TransferIQ Orchestrate
User Guide

Table Of Contents

Introduction

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

Roles

Functionality	Super Admin	MFT Admin	Business User
System Configuration	Yes		
Email Templates	Yes	Yes	
Add Users	Yes	Yes	
Add Business Unit	Yes	Yes	
Add Partner			Yes
Add Account Onboarding Data			Yes
Submit Account Onboarding for Approval			Yes
Account Creation Approvals	Yes	Yes	
Add Workflows			Yes
Submit Workflows for Approval			Yes
Review and Workflow Approvals	Yes	Yes	

Actors

Actor	Name	Description
Company	AWS	The Enterprise represents your Organization, it includes the following: Internal Users and Systems Employees / Business Users from a Business Unit / Department within your company who initiate or receive file transfers. Core Infrastructure The internal SFTP servers using AWS Transfer Family SFTP Servers and Connectors.
Partner	Rackspace	The Partner represents external organizations or third-party entities that exchange files with the enterprise. These are usually customers, suppliers, or other business collaborators.

		Partner Users External stakeholders who connect to the enterprise MFT solution through secure protocols (e.g., SFTP). Partner Hosted SFTP Server Partners often have their own hosted SFTP servers or may directly connect to the enterprise's MFT-hosted SFTP server.

Accounts

Account	Name	Description
AWS Transfer Family Account	RackspaceAWSAccount	An AWS Transfer Family Account is a user account created within the AWS Transfer Family SFTP server. It is provisioned and shared with external partners to enable secure file transfers between the partner's systems and the enterprise's MFT environment. Authentication Methods Supported AWS Transfer Family SFTP servers support the following authentication methods for partner access: Username + SSH Key (Key-Based Authentication) Partners are authenticated using a public SSH key associated with their account. Offers enhanced security and supports automated, password-less file transfers.
Partner Hosted Account	RackspacePartnerPWD Account	A Partner Hosted Account is a user account created within the partner's SFTP server. It is shared with the

		enterprise to enable secure file transfers, allowing the enterprise to connect to the partner's environment for sending or receiving files. Authentication Methods for Partner SFTP Server Username + Password Traditional authentication using a secure username and password combination. Username + SSH Key Key-based authentication using a username and a registered SSH key for enhanced security and automation.

Workflows

Account Type	Direction	Description
AWS Transfer Family Account Workflows	Inbound	Inbound Workflow (Partner → Enterprise) Partner uploads files to the AWS Transfer Family SFTP server using their AWS Transfer Family Account. Files are stored in designated S3 folders (e.g., EFTS, PFTS) for internal processing. Enterprise workflows pick up the files and route them to downstream internal systems.

	Outbound	Outbound Workflow (Enterprise → Partner) The enterprise places files into designated S3 folders. AWS Transfer Family makes these files available to the partner through their AWS Transfer Family SFTP account. The partner downloads files securely using their AWS Transfer Family credentials.
Partner Hosted Account Workflows	Inbound / Pull	Inbound Workflow (Partner → Enterprise) Partner places files in their own SFTP server. Enterprise workflow connects to the partner's SFTP server using the Partner Hosted Account to pull files. Retrieved files are processed and stored internally within the enterprise's environment.
	Outbound / Push	Outbound Workflow (Enterprise → Partner) Enterprise workflow connects to the partner's SFTP server using the Partner Hosted Account. Files are securely pushed to the partner's environment for their use.

		Ensures reliable delivery with tracking and logging.

File Transformations

Step	Description
Scan	Scans files for malware/threats
Copy	Duplicates files from source to destination
Move	Transfers files from source to destination and removes them from the source
PGP Encryption	Encrypts file by encrypting them with a PGP public key
PGP Decryption	Decrypts file by decrypting them with a PGP private key
Encode	Converts files into a specific format (e.g., Base64)
Decode	Converts encoded files back to their original format
Compress	Reduces file size using compression algorithms
Decompress	Restores compressed files to their original form
Tag	Adds labels or metadata to files for identification
Rename	Changes the name of files with the given name
Delete	Removes files from the source.

Sign Up First Time Super Admin

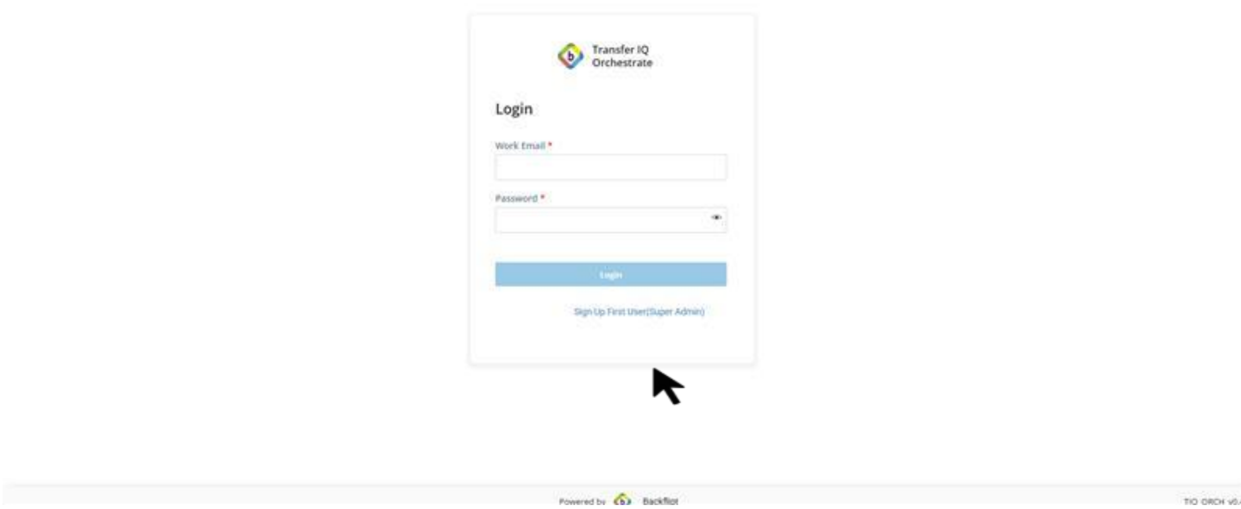
When the **Transfer IQ Orchestrate Application** is launched for the first time, the application does not contain any registered users. Since access to the application is restricted, it is necessary to add the **first user to start using the application**

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.

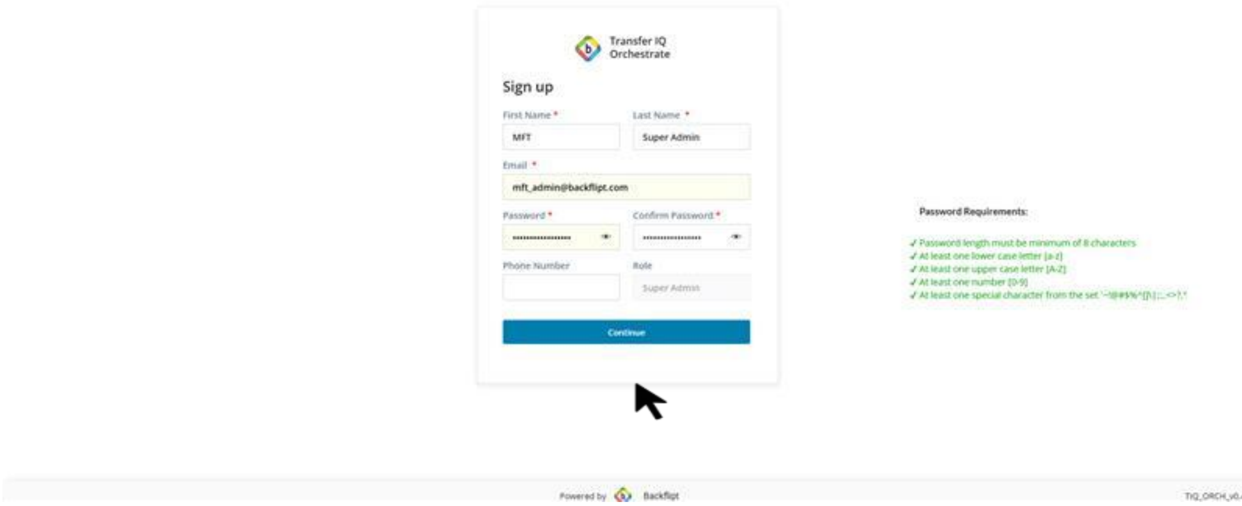
This Super Admin account acts as the foundational user, enabling full access and control of the application

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**

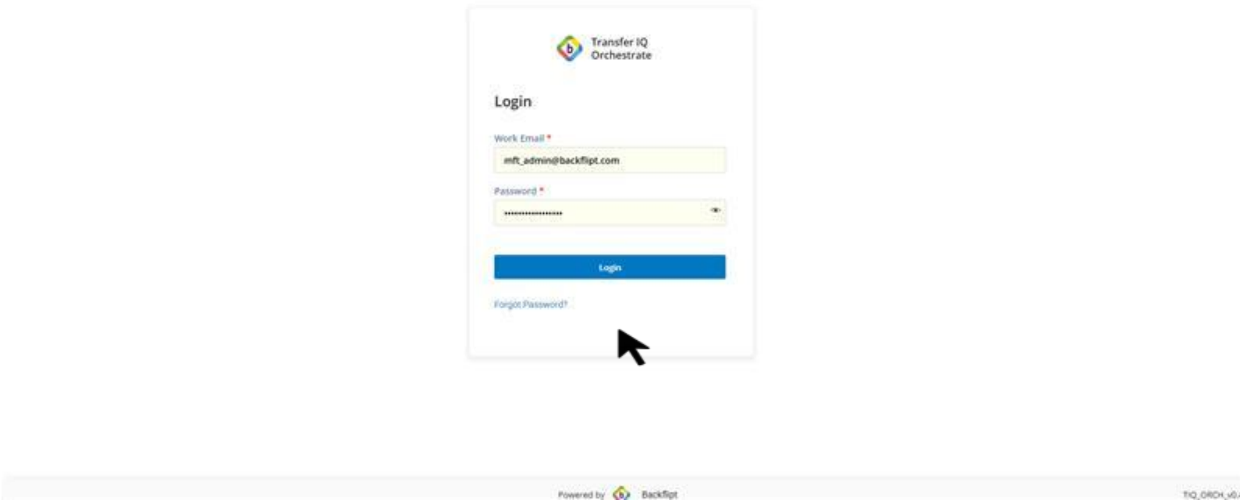


2. Once the button is clicked a signup form will be displayed with the following fields
   a. **First Name** – The first name of the Super Admin.
   b. **Last Name** – The last name of the Super Admin.
   c. **Email Address** – A valid email to be used for login and communication.
   d. **Password** – A secure password for account access.
   e. **Confirm Password** – Re-enter the password to confirm accuracy.
   f. **Phone Number** – A valid phone number for verification or support.
3. Click the **Continue** button to complete the registration process

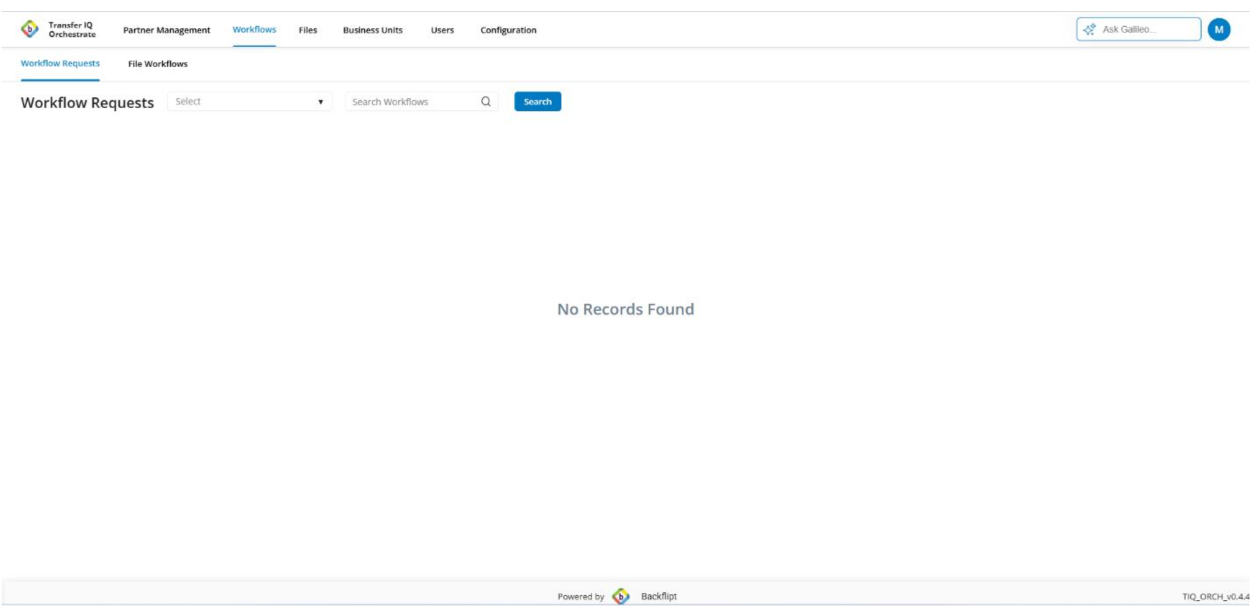


4. After the Super Admin is successfully registered, the application redirects to the following page after clicking on “Please Click Here to Login!” user will be redirected to the **Login page**.

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



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



Configuration

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

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

- SFTP Servers
- MFT Settings
- Email and SSO Settings
- Additional Settings

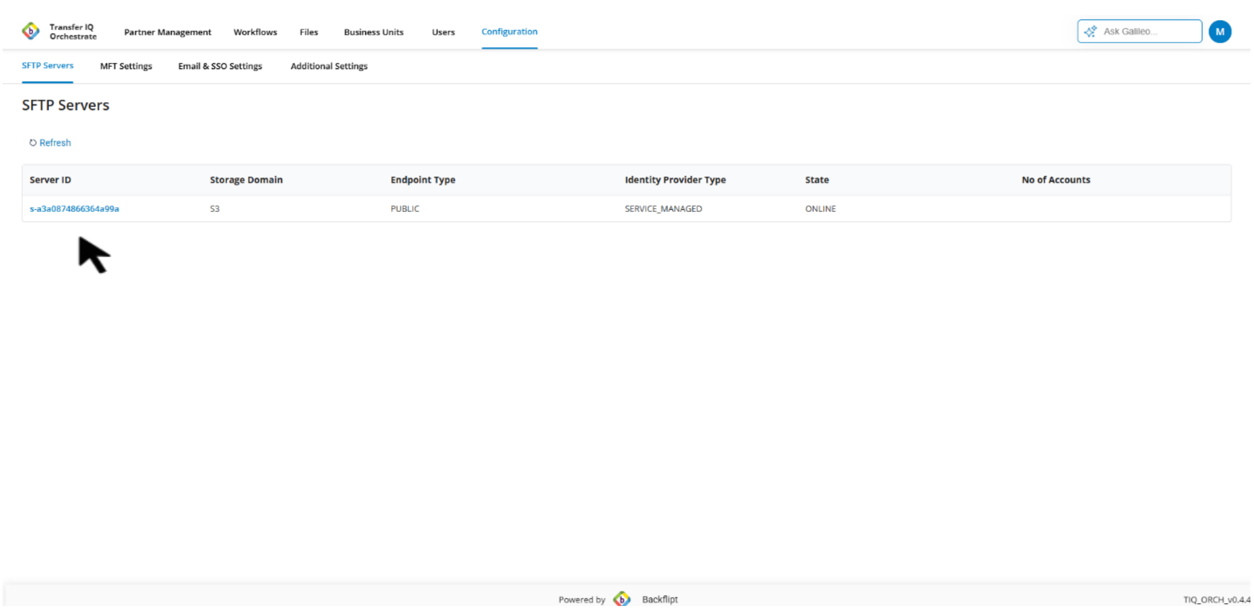
SFTP Servers

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

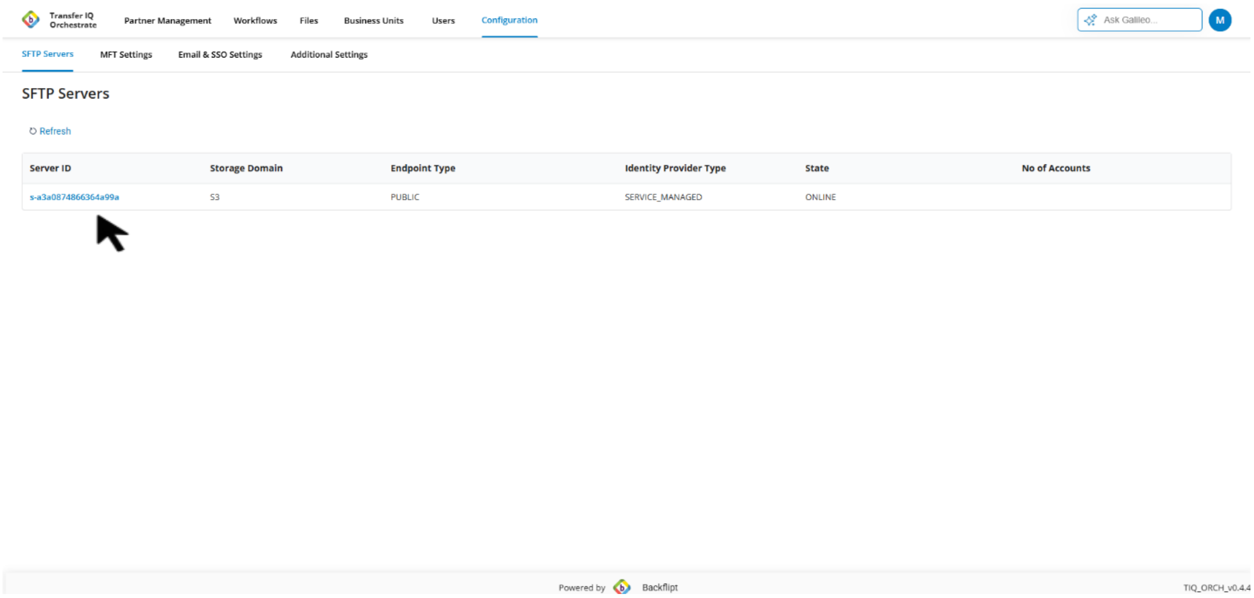
The **SFTP Servers** section displays a list of available SFTP servers configured for the company. Each server entry provides the following details:

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

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

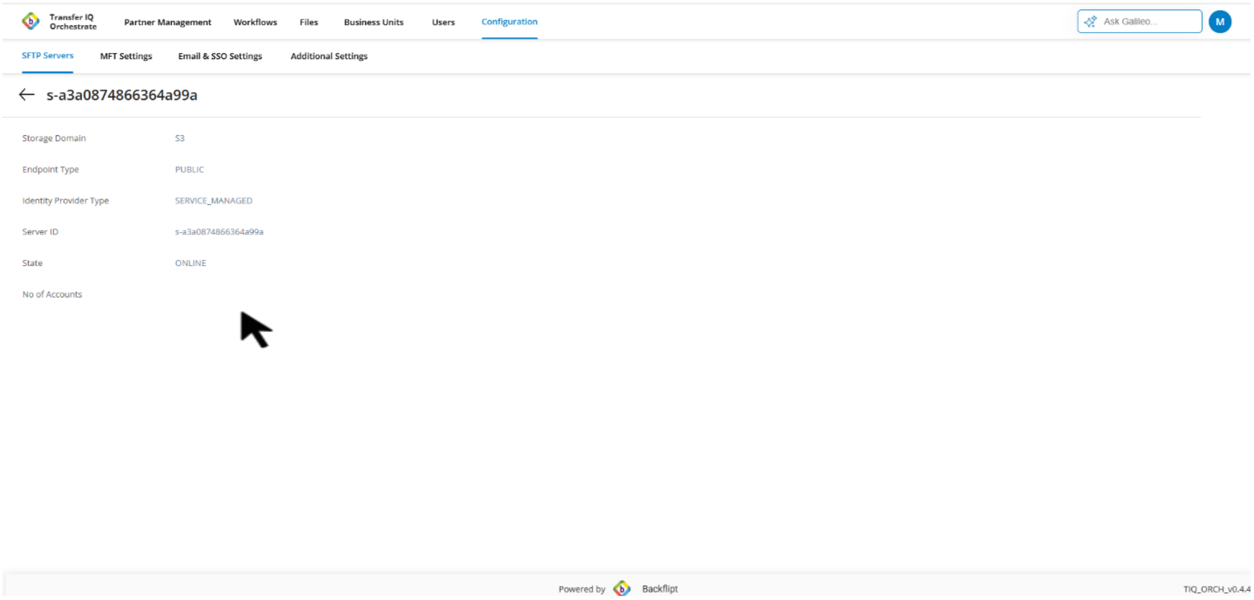


The user can also click on the server, which navigates to the server page.



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

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



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

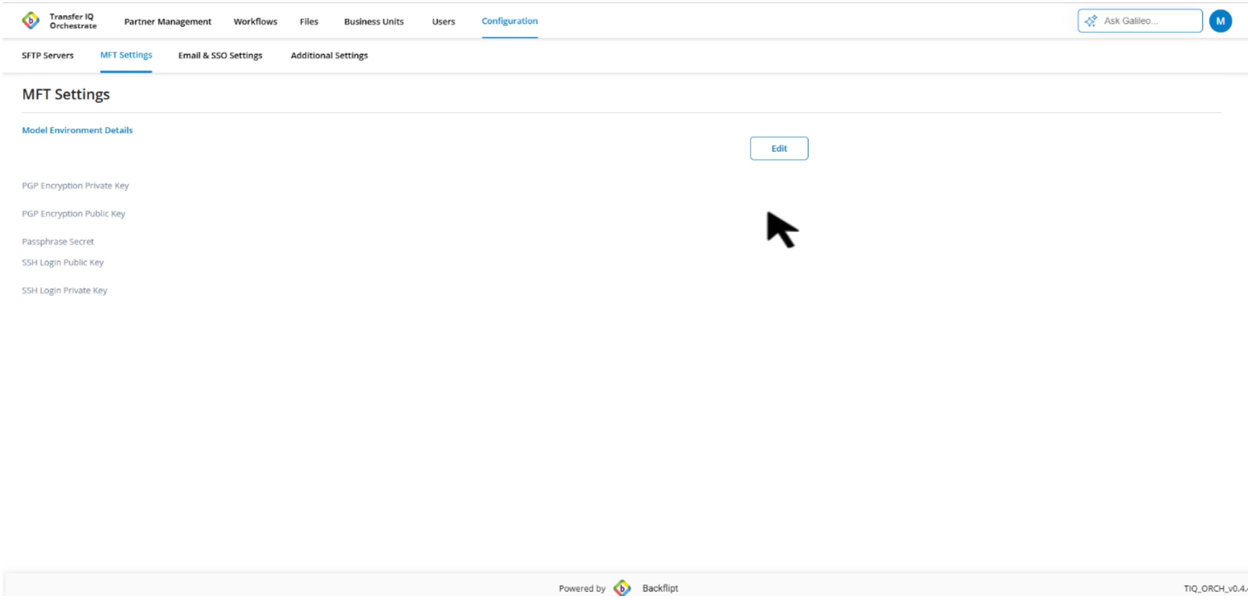
MFT Settings

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

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

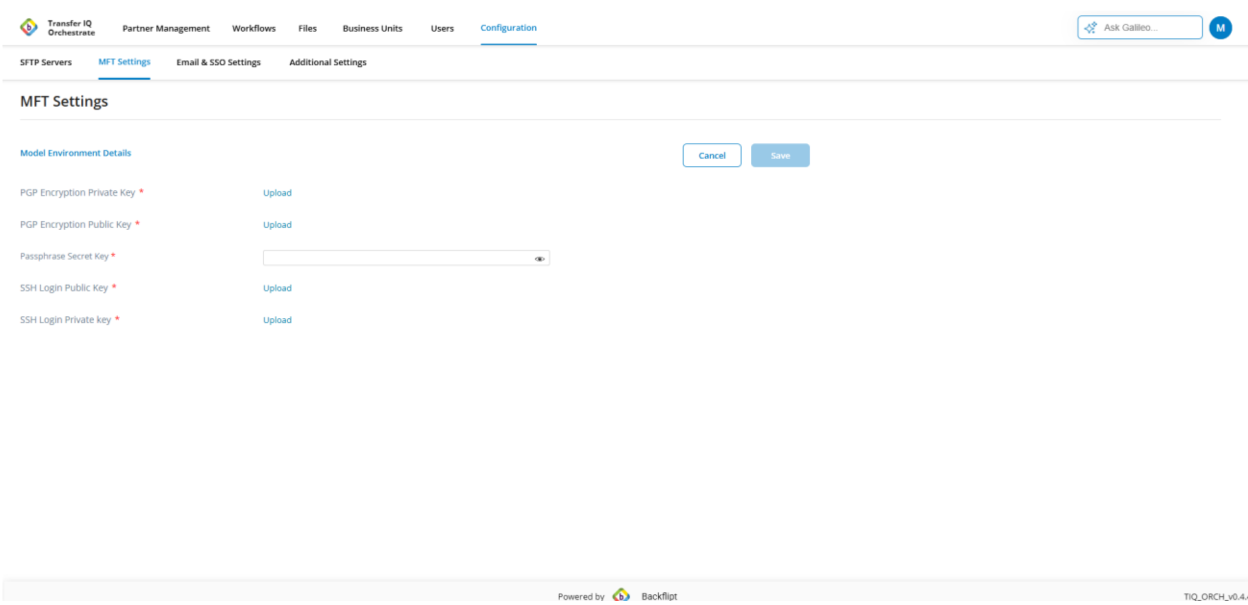
It includes the following fields:

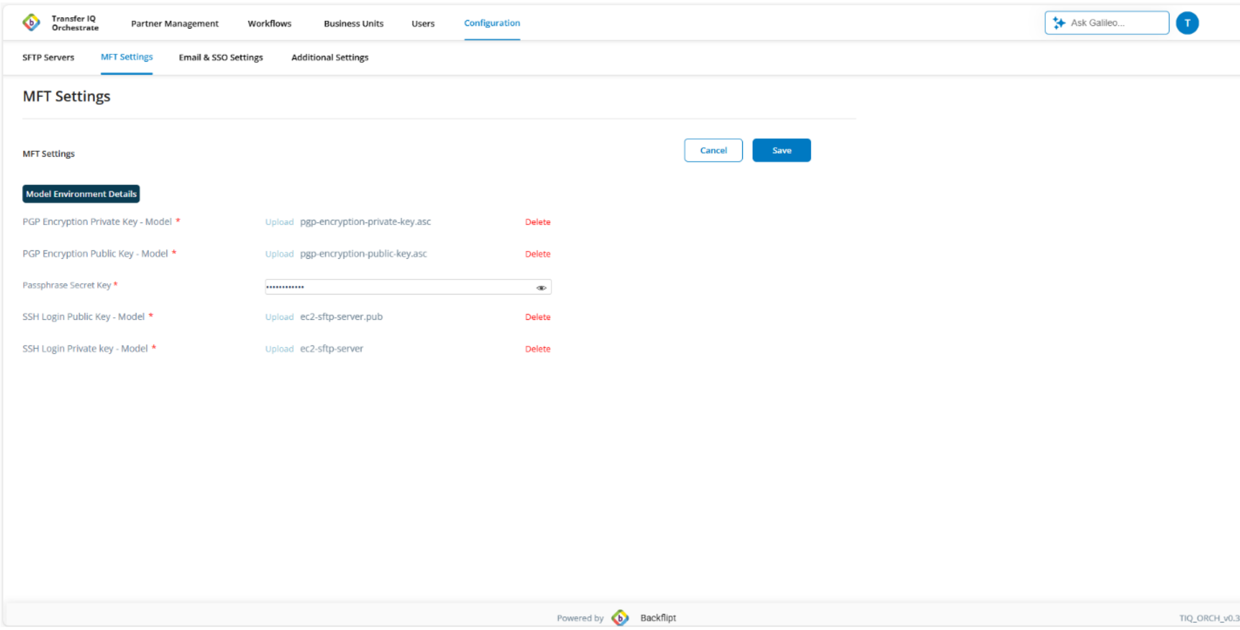
- PGP Encryption Private Key
- PGP Encryption Public Key
- Passphrase Secret Key
- SSH Login Public Key
- SSH Login Private Key



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

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





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

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

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

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

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

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

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

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

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

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

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

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

Email and SSO Settings

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

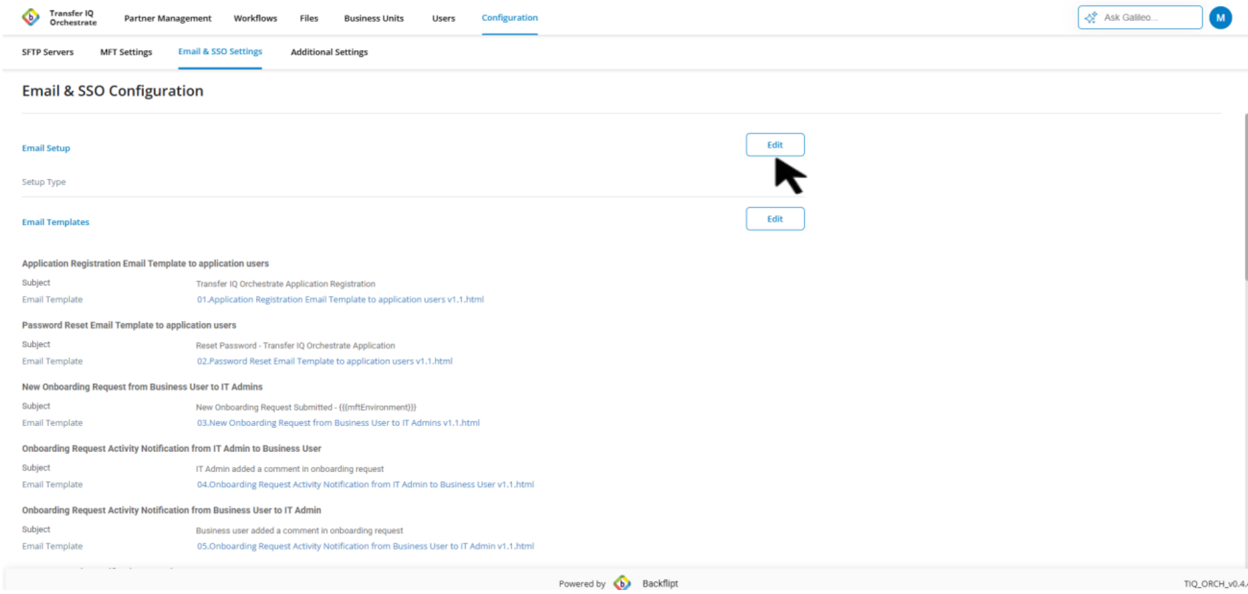
Email and SSO Settings consists of three sub sections

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

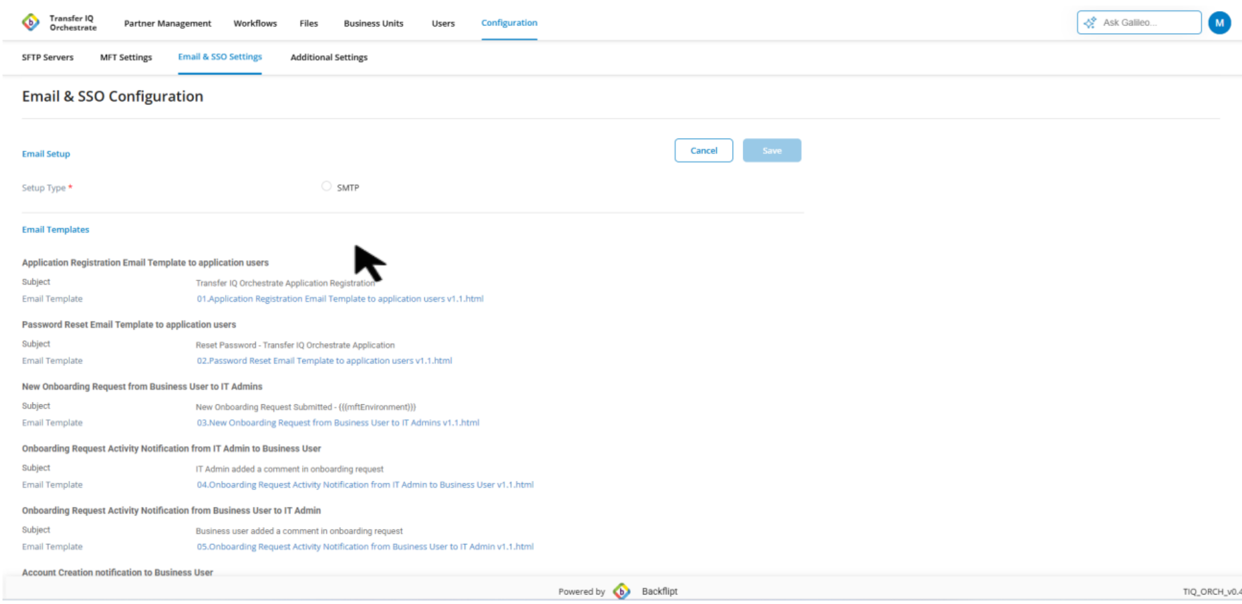
Email Setup

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

Click the Edit button to edit the email setup



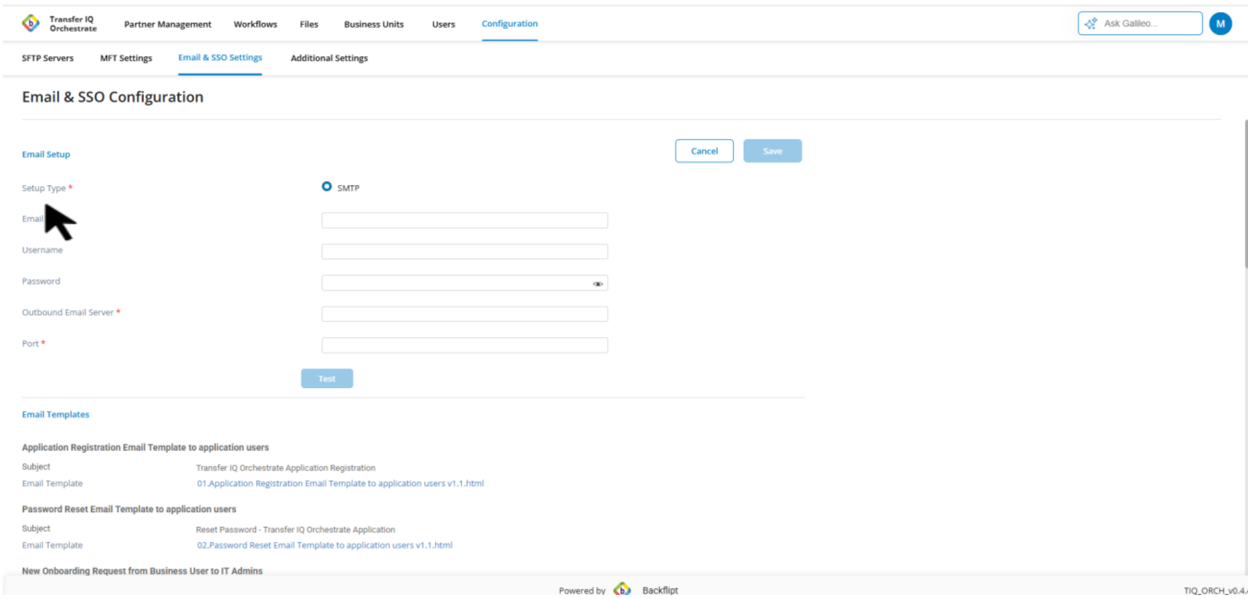
The application supports SMTP (Simple Mail Transfer Protocol) for sending emails, which requires specifying the appropriate email server and credentials.

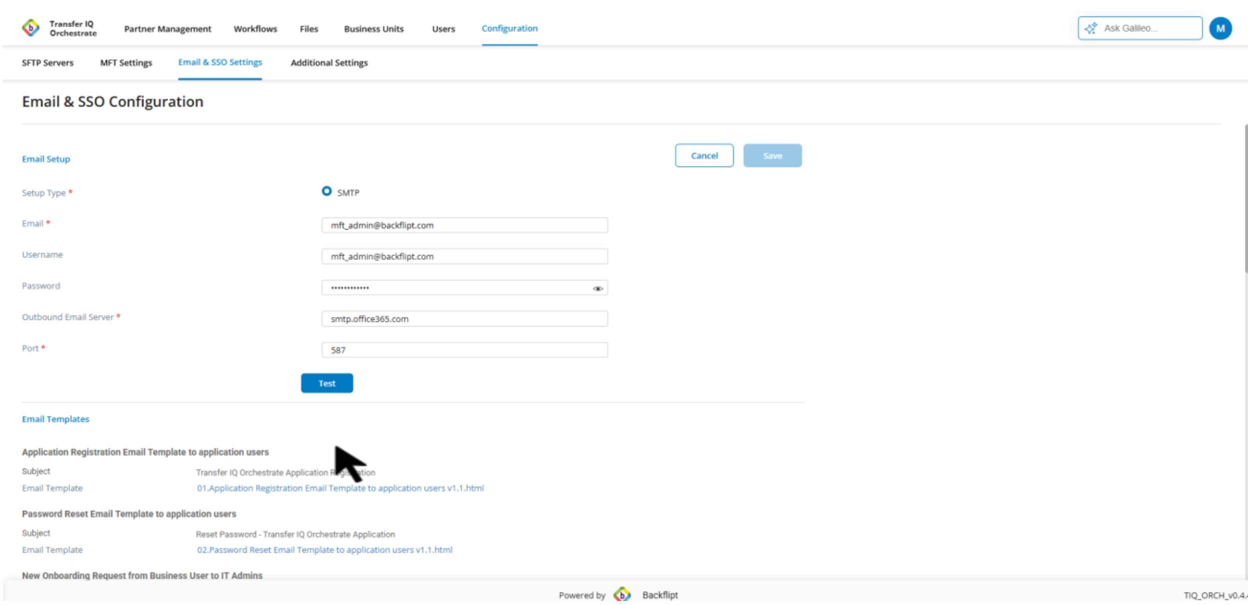


This section contains the below fields

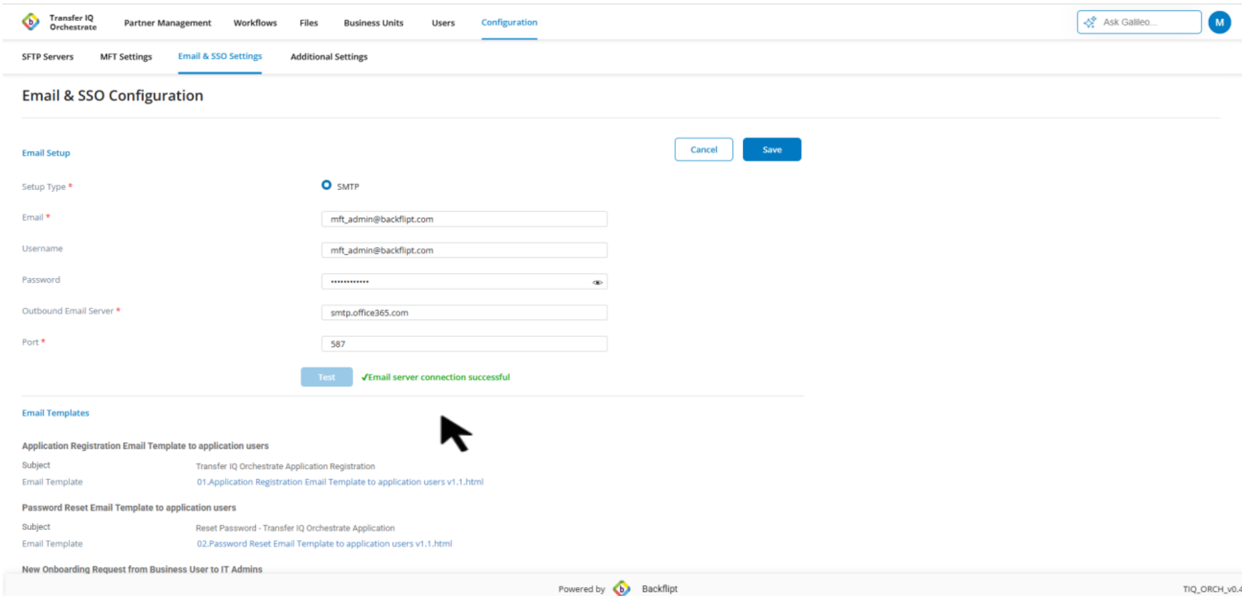
1. **Setup Type -** Specifies the method used to send emails. Transfer IQ Orchestrate application supports **SMTP**, which is a standard protocol for sending email messages between servers.
2. **Email -** The email address that will appear as the sender of system-generated emails.
3. **Username-** The 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)

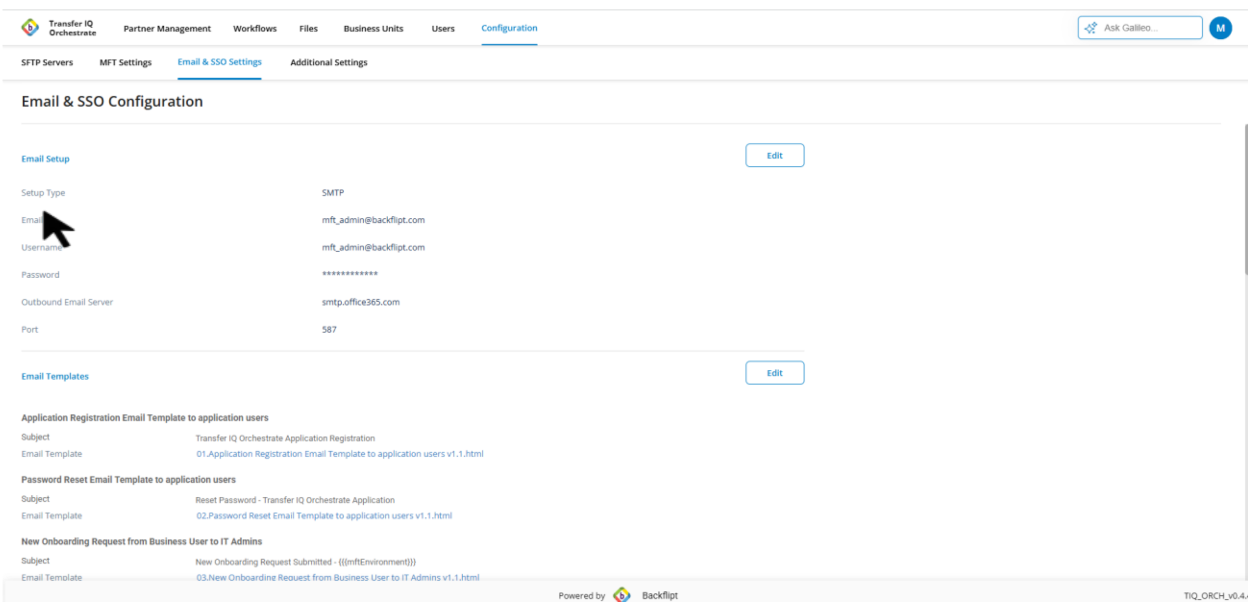




Once the Super Admin has entered all the SMTP details, Super Admin click the **"Test"** button to verify the connection. If the connection is successful, a confirmation message will be displayed indicating that the email server has been successfully connected.



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

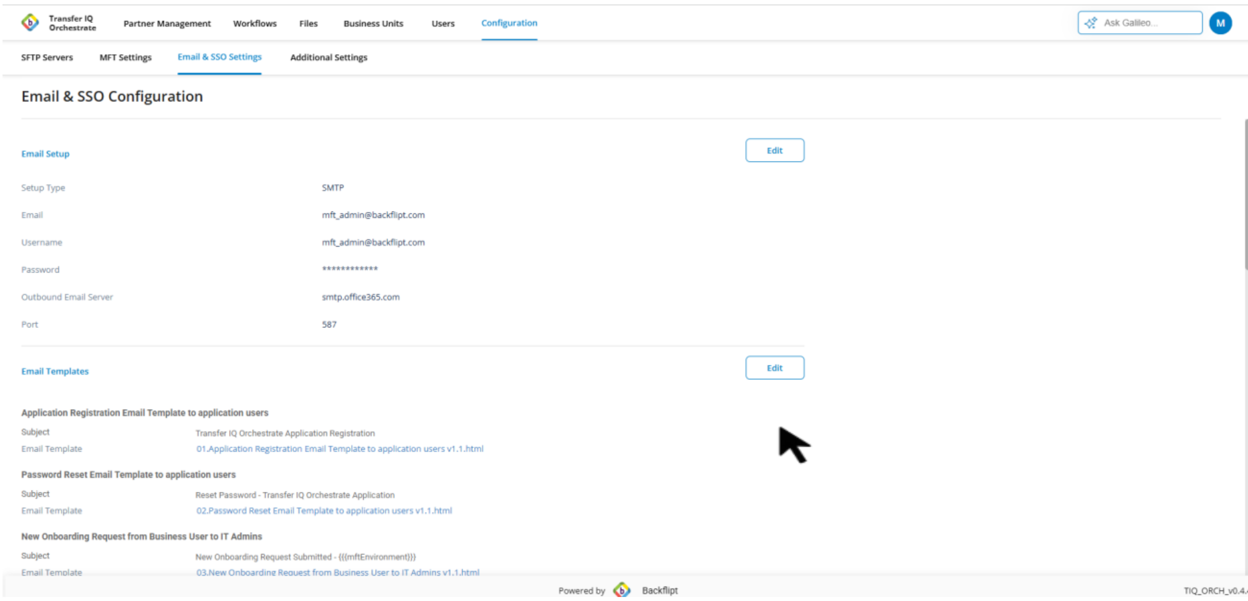


Email Templates

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.

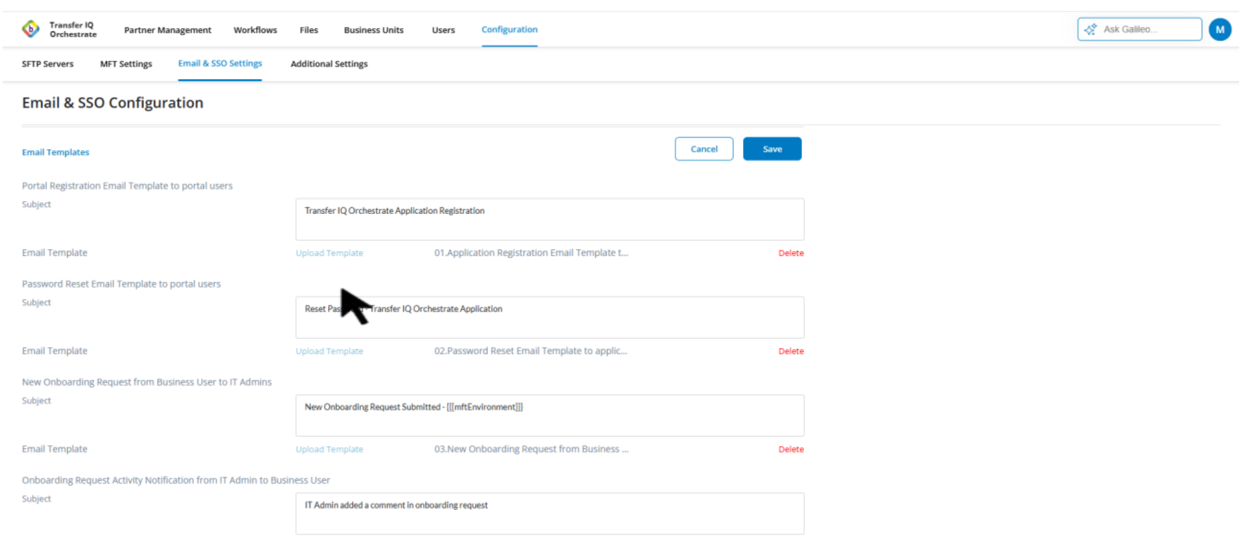
Click the edit button to make changes to the existing templates

=

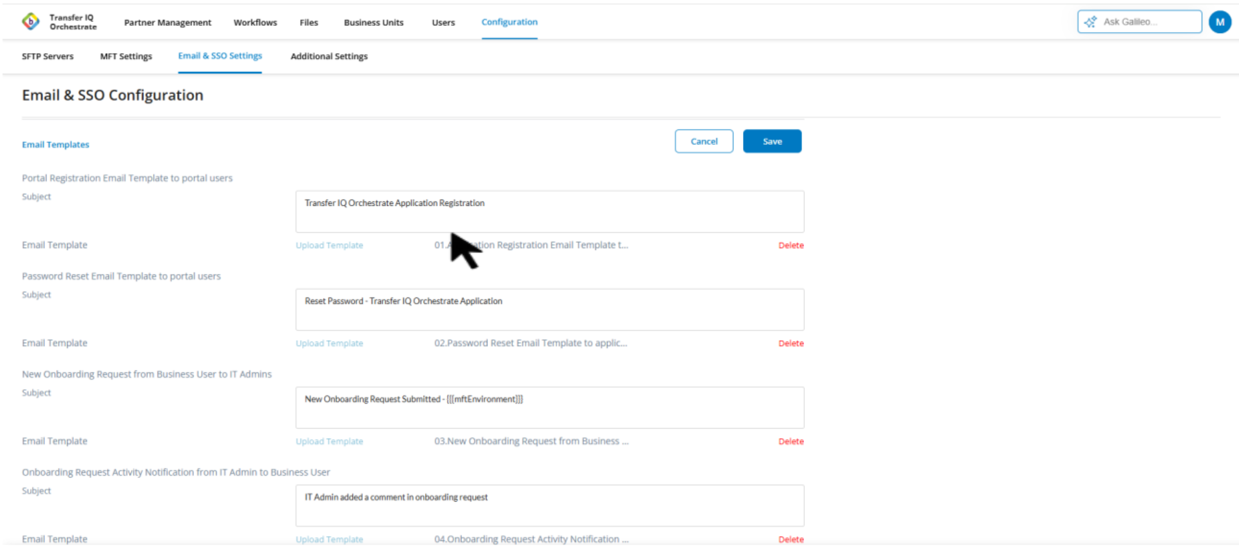


Each email template includes the following elements:

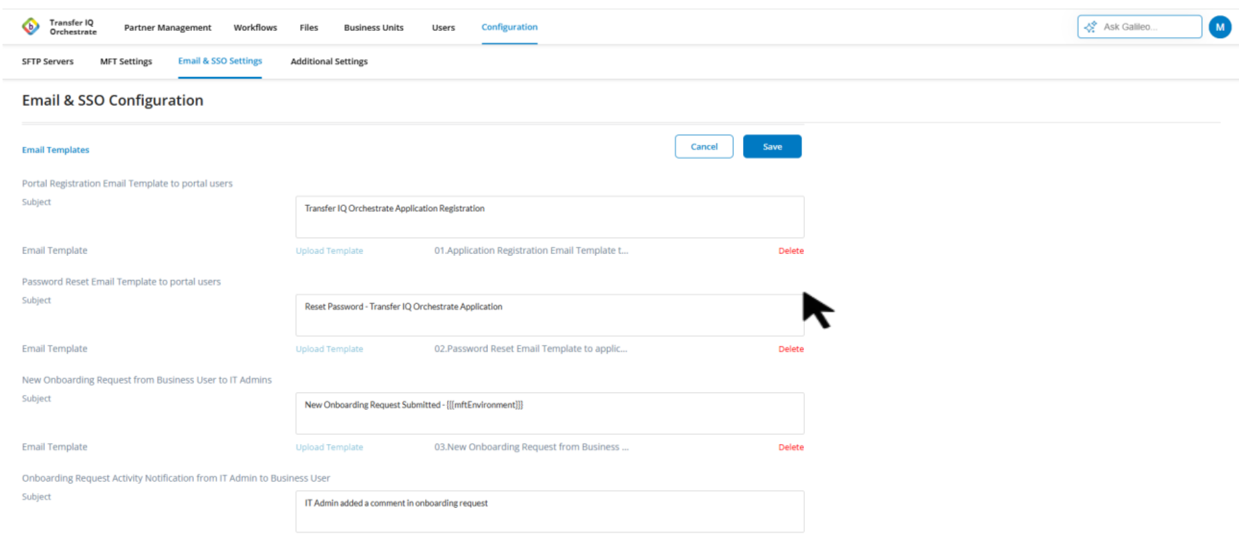
1. **Upload Button -** Allows the Super Admin to upload a custom email template file, replacing the default content if desired.



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.

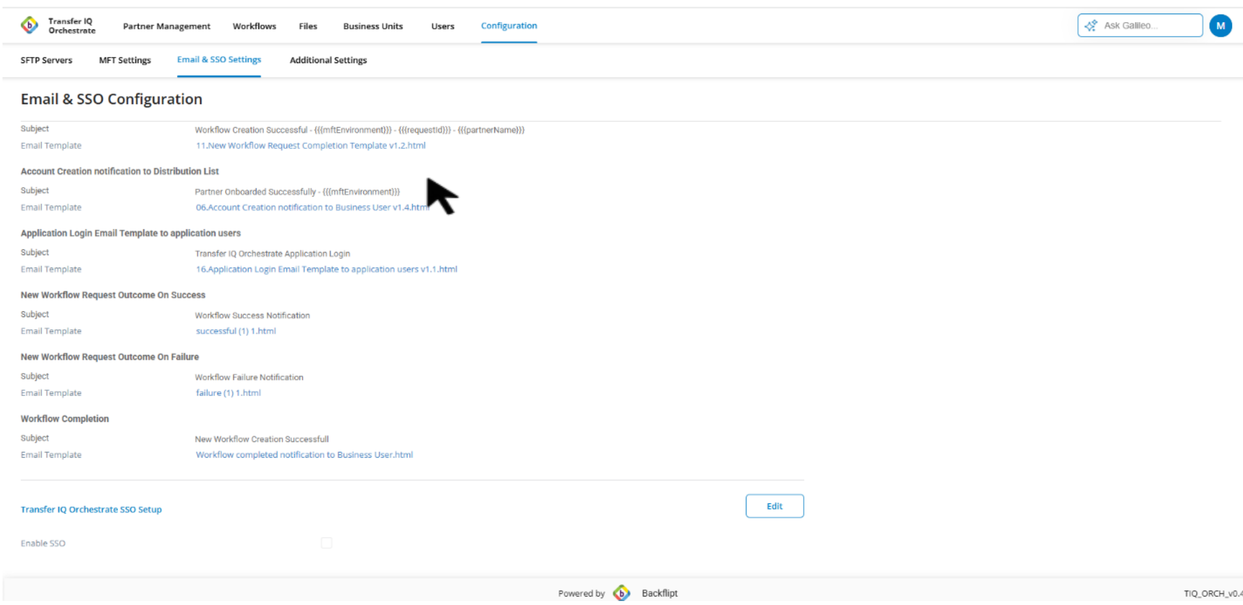


The Email Templates section contains the following templates

- Application Registration Email Template to application users
- Password Reset Email Template to application users
- New Onboarding Request from Business User to IT Admins
- Onboarding Request Activity Notification from Business User to IT Admin
- Onboarding Request Activity Notification from IT Admin to Business User
- Account Creation notification to Business User
- Onboarding completed notification to Business User
- New Workflow Request Notification to IT Admins

- Workflow Request Activity Notification from IT Admin to Business User
- Workflow Request Activity Notification from Business User to IT 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

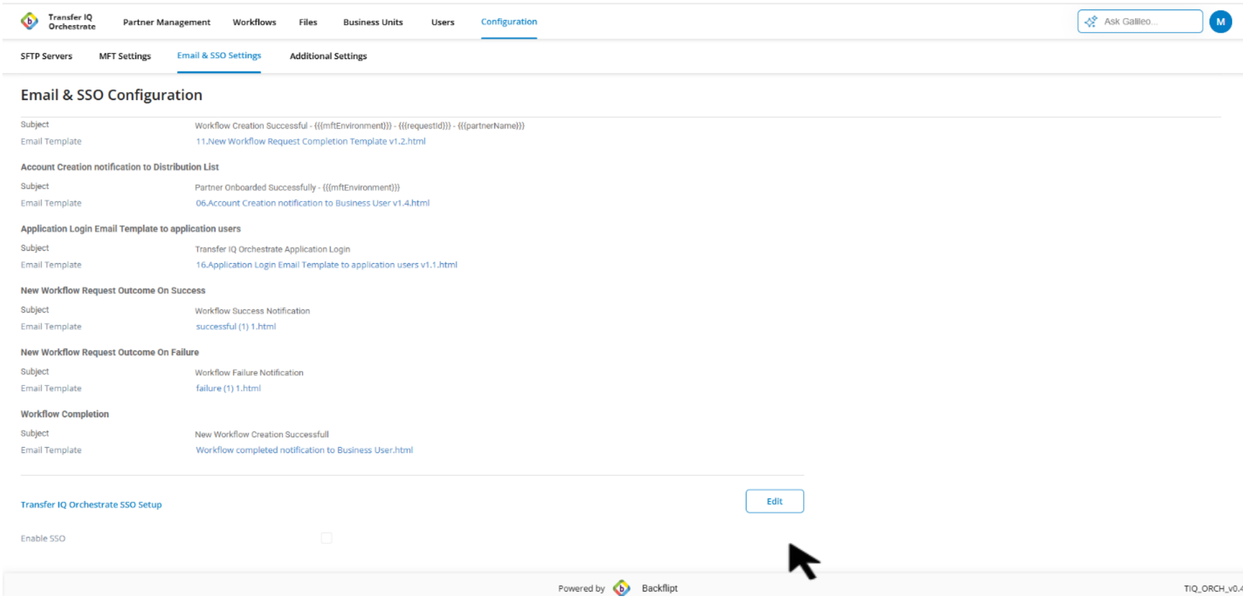


Transfer IQ Orchestrate SSO Setup

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



The SSO Section when enabled consists of the below fields

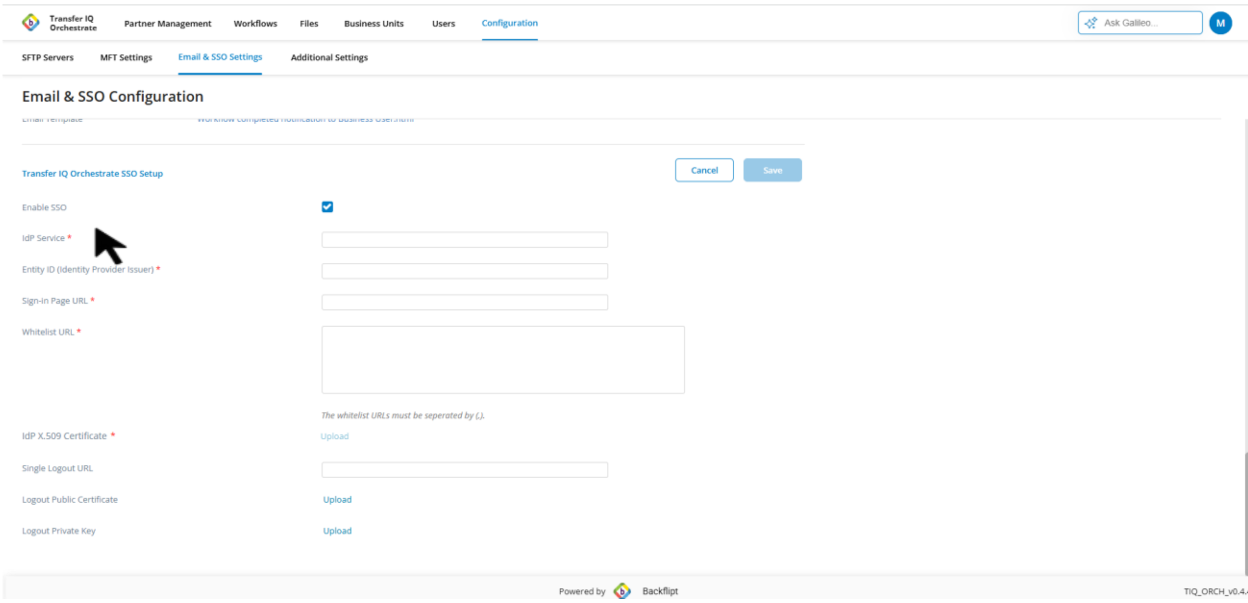
SSO Configuration Fields – Mandatory and Required Fields

- **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** - The 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

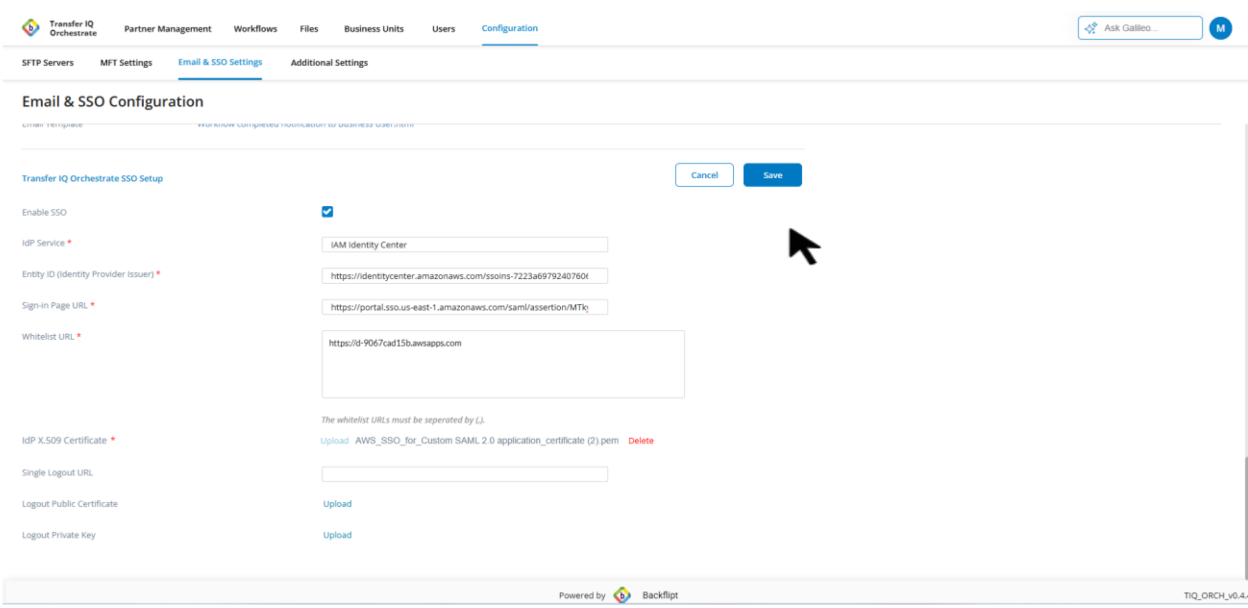
SSO Logout Configuration (Optional)

- **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.

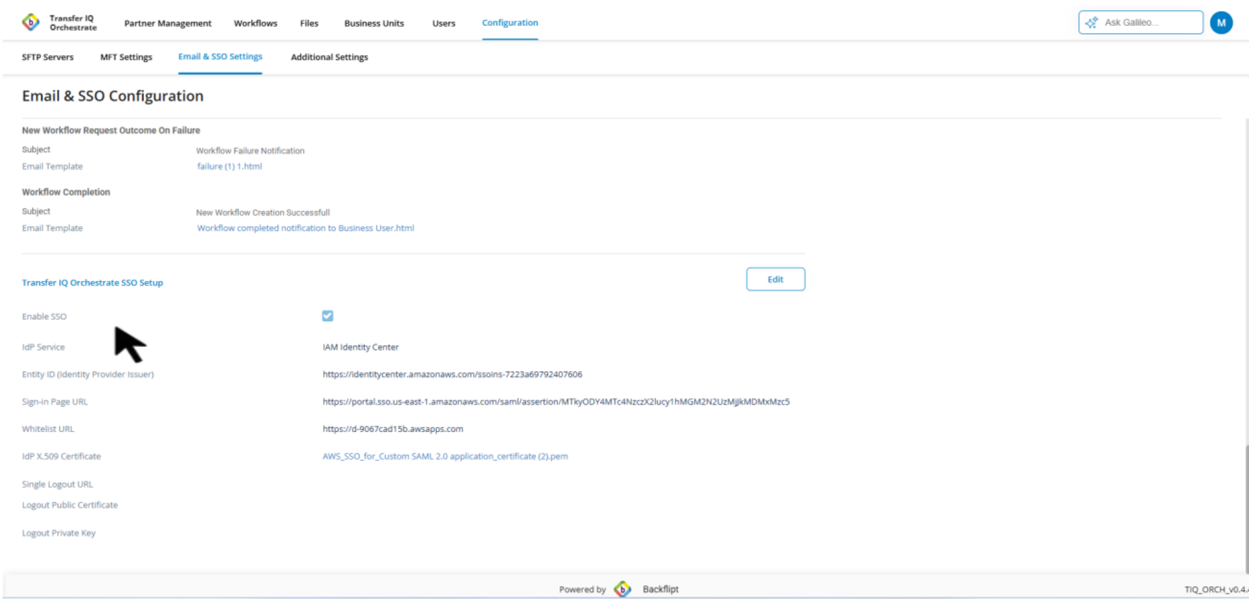
- **Logout Private Key -** A private key used by the application to sign logout requests sent to the Identity Provider. Uploading this key enhances security during the logout process.



