TransferIQ Orchestrate
Quick start guide

Table Of Contents

Introduction

The TransferIQ Orchestrate App seamlessly integrates with MFT/B2Bi solutions, providing a customized digital experience for onboarding trading partners and setting up file routes through a self-service platform with robust administrative oversight. A configurable workflow orchestrates the onboarding and file routing processes, enhancing collaboration and progress visibility for business users, administrators, and approvers. This system significantly reduces the time and resources needed to onboard and exchange files with new partners and 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

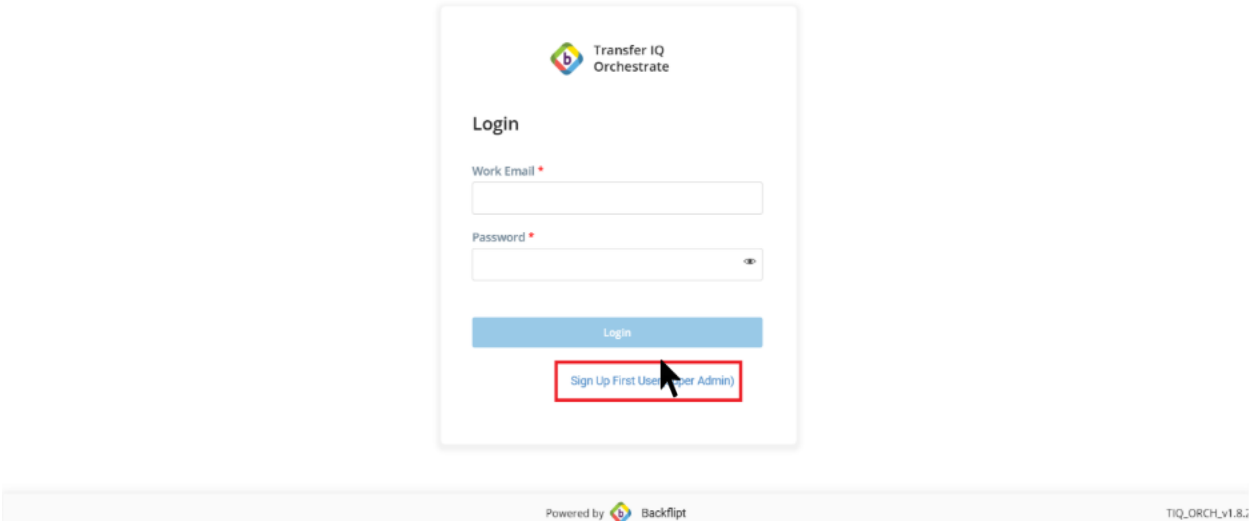
When the **Transfer IQ Orchestrate Application** is launched for the first time, the application does not contain any registered users. Since access to the application is restricted, it is necessary to add the **first user to start using the application**

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**

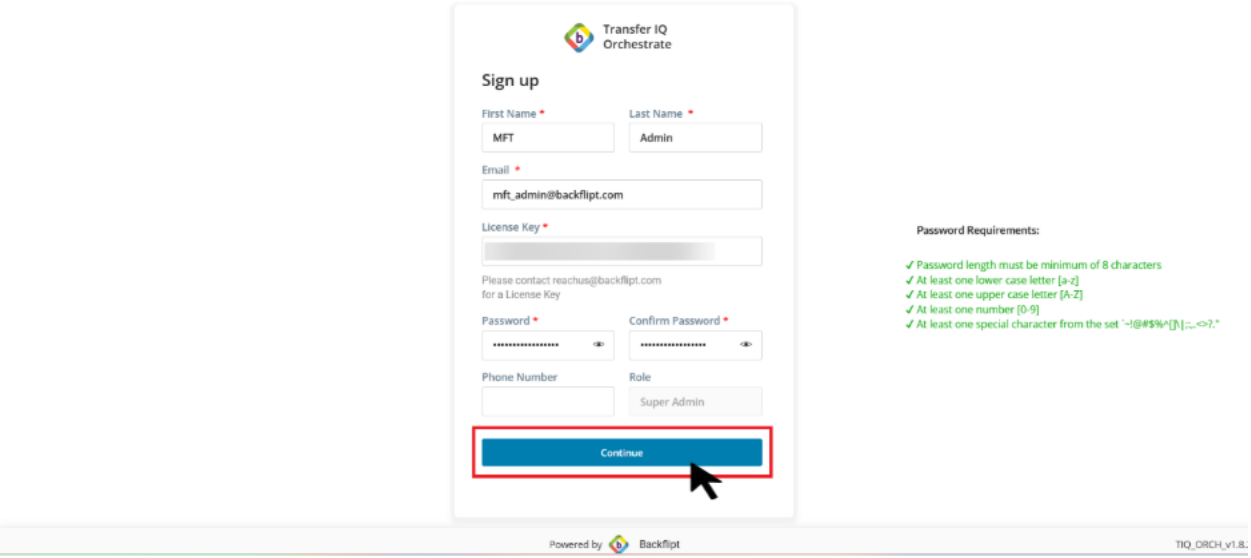


2. Once the button is clicked a signup form will be displayed with the following fields
    a. **First Name** – The first name of the Super Admin.
    b. **Last Name** – The last name of the Super Admin.
    c. **Email Address** – A valid email to be used for login and communication.
    d. **License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

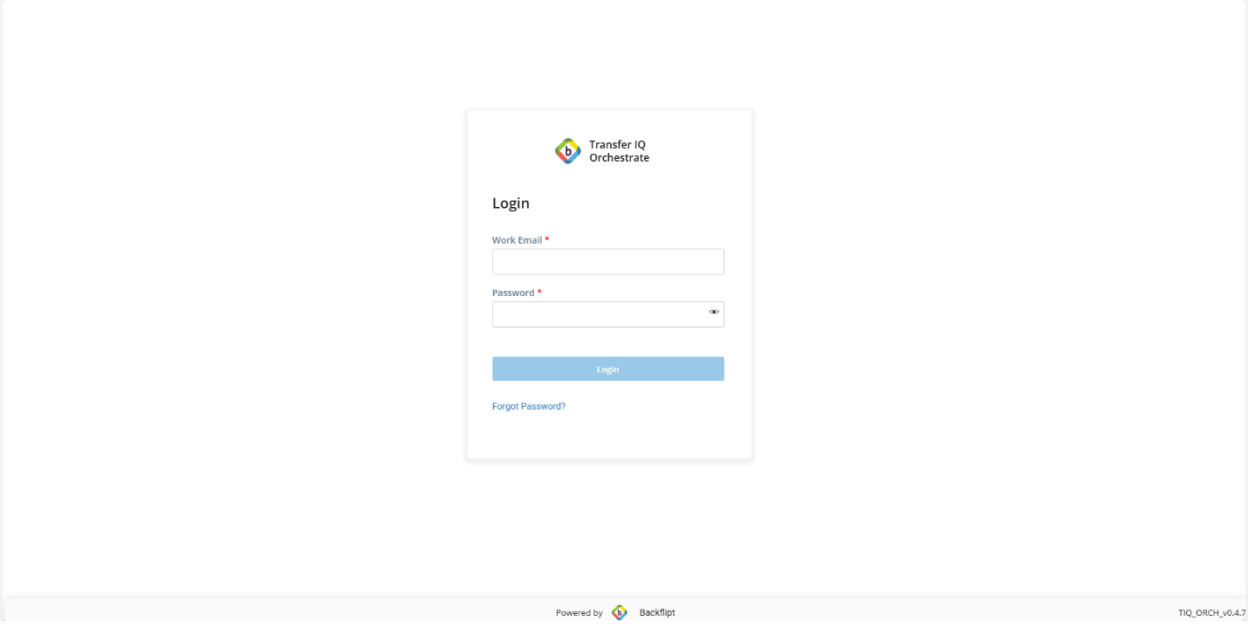
signing up for the first time. This key will then be used by the admin to log in to the application.

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

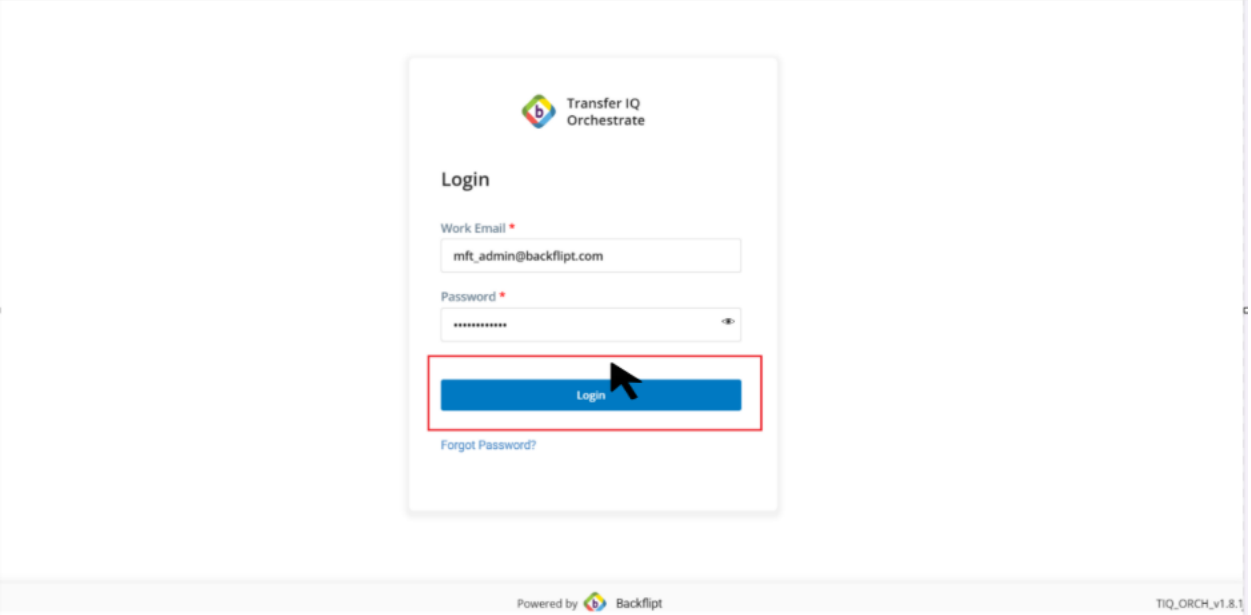
3. Click the **Continue** button to complete the registration process



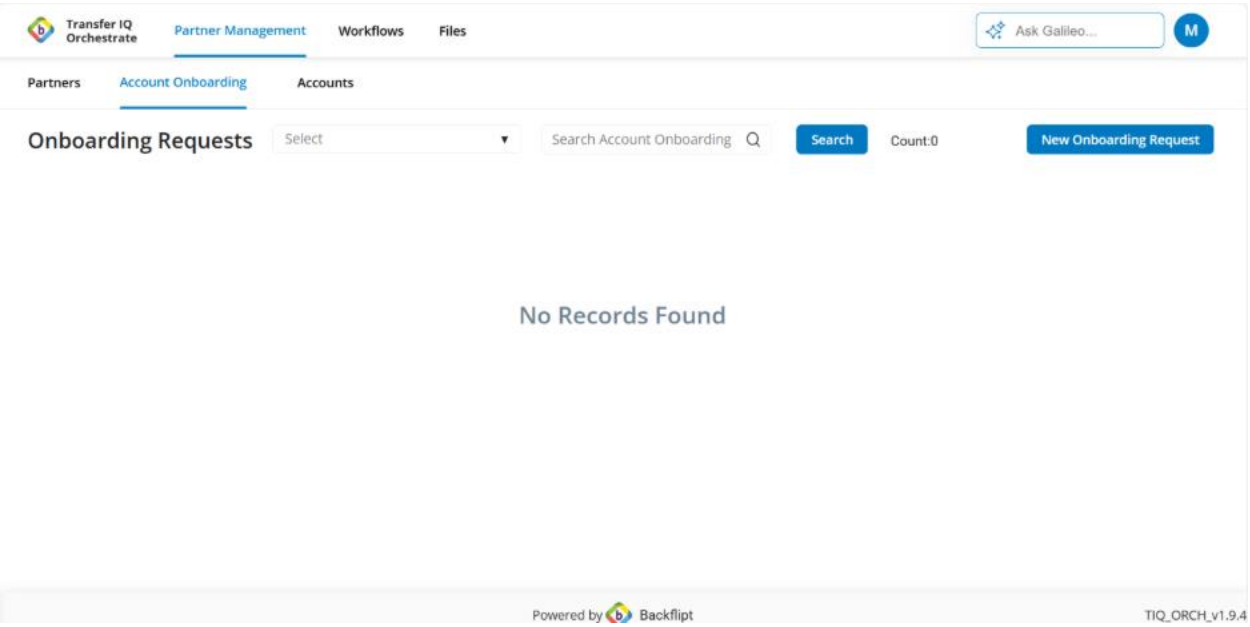
4. After the Super Admin is successfully registered, the application redirects to the following **Login page**.



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



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



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

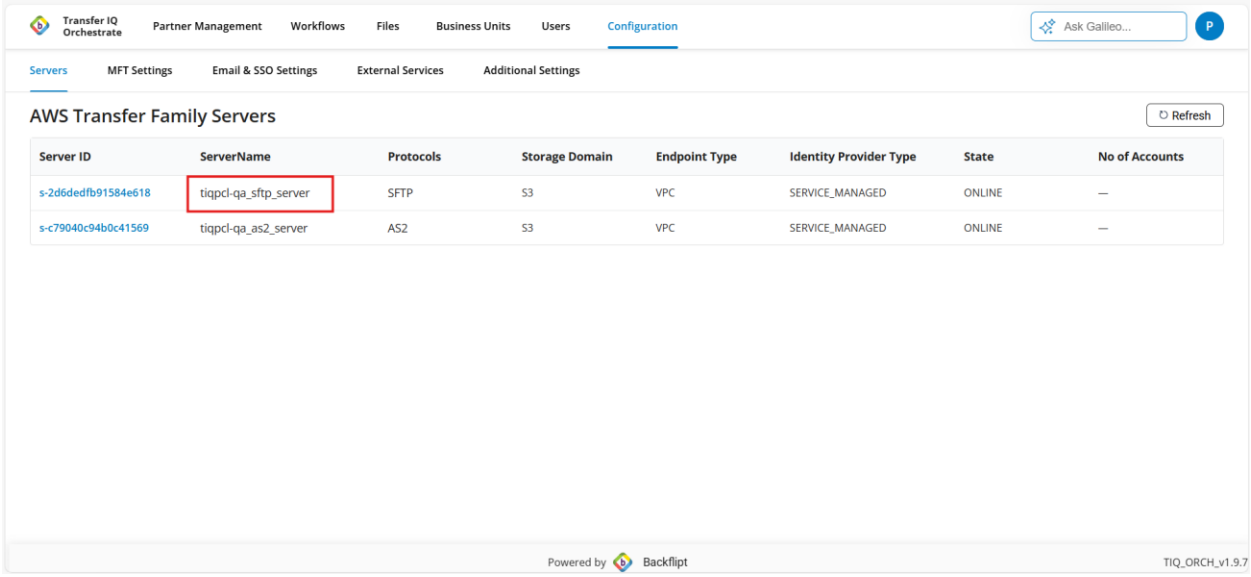
When the user clicks on Configuration tab navigates to the Servers **(AWS Transfer Family Servers)** which displays the details of the servers deployed in a table format

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).

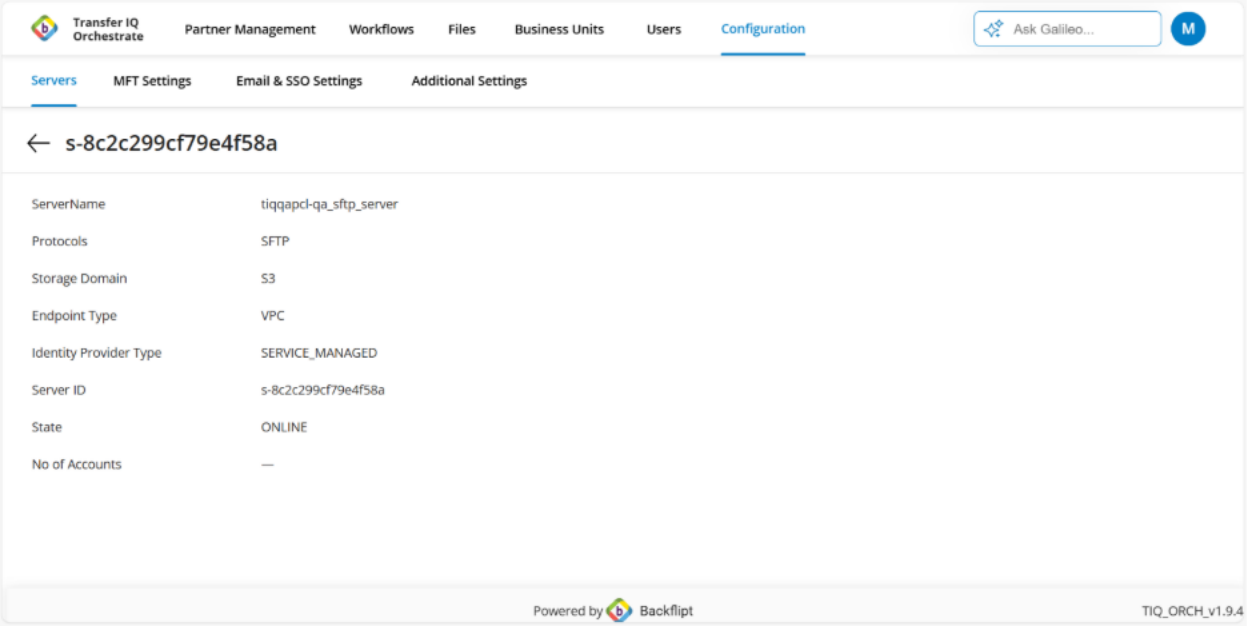
Users can click on the **Server ID** to view more detailed information about that server.



The 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:

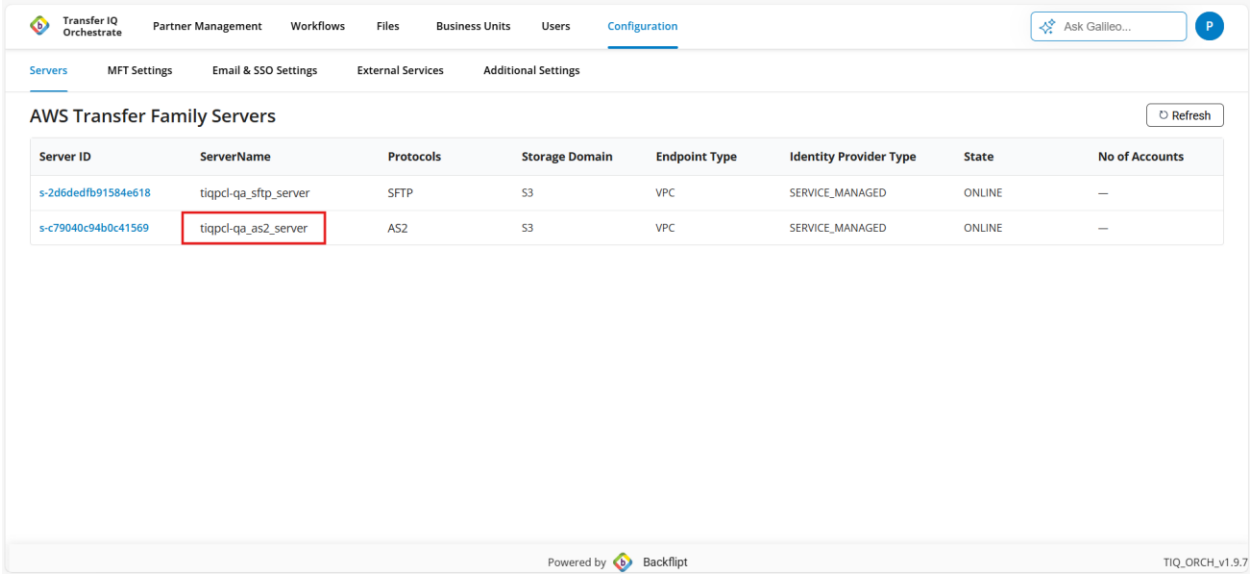
- Server Name
- Protocol
- Storage Domain
- Endpoint Type
- Identity Provider Type
- Server ID
- State
- No of Accounts



AS2 Protocol

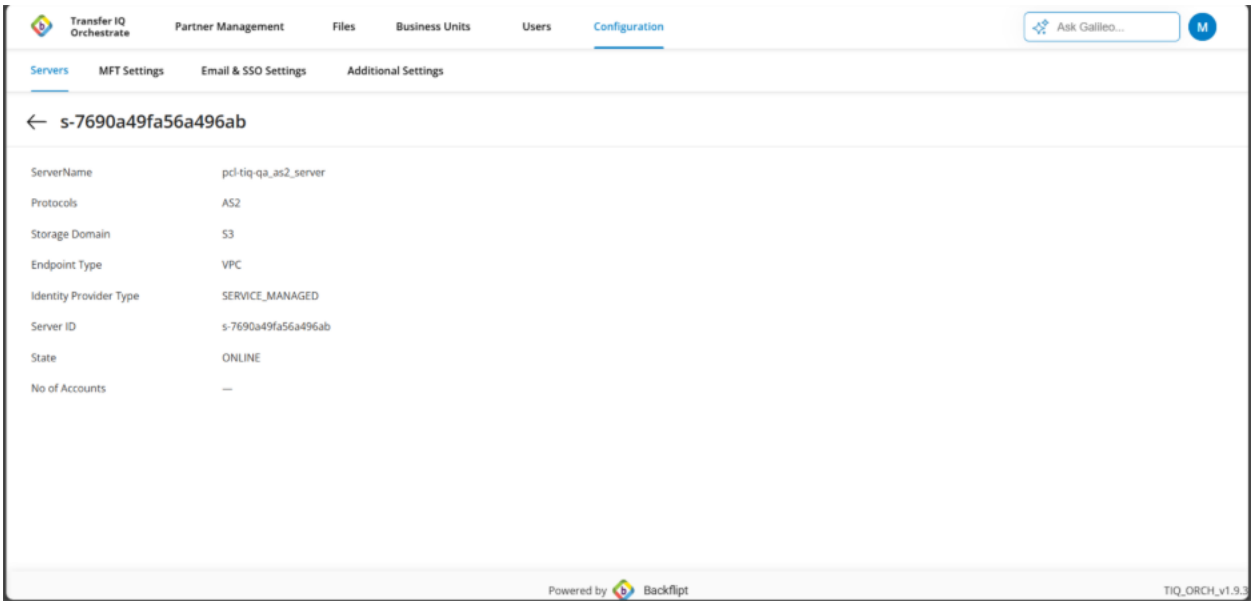
When only AS2 is deployed, The **AWS Transfer Family Server** section displays the AS2 server configured for the company with the following details

a) **Server ID:** A unique identifier for the AS2 server. This is clickable and navigates the user to the server details page.
b) **Server Name**: Name of the Server deployed, e.g. as2_server
c) **Protocol:** AS2
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 as blank (_)



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



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

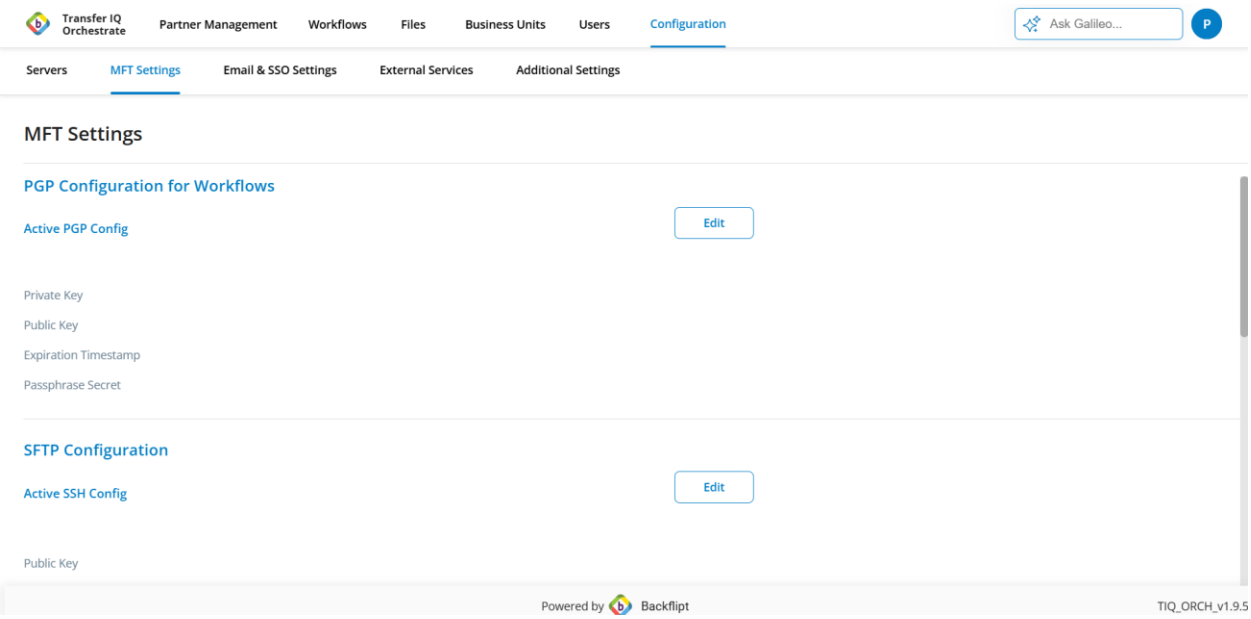
SFTP Protocol

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:

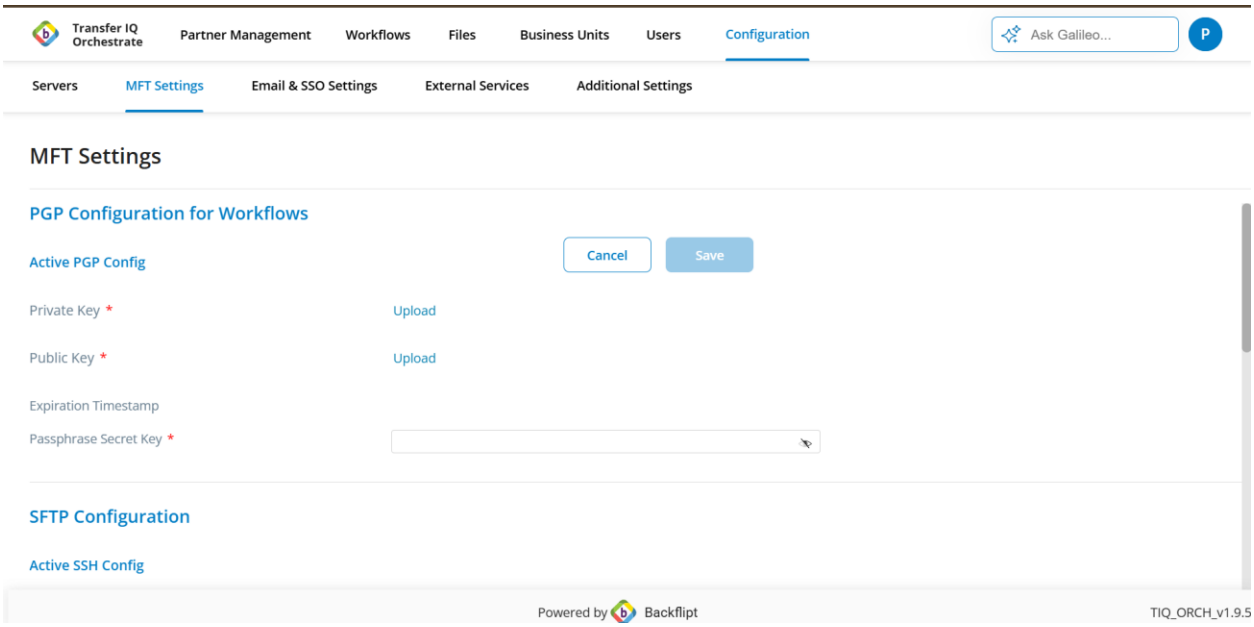
It includes the following sections:

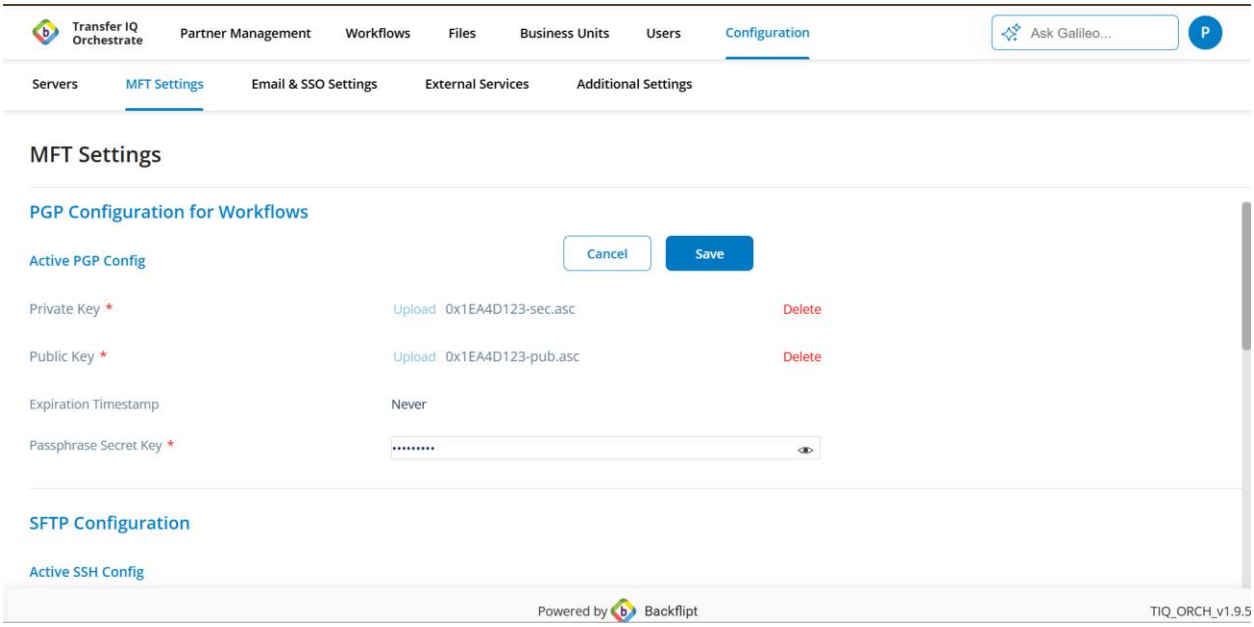
a. PGP Configuration
b. SFTP Configuration



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





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).

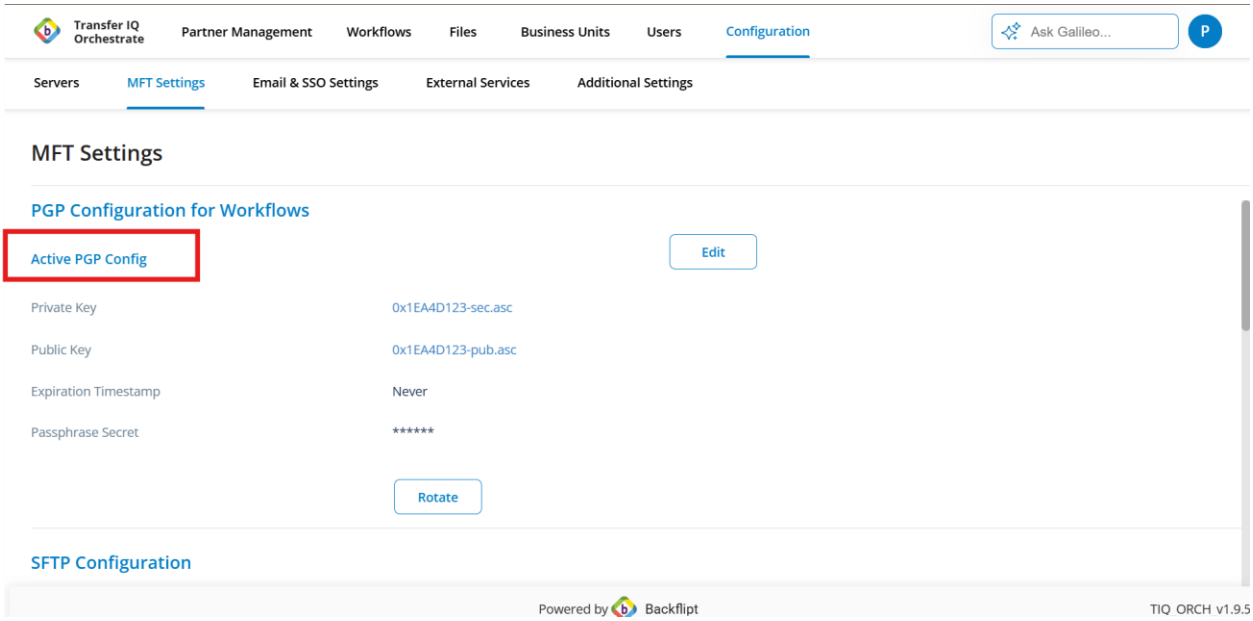
Company PGP Key Rotation

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

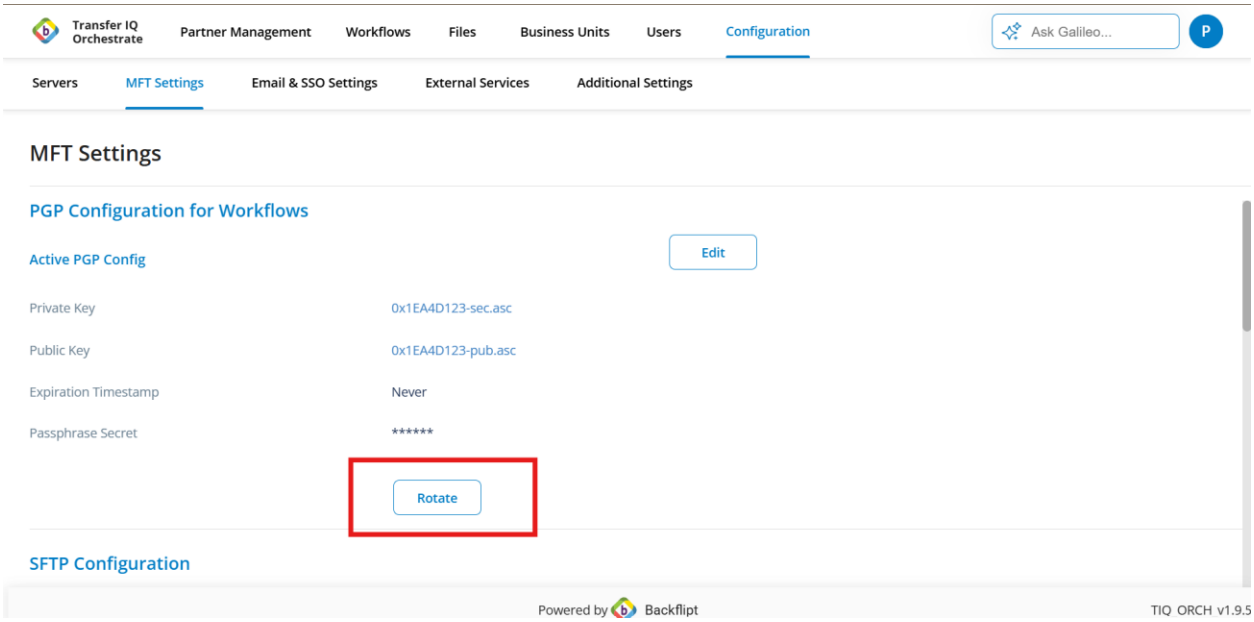
At this stage, the system continues to rely solely on the active keys for all ongoing file transfers and workflow executions.



