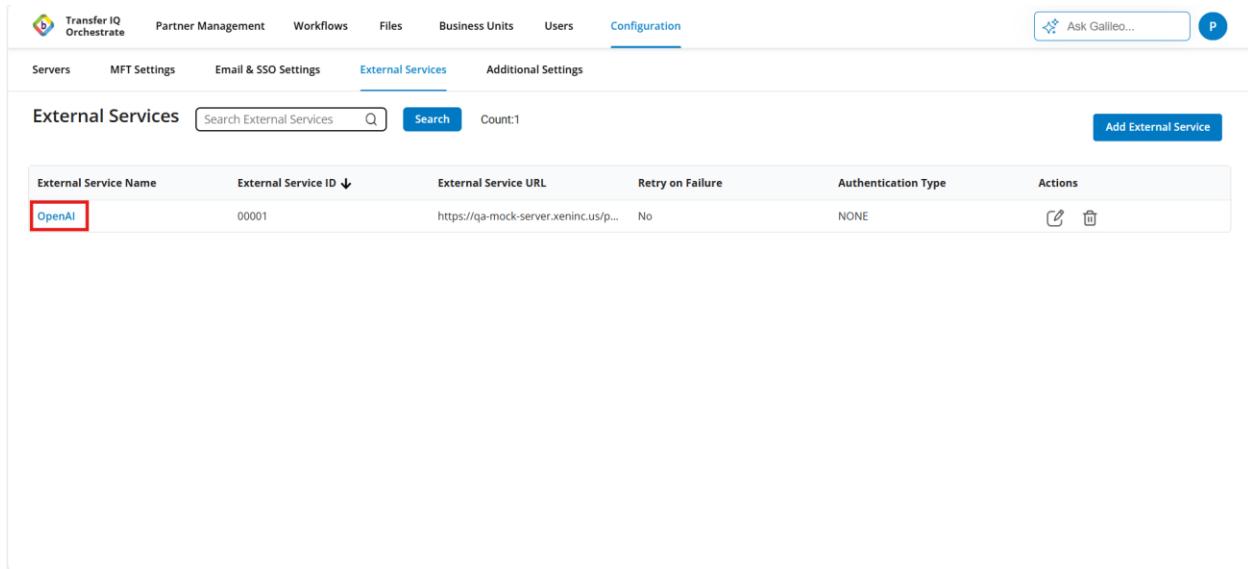


4. Modify the required fields.
5. Click **Update** to save the changes.

## Option 2: Edit from the External Service Details View Mode

1. Navigate to **Configuration > External Services**.
2. Search for the required external service.
3. Click the external service name (displayed in blue), which opens the service details in view mode.

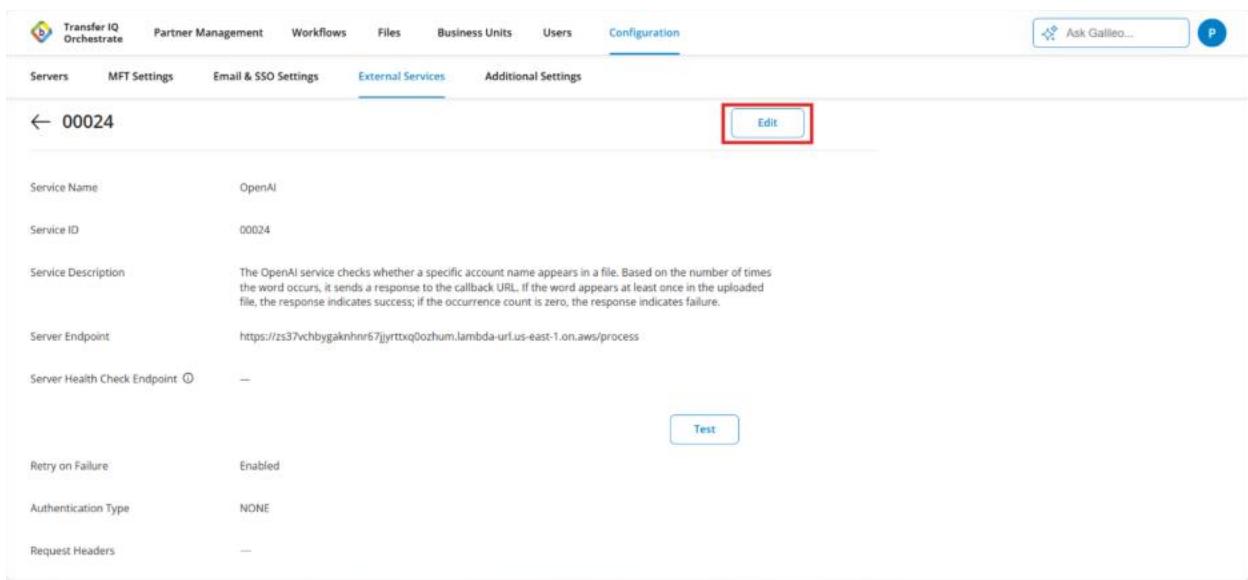




External Services

External Service Name	External Service ID	External Service URL	Retry on Failure	Authentication Type	Actions
OpenAI	00001	https://qa-mock-server.xeninc.us/p...	No	NONE	 