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



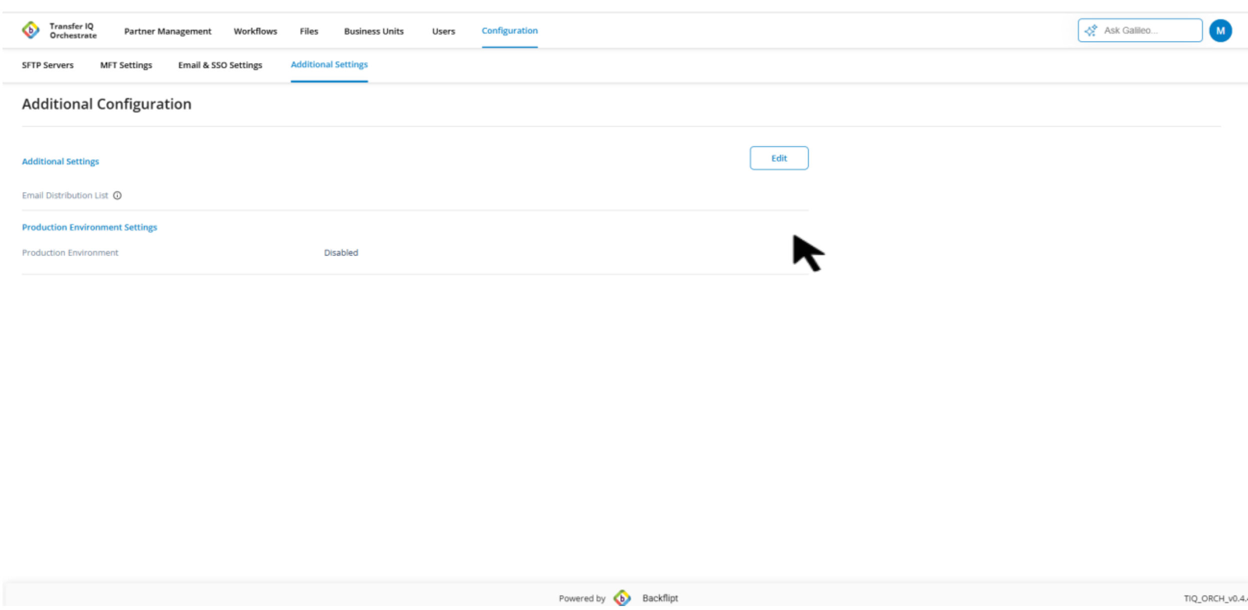
Once saved, the details will appear in view mode within the Transfer IQ Orchestrate SSO Setup section



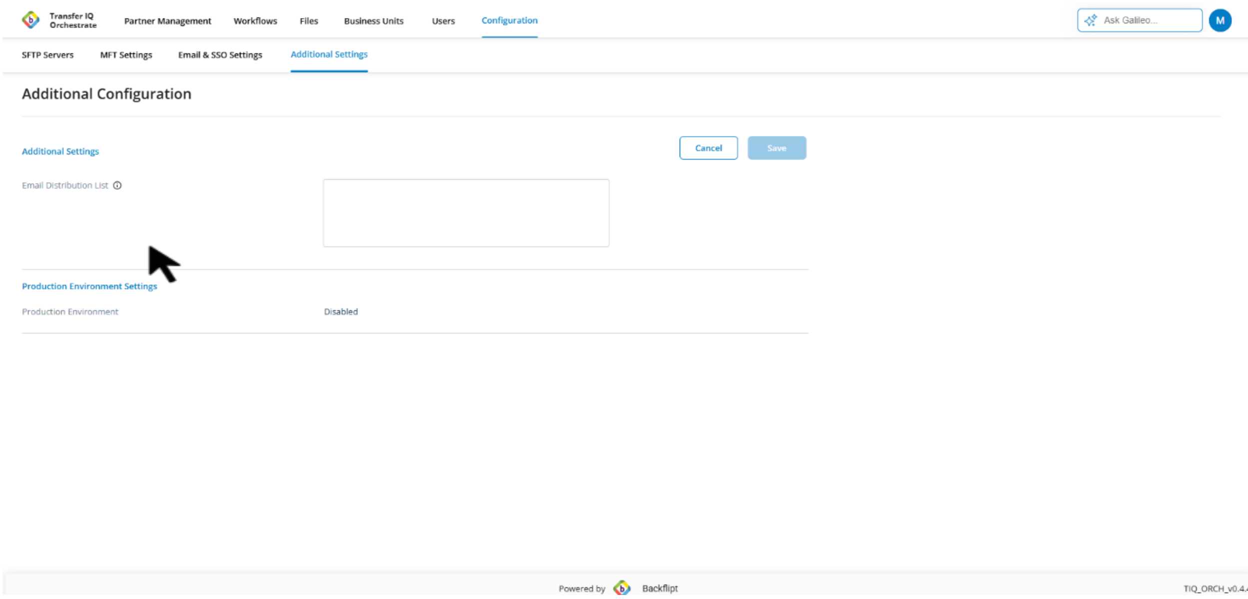
Additional Settings

The **Additional Settings** section allows the super admin to configure global settings for the application. It includes the following options:

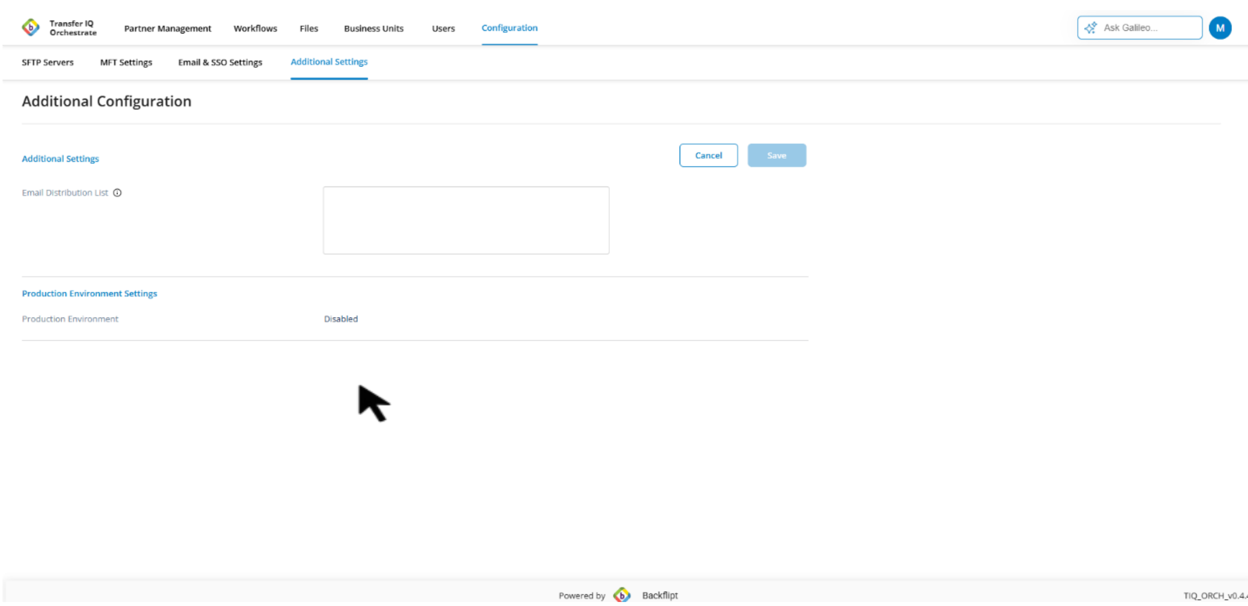
- **Email Distribution List:**
  This field allows the super admin to configure a list of email addresses that will receive system notifications and alerts.



- The user can click **Edit** to add, remove, or update email addresses in this list.



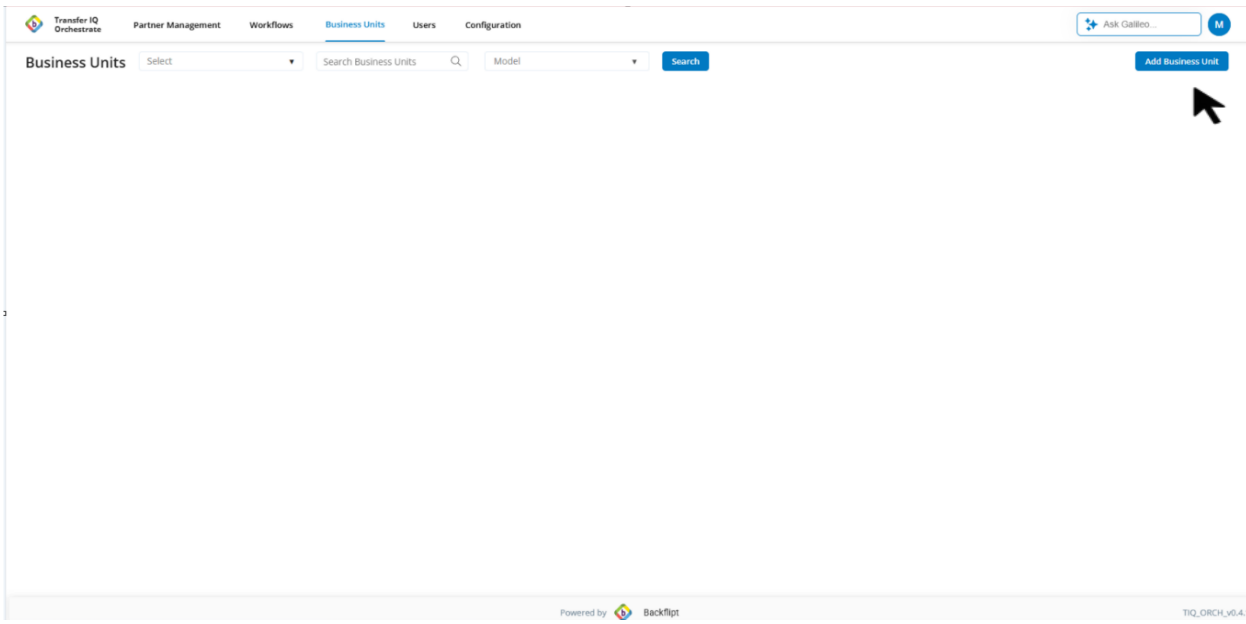
- **Production Environment Settings:**
  Displays the status of the production environment (e.g., **Disabled**). This section is read-only and cannot be modified from this screen.



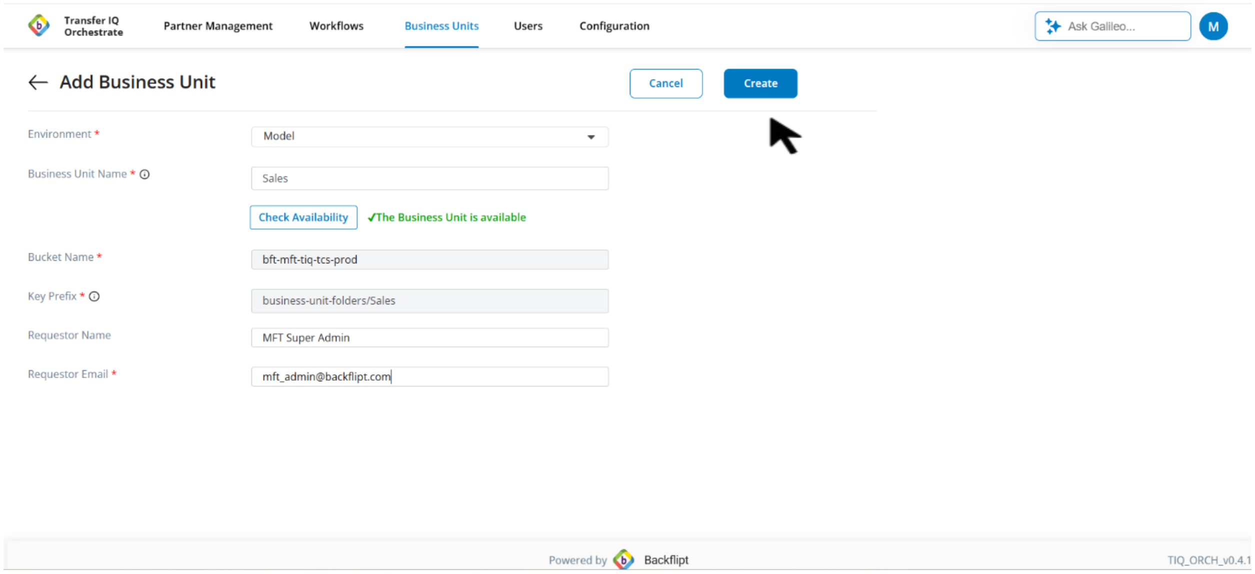
Admin adds a Business Unit:

Click the Business Unit tab to view a table displaying the following columns**: Business Unit, Key Prefix, Status, Created By.**

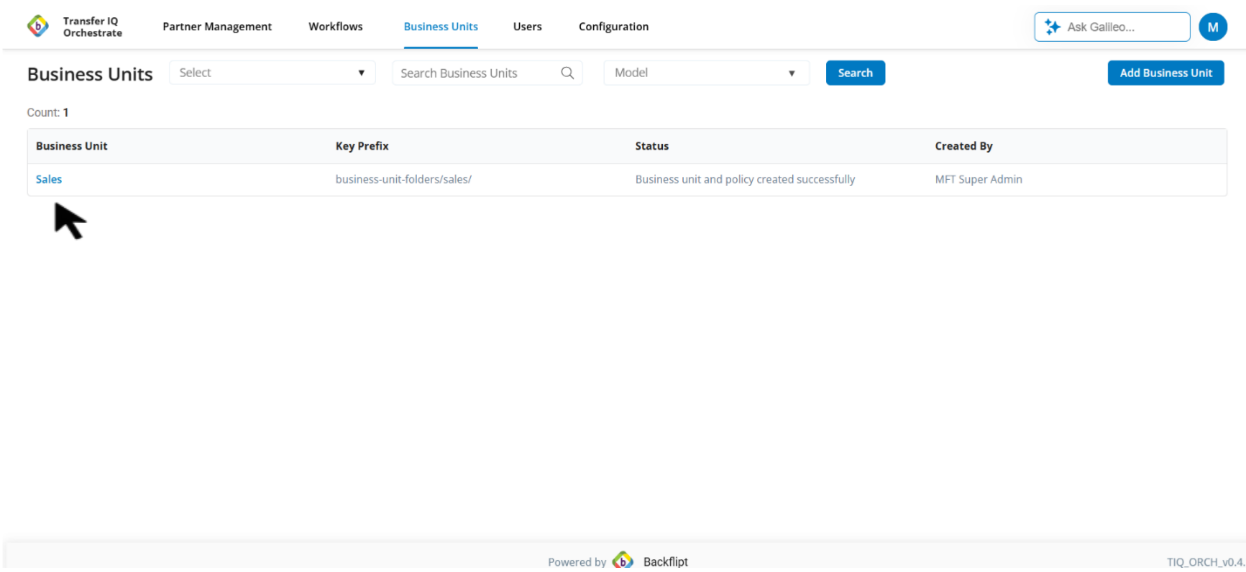
1. Click the **"Add Business Unit"** button. A window will appear with fields to enter the Environment, Business Unit Name, Requestor Name, Requestor Email.



2. The following fields **Bucket Name, Key Prefix** will be auto populated with the respective bucket name.
3. Once all the required details are given, click on the "Create" button.



4. The newly created business unit will be shown now in the Business unit tab table view.

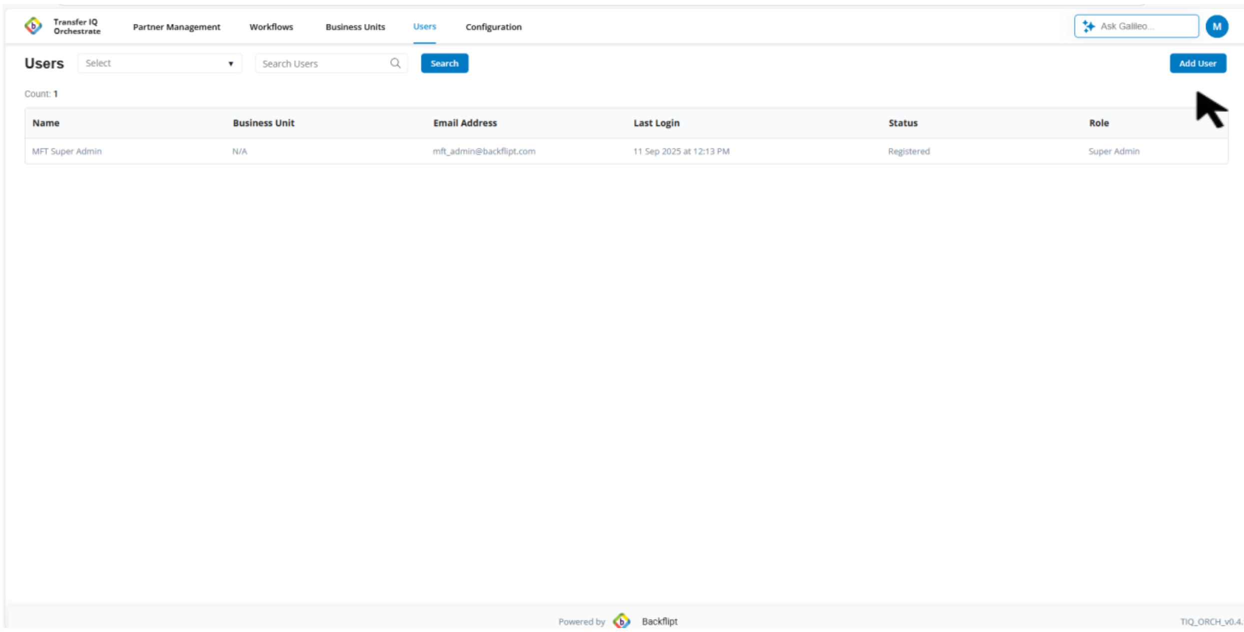


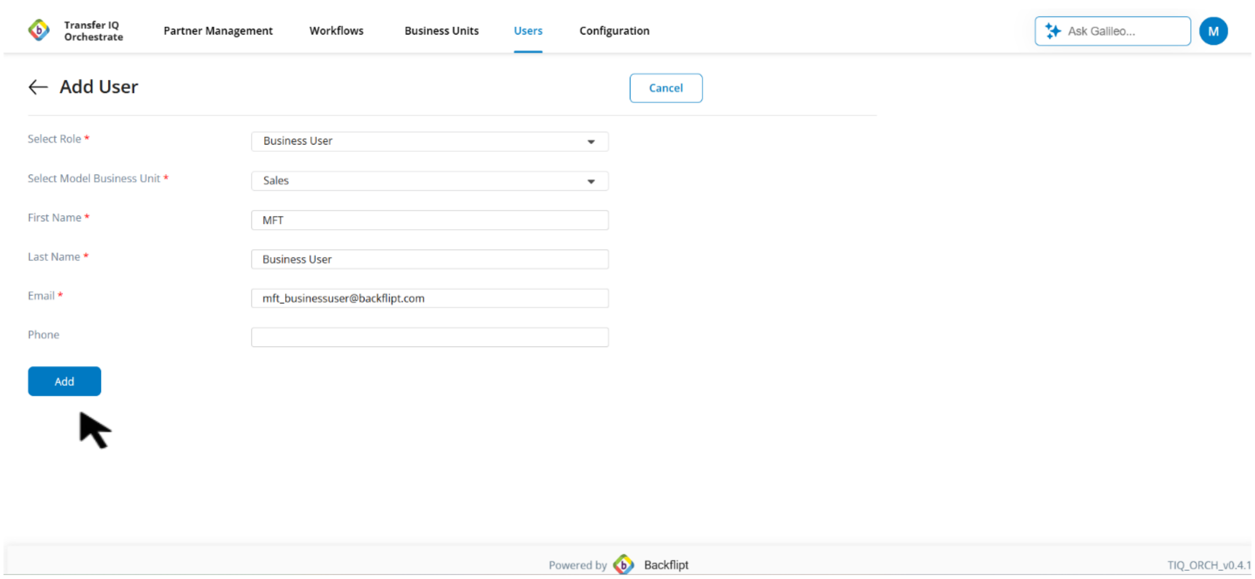
Admin Onboards a Business User:

When adding a Business User, a Business Unit must be selected for that user. Business Units are not associated with Super Admin or IT Admin roles.

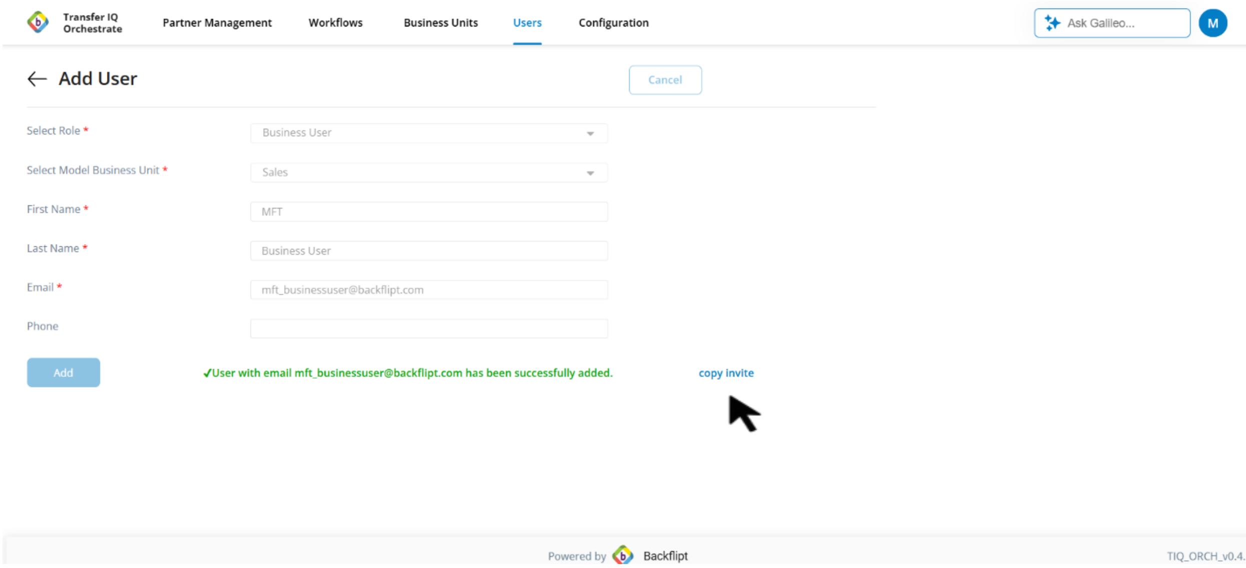
1. Click the Users tab to view a table displaying the following columns**: Name, Business Unit, Email, Last Login, Status, Role**

2. To add a new Business User, click the "**Add User**" button. A window will appear with fields to enter the user's role, first name, last name, phone number, Business Unit, and email address. After completing the form, click "Add" to save the new user.

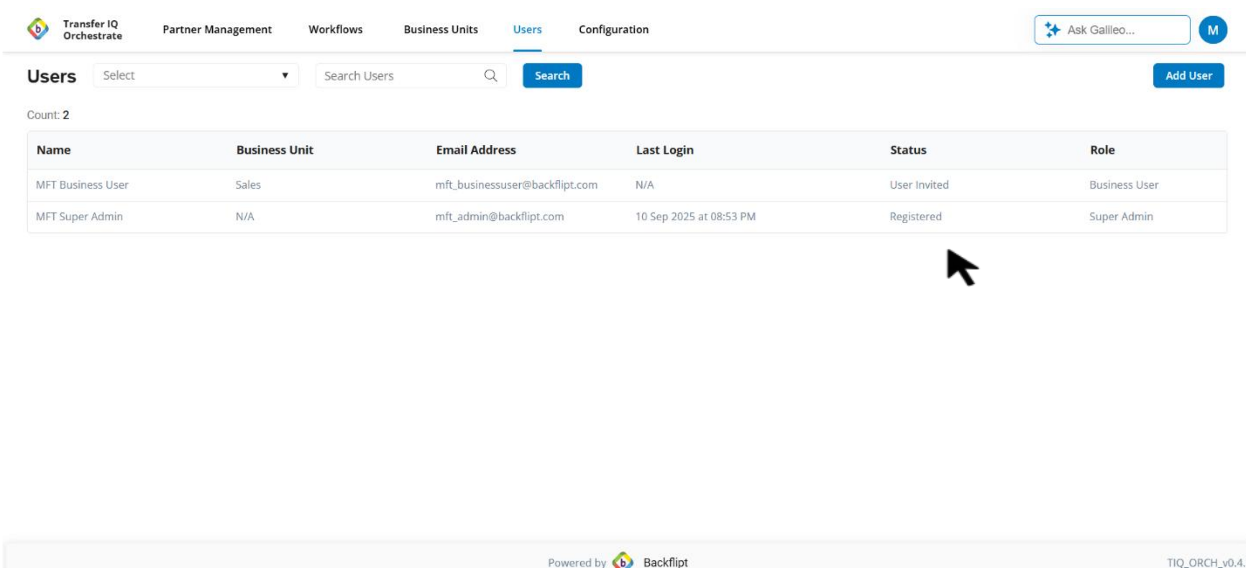




3. An invitation will be sent to the user to register for the application.

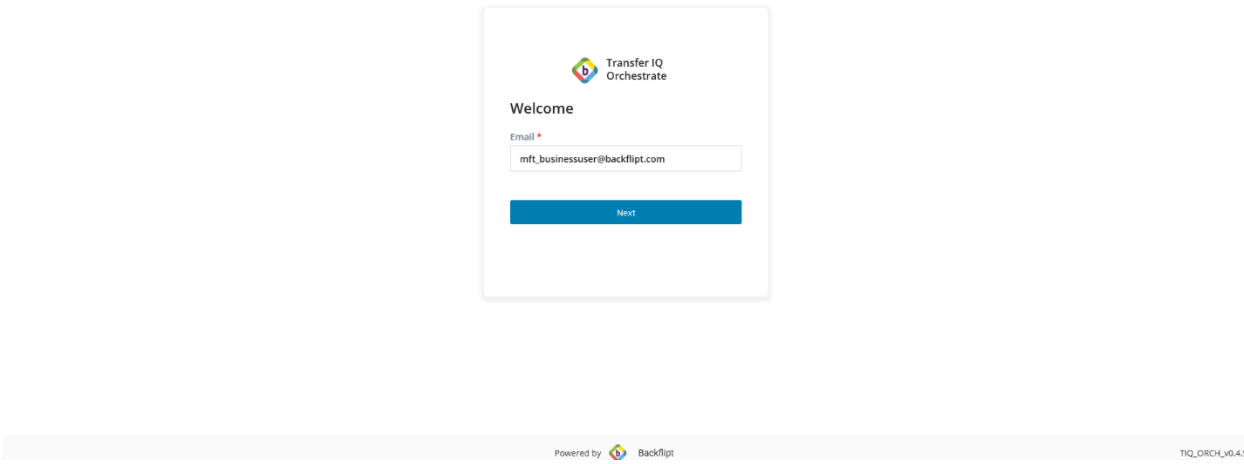


4. Added users appear in the Users tab. Users who have been invited but not yet registered will have the status "**User Invited**," while users who have completed their registration will have the status "**Registered**".

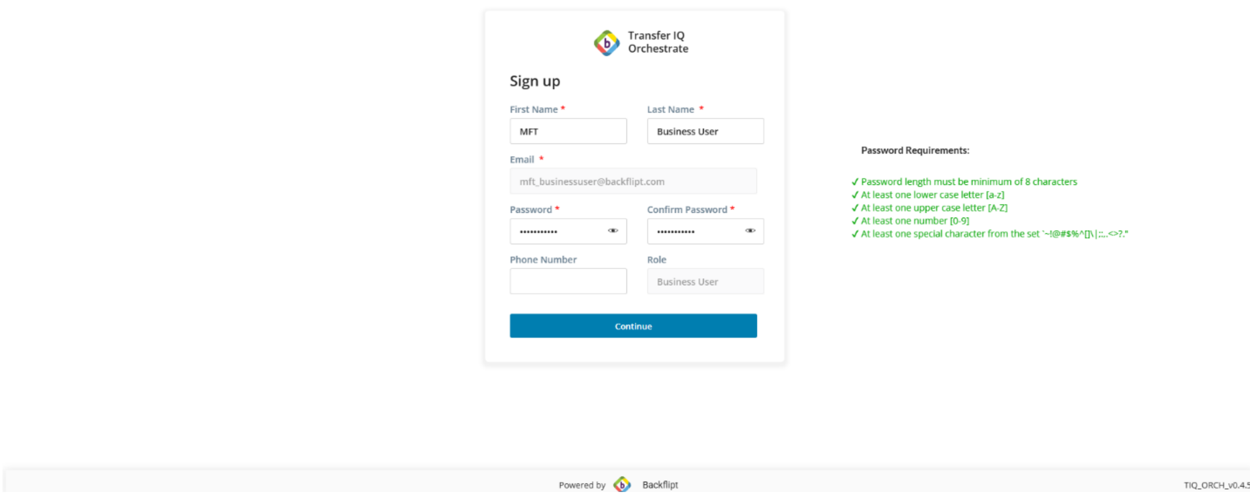


To register the business user, follow the below steps

Copy the invite, and paste it in the browser or click the registration link then the user will be redirected to the following page

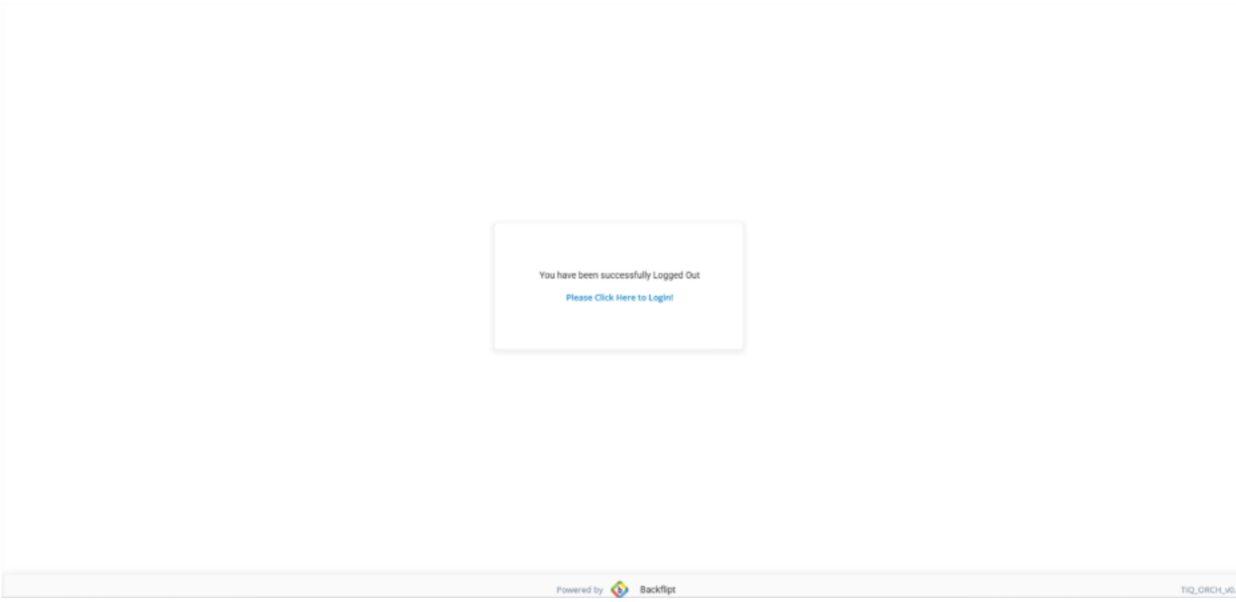


Now click on Next

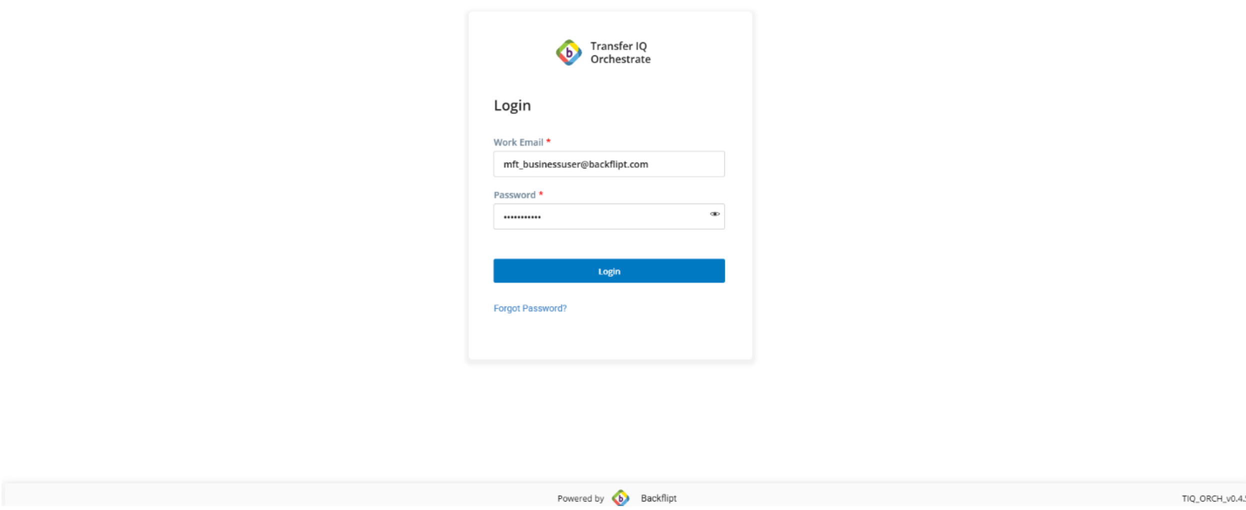


1. Once the Next button is clicked a signup form will be displayed with the following fields
   a. **First Name** – The first name of the Business User.
   b. **Last Name** – The last name of the Business User.
   c. **Email Address** – A valid email to be used for login and communication.
   d. **Password** – A secure password for account access.
   e. **Confirm Password** – Re-enter the password to confirm accuracy.
   f. **Phone Number** – A valid phone number for verification or support.

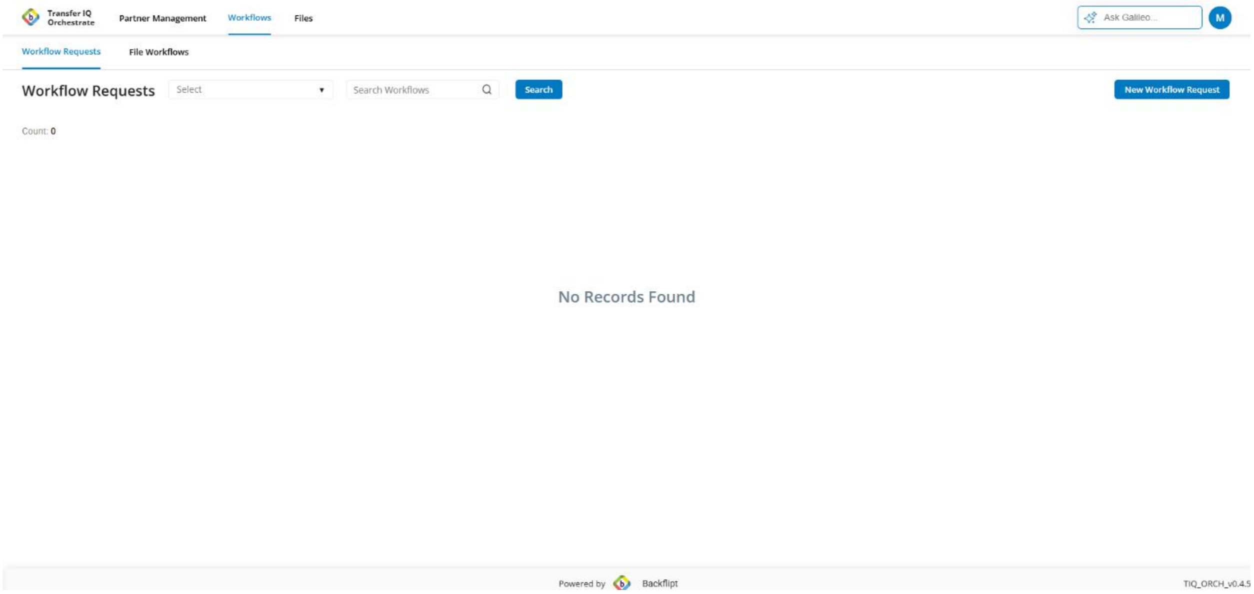
2. Click the **Continue** button to complete the registration process
3. After the Super Admin is successfully registered, the application redirects to the following page after clicking on “Please Click Here to Login!” user will be redirected to the **Login page**.



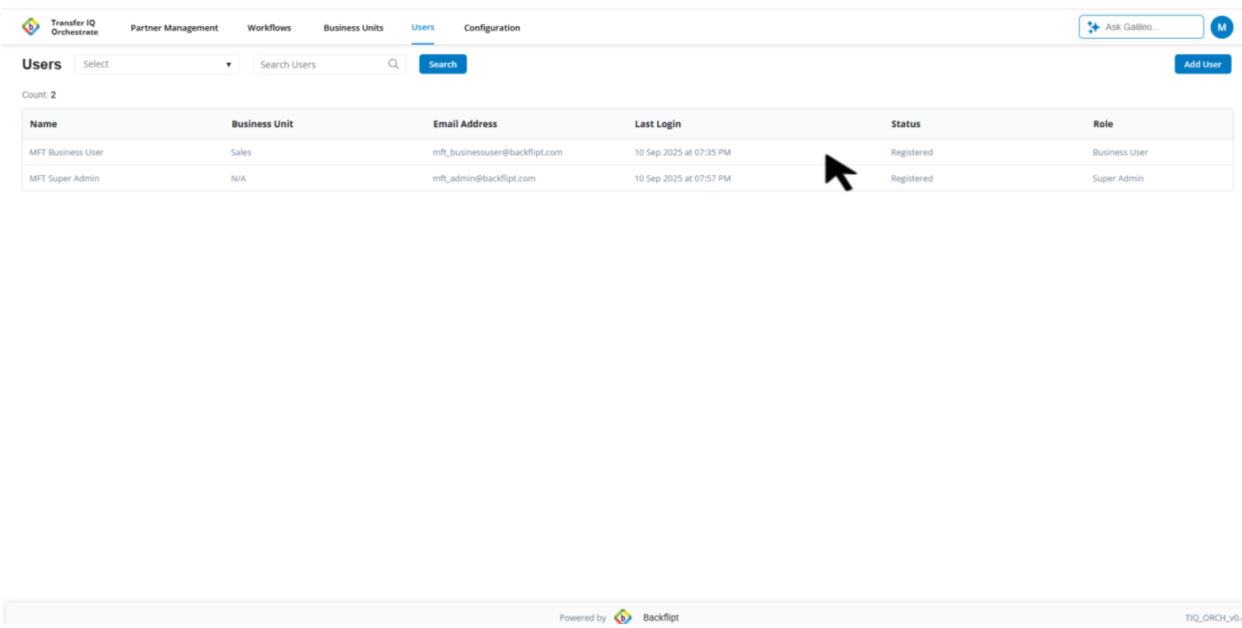
4. Enter the email and password and click the login button to login to the application



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



6. After the successful registration the status will be changed to **Registered** from **User Invited** in the Users tab

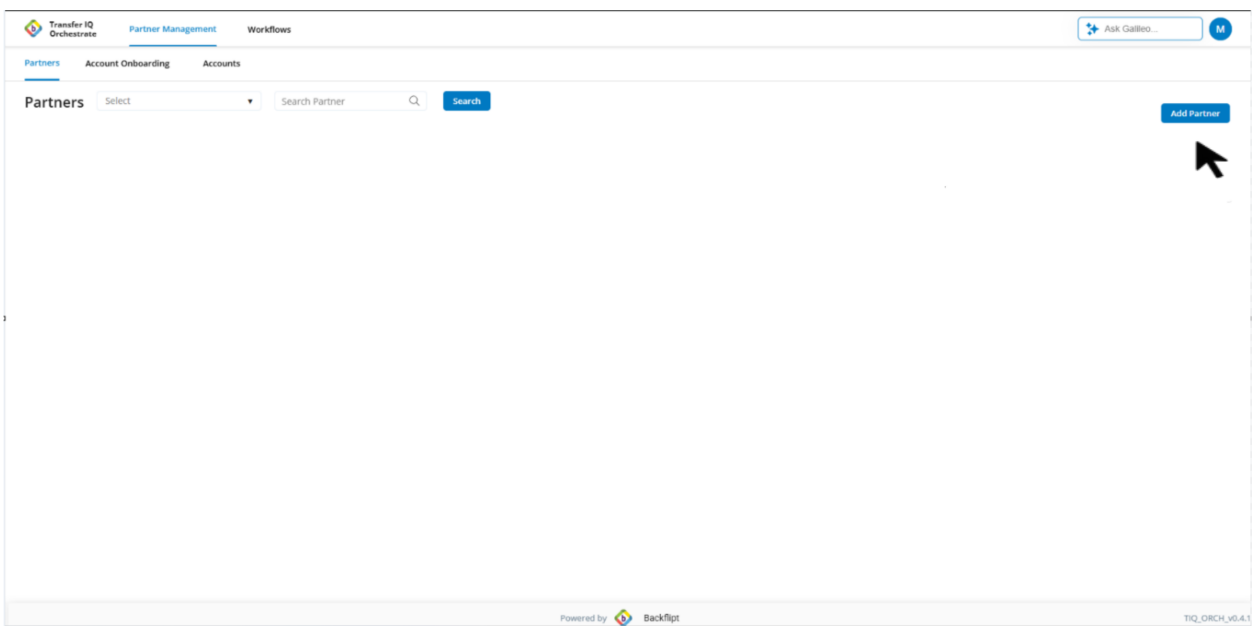


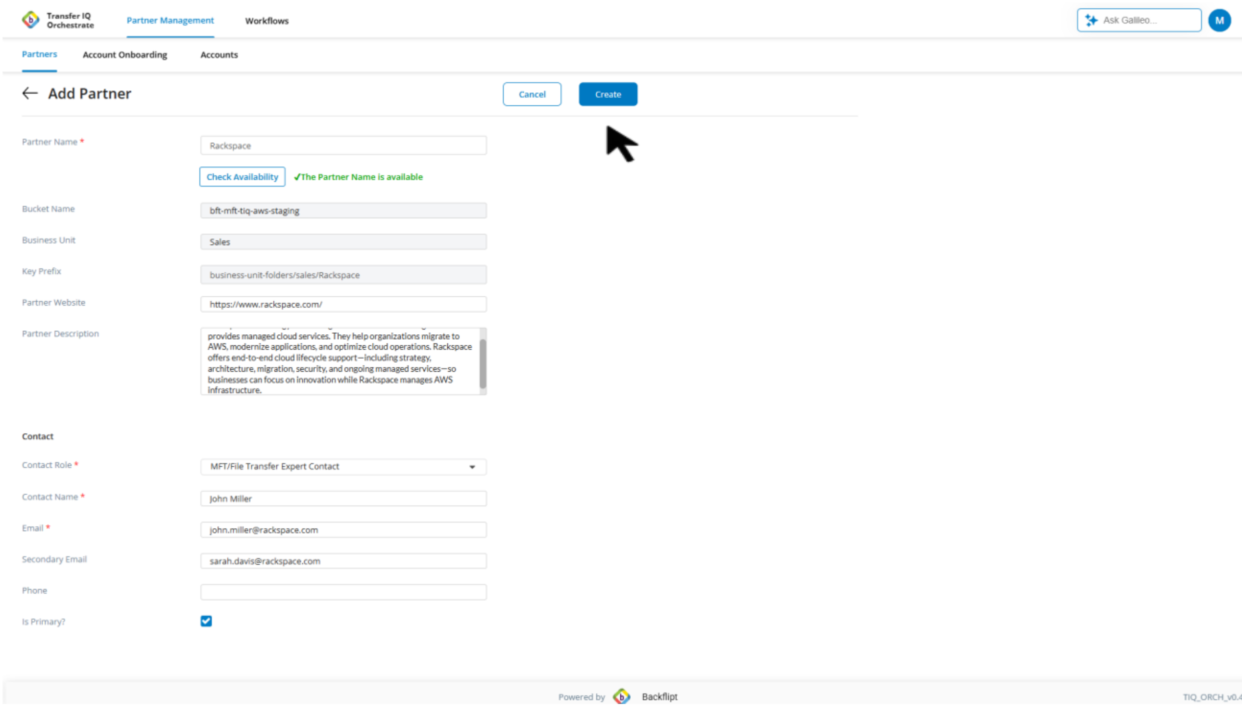
Add Partners

Business User Onboards a Partner:

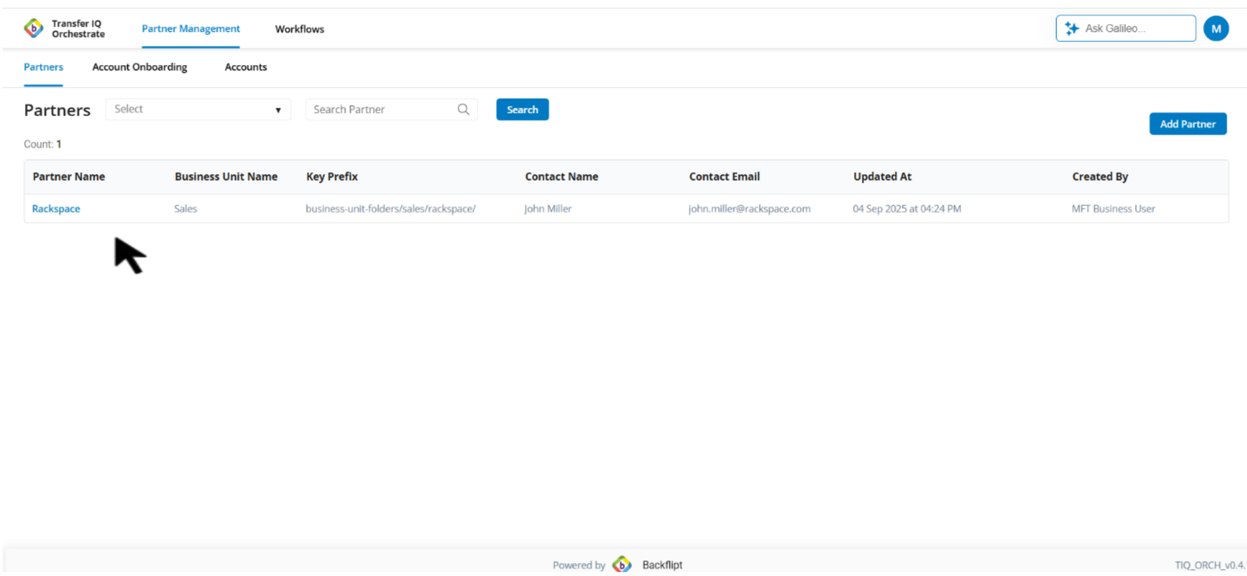
After registering and successfully logging into the application, the Business User is directed to the **Workflows** tab by default. From there, the user navigates to **Partner Management > Partners** to onboard a new partner. The Business User then completes the partner onboarding process within the application.

1. Navigates to the Partners section to view a table displaying the following columns**: Partner Name, Business Unit Name, Key Prefix, Contact Name, Contact Email, Updated At, Created By.**
2. To onboard a partner, select the "Add Partner" button, A window will appear with fields to enter the Partner Name, Partner website, and description. The form also includes sections for contact details, including contact role, name, email, secondary email, and phone number. A checkbox is provided to indicate if the contact is the primary point of contact.





3. Click the Create button to add the Partner, the newly created partner will then appear in the Partners tab.



Business User Initiates Partner Onboarding Request:

After the partner is created, an account must be created for the partner. To do this, the Business User submits an onboarding request specifying the type of account to be created. There are two types of accounts available:

1. **AWS Transfer Family Account**
2. **Partner Hosted Account**.

Once the onboarding request is submitted, it goes to the admin for approval. The account will be created only after the admin claims and creates the account

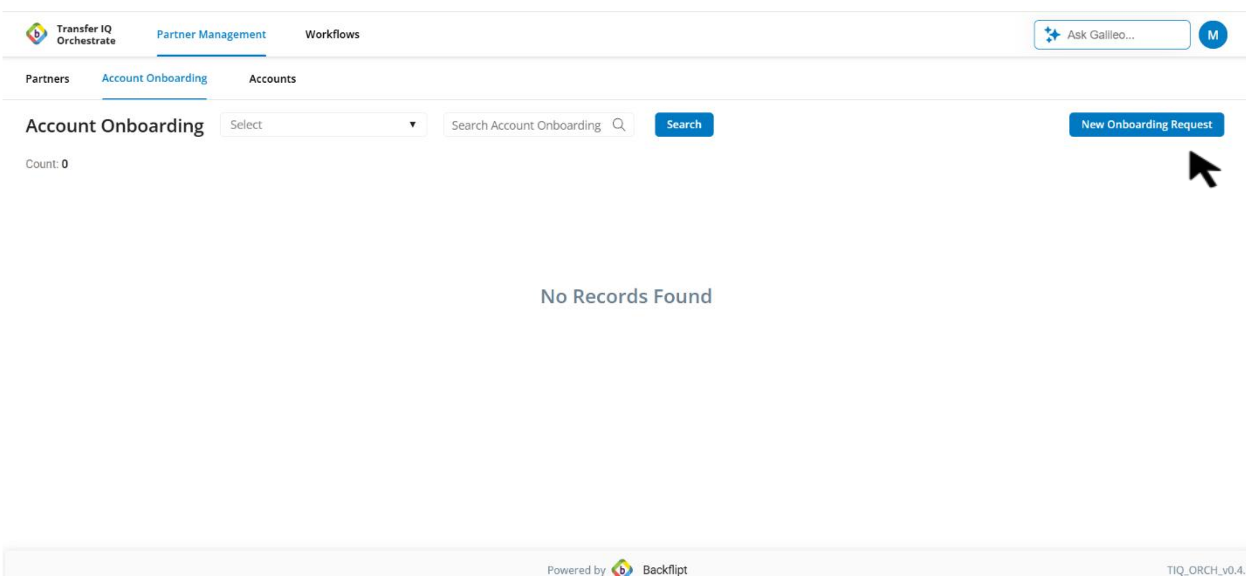
Add Partner Account (AWS Transfer Family Hosted)

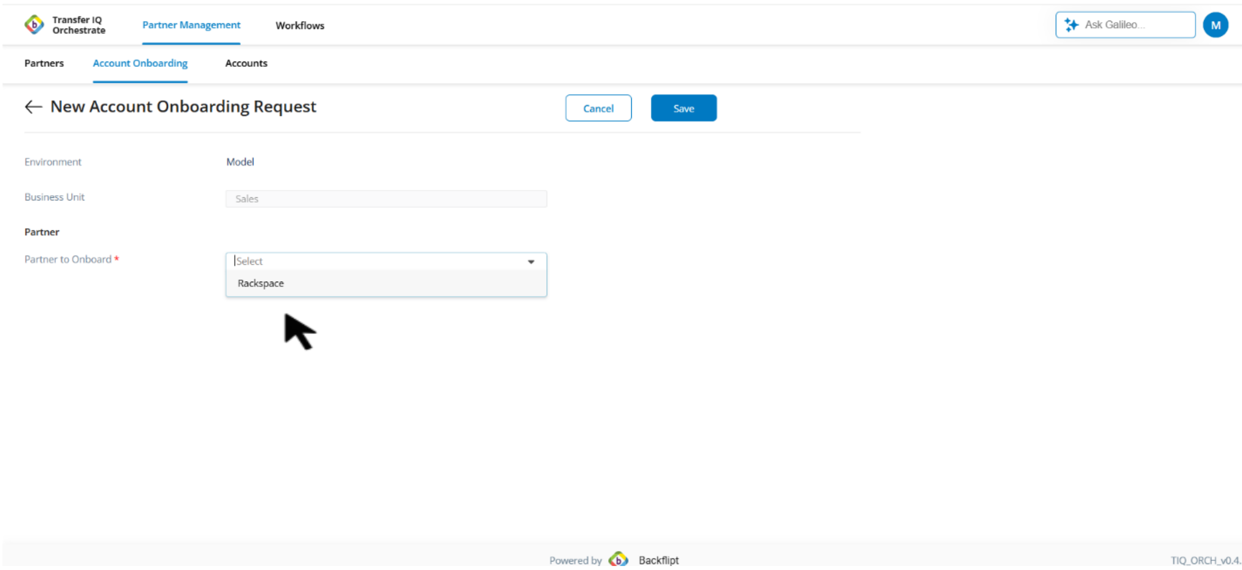
Business User Initiates Partner Onboarding Request (Business User Submission to Admin) - AWS Account

When the user clicks the **Account Onboarding** tab and clicks on "**New Onboarding Request**" button, they are redirected to the New Account Onboarding Request Form. In this form, the user sees two fields:

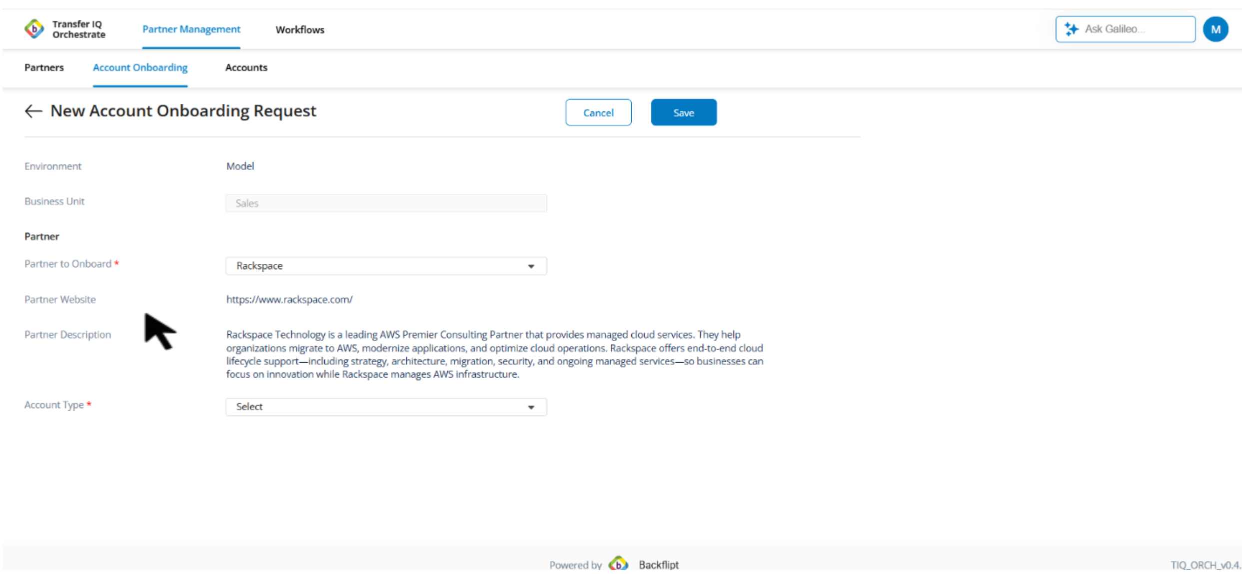
In this form, the user sees three fields:

1. **Environment** (pre-filled with "Model")
2. **Business Unit**, (pre-filled with the business unit which is associated to that Business User)
3. **Partner to Onboard**, which is a dropdown where the user selects the partner profile

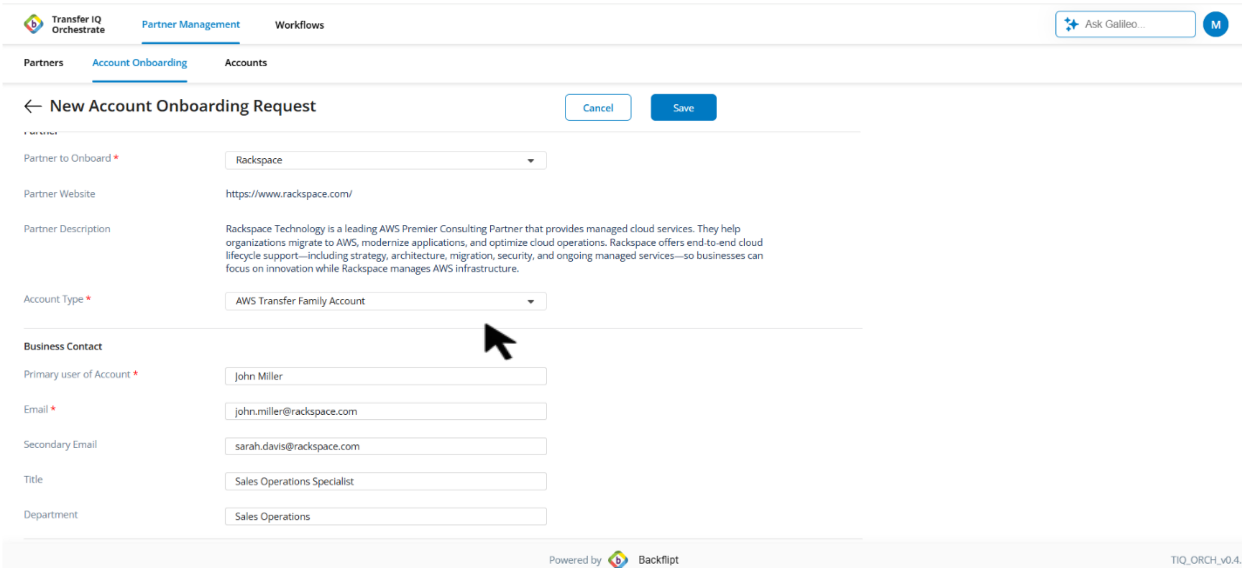


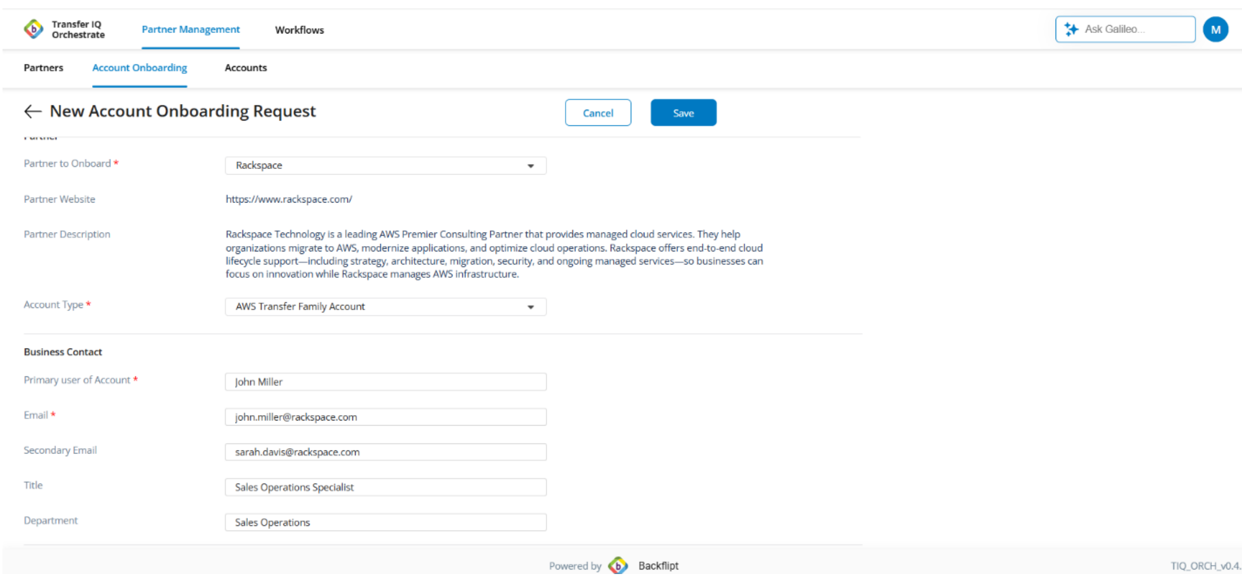


After selecting the Partner, partner details like Partner website and Partner Description fields are displayed and these cannot be edited, these fields are read-only mode.



Now when **AWS Transfer Family** account is selected, business contact form will be opened, and user has to give all the mandatory details with valid data. If not, an error will appear when attempting to save the request.



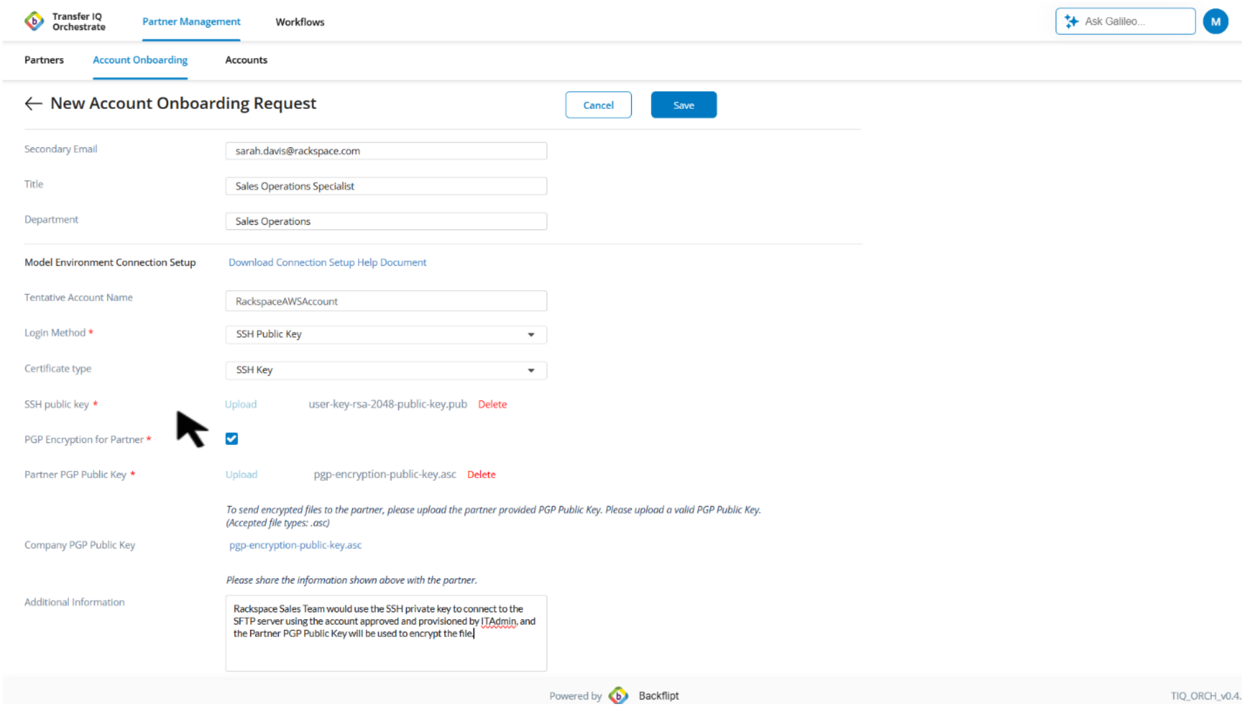


For AWS Account, only SSH key is supported for login method.

The following fields are displayed when the account type is selected as AWS Transfer Family Account.

1. **Tentative Account Name**: The Business User can provide a tentative account name, which the IIT Admin may use during account creation. This field is optional.
2. **Login Method: In** dropdown only SSH public key will be available.
3. **Certificate type:** For partner to login to the company's server, only SSH key login type is supported.
4. **SSH Public Key**: To log in to the company's server, a partner will share their SSH public key with the Business User. Business Users will upload shared partner's ssh public key.

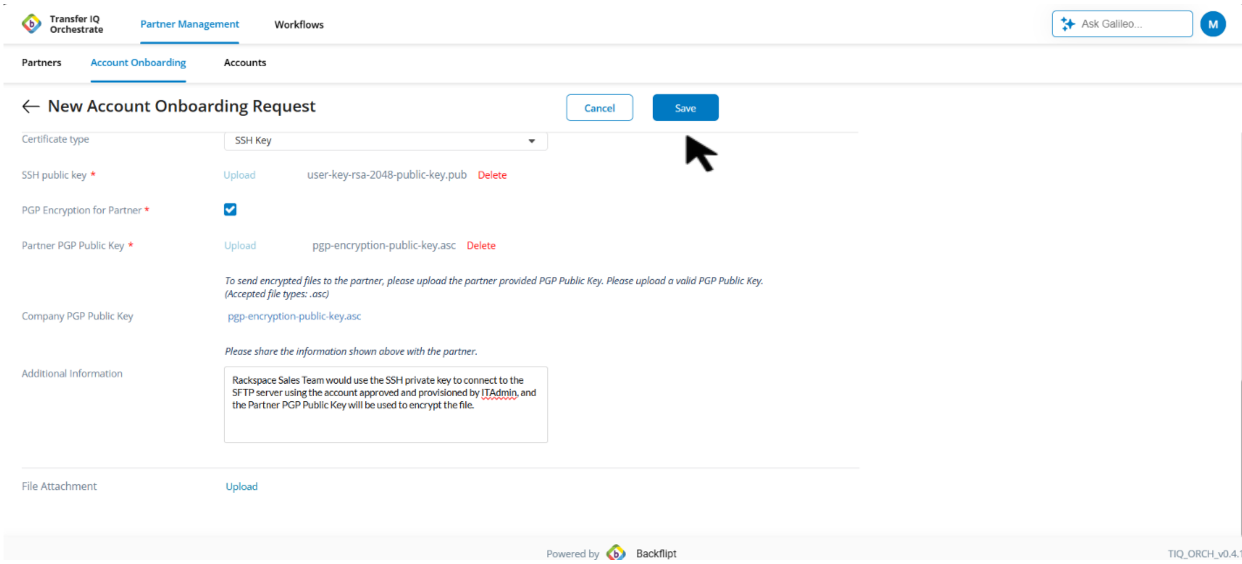
5. **PGP Encryption for Partner**: Partner will share Partner's PGP Public key to Business User. Business Users will upload shared PGP key provided by the partner. When a company wants to send files to its partner, the company will use partner's PGP public key and encrypt the files and send them to partner the partner uses their PGP private key to decrypt files sent by the company. the files receive partner uses their PGP private key to decrypt files sent by the company. the files received.