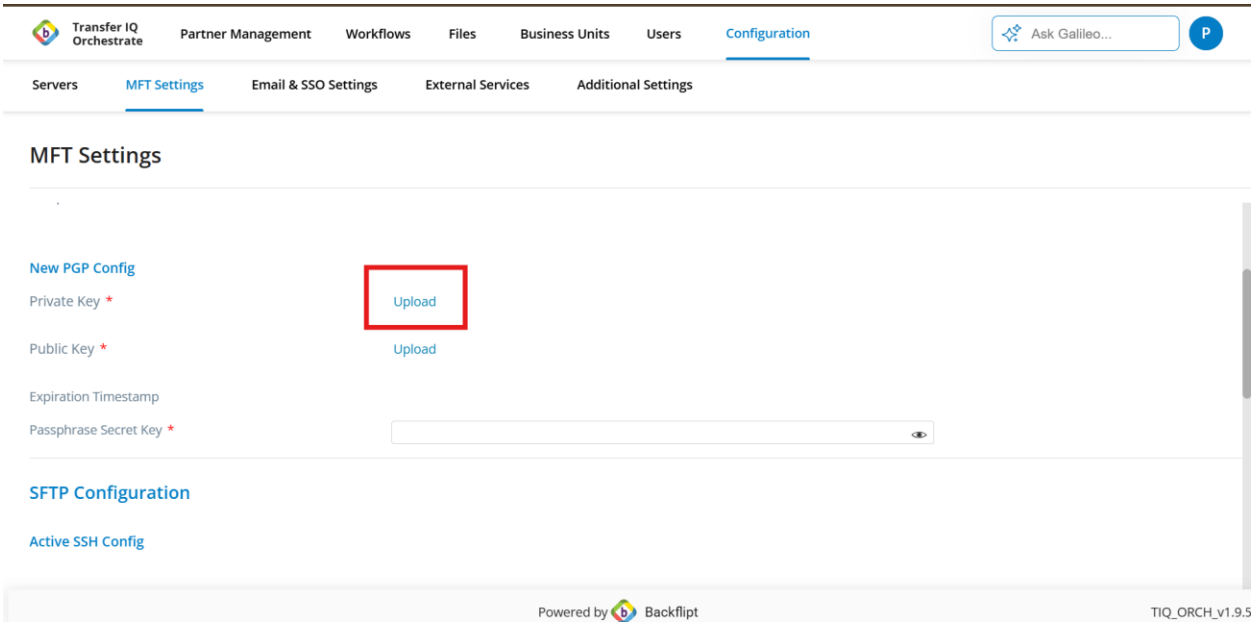
2. During Rotation

To begin the rotation process

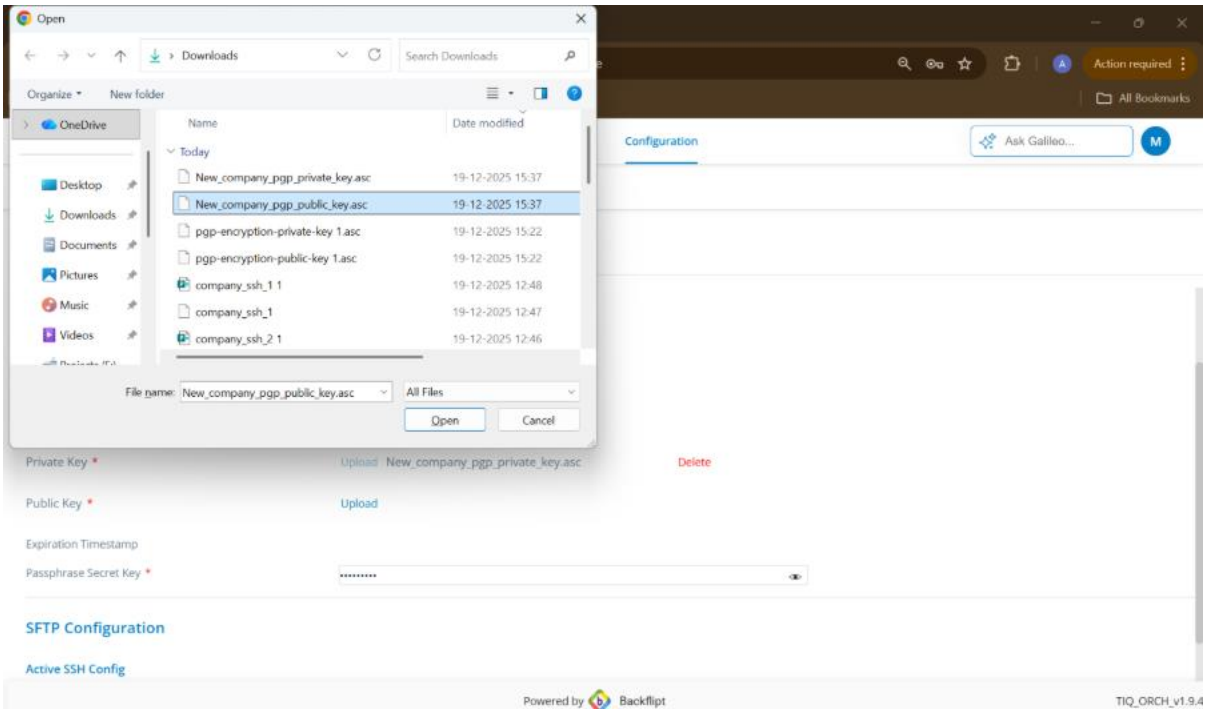
1. Navigate to **MFT Settings > Active PGP Keys**.
2. Click the **Rotate** button located next to the *Active PGP Keys* section



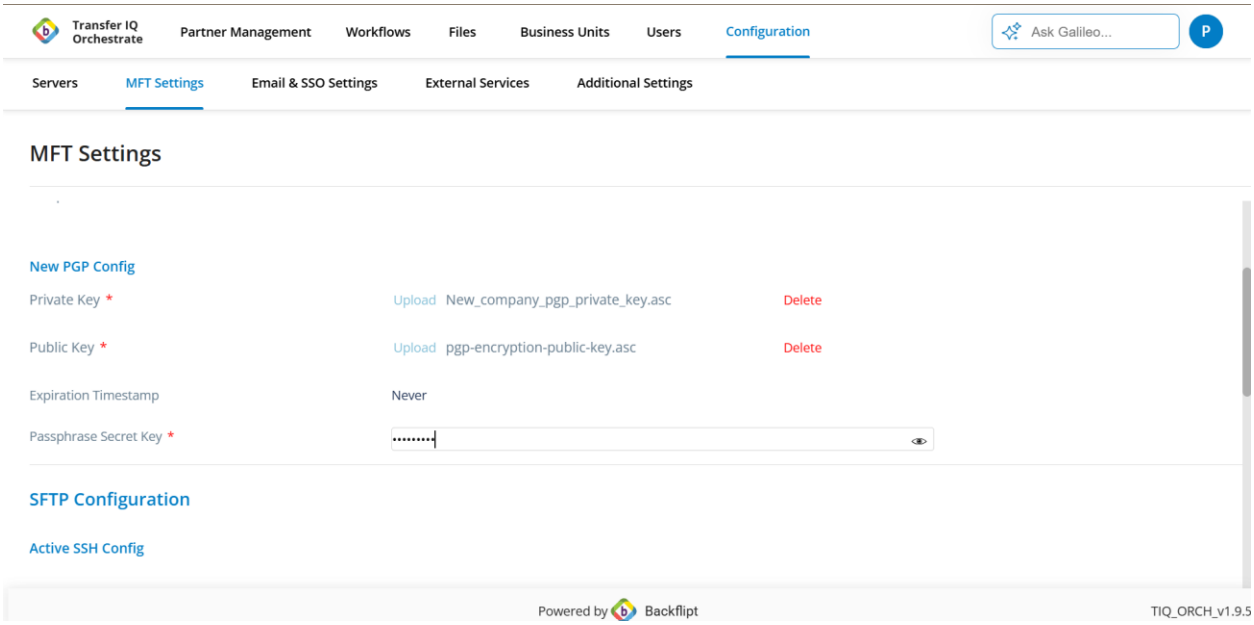
3. This action displays an additional section labeled **New PGP Keys**, which includes fields for uploading both **public** and **private** PGP keys along with the corresponding **passphrase**.
4. To upload the new keys, click the **Upload** button under the **New PGP** *Keys* section.



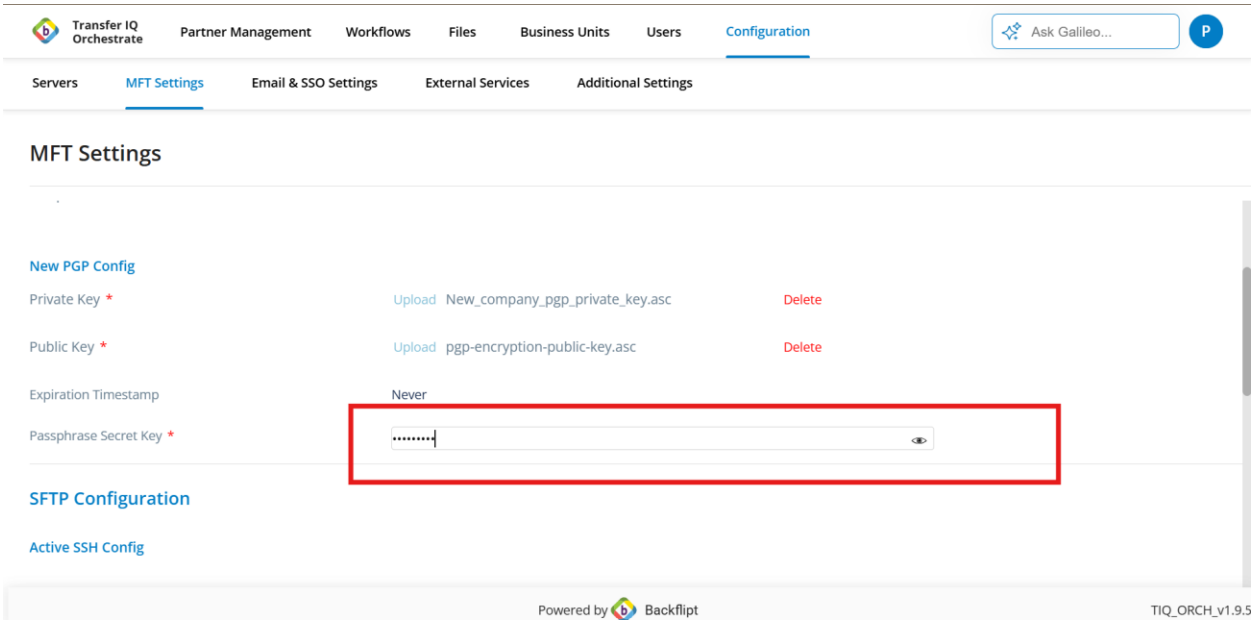
5. In the file selection dialog, choose a valid PGP key file.



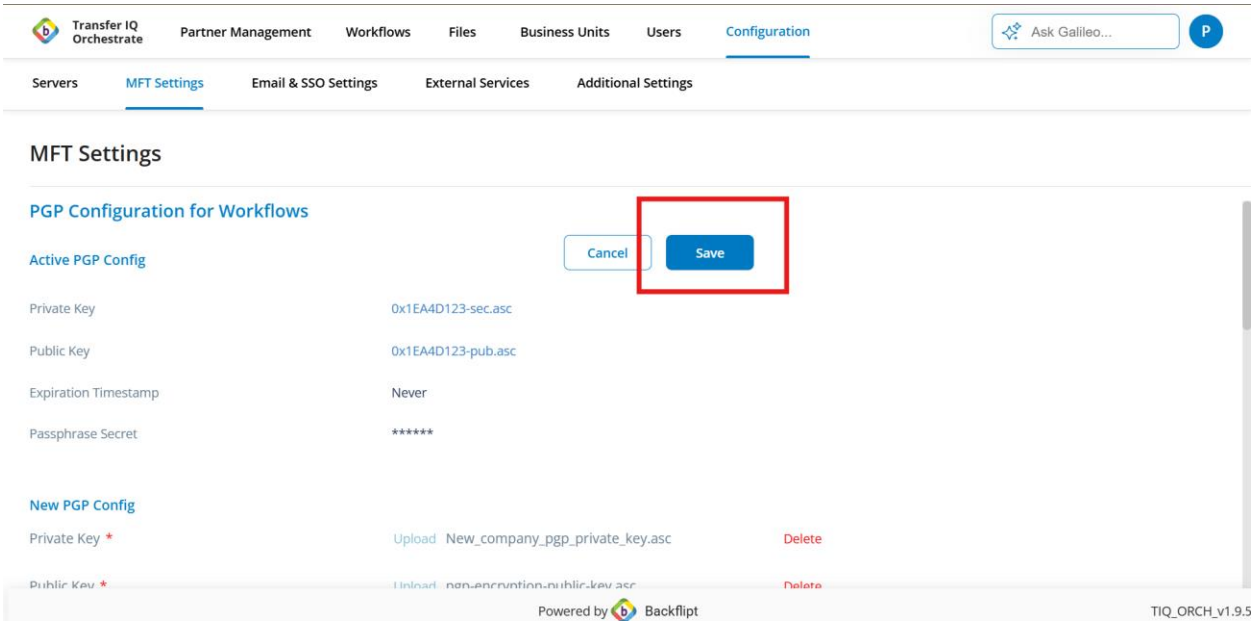
6. Once the file is uploaded successfully, the newly uploaded keys are displayed in the **MFT Settings** tab under the **New PGP Keys** section with an expiration timestamp.

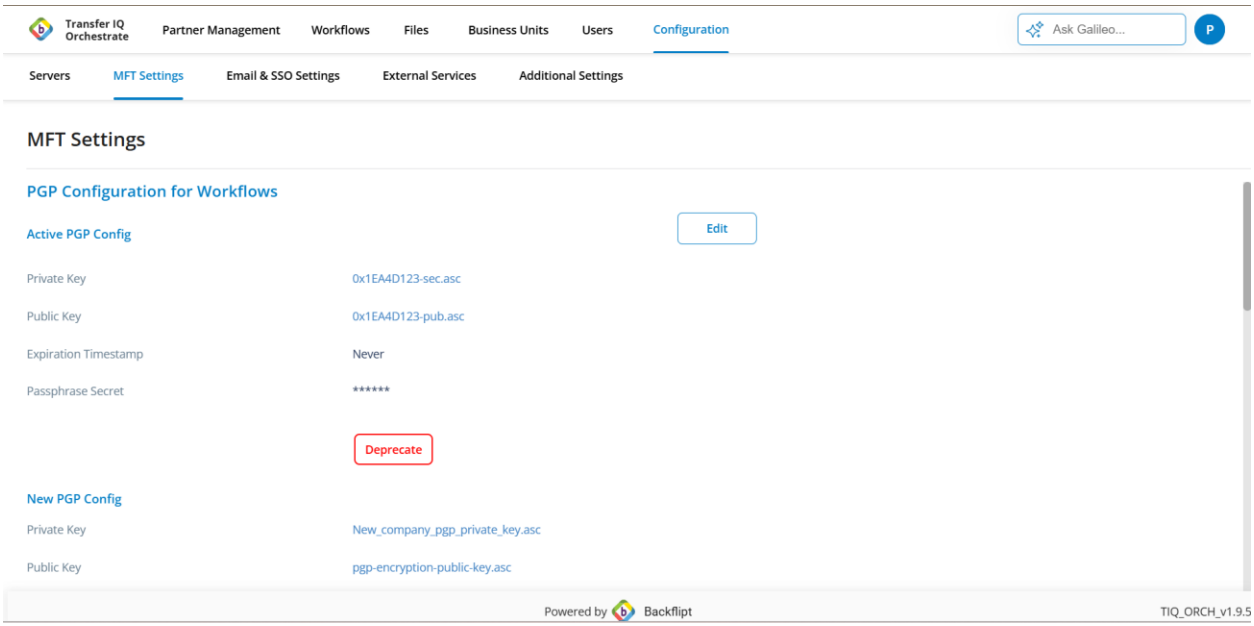


7. Enter a valid passphrase in the Passphrase Secret Key Field



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.





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.

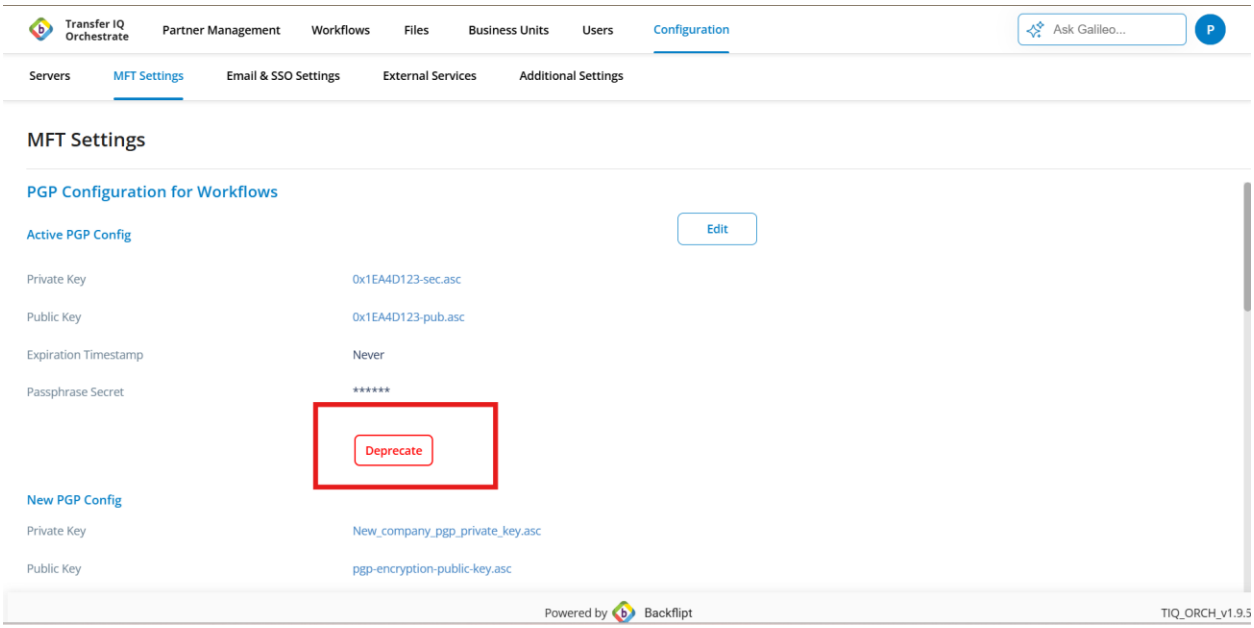
This alternating validation process — where the system switches between new and old keys — is referred to as the **ping-pong mechanism**.

PGP Key Deprecation

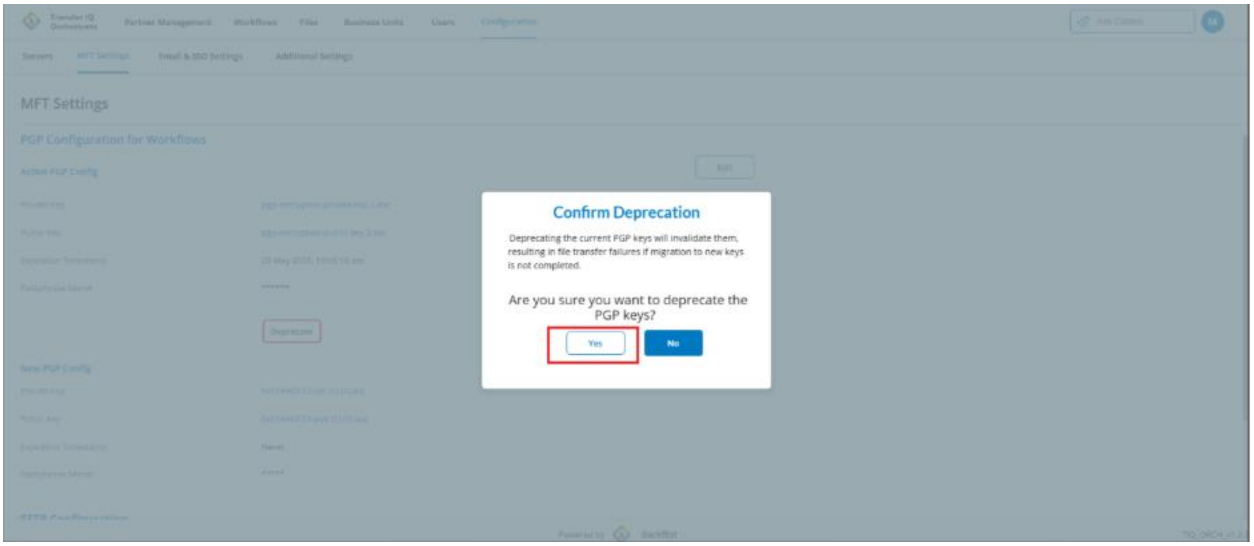
Deprecating a PGP key means disabling the old PGP key, so it can no longer encrypt or decrypt files, ensuring that only the newly rotated PGP key is used for secure file transfers.

Deprecating PGP Keys

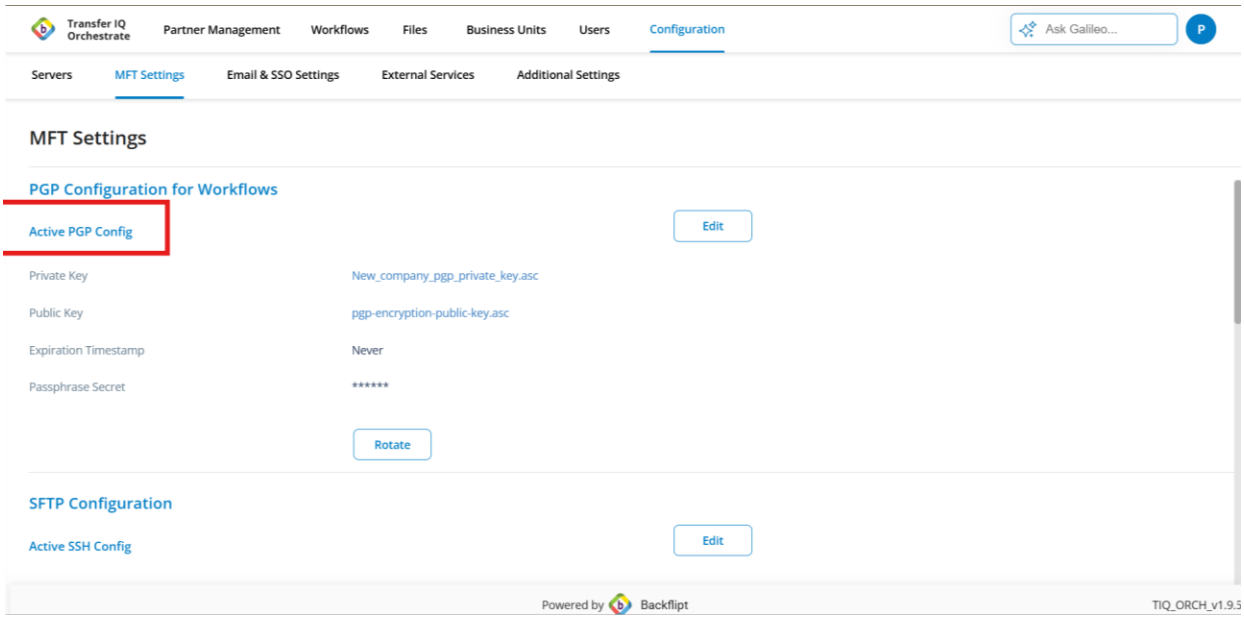
1. Navigate to the **Active PGP Keys** section in the MFT Settings tab.
2. Click the **Deprecate** button next to the old active **PGP** key.



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 key is **removed completely** from the application.



File Transfer Behavior During Deprecation

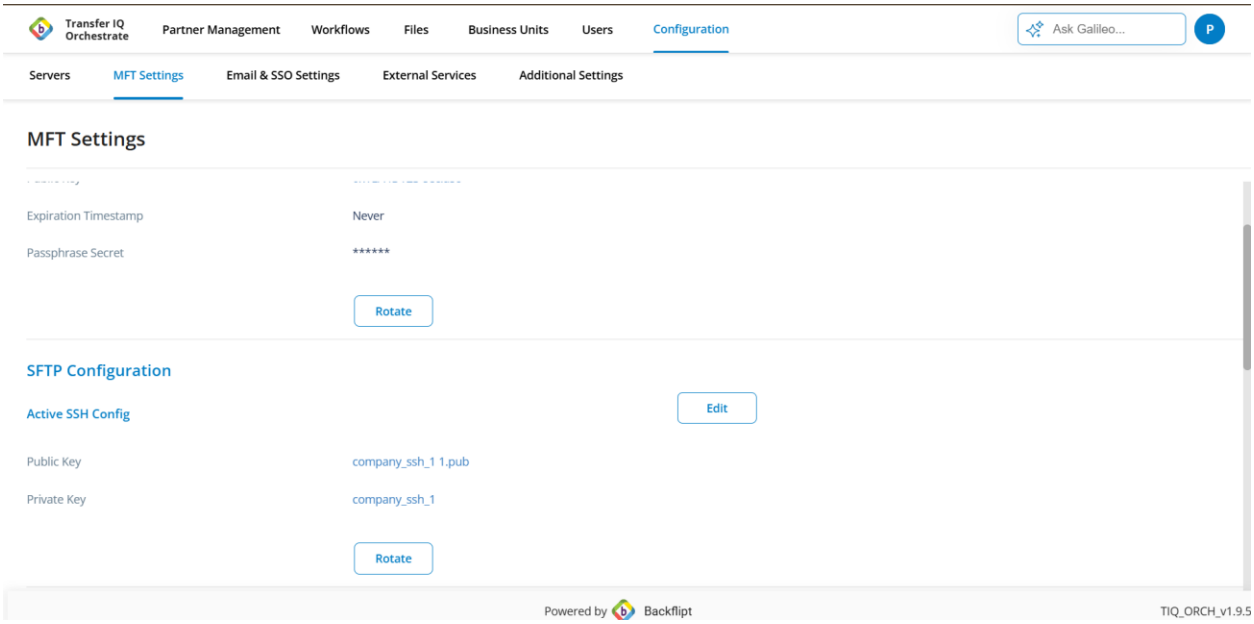
1. Once a PGP key is **deprecated**, it is **removed from the system** and will **no longer be used** for decrypting any files.
2. Files encrypted with the **new PGP key** continue to be decrypted using the new key.
3. Any file encrypted with the old, deprecated key will **fail to decrypt**, ensuring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

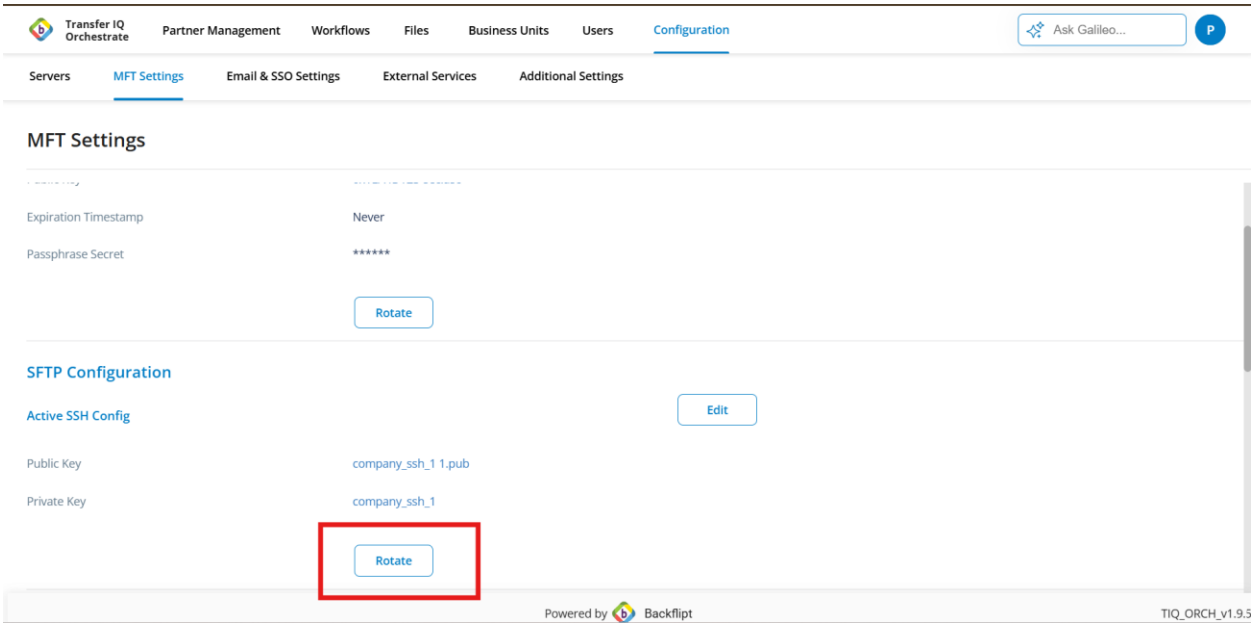
Before initiating the key rotation process, only the **active set of SSH keys** currently in use are visible under the *MFT Settings* > *Active SSH Keys* section.
These keys represent the ones actively used for establishing secure SFTP connections with partner servers.



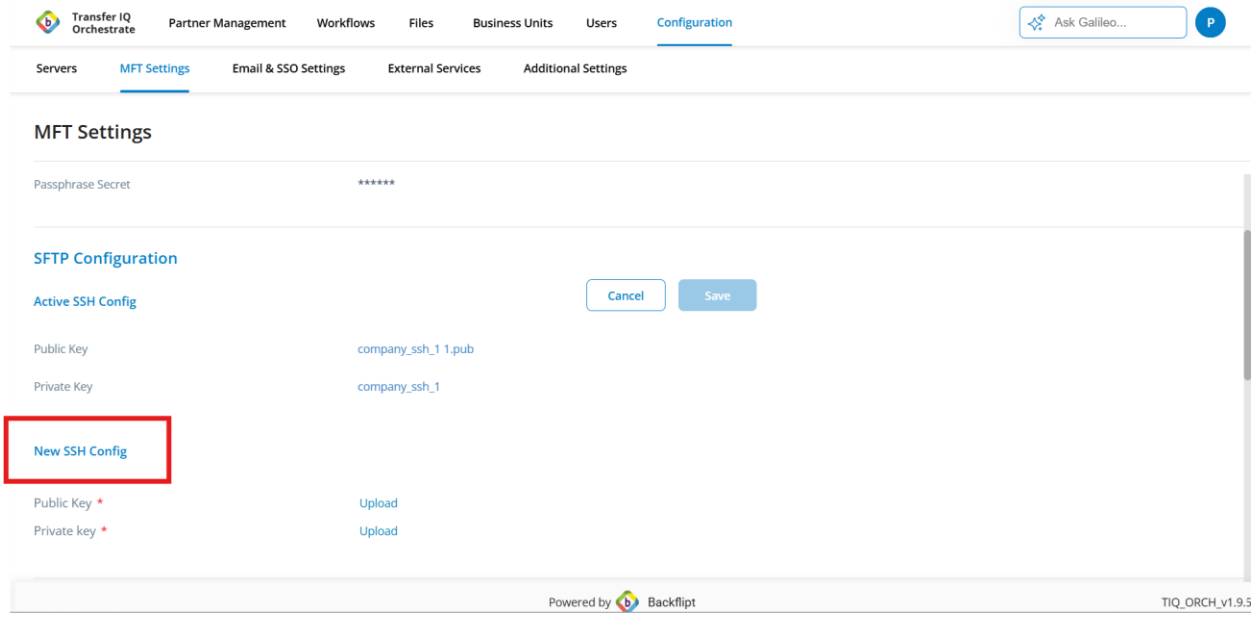
At this stage, the system continues to rely solely on the active keys for all ongoing file transfers and workflow executions.

2. During Rotation

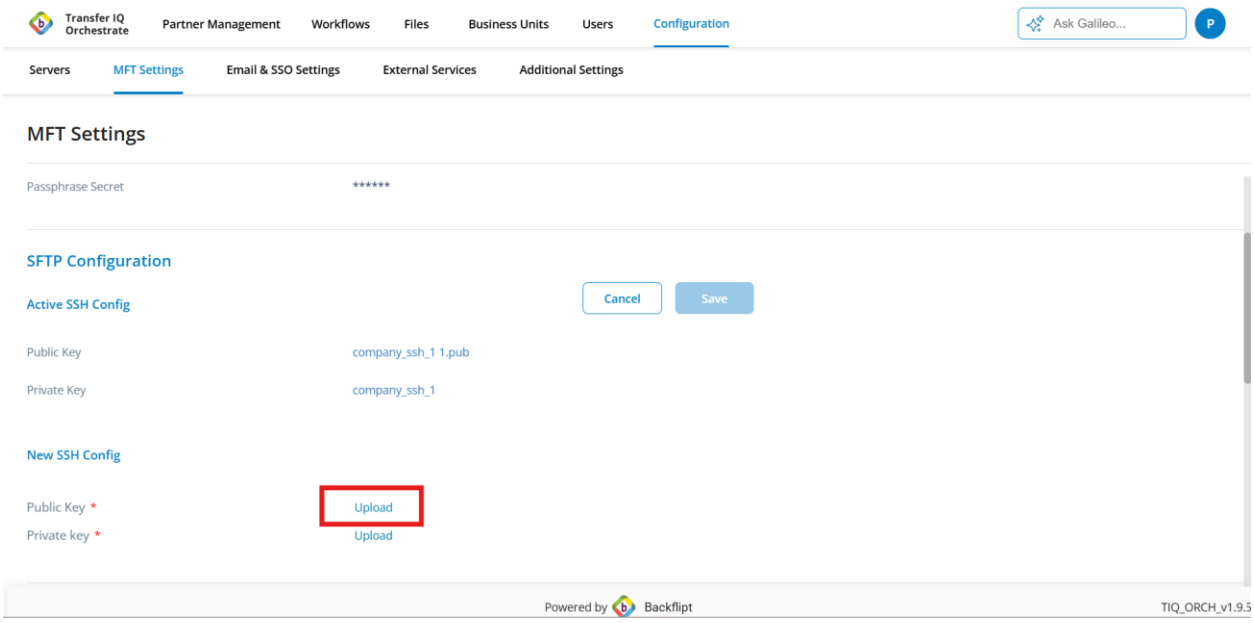
1. Navigate to **MFT Settings > Active SSH Keys**.
2. Click the **Rotate** button next to the *Active SSH Keys* section.