4. Click the **Edit** button in the form header.



← 00024

Service Name: OpenAI

Service ID: 00024

Service Description: The OpenAI service checks whether a specific account name appears in a file. Based on the number of times the word occurs, it sends a response to the callback URL. If the word appears at least once in the uploaded file, the response indicates success; if the occurrence count is zero, the response indicates failure.

Server Endpoint: https://zs37vhbygaknhn67jjjtttxq0ozhum.lambda-url.us-east-1.on.aws/process

Server Health Check Endpoint: —

Retry on Failure: Enabled

Authentication Type: NONE

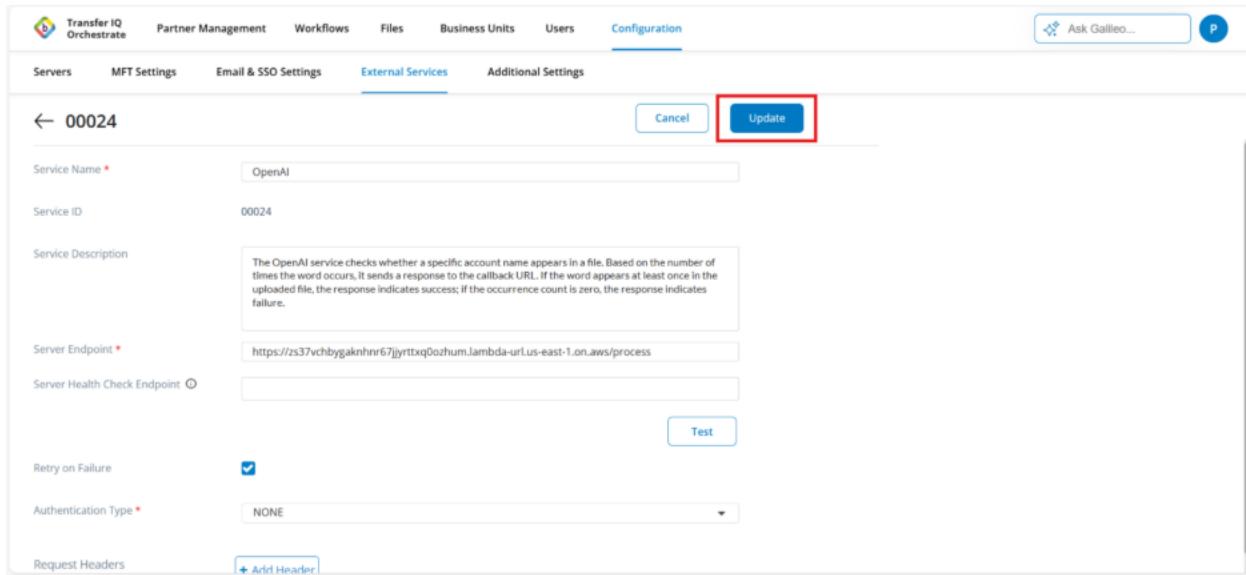
Request Headers: —

**Edit**

**Test**

5. Update the required fields.  
6. Click **Update** to save the changes.





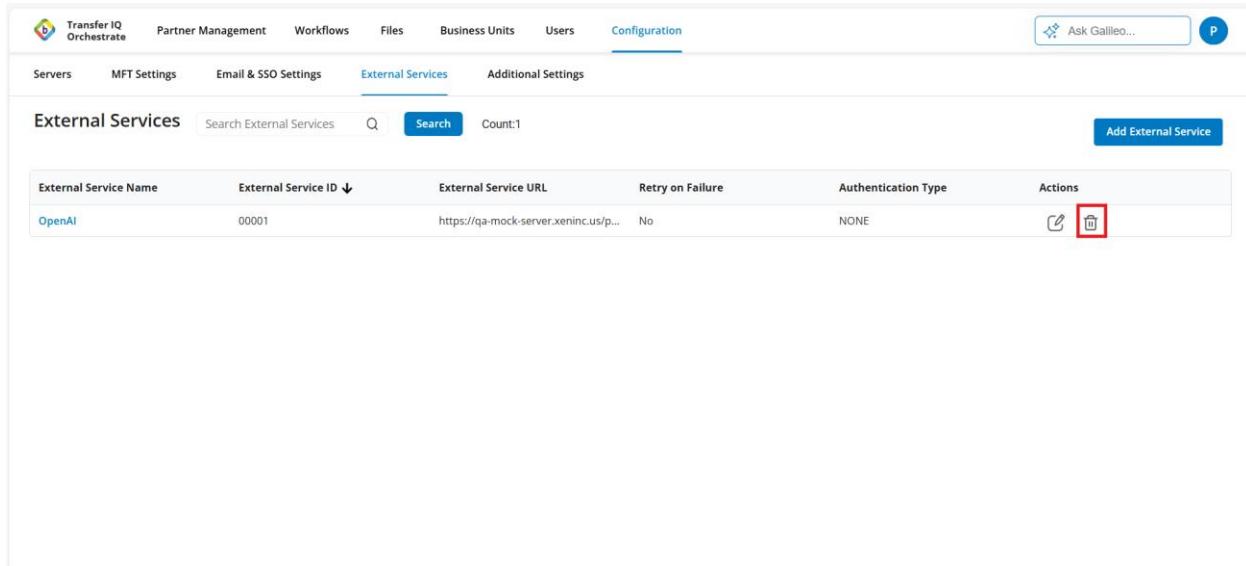
The screenshot shows the 'External Services' configuration screen for an external service named 'OpenAI' with ID '00024'. The 'Update' button is highlighted with a red box. The service description is: 'The OpenAI service checks whether a specific account name appears in a file. Based on the number of times the word occurs, it sends a response to the callback URL. If the word appears at least once in the uploaded file, the