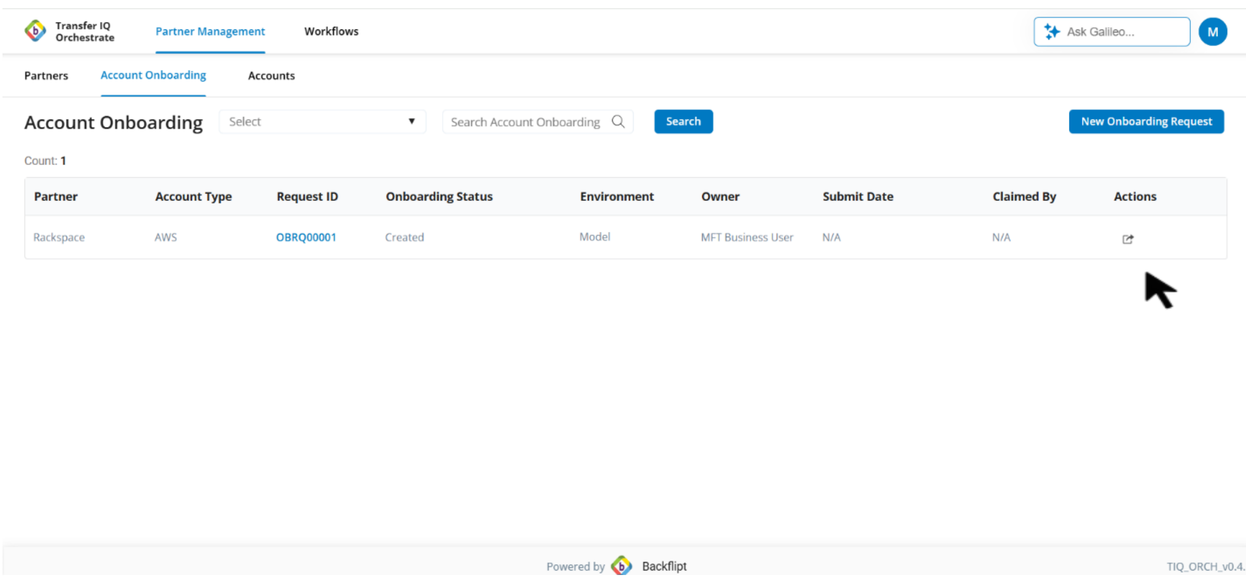
Company PGP Public key:

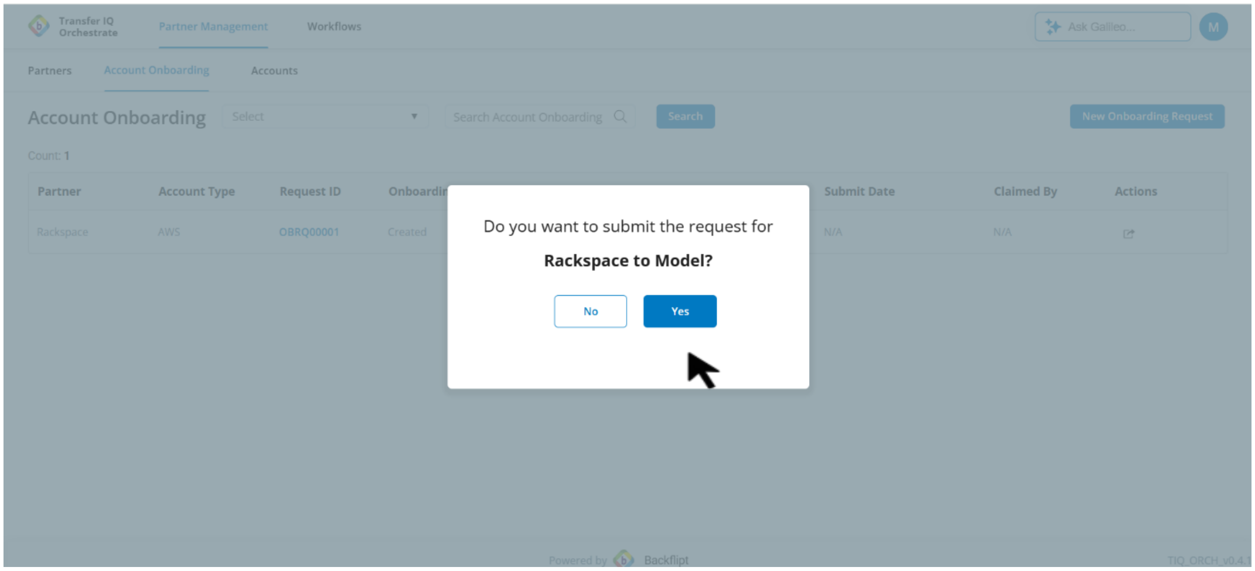
When a partner wants to send files to a company, the partner will use the company's PGP public key and encrypt the files and send them to the company. To decrypt the files sent by the partner, the company will use the company's PGP private key and decrypt the files received from the partner. This key is auto populated, when the form is filled in by the Business User.

There are two optional fields: **Additional Details** and **File Attachment**. These are not mandatory, but if the Business User wants to share extra information or upload supporting documents for the admin, Business User can use these fields to provide that additional input.



So, Business Users will upload all these above details and submit the form to Admins.

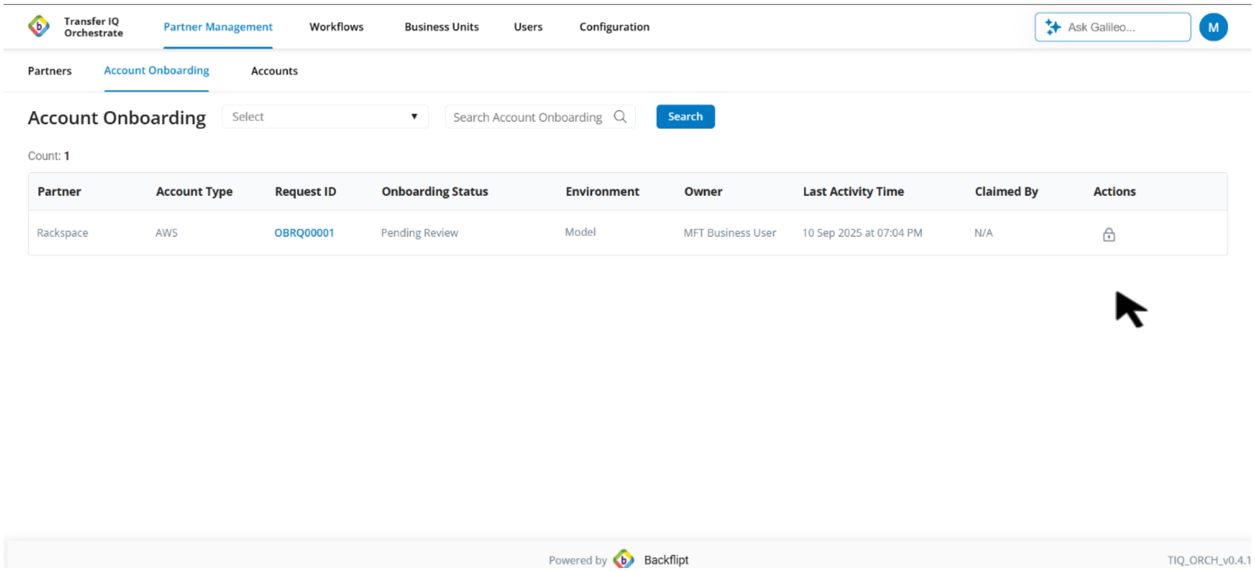


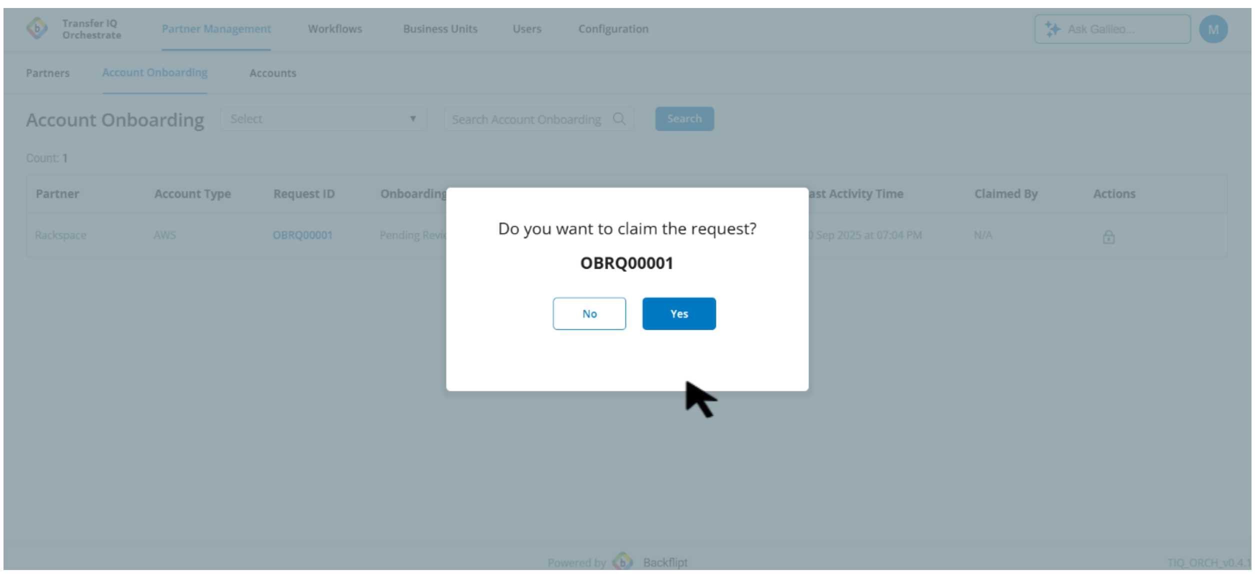


Admin Approves Partner Onboarding Request and Onboards Partner with AWS Account:

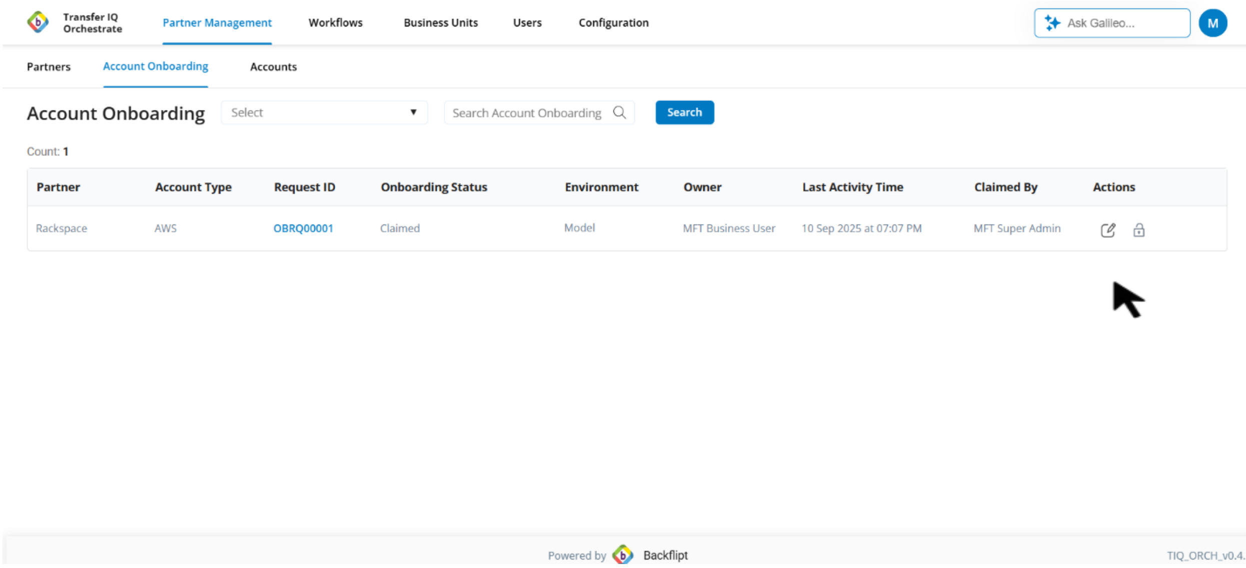
Once the onboarding request is submitted, it becomes visible to all admins under the **Account Onboarding** tab.

- An admin can claim the request to take ownership in one of two ways: by clicking the **View Request** button in the email notification sent after submission, or by locating and claiming the request directly from the **Account Onboarding** tab.

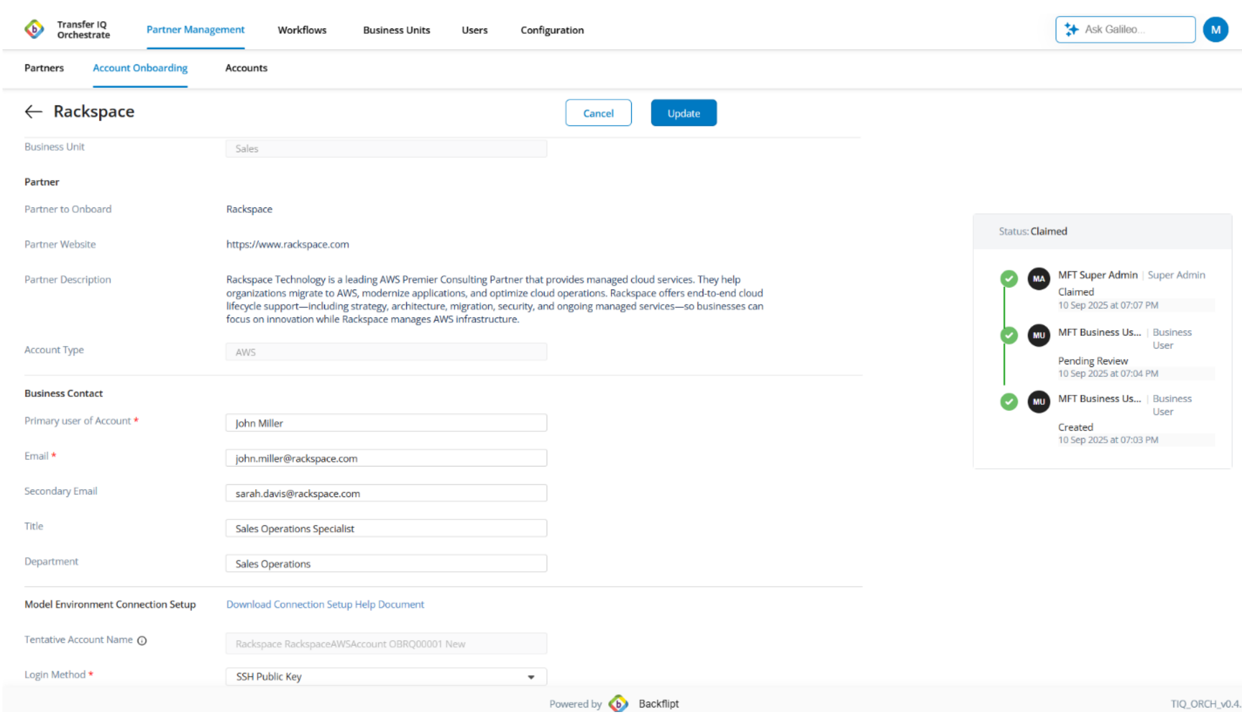




- After claiming the request, the admin can view all the details provided by the Business User in **edit mode**.
- Click the edit mode to open the request in edit mode

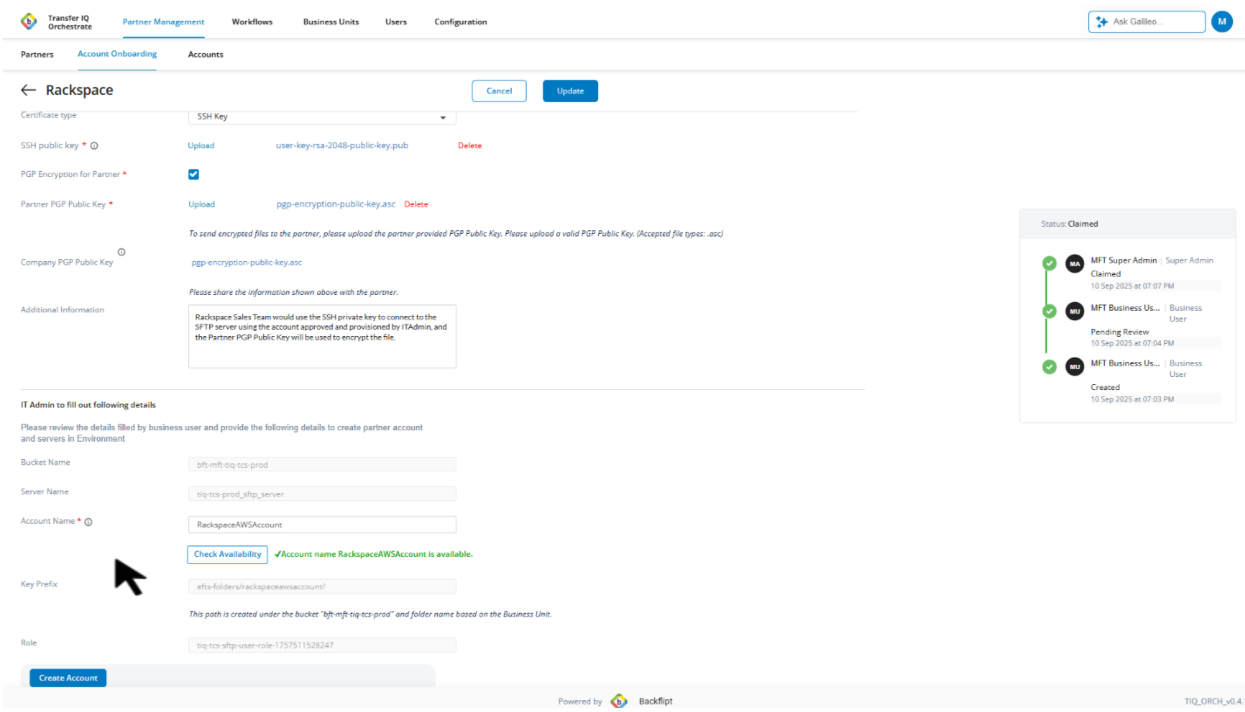


- The admin has the option to review, modify, or update any information if changes are needed. If no changes are required, the details can be left as they are.

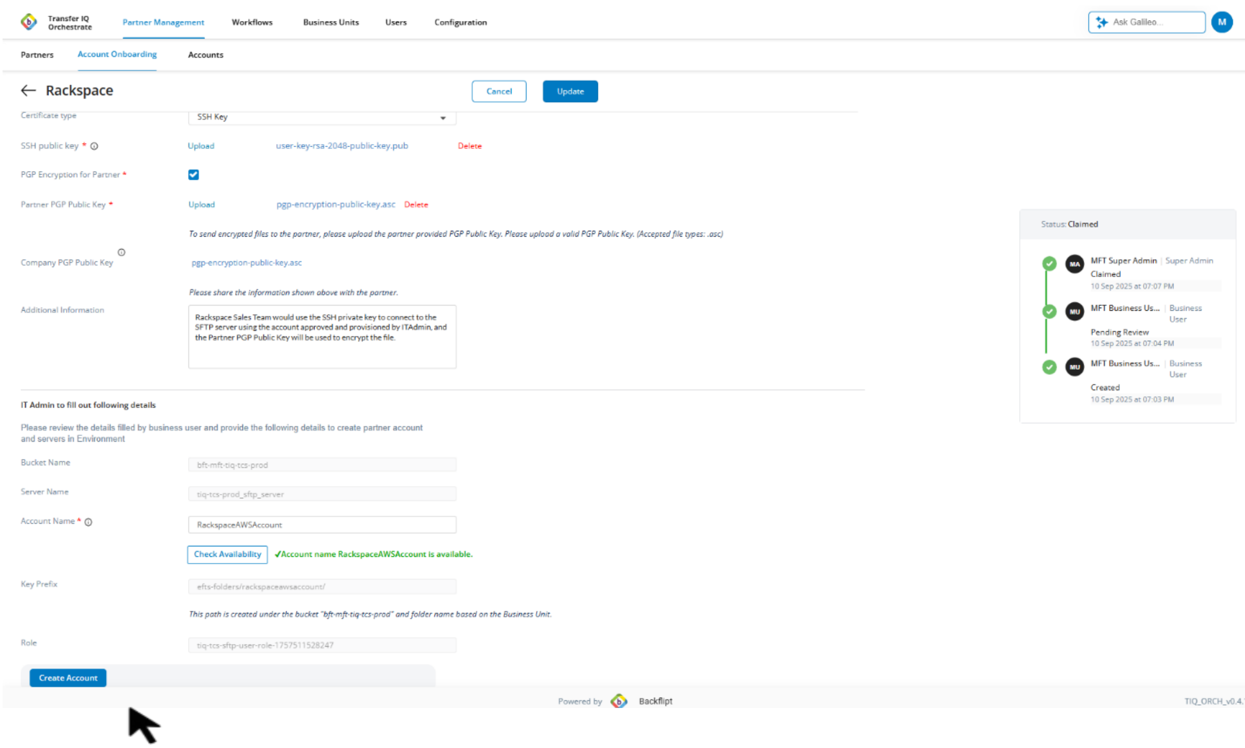


- Once all the details are correct, there is a section called **IT Admin to fill out following details which contains the following fields**
  - **Bucket Name** – Automatically populated based on the bucket name configured in the metadata settings.
  - **Server Name** - Automatically populated based on the server name configured in the metadata settings.

- **Account Name** – A unique name manually entered by the admin during account creation.
- **Key Prefix** – Automatically generated in the format: efts-folders/`{Account Name}`/, where `{Account Name}` is filled in based on the value entered in the **Account Name** field.
- **Role** – Automatically populated with a predefined role; this field is not editable.



Upon clicking on the Create Account, the account has been created



Email Notification Sent to Business User

Upon creation of the AWS account, the Business User will receive an email notification containing the following details:

Email Subject:

- Account Creation Successful – {Partner Name} – Model

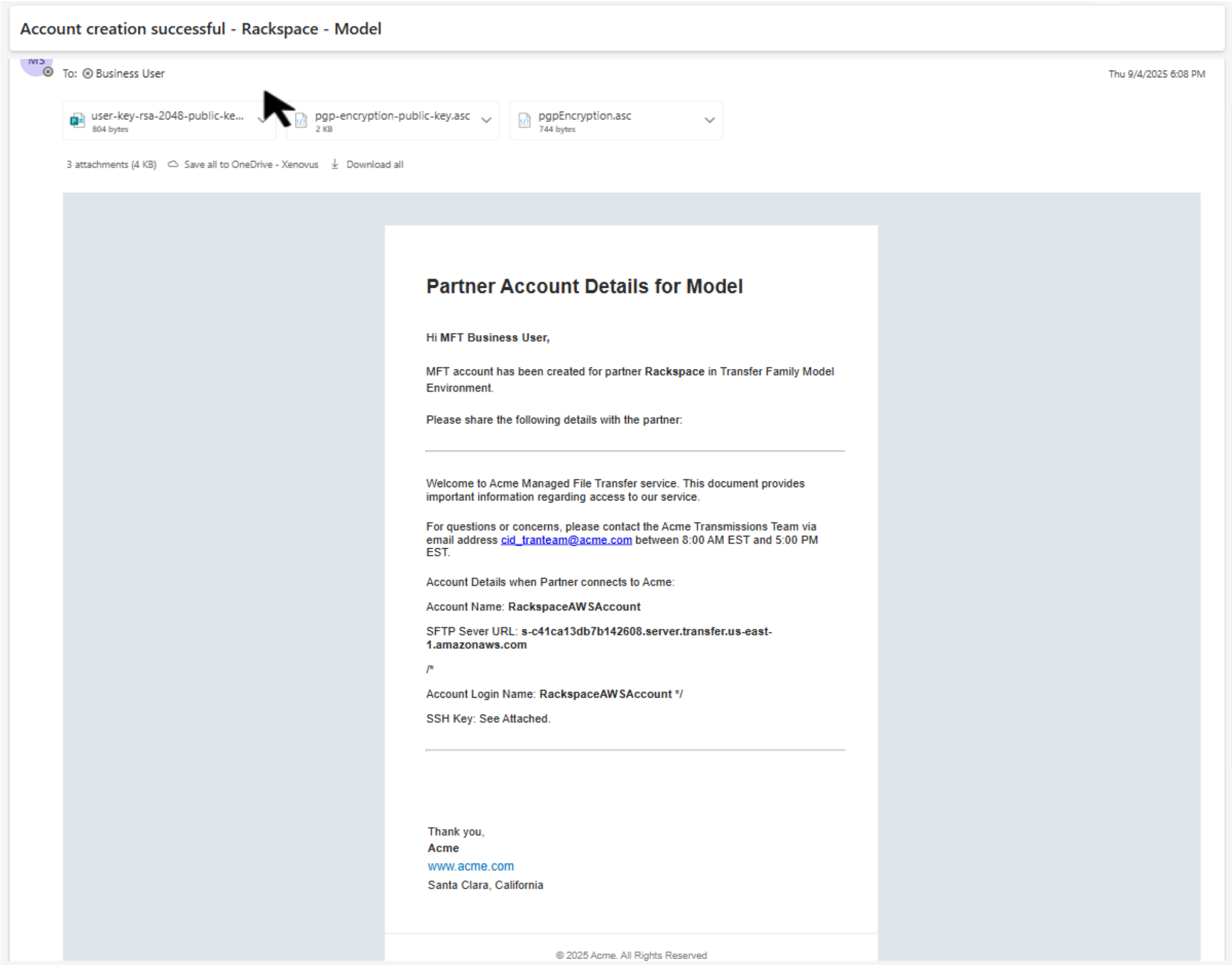
Fields in Email Notification:

- Account Name
- SFTP Server URL
- Account Login Name
- SSH Key (attached)

Additional

- Thank you note
- Company Name and Website
- Company Location
- Support Contact Email and Working Hours
- Welcome note and instructions on service access

In addition, the email will include attachments for the **SSH Public Key of** partner and the **PGP Public Keys** of both the Partner and the Company.



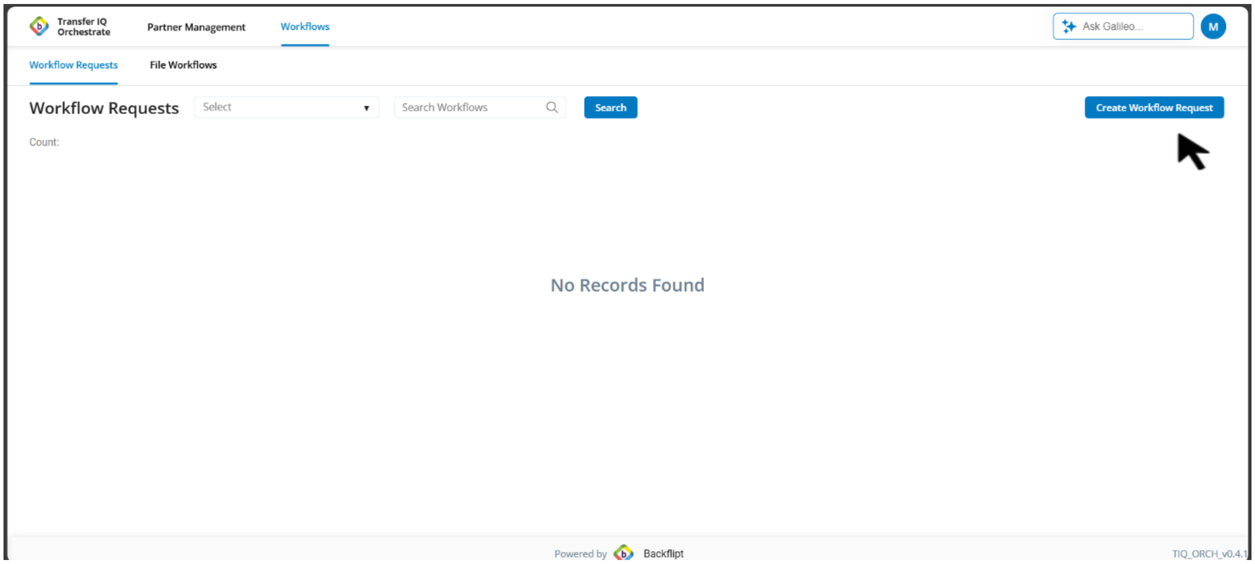
Add AWS Transfer Family Account Workflows

Add AWS Transfer Family Account Inbound Workflow

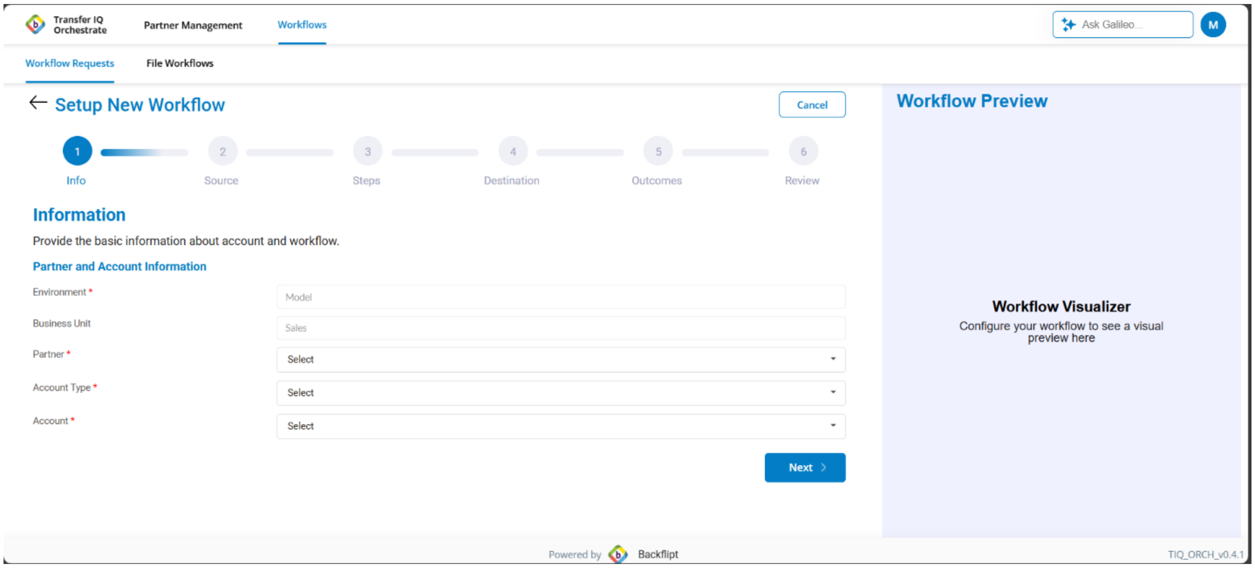
In the AWS Inbound Workflow, a partner uploads a file in the source path of company's server, the workflow is automatically triggered as soon as the file is placed into the source path. The file is processed through the defined transformation steps and then delivered to the destination specified in the workflow

To Create an AWS Inbound Workflow Business User Creates a Workflow Request with all the required details and submits the workflow request to the admin for approval.

1. Click the Workflows > Workflow Requests tab to view a table displaying the workflow request with the following columns**: Request Id,**
2. To create a new workflow request, click the "Create Workflow Request" button



3. A window will appear with a screen to **Set up a New Workflow** with various sections
    a. Info
    b. Source
    c. Steps
    d. Destination
    e. Outcomes
    f. Review



Information (Info)

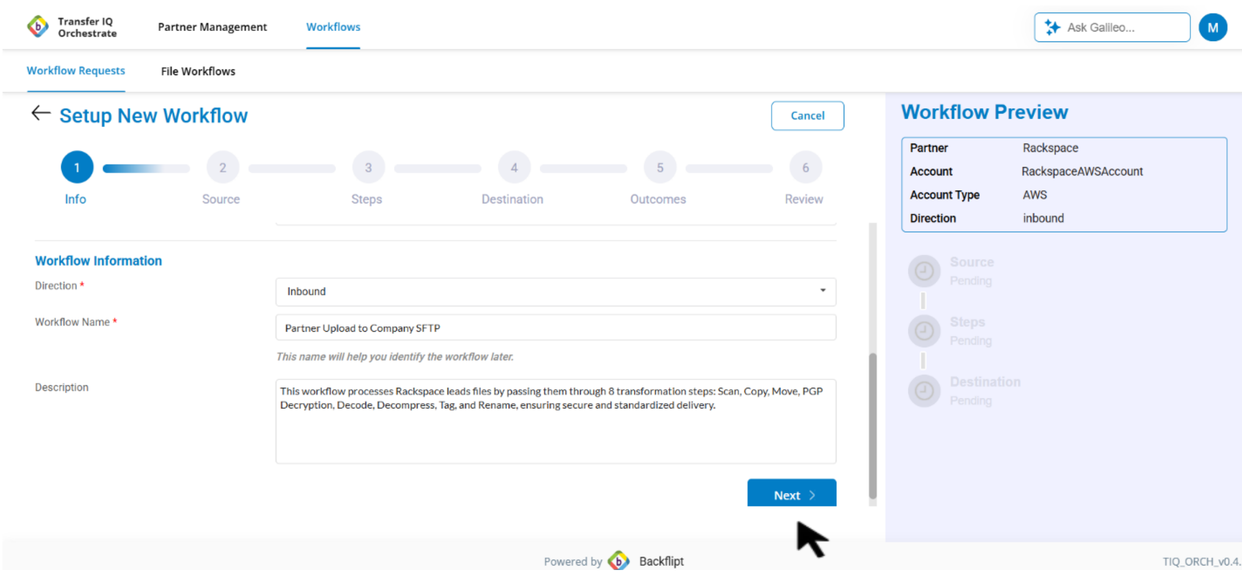
Provide the basic information about account and workflow in this section

This section contains the following fields

1. Environment – Auto populated with Model
2. Business Unit – Auto populated with the Business Unit assigned to the logged in Business User
3. Partner – A dropdown that consists of list of partners and it allows Business User to select a partner for whom the workflow needs to be created
4. Account Type – AWS Account
5. Partner Account – All the partner accounts created for the partner will be displayed in the dropdown, and allows to select a partner account out of all available options

Once the Partner Account is selected, the Workflow Information section is displayed to provide information about the Workflow with below fields

1. Direction – Select Inbound to create an Inbound Workflow
2. Workflow Name – An input field to Enter a Name for the workflow
3. Description – A file to provide a description about the workflow



Once all the information is given click the **"Next"** button to navigate to the Source Section

Source

The partner uploads the file to the source folder. All information regarding the source and trigger scheduling will be provided in the source section.

The Source Section Consists of the following section:

1. Trigger Configuration

Trigger Configuration:

This section provides details about the source folder and the file name pattern that should trigger the workflow.

The section consists of the following fields:

1. Trigger Type – Pre-filled with the "S3 Upload"
2. Bucket Name – Pre-filled with the "bft-mft-transferiq-qa"
3. Key Prefix – Folder path where the partner uploads the file pre-filled with the path ""
4. File Name Pattern - Specify the file name or pattern that should trigger the workflow.
    a. You can either enter the **exact file name** (e.g., `Sales.pdf`) or use **wildcard characters** to define a pattern:
    b. * — Matches **any number of characters**
    c. ? — Matches **exactly one character**

d. **Examples:**

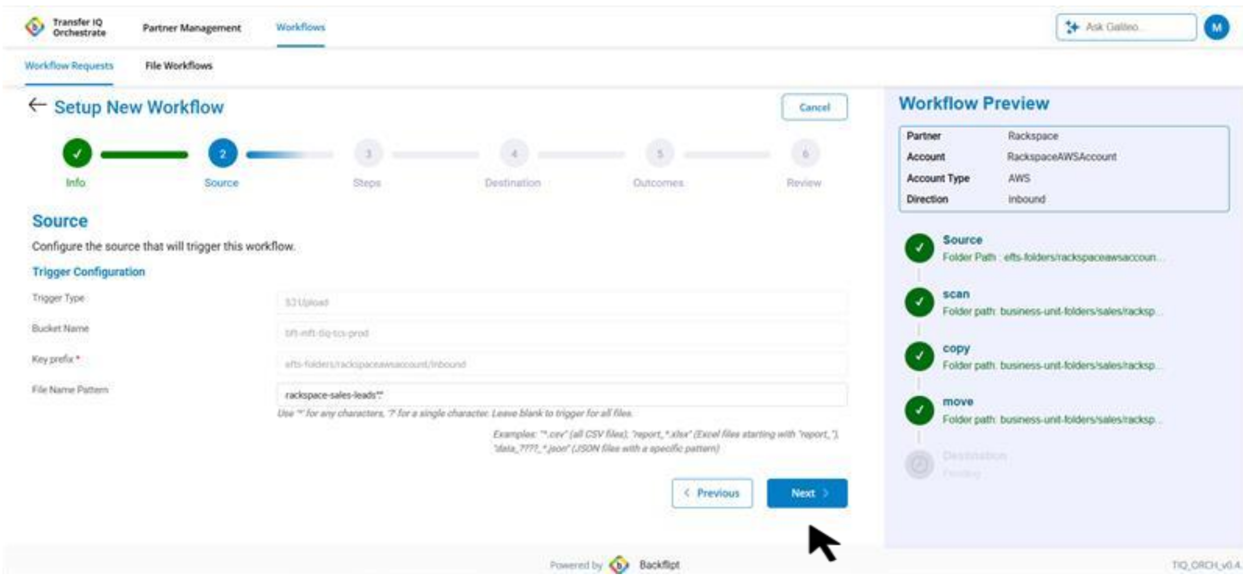
e. `*.*` – Triggers the workflow for **any file**, regardless of name or extension

f. `*.csv` – Triggers for any file with a `.csv` extension, such as `data.csv` or `report.csv`

g. "report_*.xlsx" (Excel files starting with "report_")

h. `data_????_*.Json` – Triggers for JSON files that follow a specific pattern: the file name must start with `data_`, followed by **exactly four characters.**

i. Simply leave blank to trigger for all files



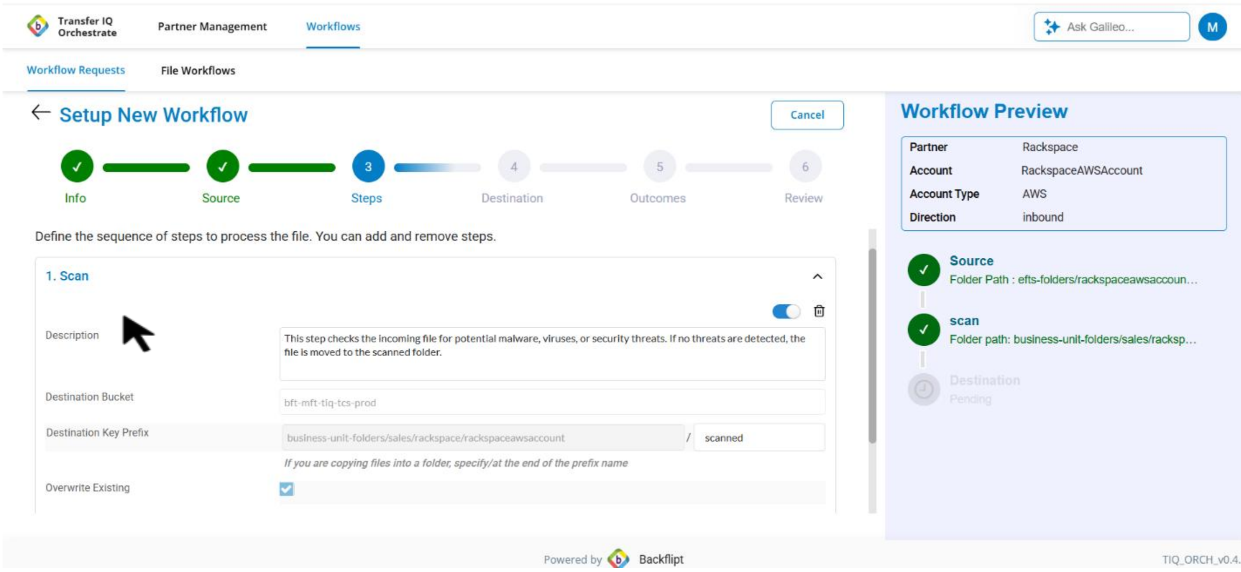
After providing all mandatory details, click Next to continue to the Steps Section

Steps:

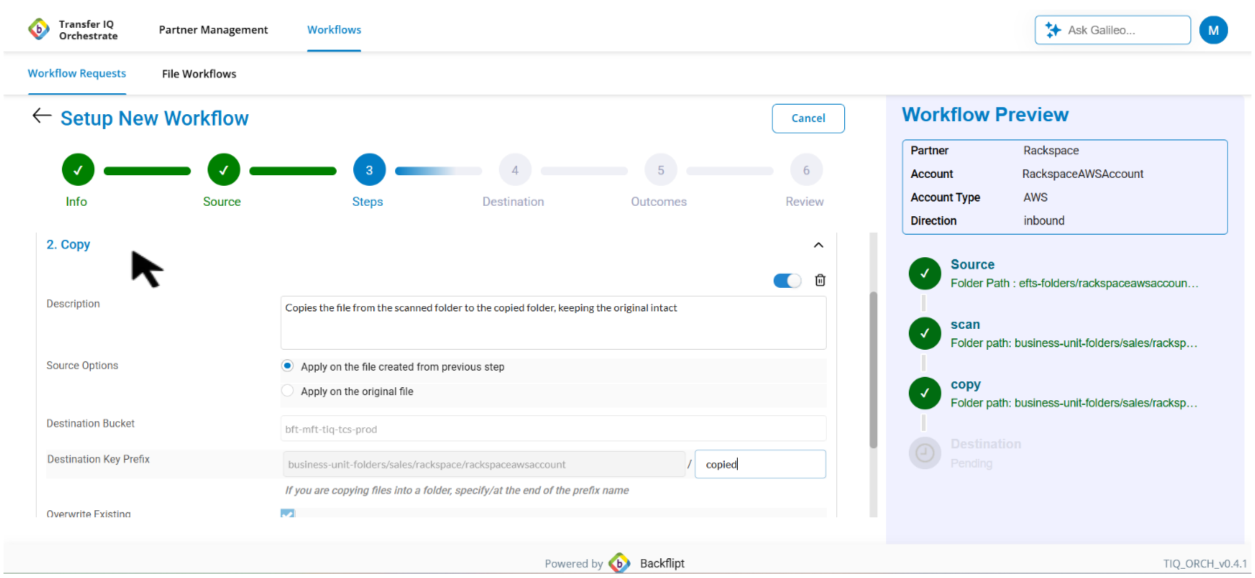
There are different Steps in the PFTS Inbound Workflow. Once the workflow is triggered the all the steps configured in the steps section will be executed and the file will be placed in the destination section:

The Steps Available in The PFTS Inbound Workflows are as follow**s**

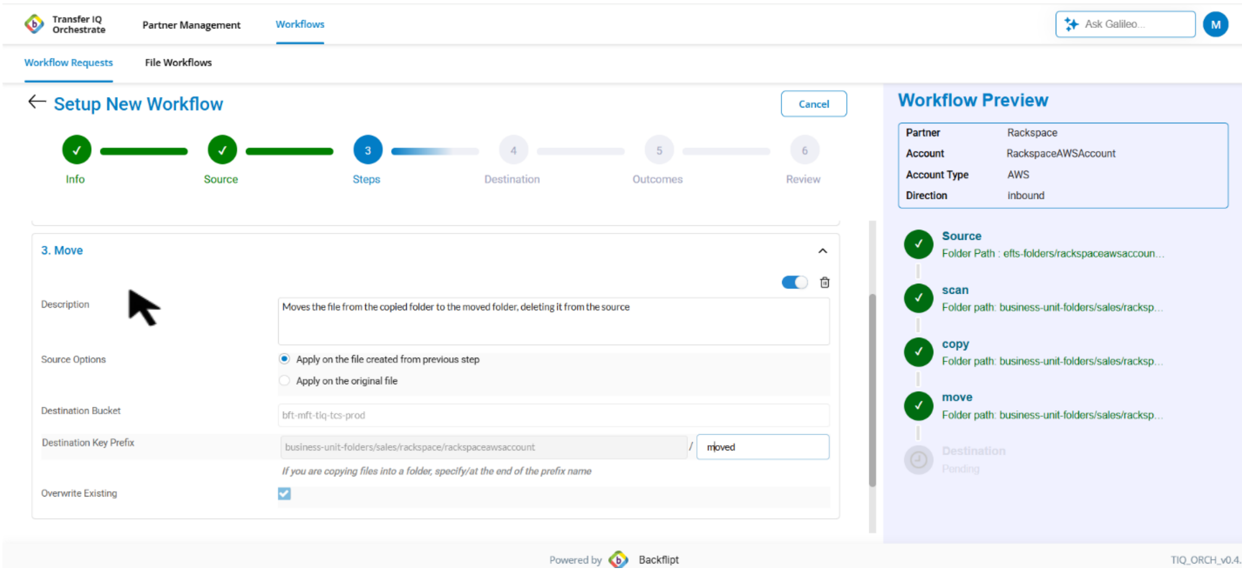
Scan - The scan step checks files or directories for potential malware, viruses, or security threats



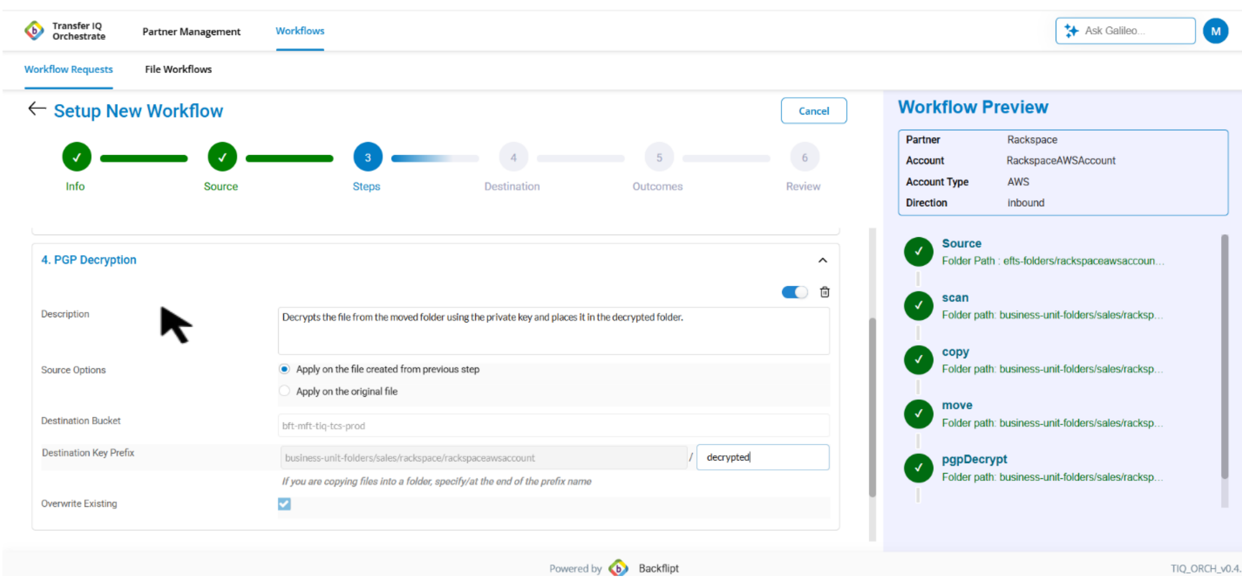
Copy - The copy step duplicates a file from the source location to the destination without deleting the original. This ensures the file remains accessible in both locations.



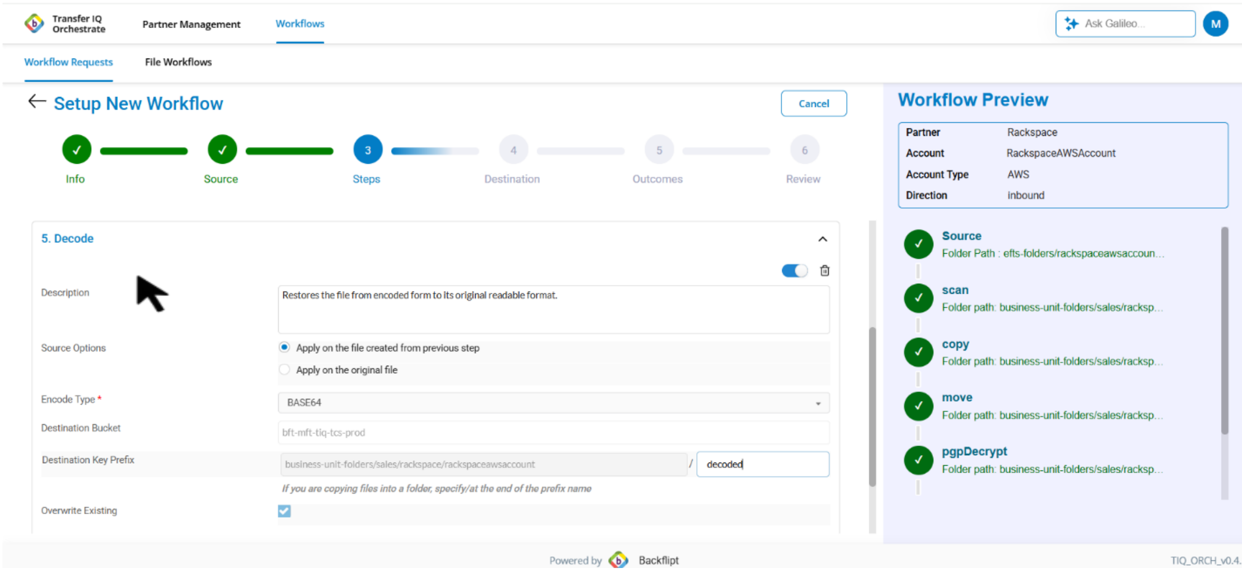
Move - The move operation shifts a file from the source location to the destination. Once moved, the file no longer exists in the source location.



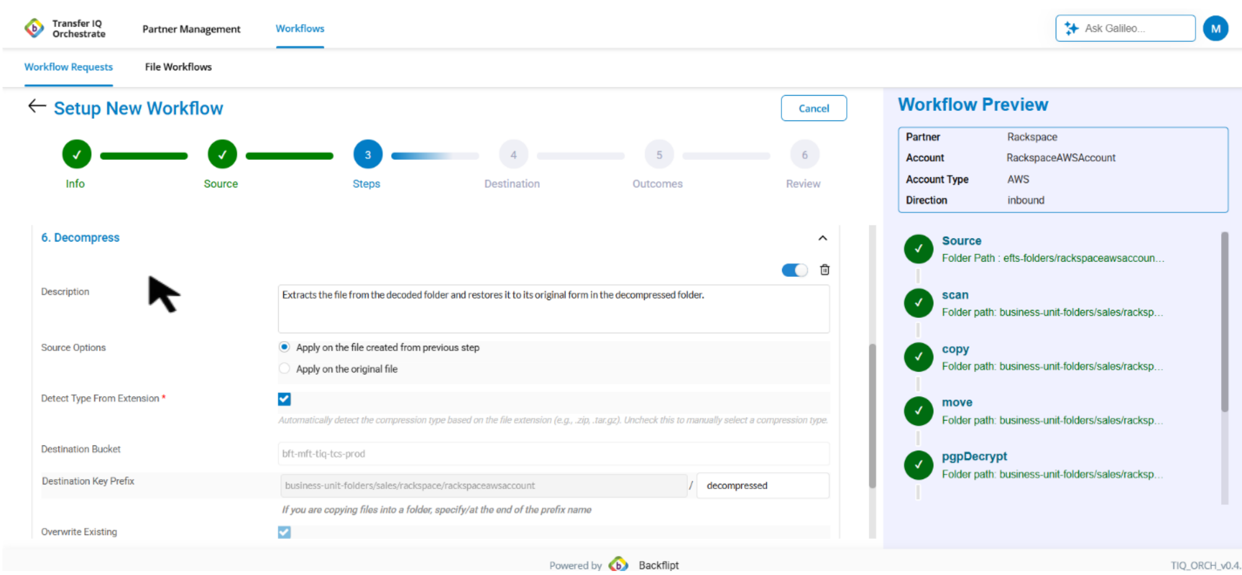
PGP Decrypt - The PGP decrypt step retrieves an encrypted file from the source location, decrypts it using the PGP private key provided in the MFT Settings tab, and places the decrypted file in the specified destination folder.



Decode - Decode step converts encoded file back to its original, readable format. It is used when a file has been encoded (for example, in Base64) and needs to be returned to its normal form so that it can be used.

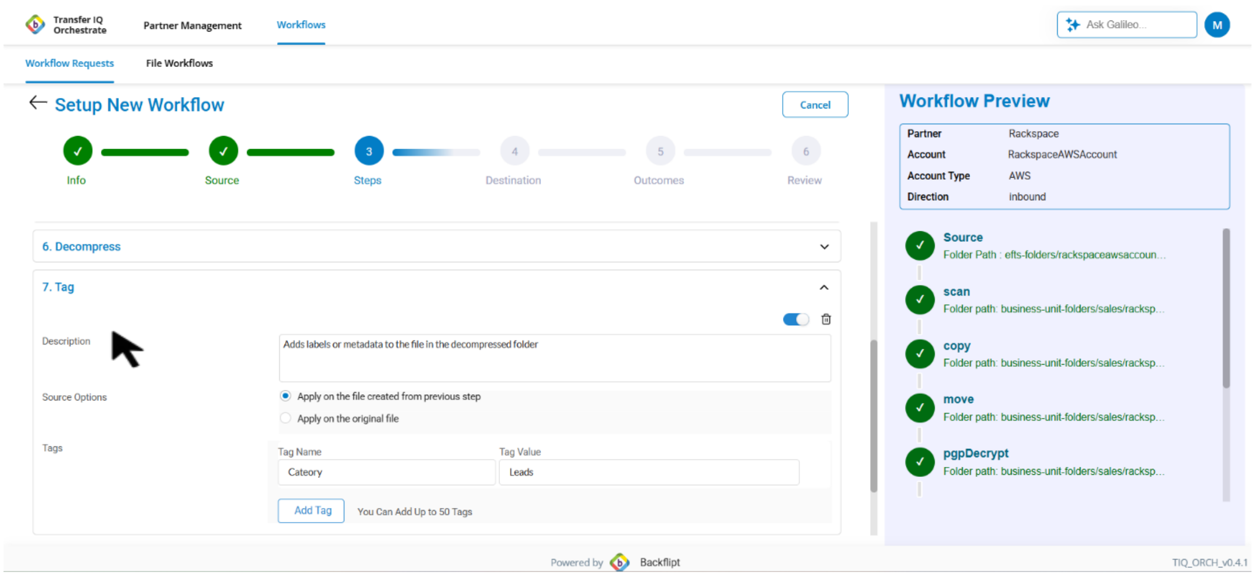


Decompress - Decompress step extracts and restores the original content from a compressed file, allowing the data to be accessed and used in its original form.

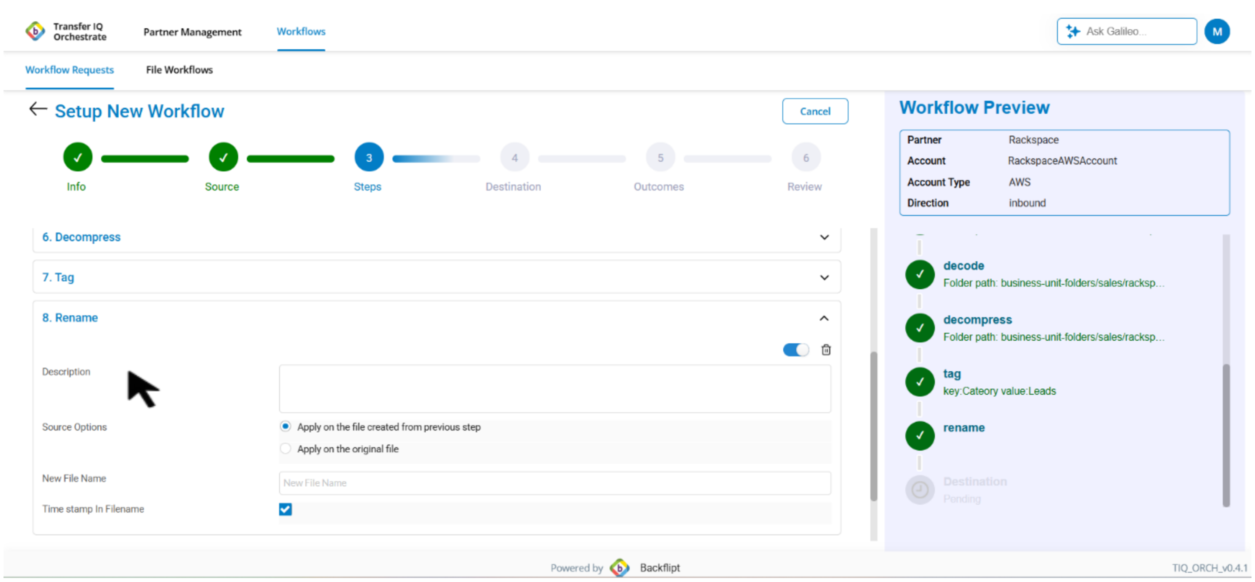


Delete - The **delete step** removes a file from its source permanently. This step is typically used to clean up files after they are no longer needed

Tag - The tag step allows adding additional information to files in the form of key-value pairs. This extra info helps describe, organize, and manage them more effectively. Up to 50 tags can be added per file.



Rename - The **rename step** changes the name of a file. This helps organize files by giving them clear, consistent, or updated names without altering their content or location.



For all the above steps there are toggling bar and delete icon

- Disabled steps will be ignored during workflow execution
- Caret symbols (^) and (v) are displayed for each step, allowing the user to expand or collapse the steps as needed.

The fields available after adding Copy**, Move, Decrypt, Scan, Decompress** and **Decode** steps are listed below.

- **Description** – A detailed description about the step added
- Source Options Consists of two options
  - **Apply on Original File** – When selected, the step will be executed on the original file located in the source.
  - **Apply on File Created from Previous Step** – When selected, the step will be executed on the output generated by the previous step.
- **Bucket Name**: Pre-filled with the name of the storage bucket configured in metadata settings (e.g., “**bft-mft-transferiq-qa**")
- **Destination Key Prefix -** The folder path or prefix within the destination bucket where the files will be placed (e.g., “Business Unit Folder}/ {Business Unit}/{Partner}/ {Partner Account}”).
- In addition to this, a custom folder can be specified in the input field next to the Destination Key Prefix. The final file location will be the combination of the key prefix path plus the custom folder entered, determining exactly where the file will be stored when the step is executed.
- **Overwrite Existing –** This checkbox is enabled by default. If a file with the same name and extension already exists, it will be overwritten.

The fields available after adding **Delete, Rename** and **Tag** steps are listed below.

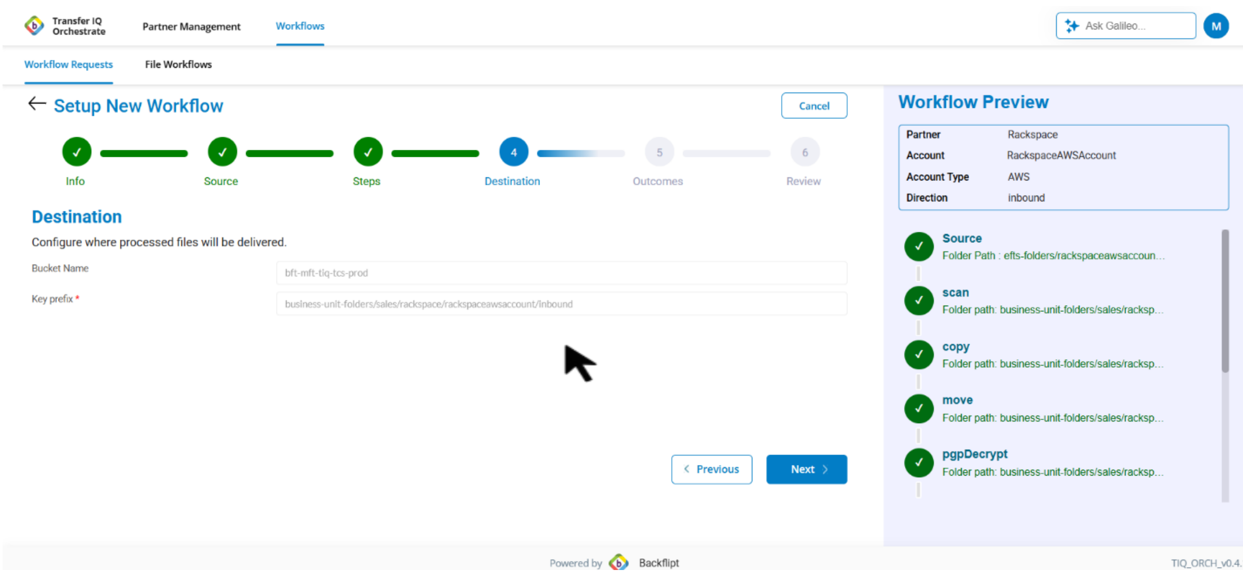
- **Description** – A detailed description about the step added
- Source Options Consists of two options
  - **Apply on Original File** – When selected, the step will be executed on the original file located in the source.
  - **Apply on File Created from Previous Step** – When selected, the step will be executed on the output generated by the previous step.
- **Bucket Name**: Pre-filled with the name of the storage bucket configured in metadata settings (e.g., “**bft-mft-transferiq-qa**")
- **Overwrite Existing –** This checkbox is enabled by default. If a file with the same name and extension already exists, it will be overwritten

Note: Since no destination key prefix is provided, the rename and tag will be applied to the path or folder from the previous step.

Destination:

1. Pre-filled with the name of the storage bucket configured in metadata settings (e.g., “**bft-mft-transferiq-qa**")

2. Key Prefix – The folder path where the uploaded files will be placed in the destination. (e.g., “{{Business Unit Folder}/ {Business Unit}/{Partner}/ {Partner Account}/{Direction}} ")



Outcomes Section

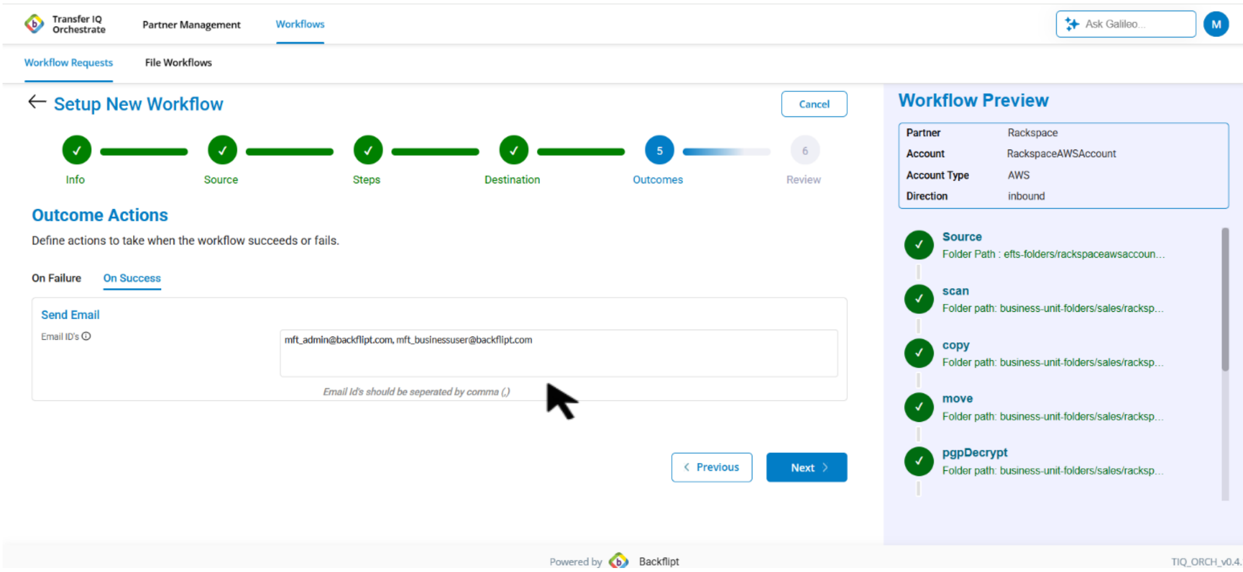
The Outcomes section consists of two tabs:

1. On Success
2. On Failure.

On Success – Notify the email entered upon successful file transfer.

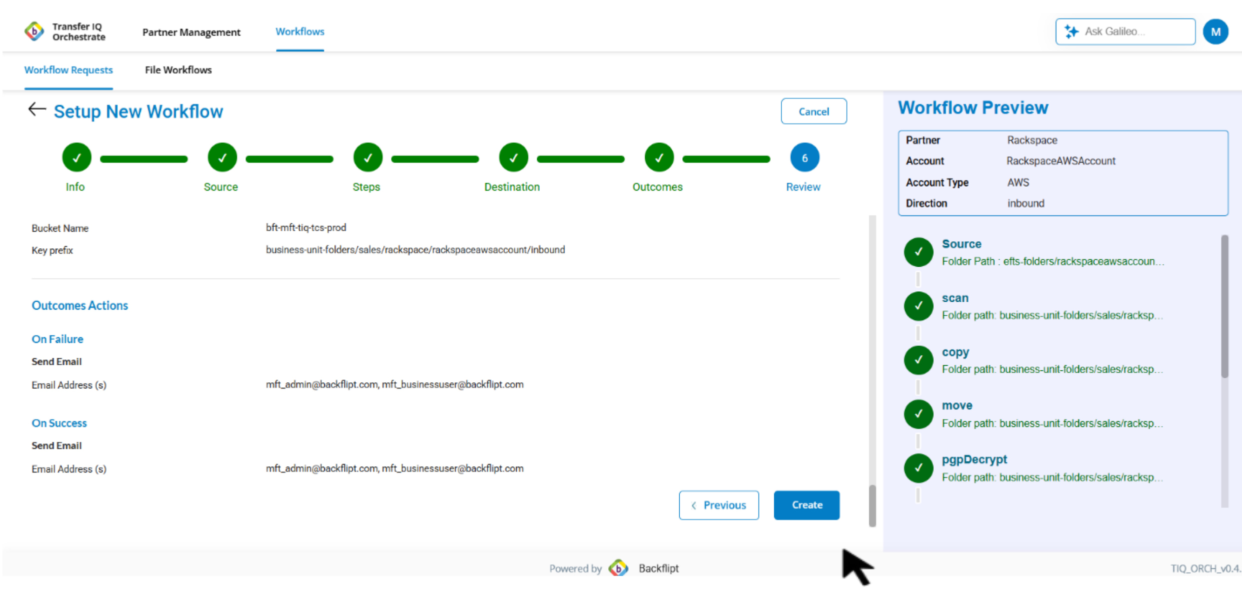
On Failure – Notify the email entered if the file transfer fails.