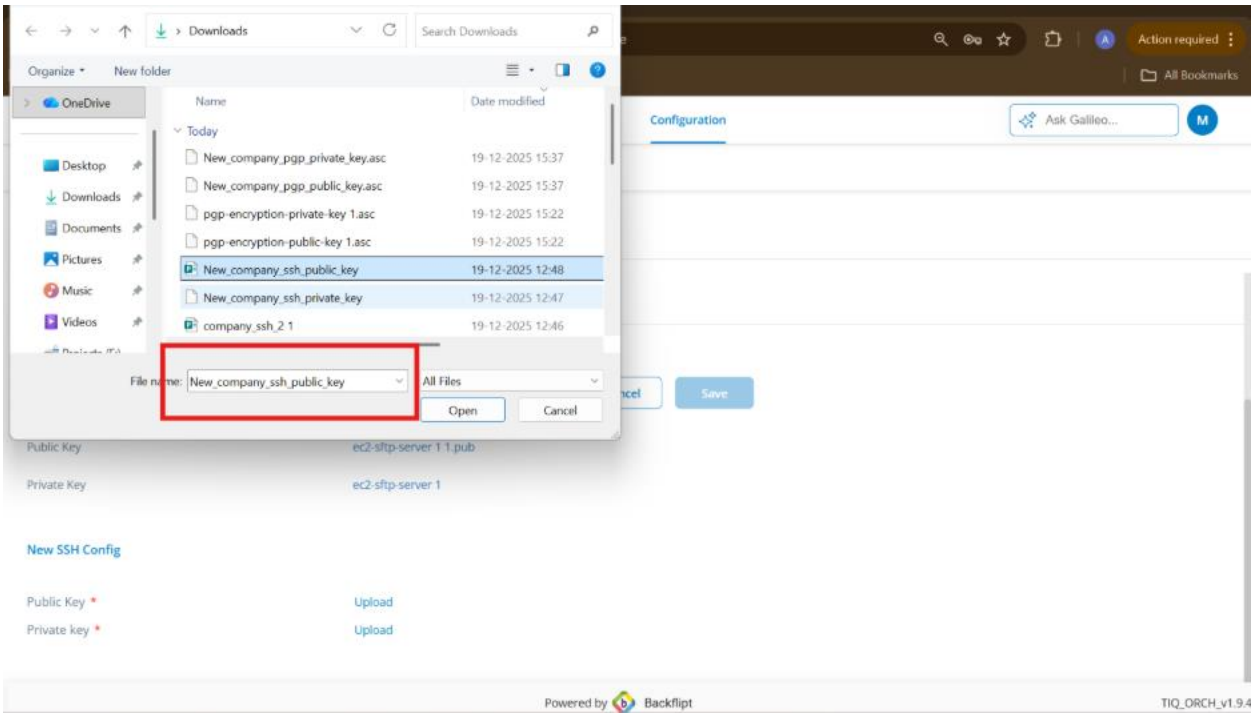
This action reveals a new section labeled **New SSH Keys**, which allows you to upload the **public** and **private** SSH keys for the new key pair.

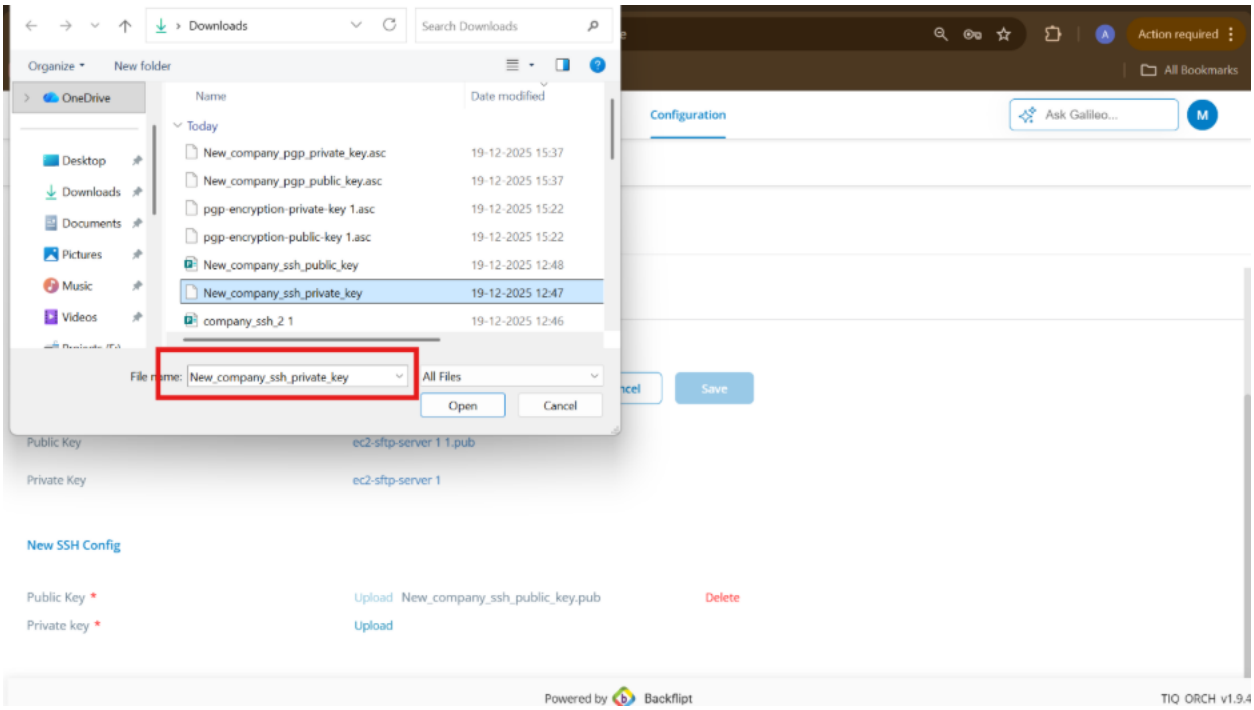


3. Under the **New SSH Keys** section, click **Upload** and select a valid SSH key file.

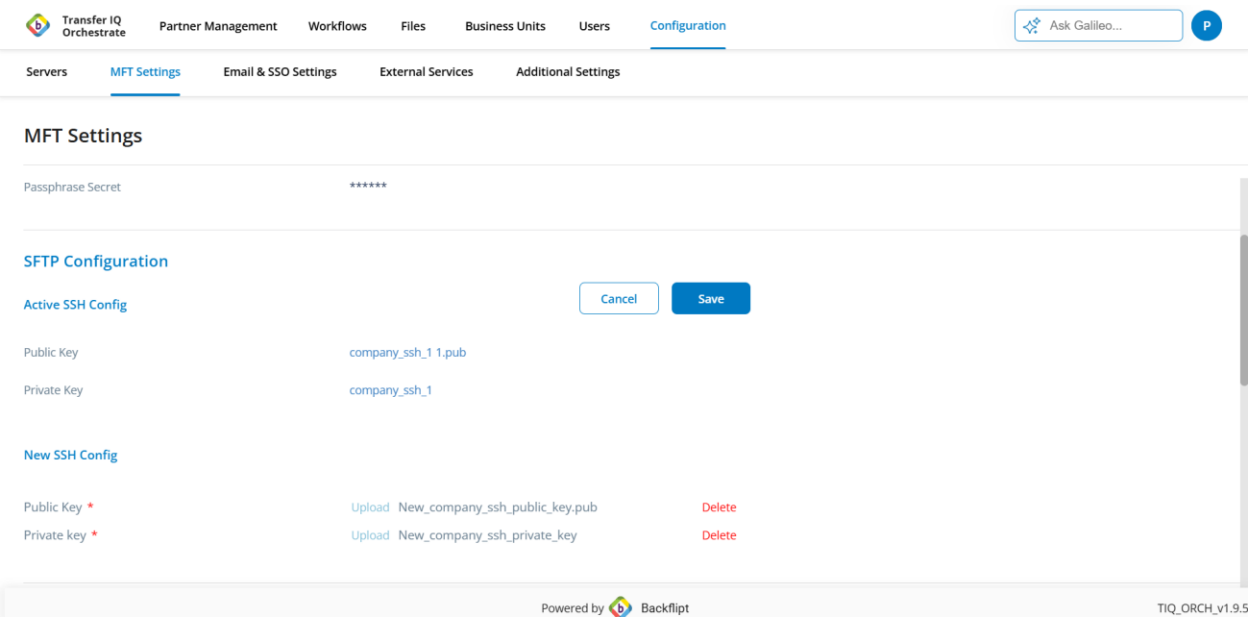


4. Select and open a file from the file selection dialog box

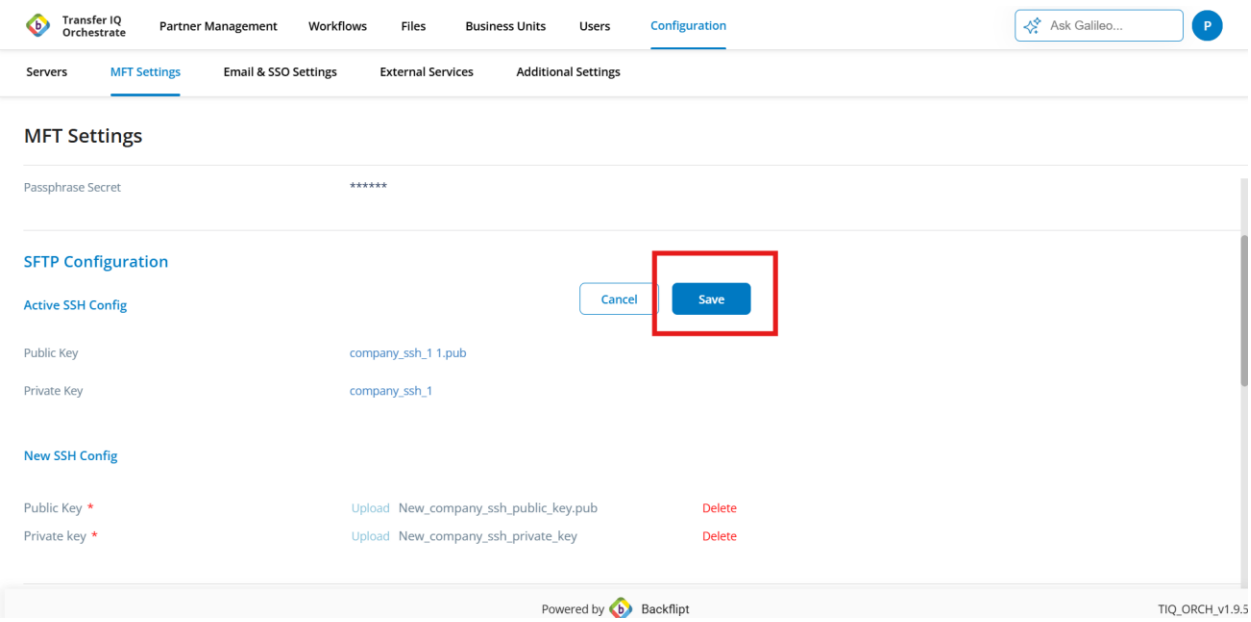




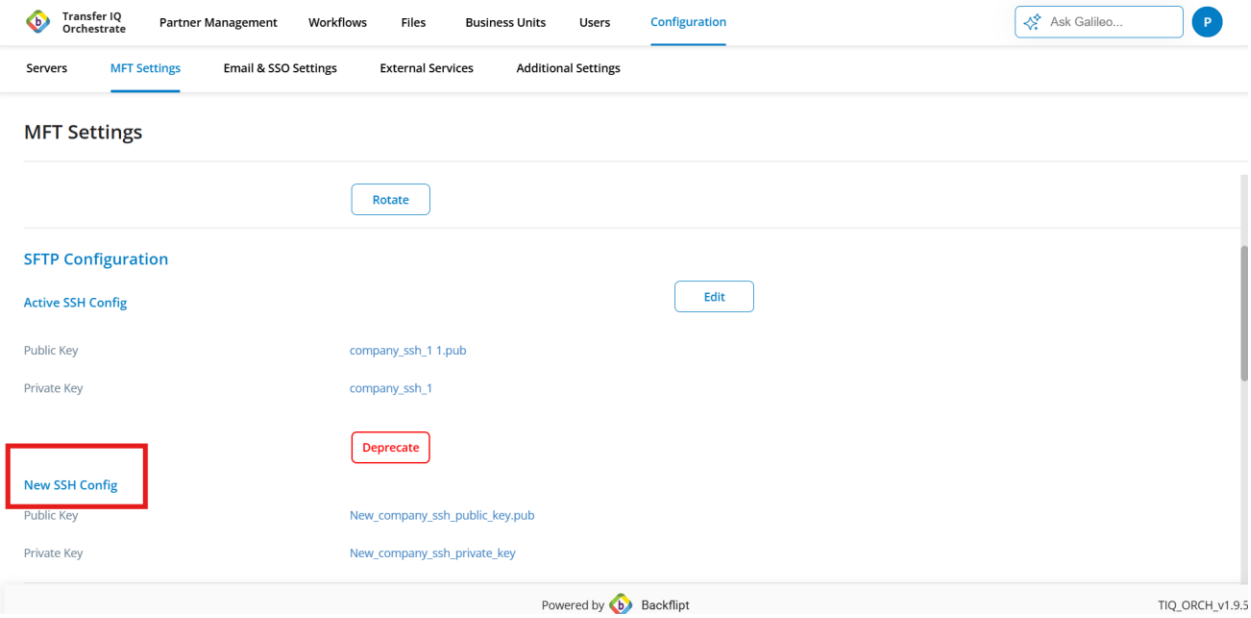
5. Once uploaded successfully, both **Active SSH Keys** and **New SSH Keys** will be displayed in the *MFT Settings* tab.



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



6. 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.



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:

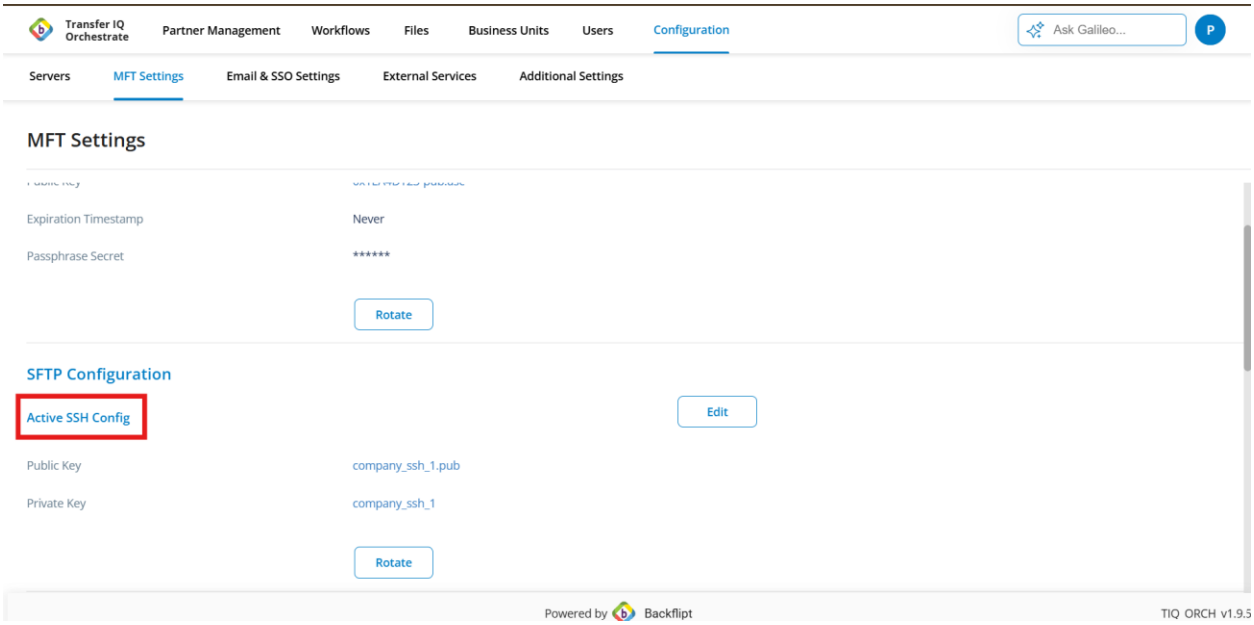
1. The system first attempts to establish the SFTP connection using the **new SSH key** uploaded under *MFT Settings*.
2. If the connection is **successful**, the corresponding connector's SSH private key is automatically updated with the **new key**, and all future connections will continue to use this 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**.

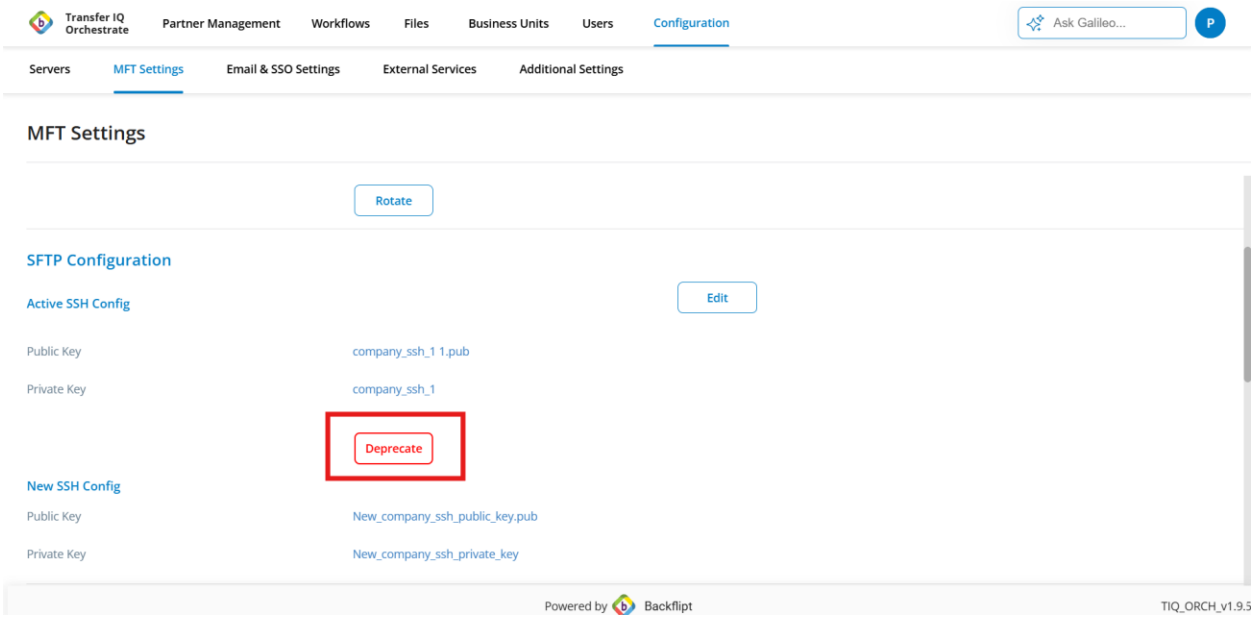
3. Deprecation (post-rotation)

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

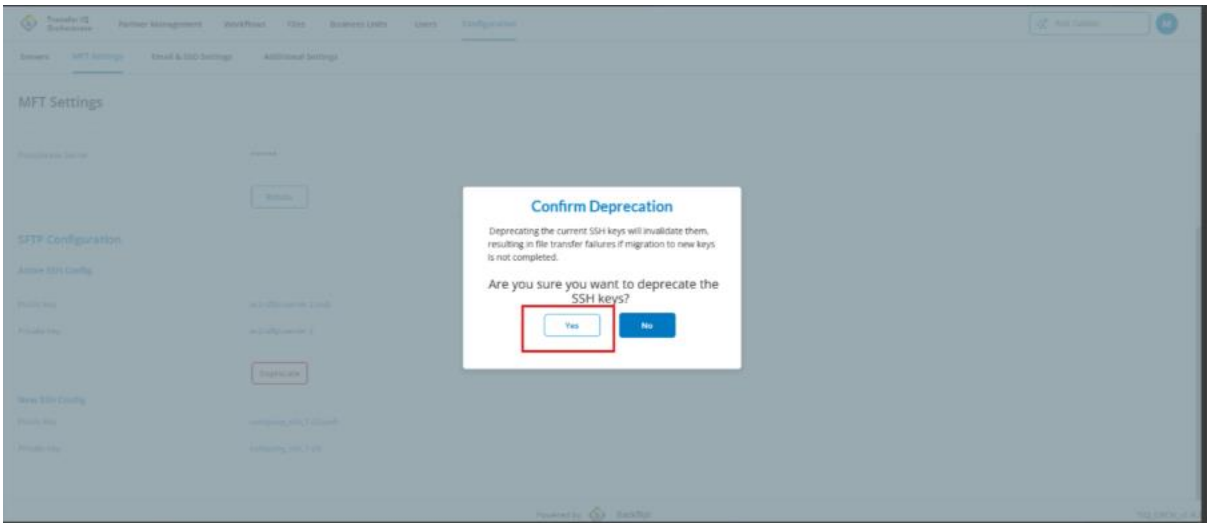
1. Navigate to the **Active SSH Keys** section in the *MFT Settings* tab.



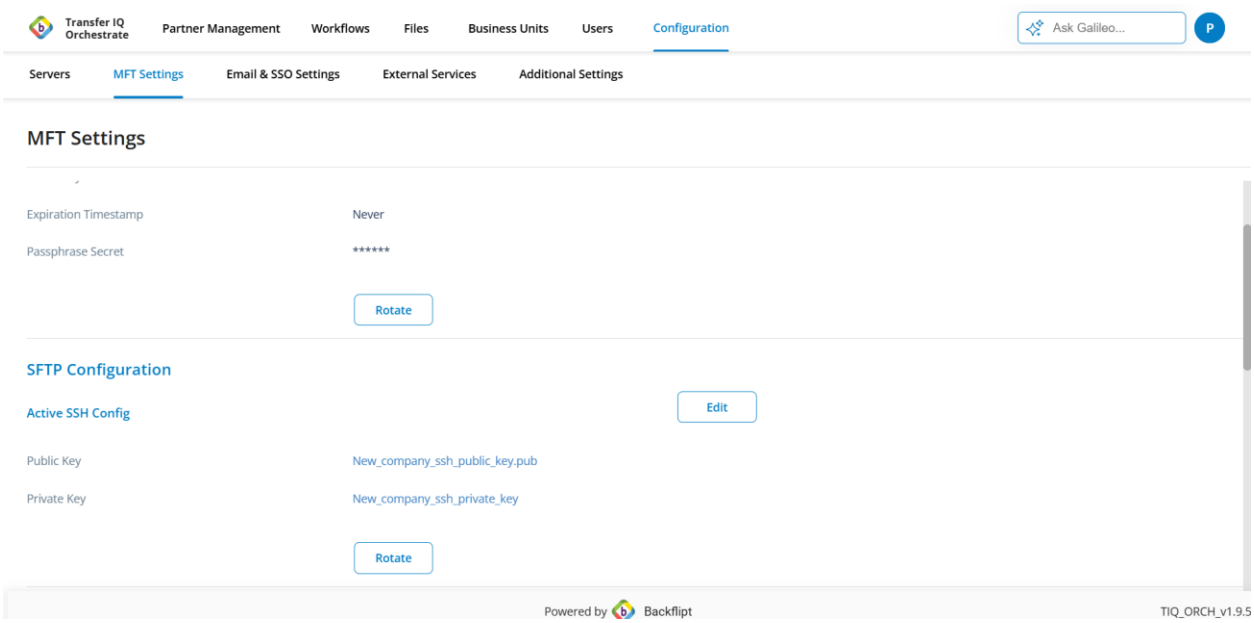
2. Click the **Deprecate** button next to the old active SSH key.



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.



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:

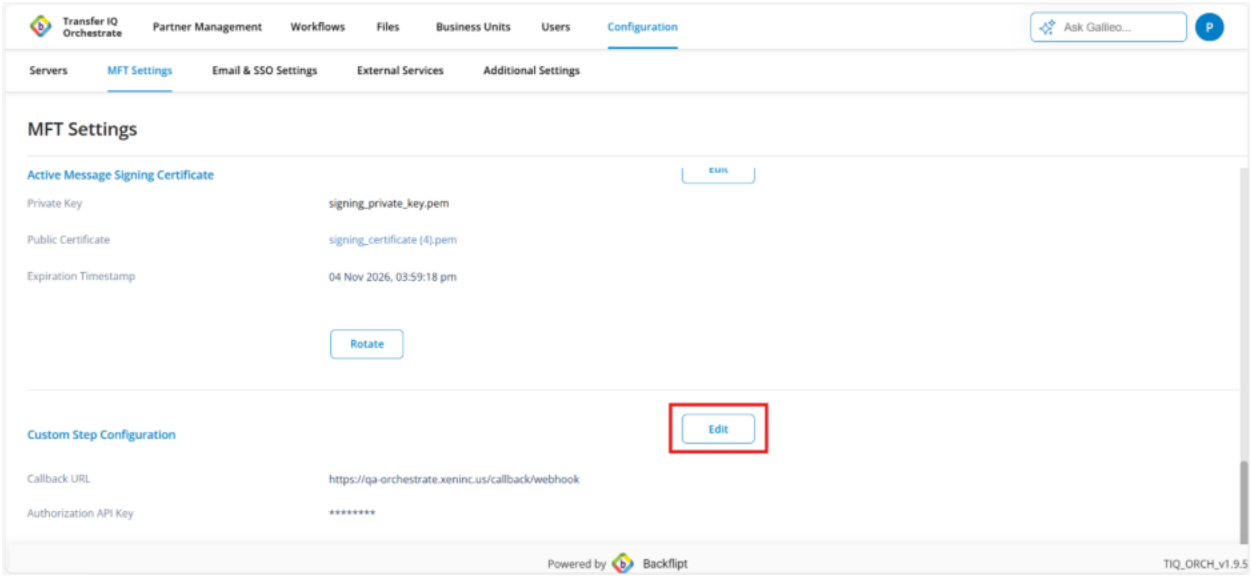
The callback URL and authentication key, which the company uses to receive responses from the external service, will be specified in the Custom step Configuration section of the MFT settings tab

This section consists of two input fields:

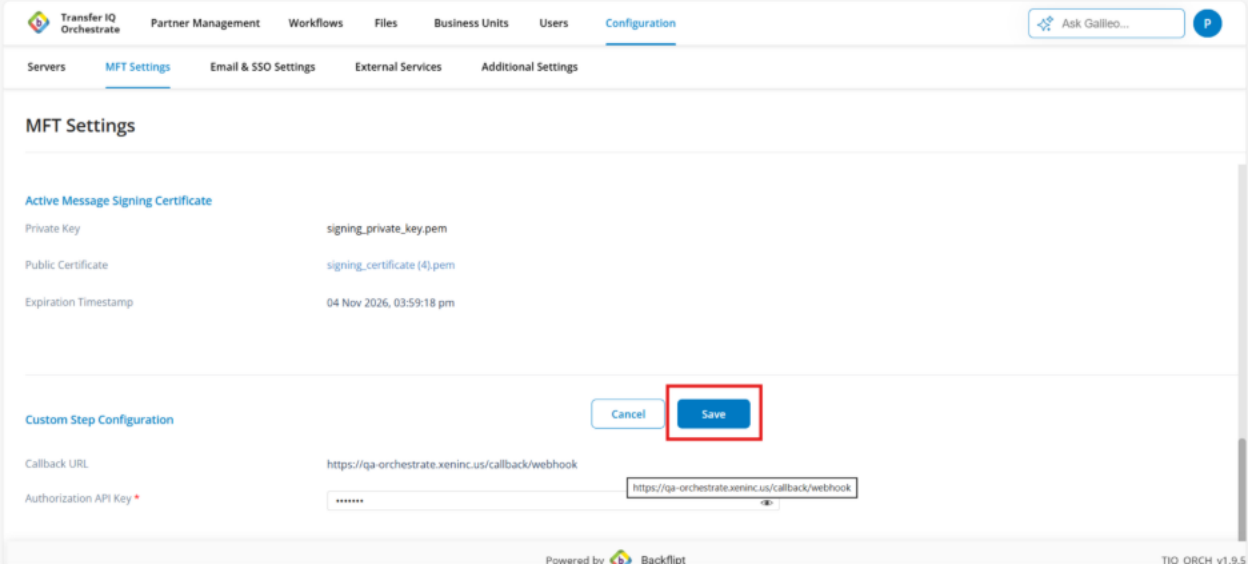
- Callback URL – This field is pre-populated with a default value when the Orchestrate application is deployed.
- Authentication Token – The company provides the authentication token in this field.

To configure customs step configuration, follow the below steps

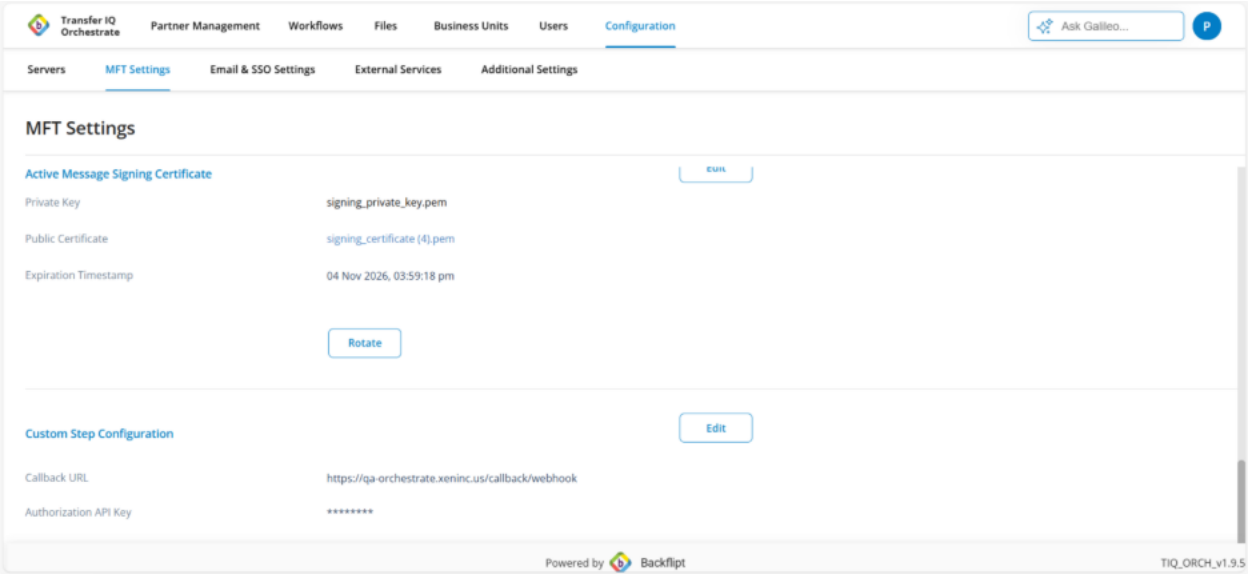
1. Navigate to Configuration > MFT Settings
2. Navigate to Custom Step Configuration in MFT Settings Tab
3. Click edit to enter the authentication token



4. Provide the authentication token and Click save



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



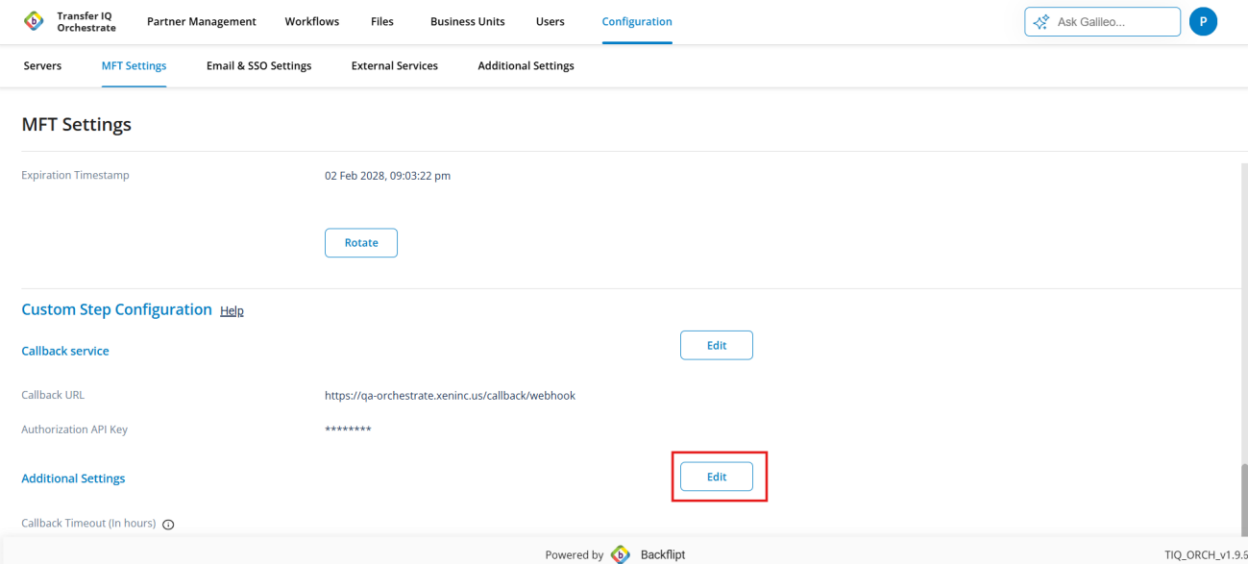
Configuring Callback Time:

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

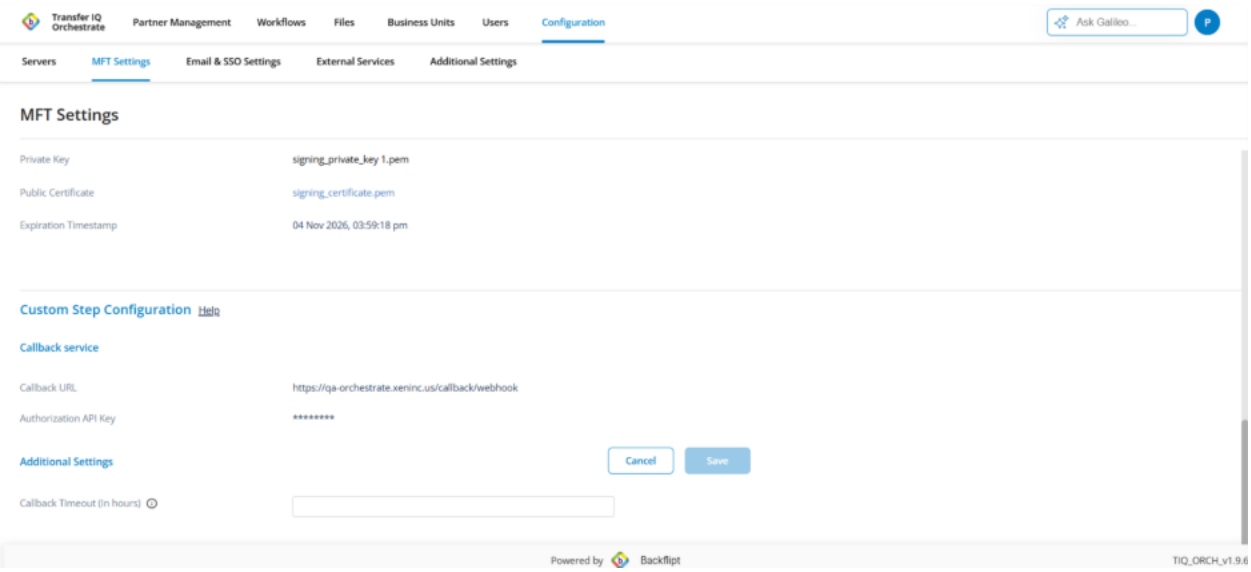
- If no response is received from the external service, the workflow transitions into a **suspended** state.
- In the suspended state, workflow execution is **paused**, and no further steps are processed until a response is received or manual action is taken.
- While suspended, the workflow status is 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