response indicates success; if the occurrence count is zero, the response indicates failure.' The server endpoint is 'https://zs37vchbygaknhn67jyrttxq0zum.lambda-url.us-east-1.on.aws/process'. The 'Request Headers' section has a '+ Add Header' button.

**Note:** The connection to an external service can be tested from the **Edit** screen, both in **view mode** and **edit mode**.

## Delete External Service

To delete an external service, follow the below steps

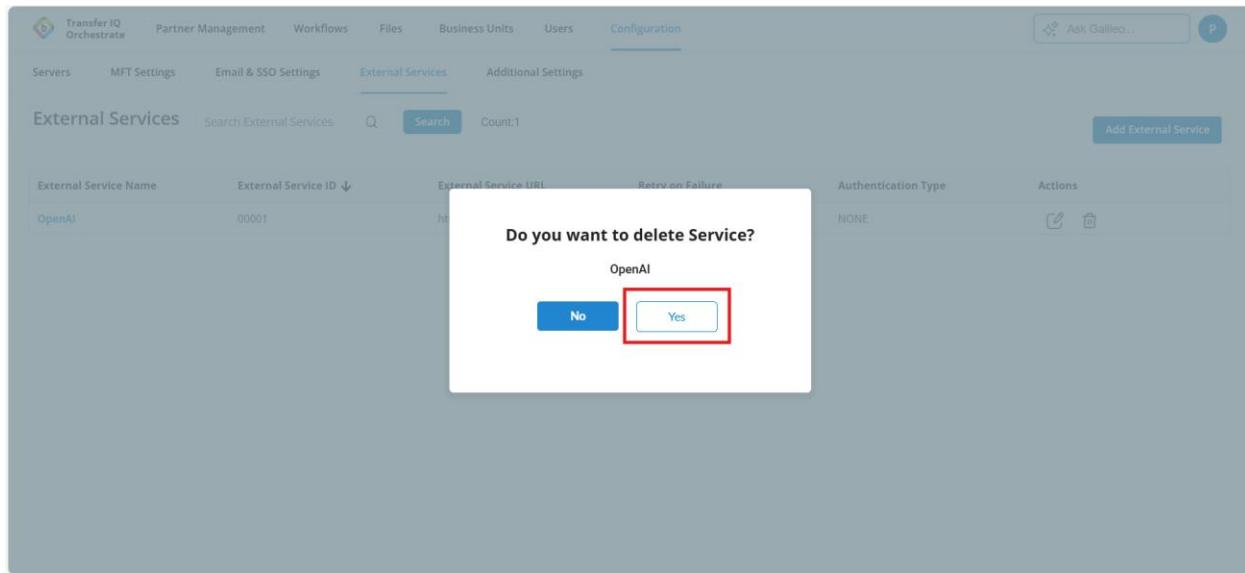
1. Click the Delete Button



The screenshot shows the 'External Services' list screen. The table has columns: External Service Name, External Service ID, External Service URL, Retry on Failure, Authentication Type, and Actions. The 'Actions' column for the 'OpenAI' service has a delete icon highlighted with a red box.

2. A confirmation popup will be displayed before the service is deleted.
3. Clicking the Yes button in the popup will remove the external service, while No will keep it unchanged.





## Support

### Backflift Standard Support Model

- Backflift's Standard Support model includes Phone and Email support.
- Email – [Support@backflift.com](mailto:Support@backflift.com)
- Phone – 408-890-2032
- Between 7 am PST to 5 pm PST