Note: Enter Comma Separated Emails to notify multiple emails

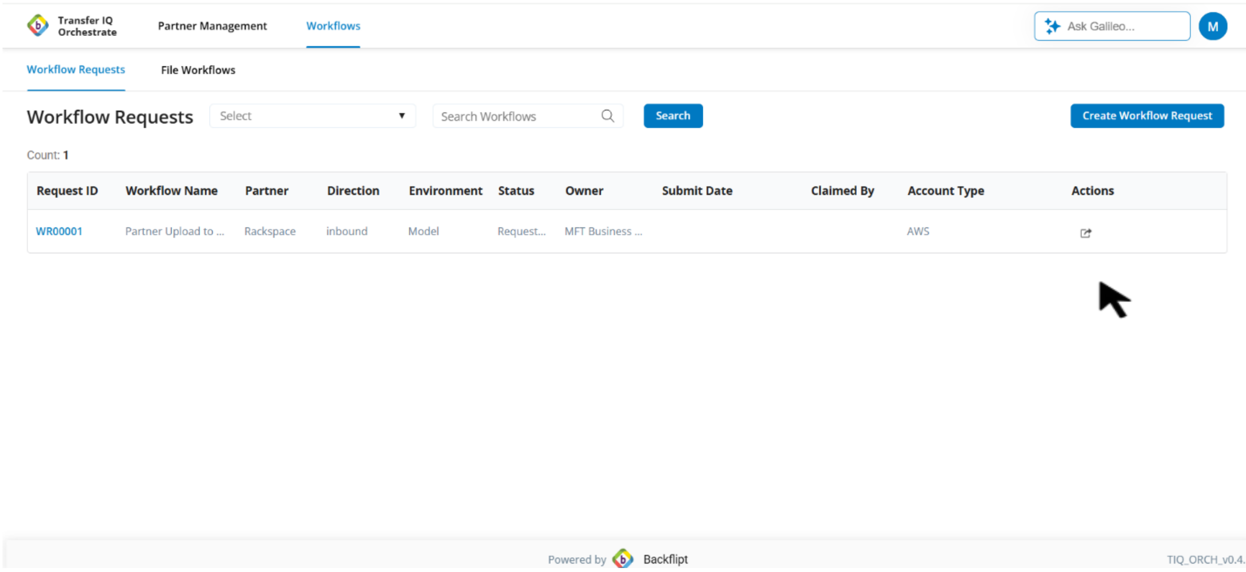


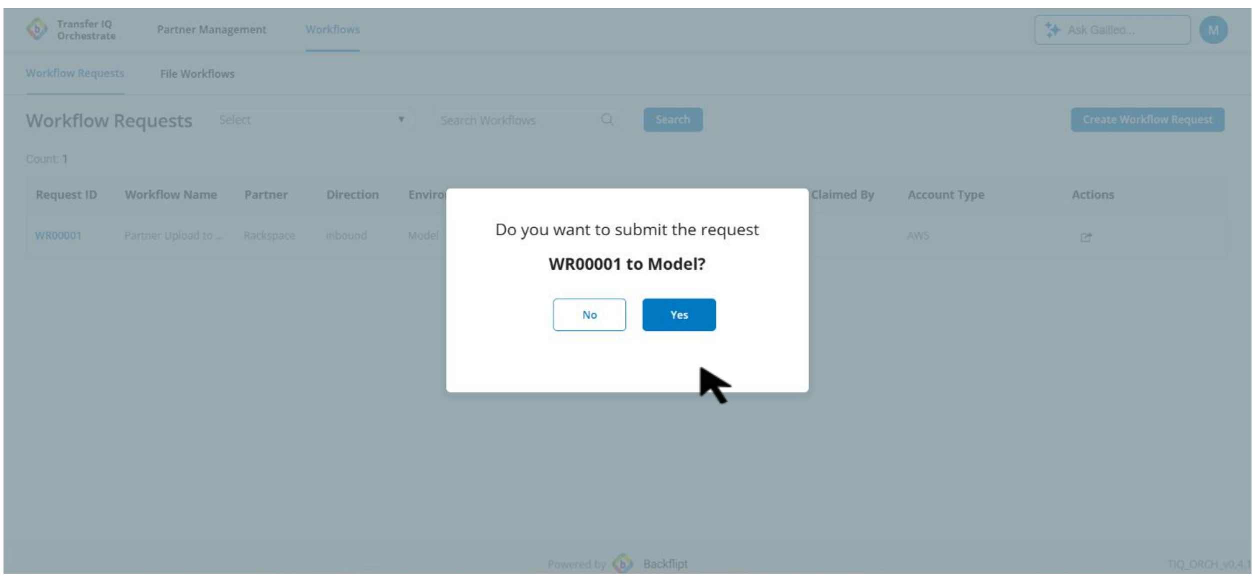
Review

Review all the details provided during the workflow request creation. If everything is correct, the Business User can proceed to create the workflow request. If any changes are needed, use the Previous button to go back and make edits



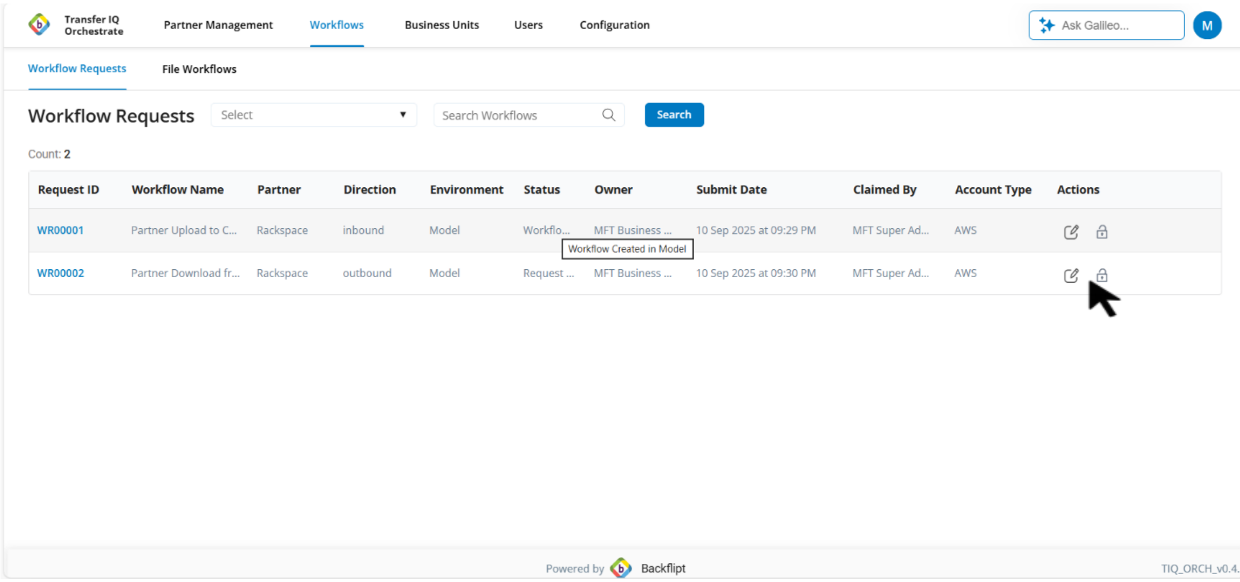
Once the workflow request creation is done, Business User submits the request to the admin for approval, it becomes visible to all admins under the Workflow Requests tab.





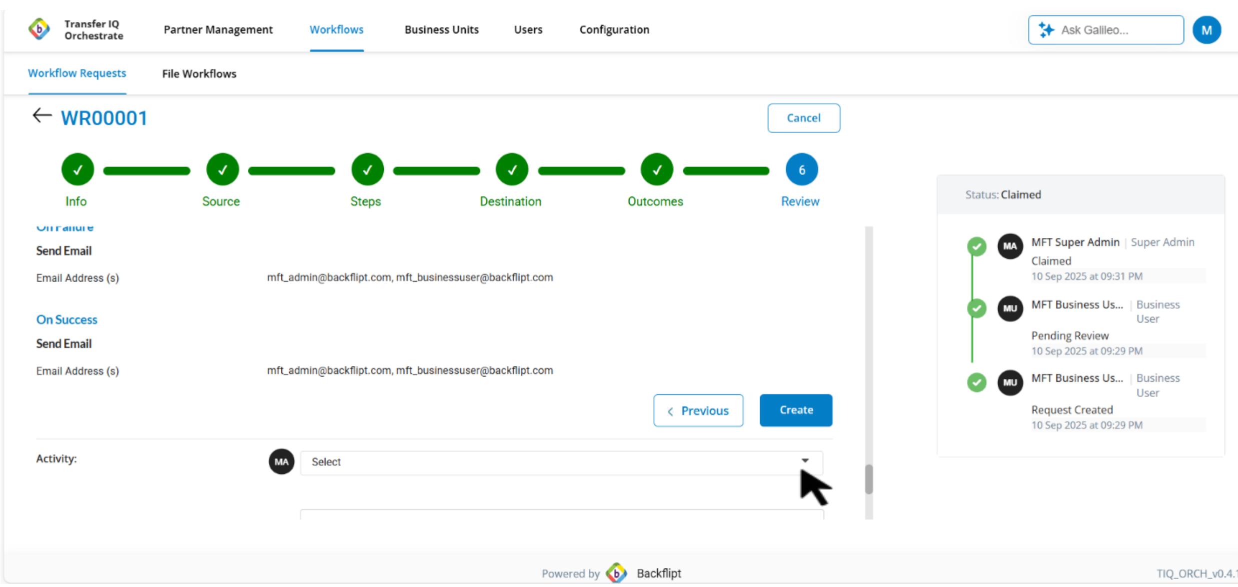
Admin Approval – AWS Inbound Workflow request

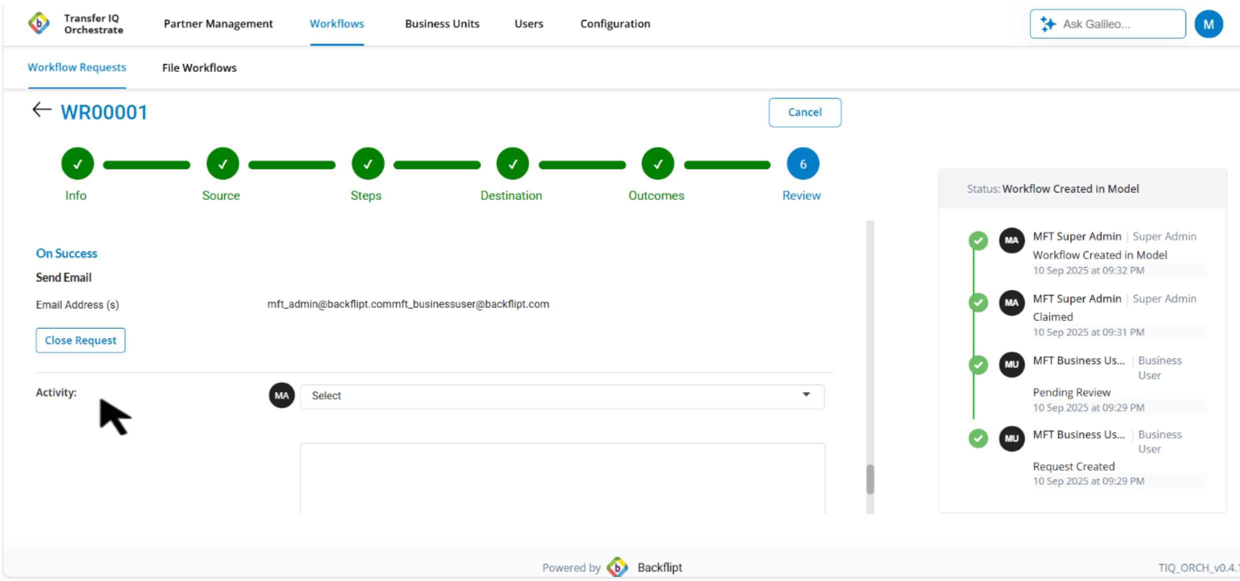
An admin can claim the request to take ownership in one of two ways: by clicking the View Request button in the email notification sent after submission, or by locating and claiming the request directly from the Account Onboarding tab.



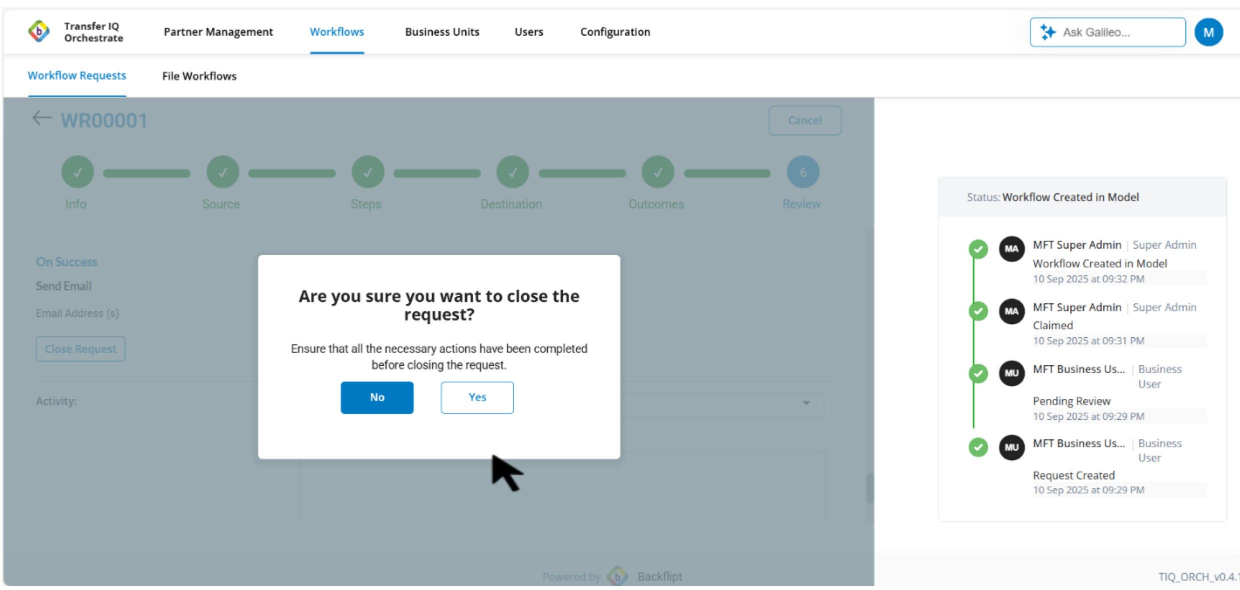
After claiming the request, the admin can view all the details provided by the Business User in edit mode. The admin has the option to review, modify, or update any information if changes are needed. If no changes are required, the details can be left as they are.

Click the Create button to create the workflow

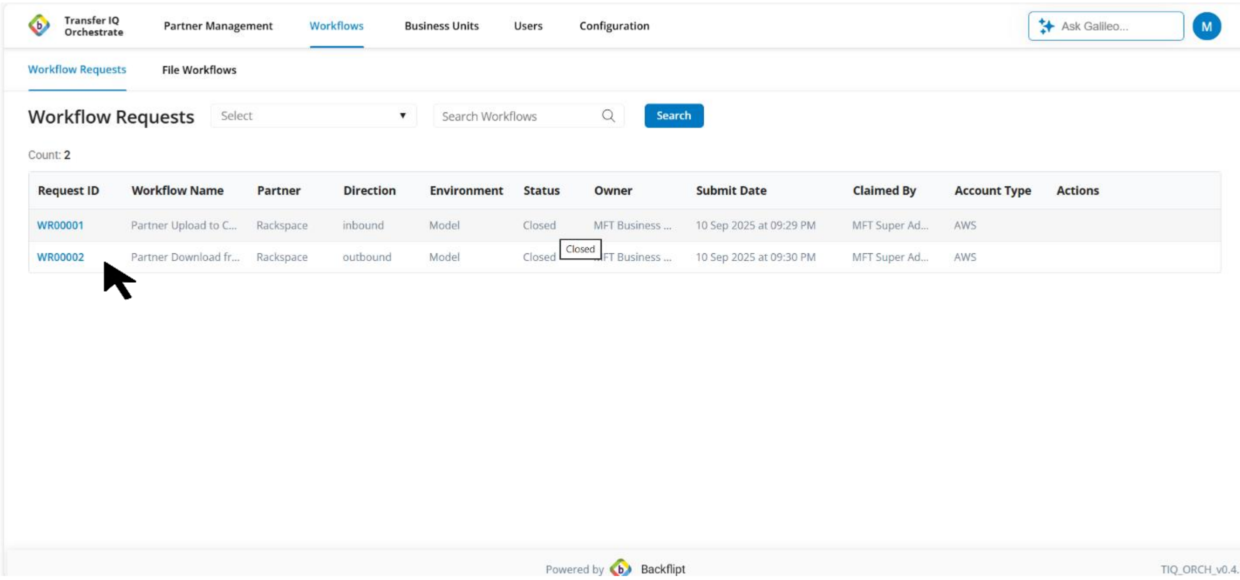




After the workflow is created, the admin can proceed to close the request, so no further action is required. Clicking on the **Close Request** button triggers a confirmation prompt.



Once confirmed, the request is marked as **Closed**, and the page redirects back to the Workflow Requests table, where the request is now listed with a status of **Closed.**



Add AWS Transfer Family Account Outbound Workflow

In the AWS Outbound Workflow, when a Business User from the company uploads a file to the specified source path, the workflow is automatically triggered. The file is processed through the defined transformation steps and then delivered to the destination specified in the workflow request.

To Create an AWS Inbound Workflow Business User Creates a Workflow Request with all the required details and submits the workflow request to the admin for approval.

Information (Info)

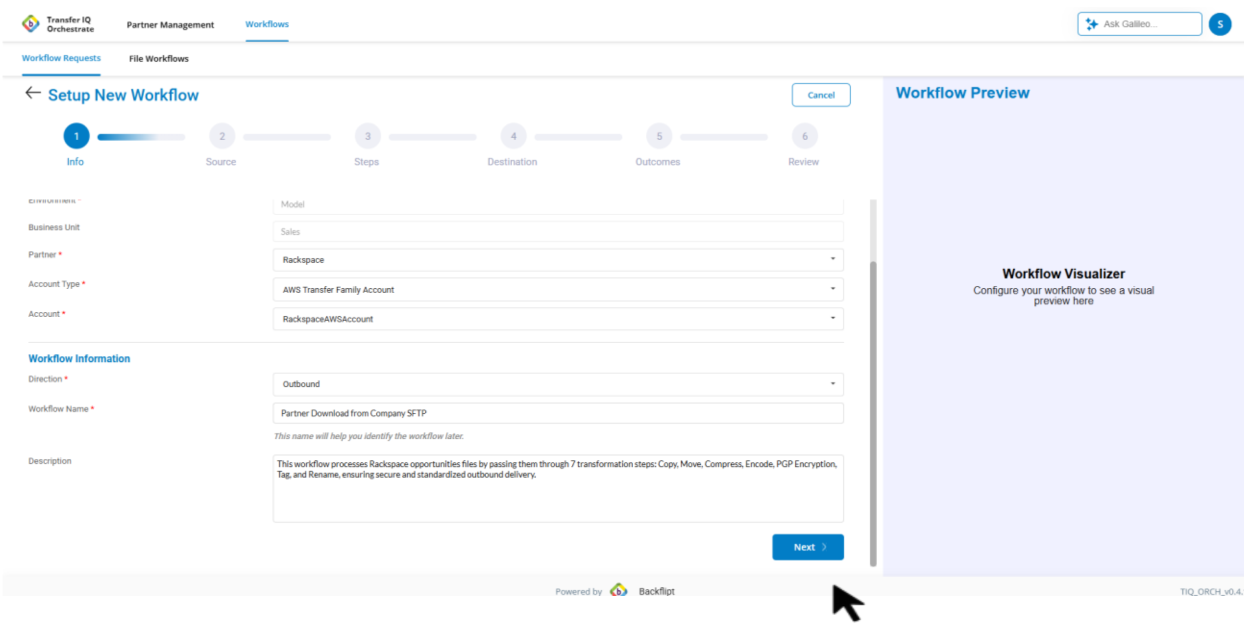
Provide the basic information about account and workflow in this section

This section contains the following fields

1. Environment – Auto populated with Model
2. Business Unit – Auto populated with the Business Unit assigned to the logged in Business User
3. Partner – A dropdown that consists of list of partners and it allows Business User to select a partner for whom the workflow needs to be created
4. Account Type – AWS Account
5. Partner Account – All the partner accounts created for the partner will be displayed in the dropdown, and allows to select a partner account out of all available options

Once the Partner Account is selected, the Workflow Information section is displayed to provide information about the Workflow with below fields

1. Direction – Select Outbound to create an Inbound Workflow
2. Workflow Name – An input field to Enter a Name for the workflow
3. Description – A field to provide a description about the workflow



Once all the information is done click the **"Next"** button to navigate to the Source Section

Source

The partner uploads the file to the source folder. All information regarding the source and trigger scheduling will be provided in the source section.

The Source Section Consists of the following section:

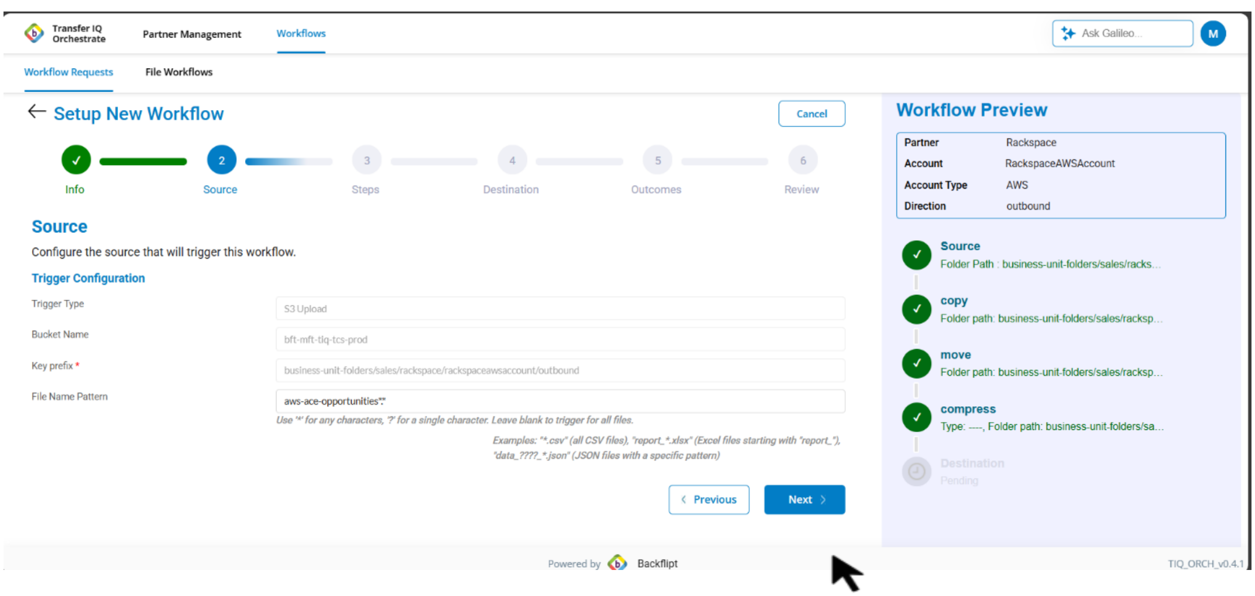
1. Trigger Configuration

Trigger Configuration:

This section provides details about the source folder and the file name pattern that should trigger the workflow.

The section consists of the following fields:

1. **Trigger Type** – Pre-filled with the “S3 Upload”
2. **Bucket Name** – Pre-filled with the name of the storage bucket configured in metadata settings (e.g., “**bft-mft-transferiq-qa**")
3. **Key Prefix** – Folder path where the partner uploads the file pre-filled with the path “{{Business Unit Folder}/{Business Unit}/{Partner}/{Partner Account}/{Direction}}”
4. **File Name Pattern** - Specify the file name or pattern that should trigger the workflow.
    a. You can either enter the **exact file name** (e.g., `Sales.pdf`) or use **wildcard characters** to define a pattern:
    b. `*` — Matches **any number of characters**
    c. `?` — Matches **exactly one character**
    d. **Examples:**
    e. `*.*` – Triggers the workflow for **any file**, regardless of name or extension
    f. `*.csv` – Triggers for any file with a `.csv` extension, such as `data.csv` or `report.csv`
    g. "report_*.xlsx" (Excel files starting with "report_")
    h. `data_????_*.json` – Triggers for JSON files that follow a specific pattern: the file name must start with `data_`, followed by **exactly four characters.**
    i. Simply leave blank to trigger for all files



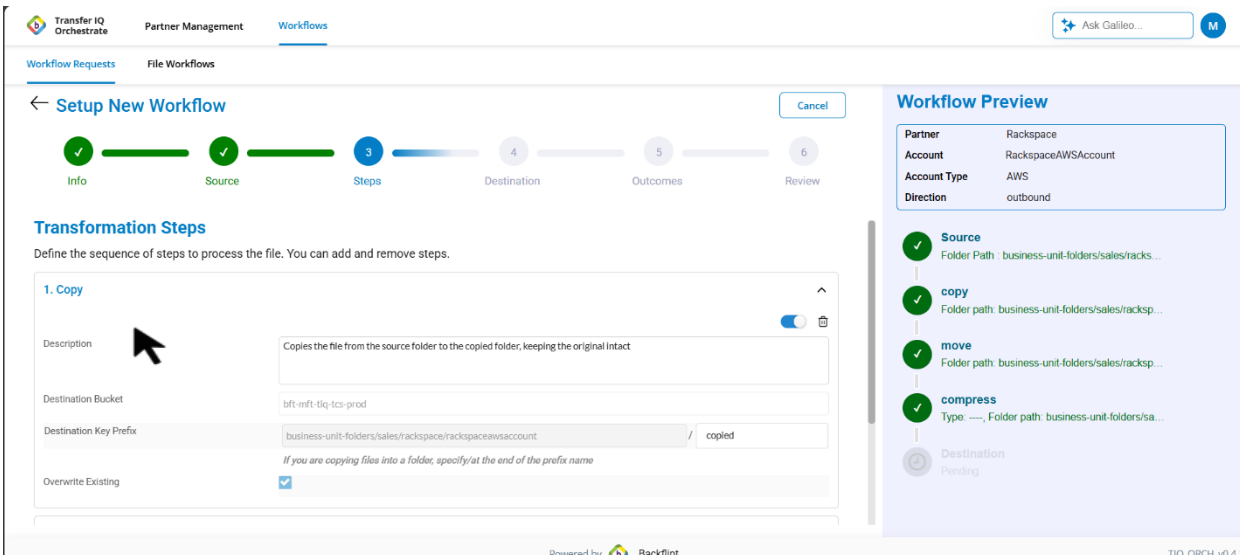
After providing all mandatory details, click Next to continue to the Steps Section

Steps:

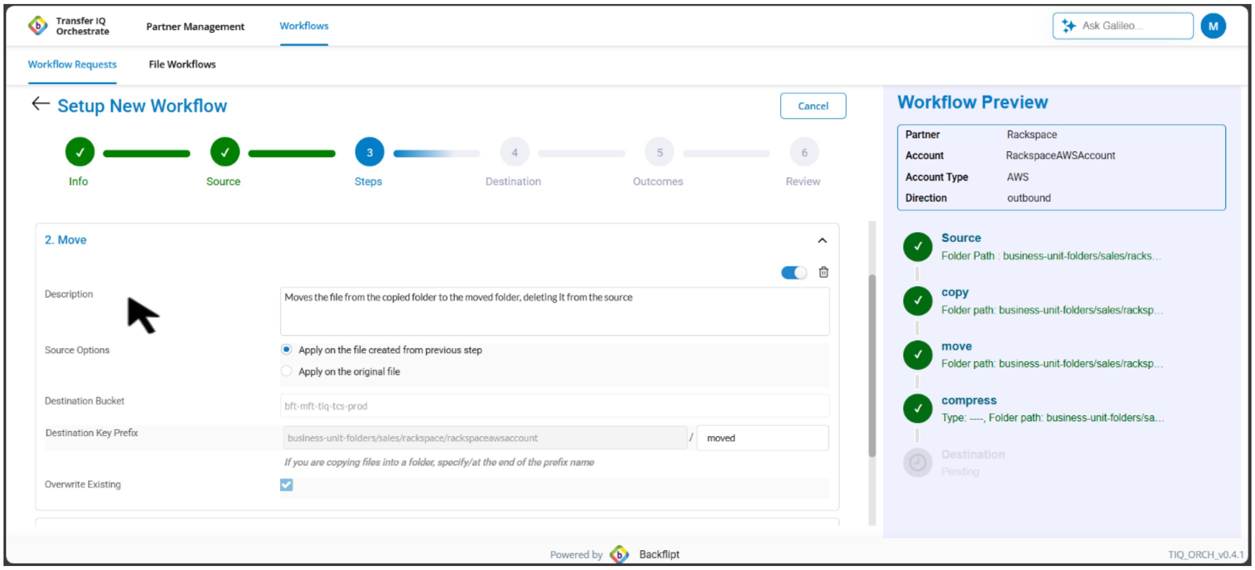
There are different Steps in the EFTS Outbound Workflow. Once the workflow is triggered the all the steps configured in the steps section will be executed and the file will be placed in the destination section:

The Steps Available in The EFTS Outbound Workflows are as follows

Copy - The copy step duplicates a file from the source location to the destination without deleting the original. This ensures the file remains accessible in both locations.

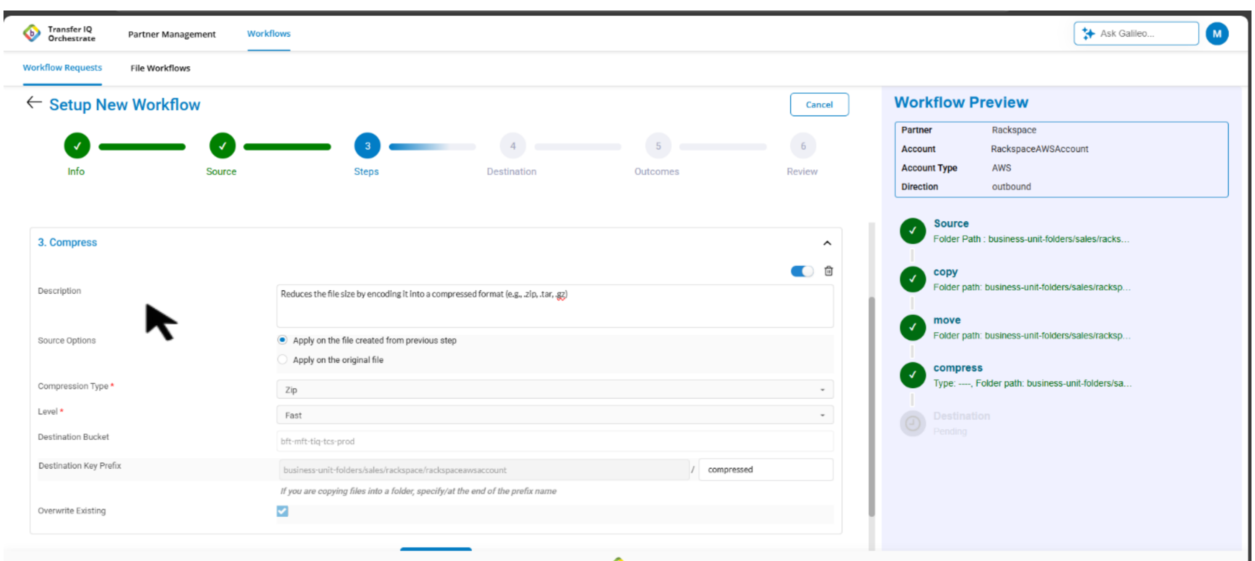


Move - The move operation shifts a file from the source location to the destination. Once moved, the file no longer exists in the source location.



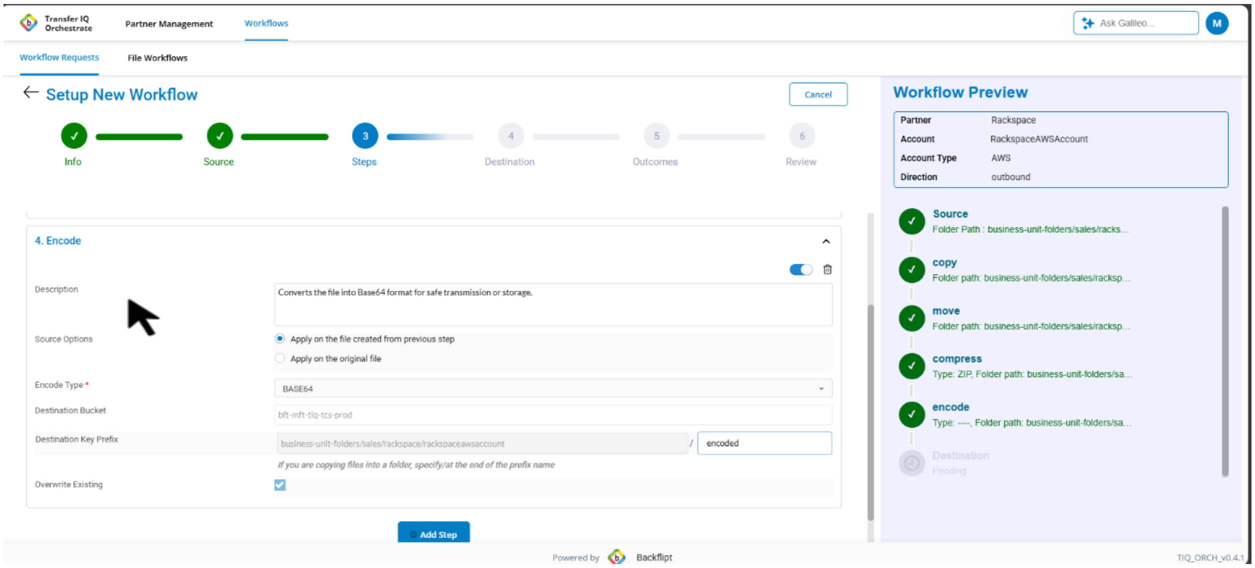
Compress:

Compression reduces the overall size of a file or folder by applying algorithms that represent the same data more efficiently. This helps save storage space and improves transfer speed over networks. Common compressed formats include `.zip`, `.tar`, and `.gz`. Compression can be either **lossless**, where no data is lost, or **lossy**, where some data is discarded to achieve higher reduction.



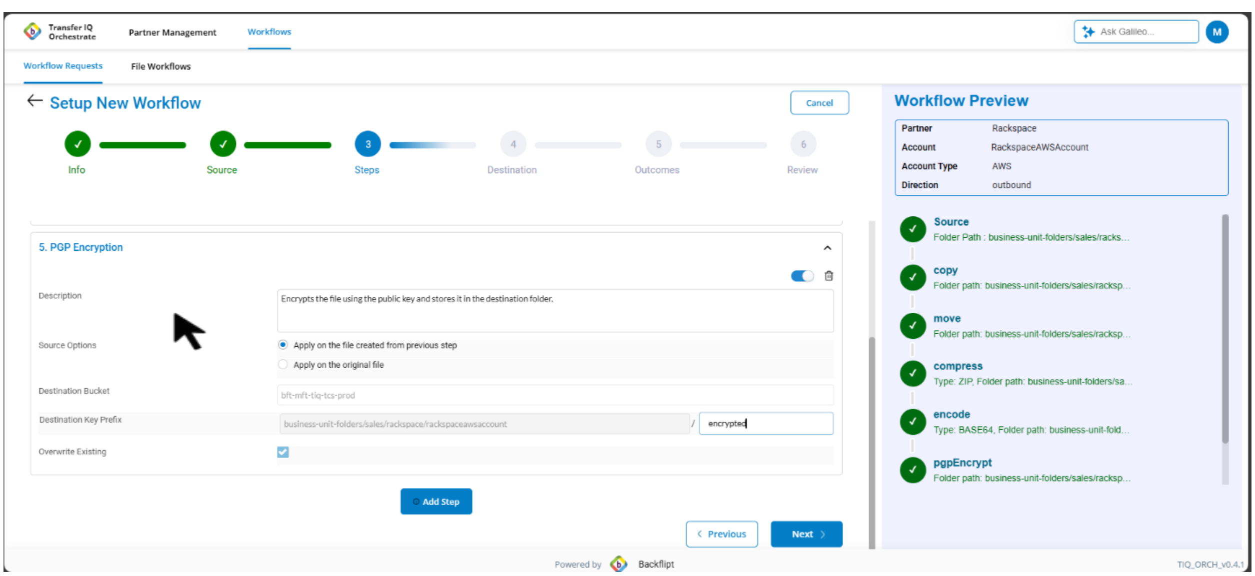
Encode:

Encoding transforms data from one representation to another to ensure compatibility, integrity, or security during storage or transmission. For example, **Base64 encoding** converts binary data into text characters so it can be safely transmitted in systems that only support text. While encoding preserves the original information, it usually increases file size and is not intended for data compression.



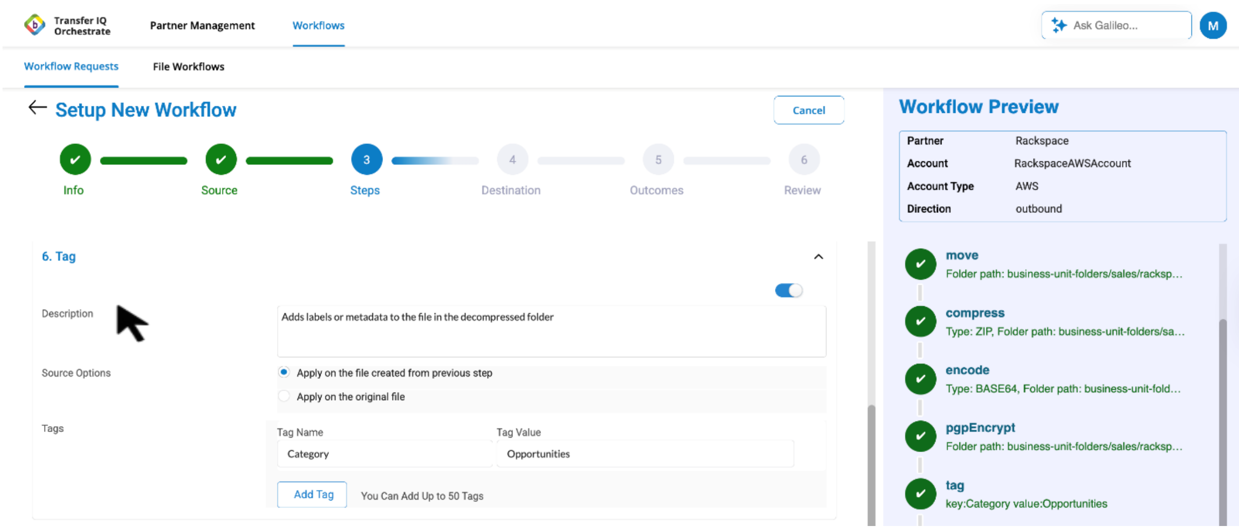
Encrypt:

Encryption is the process of converting readable data (plaintext) into an unreadable format (ciphertext) to protect it from unauthorized access. In the context of **PGP (Pretty Good Privacy) encryption**, a file from the source location is encrypted using the recipient's **public key**. Once encrypted, only the corresponding **private key** can decrypt and access the file. The encrypted file is then moved to the specified destination, ensuring secure transmission and storage. Encryption does not reduce file size but focuses on **data confidentiality and security**.

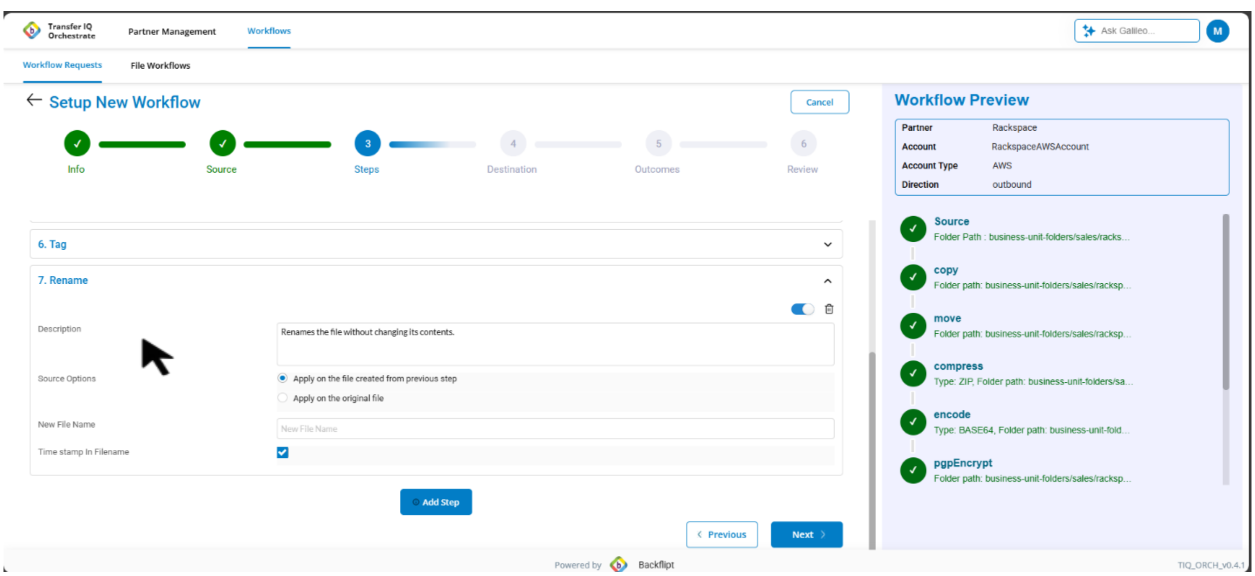


Delete - The **delete step** removes a file from its source permanently. This step is typically used to clean up files after they are no longer needed

Tag - The tag step allows adding additional information to files in the form of key-value pairs. This extra info helps describe, organize, and manage them more effectively. Up to 50 tags can be added per file.



Rename - The **rename step** changes the name of a file. This helps organize files by giving them clear, consistent, or updated names without altering their content or location.



For all the above steps there are toggling bar

- Disabled steps will be ignored during workflow execution

- Caret symbols (^) and (v) are displayed for each step, allowing the user to expand or collapse the steps as needed.

The fields available after adding **Copy, Move, Encrypt, Compress** and **Encode** steps are listed below.

- **Description** – A detailed description about the step added
- Source Options Consists of two options
  - **Apply on Original File** – When selected, the step will be executed on the original file located in the source.
  - **Apply on File Created from Previous Step** – When selected, the step will be executed on the output generated by the previous step.
- **Bucket Name**: Pre-filled with the name of the storage bucket configured in metadata settings (e.g., "**bft-mft-transferiq-qa**")
- **Destination Key Prefix -** The folder path or prefix within the destination bucket where the files will be placed (e.g., `Business Unit Folder/sales/{Partner}/{Partner name}`).
- In addition to this, a custom folder can be specified in the input field next to the Destination Key Prefix. The final file location will be the combination of the key prefix path plus the custom folder entered, determining exactly where the file will be stored when the step is executed.
- **Overwrite Existing** – This checkbox is enabled by default. If a file with the same name and extension already exists, it will be overwritten.

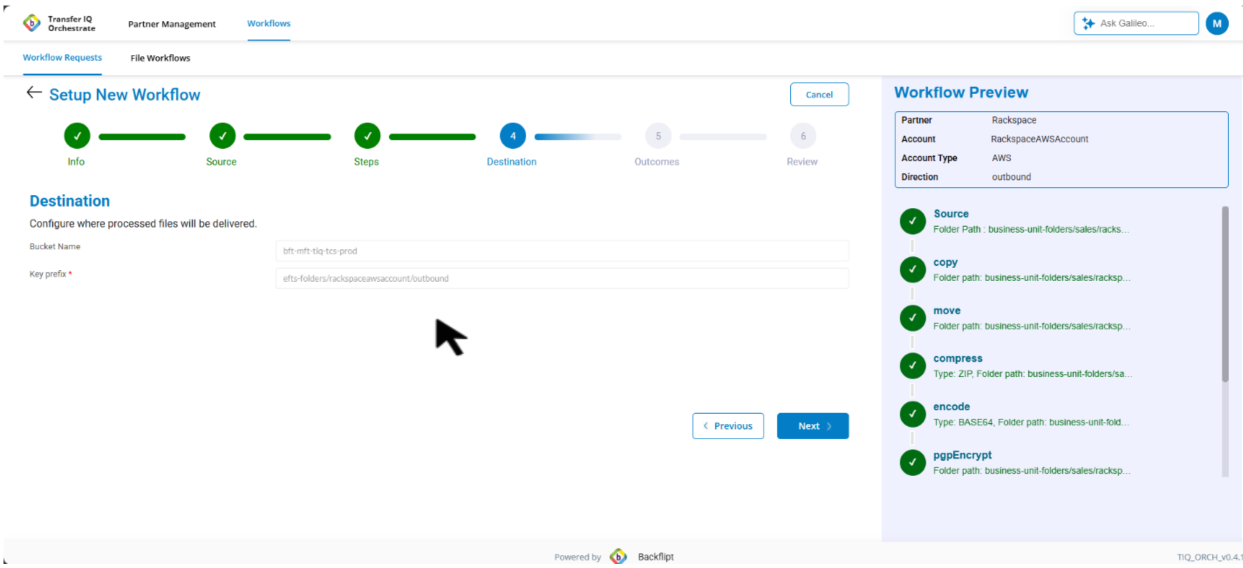
The fields available after adding **Delete, Rename** and **Tag** steps are listed below.

- **Description** – A detailed description about the step added
- Source Options Consists of two options
  - **Apply on Original File** – When selected, the step will be executed on the original file located in the source.
  - **Apply on File Created from Previous Step** – When selected, the step will be executed on the output generated by the previous step.
- **Bucket Name**: The name of the storage bucket configured in metadata settings.
- **Overwrite Existing** – This checkbox is enabled by default. If a file with the same name and extension already exists, it will be overwritten

Note: Since no destination key prefix is provided, the rename and tag will be applied to the path or folder from the previous step.

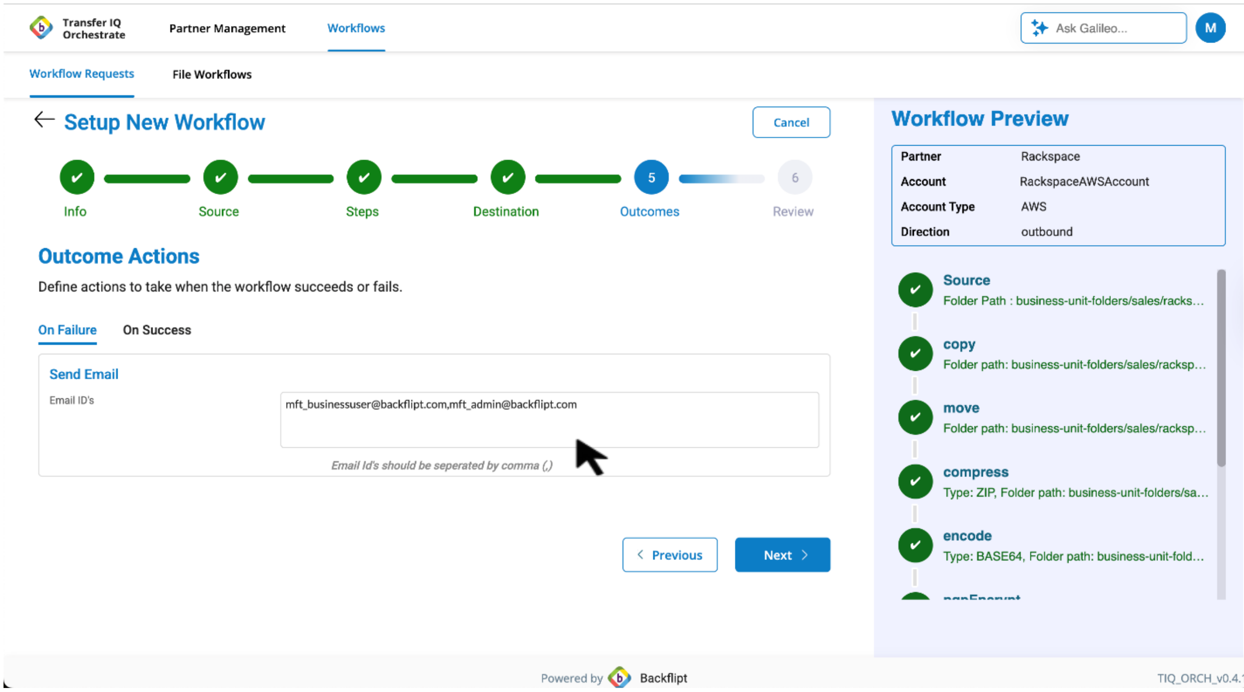
Destination:

1. **Bucket Name** - Pre-filled with the name of the storage bucket configured in metadata settings (e.g., “**bft-mft-transferiq-qa**")
2. **Key Prefix** – The folder path where the uploaded files will be placed in the destination. (e.g., “{{EFTS-Folder}/ {Partner Account}/{Direction}} ")



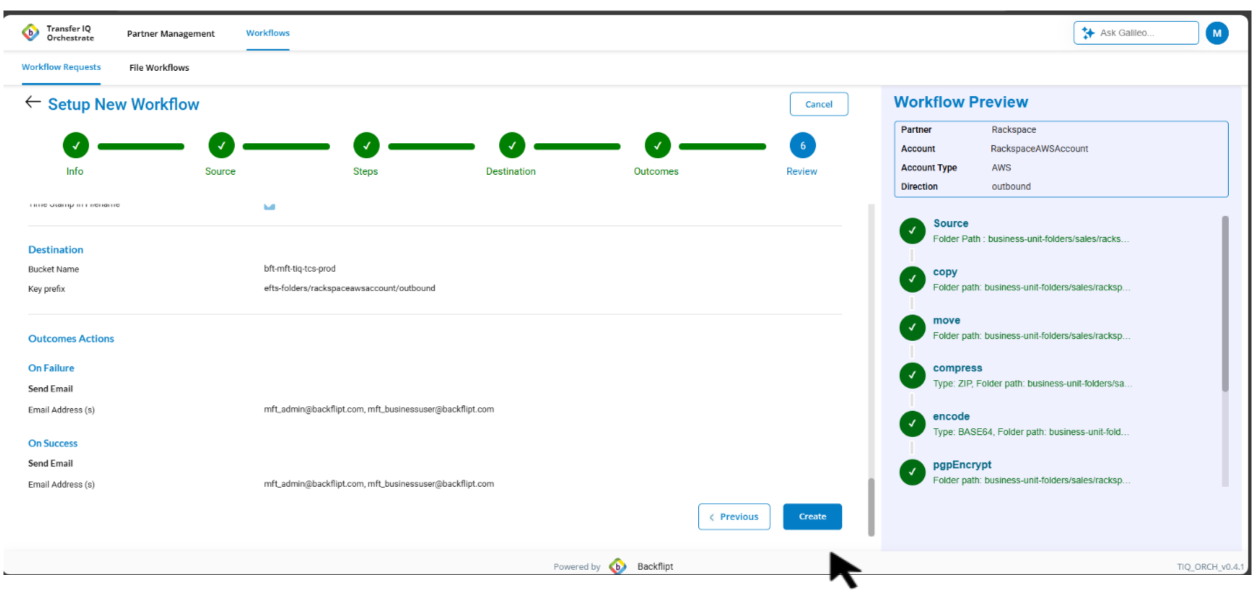
Outcome Actions:

Users can add email addresses in both the ‘**On Success**’ and ‘**On Failure**’ tabs. When the workflow completes, the specified recipients will receive notifications indicating whether the workflow execution was successful or failed

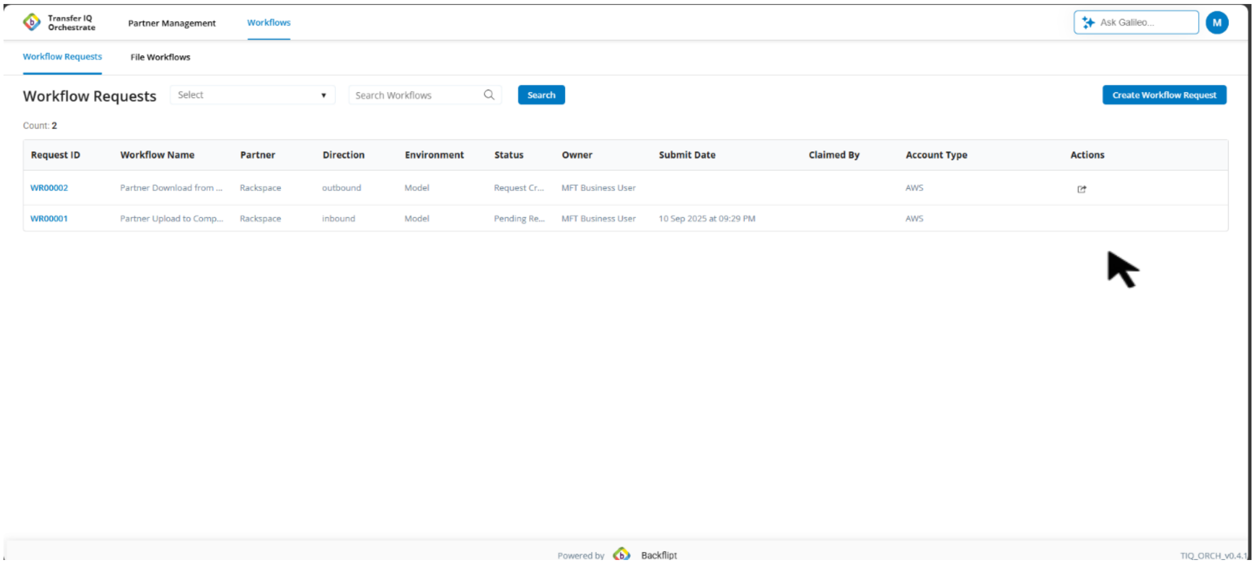


Review Section:

In View mode, all workflow details and configured steps up to the then displayed, enabling the user to thoroughly review the configuration prior to creating the workflow



Once the workflow request creation is done, Business User submits the request to the admin for approval



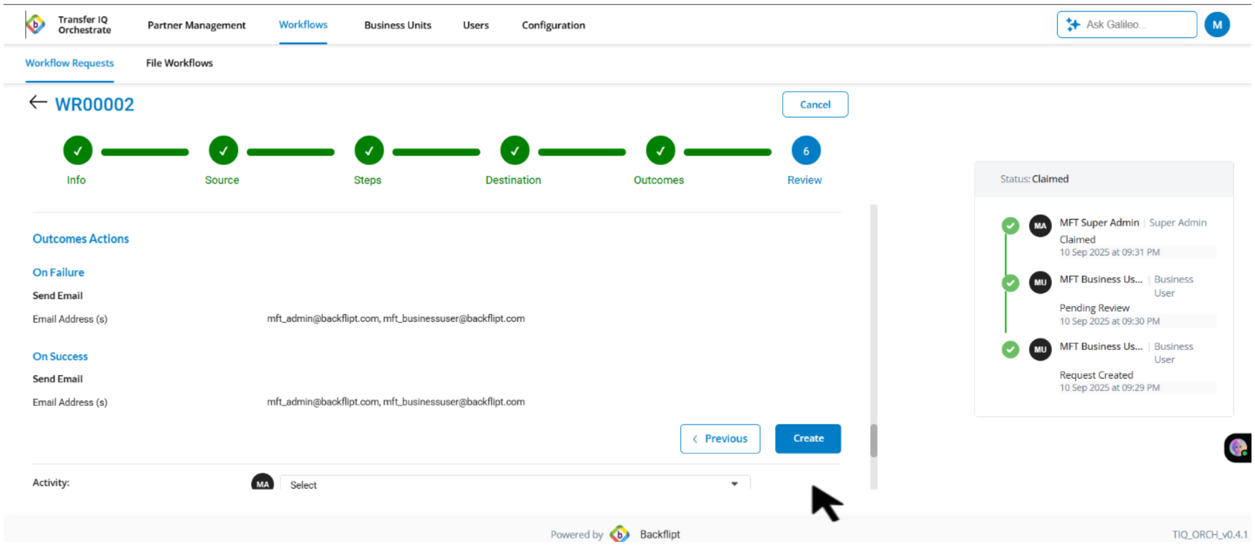
It becomes visible to all admins under the Workflow Requests tab.

Admin Approval – AWS Outbound Workflow request

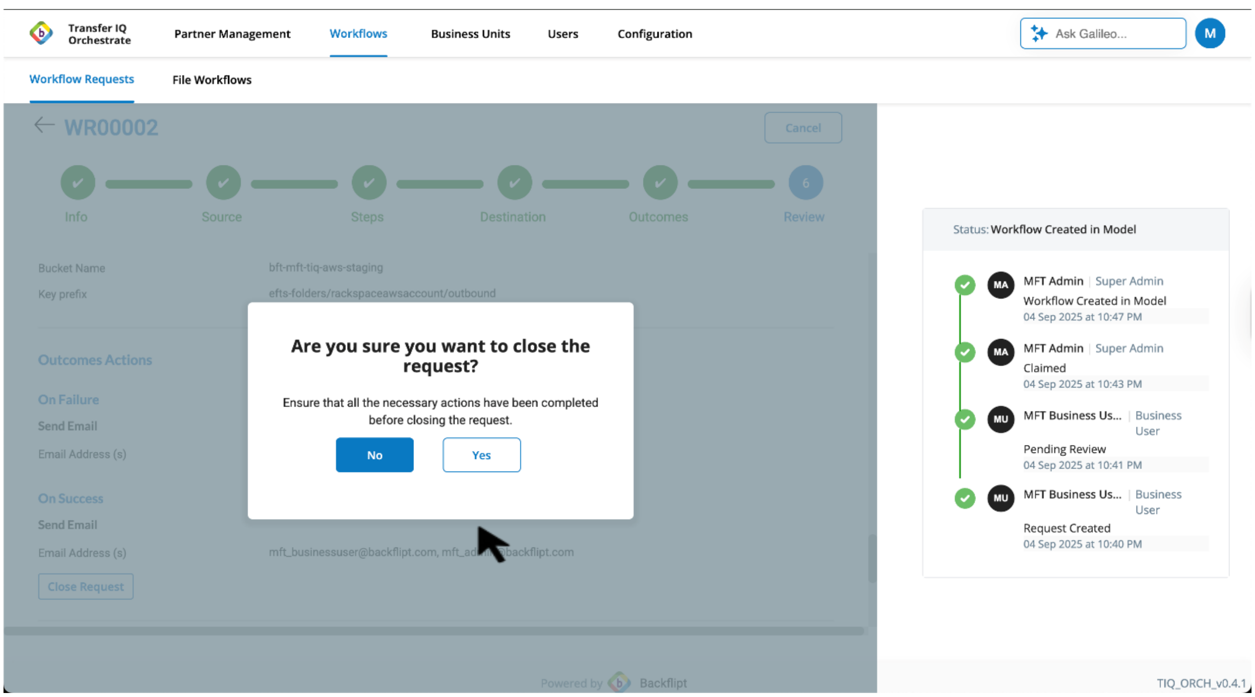
An admin can claim the request to take ownership in one of two ways: by clicking the View Request button in the email notification sent after submission, or by locating and claiming the request directly from the Account Onboarding tab.

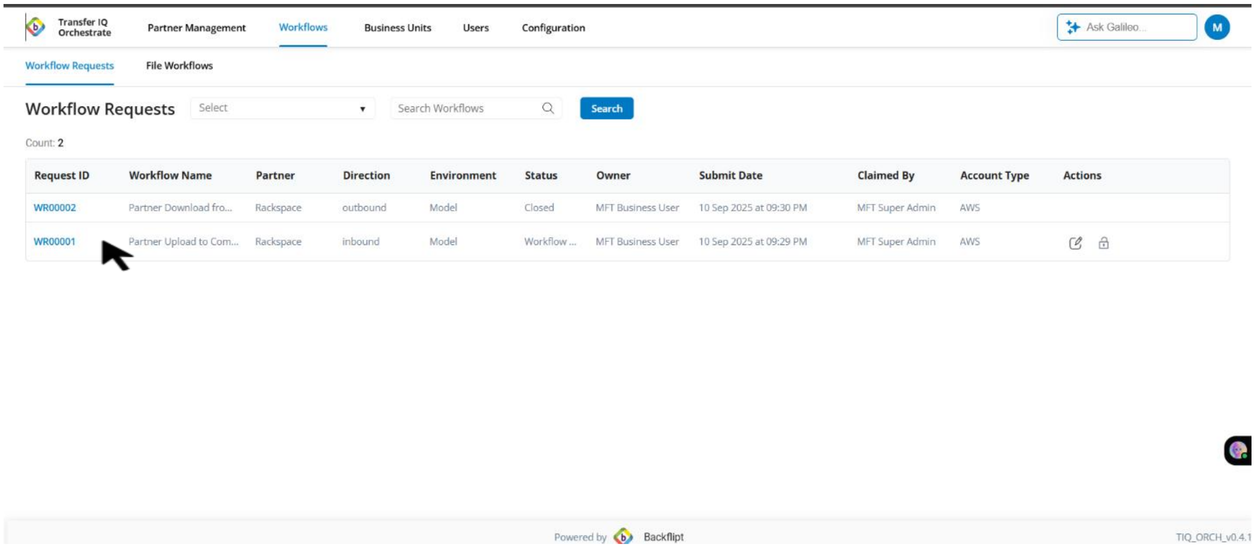
After claiming the request, the admin can view all the details provided by the Business User in edit mode. The admin has the option to review, modify, or update any information if changes are needed. If no changes are required, the details can be left as they are.

Click the Create button to create the workflow



After the workflow is created, the admin can proceed to close the request, as no further action is required. Clicking on the **Close Request** button triggers a confirmation prompt. Once confirmed, the request is marked as **Closed**, and the page redirects back to the Workflow Requests table, where the request is now listed with a status of **Closed**.





Add Partner Account (Partner SFTP Hosted)

Business User Initiates Partner Onboarding Request (Business User Submission to Admin)- Partner Account

In the **Partner Hosted Account** type, the partner provides details of partner's own SFTP server where the account exists. Using this information, an account is created in the application to connect to the partner's external SFTP server through **AWS SFTP Connectors**.

While creating the connector, two login methods can be used for authentication:

1. **Password**
2. **SSH Key**.

In the password-based login method, the partner provides a username and password for partner's SFTP server. The company uses these credentials to access the partner's server.

In SSH key-based login method, the company generates a pair of SSH keys consisting of a **public key** and a **private key**, which are stored in the **MFT Settings** tab of the application. The **public key** is shared with the partner. The partner attaches this public key to the relevant user account on partner's SFTP server to allow key-based authentication.

To connect to the partner's server, the company uses the company's **private key** that matches the shared public key.