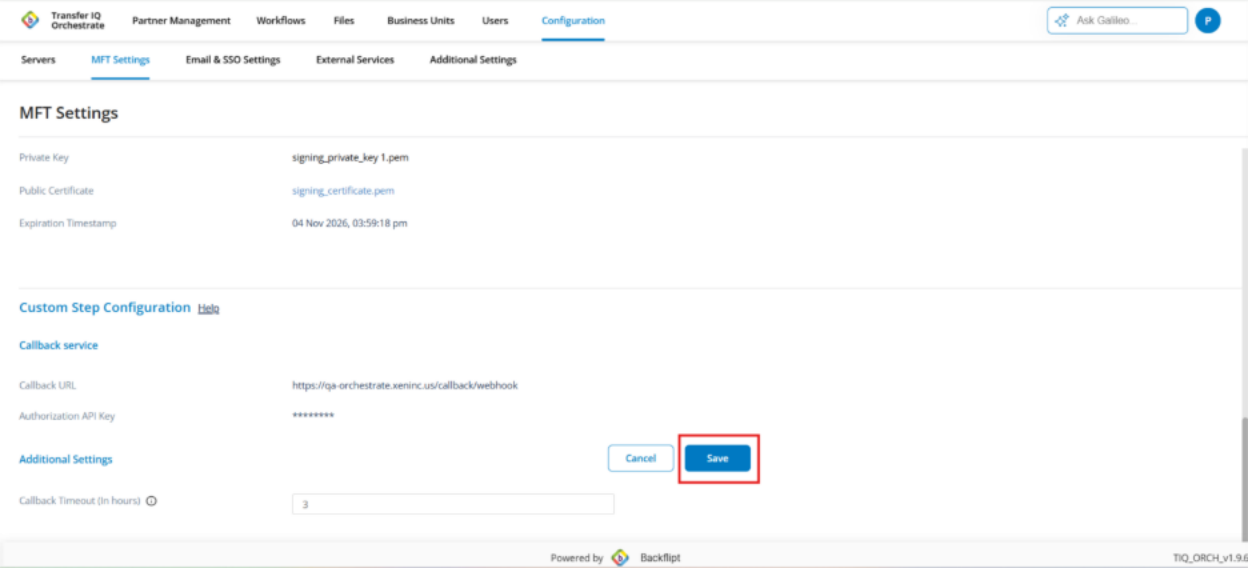
1. Navigate to Configuration > MFT Settings > Custom Step Configuration
2. Navigate to Additional Settings Sections in Custom Step Configuration
3. Click the Edit button



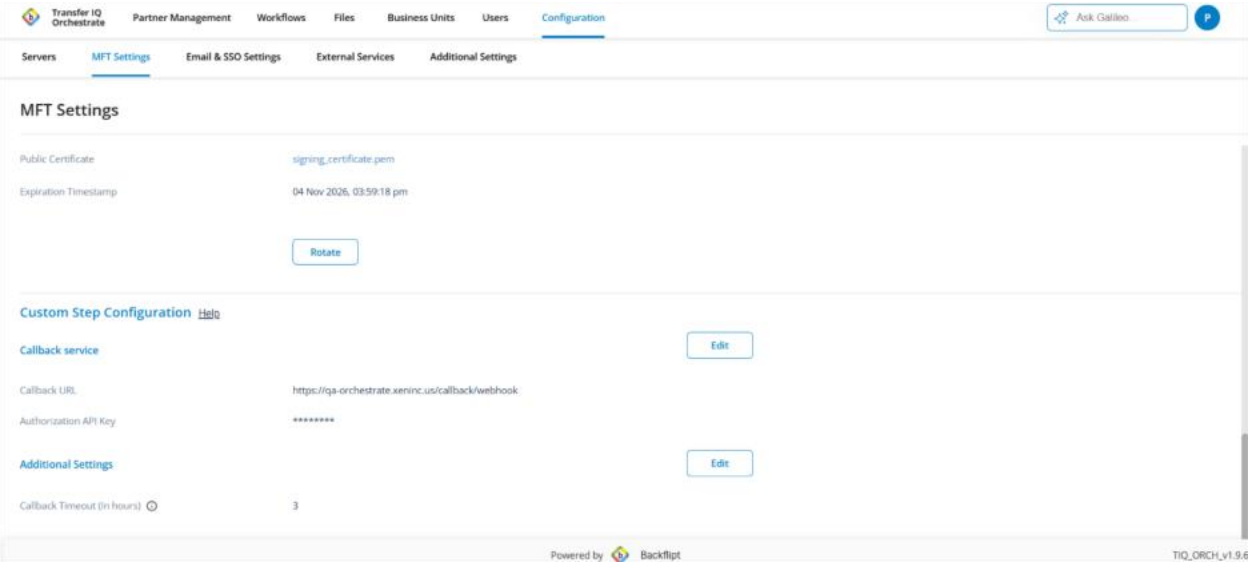
4. Configure the Callback Time in hours



5. Once configured, Click the Save



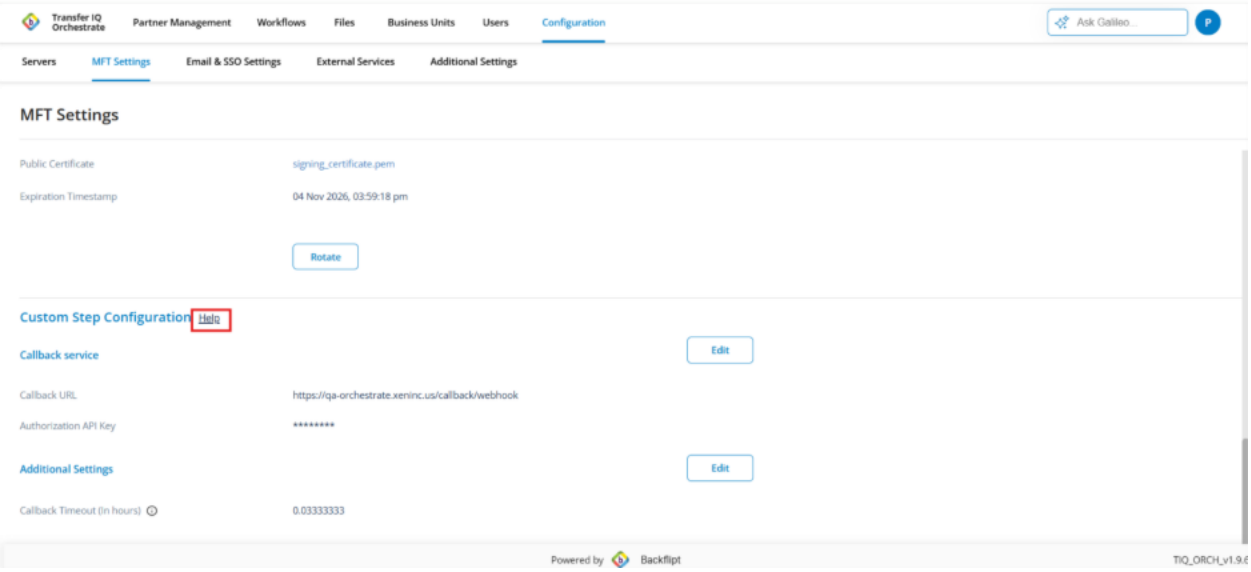
6. Once saved the callback time will be displayed in view mode



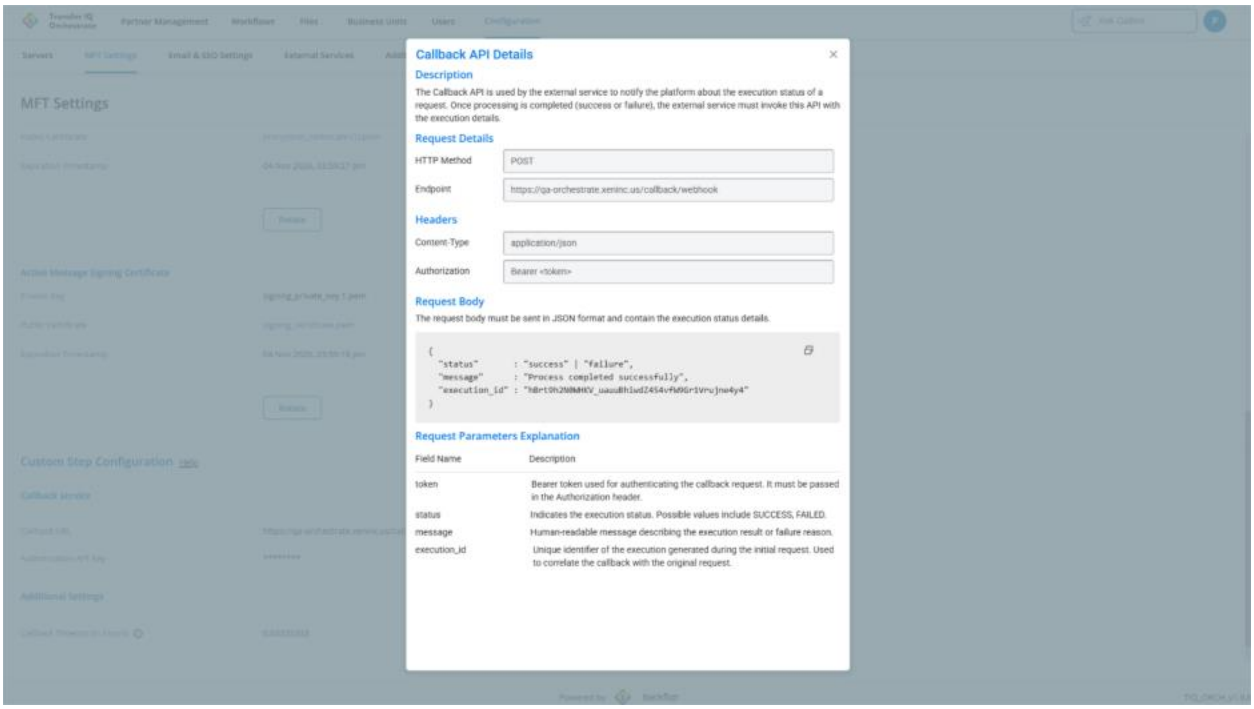
Note: If the callback time is not configured, it will default to 2 hours.

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



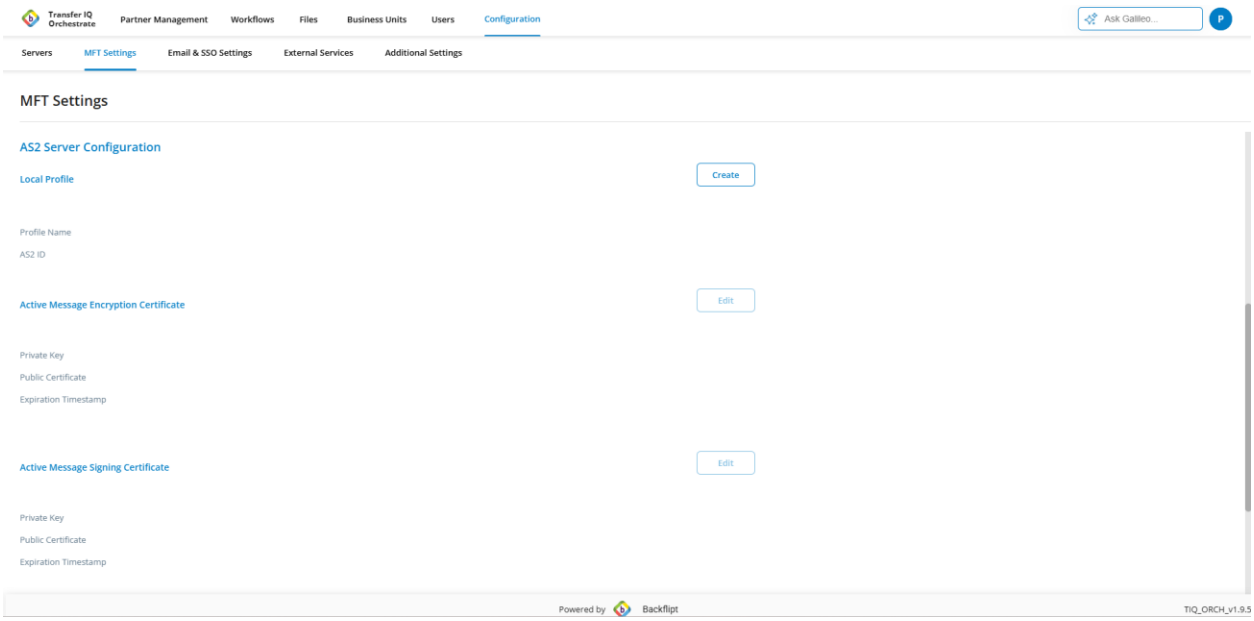
AS2 Protocol

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



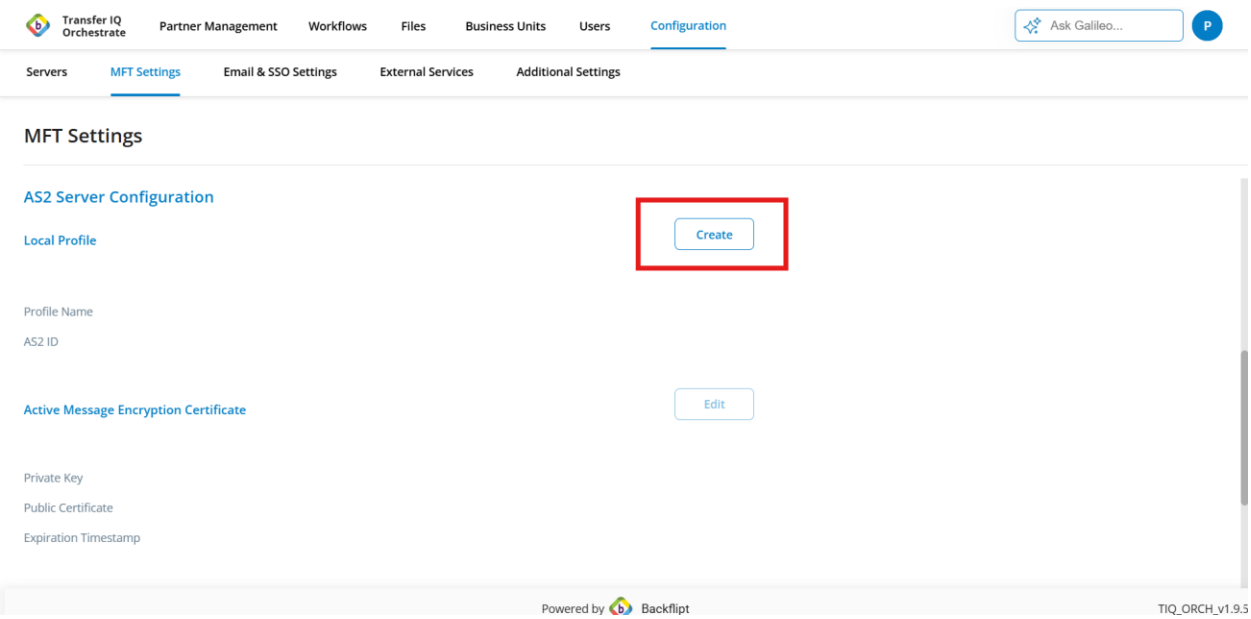
Local Profile:

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

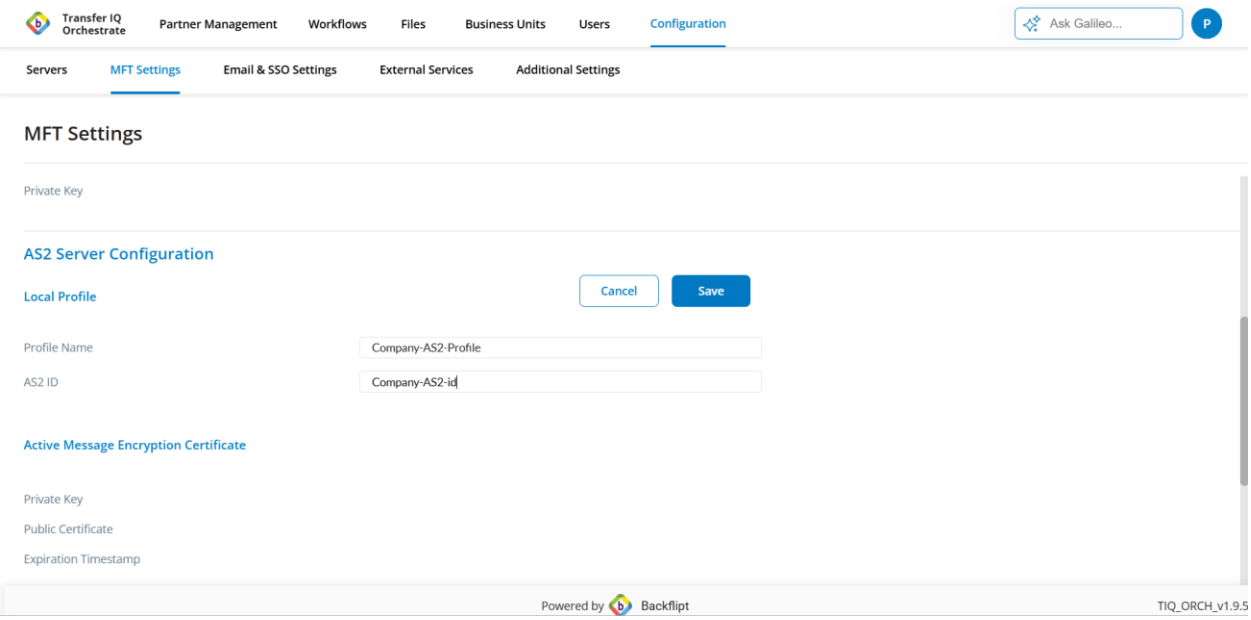
- **Profile Name**
- **AS2 ID**

Creating the Local Profile

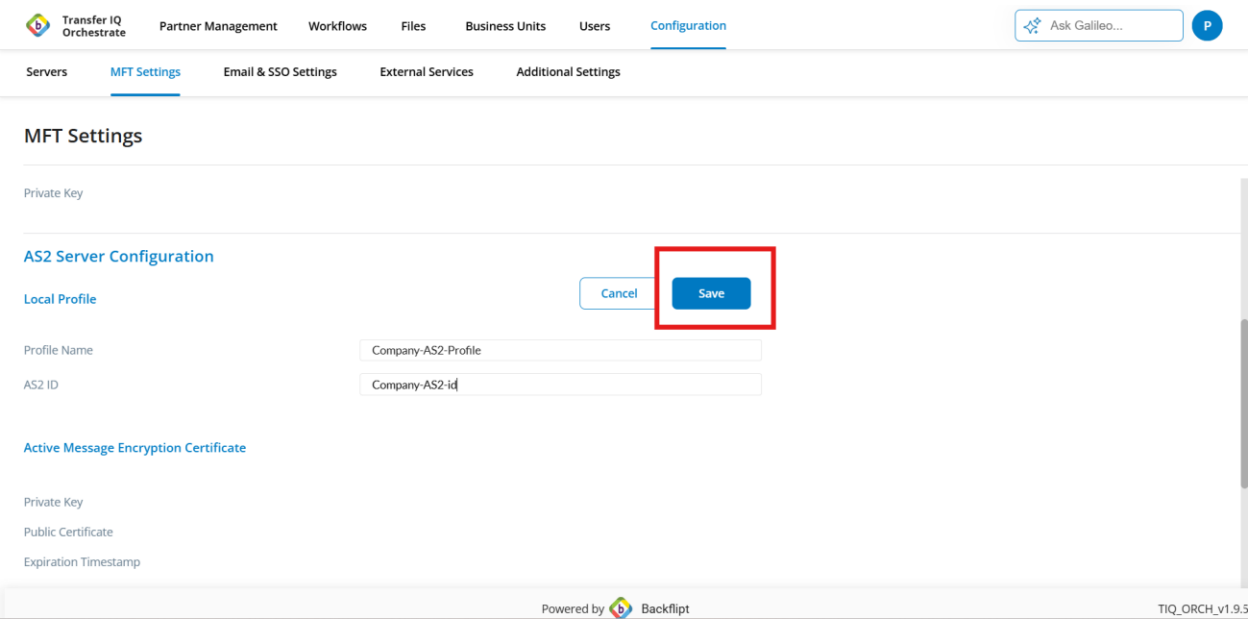
1. Navigate to **Configuration → MFT Settings → Local Profile**.
2. The page appears blank when no profile is configured.
3. Click Create



4. Enter the following details:
    a. **Profile Name**
    b. **AS2 ID**

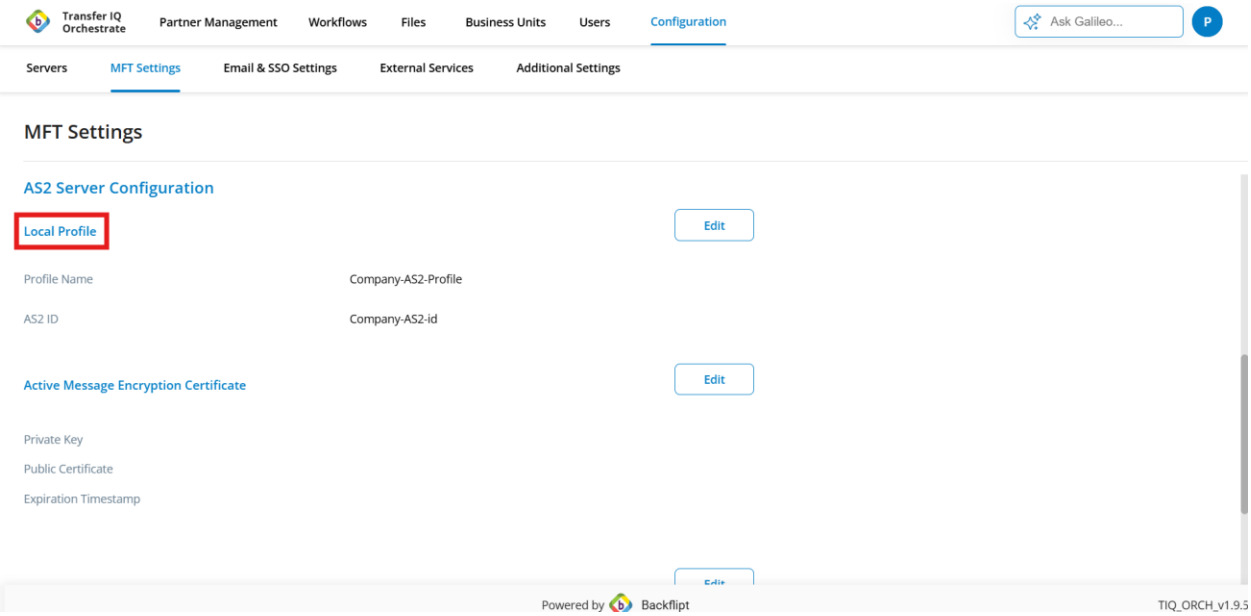


5. Click **Save**.

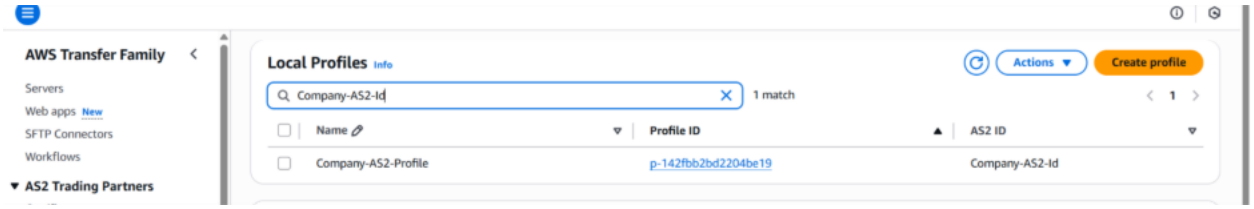


Outcome:

1. The Local Profile is created in the application.



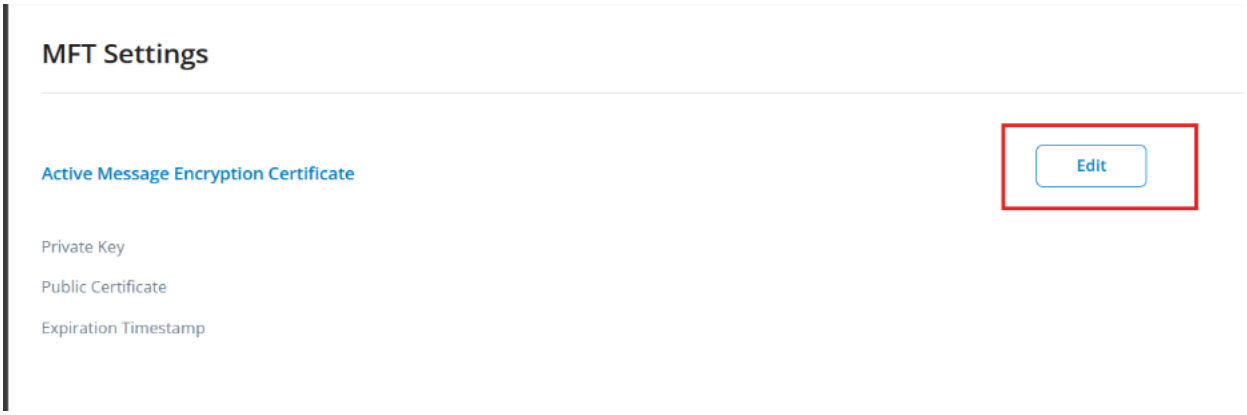
2. The same profile is automatically created under **AWS Transfer Family → Servers** to maintain consistency between the application and AWS.



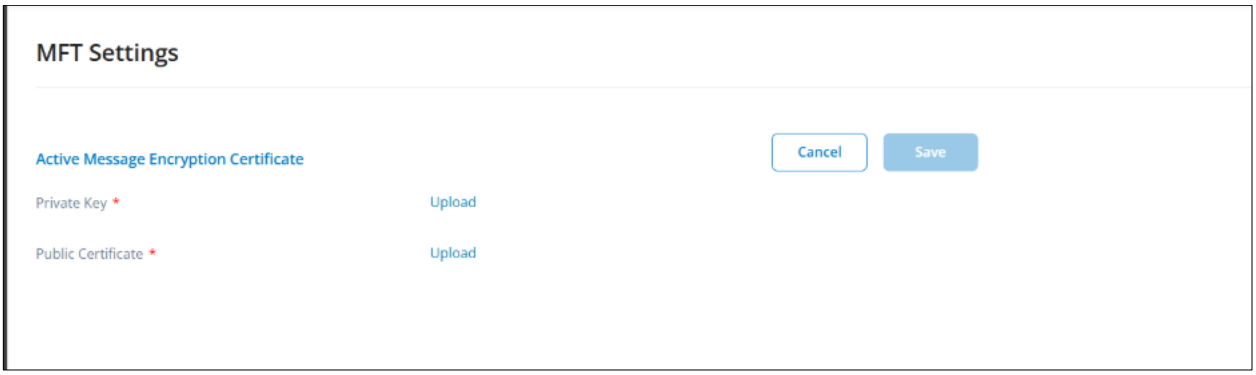
3. After creation, the **AS2 ID becomes locked and cannot be modified**.
4. A Local Profile **must be created before** configuring AS2 Agreements, as it represents the company during all AS2 exchanges.
5. The AS2 ID must be **unique**, as trading partners use this value to identify your company.

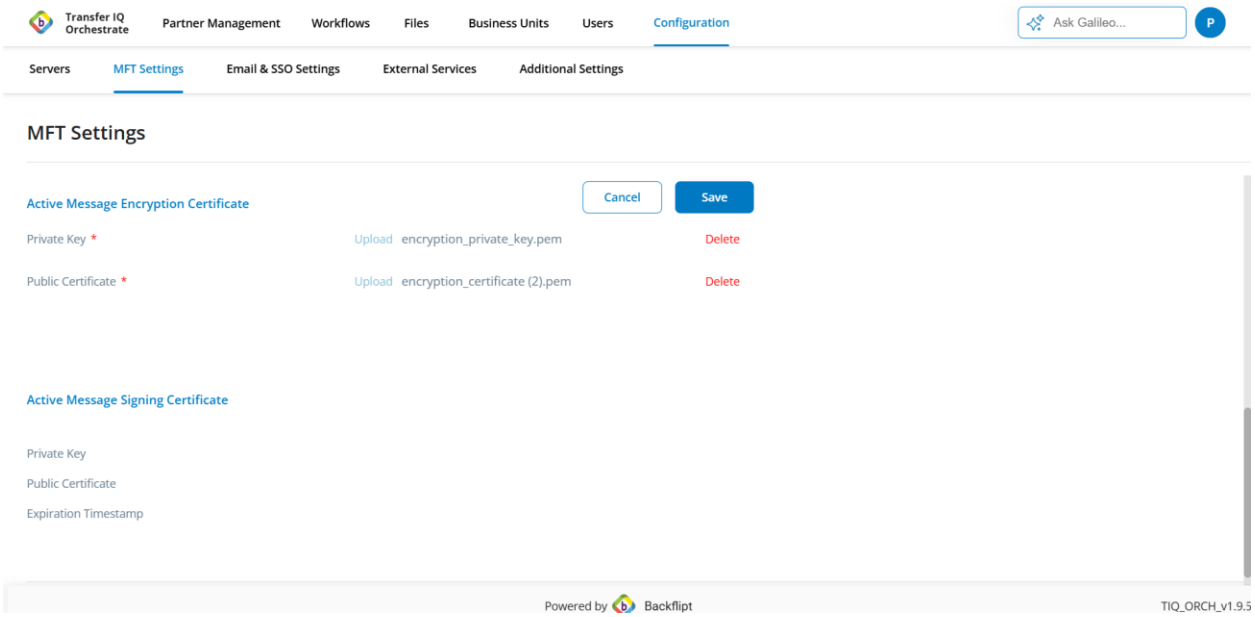
Message Encryption Certificates

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.

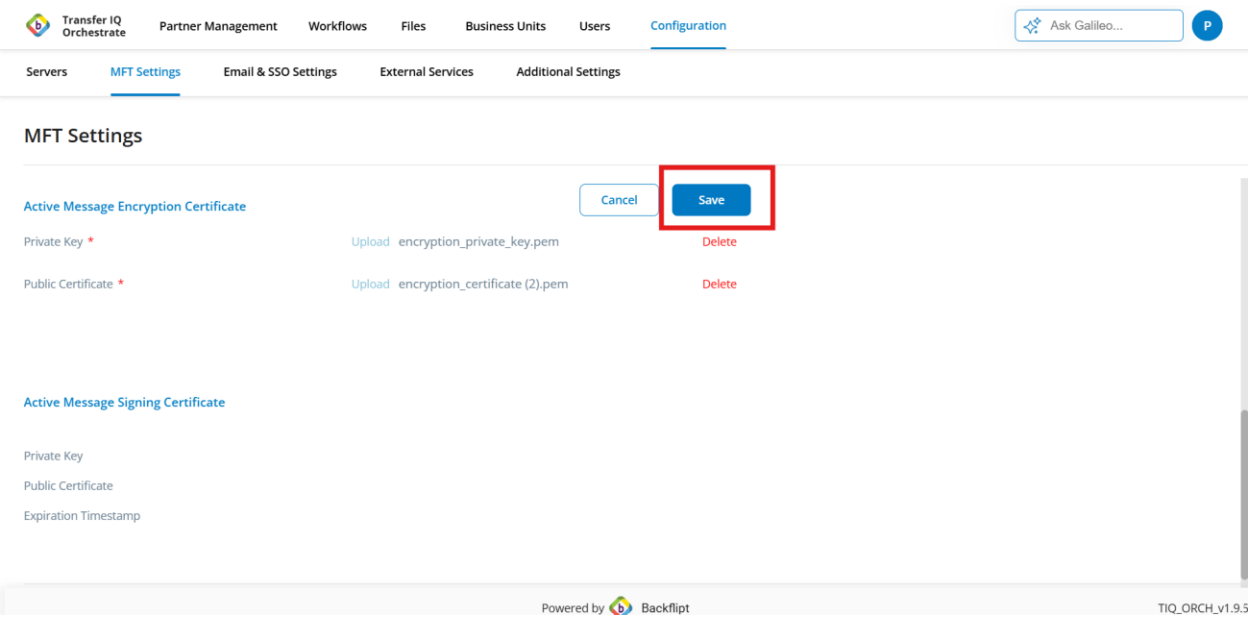


4. This section contains of the below certificates:
   a. Message Encryption Public Certificate
   b. Message Encryption Private Key

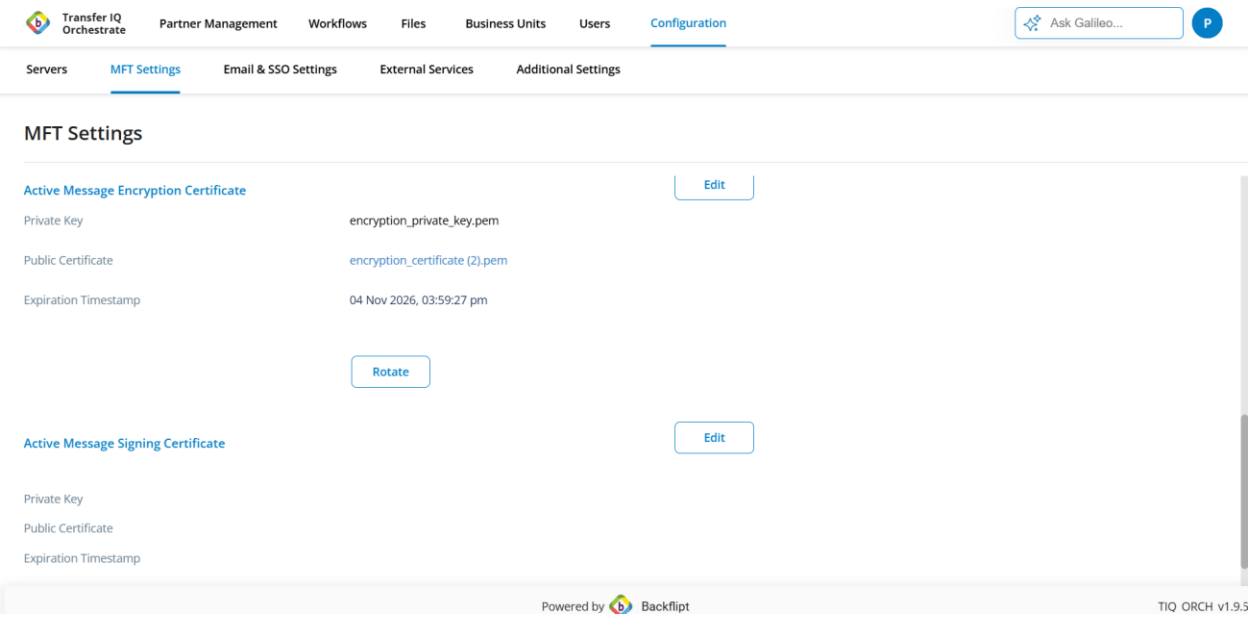

MFT Settings
Active Message Encryption Certificate
Cancel
Save
Private Key *
Upload
Public Certificate *
Upload

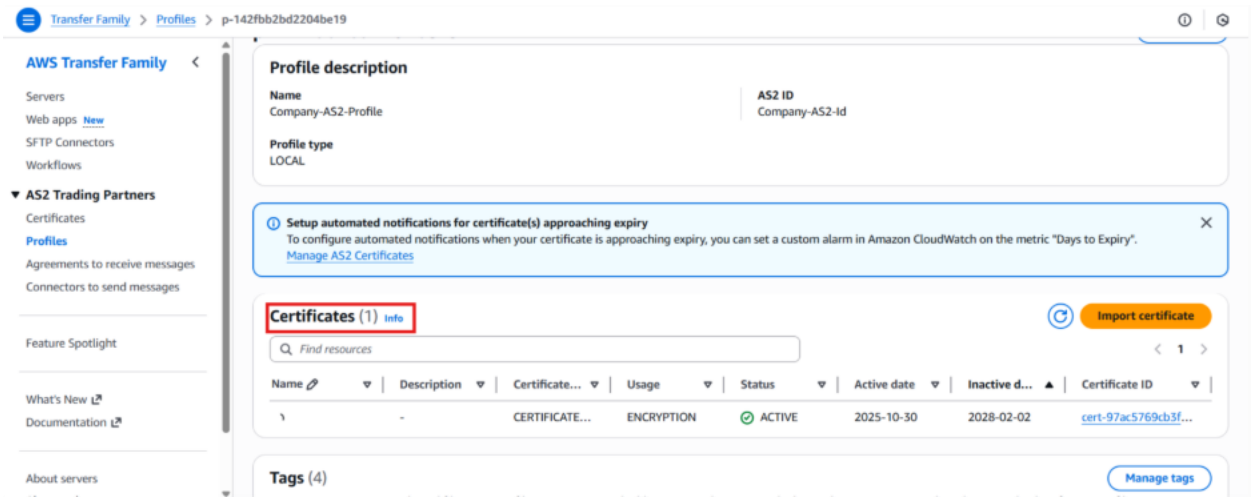

Transfer IQ Orchestrate
Partner Management
Workflows
Files
Business Units
Users
Configuration
Ask Galileo...
P
Servers
MFT Settings
Email & SSO Settings
External Services
Additional Settings
MFT Settings
Active Message Encryption Certificate
Cancel
Save
Private Key *
Upload
encryption_private_key.pem
Delete
Public Certificate *
Upload
encryption_certificate (2).pem
Delete
Active Message Signing Certificate
Private Key
Public Certificate
Expiration Timestamp
Powered by Backflipt
TIQ_ORCH_v1.9.5

5. Click Save



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





Message Encryption Public Certificate

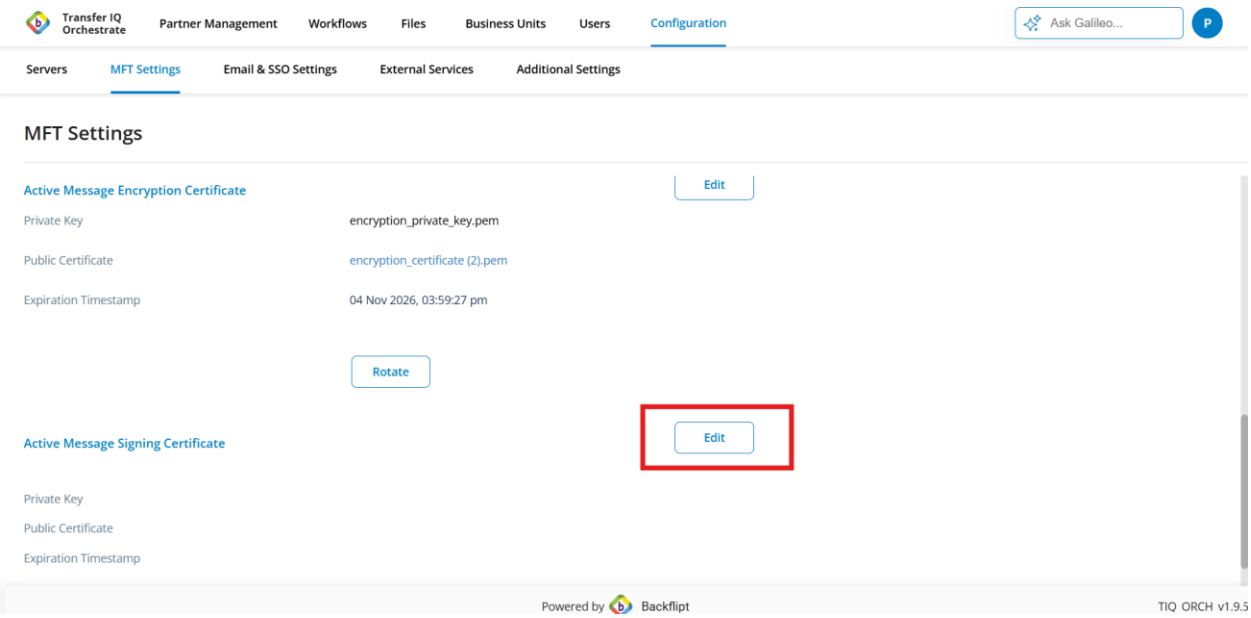
1. This is the public part of the certificate used to **encrypt AS2 messages**.
2. When a partner needs to send AS2 files to the company, the company provides this **encryption public certificate** to the partner.
3. The partner uses this certificate to **encrypt the AS2 message** before sending it. 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:

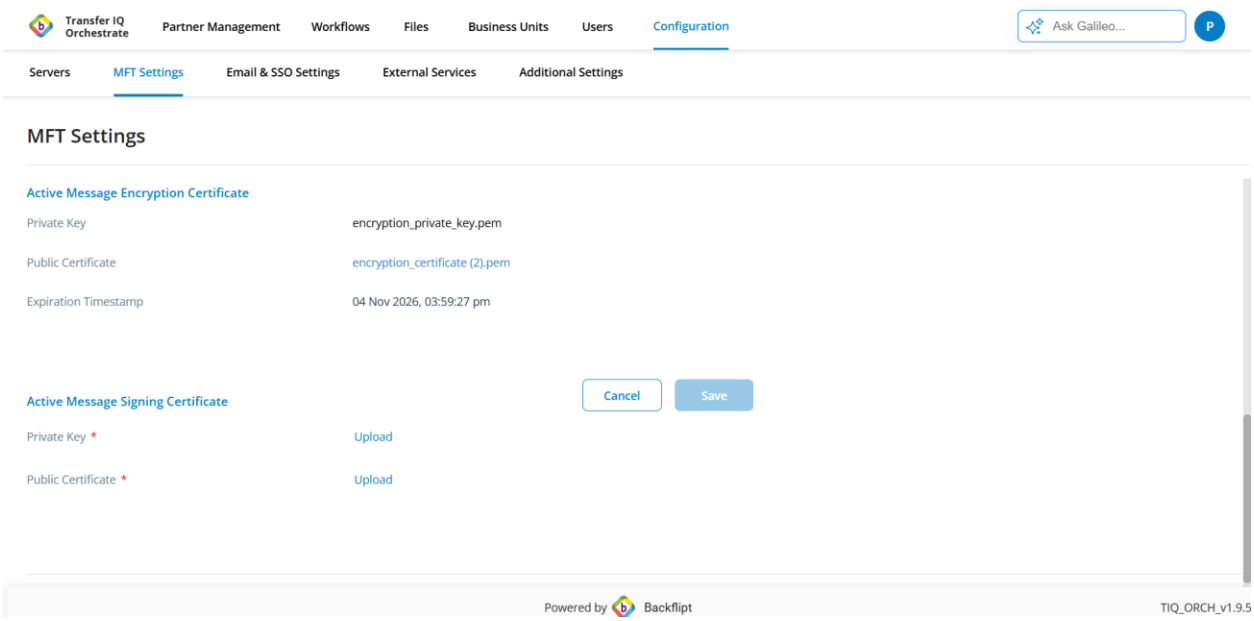
1. This is the private key that matches the public encryption certificate.
2. The company keeps this key **secure and confidential** and never shares it.
3. When the company receives an encrypted AS2 message from a partner, the company uses this **private key** to decrypt the message and read its contents.

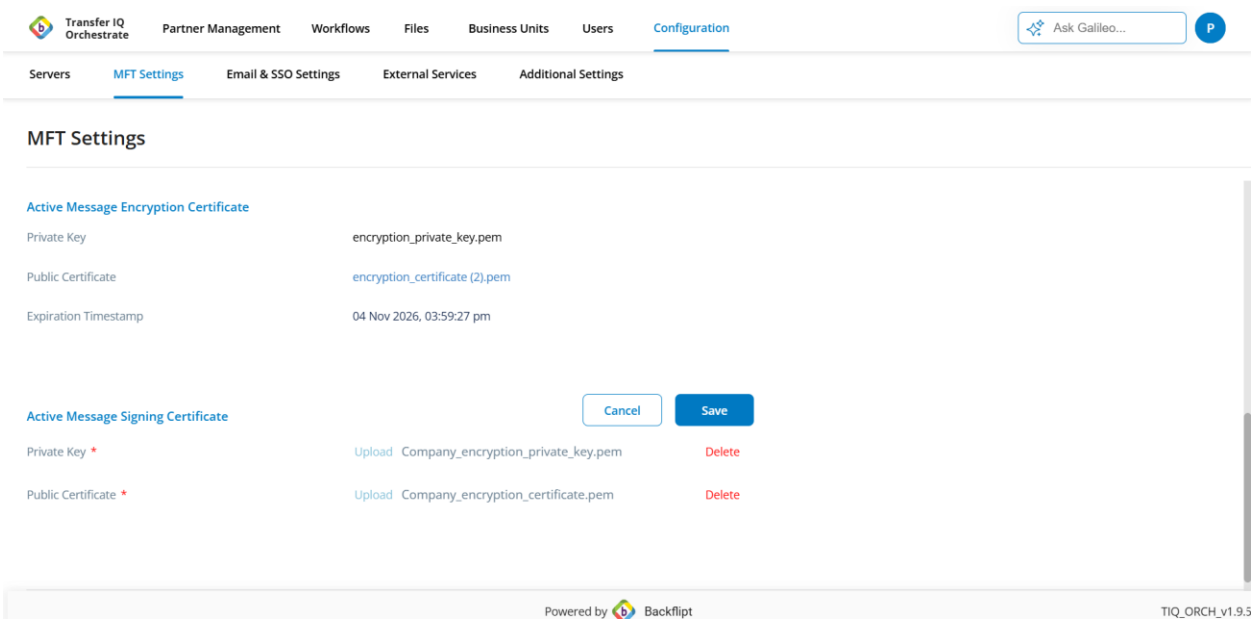
Message Signing Certificates:

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

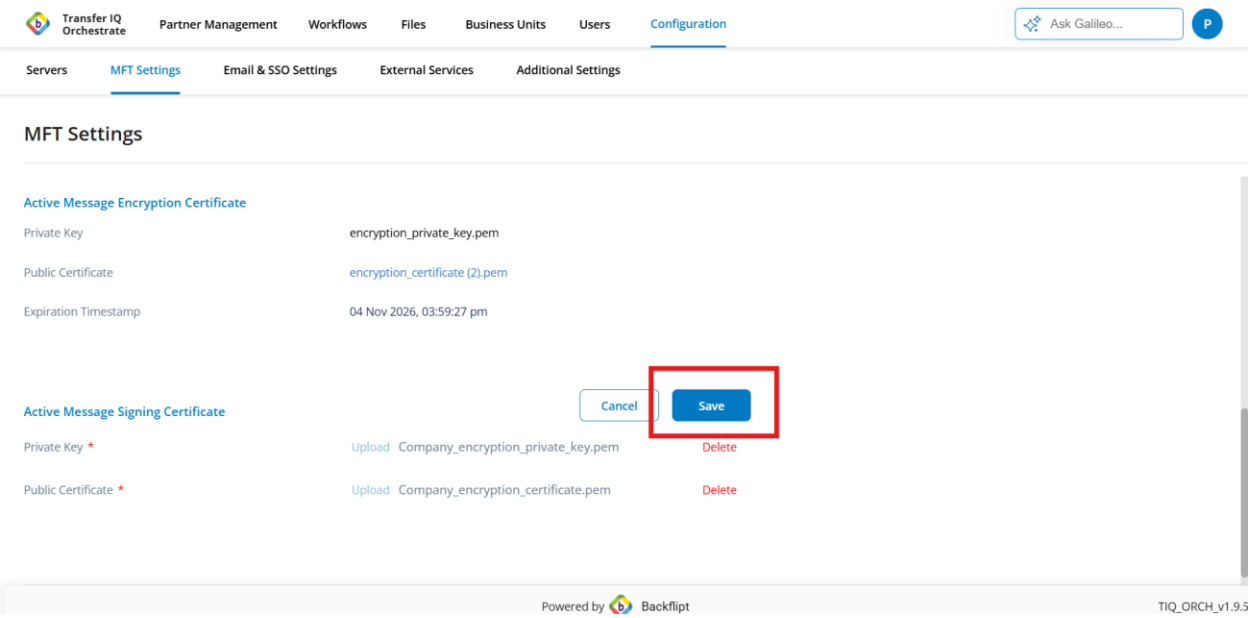


4. This section contains of the below certificates:
    a. Message Signing Public Certificate
    b. Message Signing Private Key

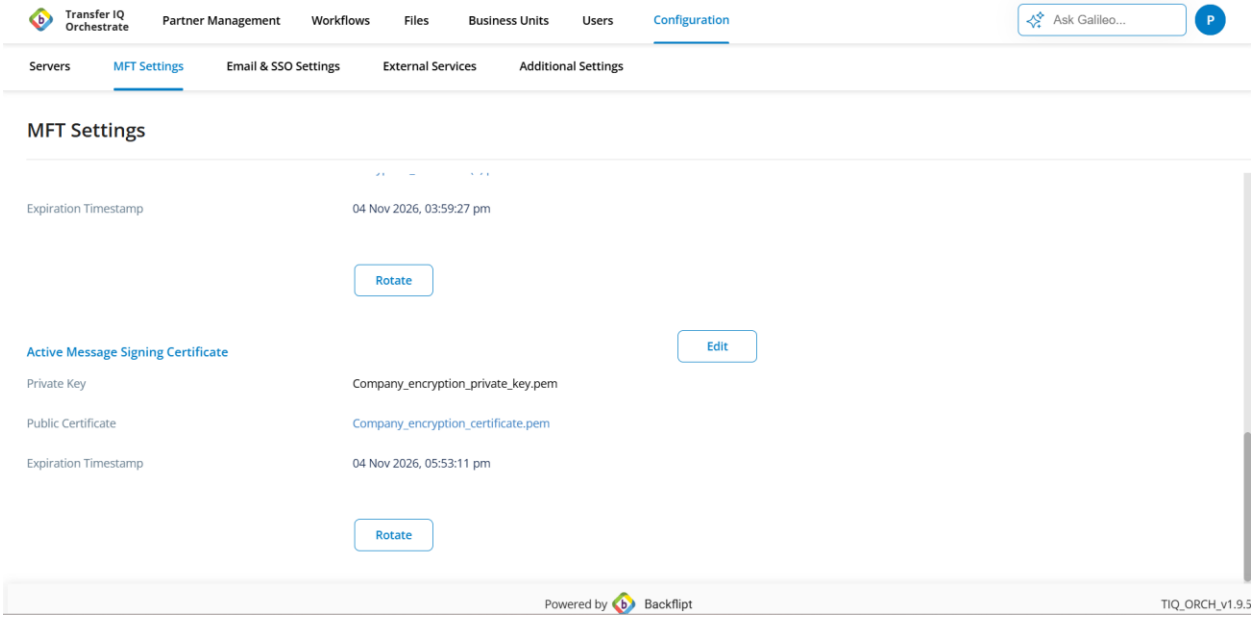

Transfer IQ Orchestrate
Partner Management
Workflows
Files
Business Units
Users
Configuration
Ask Galileo...
P
Servers
MFT Settings
Email & SSO Settings
External Services
Additional Settings
MFT Settings
Active Message Encryption Certificate
Private Key
encryption_private_key.pem
Public Certificate
encryption_certificate (2).pem
Expiration Timestamp
04 Nov 2026, 03:59:27 pm
Active Message Signing Certificate
Cancel
Save
Private Key *
Upload
Public Certificate *
Upload
Powered by Backflipt
TIQ_ORCH_v1.9.5


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
Public Certificate
encryption_certificate (2).pem
Expiration Timestamp
04 Nov 2026, 03:59:27 pm
Active Message Signing Certificate
Cancel
Save
Private Key *
Upload
Company_encryption_private_key.pem
Delete
Public Certificate *
Upload
Company_encryption_certificate.pem
Delete
Powered by Backflipt
TIQ_ORCH_v1.9.5

5. Click Save



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



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**

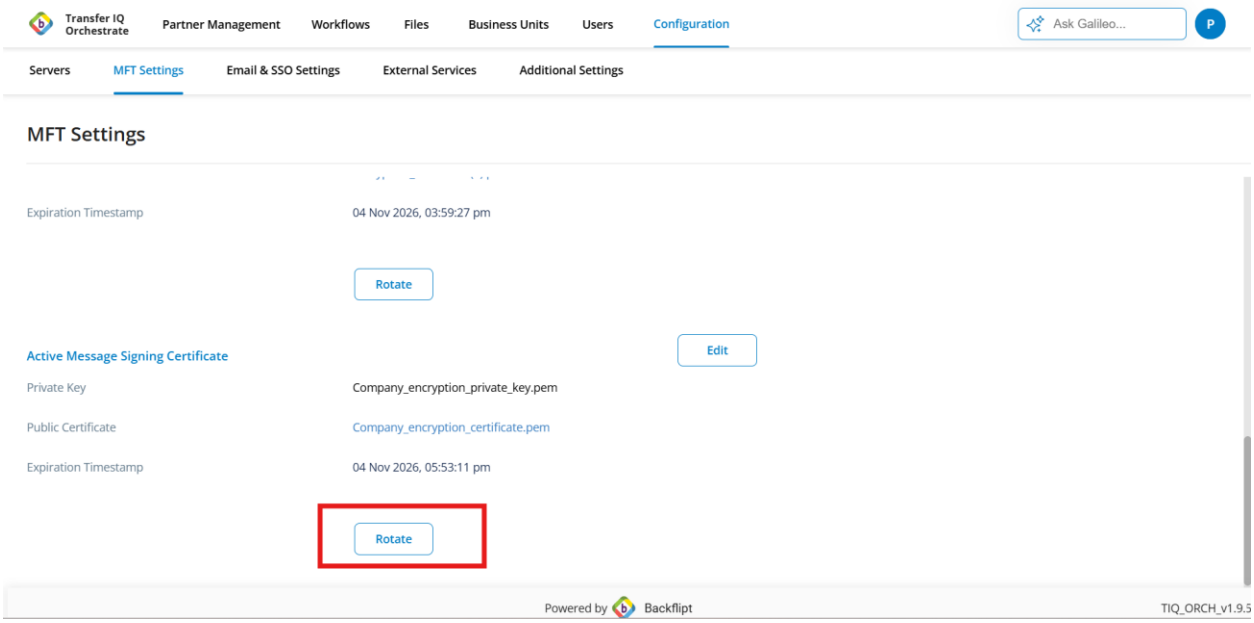
Before Rotation:

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.

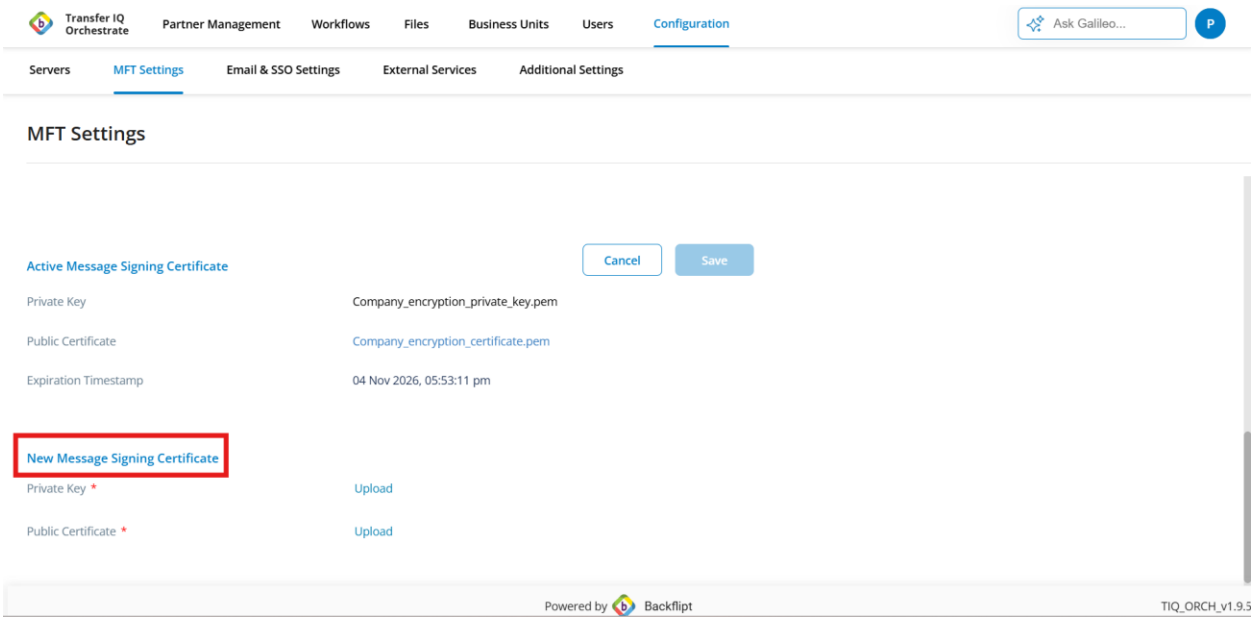
During Rotation

To begin the rotation process

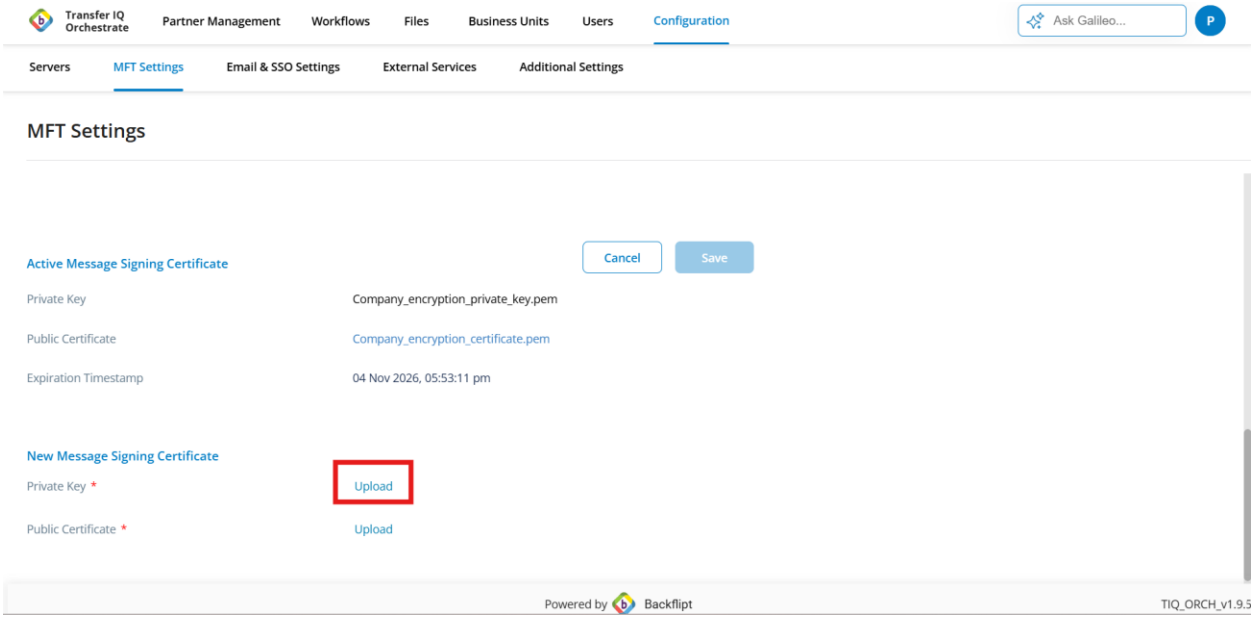
1. Navigate to **MFT Settings > Active Message Encryption Certificate**
2. Click the **Rotate** button located next to the **Active Message Encryption Certificate**



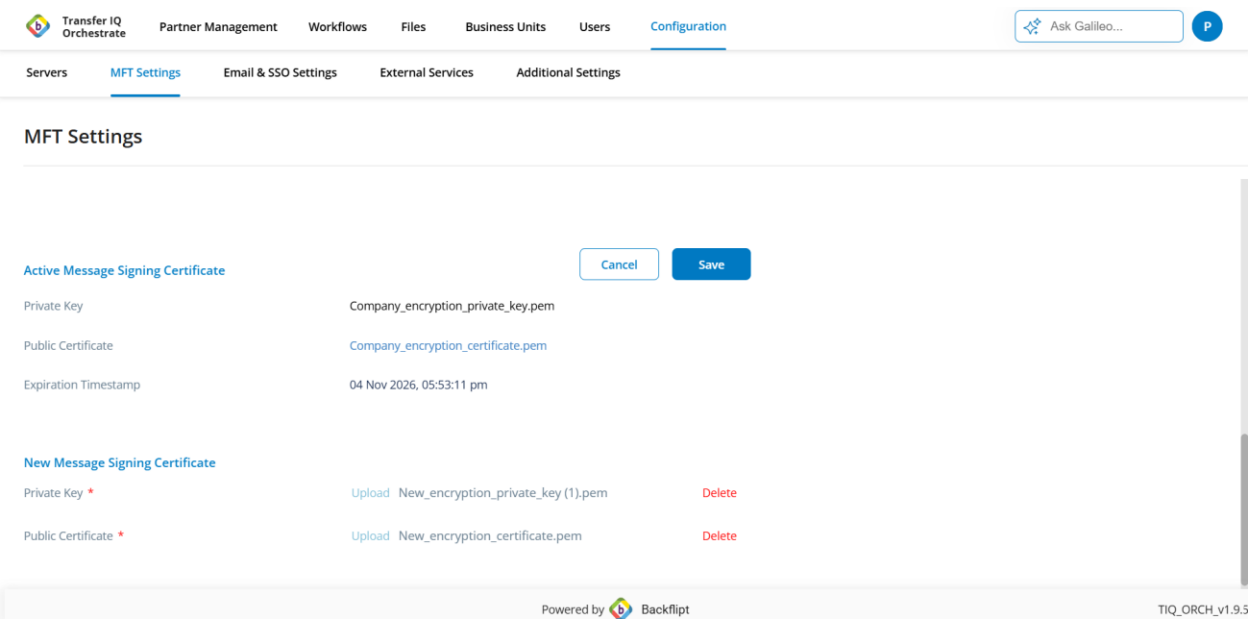
3. This action displays an additional section labeled **New Message Encryption Certificate** which includes fields for uploading both **public** and **private** Encryption Certificates.



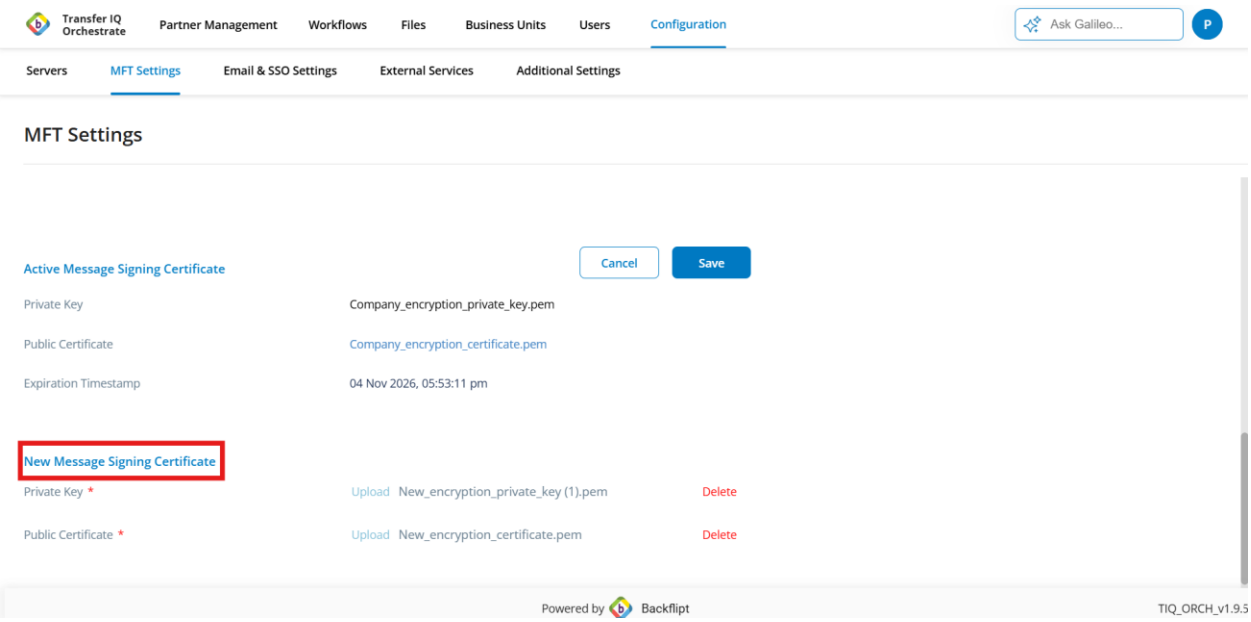
4. To upload the **New Message Encryption Certificate**, click the **Upload** button under the **New Message Encryption Certificate** section.



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**



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.



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**

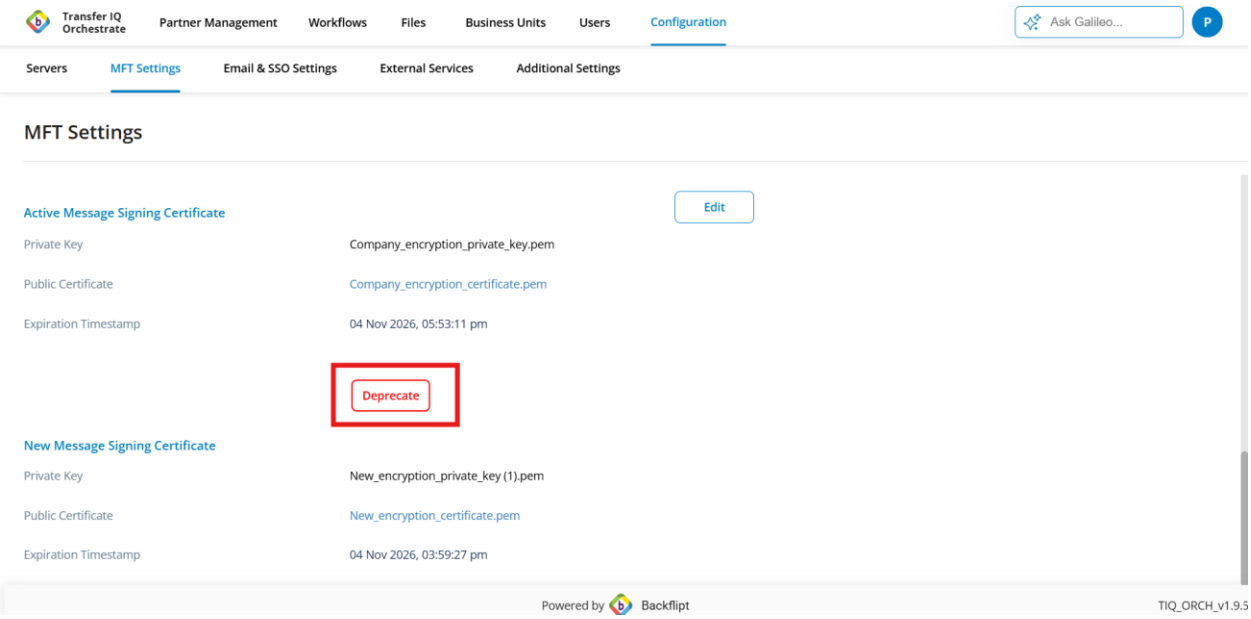
3. **Decryption succeeds** if the partner profile on the partner server contains:
    a. **either** the old certificate,
    b. **or** the new certificate,
    c. **or both certificates**.
4. If the file is encrypted using any of the certificates available on the partner server, the system can decrypt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

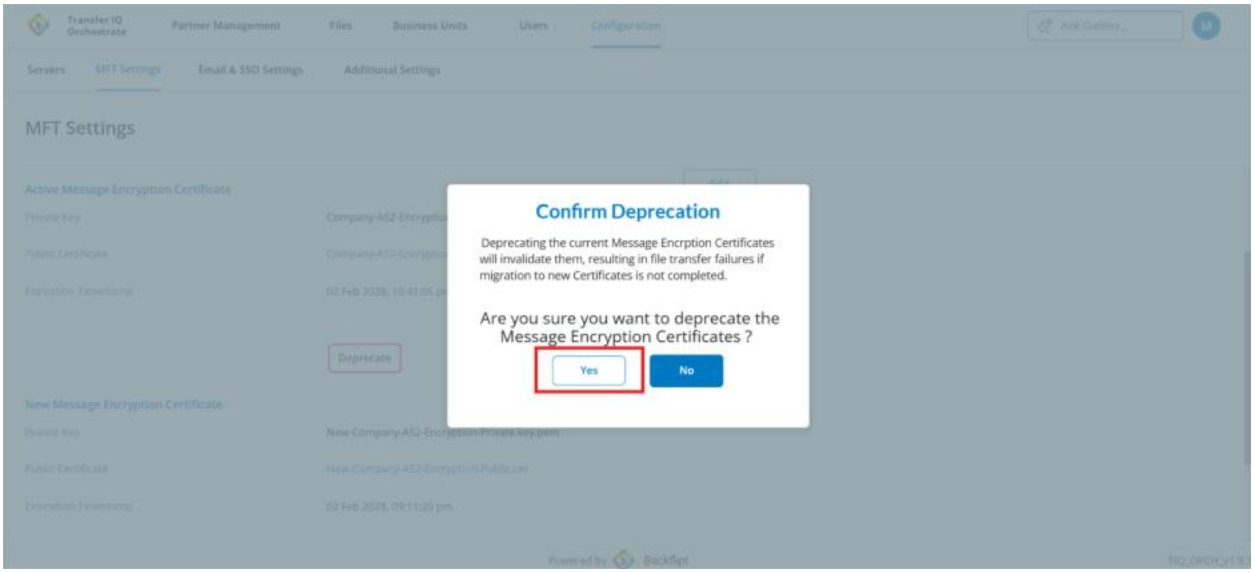
Deprecating Message Encryption Certificates

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**

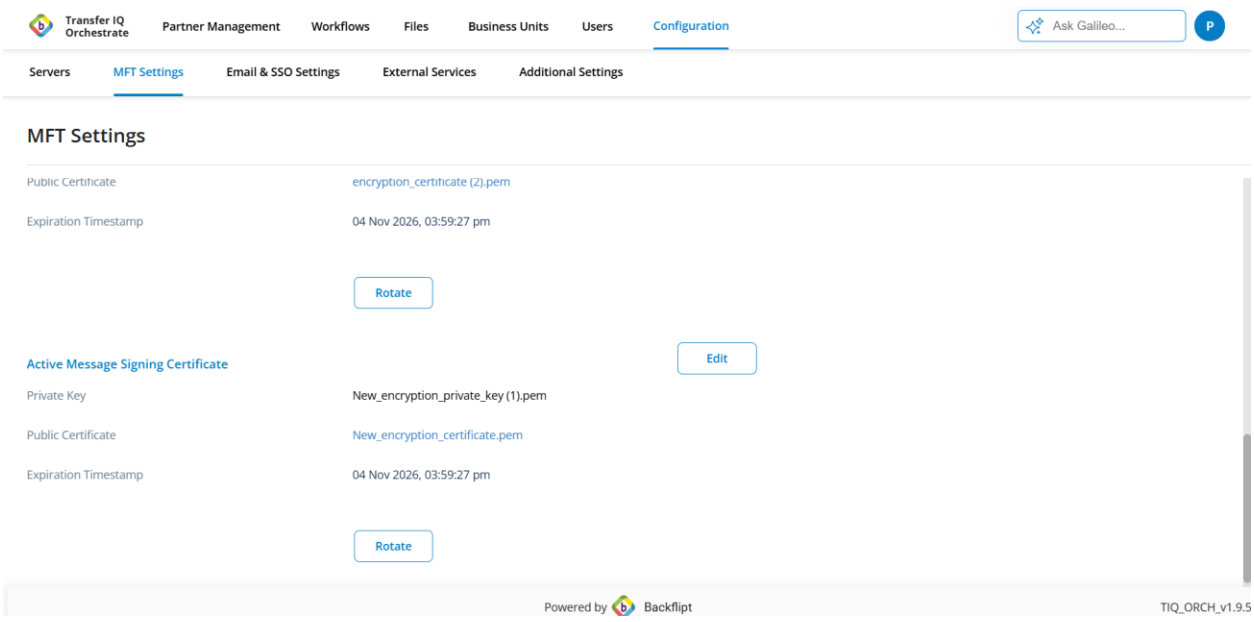


3. A **popup** is displayed asking for confirmation to deprecate the selected key.

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.