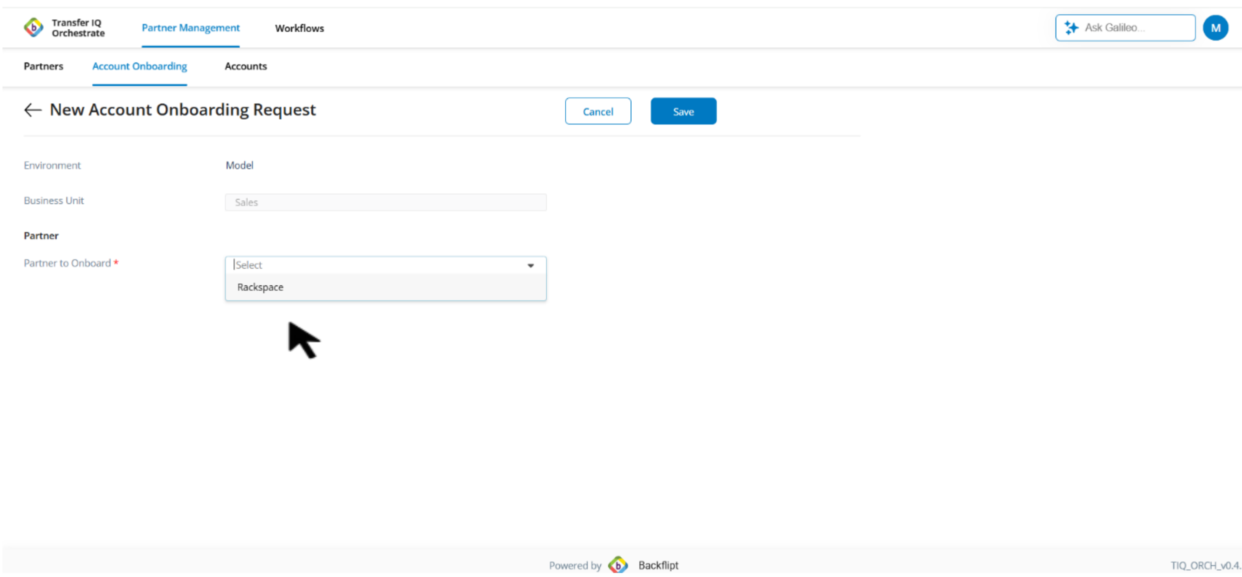
Partner Hosted Account

To Create a Partner Hosted Account with Password Login Type, Business Users click the **Account Onboarding** tab and click on "**New Onboarding Request**" button, they are redirected to the New Account Onboarding Request Form. In this form, the user sees two fields:

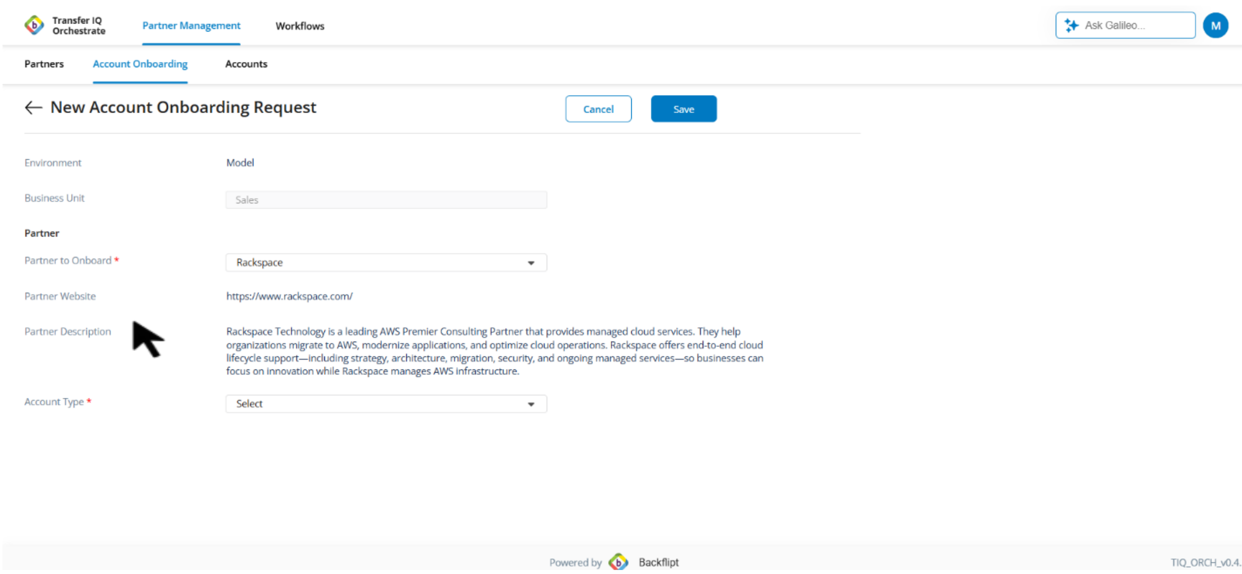
• **Environment** (pre-filled with "Model")

• **Business Unit**, (pre-filled with the business unit which is associated to that Business User)

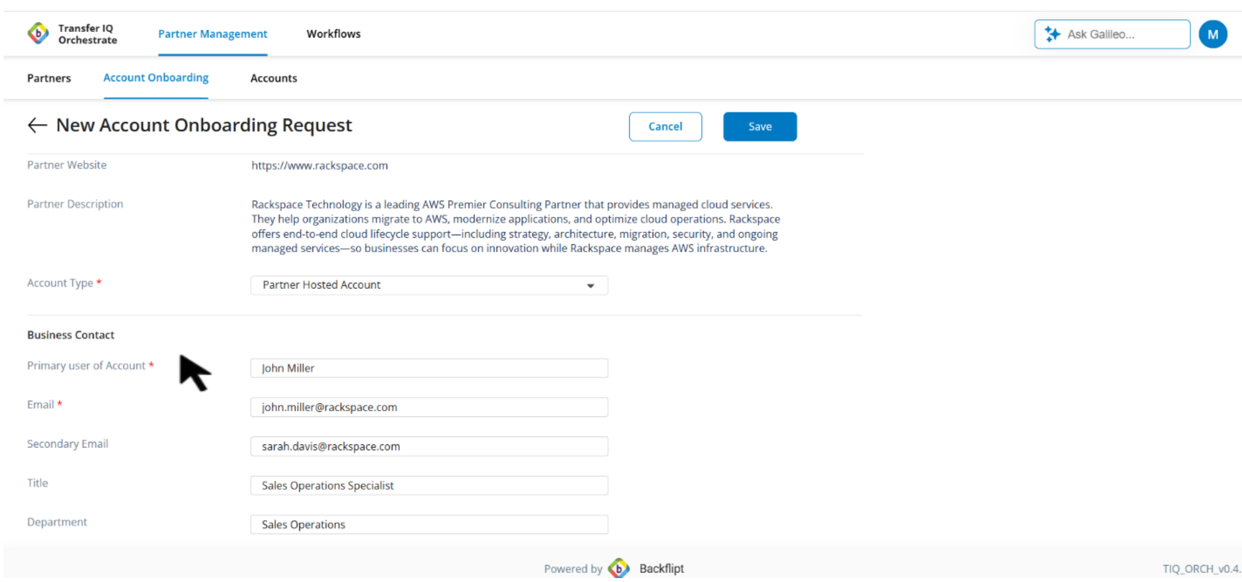
• **Partner to Onboard**, which is a dropdown where the user selects the partner profile



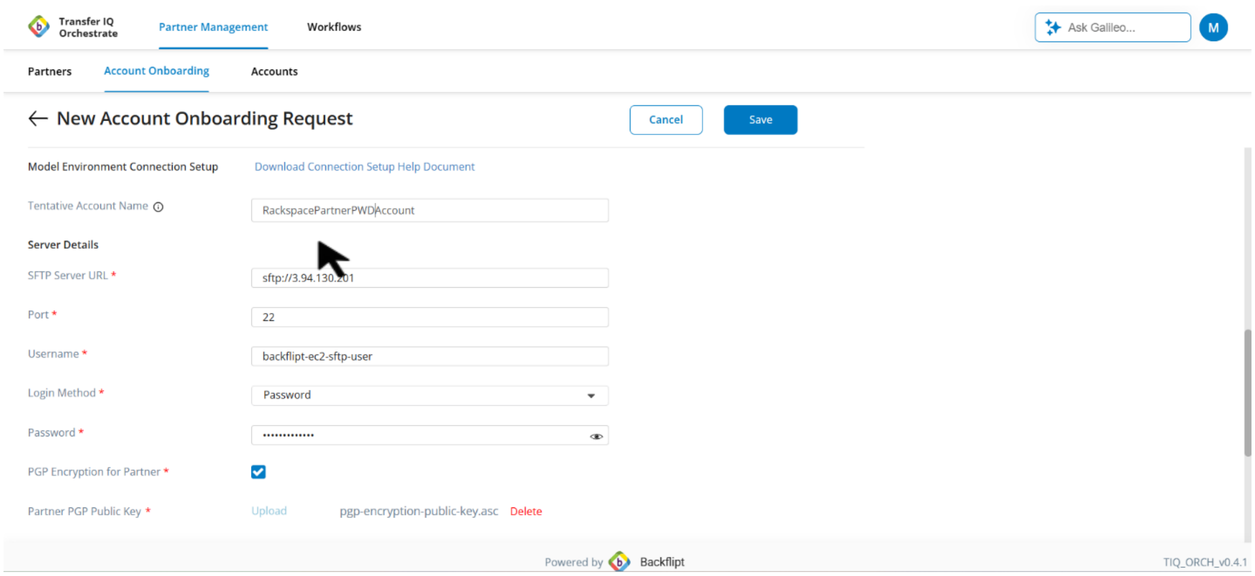
1. After selecting the Partner, partner details like Partner website and Partner Description fields are displayed and these cannot be edited, these fields are read-only mode.



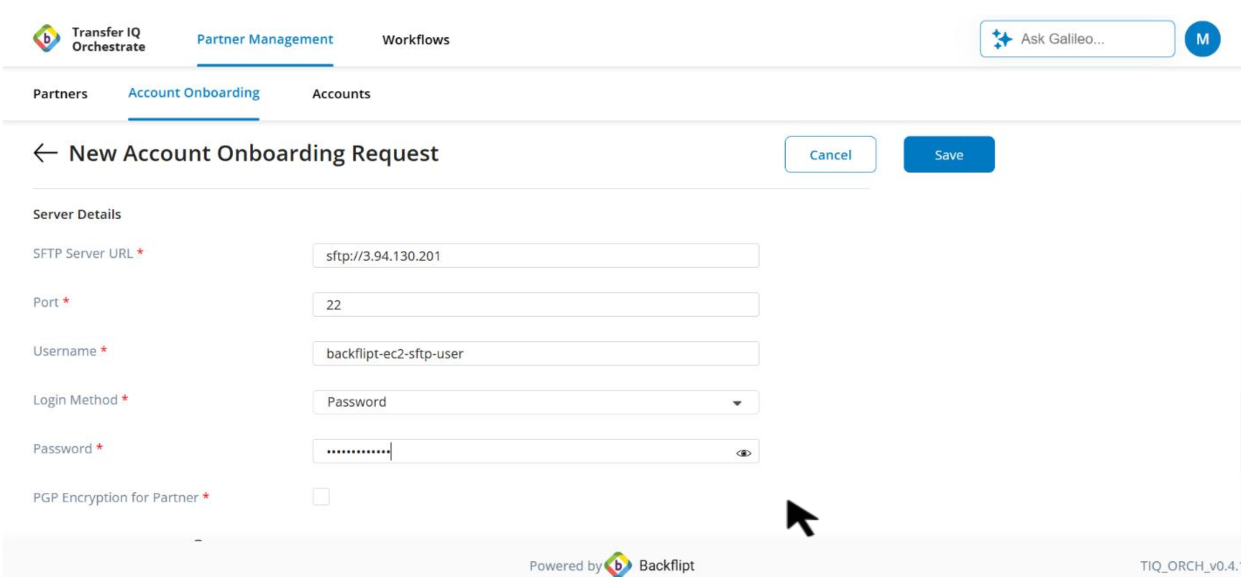
2. Once the account type is selected, the **Business Contact Form** is displayed. The Business User must fill in all mandatory fields with valid data. If any required information is missing or incorrect, an error message will appear when attempting to save the onboarding request.



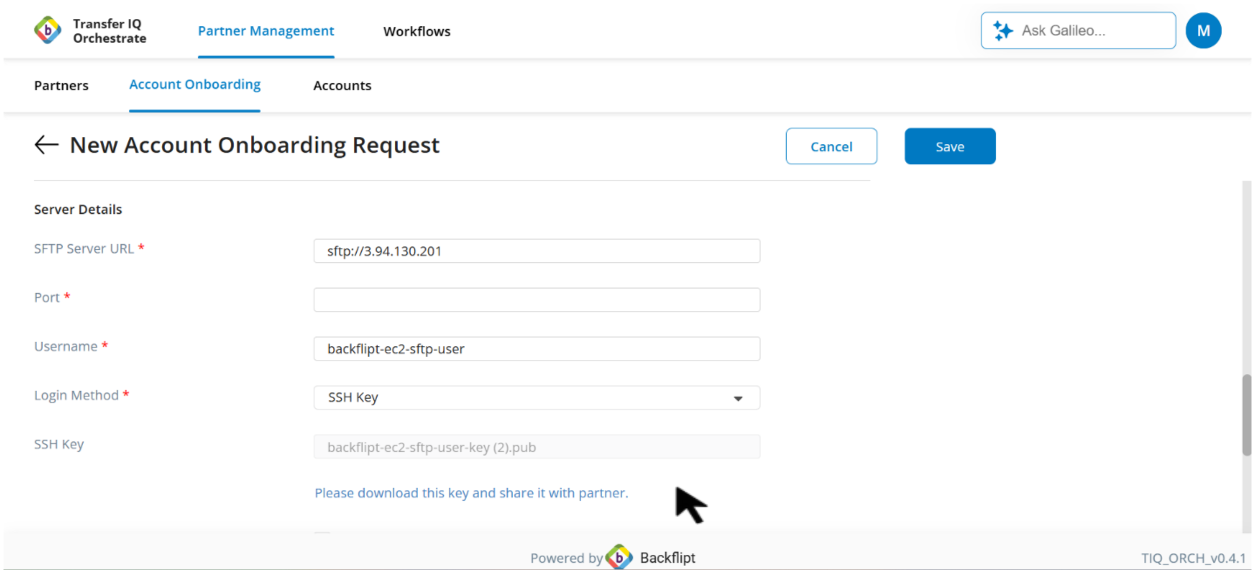
3. **Tentative Account Name**: To give any account name, The Business User may suggest an account name. The IT Admin may use this name when creating the account by the Business User. This field is not mandatory



4. After completing the contact form and giving the tentative account name, the Business User must provide the **partner's server details** in the following fields:
   a. **Server URL** – Must begin with **sftp://**
   b. **Port** – A valid port number used by the partner's SFTP server
   c. **Username** – The username of the account on the partner's server
   d. **Login Method** – Choose between **Password** or **SSH Key**
   e. If **Password** is selected as the login method, an additional field will appear to enter the password associated with the provided username.

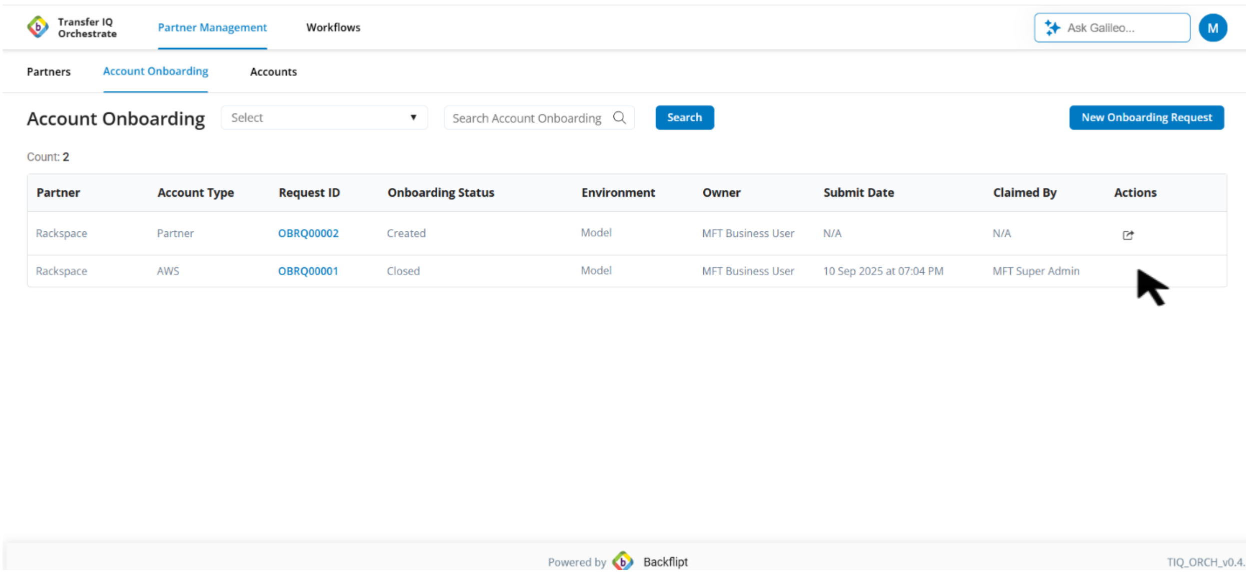


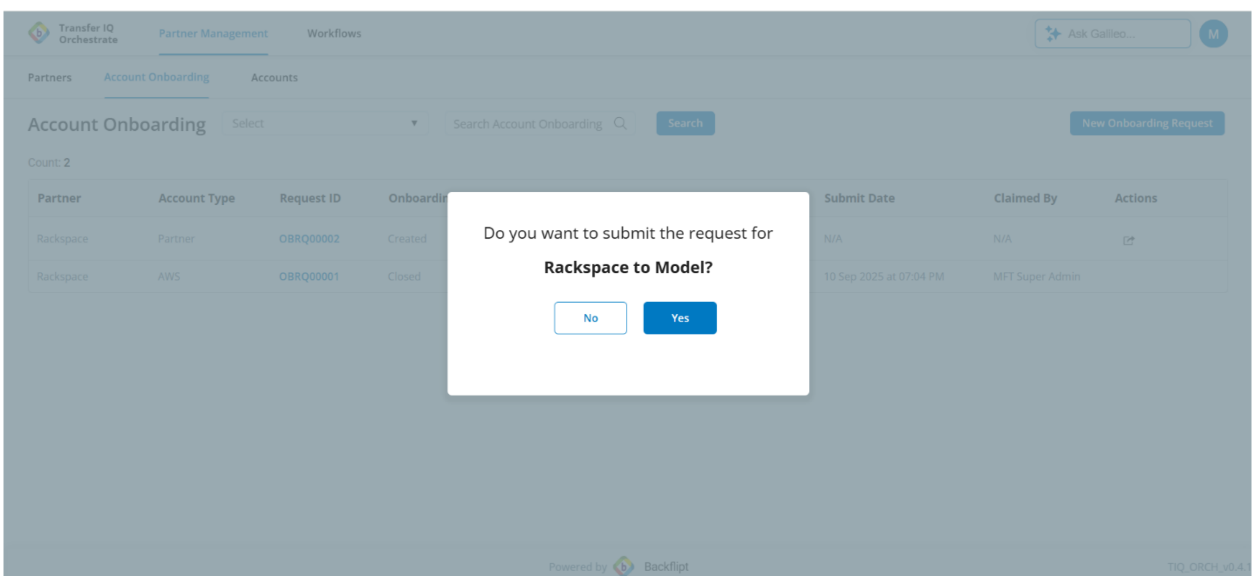
f. If **SSH Key** is selected, the SSH key uploaded in the **MFT Settings** tab will be used. This key will later be shared with the partner, who must attach it to the user account on their SFTP server to allow connection.



5. **Note:** It is important to ensure that the server details provided are accurate and that the partner's server supports the selected login method. Incorrect service configuration may result in connection failures
6. Below the server details section, there is a checkbox labeled **"PGP Encryption for Partner."** When selected, it allows the Business User to upload the **PGP encryption public key** provided by the partner
   a. When the company needs to send encrypted files to the partner, the Business User must upload the **PGP public key** provided by the partner. Only files with the **.asc** extension containing valid PGP public keys are accepted during the upload process.
   b. When a partner wants to send files to a company, the partner will use the company's PGP public key and encrypt the files and send them to the company. To decrypt the files sent by the partner, the company will use the company's PGP private key and decrypt the files received from the partner. This key is auto populated when the form is filled by the Business User.
7. There are two optional fields: **Additional Details** and **File Attachment**. These are not mandatory, but if the Business User wants to share extra information or upload supporting documents for the admin, Business User can use these fields to provide that additional input.

Once all the details are given, the Business User saves the onboarding request by clicking the save button. Once the request is saved the request will be visible in the Account Onboarding Tab table view with a submit button to submit the request to the admin for approval. Once the request is submitted all the admins are notified about the request submission

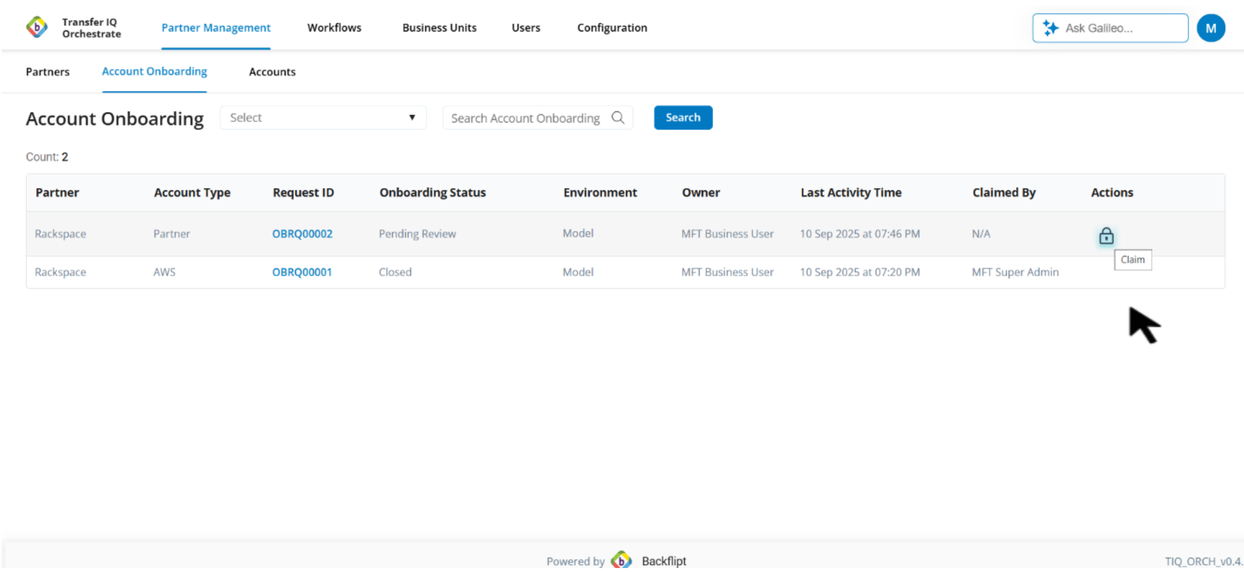


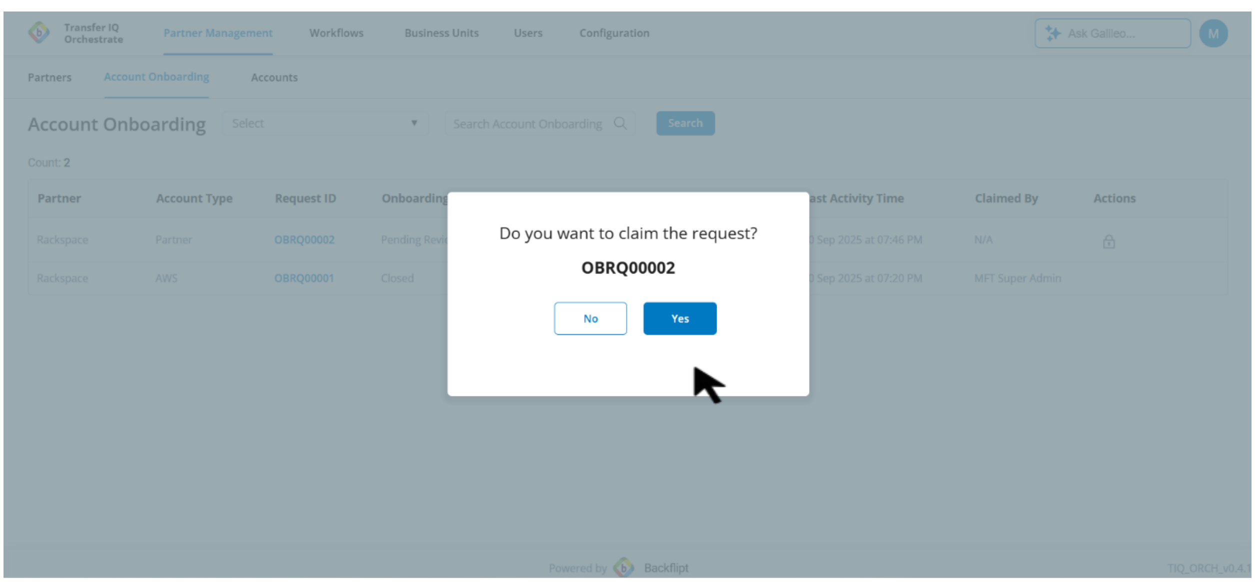


Admin Approves Partner Onboarding Request and Onboards Partner with Partner Account:

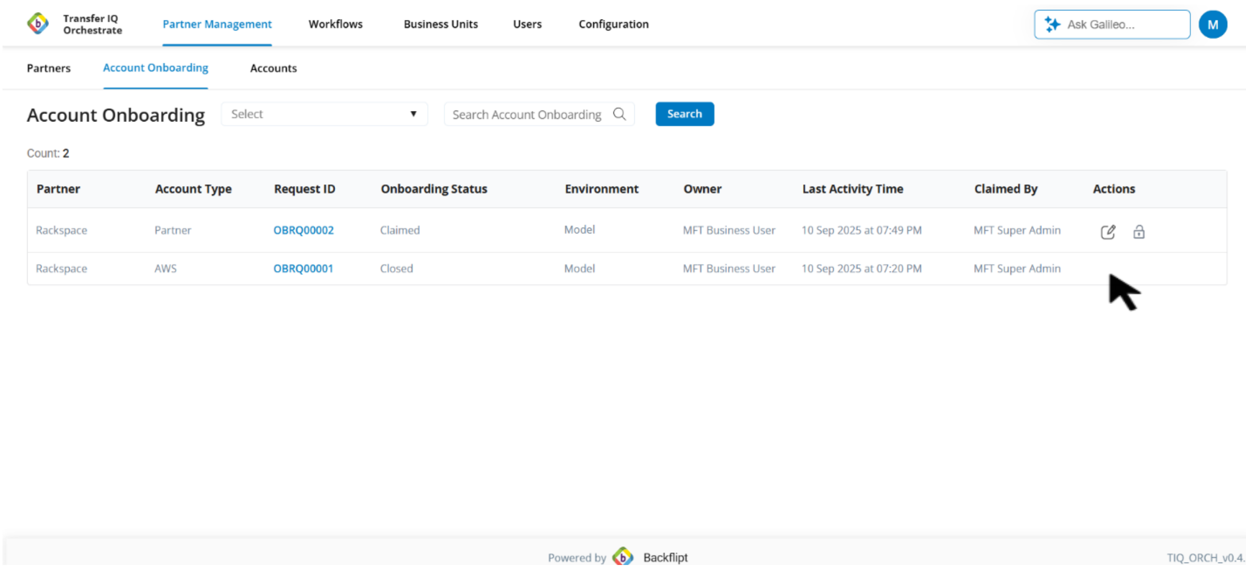
Once the onboarding request is submitted, it becomes visible to all admins under the **Account Onboarding** tab.

- An admin can claim the request to take ownership in one of two ways: by clicking the **View Request** button in the email notification sent after submission, or by locating and claiming the request directly from the **Account Onboarding** tab.





- After claiming the request, the admin can view all the details provided by the Business User in **edit mode**.
- Click the edit mode to open the request in edit mode

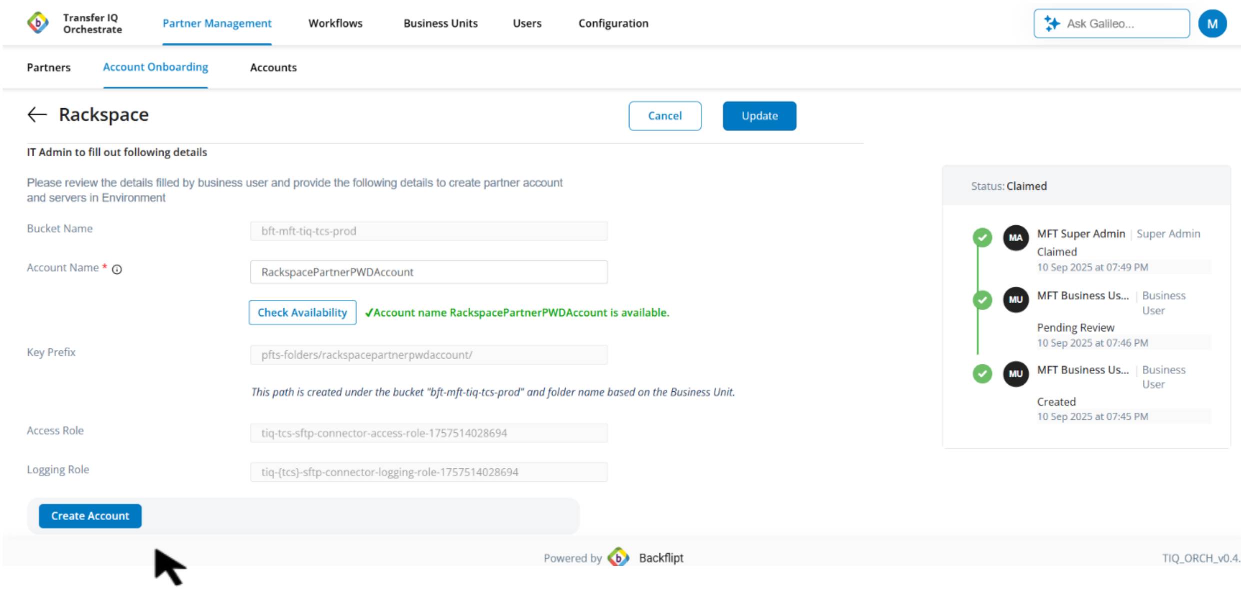


- The admin has the option to review, modify, or update any information if changes are needed. If no changes are required, the details can be left as they are.

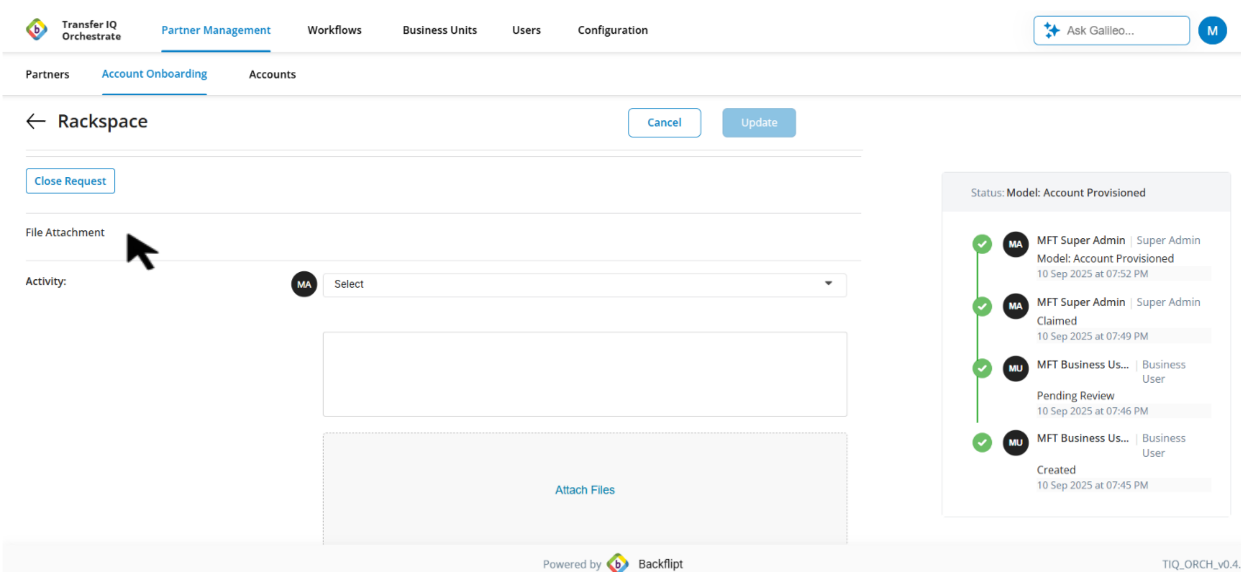
Once all the details are correct, there is a section called **IT Admin to fill out following details which contains the following fields**

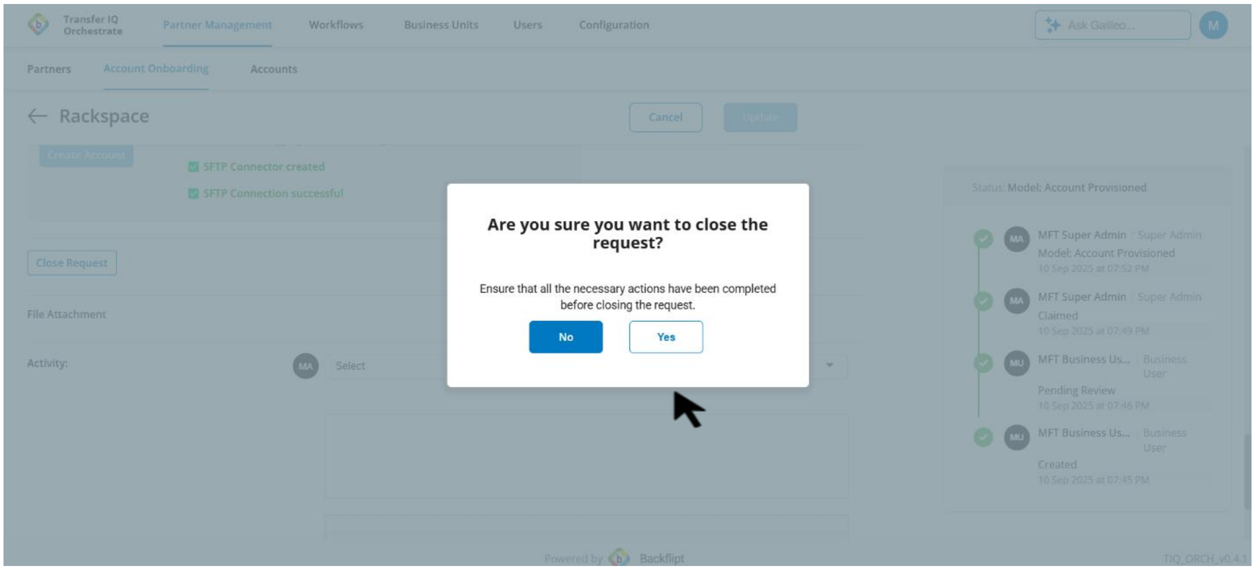
1. **Bucket Name** – Automatically populated based on the bucket name configured in the metadata settings.
2. **Account Name** – A unique name manually entered by the admin during account creation.
3. **Key Prefix** – Automatically generated in the format: `PFTS Folder/ {Account Name}/`, where `{Account Name}` is filled in based on the value entered in the **Account Name** field.
4. **Access Role** – Automatically populated with a predefined access role; this field is not editable.
5. **Logging Role** – Automatically populated with a predefined logging role; this field is also not editable.

Once the admin enters a value in the **Account Name** field, a **Check Availability** option appears to verify if the account name is unique and available. After confirming availability, the admin can click the **Create Account** button to proceed with account creation. Upon successful creation, a toast message is displayed confirming that the account has been created.

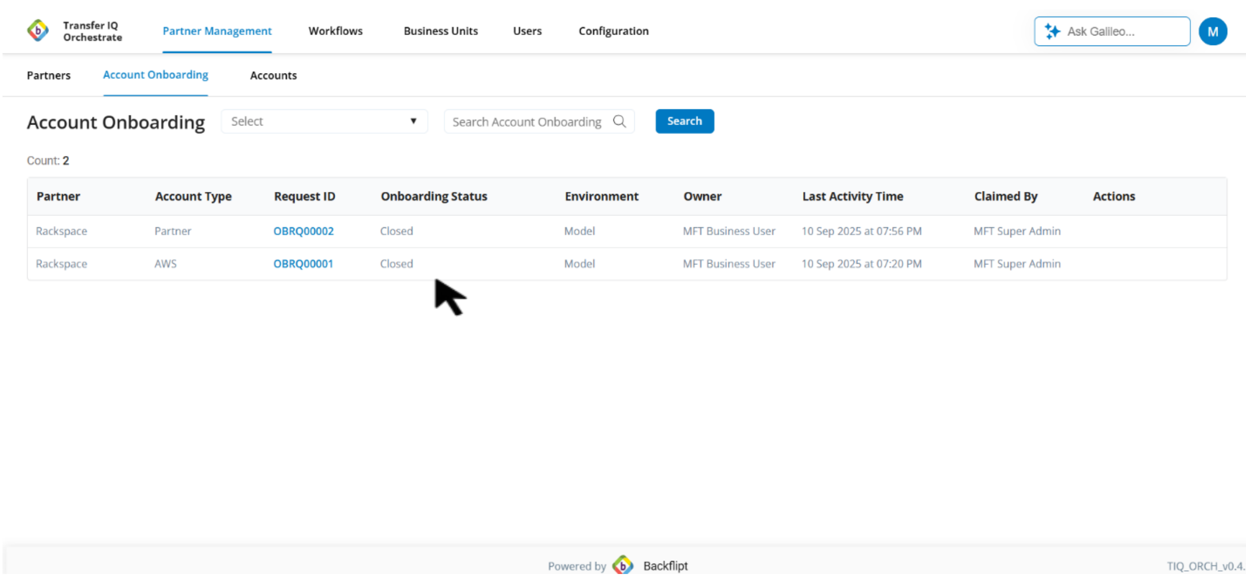


After the account is created, the admin can proceed to close the request, as no further action is required. Clicking on the **Close Request** button triggers a confirmation prompt.





Once confirmed, the request is marked as **Closed**, and the page redirects back to the **Account Onboarding** table, where the request is now listed with a status of **Closed**.



Email Notification Sent to Business User

When a Partner Account is created the Business User will receive an email notification containing the following details:

Email Subject:

- Account Creation Successful – {Partner Name} – Model

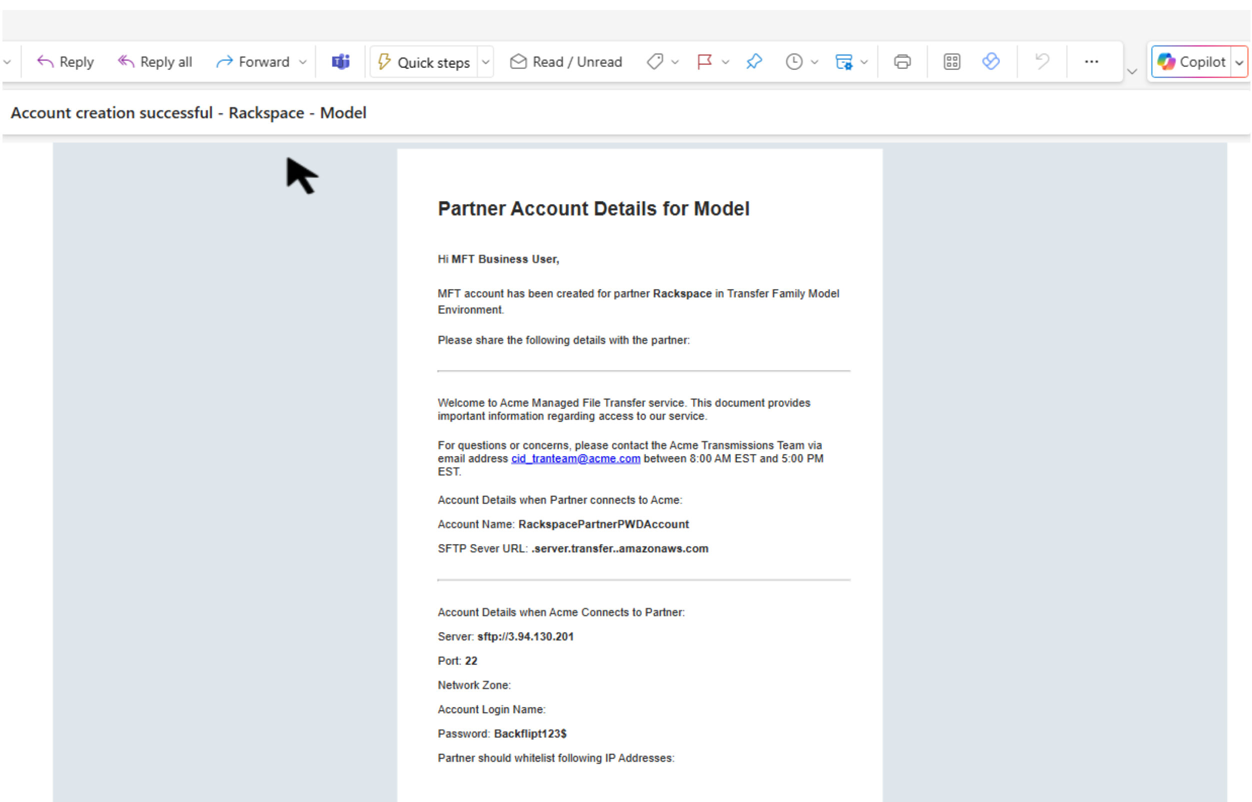
Fields in Email Notification:

- Account Name
- SFTP Server URL
- Port
- Network Zone
- Password/SSH Key (Depending upon the login method selected during account creation)
- Partner should whitelist following IP Addresses

Additional

- Thank you note
- Company Name and Website
- Company Location
- Support Contact Email and Working Hours
- Welcome note and instructions on service access

In addition, the **PGP Encryption Public Key file** will be attached to the email.



Add Partner Hosted Account Workflows

Add Partner Hosted Account Inbound Workflow

In the Partner-Hosted Account Inbound Workflow, the partner uploads a file to their server. The application pulls the file from the source specified by the partner at a scheduled time, which is defined during the creation of the inbound workflow. At the scheduled time, the workflow is triggered, pulls the file from the partner's server, and places it in the destination company's server.

To Create a Partner Hosted Inbound Workflow Business User Creates a Workflow Request with all the required details and submits the workflow request to the admin for approval.

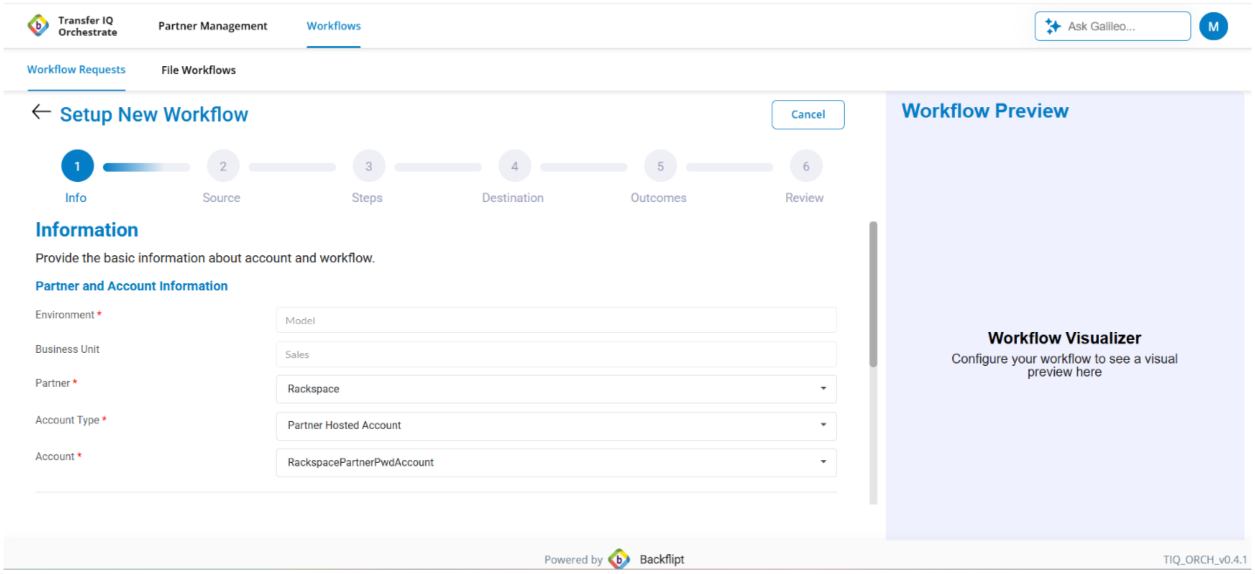
1. Click the Workflows > Workflow Requests tab to view a table displaying the workflow request with the following columns**: Request Id,**
2. To create a new workflow request, click the "Create Workflow Request" button. A window will appear with a screen to **Set up a New Workflow** with various sections
    a. Info
    b. Source
    c. Steps
    d. Destination
    e. Outcomes
    f. Review

Information (Info)

Provide the basic information about account and workflow in this section

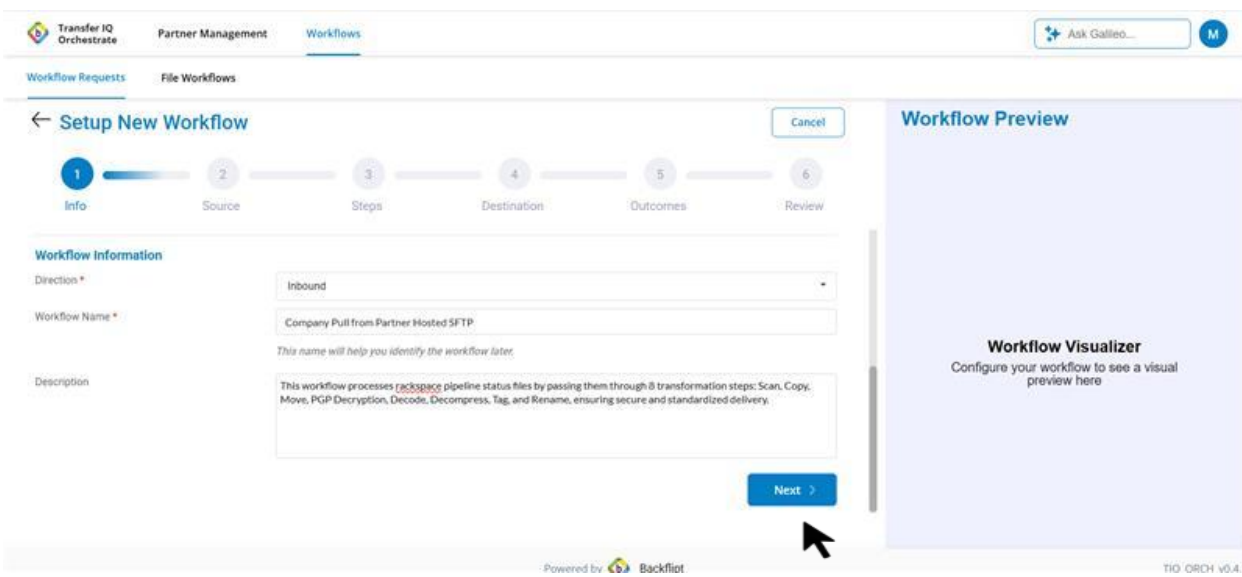
This section contains the following fields

1. Environment – Auto populated with Model
2. Business Unit – Auto populated with the Business Unit assigned to the logged in Business User
3. Partner – A dropdown that consists of list of partners and it allows Business User to select a partner for whom the workflow needs to be created
4. Account Type – Partner Hosted account
5. Partner Account – All the partner accounts created for the partner will be displayed in the dropdown, and allows to select a partner account out of all available options



Once the Partner Account is selected, the Workflow Information section is displayed to provide information about the Workflow with below fields

1. Direction – Select Inbound to create an Inbound Workflow
2. Workflow Name – An input field to Enter a Name for the workflow
3. Description – A field to provide a description about the workflow



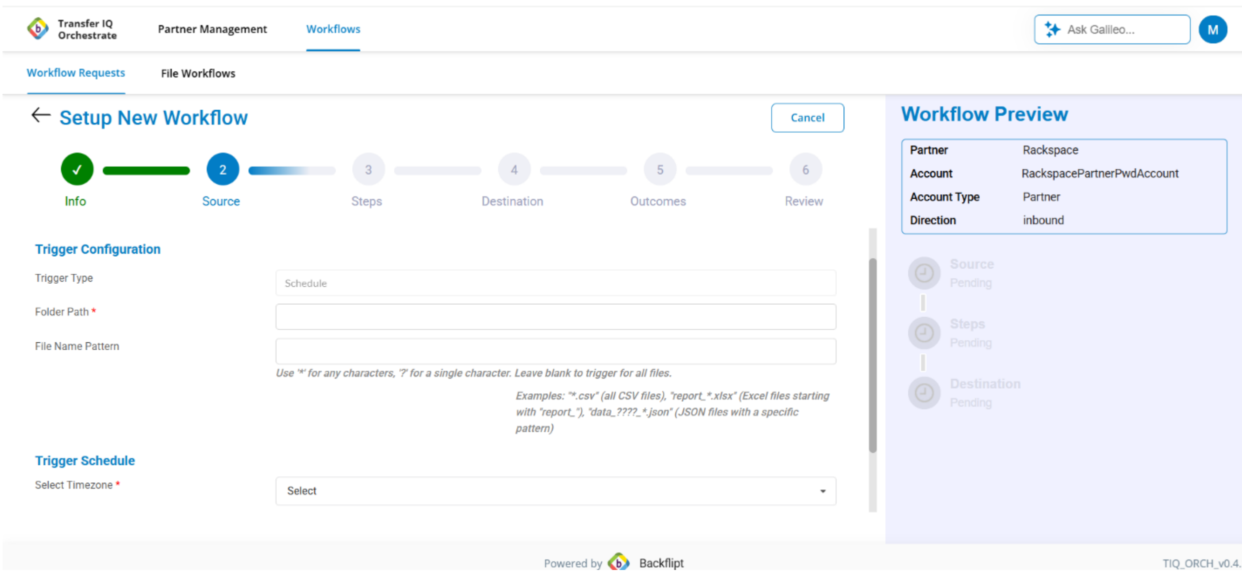
Once all the information is done click the **"Next"** button to navigate to the Source Section

Source

The partner uploads the file to the source folder. All information regarding the source and trigger scheduling will be provided in the source section.

The Source Section Consists of two sub sections:

1. Trigger Configuration
2. Trigger Schedule



Trigger Configuration:

This section provides details about the source folder and the file name pattern that should trigger the workflow.

The section consists of the following fields:

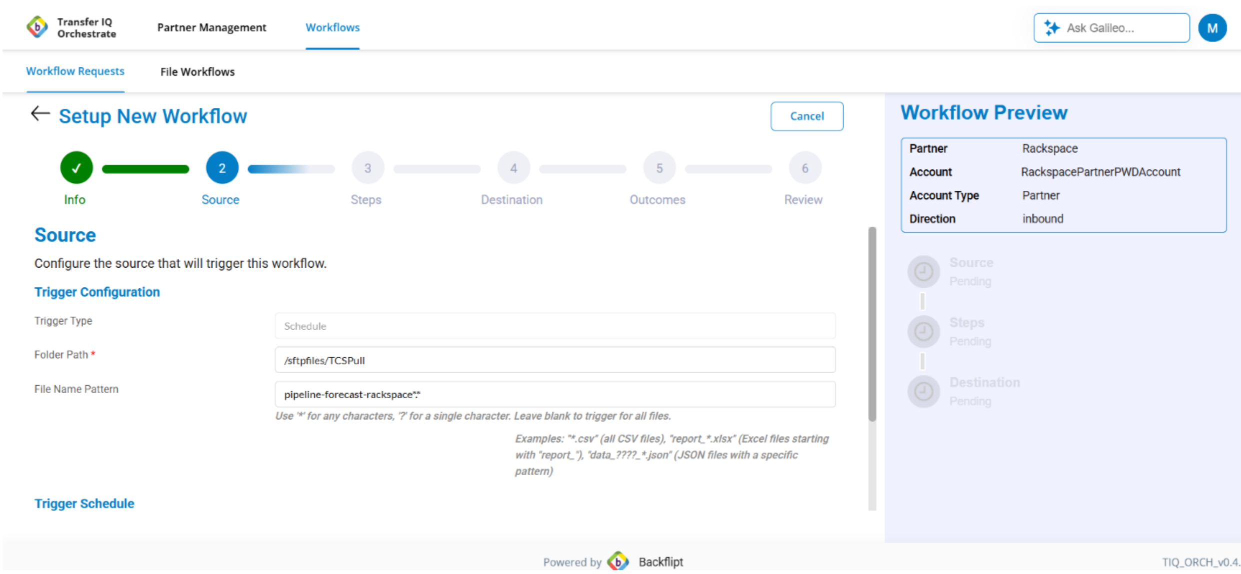
1. Trigger Type – Pre-filled with "Schedule" because the workflow is triggered in a schedule time
2. Folder Path – folder path where the partner uploads the file(shared by partner)
3. File Name Pattern - Specify the file name or pattern that should trigger the workflow.
    - **a.** You can either enter the **exact file name** (e.g., `Sales.pdf`) or use **wildcard characters** to define a pattern:
    - **b.** `*` — Matches **any number of characters**
    - **c.** `?` — Matches **exactly one character**
    - d. **Examples:**
    - e. `*.*` – Triggers the workflow for **any file**, regardless of name or extension

f. `*.csv` – Triggers for any file with a `.csv` extension, such as `data.csv` or `report.csv`

g. "report_*.xlsx" (Excel files starting with "report_")

h. `data_????_*.json` – Triggers for JSON files that follow a specific pattern: the file name must start with `data_`, followed by **exactly four characters**

i. Simply leave blank to trigger for all files



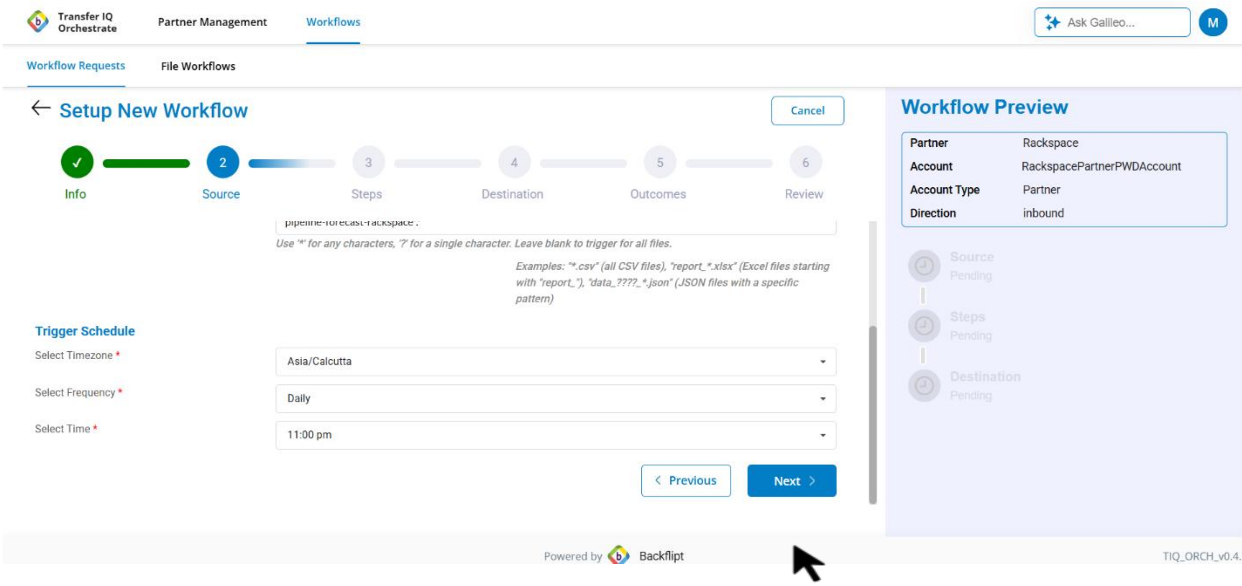
Trigger Schedule

This section provides all the necessary information to configure when the schedule should be triggered.

It includes the following fields:

1. **Select Timezone** – A dropdown to choose the desired time zone (e.g., America/NewYork).
2. **Select Frequency** – A dropdown to select how often the schedule should run: Daily, Weekly, or Monthly.
3. **Select Time** – A dropdown to choose the specific time for the trigger, displayed in 12-hour format with both A.M. and P.M. options.

After providing all mandatory details, click Next to continue to the Steps Section



Steps

There are different Steps in the PFTS Inbound Workflow. Once the workflow is triggered the all the steps configured in the steps section will be executed and the file will be placed in the destination section:

The Steps Available in The PFTS Inbound Workflows are as follow**s**

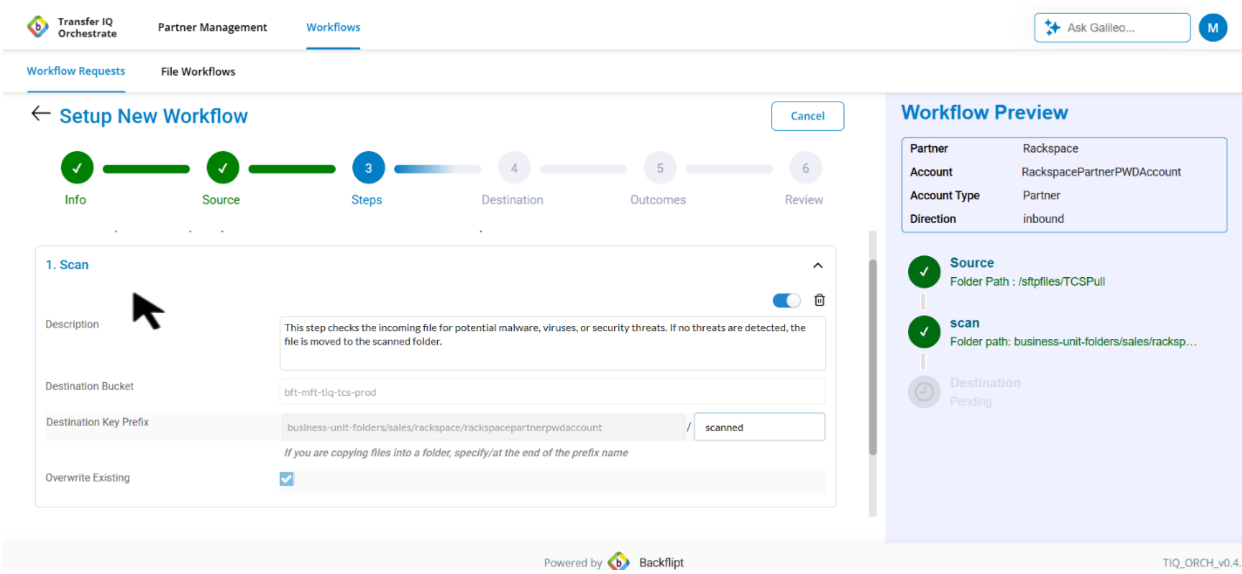
Scan - The scan steps check files or directories for potential malware, viruses, or security threats

Below Fields are available after adding the Scan Step

- Description – A detailed description about the step added
- Source Options Consists of two options
    - **Apply on Original File** – When selected, the step will be executed on the original file located in the source.
    - **Apply on File Created from Previous Step** – When selected, the step will be executed on the output generated by the previous step.
- **Bucket Name**: The name of the storage bucket configured in metadata settings.
- **Destination Key Prefix -** The folder path or prefix within the destination bucket where the files will be placed (e.g., `Business Unit Folder/sales/{Partner}/{Partner name}`). In addition to this, a custom folder can be specified in the input field next to the Destination Key Prefix. The final file

location will be the combination of the prefix path plus the custom folder entered, determining exactly where the file will be stored after the step is executed.

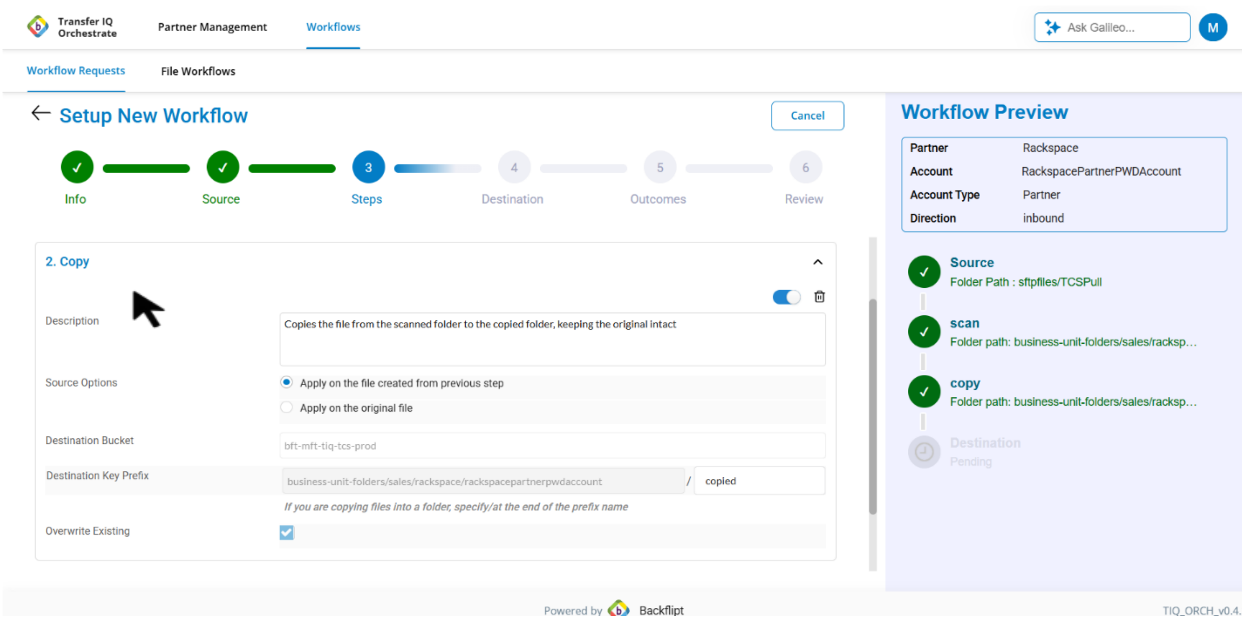
- **Overwrite Existing** – This checkbox is enabled by default. If a file with the same name and extension already exists, it will be overwritten.



Copy - The copy step duplicates a file from the source location to the destination without deleting the original. This ensures the file remains accessible in both locations.

Below Fields are available after adding the Copy Step

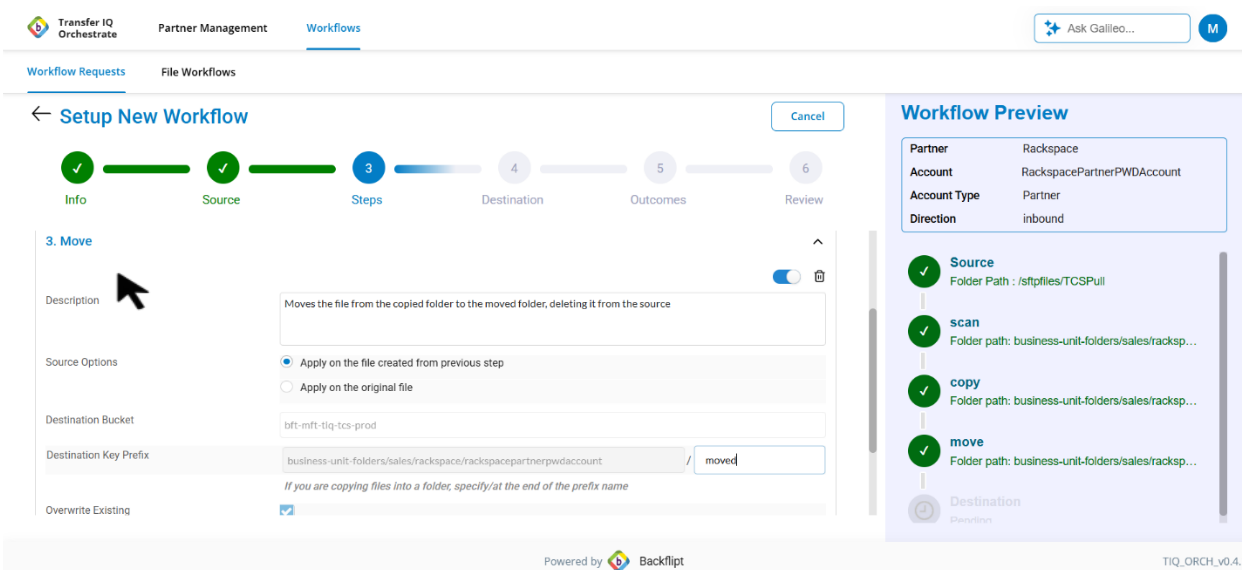
- Description – A detailed description about the step added
- Source Options Consists of two options
  - **Apply on Original File** – When selected, the step will be executed on the original file located in the source.
  - **Apply on File Created from Previous Step** – When selected, the step will be executed on the output generated by the previous step.
- **Bucket Name**: The name of the storage bucket configured in metadata settings.
- **Destination Key Prefix -** The folder path or prefix within the destination bucket where the files will be placed (e.g., `Business Unit Folder/sales/{Partner}/{Partner name}`). In addition to this, a custom folder can be specified in the input field next to the Destination Key Prefix. The final file location will be the combination of the prefix path plus the custom folder entered, determining exactly where the file will be stored after the step is executed.
- **Overwrite Existing** – This checkbox is enabled by default. If a file with the same name and extension already exists, it will be overwritten.



Move - The move operation shifts a file from the source location to the destination. Once moved, the file no longer exists in the source location.

Below Fields are available after adding the Move Step

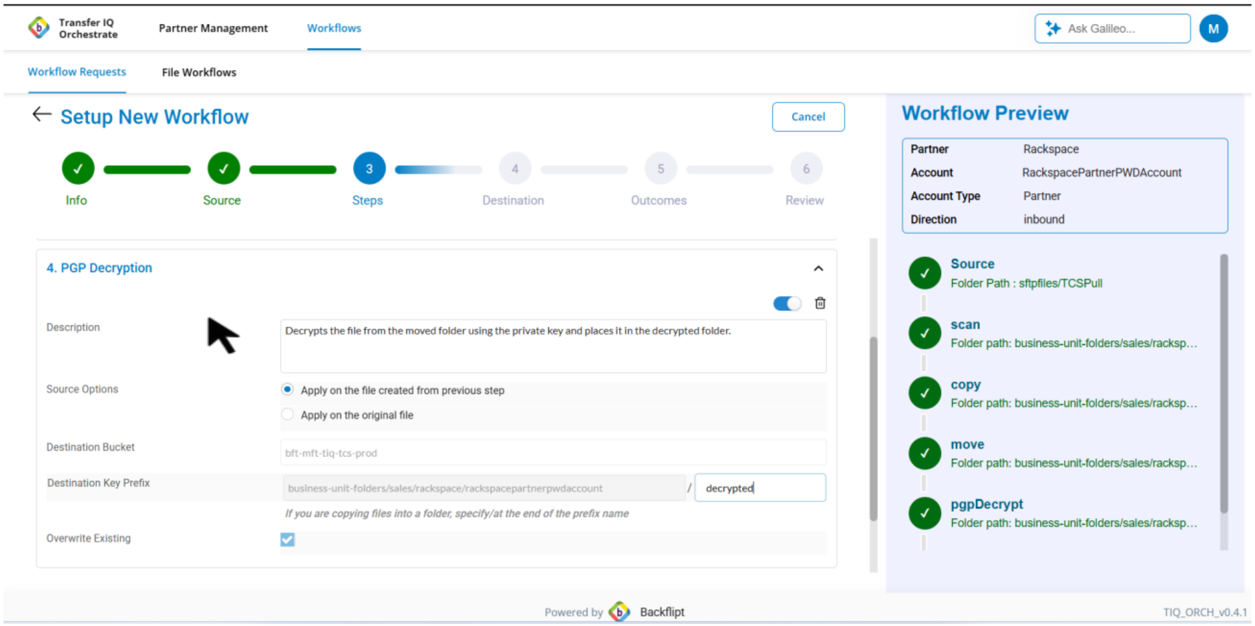
- Description – A detailed description about the step added
- Source Options Consists of two options
  - **Apply on Original File** – When selected, the step will be executed on the original file located in the source.
  - **Apply on File Created from Previous Step** – When selected, the step will be executed on the output generated by the previous step.
- **Bucket Name**: The name of the storage bucket configured in metadata settings.
- **Destination Key Prefix -** The folder path or prefix within the destination bucket where the files will be placed (e.g., `Business Unit Folder/sales/{Partner}/{Partner name}`). In addition to this, a custom folder can be specified in the input field next to the Destination Key Prefix. The final file location will be the combination of the prefix path plus the custom folder entered, determining exactly where the file will be stored after the step is executed.
- **Overwrite Existing** – This checkbox is enabled by default. If a file with the same name and extension already exists, it will be overwritten.