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**

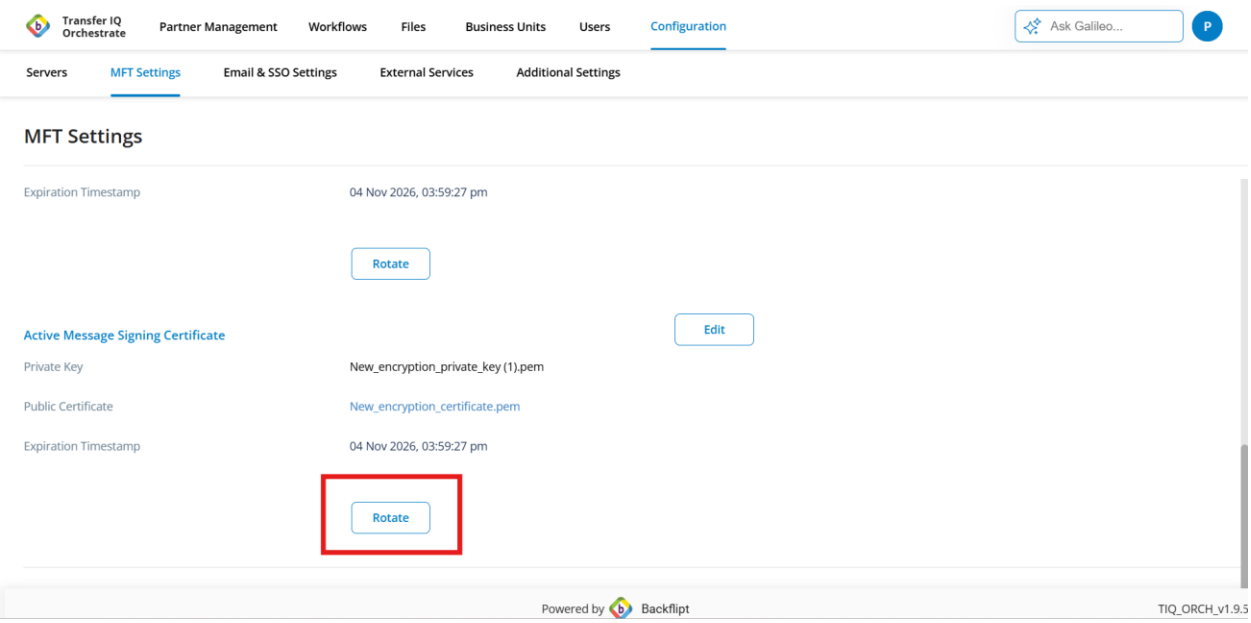
Before Rotation:

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**.

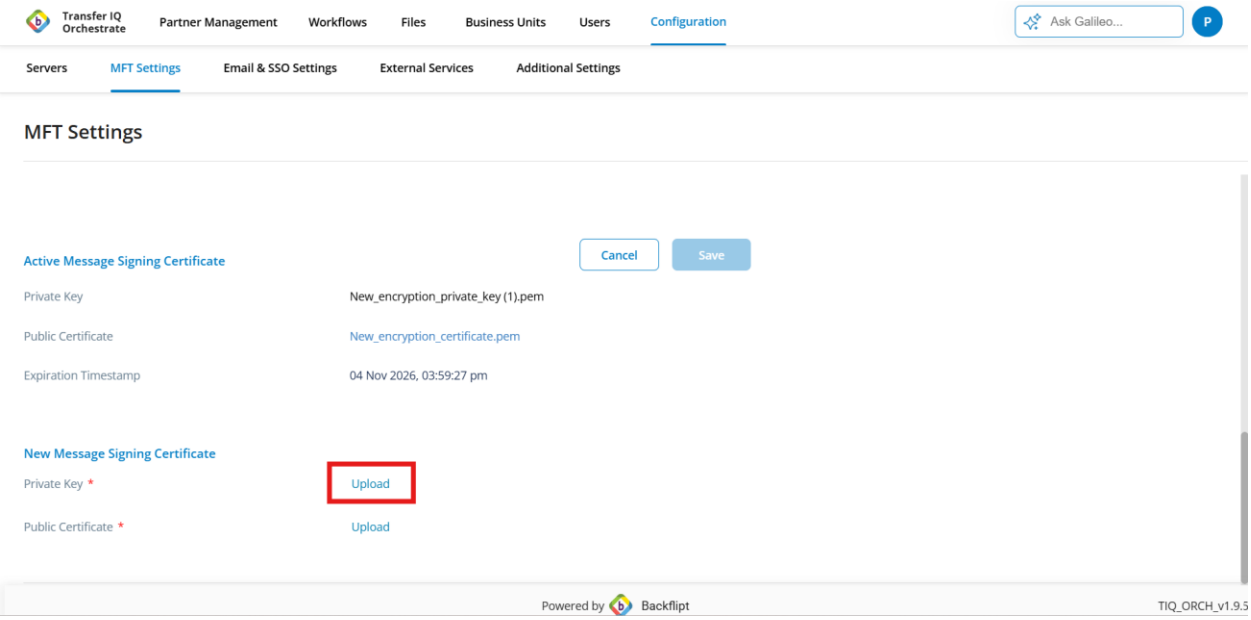
During Rotation

To begin the rotation process

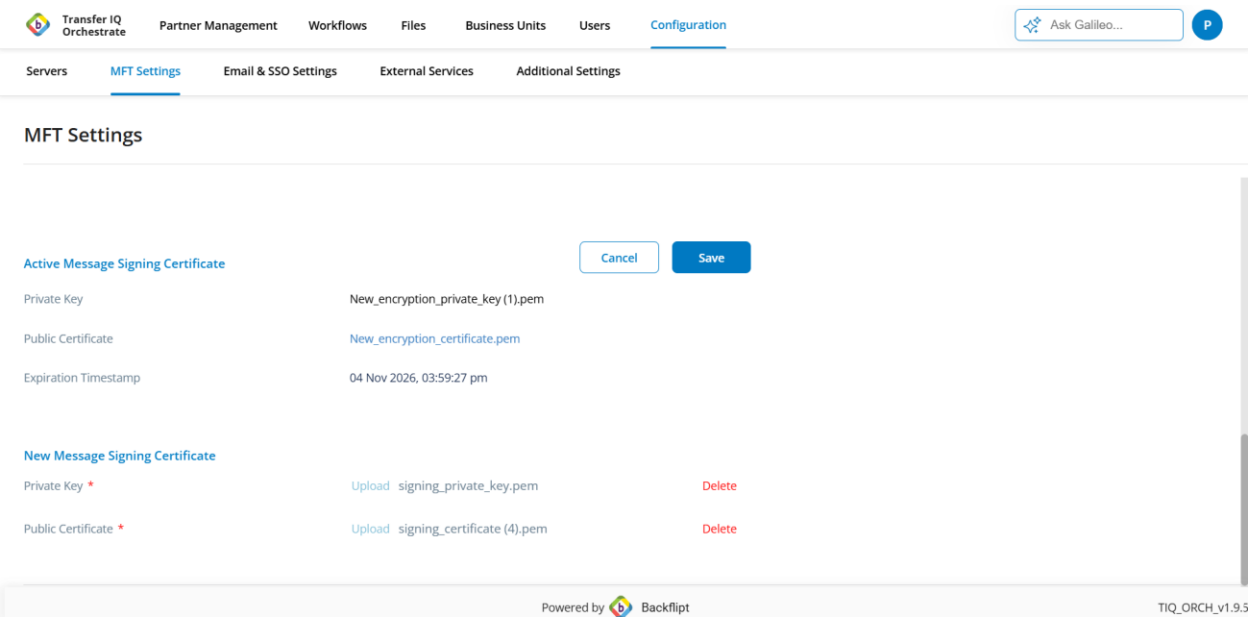
1. Navigate to **MFT Settings > Active Message Signing Certificate**
2. Click the **Rotate** button located next to the **Active Message Signing Certificate**



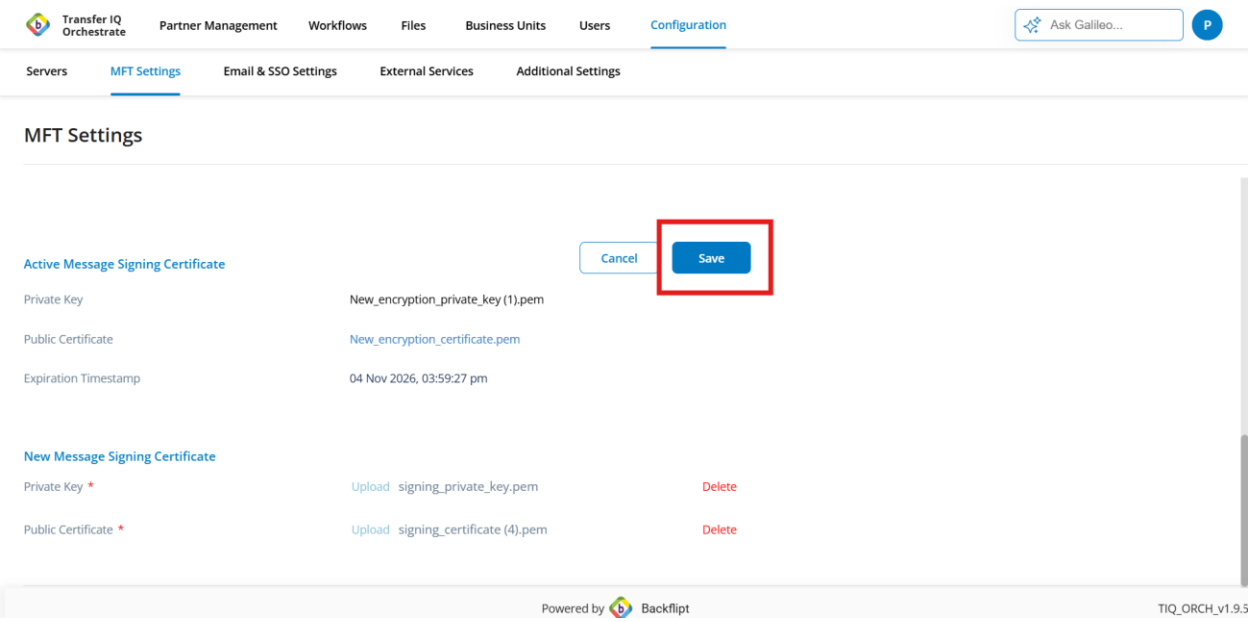
3. This action displays an additional section labeled **New Message Signing Certificate** which includes fields for uploading both **public** and **private** Signing Certificates
4. To upload the **New Message Signing Certificate**, click the **Upload** button under the **New Message Signing Certificate**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



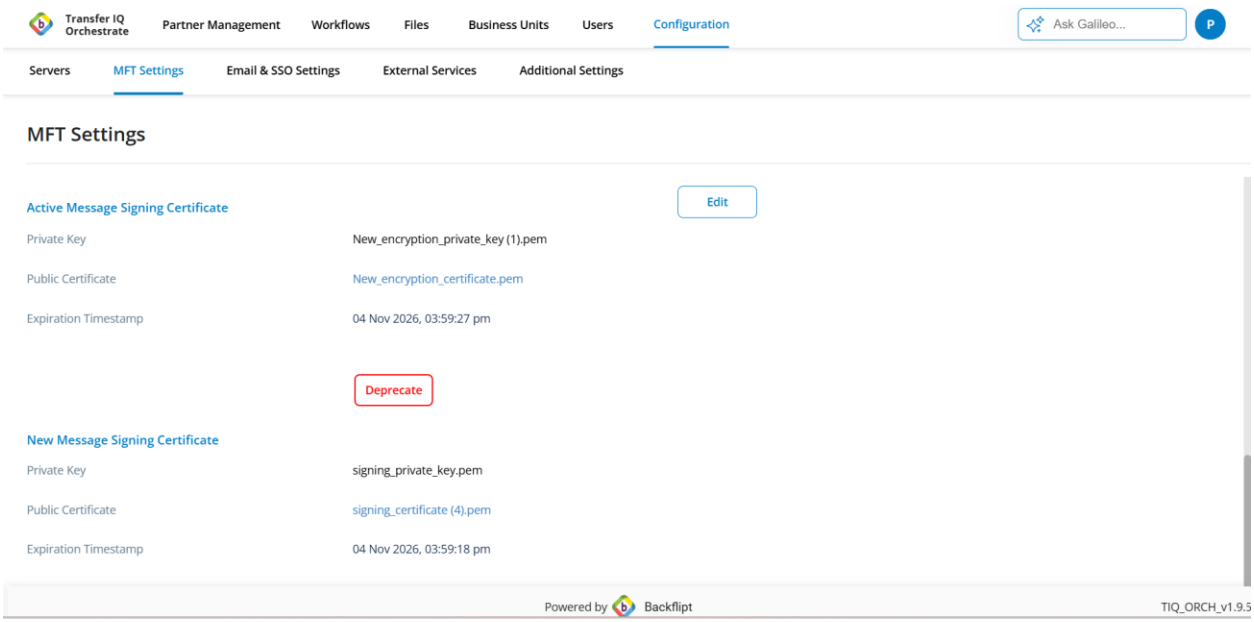
5. In the file selection dialog, choose a valid Signing Certificate.
6. Once the file is uploaded successfully, the newly uploaded keys are displayed in the **MFT Settings** tab under the **New Message Signing Certificates section**



7. Click **Save**.



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

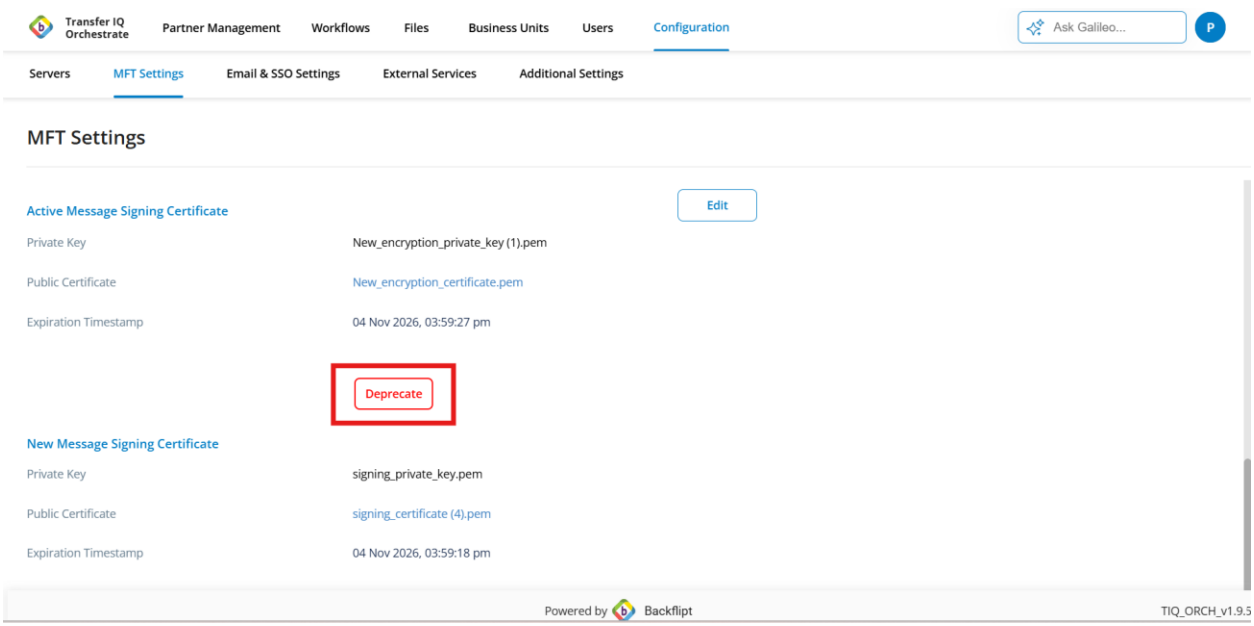
1. **Two certificates** are visible in the **MFT Settings** tab.
2. Once the certificates are rotated, the **new certificate pair** is also attached to the **Enterprise Local Profile**, along with the old one.
3. Out of the two available certificates, **the certificate with the later expiration date (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

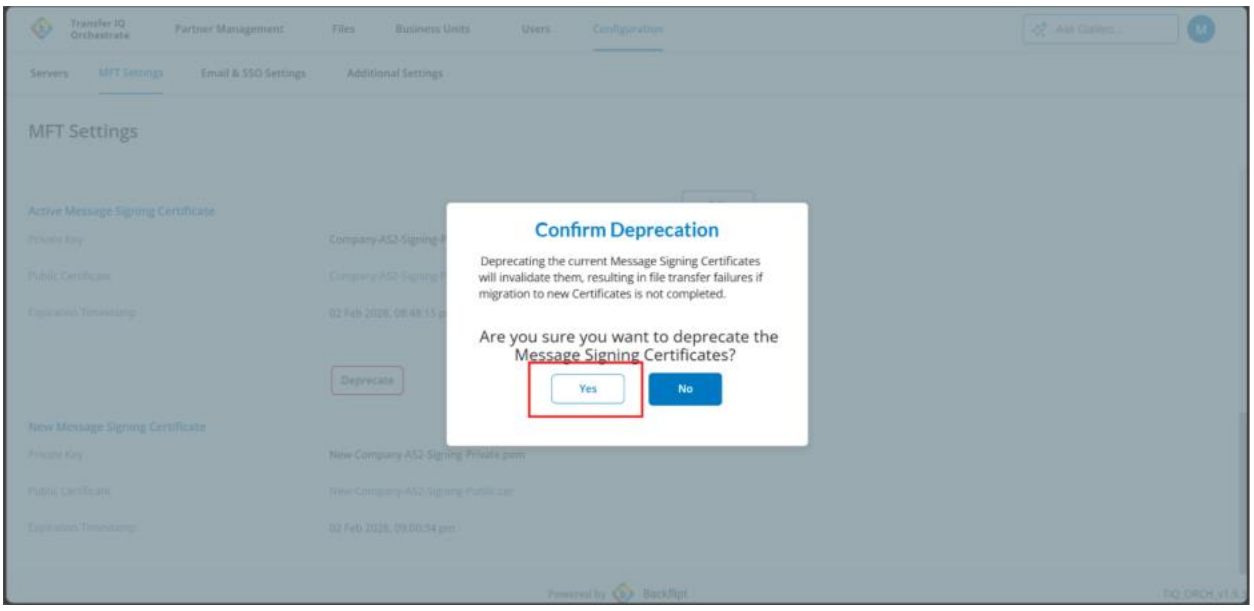
Deprecating a Certificate means disabling the old Certificate, so it can no longer used for signing outgoing messages, ensuring that only the newly rotated Signing Certificate is used.

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**



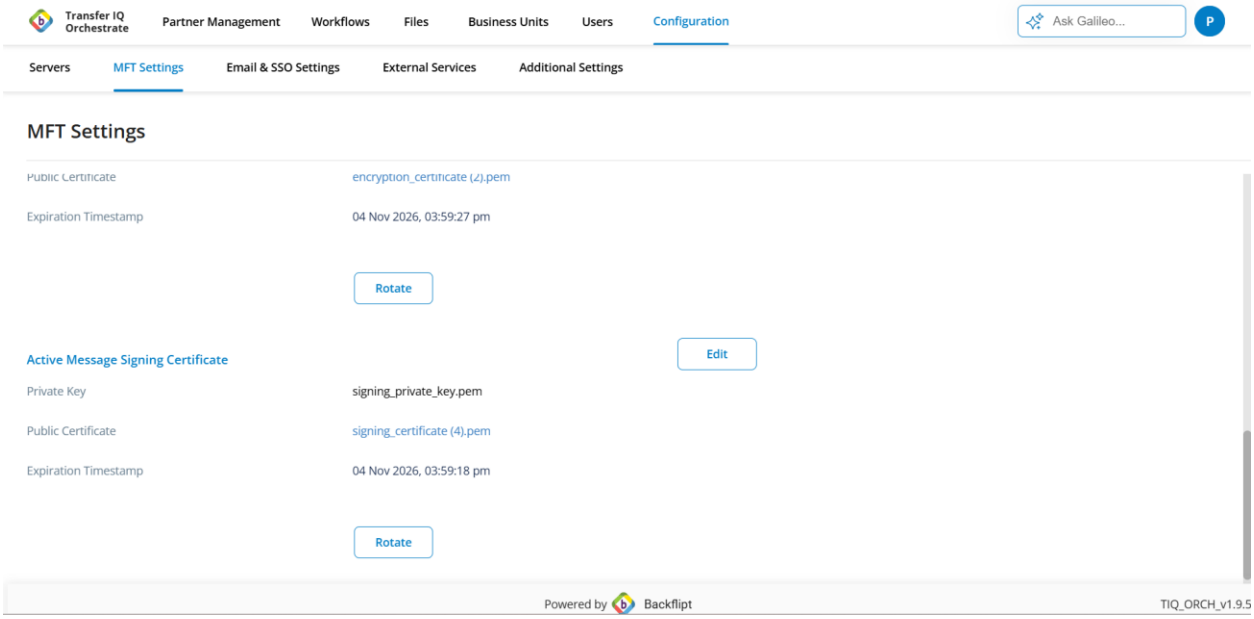
3. A **popup** is displayed asking for confirmation to deprecate the selected certificate
4. Confirm the action by clicking the **Yes button** in the popup. The system marks the key as **deprecated**, indicating it is no longer active for encrypting or decrypting new files



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



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

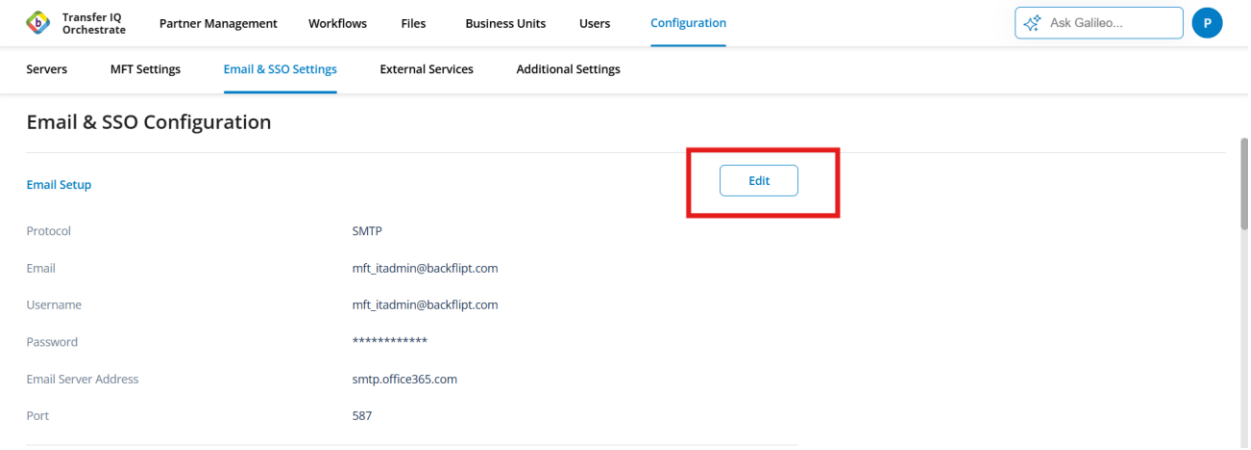
Email and SSO Settings consists of three sub sections

1. Email Setup
2. Email Templates
3. SSO Settings

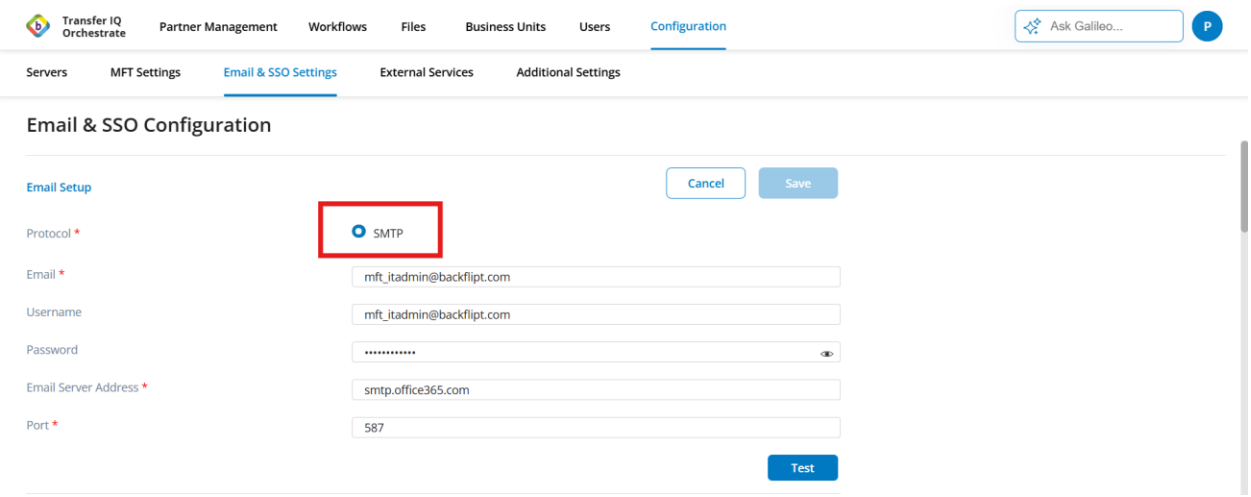
Email Setup

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

Click the Edit button to edit the email setup

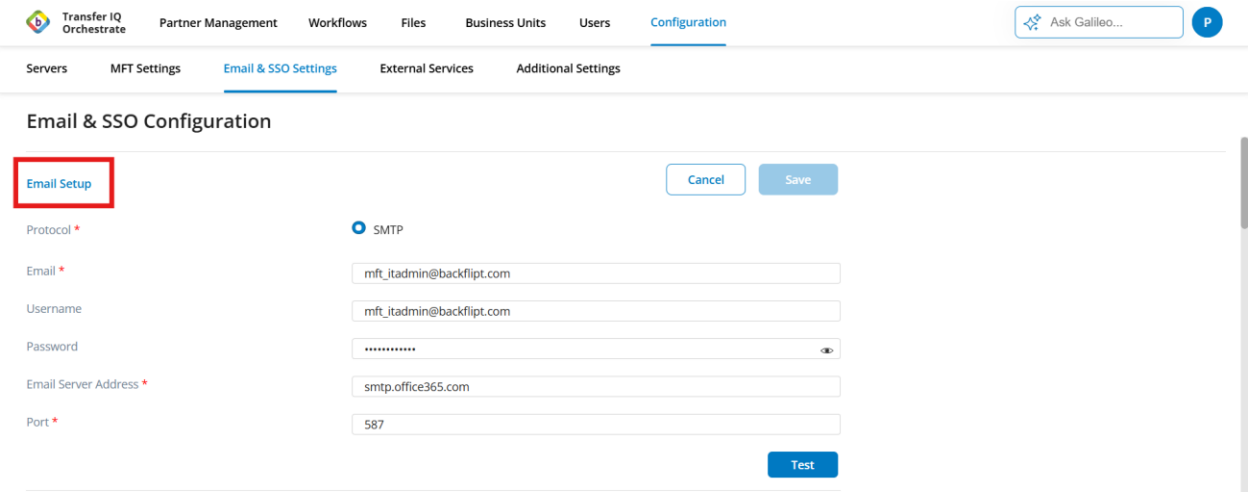


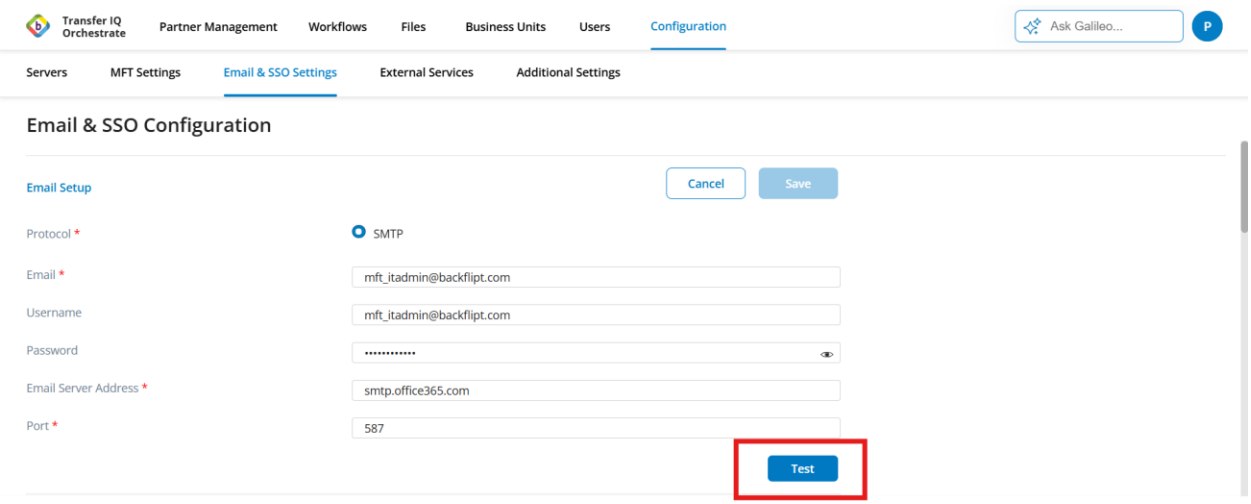
The application supports SMTP (Simple Mail Transfer Protocol) for sending emails, which requires specifying the appropriate email server and credentials.



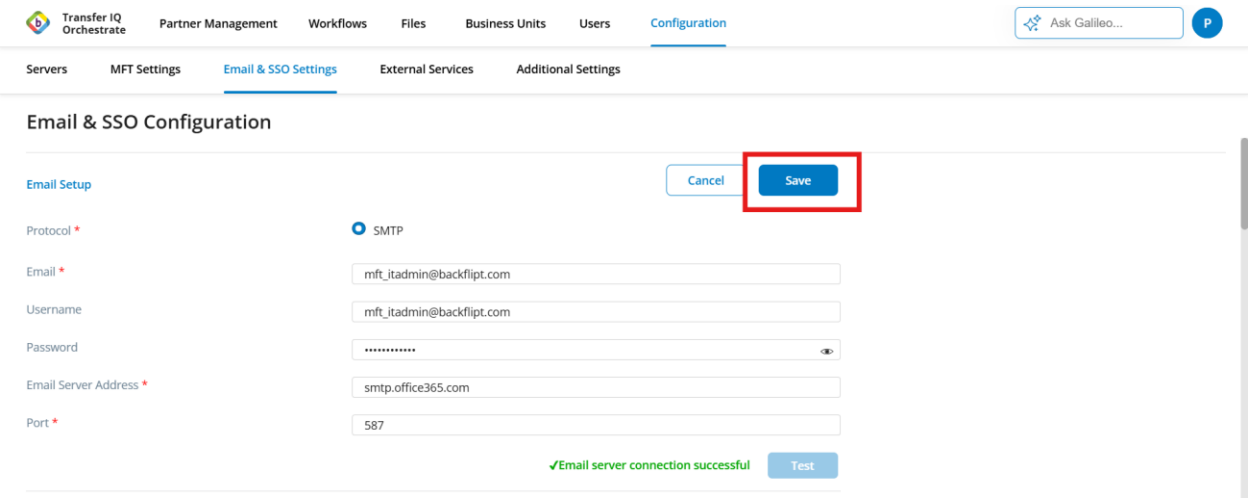
This section contains the below fields

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

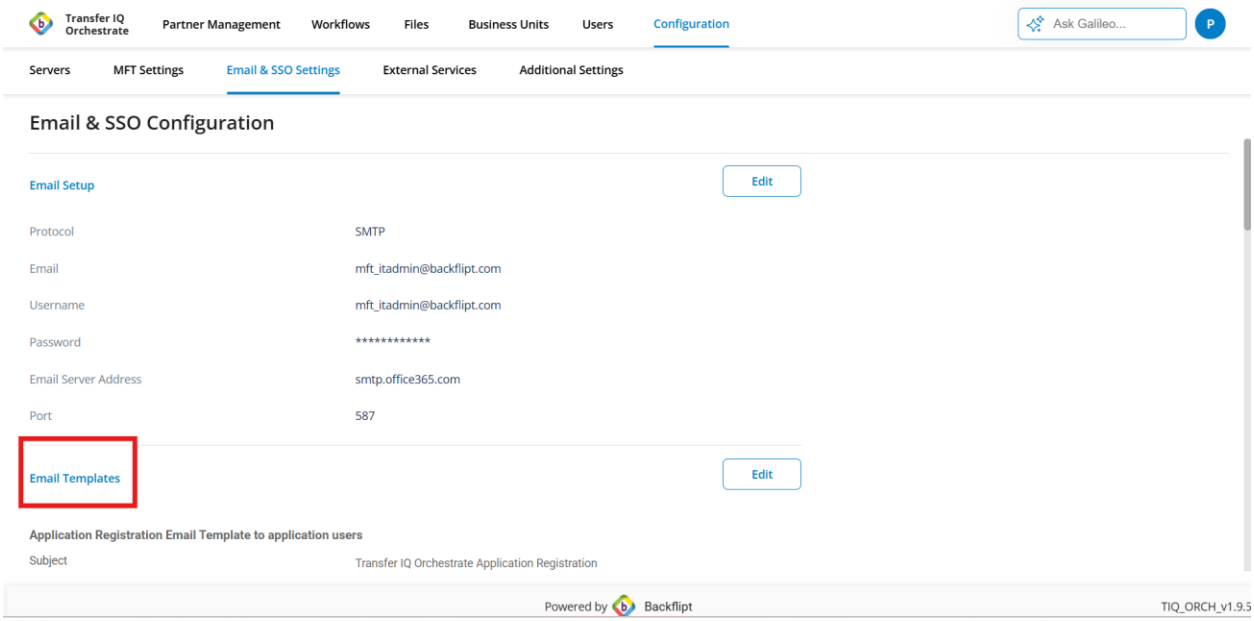




Once the Super Admin has entered all the SMTP details, Super Admin click the **"Test"** button to verify the connection. If the connection is successful, a confirmation message will be displayed indicating that the email server has been successfully connected.



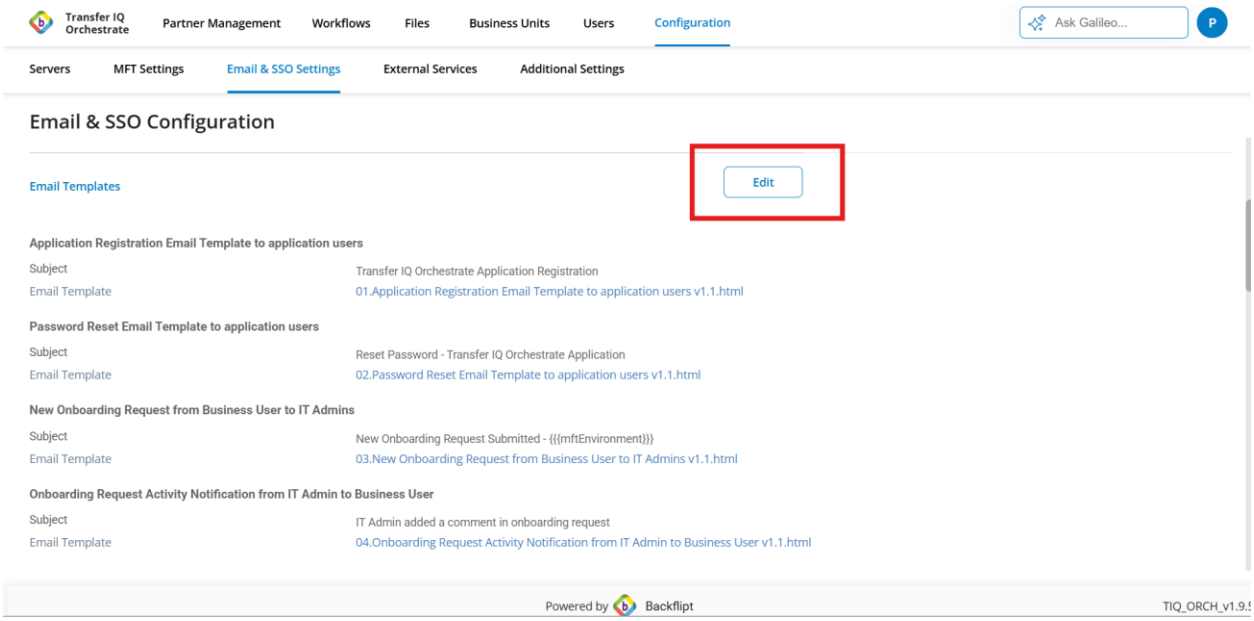
After a successful test, click the **"Save"** button to save the details. Once saved, the details will appear in **view mode** within the **Email Setup** section



Email Templates

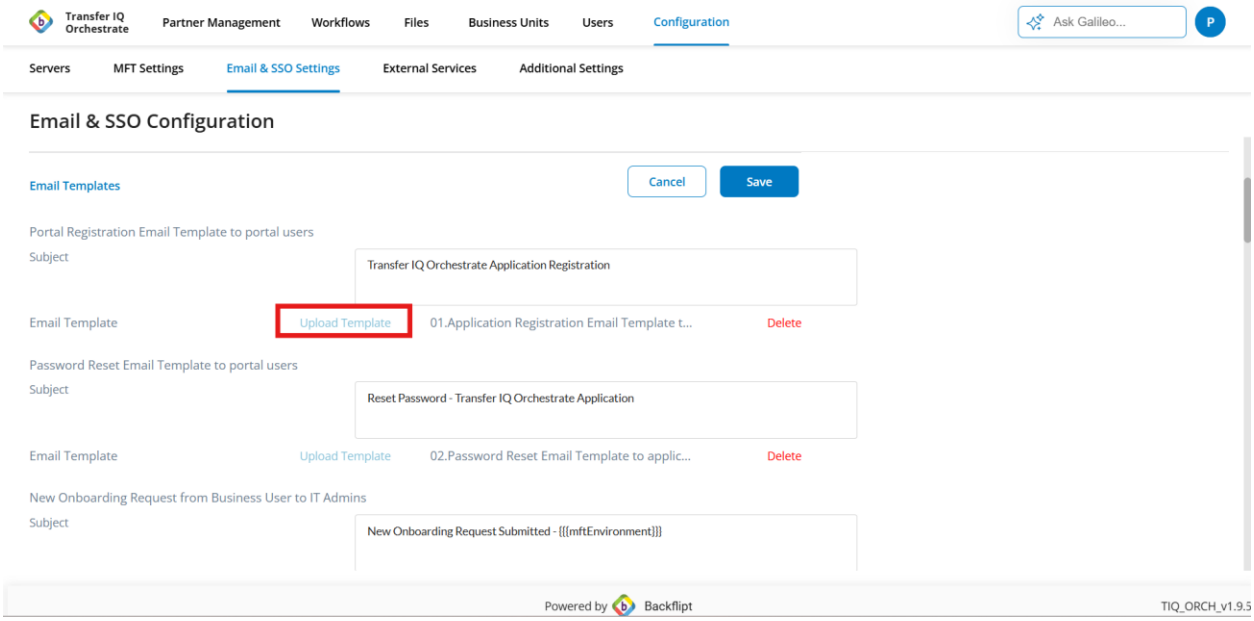
Upon the first login of the **First Super Admin**, a set of default **Email Templates** is automatically populated in the email templates section. These templates define the content and subject lines for various system-generated emails such as user invitations, password resets, and notifications etc.

Click the edit button to make changes to the existing templates

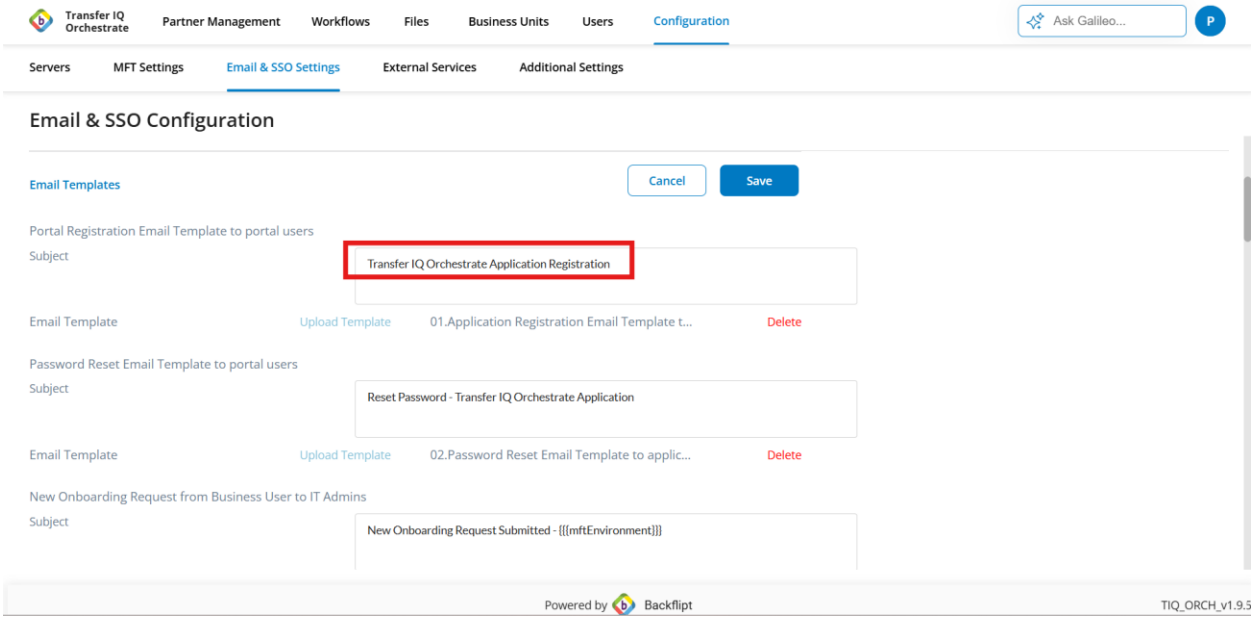


Each email template includes the following elements:

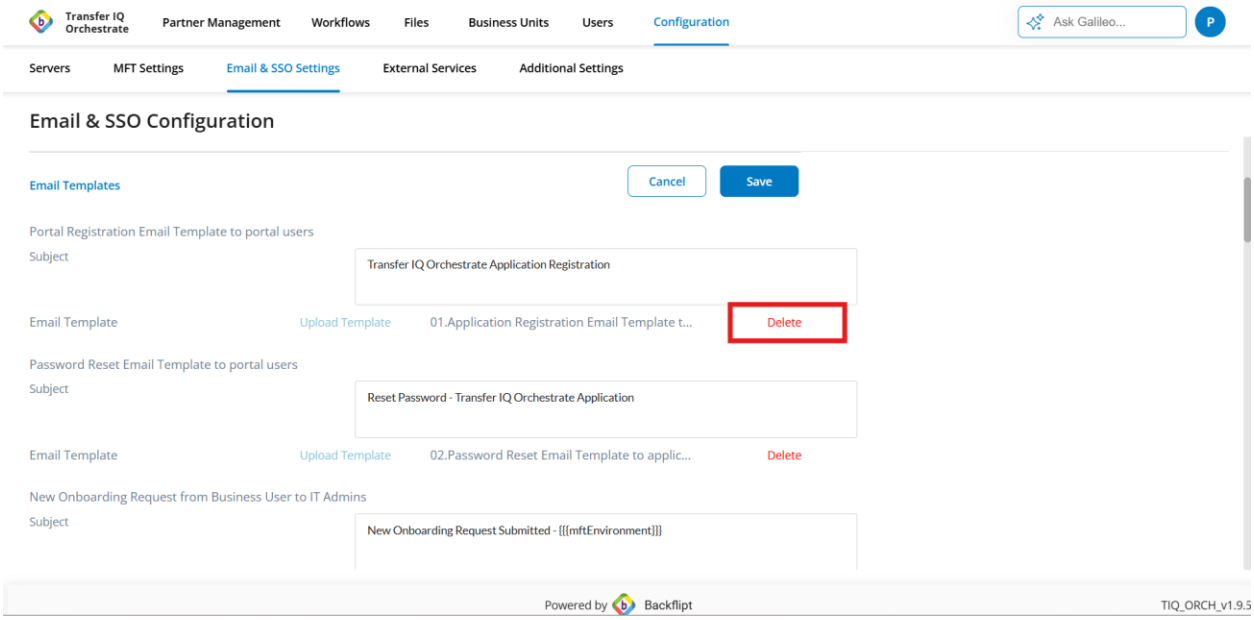
1. **Upload Button -** Allows the Super Admin to upload a custom email template file, replacing the default content if desired.



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



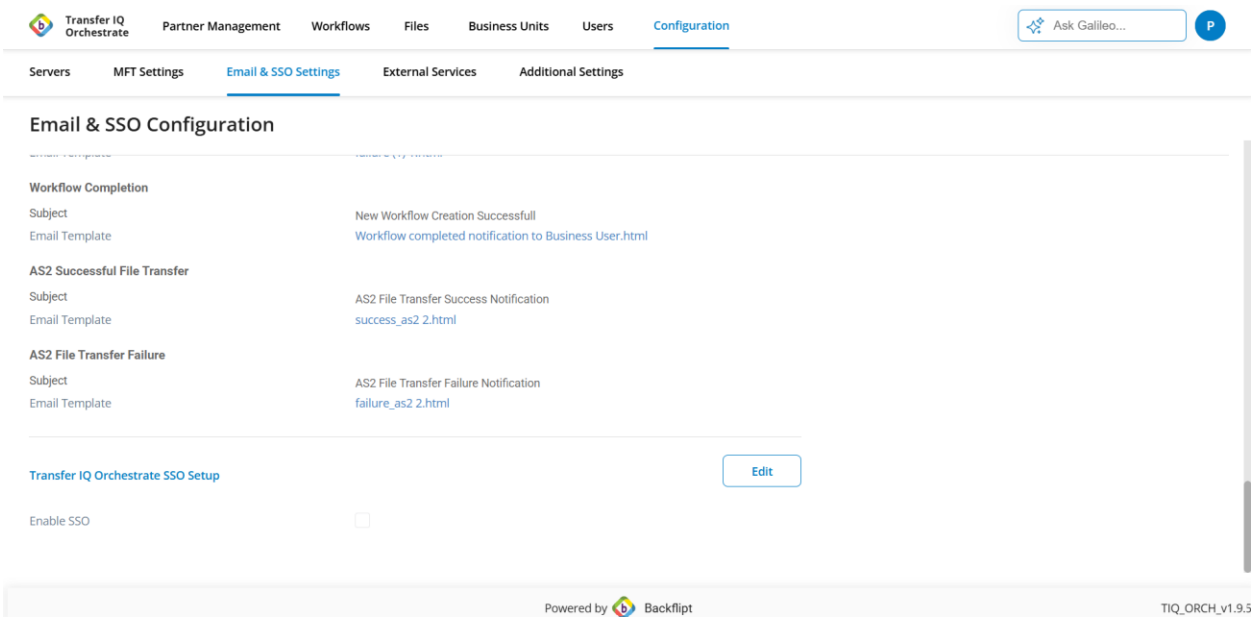
3. **Delete Button -** Removes the previously uploaded template and helps to upload a new template.



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
Edit
Enable SSO
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.

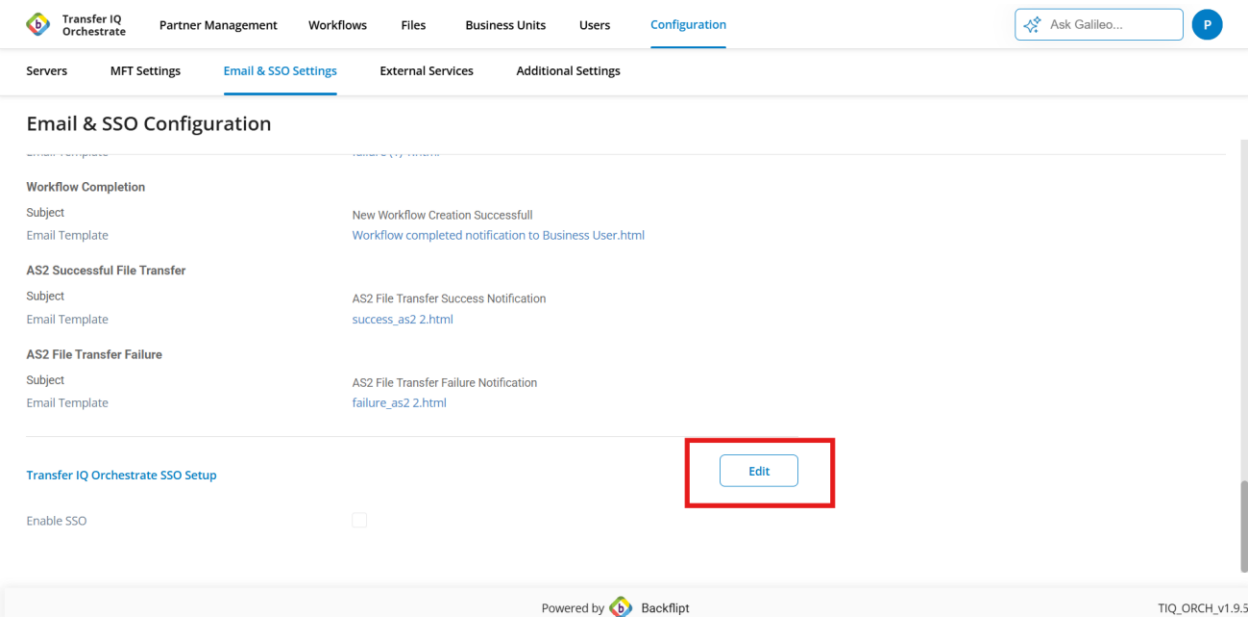
Instead of managing separate usernames and passwords for each application, users log in through a central **Identity Provider (IdP)** like **AWS IAM Identity Center**.

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.



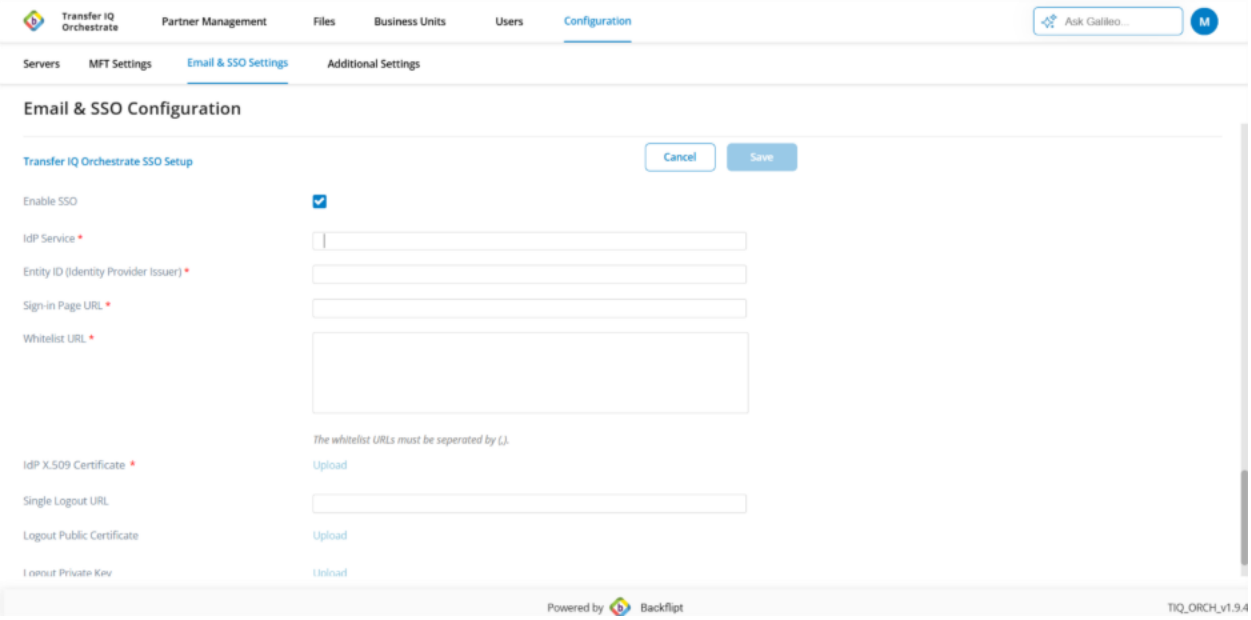
The SSO Section when enabled consists of the below fields

SSO Configuration Fields – Mandatory and Required Fields

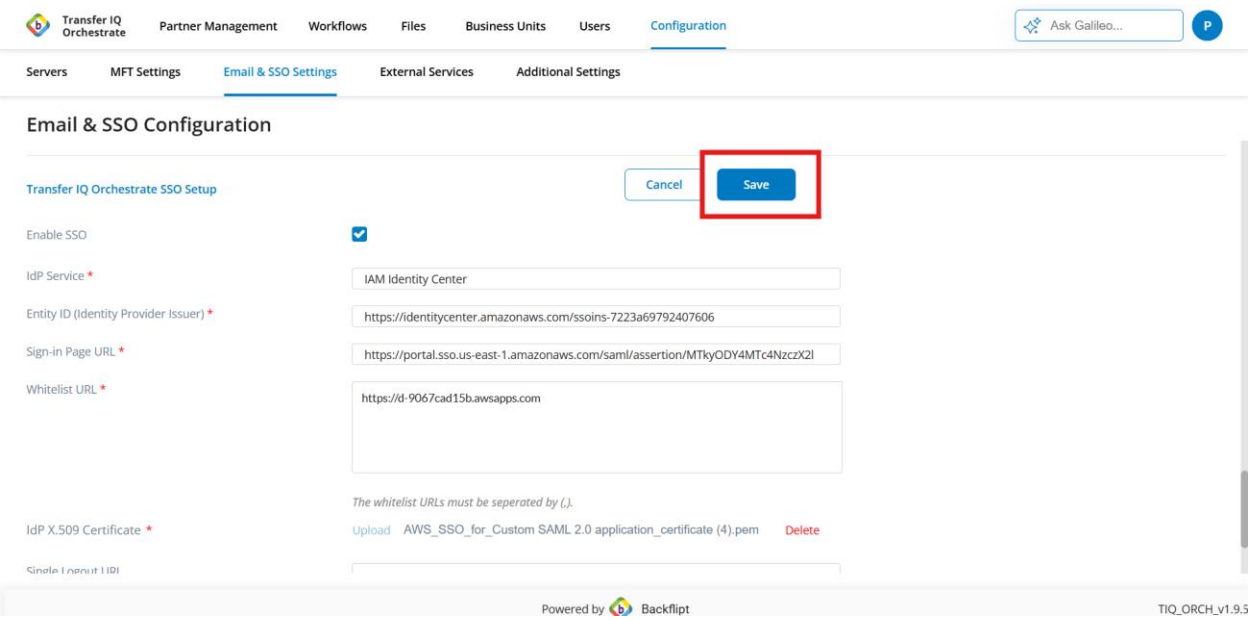
- **IdP Service -** The Identity Provider used for SSO. (e.g., **IAM Identity Center**
- **Entity ID -** This is the **Issuer URL** that uniquely identifies the IAM Identity Center.
- **Sign-in Page URL -** This is the AWS SAML Assertion Consumer Service (ACS) URL from IAM Identity Center, where users 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)

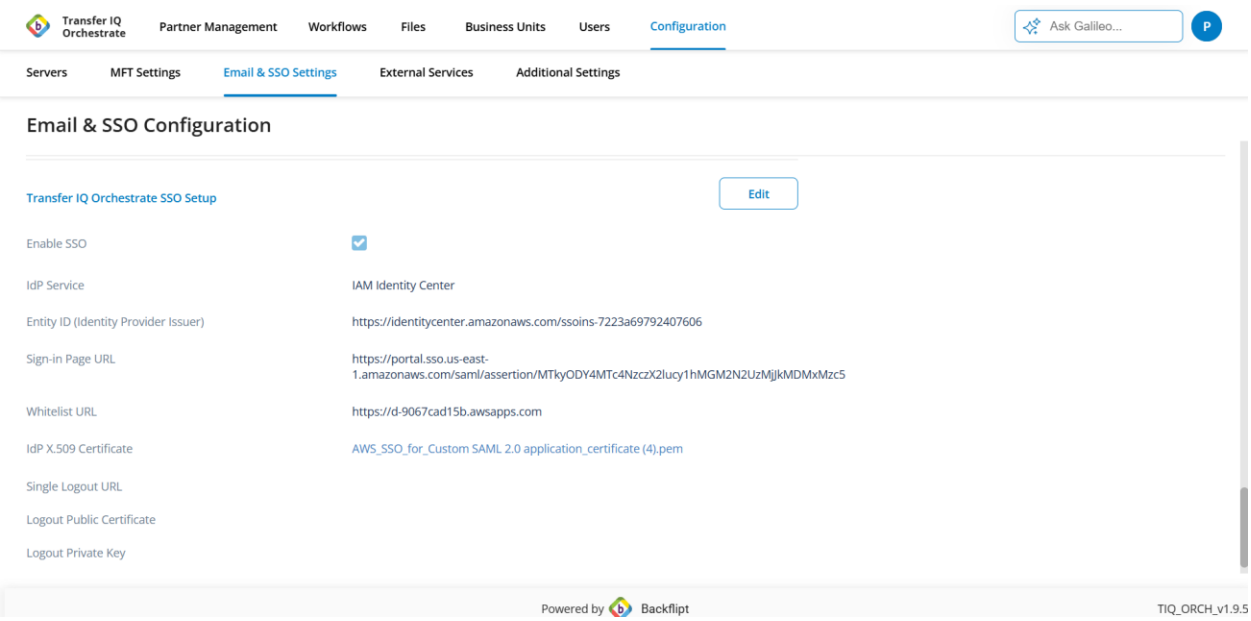
- **Single Logout URL -** This is the URL where users are redirected to log out from the Identity Provider when they sign out of the application. It helps ensure that the user is logged out from all connected applications in a single action.
- **Logout Public Certificate-** A public certificate used 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.



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



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



External Services

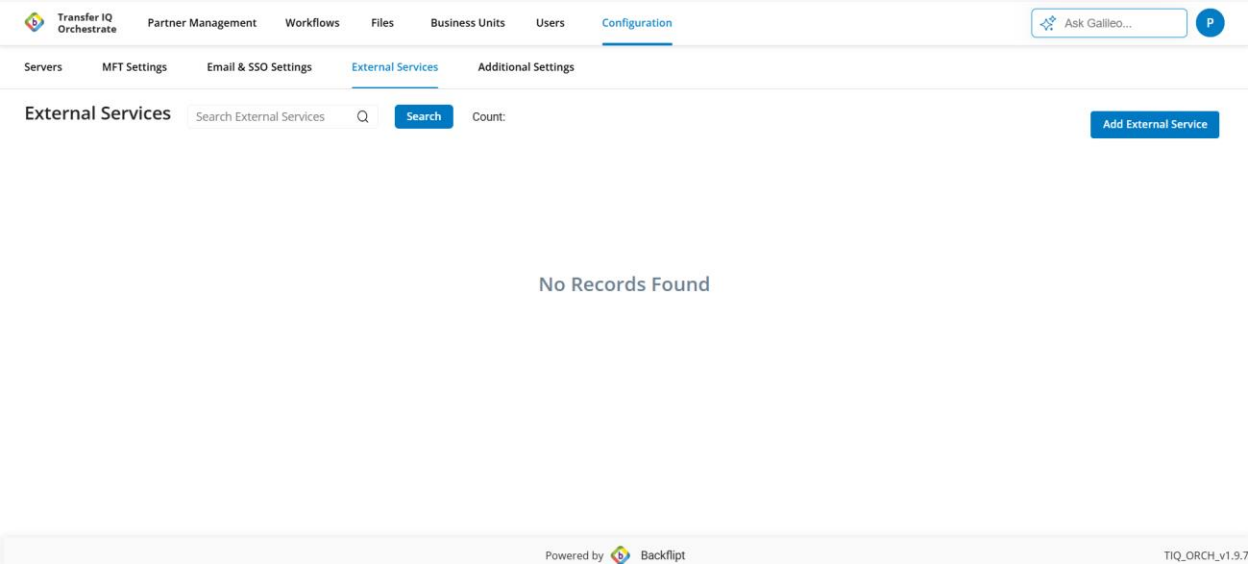
External Services can be created and configured within the External Services Section of the Configuration tab of orchestrate application. Once an External Service is created, it can be associated with a custom workflow step. When a workflow that includes this custom step is triggered, the configured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

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

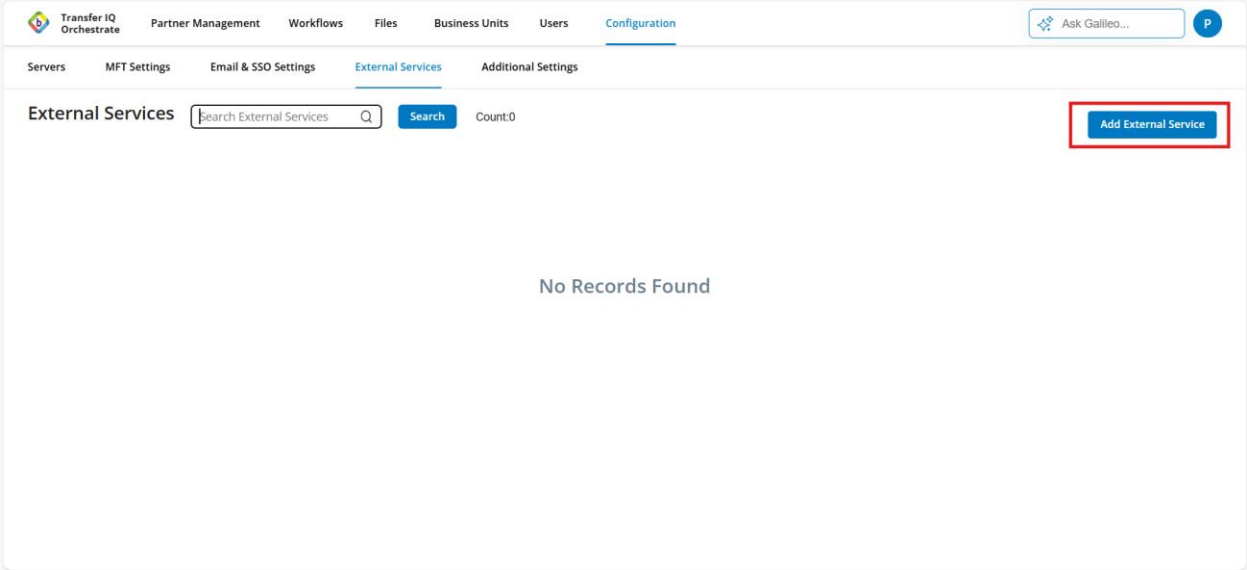
Creating an External Service:

To create an external service:

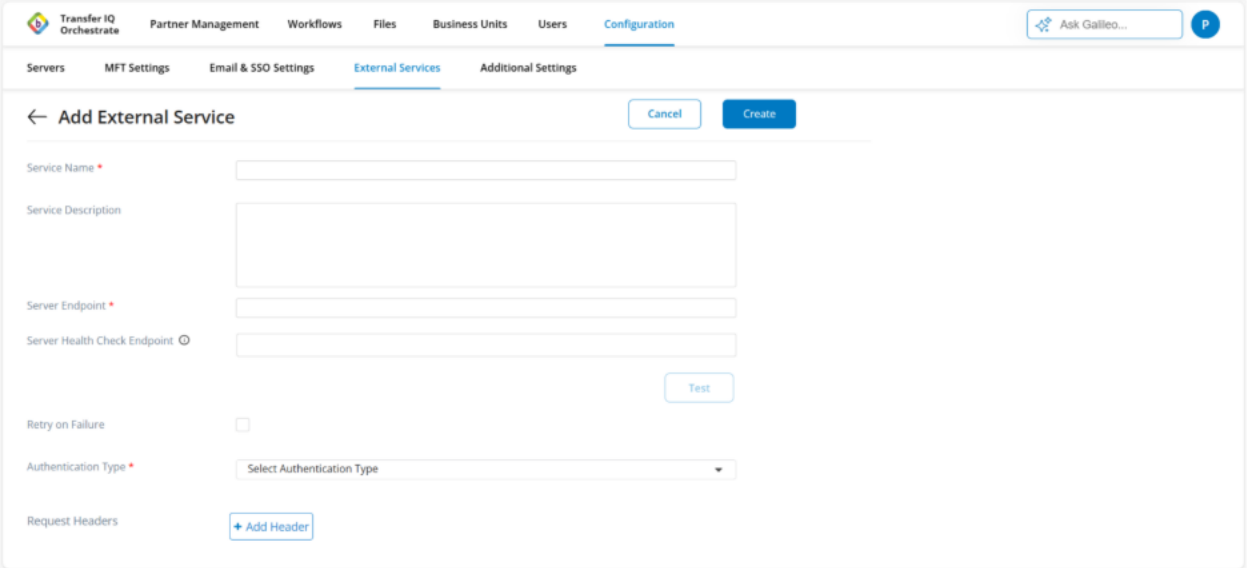
1. Navigate to Configuration > External Services (if there are no external services created yet No Records Found Text will be displayed)



2. Click on Add External Service

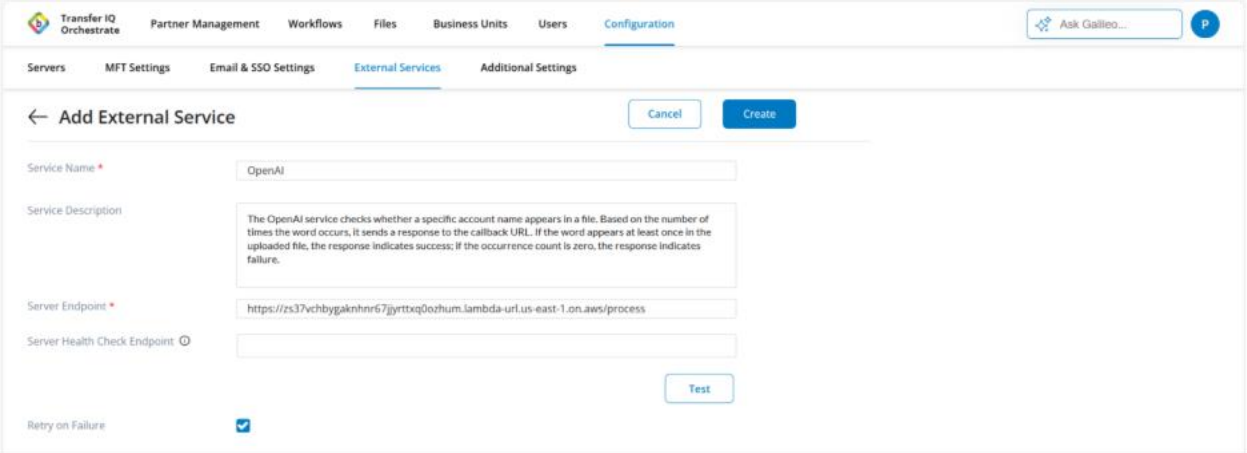


3. Once the **Add External Service** button is clicked, the **Add External Service** form is displayed with the following fields and buttons:

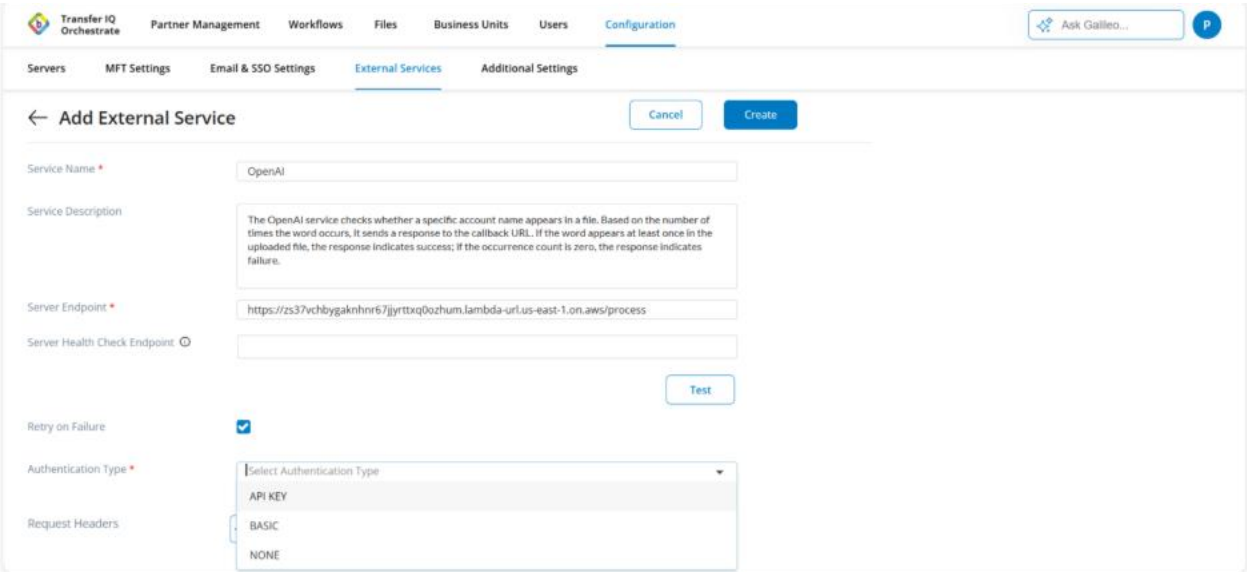


a. **Service Name * (Mandatory) -** This field is used to enter a unique name for the external service. The service name is required and helps identify the external service when configuring and selecting it in workflow custom steps.
b. **Service Description -** This optional field allows the user to 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

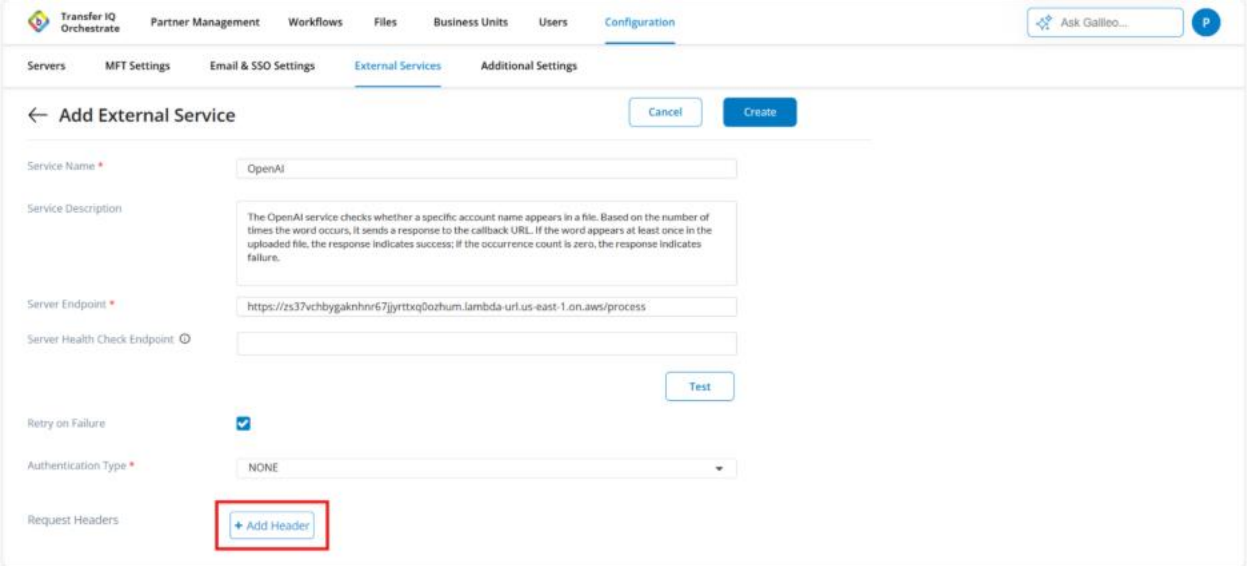


i. **None** - This option indicates that no authentication is required to access the external service. When selected, the request is sent without any authentication credentials.