PGP Decrypt - The PGP decrypt step retrieves an encrypted file from the source location, decrypts it using the PGP private key provided in the MFT Settings tab, and places the decrypted file in the specified destination folder.

Below Fields are available after adding the Decrypt Step

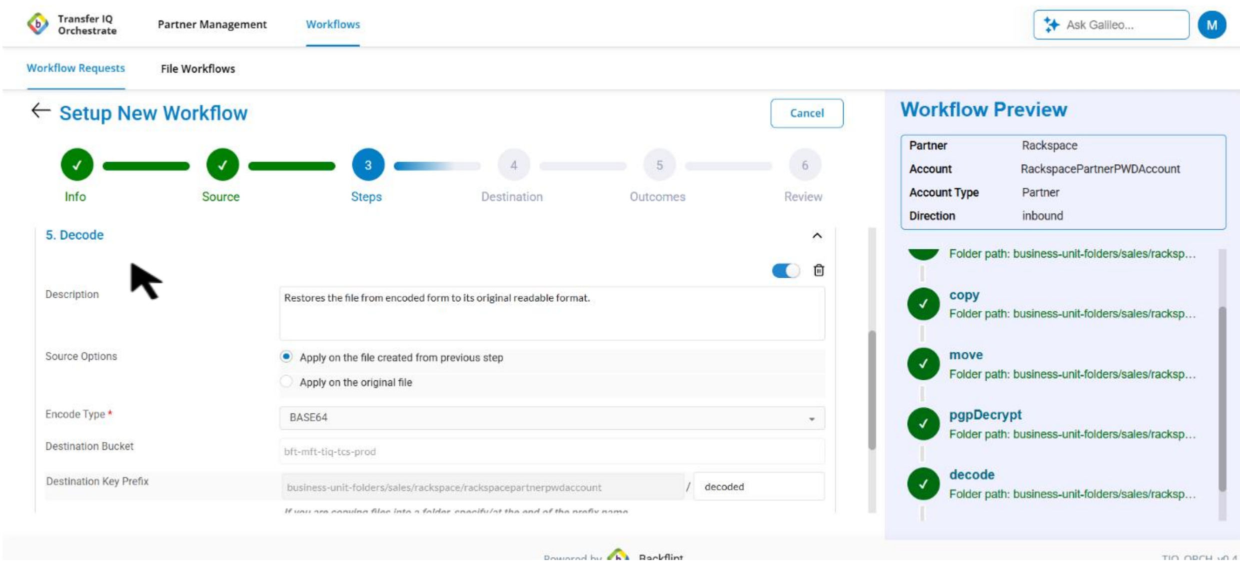
- Description – A detailed description about the step added
- Source Options Consists of two options
  - **Apply on Original File** – When selected, the step will be executed on the original file located in the source.
  - **Apply on File Created from Previous Step** – When selected, the step will be executed on the output generated by the previous step.
- **Bucket Name**: The name of the storage bucket configured in metadata settings.
- **Destination Key Prefix -** The folder path or prefix within the destination bucket where the files will be placed (e.g., `Business Unit Folder/sales/{Partner}/{Partner name}`). In addition to this, a custom folder can be specified in the input field next to the Destination Key Prefix. The final file location will be the combination of the prefix path plus the custom folder entered, determining exactly where the file will be stored after the step is executed.
- **Overwrite Existing** – This checkbox is enabled by default. If a file with the same name and extension already exists, it will be overwritten.



Decode - Decode step converts encoded file back to its original, readable format. It is used when a file has been encoded (for example, in Base64) and needs to be returned to its normal form so that it can be used

Below Fields are available after adding the Decode Step

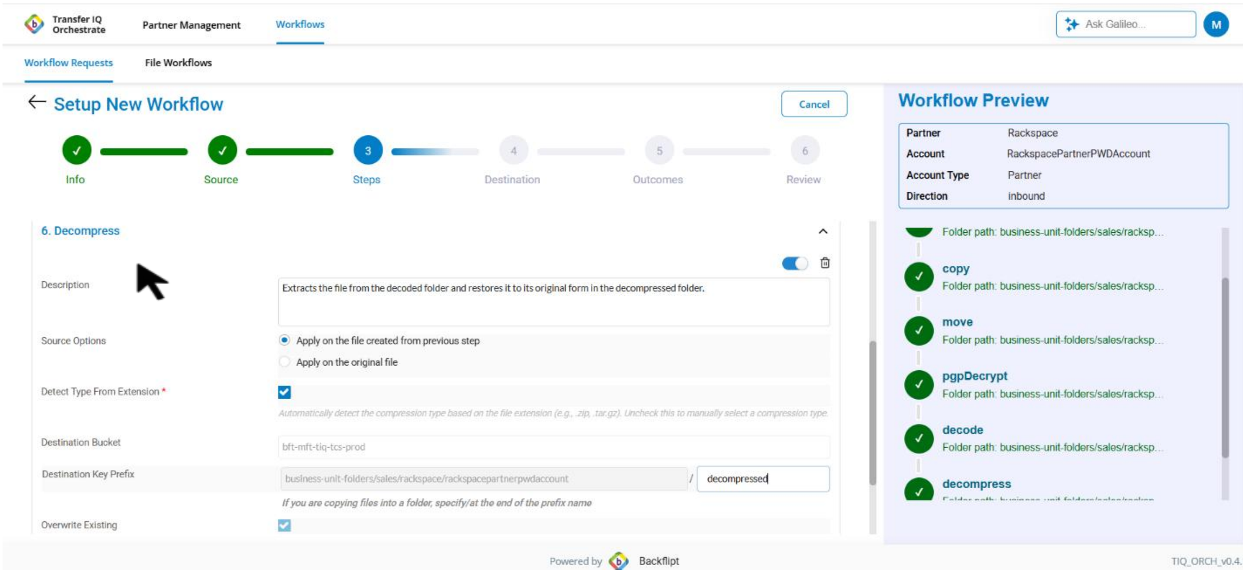
- Description – A detailed description about the step added
- Source Options Consists of two options
  - **Apply on Original File** – When selected, the step will be executed on the original file located in the source.
  - **Apply on File Created from Previous Step** – When selected, the step will be executed on the output generated by the previous step.
- Encode Type – A dropdown to select the encode type (Supported type: Base64)
- **Bucket Name**: The name of the storage bucket configured in metadata settings.
- **Destination Key Prefix -** The folder path or prefix within the destination bucket where the files will be placed (e.g., `Business Unit Folder/sales/{Partner}/{Partner name}`). In addition to this, a custom folder can be specified in the input field next to the Destination Key Prefix. The final file location will be the combination of the prefix path plus the custom folder entered, determining exactly where the file will be stored after the step is executed.
- **Overwrite Existing** – This checkbox is enabled by default. If a file with the same name and extension already exists, it will be overwritten.



Decompress - Decompress step extracts and restores the original content from a compressed file, allowing the data to be accessed and used in its original form.

Below Fields are available after adding the Decompress Step

- Description – A detailed description about the step added
- Source Options Consists of two options
    - **Apply on Original File** – When selected, the step will be executed on the original file located in the source.
    - **Apply on File Created from Previous Step** – When selected, the step will be executed on the output generated by the previous step.
- **Bucket Name-** The name of the storage bucket configured in metadata settings.
- **Detect Type From Extension-** A checkbox that Automatically detect the compression type based on the file extension (e.g., .zip, .tar.gz). Uncheck this to manually select a compression type.
- Compression Type – A dropdown to select the Compression type (zip, tar,gzip,zstd)
- Select either detect type from extension or Compression type
- **Destination Key Prefix -** The folder path or prefix within the destination bucket where the files will be placed (e.g., `Business Unit Folder/sales/{Partner}/{Partner name}`). In addition to this, a custom folder can be specified in the input field next to the Destination Key Prefix. The final file location will be the combination of the prefix path plus the custom folder entered, determining exactly where the file will be stored after the step is executed.
- **Overwrite Existing** – This checkbox is enabled by default. If a file with the same name and extension already exists, it will be overwritten.

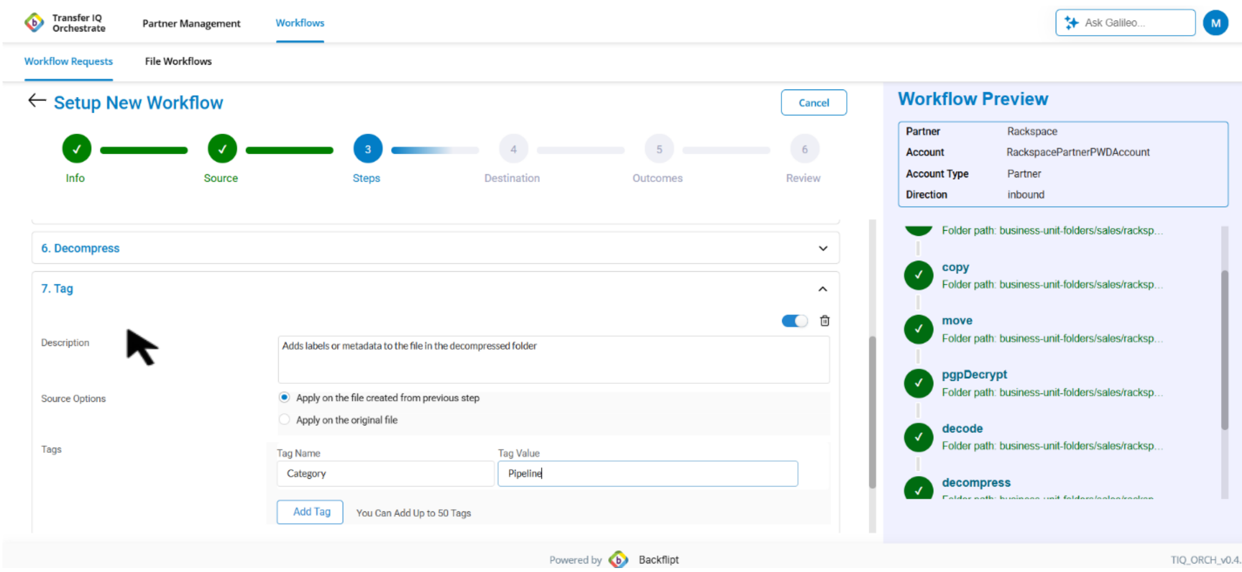


Tag - The tag step allows adding additional information to files in the form of key-value pairs. This extra info helps describe, organize, and manage them more effectively. Up to 50 tags can be added per file.

Below Fields are available after adding the Tag Step

- Description – A detailed description about the step added
- Source Options Consists of two options
  - **Apply on Original File** – When selected, the step will be executed on the original file located in the source.
  - **Apply on File Created from Previous Step** – When selected, the step will be executed on the output generated by the previous step.

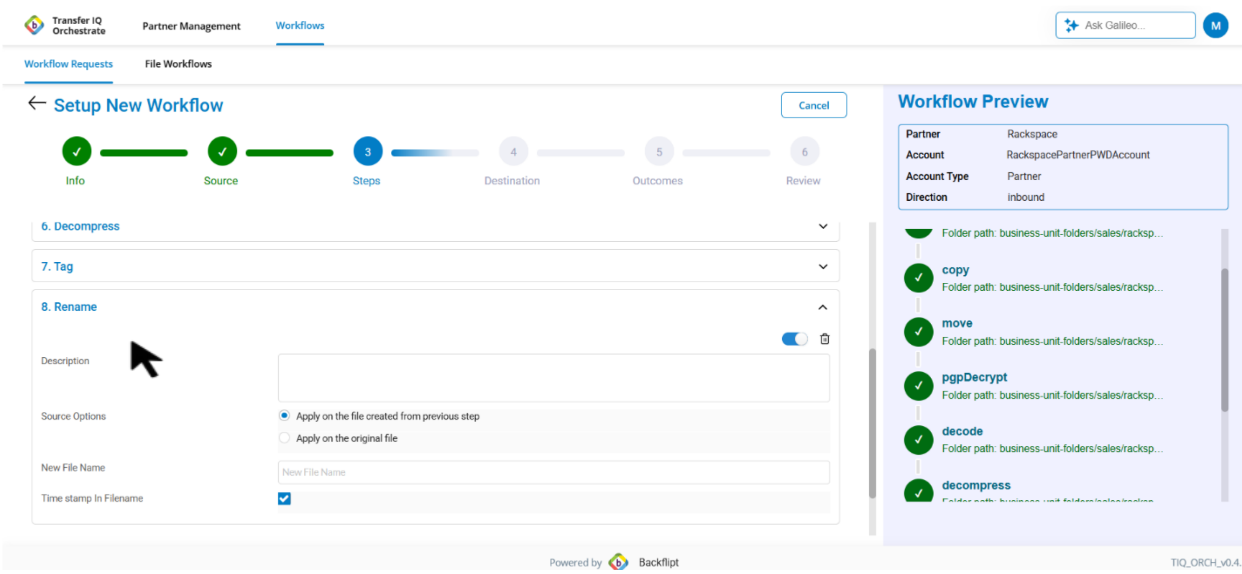
This section includes fields for **Tag Name** and **Tag Value** to add tags to a file. To add more tags, click the **Add Tag** button. Each tag also has a **Remove** button, allowing it to be deleted if needed.



Rename - The **rename step** changes the name of a file. This helps organize files by giving them clear, consistent, or updated names without altering their content or location.

Below Fields are available after adding the Rename Step

- Description – A detailed description about the step added
- Source Options Consists of two options
  - **Apply on Original File** – When selected, the step will be executed on the original file located in the source.
  - **Apply on File Created from Previous Step** – When selected, the step will be executed on the output generated by the previous step.
- **New File Name** – Enter the Renamed New file name
- **Timestamp in Filename** –
- A checkbox that, when enabled, adds a timestamp to the file name during the rename step execution



In addition to adding the steps there are some other actions like deleting and disabling a step

Delete - The **delete step** removes a file from its source permanently. This step is typically used to clean up files after they are no longer needed

Below Fields are available after adding the Copy Step

- Description – A detailed description about the step added
- Source Options Consists of two options
    - **Apply on Original File** – When selected, the step will be executed on the original file located in the source.
    - **Apply on File Created from Previous Step** – When selected, the step will be executed on the output generated by the previous step.

Disable a Step

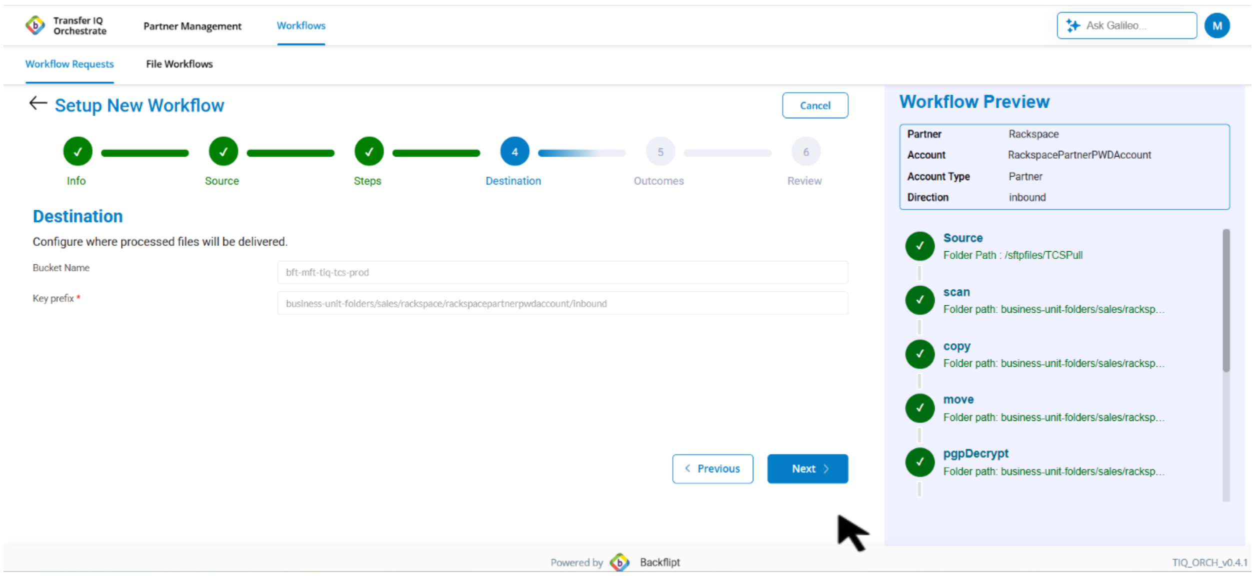
A toggle switch is located at the top-right corner of each step. When enabled, the step will be executed as part of the workflow. If disabled, the step will be skipped during workflow execution.

Once all the steps are added, click the next button to navigate to the destination section

Destination

The Destination section contains all the necessary details about where the file should be delivered.

1. **Bucket Name** – Pre-filled bucket name configured in metadata settings
2. **Key Prefix** – An auto-populated, non-editable folder path indicating where the file will be placed after the transfer.



Outcome Actions

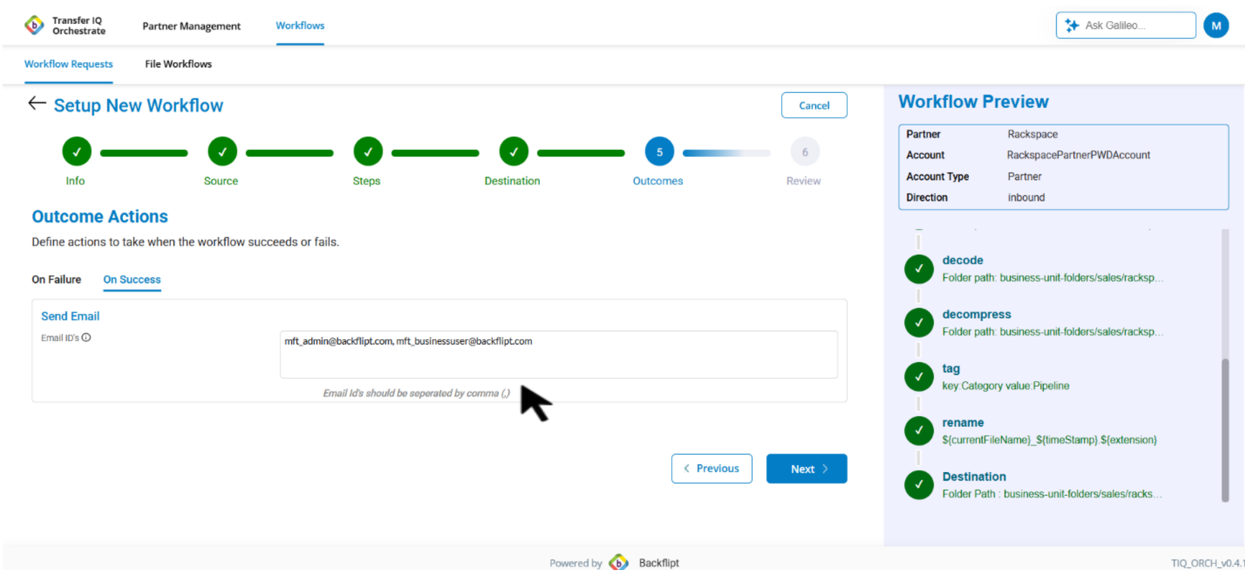
The Outcomes section consists of two tabs:

1. On Success
2. On Failure.

On Success – Notify the email entered upon successful file transfer.

On Failure – Notify the email entered if the file transfer fails.

Note: Enter Comma Separated Emails to notify multiple emails

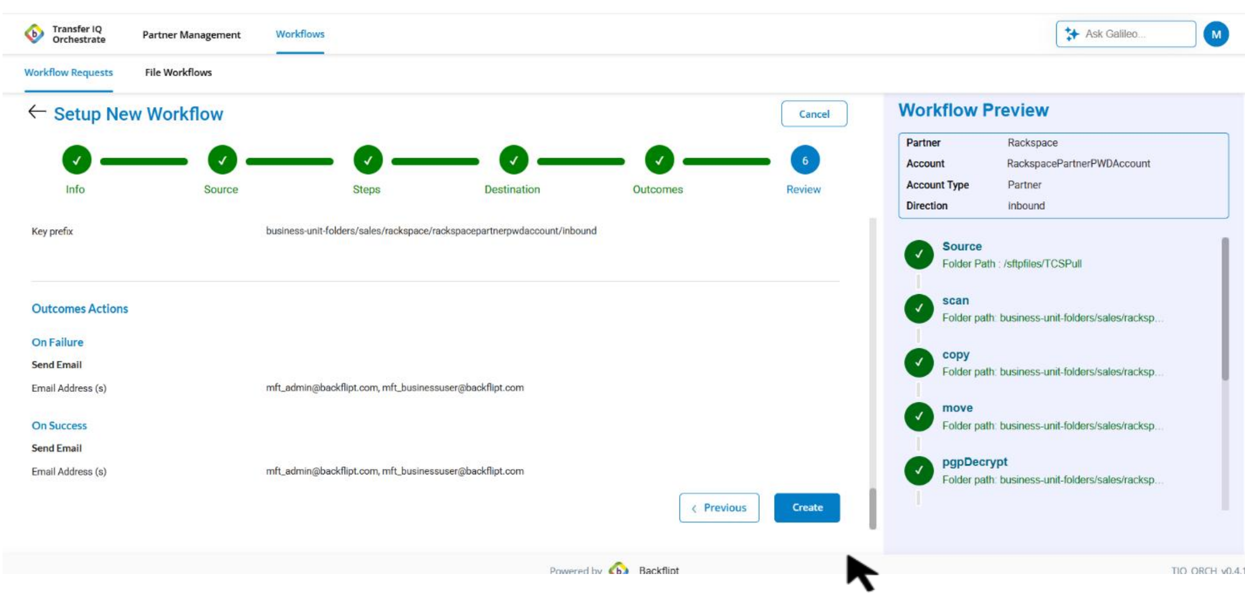


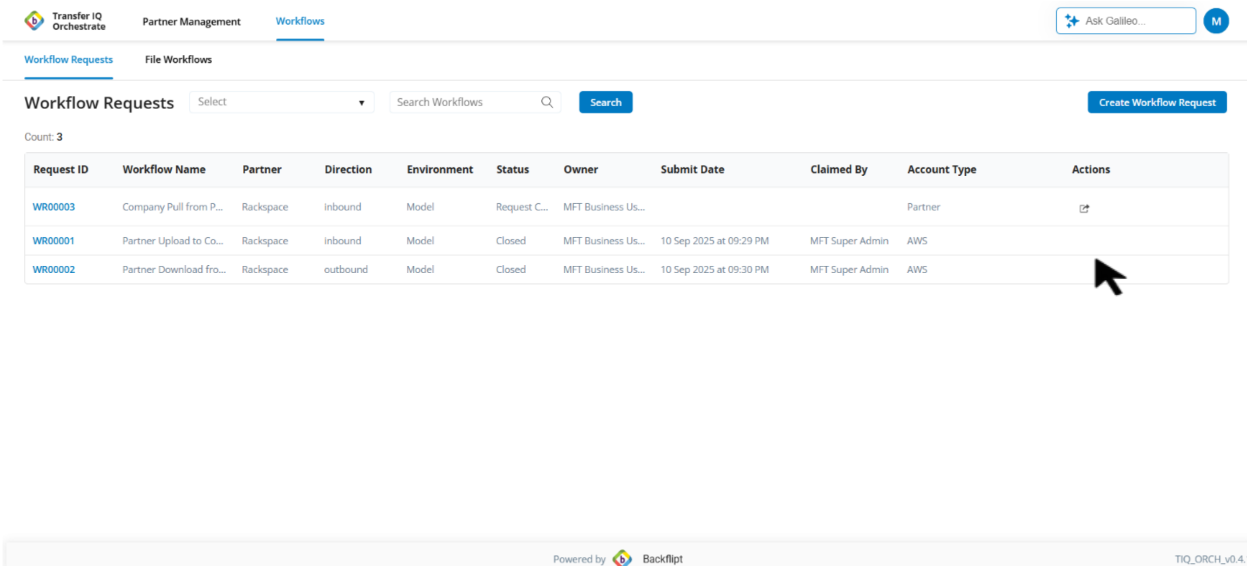
Review

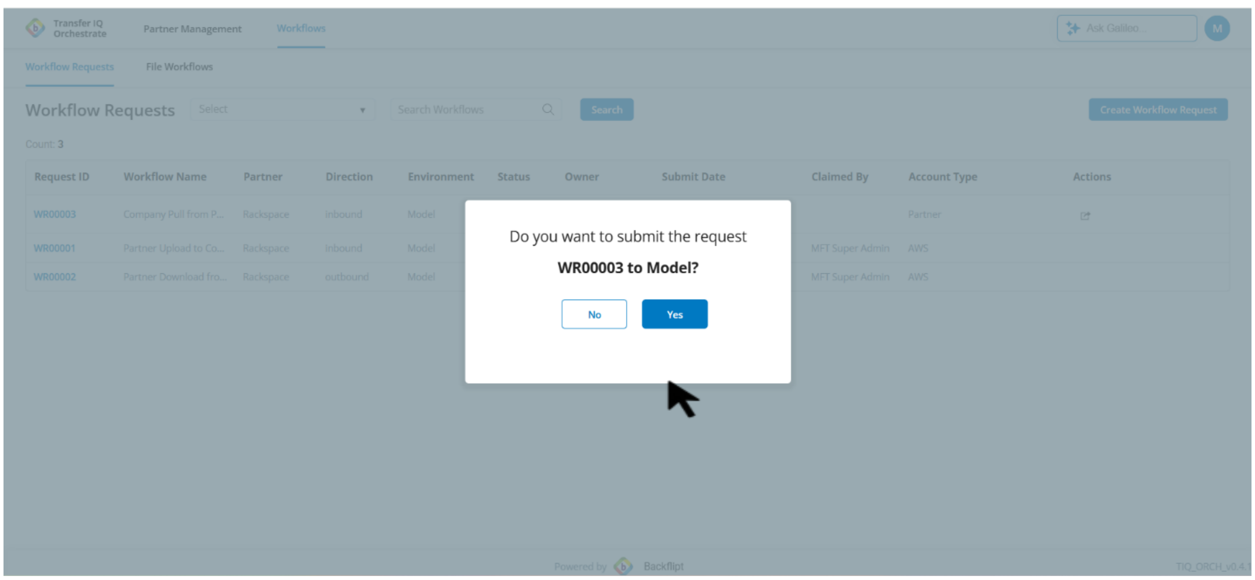
Review all the details provided during the workflow request creation. If everything is correct, the Business User can proceed to create the workflow request. If any changes are needed, use the Previous button to go back and make edits

Once the workflow request creation is done, Business User submits the request to the admin for approval

, it becomes visible to all admins under the Workflow Requests tab.

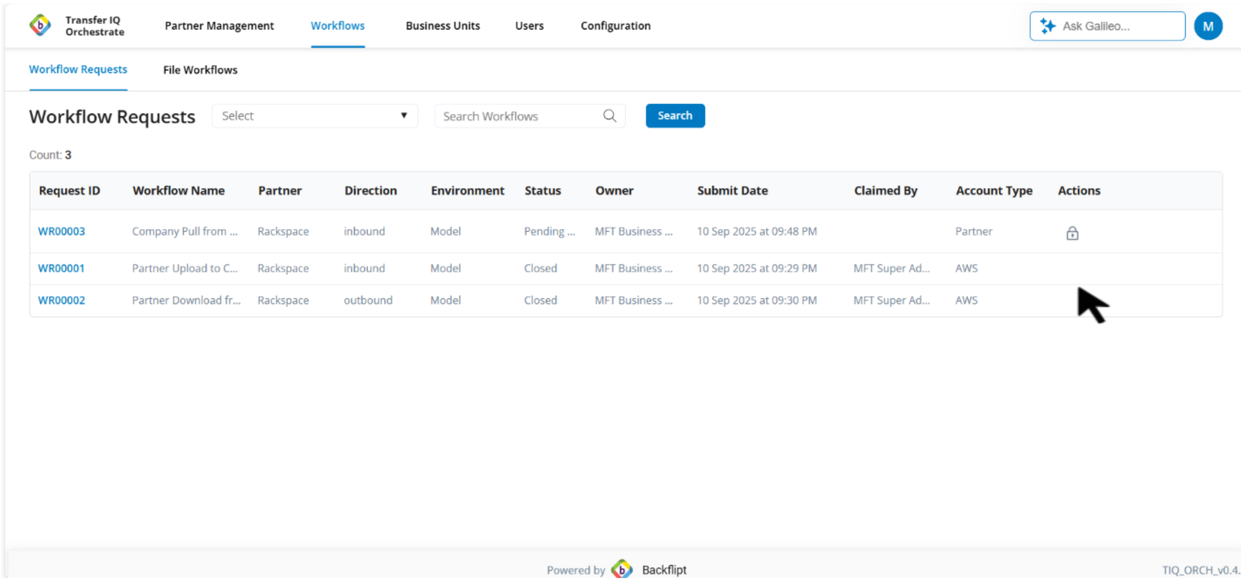


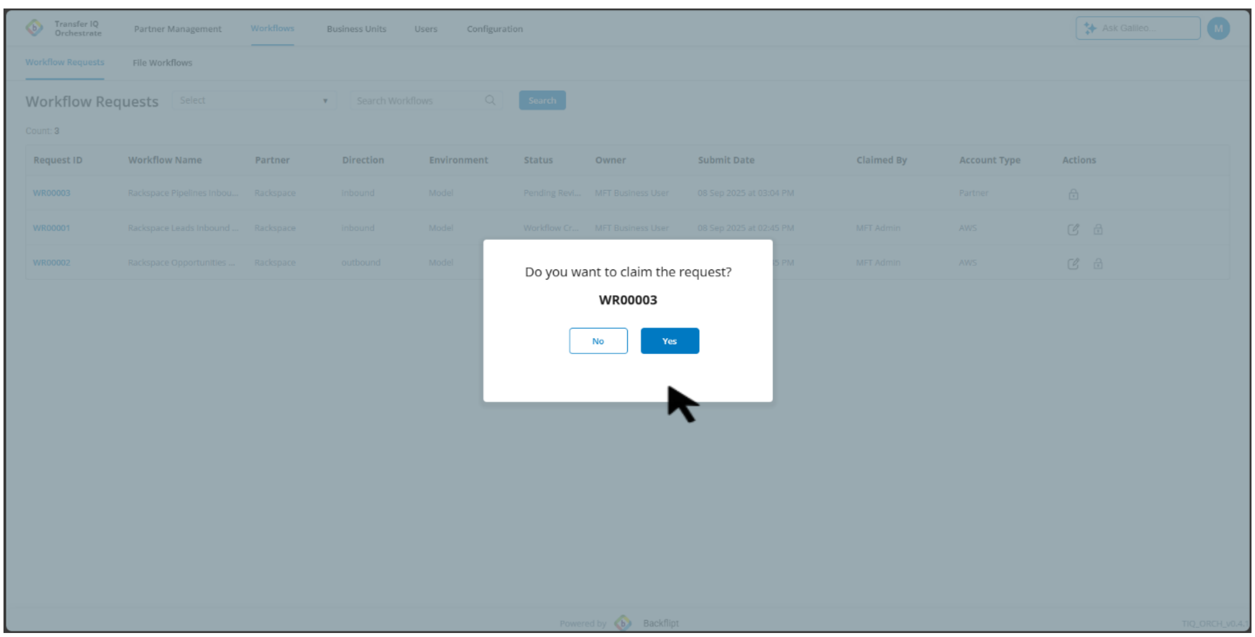




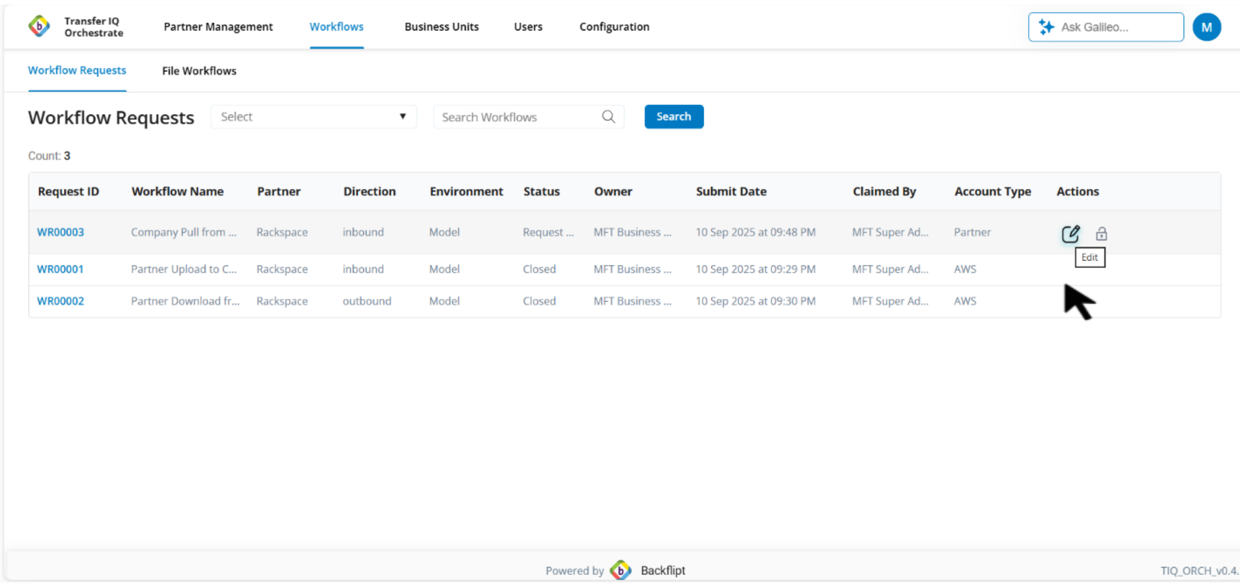
Admin Approval – PFTS Inbound Workflow request

An admin can claim the request to take ownership in one of two ways: by clicking the View Request button in the email notification sent after submission, or by locating and claiming the request directly from the Account Onboarding tab.



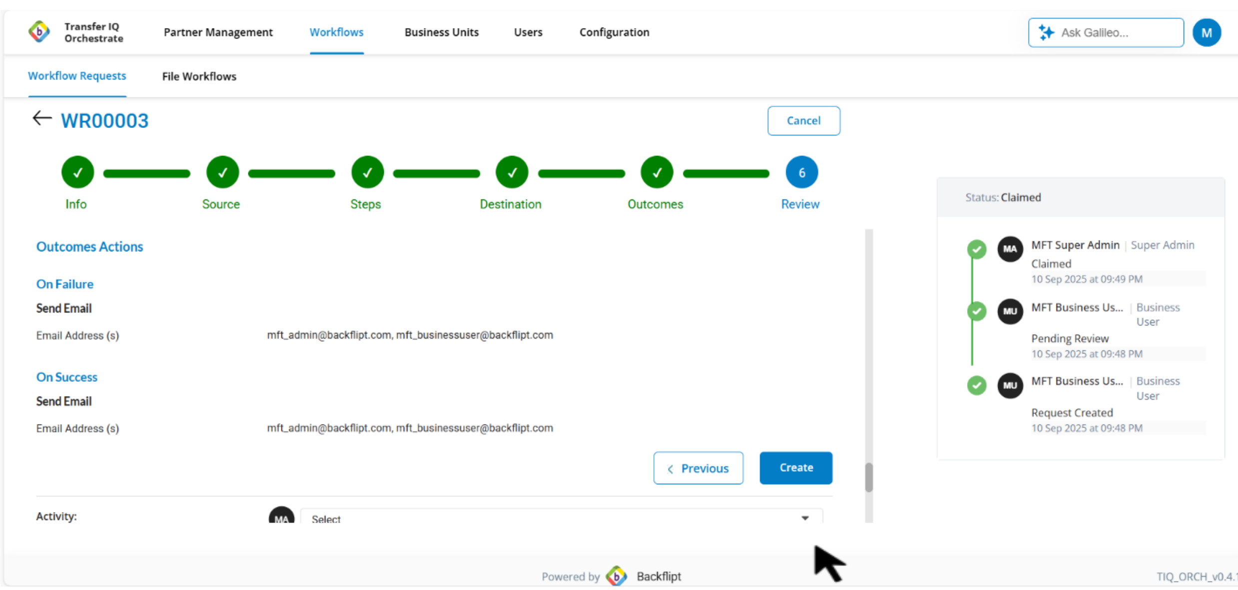


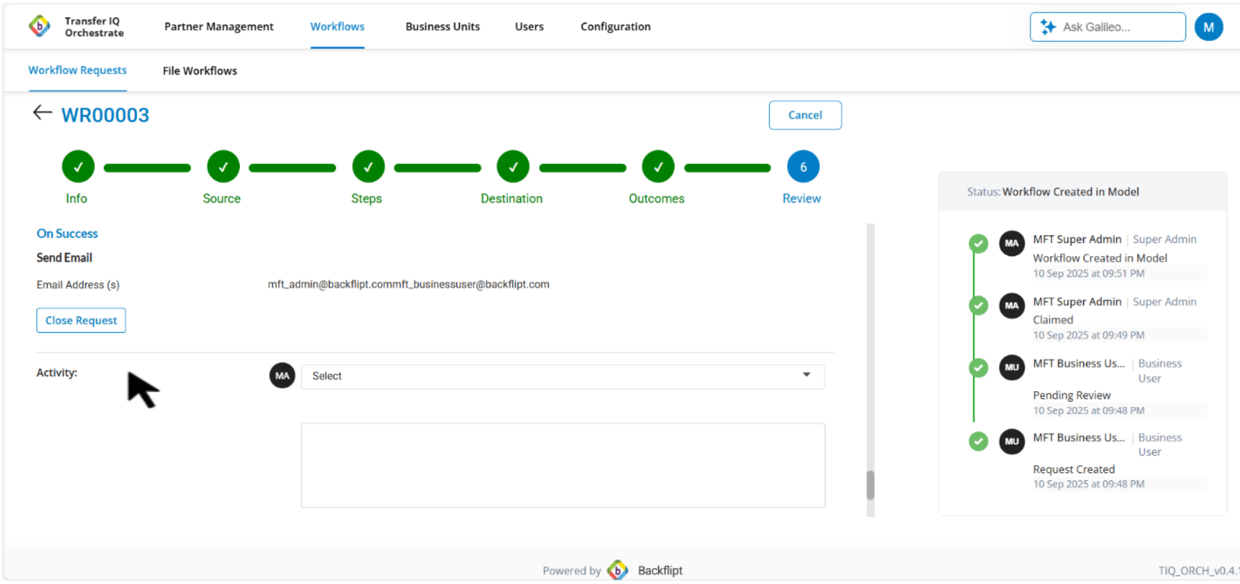
After claiming the request, the admin can view all the details provided by the Business User in edit mode.



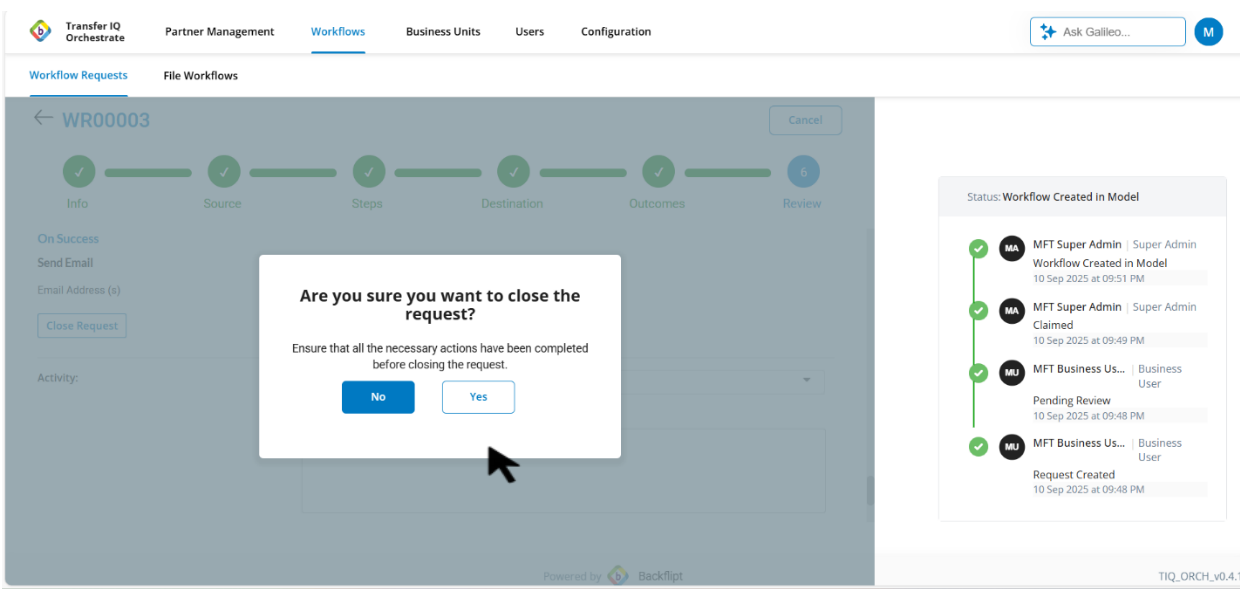
The admin has the option to review, modify, or update any information if changes are needed. If no changes are required, the details can be left as they are.

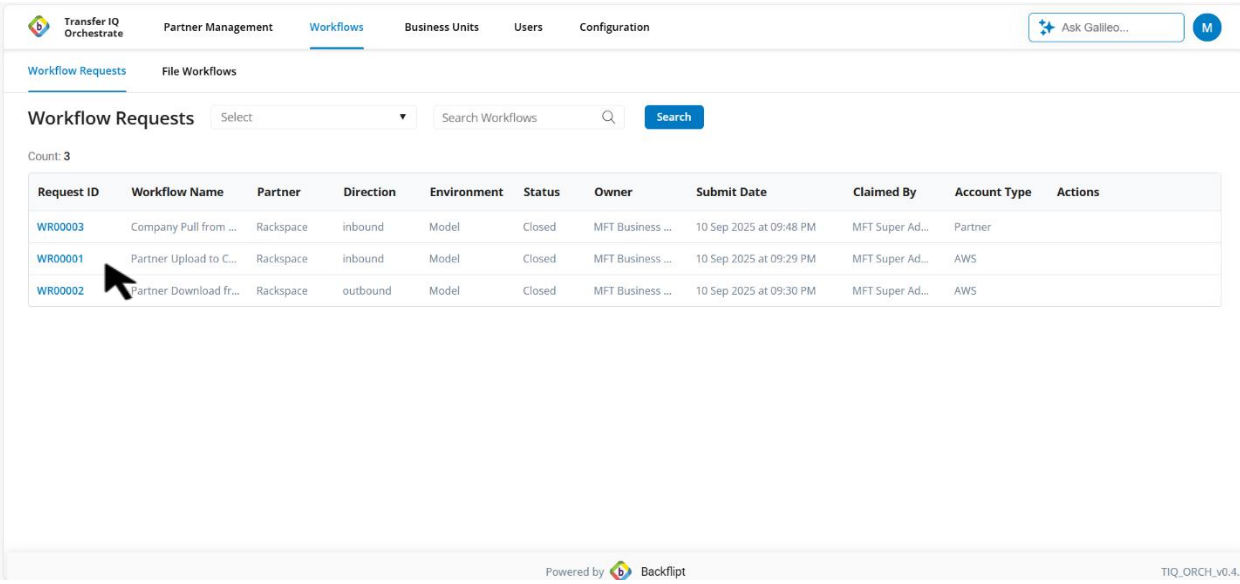
Click the Create button to create the workflow





After the workflow is created, the admin can proceed to close the request, as no further action is required. Clicking the **Close Request** button triggers a confirmation prompt. Once confirmed, the request is marked as **Closed**, and the page redirects back to the Workflow Requests table, where the request is now listed with a status of **Closed**.





Add Partner Hosted Account Outbound Workflow

In the Partner-Hosted Account Outbound Workflow, the company uploads a file in the aws s3 bucket. The application pushes the file to the destination shared by the partner which the Business User defined during the creation of the outbound workflow.

To Create a Partner Hosted Outbound Workflow Business User Creates a Workflow Request with all the required details and submits the workflow request to the admin for approval.

1. Click the Workflows > Workflow Requests tab to view a table displaying the workflow request with the following columns**: Request Id,**
2. To create a new workflow request, click the "Create Workflow Request" button. A window will appear with a screen to **Set up a New Workflow** with various sections
    a. Info
    b. Source
    c. Steps
    d. Destination
    e. Outcome

Information (Info)

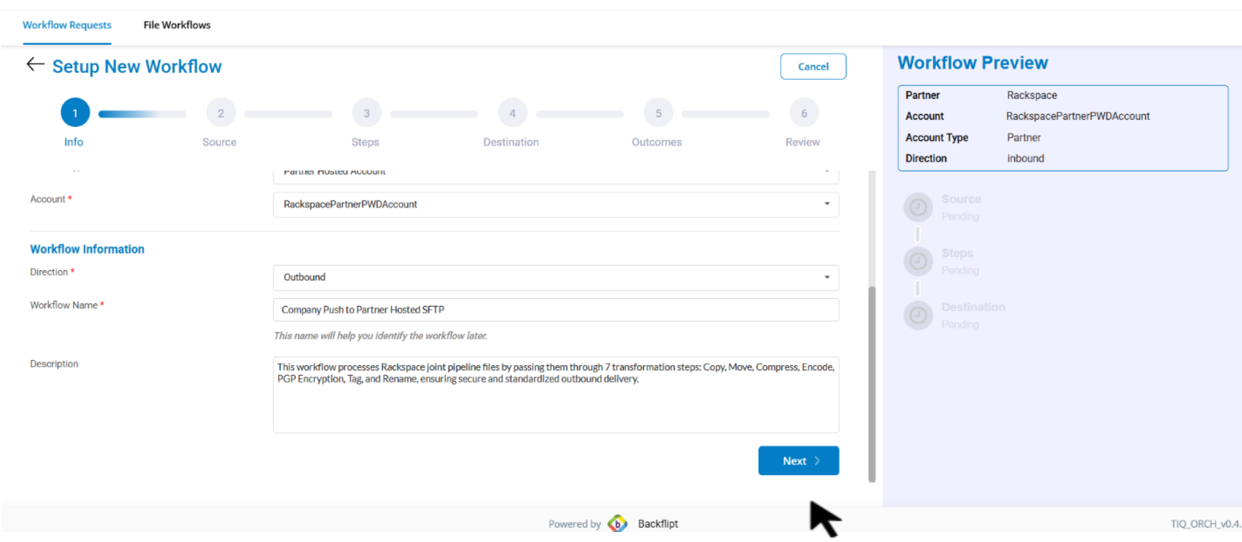
Provide the basic information about account and workflow in this section

This section contains the following fields

1. Environment – Auto populated with Model
2. Business Unit – Auto populated with the Business Unit assigned to the logged in Business User
3. Partner – A dropdown that consists of list of partners and it allows Business User to select a partner for whom the workflow needs to be created
4. Account Type – Partner Hosted account
5. Partner Account – All the partner accounts created for the partner will be displayed in the dropdown, and allows to select a partner account out of all available options

Once the Partner Account is selected, the Workflow Information section is displayed to provide information about the Workflow with below fields

1. Direction – Select Inbound to create a Inbound Workflow
2. Workflow Name – An input field to Enter a Name for the workflow
3. Description – A field to provide a description about the workflow



Once all the information is done click the **"Next"** button to navigate to the Source Section

Source

The Business User uploads the file to the source folder in S3 Bucket. All information regarding the source and trigger scheduling will be provided in the source section.

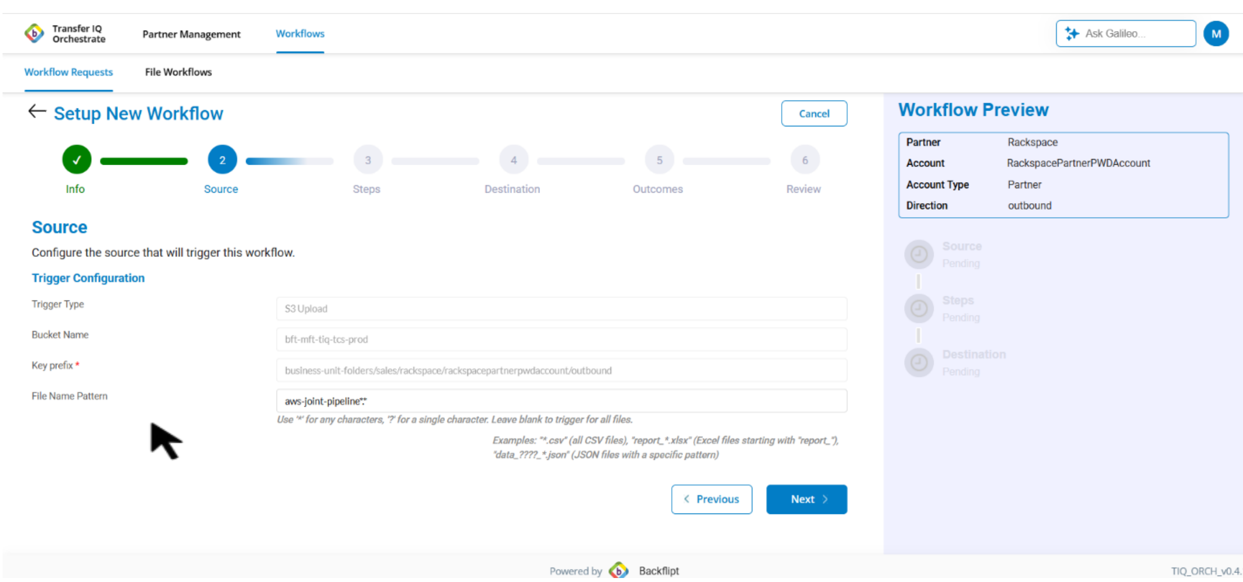
The Source Section Consists of Trigger Configuration sub section

Trigger Configuration:

This section provides details about the source folder and the file name pattern that should trigger the workflow.

The section consists of the following fields:

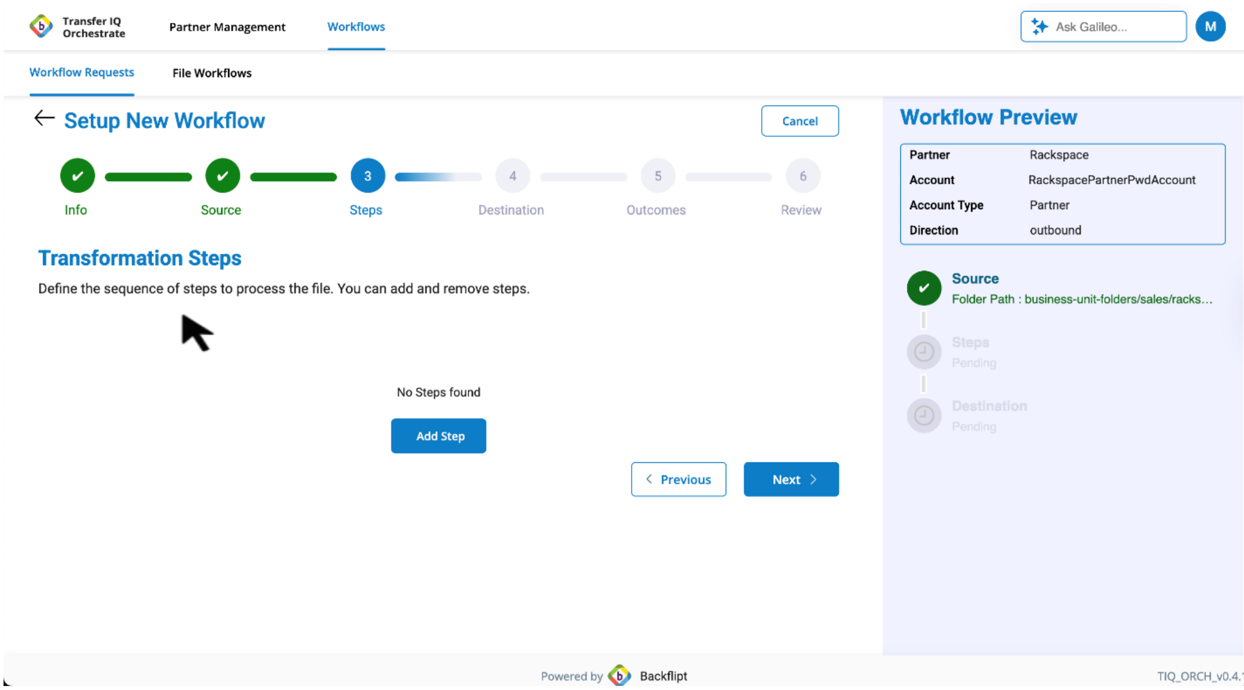
1. Trigger Type – Pre-filled with “S3 Upload” because the Business User Uploads the file in S3 Folder Path
2. Bucket Name – Pre-filled Bucket name
3. Key Prefix – Folder Path where the Business User uploads the file
4. File Name Pattern - Specify the file name or pattern that should trigger the workflow.
   a. You can either enter the **exact file name** (e.g., `Sales.pdf`) or use **wildcard characters** to define a pattern:
   b. `*` — Matches **any number of characters**
   c. `?` — Matches **exactly one character**
   d. **Examples:**
   e. `*.*` – Triggers the workflow for **any file**, regardless of name or extension
   f. `*.csv` – Triggers for any file with a `.csv` extension, such as `data.csv` or `report.csv`
   g. "report_*.xlsx" (Excel files starting with "report_")
   h. `data_????_*.json` – Triggers for JSON files that follow a specific pattern: the file name must start with `data_`, followed by **exactly four characters.**
   i. Simply leave blank to trigger for all files



Once all the fields are provided, click the next button to navigate to the steps section

Steps

There are different Steps in the PFTS Outbound Workflow. Once the workflow is triggered the all the steps configured in the steps section will be executed and the file will be placed in the destination section:



The Steps Available in The PFTS Outbound Workflows are as follow**s**

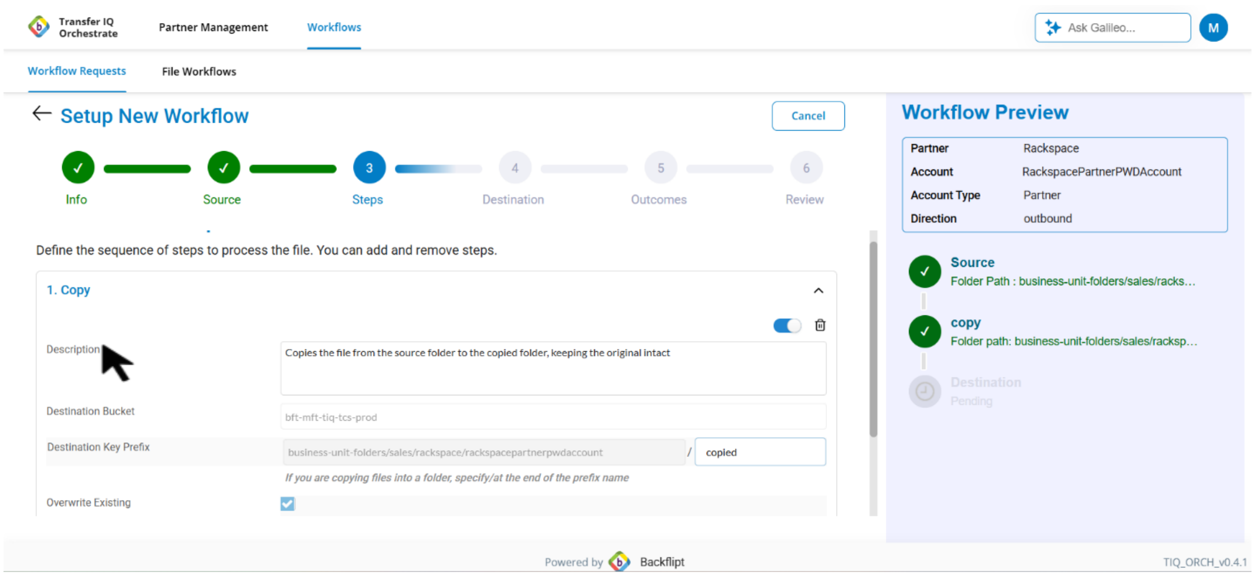
Copy - The copy step duplicates a file from the source location to the destination without deleting the original. This ensures the file remains accessible in both locations.

Below Fields are available after adding the Copy Step

- Description – A detailed description about the step added
- Source Options Consists of two options
  - **Apply on Original File** – When selected, the step will be executed on the original file located in the source.
  - **Apply on File Created from Previous Step** – When selected, the step will be executed on the output generated by the previous step.
- **Bucket Name**: The name of the storage bucket configured in metadata settings.
- **Destination Key Prefix -** The folder path or prefix within the destination bucket where the files will be placed (e.g., `Business Unit Folder/sales/{Partner}/{Partner name}`). In addition to this, a custom folder can be specified in the input field next to the Destination Key Prefix. The final file

location will be the combination of the prefix path plus the custom folder entered, determining exactly where the file will be stored after the step is executed.

- **Overwrite Existing** – This checkbox is enabled by default. If a file with the same name and extension already exists, it will be overwritten.

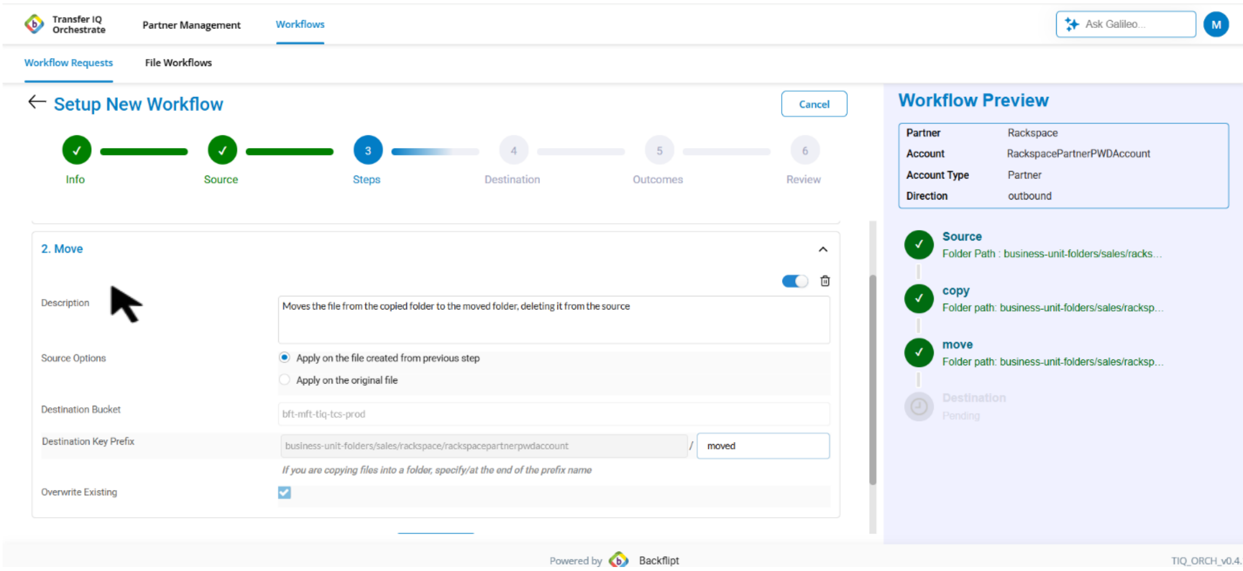


Move - The move operation shifts a file from the source location to the destination. Once moved, the file no longer exists in the source location.

Below Fields are available after adding the Move Step

- Description – A detailed description about the step added
- Source Options Consists of two options
  - **Apply on Original File** – When selected, the step will be executed on the original file located in the source.
  - **Apply on File Created from Previous Step** – When selected, the step will be executed on the output generated by the previous step.
- **Bucket Name**: The name of the storage bucket configured in metadata settings.
- **Destination Key Prefix -** The folder path or prefix within the destination bucket where the files will be placed (e.g., `Business Unit Folder/sales/{Partner}/{Partner name}`). In addition to this, a custom folder can be specified in the input field next to the Destination Key Prefix. The final file location will be the combination of the prefix path plus the custom folder entered, determining exactly where the file will be stored after the step is executed.

- **Overwrite Existing** – This checkbox is enabled by default. If a file with the same name and extension already exists, it will be overwritten.

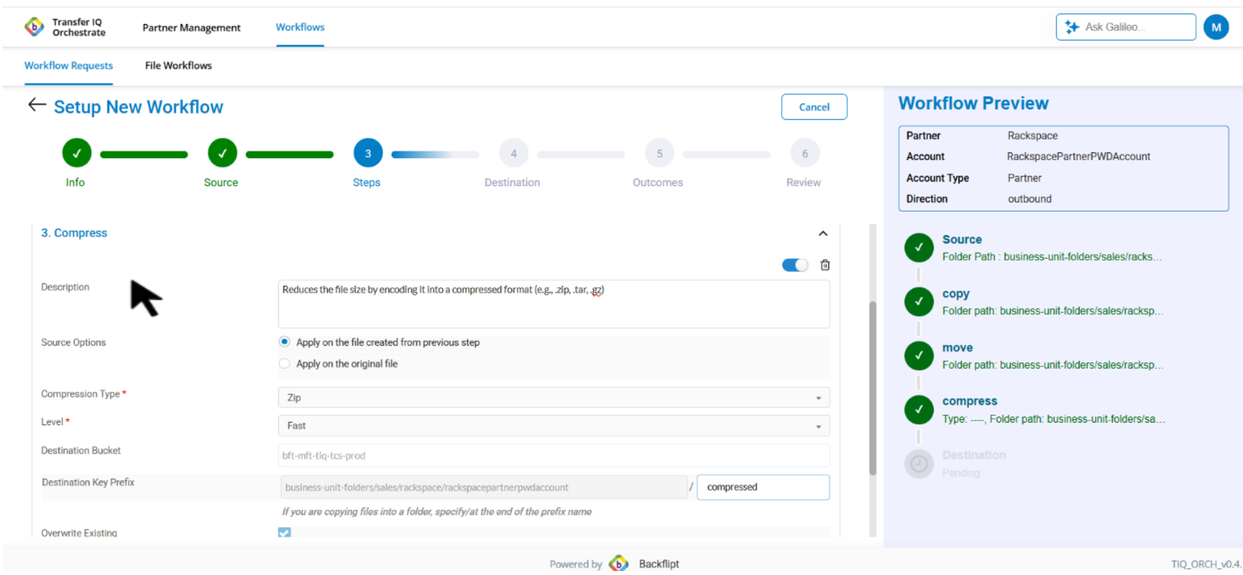


Compress - The Compress step reduces the file size by packaging the original content into a compressed format, making it more efficient for storage or transfer based on Compression Type and level

Below Fields are available after adding the compress Step

- Description – A detailed description about the step added
- Source Options Consists of two options
  - **Apply on Original File** – When selected, the step will be executed on the original file located in the source.
  - **Apply on File Created from Previous Step** – When selected, the step will be executed on the output generated by the previous step.
- Compression Type – A dropdown to select the compression type which Specifies the format used for compression (e.g., ZIP, GZIP, TAR)
  - Available options – zip, tar, zstd, gzip
- Compression Level - Defines the degree of compression applied
  - **Available levels – Store, Fastest, Fast, Normal, Good, Better, Best**
- **Bucket Name-** The name of the storage bucket configured in metadata settings.
- **Detect Type From Extension-** A checkbox that Automatically detect the compression type based on the file extension (e.g., .zip, .tar.gz). Uncheck this to manually select a compression type.
- Compression Type – A dropdown to select the Compression type (zip, tar,gzip,zstd)

- Select either detect type from extension or Compression type
- **Destination Key Prefix -** The folder path or prefix within the destination bucket where the files will be placed (e.g., `Business Unit Folder/sales/{Partner}/{Partner name}`). In addition to this, a custom folder can be specified in the input field next to the Destination Key Prefix. The final file location will be the combination of the prefix path plus the custom folder entered, determining exactly where the file will be stored after the step is executed.
- **Overwrite Existing** – This checkbox is enabled by default. If a file with the same name and extension already exists, it will be overwritten.



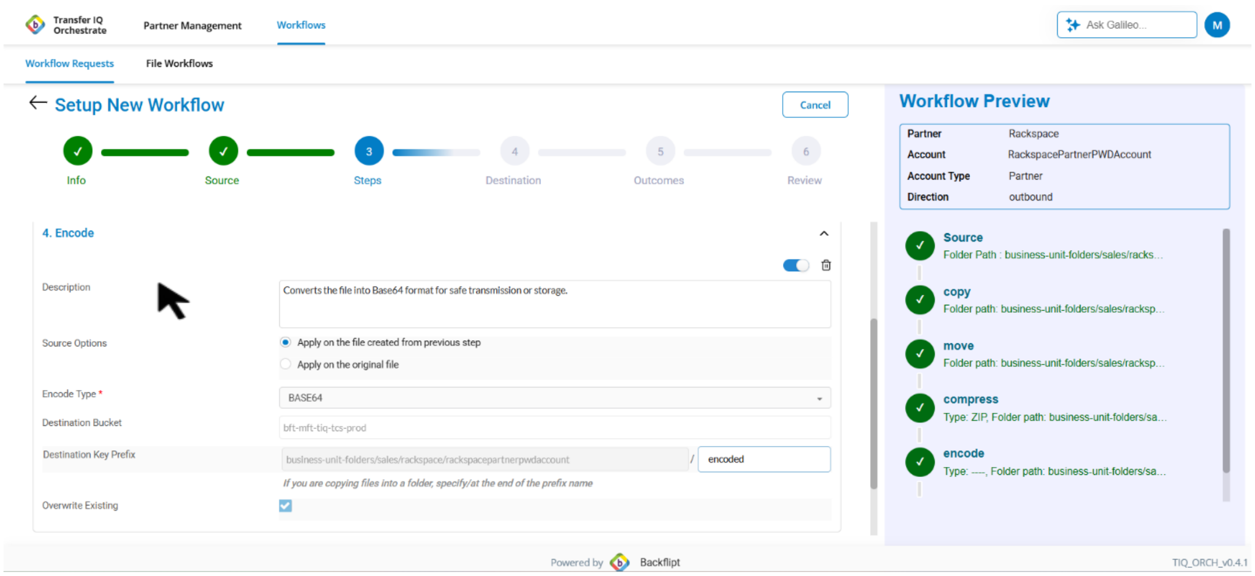
Encode - The Encode step converts a file from its original, readable format into an encoded format (for example, Base64). This is typically done to ensure safe transmission or storage of the file in systems that require encoded data.