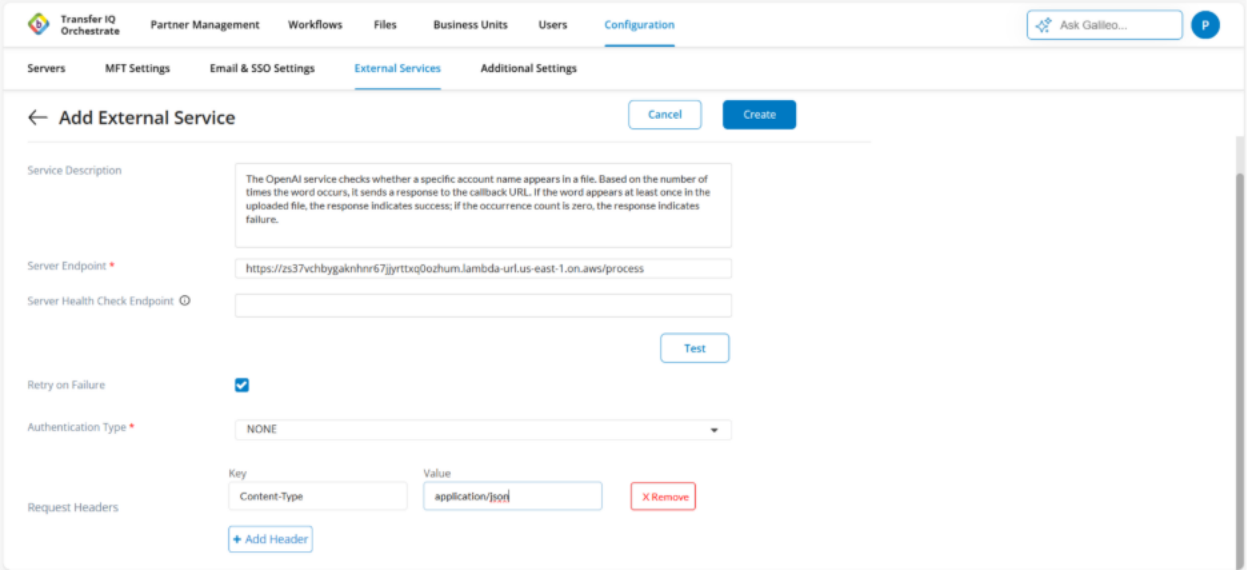
ii. **Basic** - This option enables Basic Authentication, where a username and password are required. When **Basic** is selected, additional fields are displayed to capture the username and password.

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.

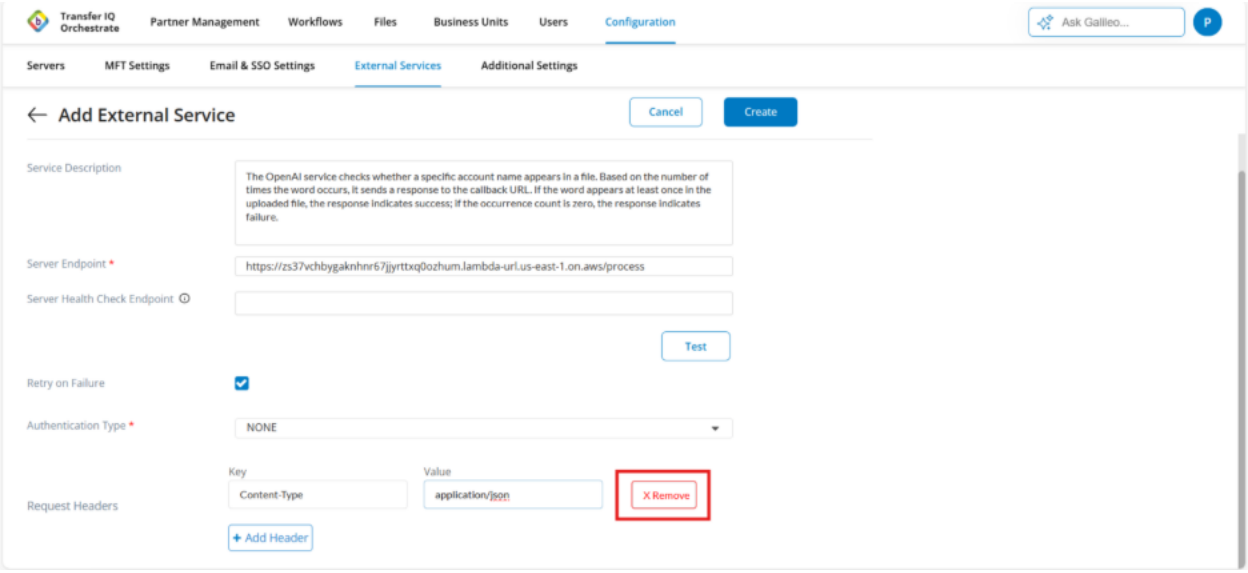
4. **Request Headers**
   a. This section allows users to define custom HTTP request headers that will be included when invoking the external service.
   b. Click the add header button

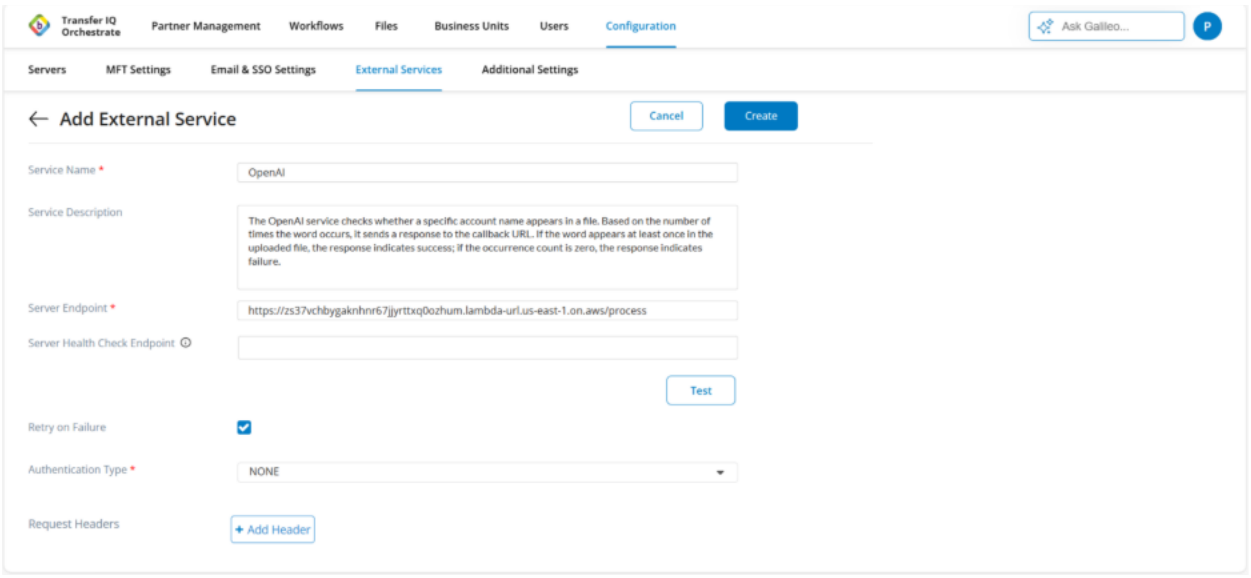


   c. Clicking the **Add Header** button displays two input fields—**Key** and **Value**—along with a **Remove** button. This enables administrators to add one or more key–value header pairs and remove any existing headers as needed
   d. Request headers are commonly used to pass authorization tokens, Content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

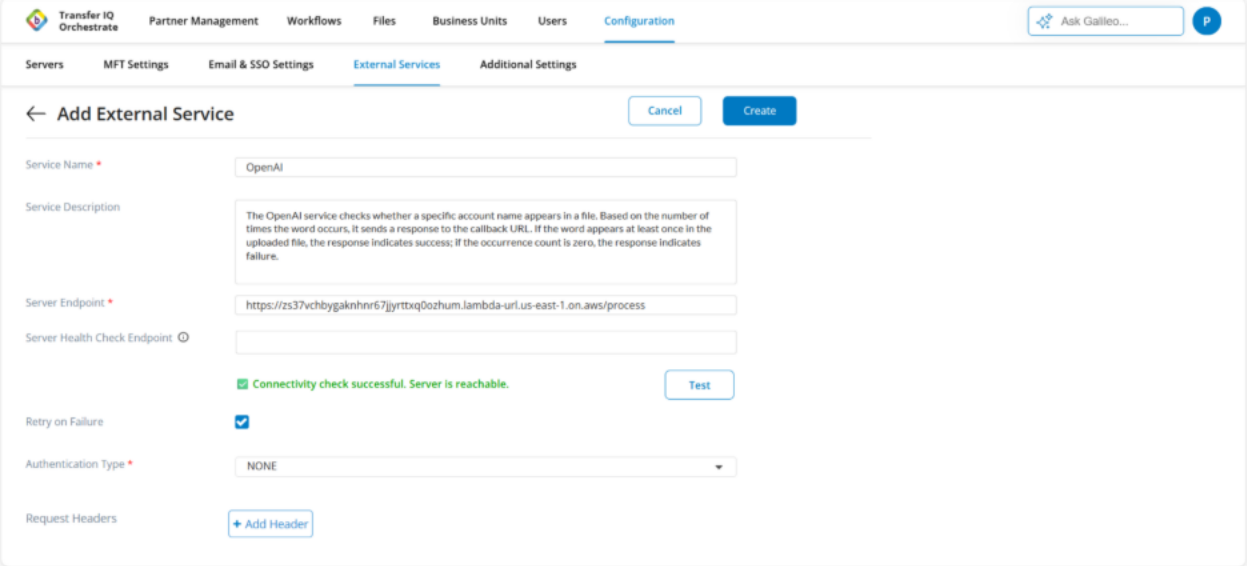


f. Clicking the remove button will remove the added header

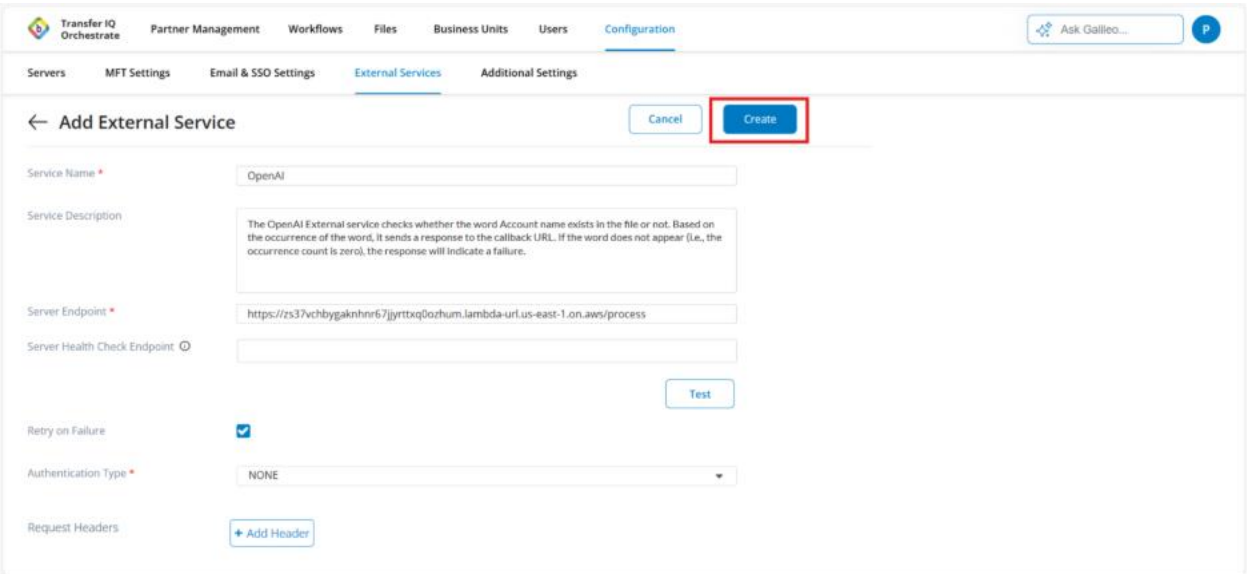




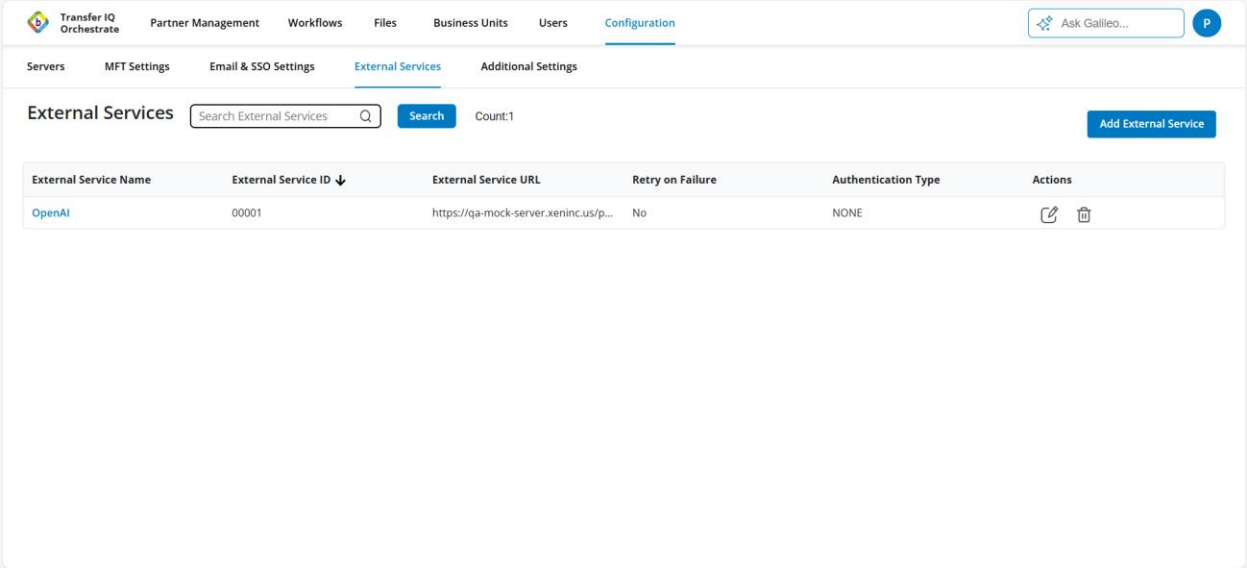
5. **Test External Service -** The **Test** button is used to validate the connectivity and availability of the configured external service before saving the configuration. When clicked, the system sends a request to the **Server Health Check Endpoint** (or the primary server endpoint if a health check 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.
    a. Based on the outcome of the test, the system displays appropriate messages to inform the user of the result:
    b. 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



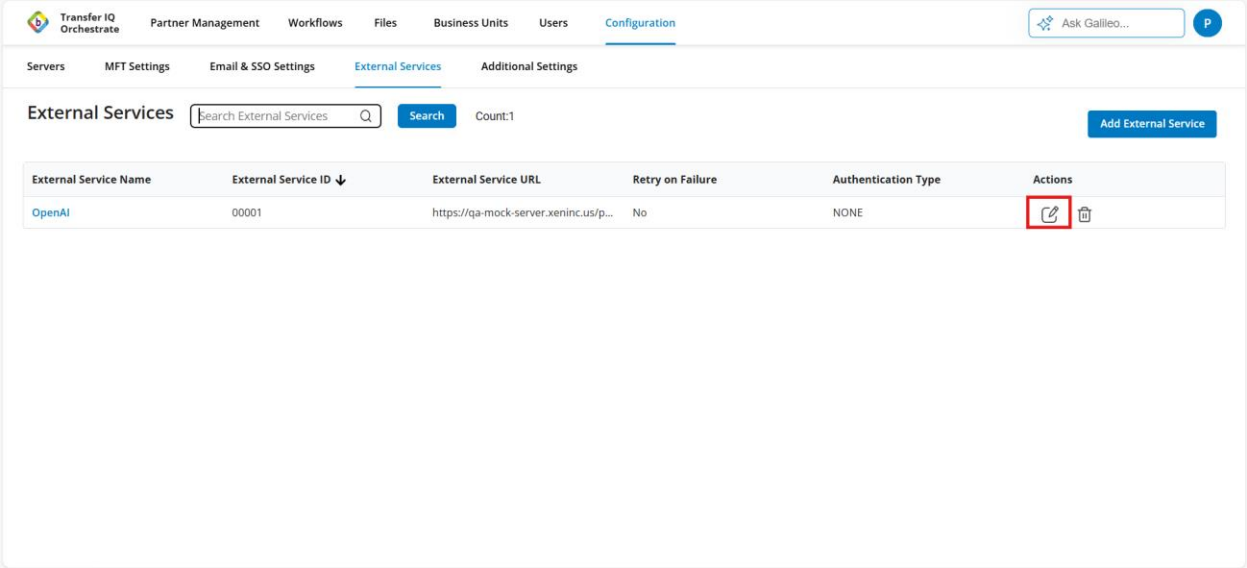
Update External Service:

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:

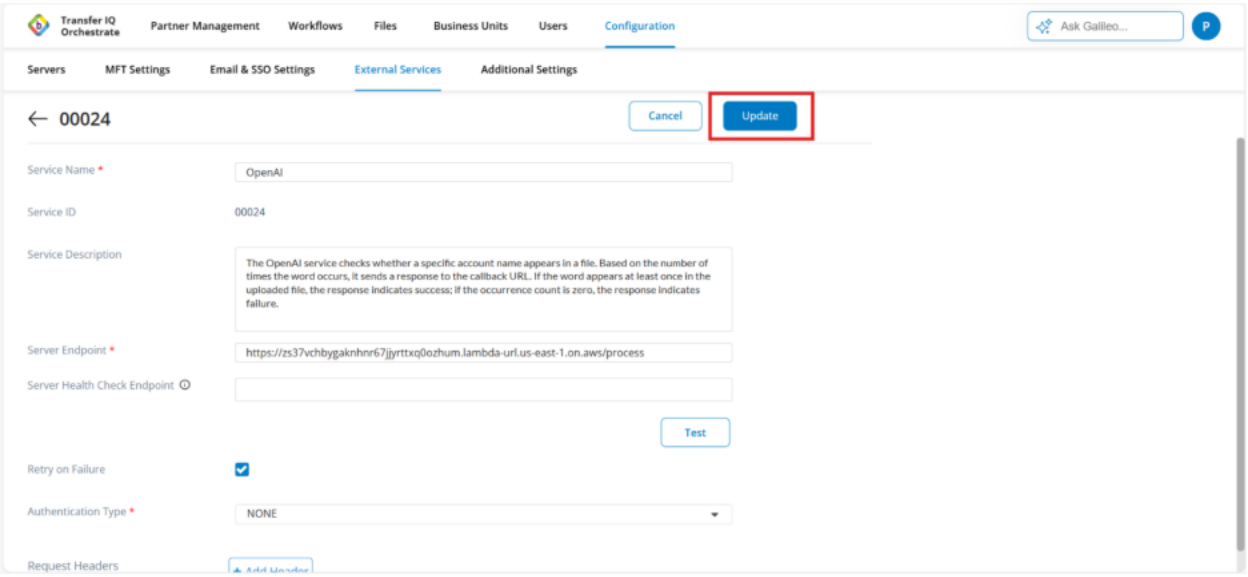
1. Click the **Edit** icon next to the external service in the view table.
2. By navigating to the external service's detail view and clicking the **Edit** button.

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.

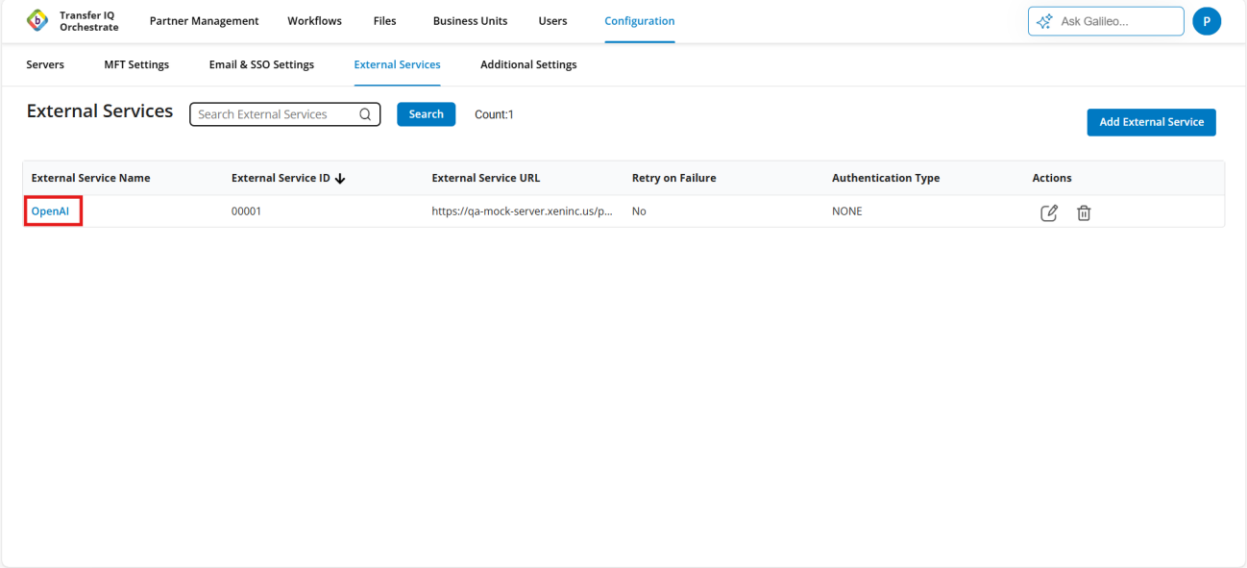


4. Modify the required fields.
5. Click **Update** to save the changes.

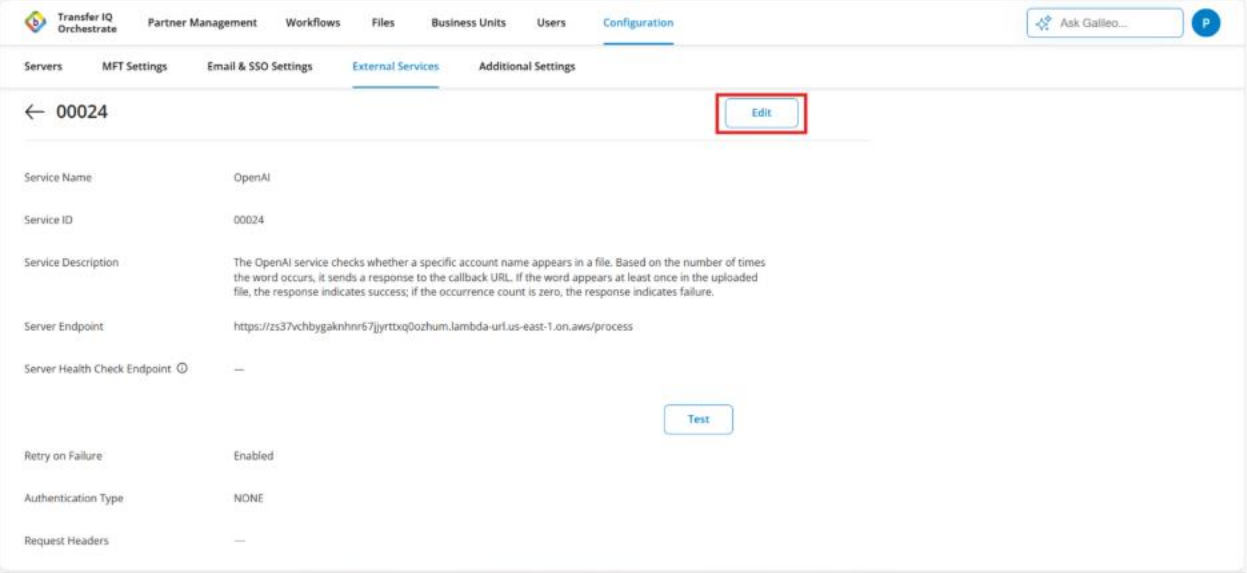


Option 2: Edit from the External Service Details View Mode

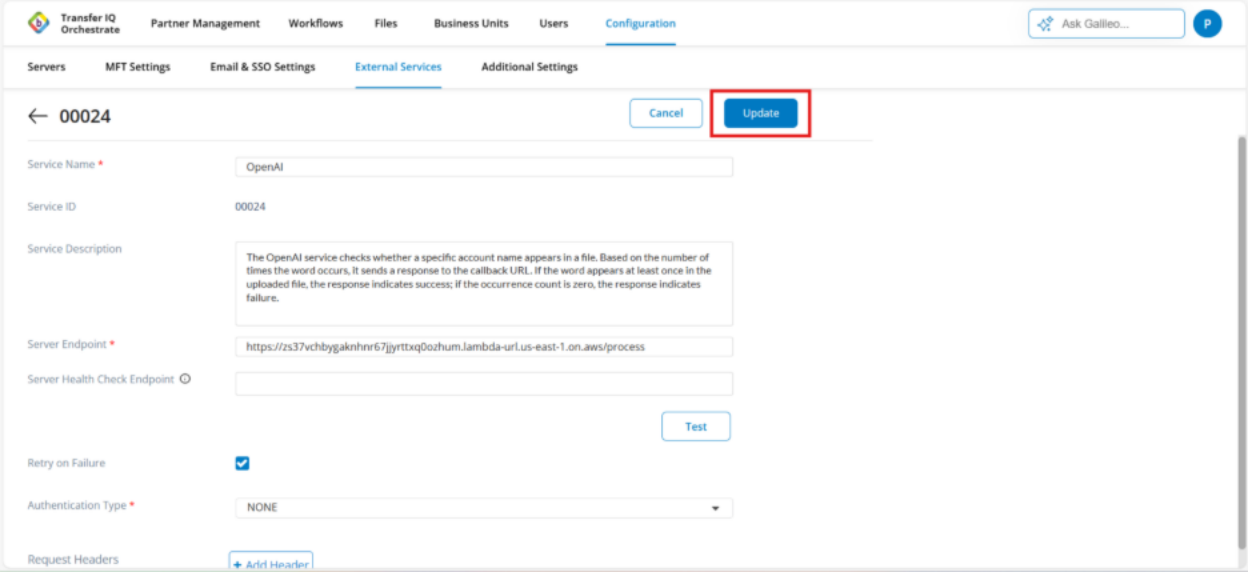
1. Navigate to **Configuration > External Services**.
2. Search for the required external service.
3. Click the external service name (displayed in blue), which opens the service details in view mode.



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



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

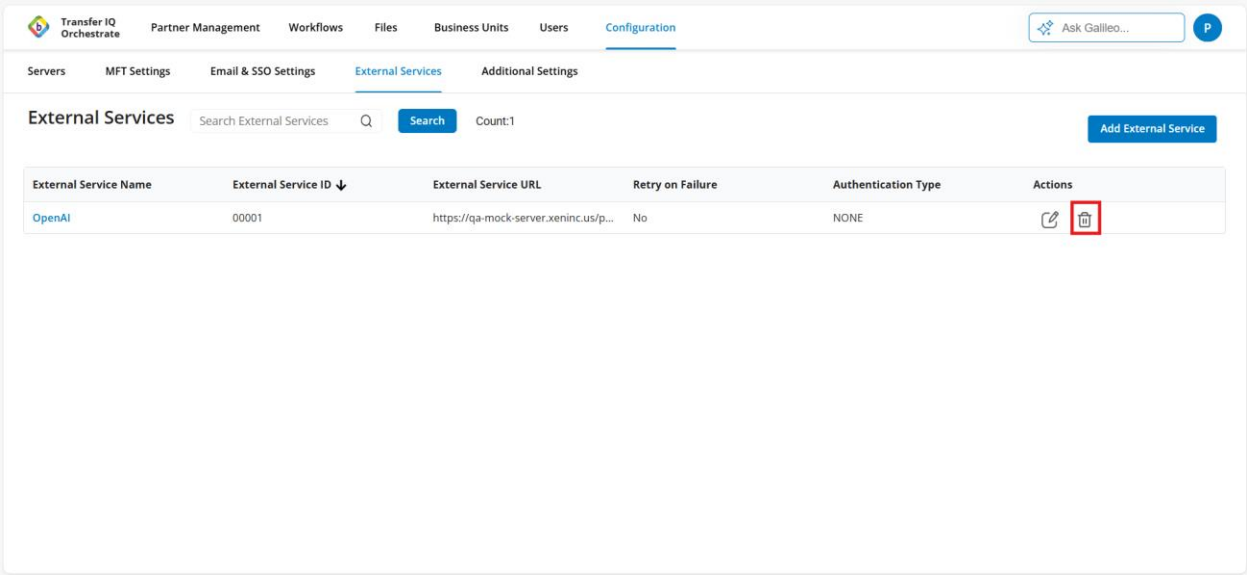


Note: The connection to an external service can be tested from the **Edit** screen, both in **view mode** and **edit mode**.

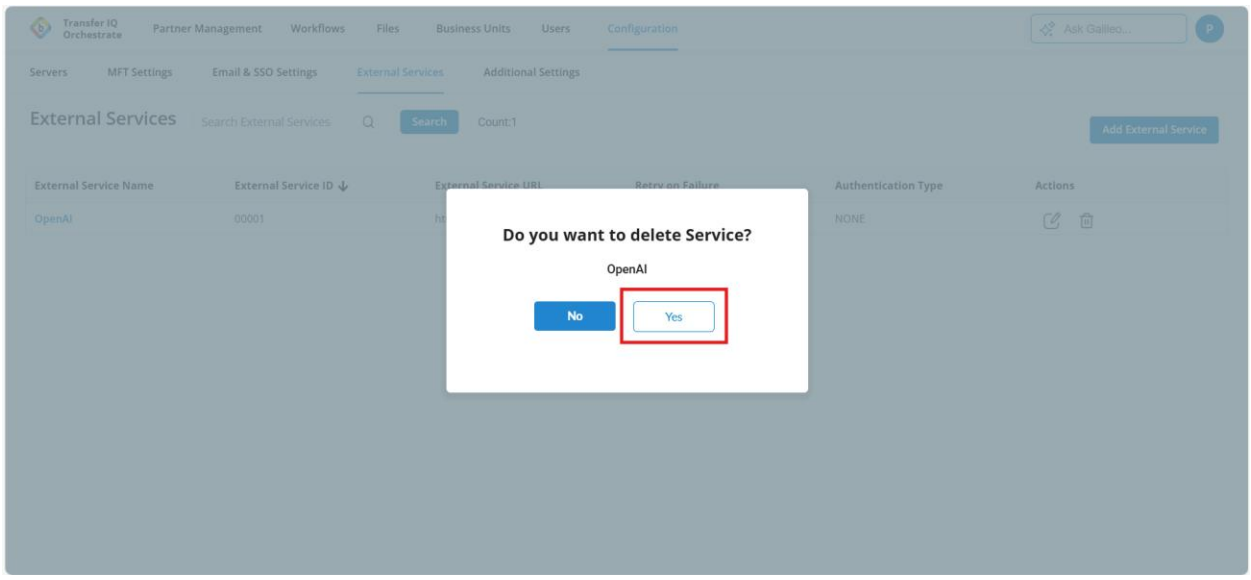
Delete External Service

To delete an external service, follow the below steps

1. Click the Delete Button



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

Backflipt Standard Support Model

- Backflipt's Standard Support model includes Phone and Email support.
- Email – Support@backflipt.com
- Phone – 408-890-2032
- Between 7 am PST to 5 pm PST