Below Fields are available after adding the Decode Step

- Description – A detailed description about the step added
- Source Options Consists of two options
  - **Apply on Original File** – When selected, the step will be executed on the original file located in the source.
  - **Apply on File Created from Previous Step** – When selected, the step will be executed on the output generated by the previous step.
- Encode Type – A dropdown to select the encode type (Supported type: Base64)
- **Bucket Name**: The name of the storage bucket configured in metadata settings.
- **Destination Key Prefix -** The folder path or prefix within the destination bucket where the files will be placed (e.g., `Business Unit`

Folder/sales/{Partner}/{Partner name}). In addition to this, a custom folder can be specified in the input field next to the Destination Key Prefix. The final file location will be the combination of the prefix path plus the custom folder entered, determining exactly where the file will be stored after the step is executed.

- **Overwrite Existing** – This checkbox is enabled by default. If a file with the same name and extension already exists, it will be overwritten.

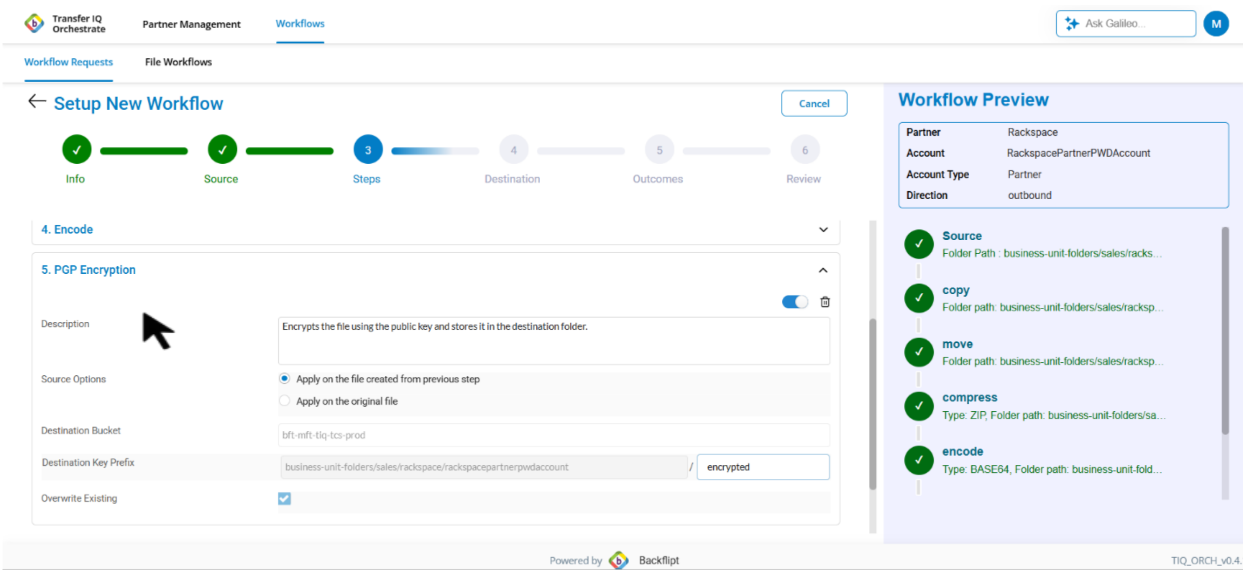


PGP Encrypt - The PGP encrypt step retrieves a plain file from the source location, encrypts it using the PGP public key provided during account creation, and places the encrypted file in the specified destination folder.

Below Fields are available after adding the Decrypt Step

- Description – A detailed description about the step added
- Source Options Consists of two options
    - **Apply on Original File** – When selected, the step will be executed on the original file located in the source.
    - **Apply on File Created from Previous Step** – When selected, the step will be executed on the output generated by the previous step.
- **Bucket Name**: The name of the storage bucket configured in metadata settings.
- **Destination Key Prefix -** The folder path or prefix within the destination bucket where the files will be placed (e.g., Business Unit Folder/sales/{Partner}/{Partner name}). In addition to this, a custom folder can be specified in the input field next to the Destination Key Prefix. The final file location will be the combination of the prefix path plus the custom folder entered, determining exactly where the file will be stored after the step is executed.

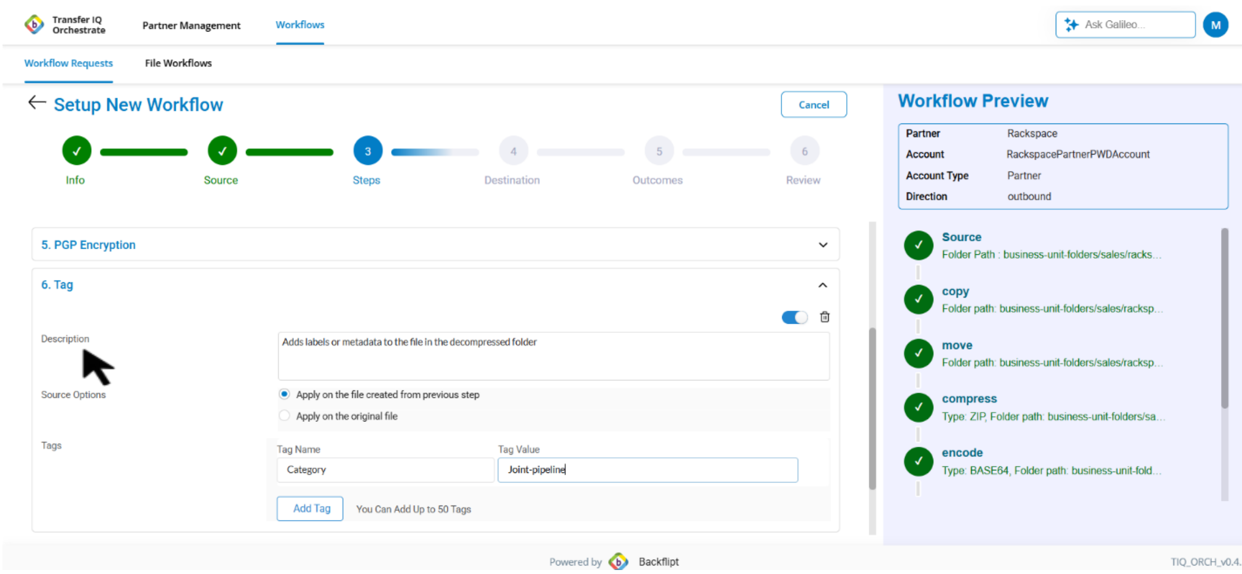
- **Overwrite Existing** – This checkbox is enabled by default. If a file with the same name and extension already exists, it will be overwritten.



Tag - The tag step allows adding additional information to files in the form of key-value pairs. This extra info helps describe, organize, and manage them more effectively. Up to 50 tags can be added per file.

Below Fields are available after adding the Tag Step

- Description – A detailed description about the step added
- Source Options Consists of two options
  - **Apply on Original File** – When selected, the step will be executed on the original file located in the source.
  - **Apply on File Created from Previous Step** – When selected, the step will be executed on the output generated by the previous step.
- **Tags Step** – This section includes fields for **Tag Name** and **Tag Value** to add tags to a file. To add more tags, click the **Add Tag** button. Each tag also has a **Remove** button, allowing it to be deleted if needed.

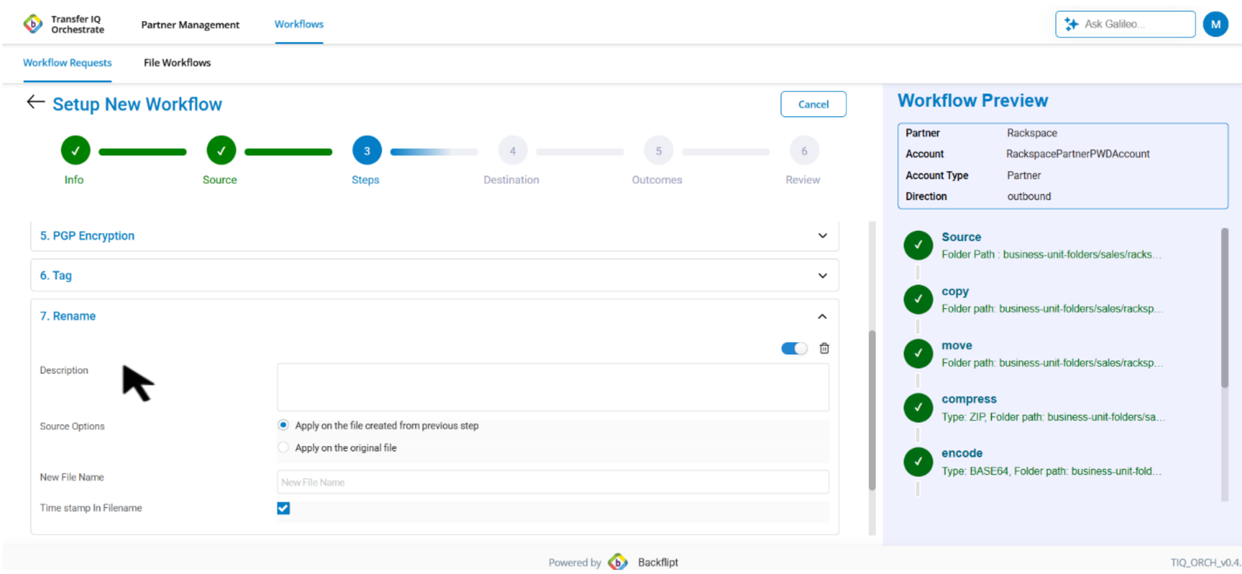


Rename - The **rename step** changes the name of a file. This helps organize files by giving them clear, consistent, or updated names without altering their content or location.

Below Fields are available after adding the Rename Step

- Description – A detailed description about the step added
- Source Options Consists of two options
  - **Apply on Original File** – When selected, the step will be executed on the original file located in the source.
  - **Apply on File Created from Previous Step** – When selected, the step will be executed on the output generated by the previous step.
- **New File Name** – Enter the Renamed New file name
- **Timestamp in Filename** – A checkbox that, when enabled, adds a timestamp to the file name during the rename step execution

In addition to adding the steps there are some other actions like deleting and disabling a step



Delete a Step

A delete icon button is available to remove a step after it has been added. To delete a step, click the delete button. A confirmation popup will appear with "Yes" and "No" options, along with a final **Delete** button:

- If **"Yes"** is selected and the **Delete** button is clicked, the step will be permanently removed.
- If **"No"** is selected, the popup will close, and the step will remain unchanged.

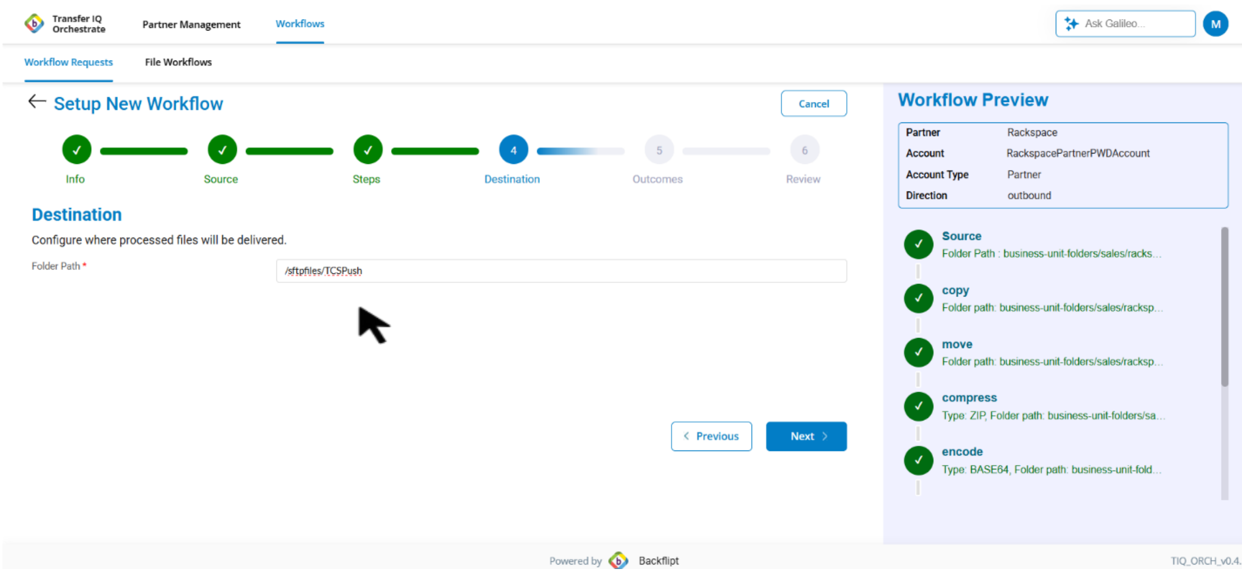
Sure! Here's a clear and polished rephrased version:

Disable a Step

A toggle switch is located at the top-right corner of each step. When enabled, the step will be executed as part of the workflow. If disabled, the step will be skipped during workflow execution.

Once all the steps are added, click the next button to navigate to the destination section

Destination



Outcomes

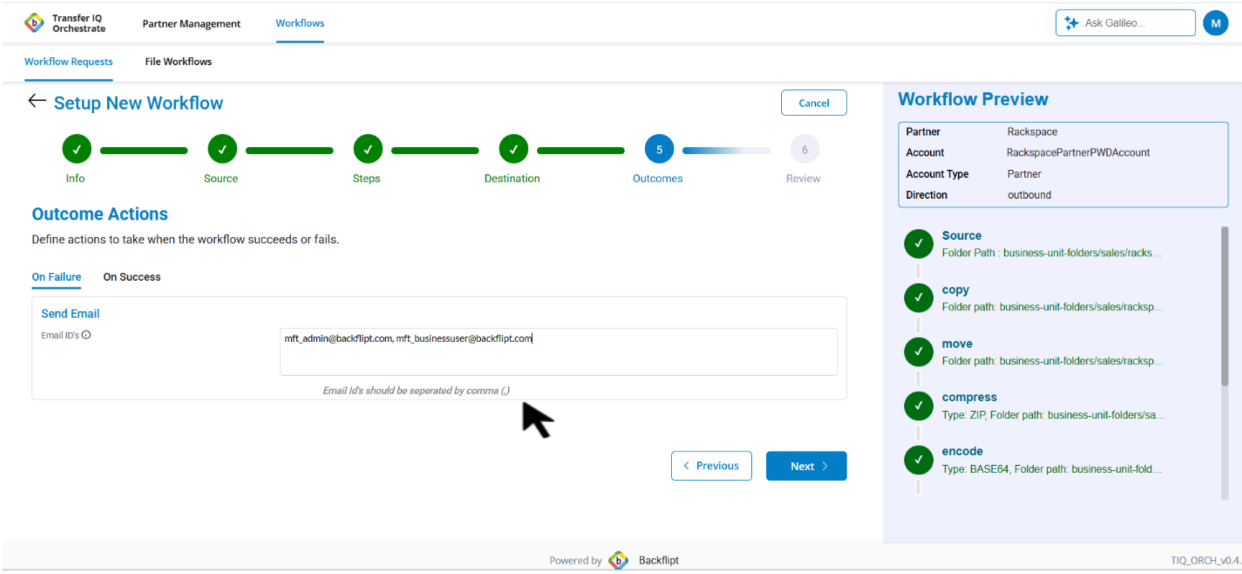
The Outcomes section consists of two tabs:

1. On Success
2. On Failure.

On Success – Notify the email entered upon successful file transfer.

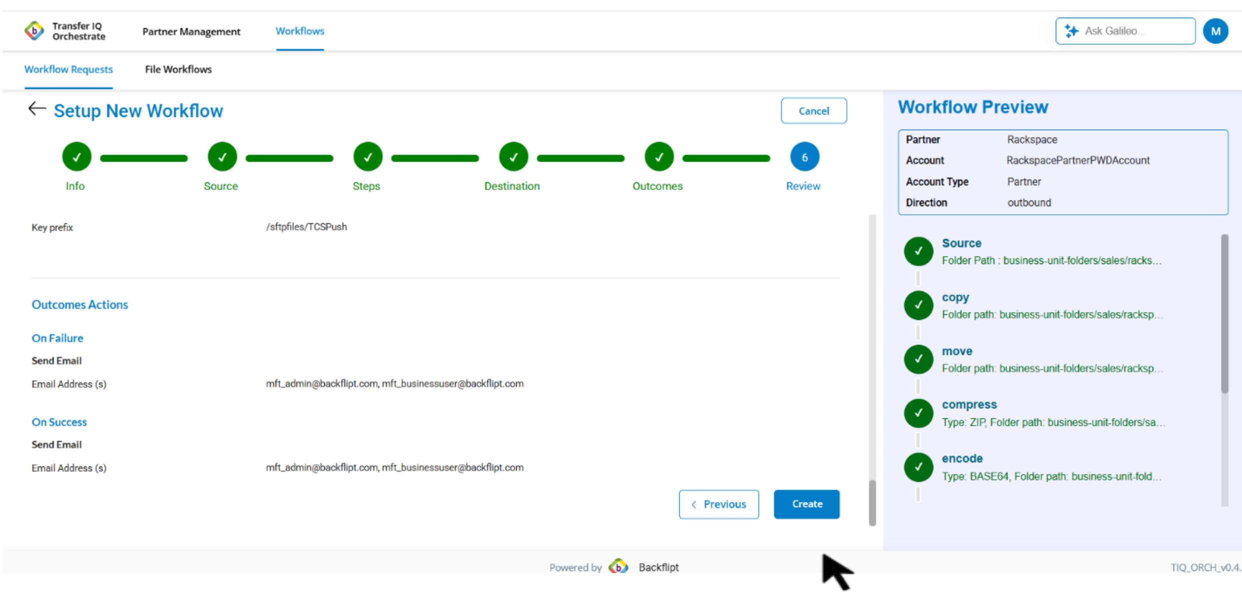
On Failure – Notify the email entered if the file transfer fails.

Note: Enter Comma Separated Emails to notify multiple emails

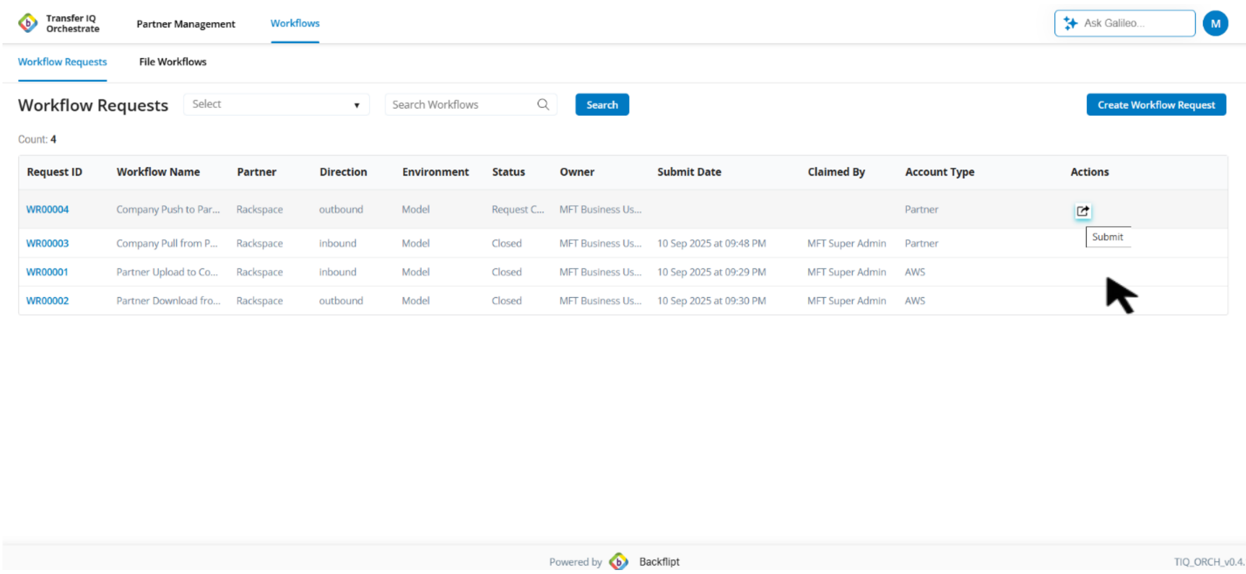


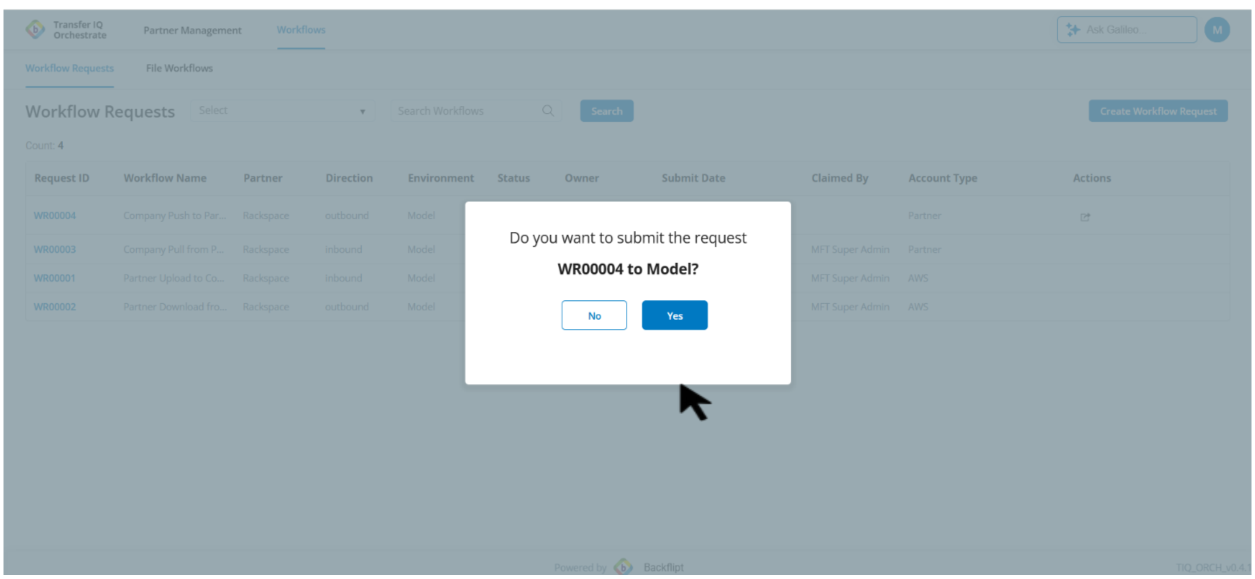
Review

Review all the details provided during the workflow request creation. If everything is correct, the Business User can proceed to create the workflow request. If any changes are needed, use the Previous button to go back and make edits



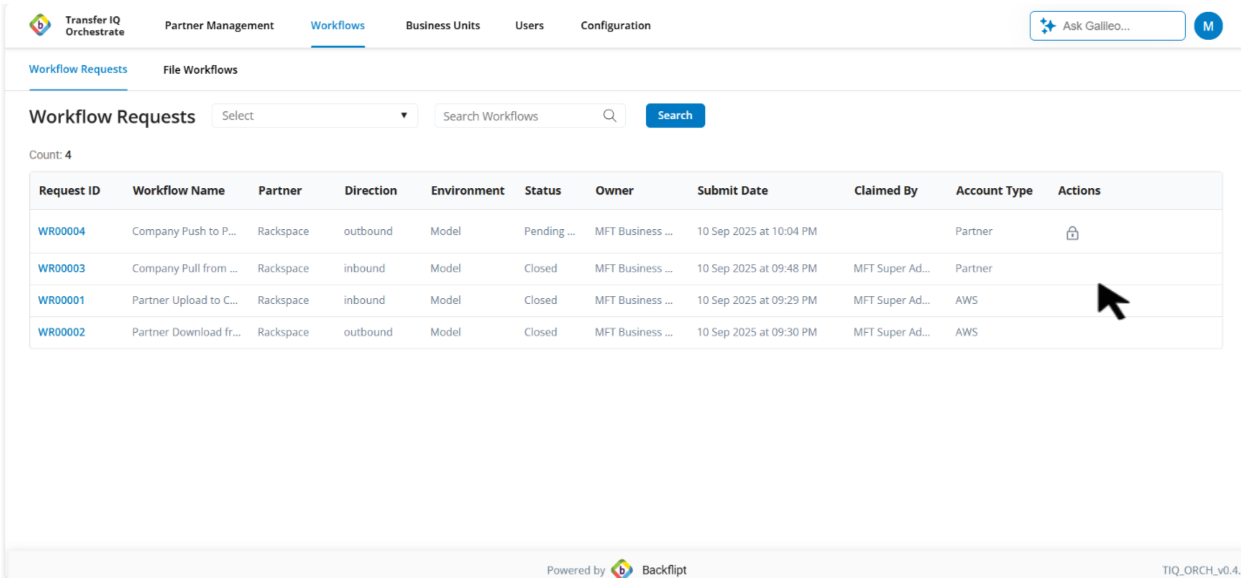
Once the workflow request creation is done, Business User submits the request to the admin for approval, it becomes visible to all admins under the Workflow Requests tab.

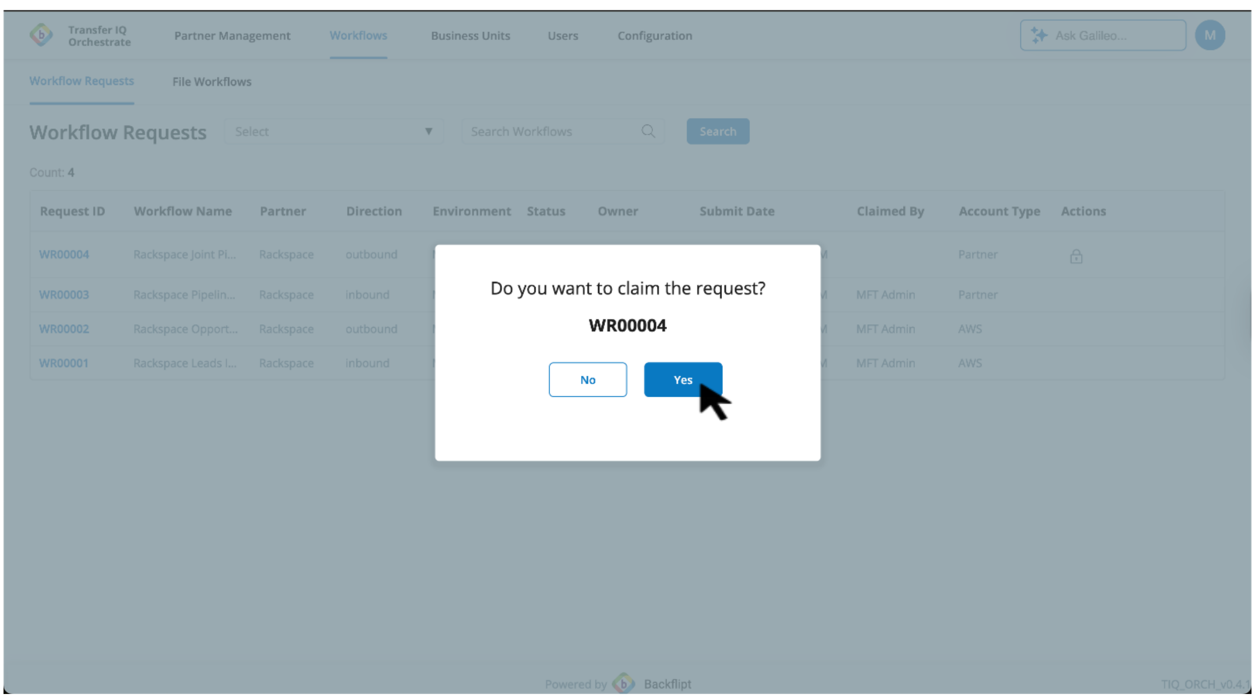




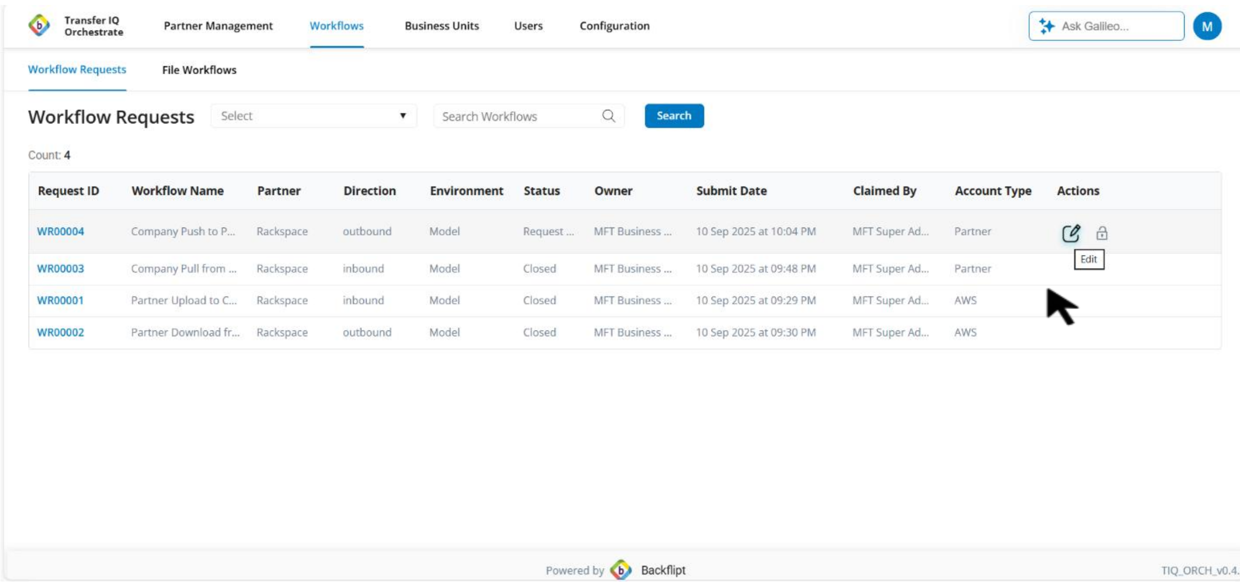
Admin Approval – PFTS Outbound Workflow request

An admin can claim the request to take ownership in one of two ways: by clicking the View Request button in the email notification sent after submission, or by locating and claiming the request directly from the Account Onboarding tab.

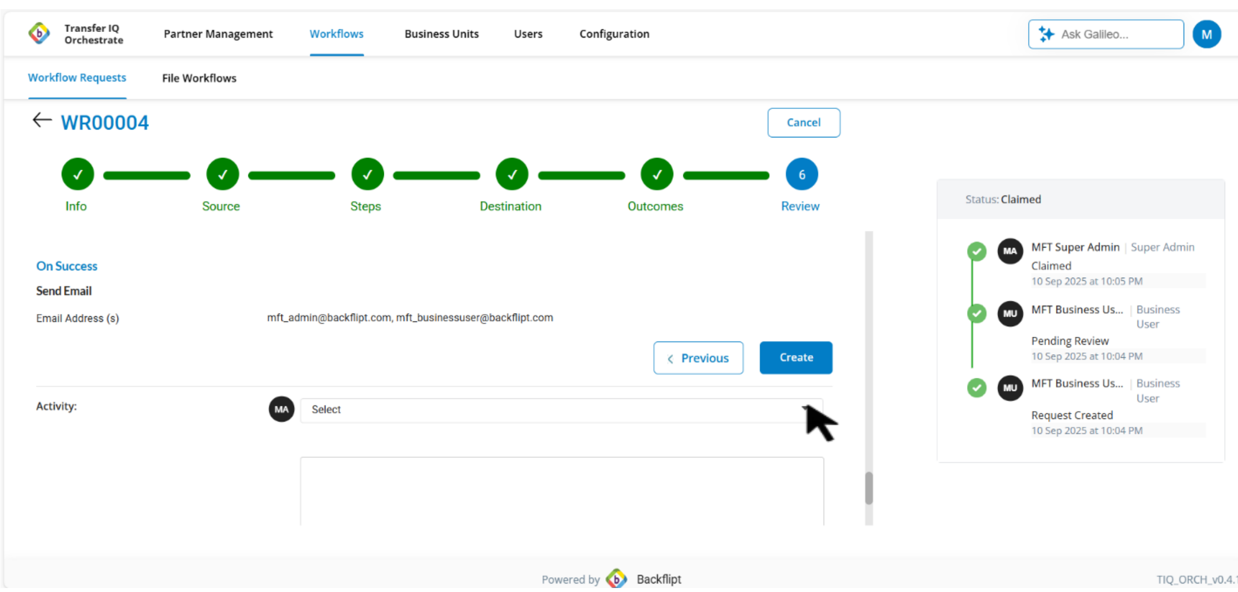




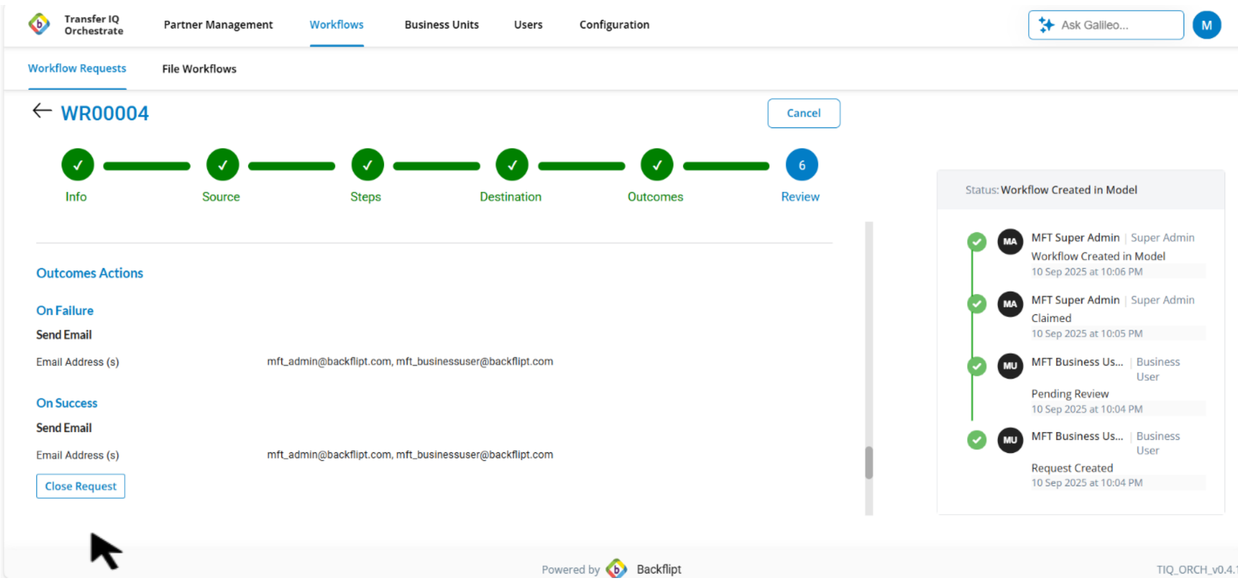
After claiming the request, the admin can view all the details provided by the Business User in edit mode.

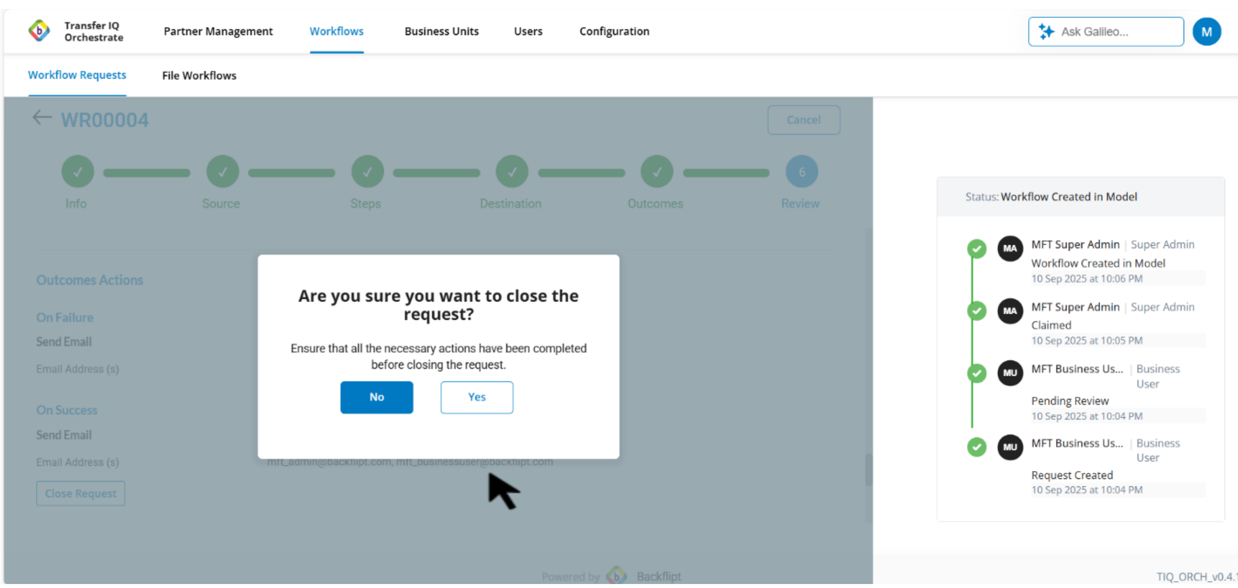


The admin has the option to review, modify, or update any information if changes are needed. If no changes are required, the details can be left as they are and Click the Create button to create the workflow

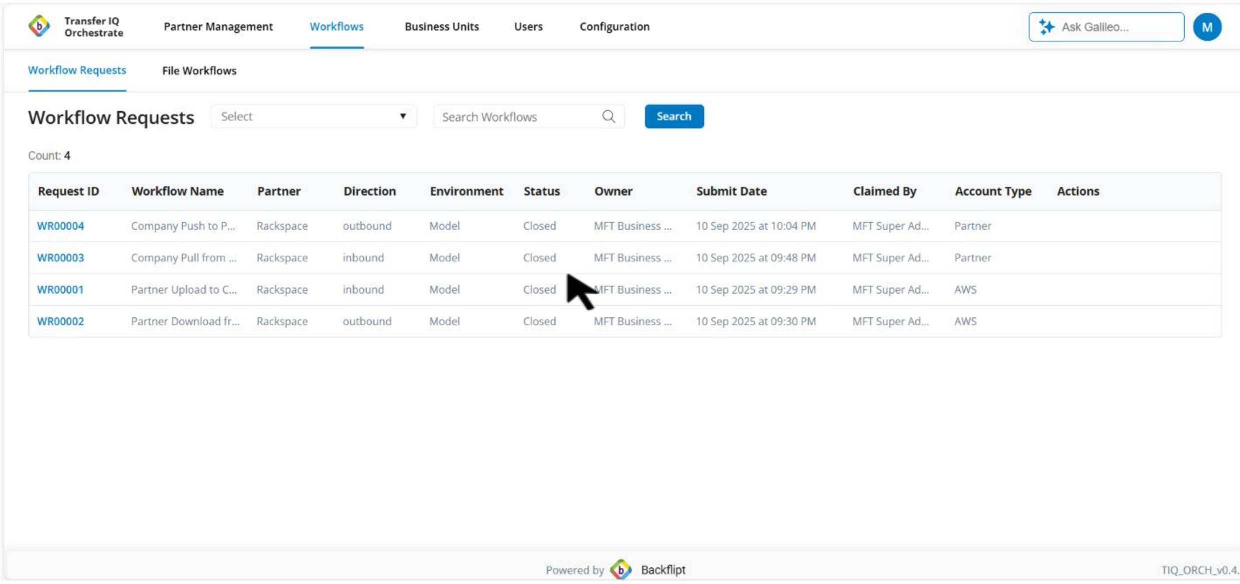


After the workflow is created, the admin can proceed to close the request, as no further action is required. Clicking the **Close Request** button triggers a confirmation prompt.





Once confirmed, the request is marked as **Closed**, and the page redirects back to the Workflow Requests table, where the request is now listed with a status of **Closed**.



File Transfers

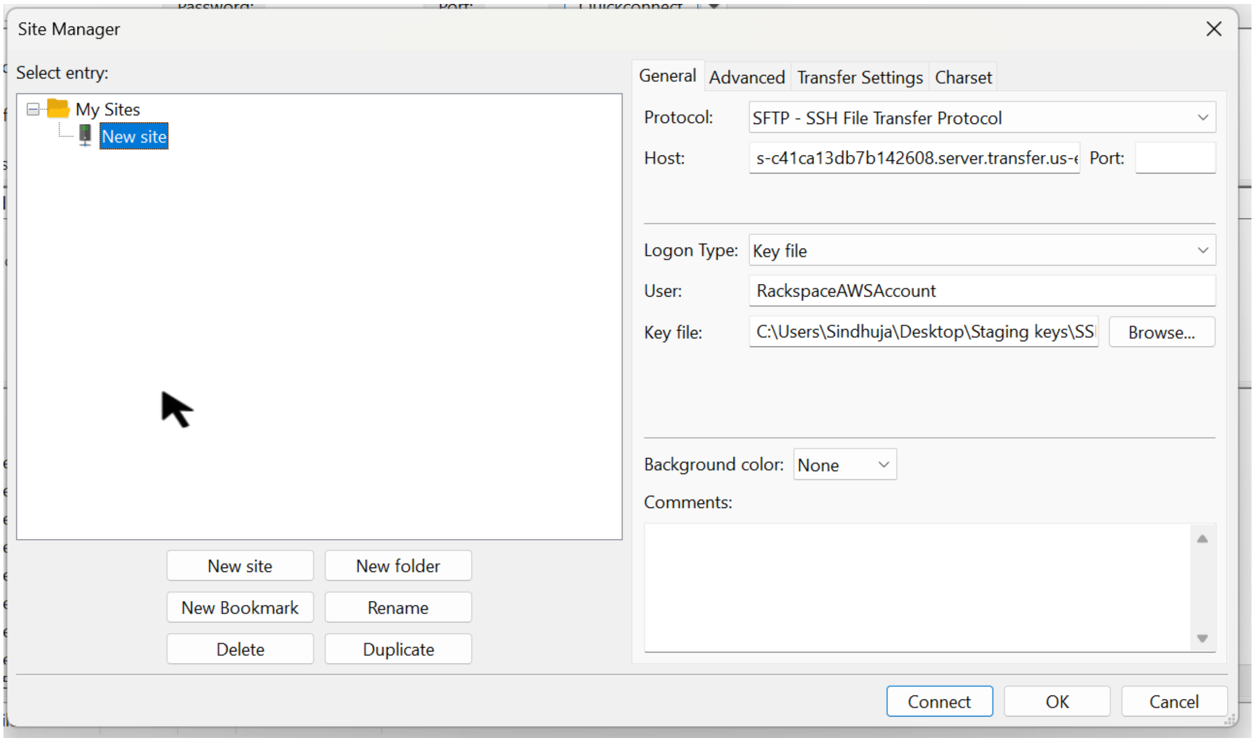
File Transfer for AWS Transfer Family Account Inbound Workflow

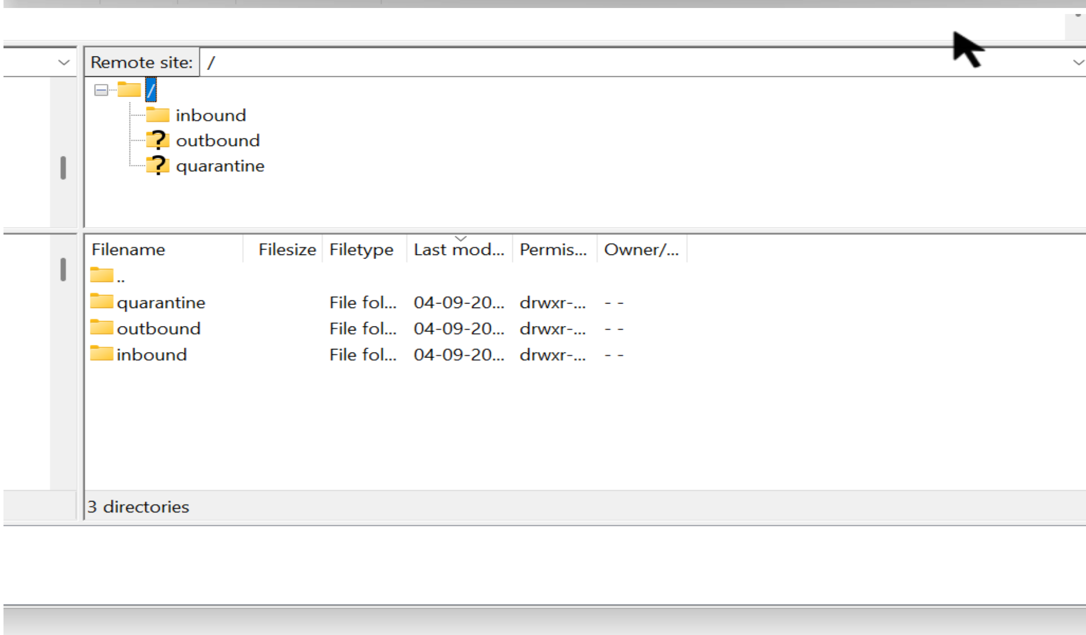
All incoming files from the partner to the company's business unit folder on the company's server will come under AWS Inbound File transfers

In AWS Inbound File Transfer, the partner connects to the company server using an external client (e.g., FileZilla) using the following details

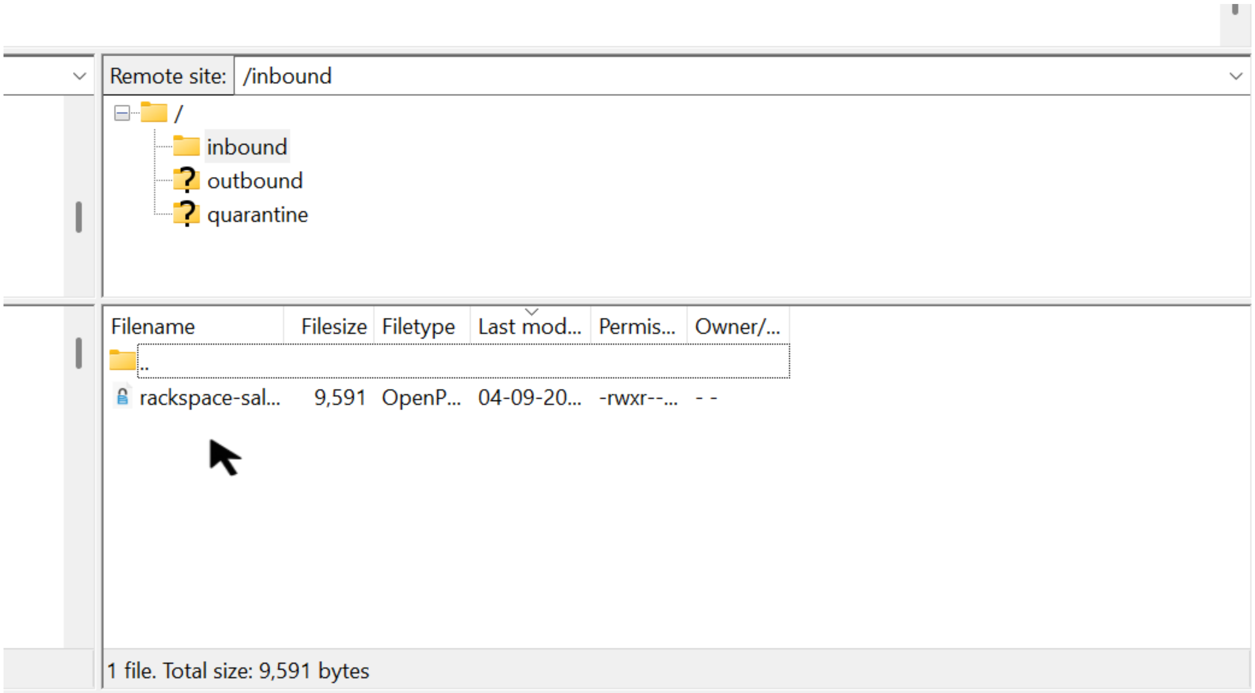
- Server SFTP endpoint
- SSH private key
- Username.

Click the Connect button to connect to the server





1. Once the partner connects to the Server, Partner uploads files into the inbound folder within the user account folder (for example:`efts-folder/{partneraccount}/inbound`)

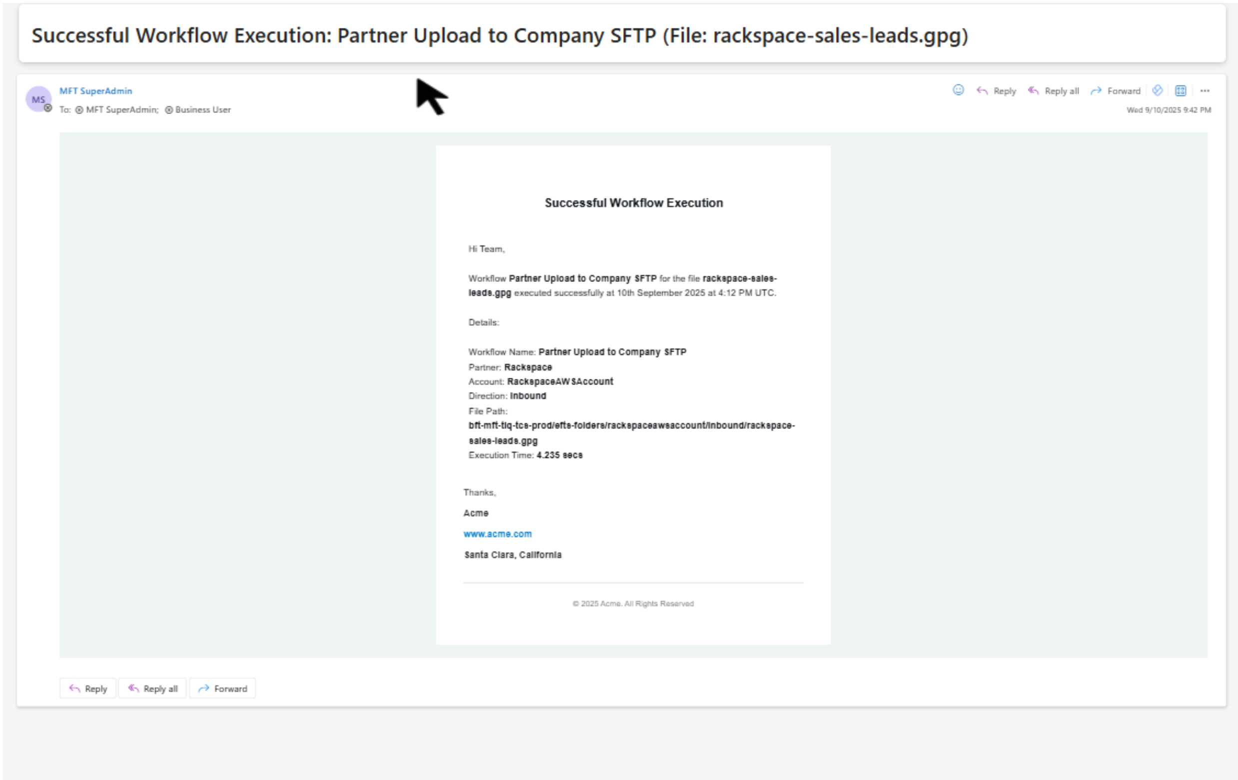


2. This folder serves as the source location as it is specified during workflow creation.
3. Once a file is placed in the source folder, all workflows associated with that user account are evaluated. If there is a single workflow, it is triggered immediately. If multiple workflows exist for the account, the best matching workflow based on the uploaded file will be triggered and The steps defined in the chosen workflow are executed.
4. Finally, the processed file is placed into the destination folder within the company's destination bucket. For example, the destination path could be: `Bucket/BusinessUnitFolder/Partner/partneraccount/inbound`, as specified during the workflow setup.

Workflow Execution Status Email for AWS Inbound File Transfer

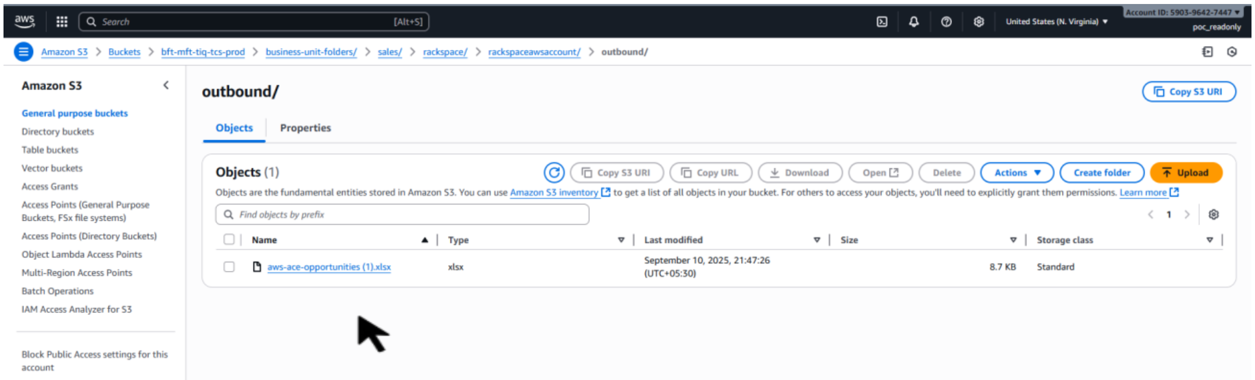
- If the file transfer and workflow execution are successful, an email notification is sent to the addresses specified in the **"OnSuccess"** tab of the *Outcomes* section during workflow creation.

- If the transfer or workflow fails, an email is sent to the addresses specified in the **"OnFailure"** tab of the *Outcomes* section.
- If no email addresses are provided in either section, **no notifications** will be sent.



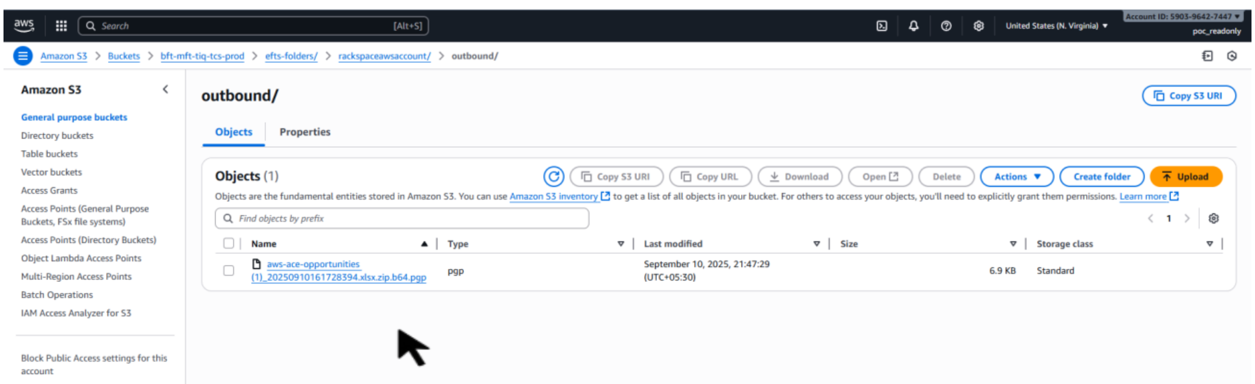
File Transfer for AWS Transfer Family Account Outbound Workflow

1. All outgoing files from the company to the partner for AWS Accounts come under AWS Outbound File Transfers.
2. For AWS Outbound File Transfers, the company accesses the AWS console using the Business User login credentials.
3. Once the login is successful, the Business User uploads the file to the S3 bucket within the business unit folder (for example: `Bucket/BusinessUnitFolder/Partner/partneraccount/outbound`). This folder serves as the source location, as it is specified during workflow creation.



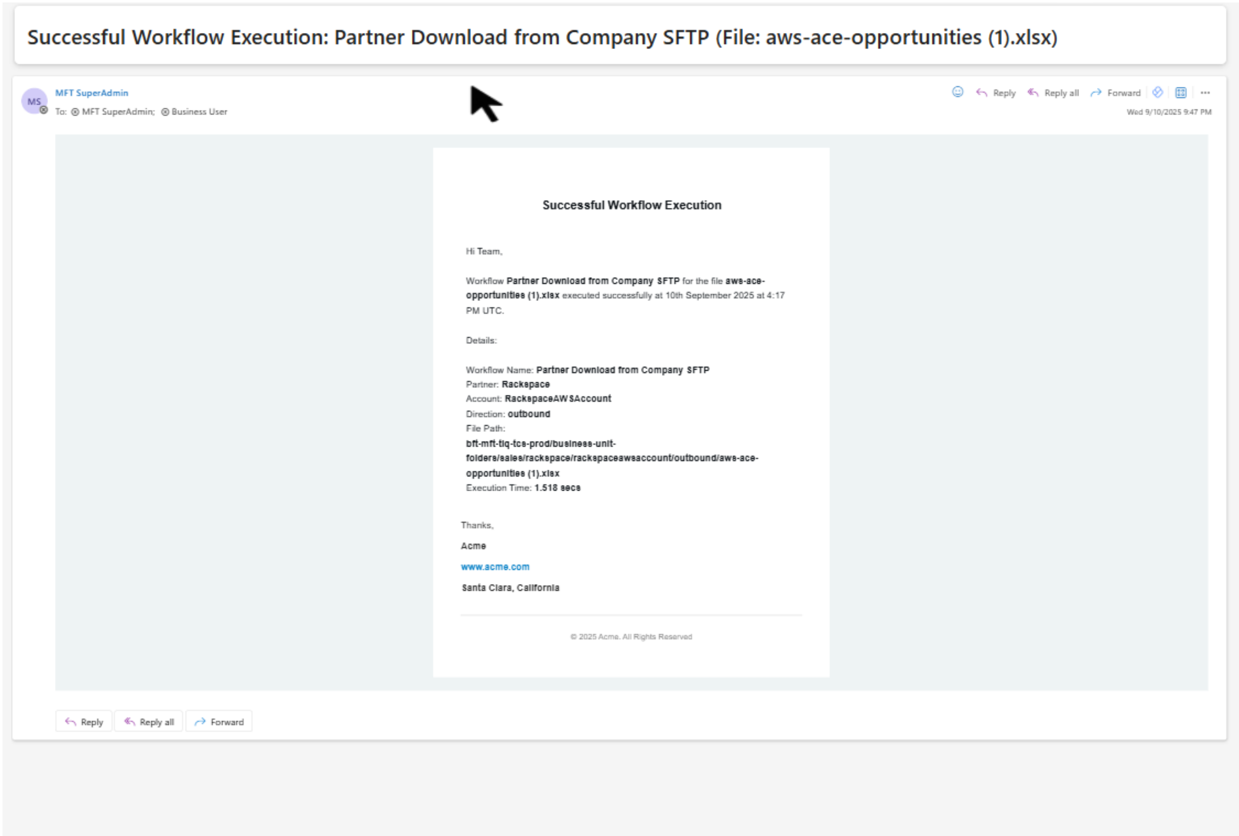
4. When a file is placed in the source folder, all workflows associated with that user account are evaluated. If only one workflow exists, it is triggered immediately. If multiple workflows are available, the best matching workflow based on the file is triggered, and the steps defined in the selected workflow are executed.

Finally, the processed file is transferred to the destination folder or endpoint, as defined in the workflow setup.



Workflow Execution Status Email for AWS Outbound File Transfer

- If the file transfer and workflow execution are successful, an email notification is sent to the addresses specified in the **"OnSuccess"** tab of the *Outcomes* section during workflow creation.
- If the transfer or workflow fails, an email is sent to the addresses specified in the **"OnFailure"** tab of the *Outcomes* section.



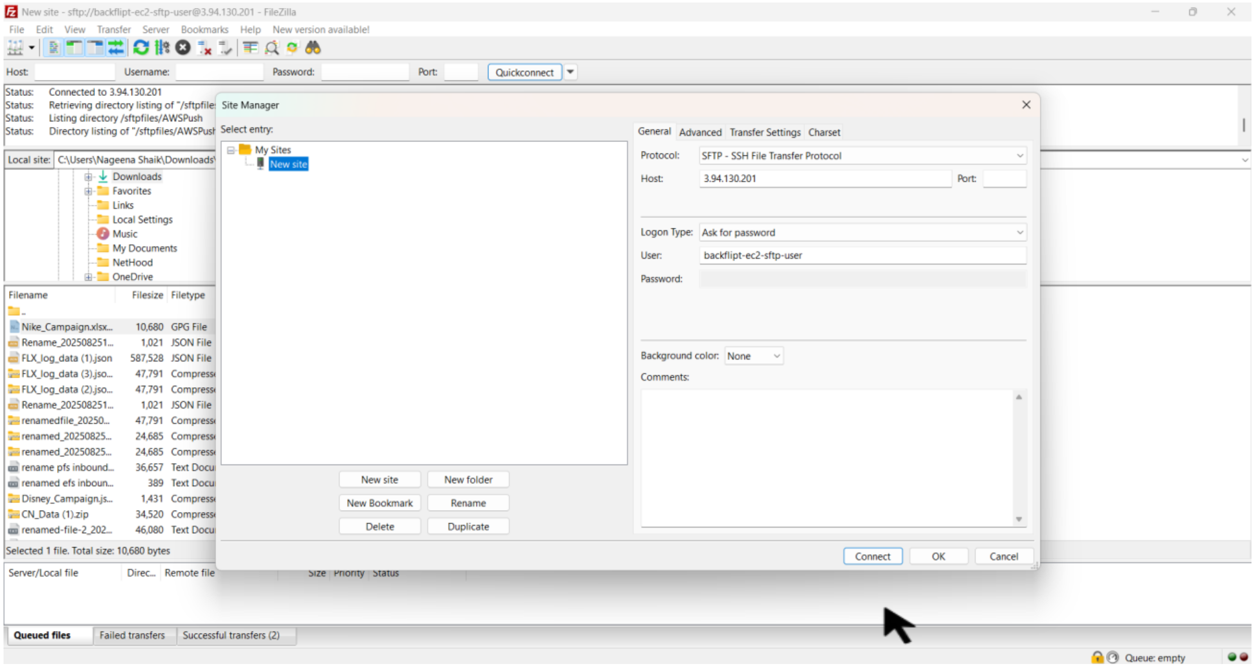
If no email addresses are provided in either section, **no notifications** will be sent

File Transfer for Partner Hosted Account Inbound Workflow

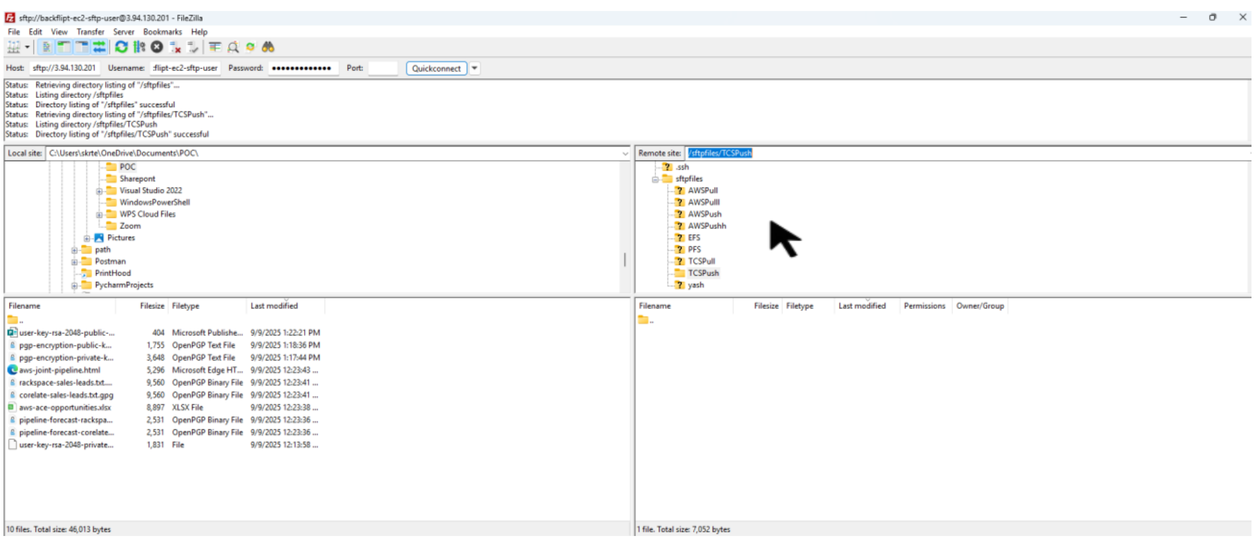
All incoming files from the partner's external server to the company's s3 bucket come under **PFTS Inbound File Transfers**.

In PFTS Inbound File Transfers, the partner connects to their server using an external client (e.g., FileZilla) with the following details:

- Server SFTP endpoint
- SSH private key/Password - Based on Login Method Selected
- Username



Once connected, the partner uploads files to the source folder. This source folder is provided by the partner to the company, and the company creates workflows based on this specified folder.



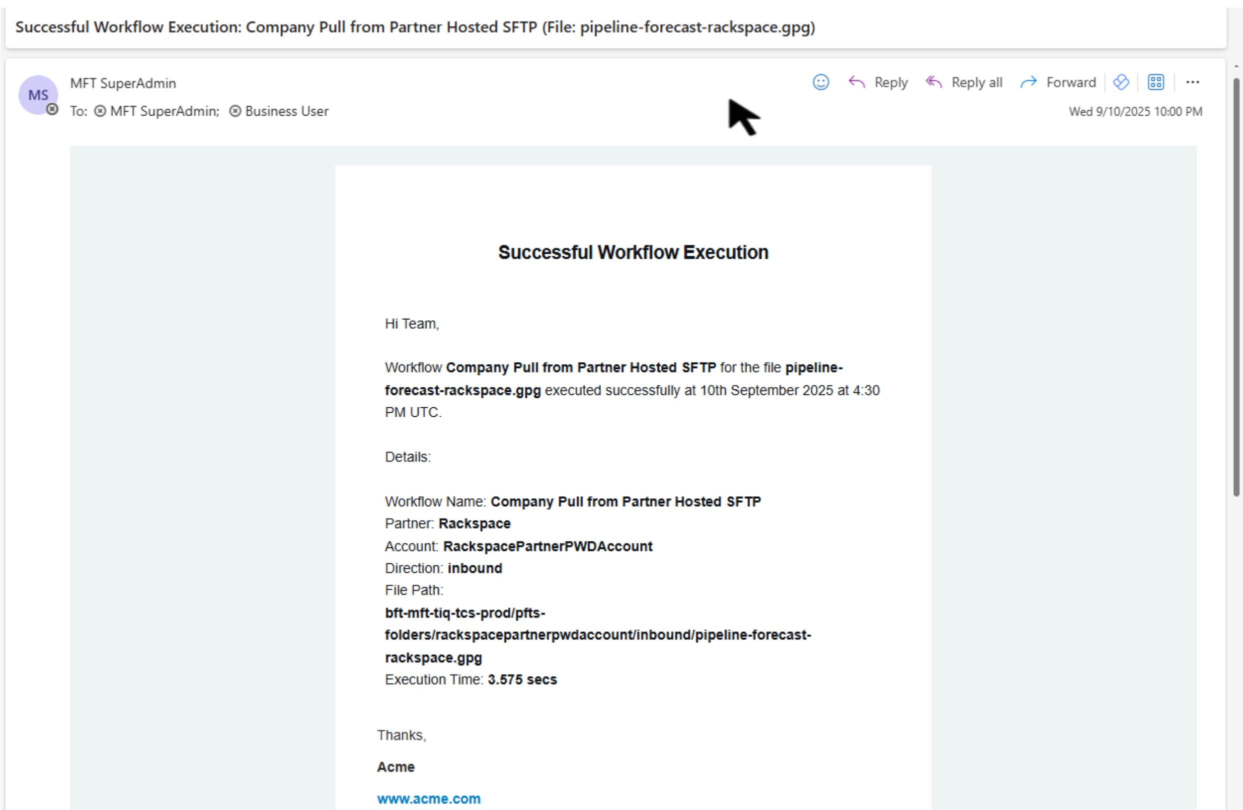
Workflows in PFTS Inbound File Transfers are triggered according to a scheduled time set during workflow creation. Files are pulled from the partner's server on this scheduled basis.

1. When the scheduled time arrives, all workflows associated with the account are evaluated. If there is only one workflow, it is triggered immediately. If multiple workflows exist, the best matching workflow based on the uploaded file is triggered.

2. Upon workflow trigger, the file is pulled from the partner's server into the company's S3 bucket at the path: `pfts-folders/partneraccount/inbound`.
3. After the file is pulled into the company's bucket, the steps defined in the selected workflow are executed.
4. Finally, the processed file is placed into the destination folder within the company's destination bucket. For example, the destination path might be: `Bucket/BusinessUnitFolder/Partner/partneraccount/inbound`, as specified during the workflow setup.

Workflow Execution Status Email for PFTS Inbound File Transfers

- If the file transfer and workflow execution are successful, an email notification is sent to the addresses specified in the **"OnSuccess"** tab of the *Outcomes* section during workflow creation.

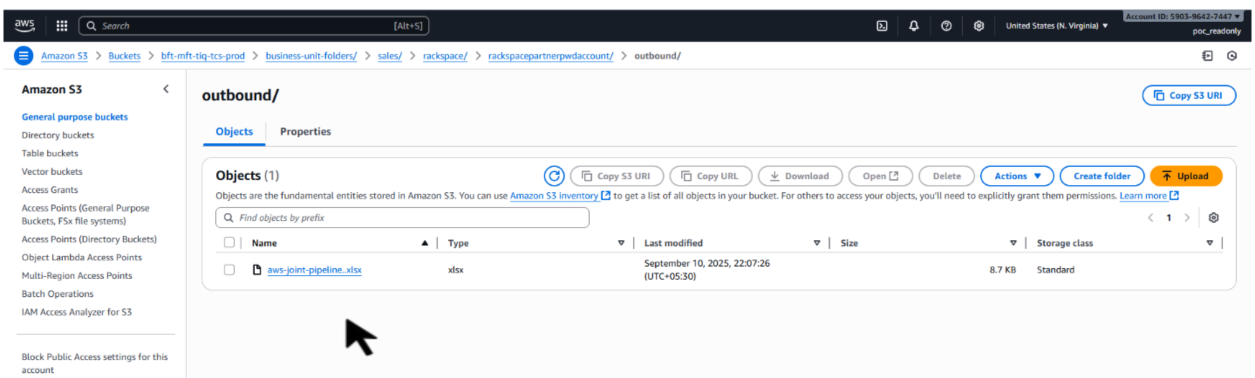


- If the transfer or workflow fails, an email is sent to the addresses specified in the **"OnFailure"** tab of the *Outcomes* section.
  If no email addresses are provided in either section, **no notifications** will be sent

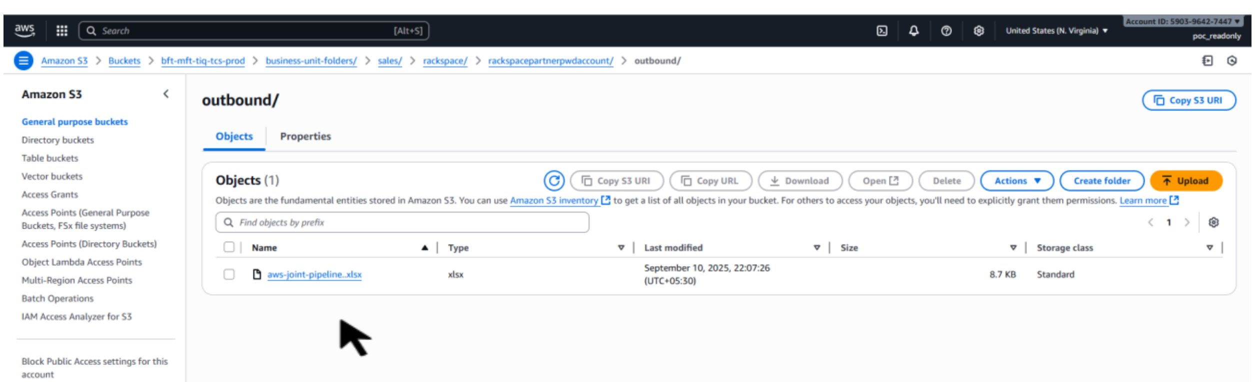
File Transfer for Partner Hosted Account Outbound Workflow

All outgoing files from the company's S3 bucket to the partner's external server come under **PFTS Outbound File Transfers**.

5. In PFTS Outbound File Transfers, the company **pushes** files from source folder in its **Company's** S3 bucket to the partner's external server. This process is **not scheduled** — the file transfer is **triggered immediately** when a file is placed in the source folder.
6. For AWS Outbound File Transfers, the company accesses the AWS console using the Business User login credentials.
7. Once the login is successful, the Business User uploads the file to the S3 bucket within the business unit folder (for example: `Bucket/BusinessUnitFolder/Partner/partneraccount/outbound`). This folder serves as the source location, as it is specified during workflow creation.



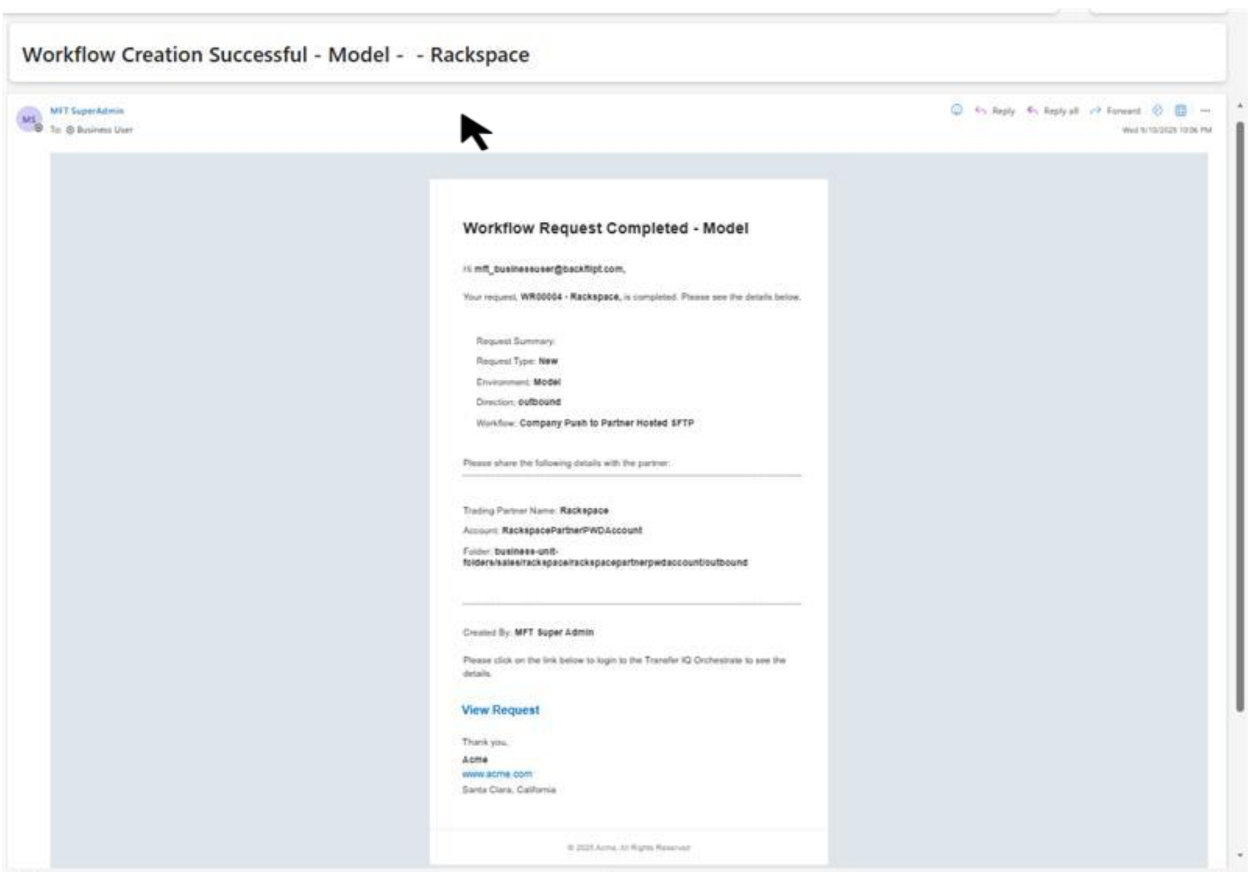
8. Once the workflow is triggered, the file is pushed from the company's S3 bucket (Business Unit folder) to the company's PFTS S3 bucket at the following path: **`pfts-folders/partneraccount/outbound`**



9. After the file has been successfully transferred to the PFTS S3 bucket, the steps defined in the selected workflow continue execution.
10. Finally, the processed file is delivered to the destination folder on the partner’s server. This destination path is provided by the partner and configured by the company during the workflow setup in the "Destination" section.

Workflow Execution Status Email for PFTS Outbound File Transfer

- If the file transfer and workflow execution are successful, an email notification is sent to the addresses specified in the **"OnSuccess"** tab of the *Outcomes* section during workflow creation.



- If the transfer or workflow fails, an email is sent to the addresses specified in the **"OnFailure"** tab of the *Outcomes* section.
  If no email addresses are provided in either section, **no notifications** will be sent

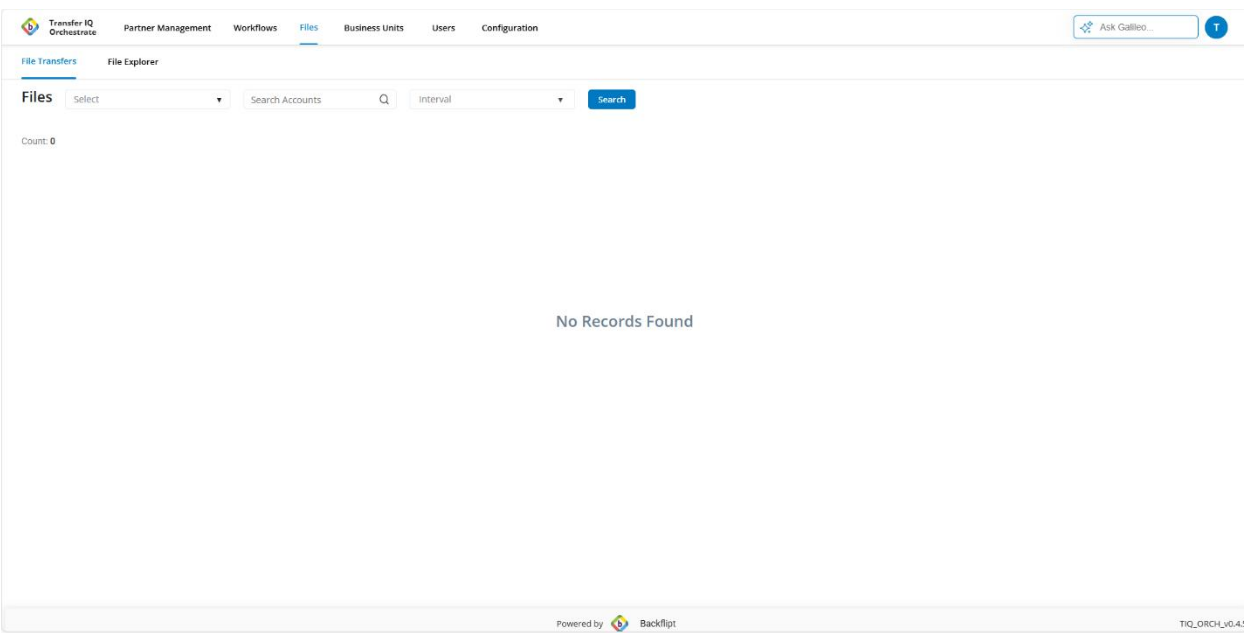
Files

The File tab consists of two tabs file transfers and file explorer. It allows users to upload files via file explorer tab and monitor the uploaded file transfer status in file transfer tab.

File Transfer:

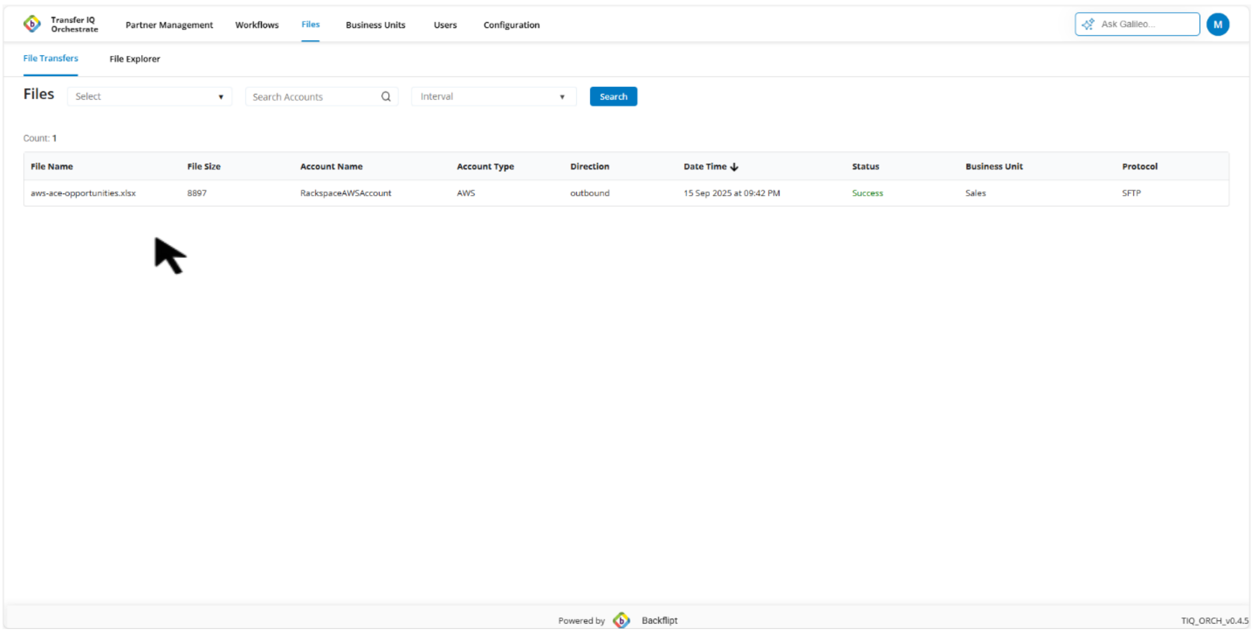
The File Transfers tab provides a summary of all file transfers performed through the system. It allows users to monitor inbound and outbound file activities, check transfer details, and verify whether each transfer was successful or not. This section is mainly used for tracking and troubleshooting file transfers.

Upon clicking on the File tab user will be redirected to the Files>File Transfers section. When no file transfers are done, initially no records will be displayed.



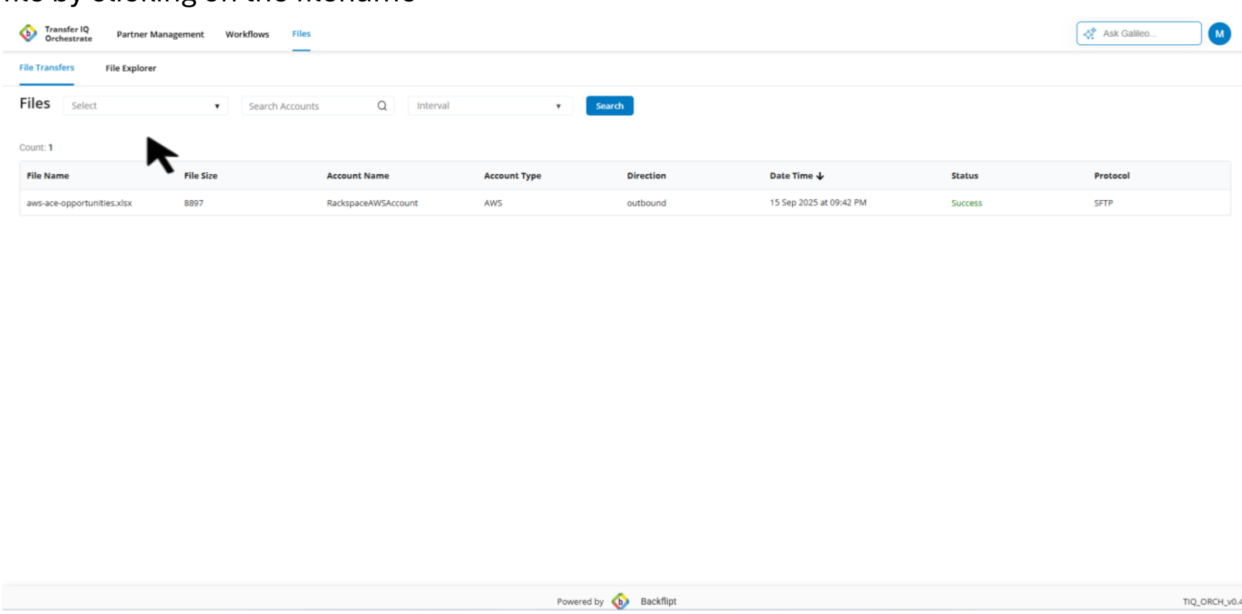
Admin Screen:

Admin can view the file transfer status of all business units. Once file transfer is completed, user can view the details related to the transferred status of the file



Business User Screen:

Business User can view the file transfer status of only the associated business unit. Once file transfer is completed, user can view the details related to the transferred status of the file by clicking on the filename

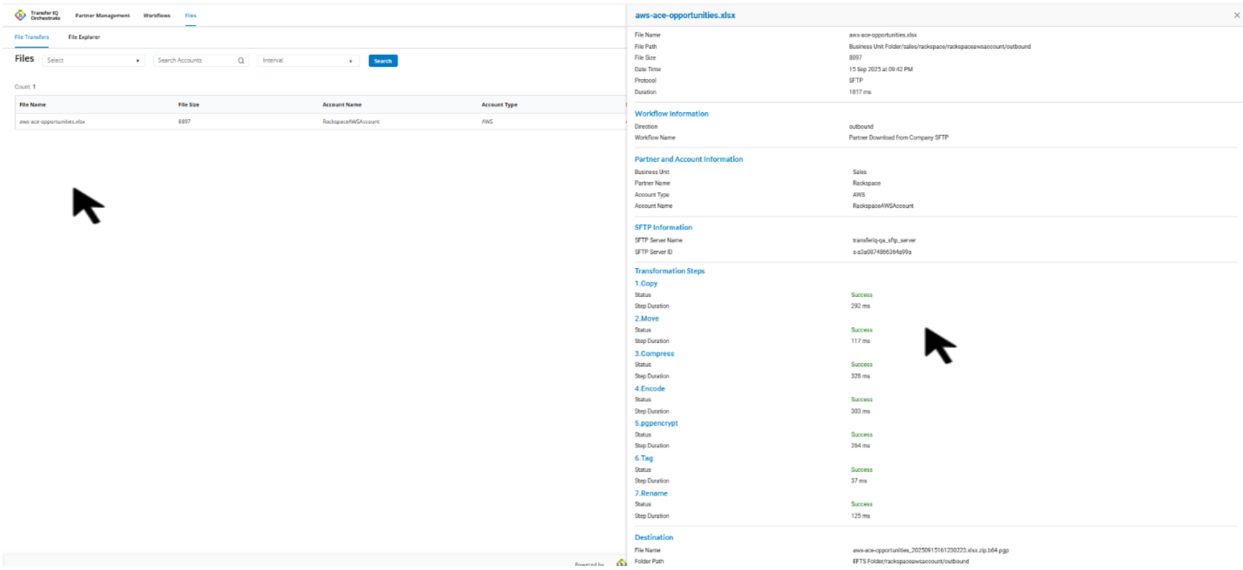


The Files table in the File Transfers tab consists of several columns, each providing specific details about the transfer.

- **File Name:** This column displays the name of the file that has been transferred. It helps users quickly identify which specific file is part of the transfer. If the field is empty, it means no file name was captured for that record.
- **File Size:** The File Size column shows the size of the file, which ensures that the complete file was transferred successfully.
- **Account Name:** This column indicates the name of the account involved in the transfer. It helps in identifying which external partner or internal account the file belongs to, making tracking easier.
- **Account Type:** This column specifies the type of account associated with the transfer. For example, it may show Partner or AWS account type. This information helps in classifying the transfer source or destination.
- **Direction:** This column highlights whether the file transfer is inbound or outbound. Inbound transfers refer to files coming into the system, while outbound transfers represent files being sent out to partners or external systems.
- **Date Time:** This column records the exact date and time when the transfer occurred. Having a timestamp helps in tracking the file movement.
- **Status:** This column shows the outcome of the transfer, with three possible values:

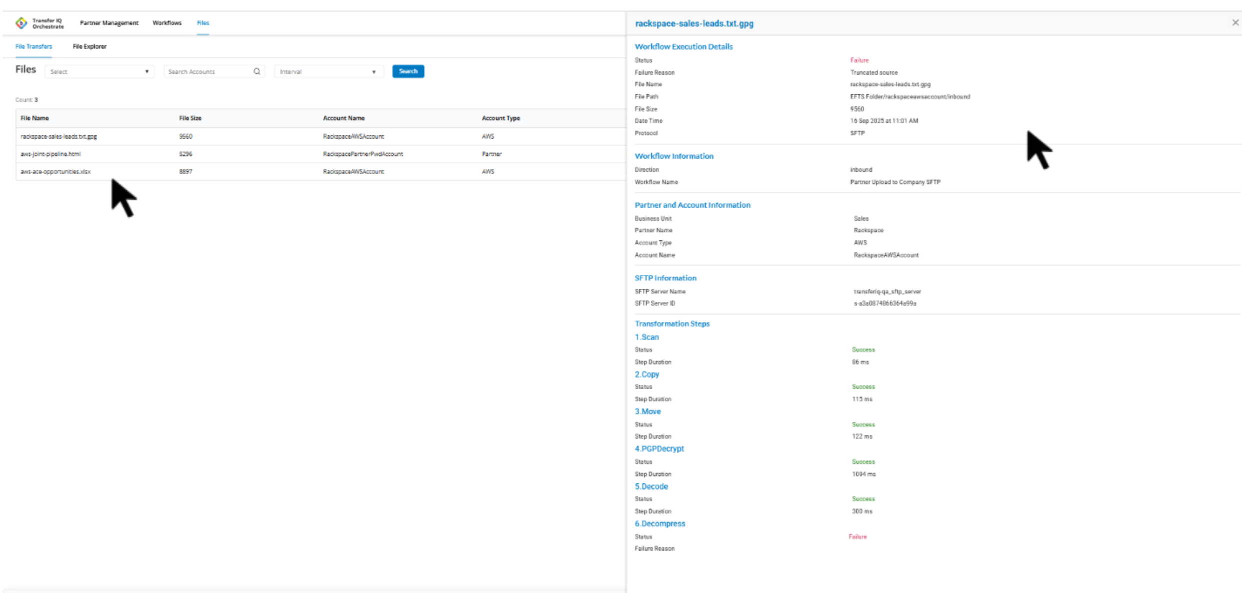
1. **Success** → The file transfer is completed successfully. This means all the transformation steps have been executed without any errors, and the file has been transferred correctly.

- When the file transfer is successful, the detailed view shows all the sections including workflow execution details, workflow information, partner and account details, SFTP information, transformation steps, and the destination section. Each transformation step (like copy, compress, encrypt, etc.) will also display its status and duration.



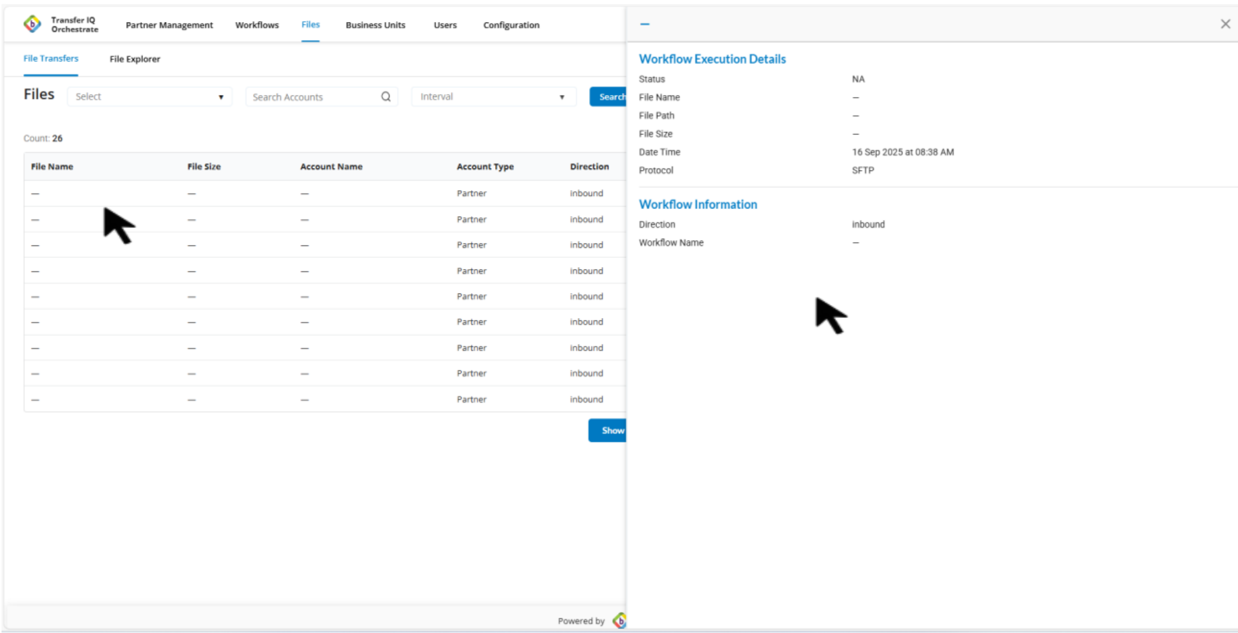
2. **Failure** → If any transformation step fails during the process, the file is not transferred successfully. In this case, the entire status of the transfer is marked as Failure.

- If the file transfer has failed, the detailed view still shows all the sections. In the transformation steps, you can clearly see which specific step has failed, along with the reason for failure. This helps in identifying the exact issue that caused the transfer to fail.



3. **NA** → This status appears when the uploaded file does not match the required file name pattern or when no workflow is triggered. Since the transformation steps are not executed in such cases, the transfer is marked as NA.

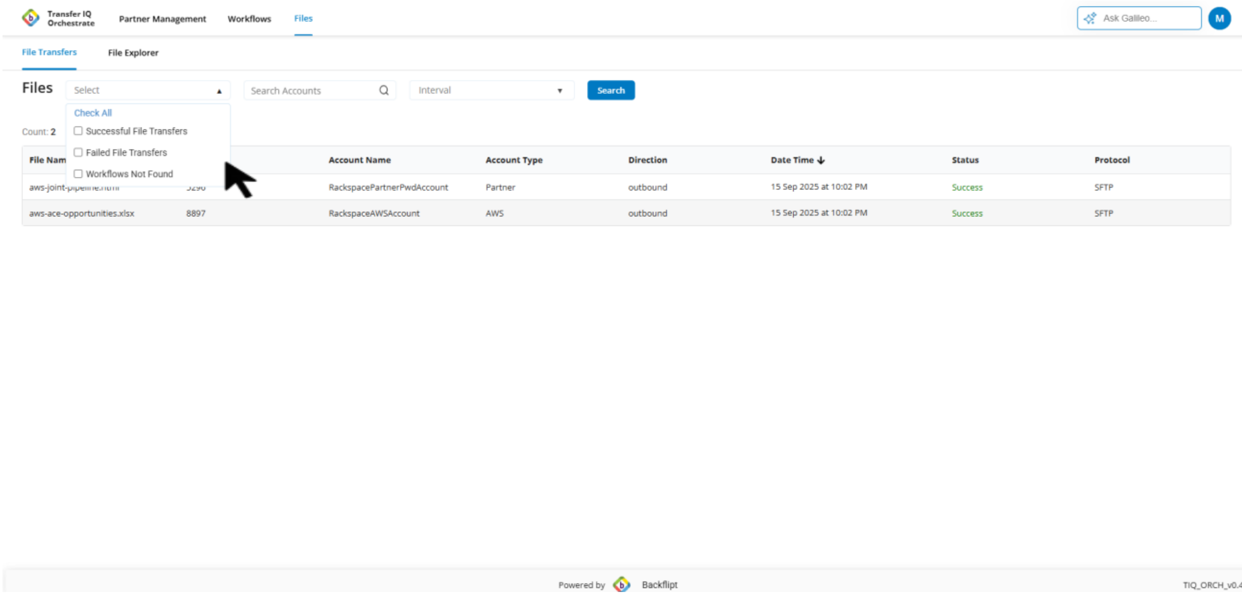
- When the status is NA, it means no workflow was triggered because the file did not match the required file name pattern. In this case, the detailed view only shows the Workflow Execution Details and Workflow Information sections. Other sections like partner details, transformation steps, and destination are not shown.



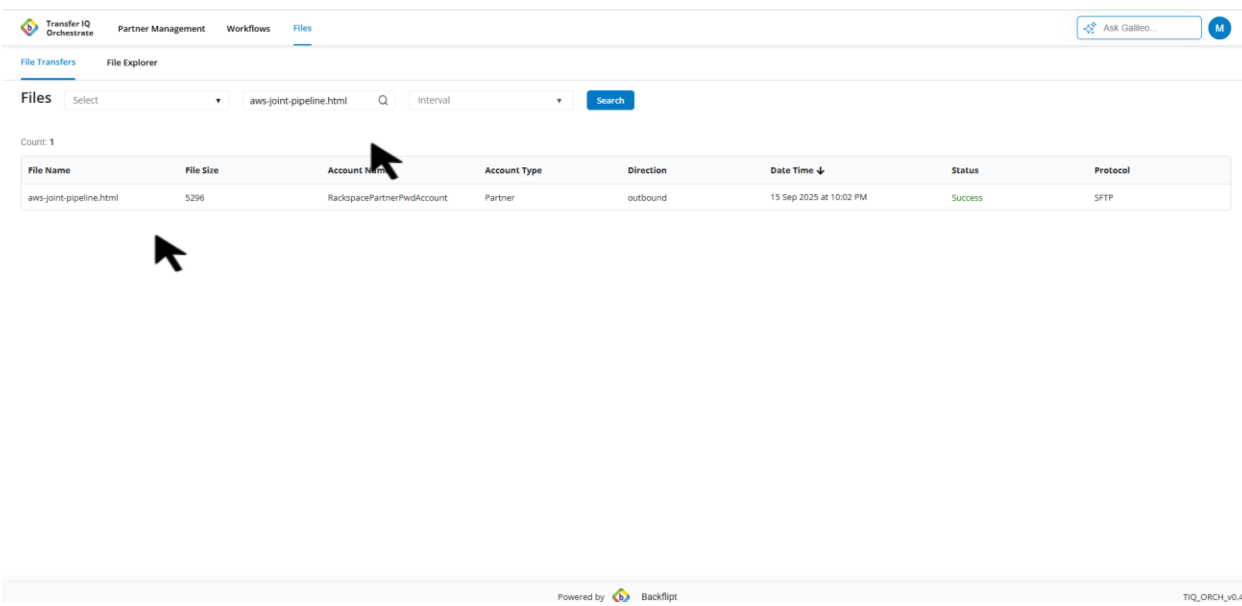
- **Business Unit:** This column displays the business unit of the business user who has submitted the workflow request. It provides clarity on which business unit is responsible for the transfer and ensures accountability within the organization.
- **Protocol:** This column displays the protocol used for transferring the file, such as **SFTP**. It indicates the method by which the file was transmitted securely, ensuring compliance with security and integration standards.

The Filters in the File Transfers tab help users quickly view files based on their transfer status. The available options are:

- **Successful File Transfers** – Shows only the files that were transferred successfully, with all transformation steps completed.
- **Failed File Transfers** – Displays files where the transfer failed, allowing users to check which step went wrong.
- **Workflows Not Found** – Lists files marked as NA, meaning no workflow was triggered because the file did not match the required pattern.
- **Check All** – Selects all the above filters together, so users can view every type of file transfer in one go.



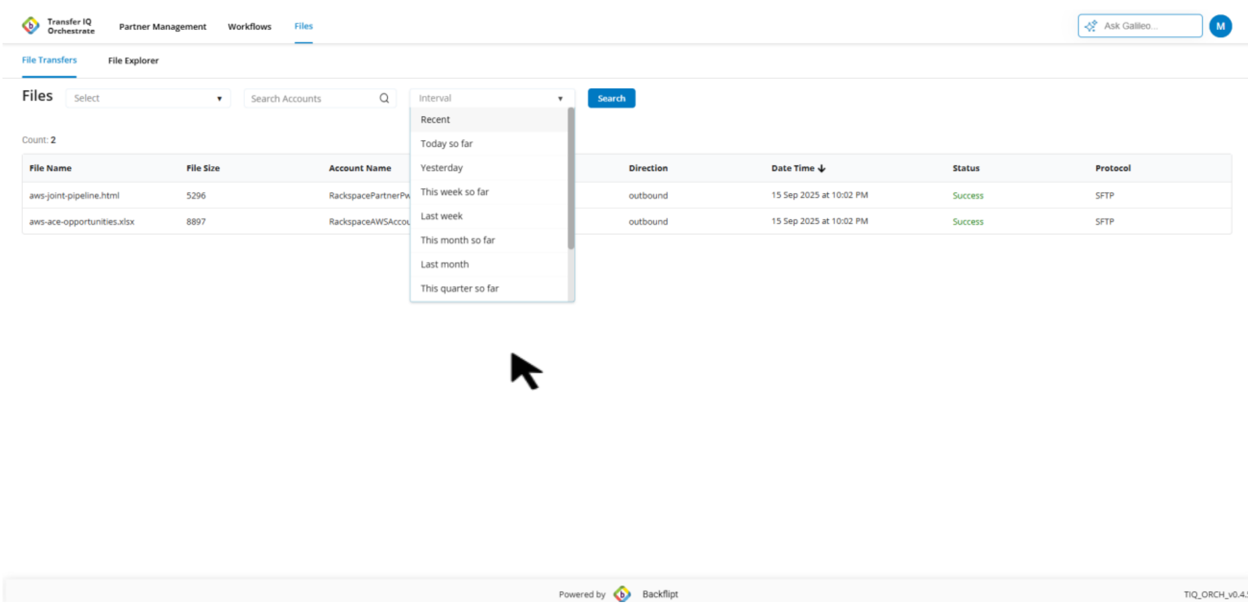
The Search bar allows users to quickly find specific file transfers without scrolling through the entire list. Users can search across multiple columns, including Source File Name, Source File Size, Account Name, Account Type, Direction, Protocol, and Business Unit Name. By entering a keyword or value, the system filters the records and displays only the matching results, making it easier to locate the required file transfer.

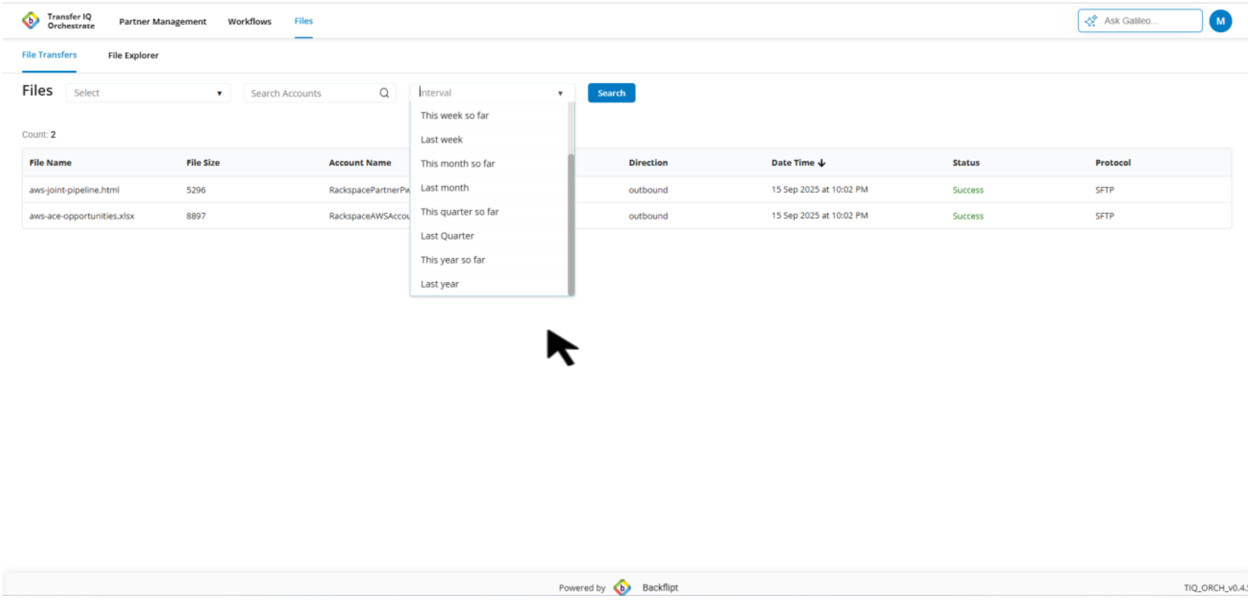


The Interval filter allows users to view file transfers within a specific time range. It helps narrow down results based on when the transfers occurred. The available options are:

- **Recent** – Displays the most recent file transfers.

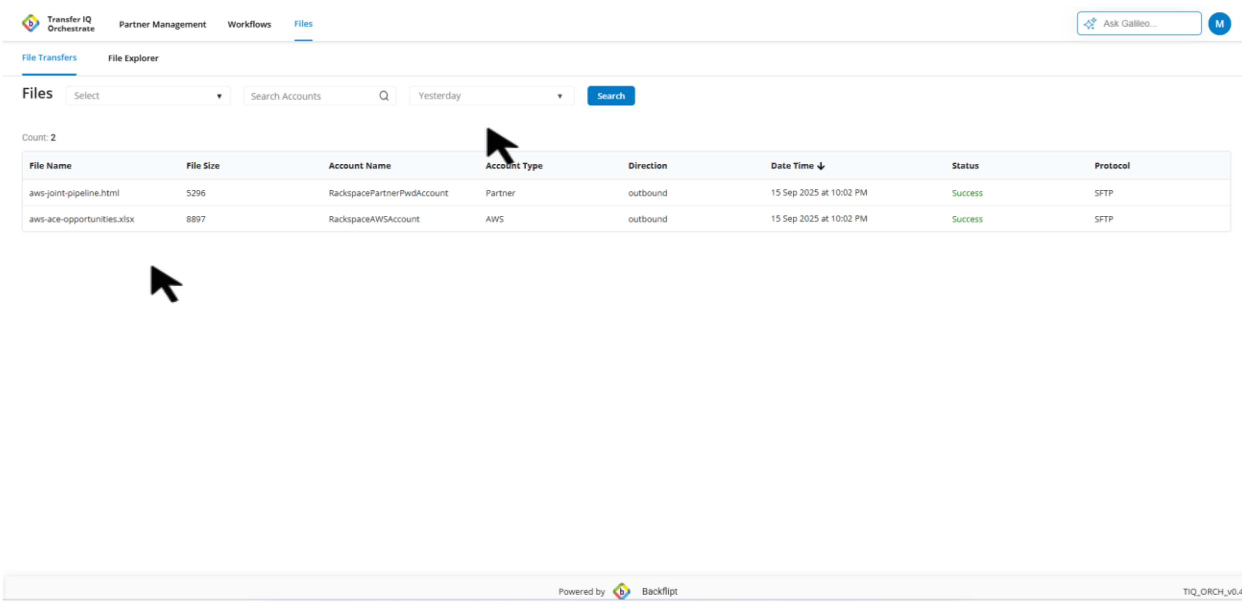
- **Today so far** – Shows transfers that happened during the current day.
- **Yesterday** – Lists transfers completed the previous day.
- **This week so far** – Displays all transfers from the start of the current week until now.
- **Last week** – Shows transfers from the previous week.
- **This month so far** – Lists transfers from the beginning of the current month up to the present time.
- **Last Month** – Shows transfers from the entire previous month.
- **This quarter so far** – Displays all transfers from the start of the current quarter up to now.
- **Last Quarter** – Shows transfers from the entire previous quarter.
- **This year so far** – Lists transfers from the beginning of the current year until now.
- **Last Year** – Shows transfers from the entire previous year.





This makes it easier for users to track and review file transfers over different time periods.

If the user selects any interval, the file transfers that occurred during that time peroid will be displayed.



File Explorer

The **File Explorer** section is designed to support secure file transfers from the company to its external partners. It specifically handles all **outbound file transfers**, meaning any files that are sent from the company to a partner.

There are two types of outbound transfers:

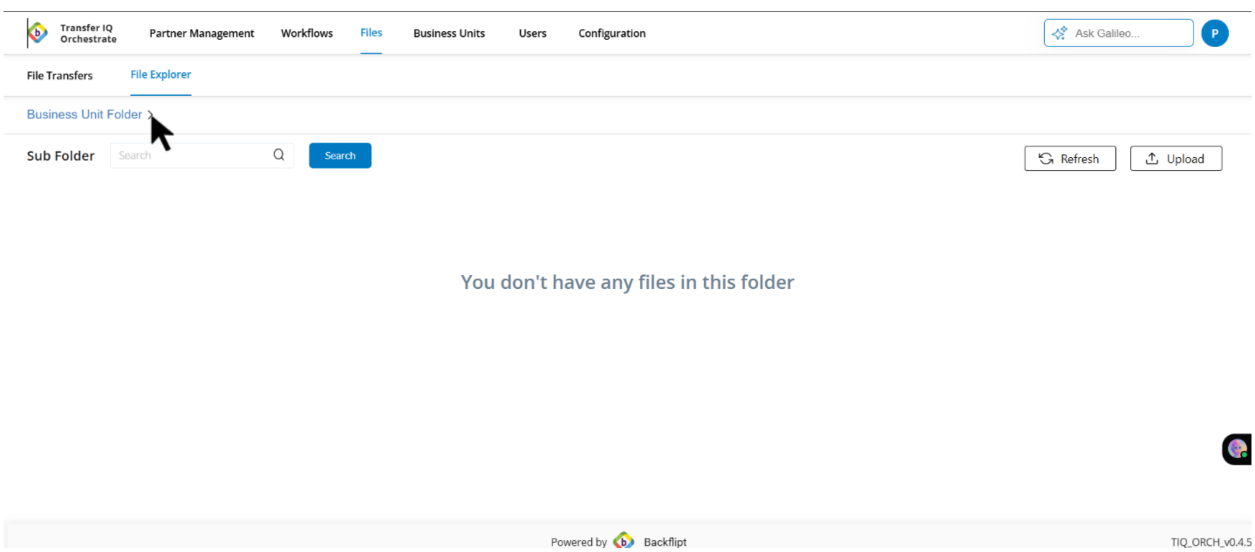
1. **AWS Outbound File Transfers**
2. **PFTS Outbound File Transfers**

Usually, to send these files, the company logs in to the **AWS Console** and uploads the files in the source. But with the **File Explorer**, the company can do all outbound transfers directly through the orchestrate application. This makes the process easier and avoids the need to use the AWS Console.

Admins have access to all Business Unit folders, which are stored under one main folder. This setup keeps file transfers secure, organized, and easy to manage.

To View the file explorer sections

1. Navigate to Files > File Explorer



Each **Business Unit** is set up in the application and linked to specific users. When a business user logs in, Business user can only see and use the folder for their own Business Unit.

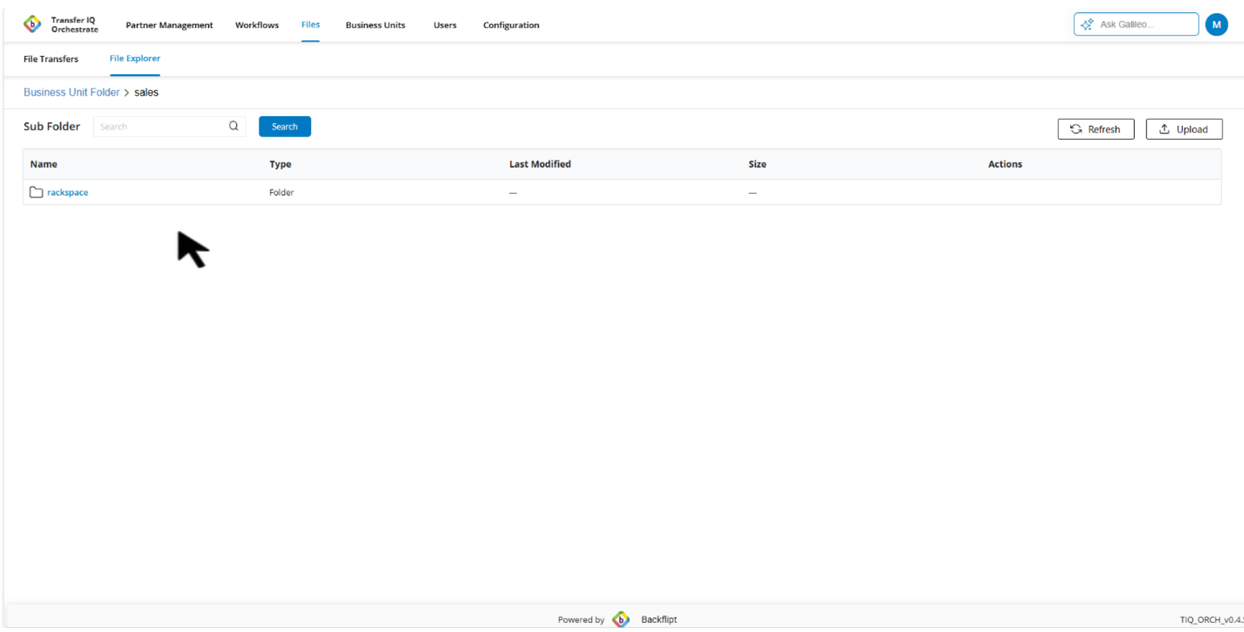
Folder Creations in the File Explorer Section

In the File Explorer section, an **admin** will have access to a main **Business Unit folder**, which contains subfolders for **each Business Unit**.

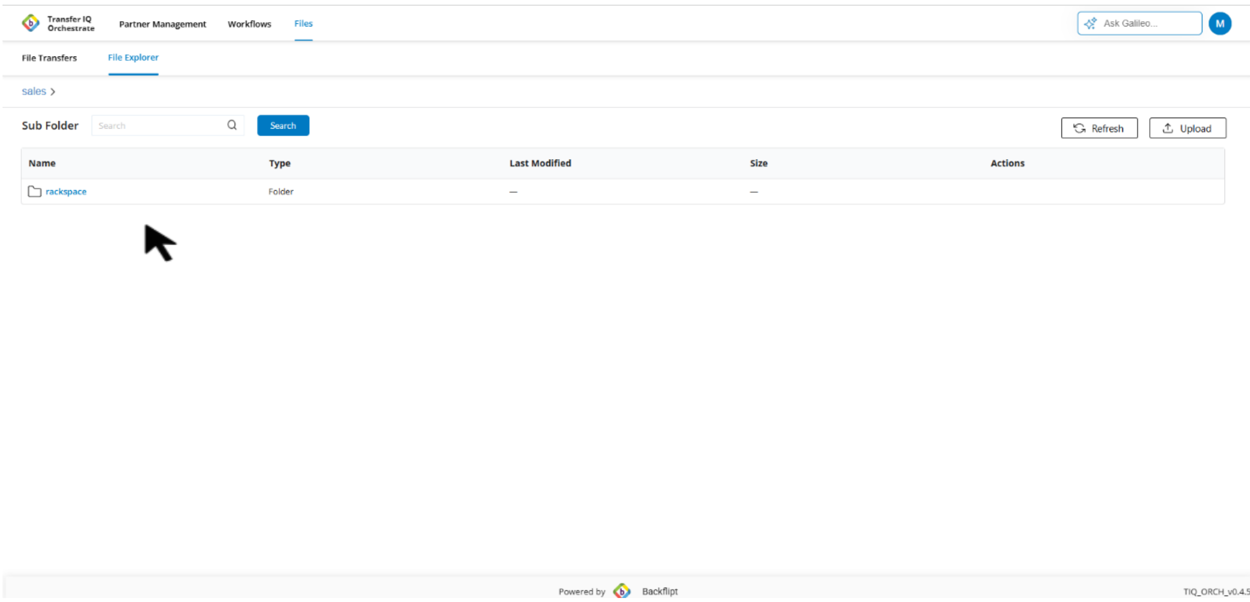
A **business user** will only see the folder assigned to the specific **Business Unit** linked to that user account.

a. Whenever a **partner** is created a folder within the assigned business unit folder will be automatically created.

Admin View

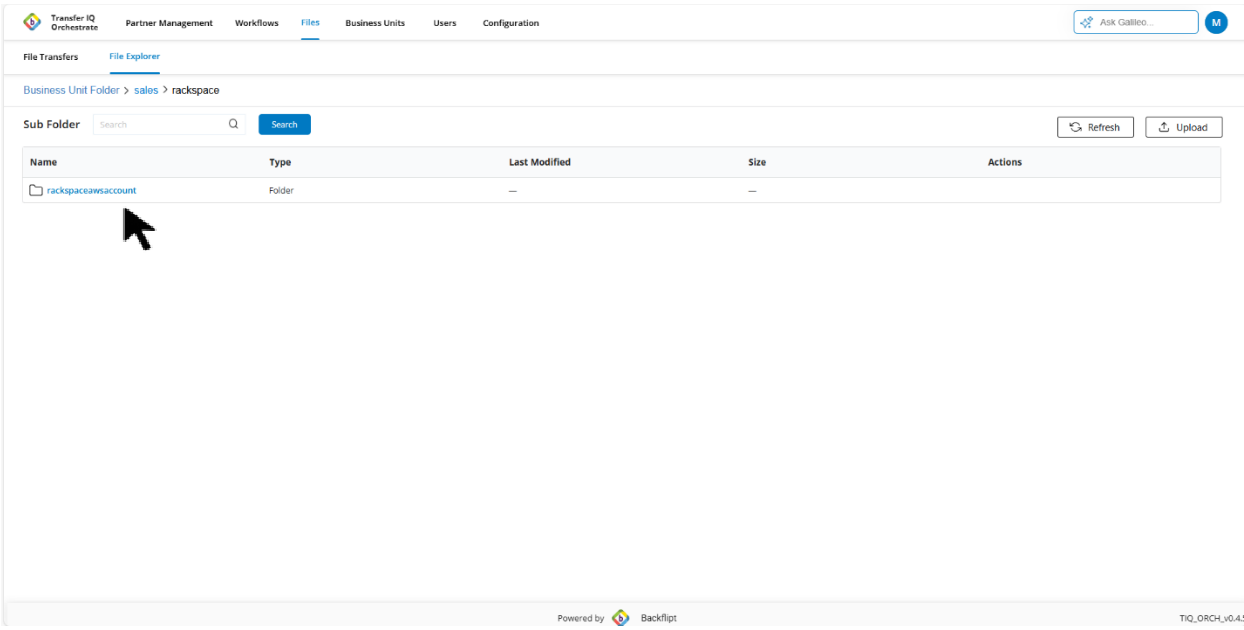


Business User View

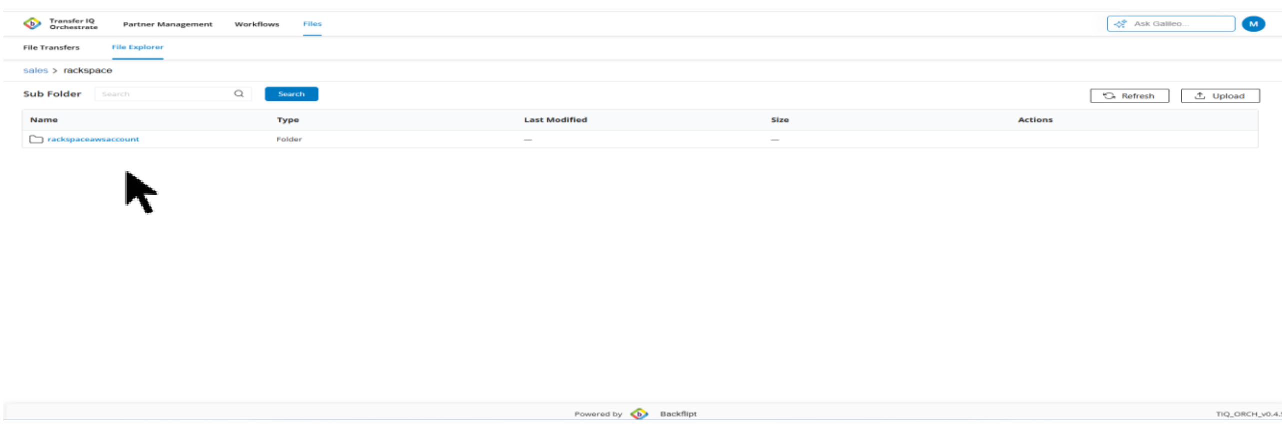


b. Whenever a **partner account** is created (either of type **AWS** or **PFTS)** a subfolder with the **partner account name** will be automatically created inside the relevant Business Unit folder.

Admin View



Business User View



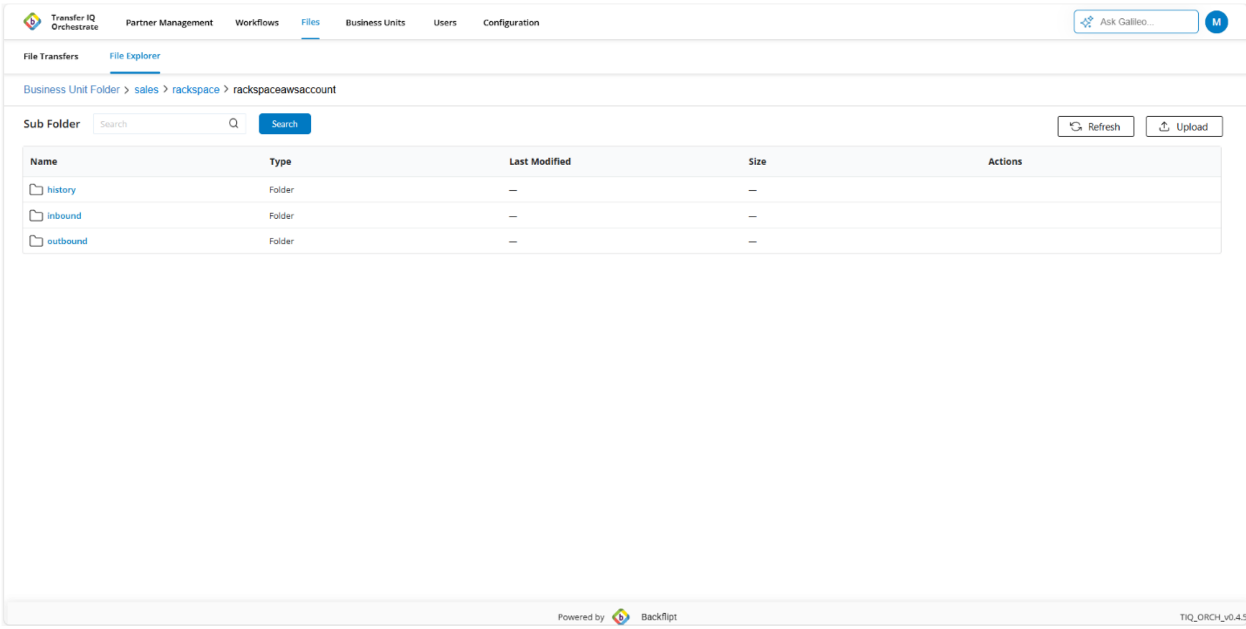
c. The partner account folder will include the following three subfolders:

- **Inbound –** contains of all the files received from the partner
- **Outbound –** source folder for the company to upload and send files to the partner
- **History –** to keep a track of all the files that have been transferred

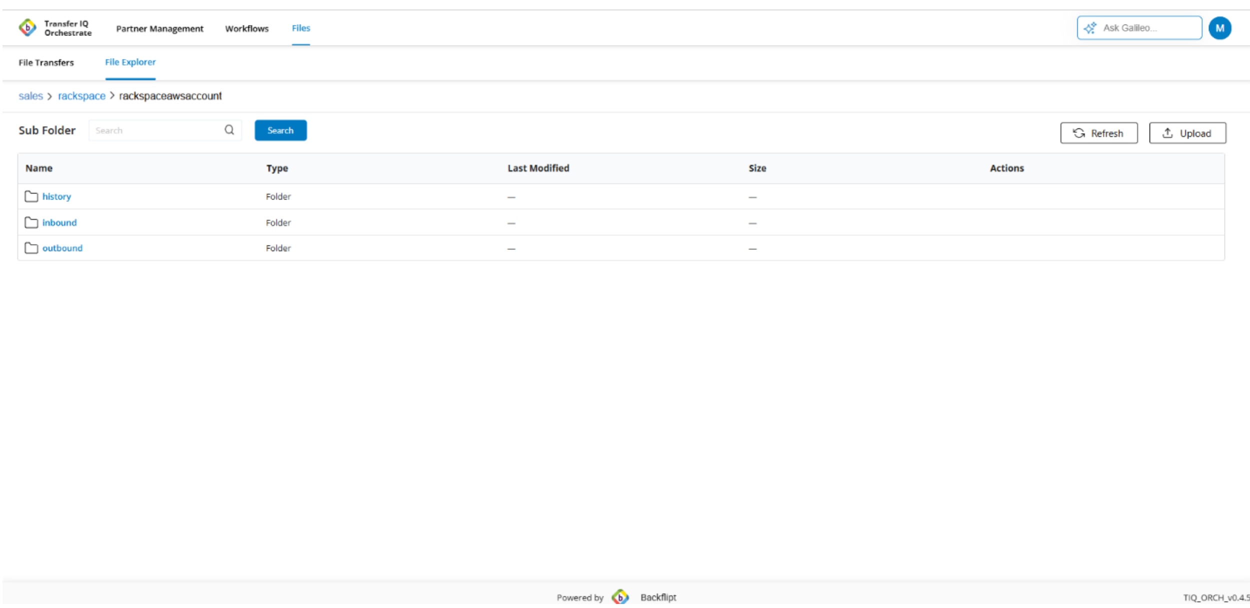
These folders will be visible in two places:

- Under the assigned Business Unit folder in the **business user's** File Explorer view
- Under the same Business Unit folder in the **admin's** File Explorer view

Admin View:



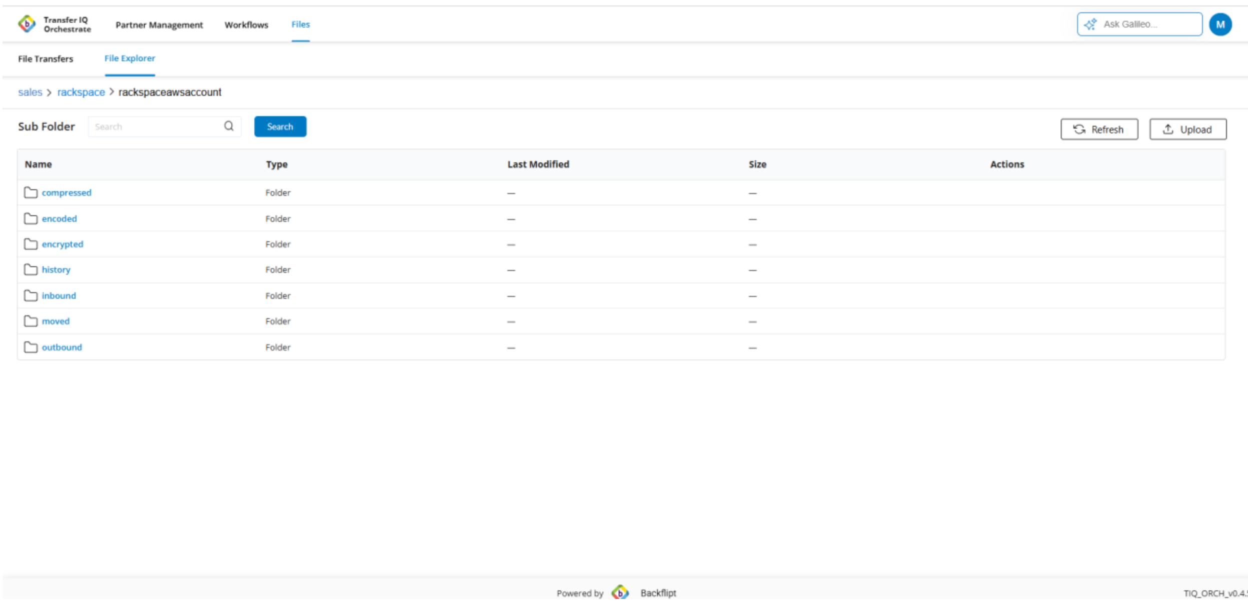
Business User View:



d. Once workflow is created for the account following folders will be created according to the configured workflow for the account. These folders will be visible in two places:

- Under the assigned Business Unit folder in the **business user's** File Explorer view
- Under the same Business Unit folder in the **admin's** File Explorer view

Business User View:

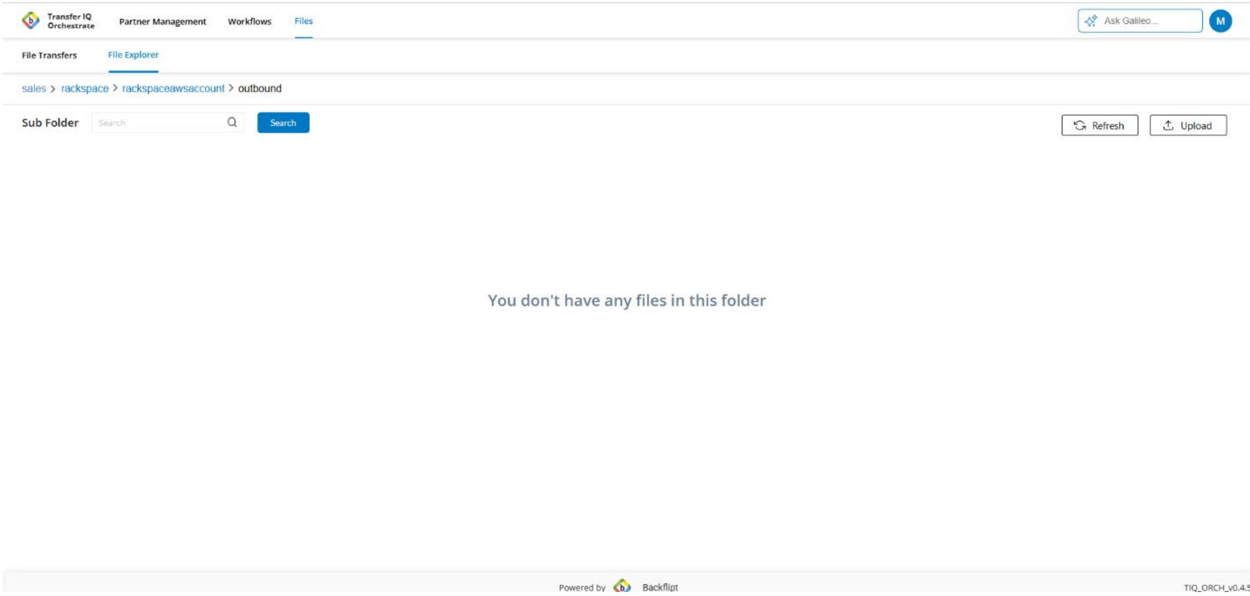


This setup ensures that files are organized by Business Unit and partner, and access to files is controlled based on the user role.

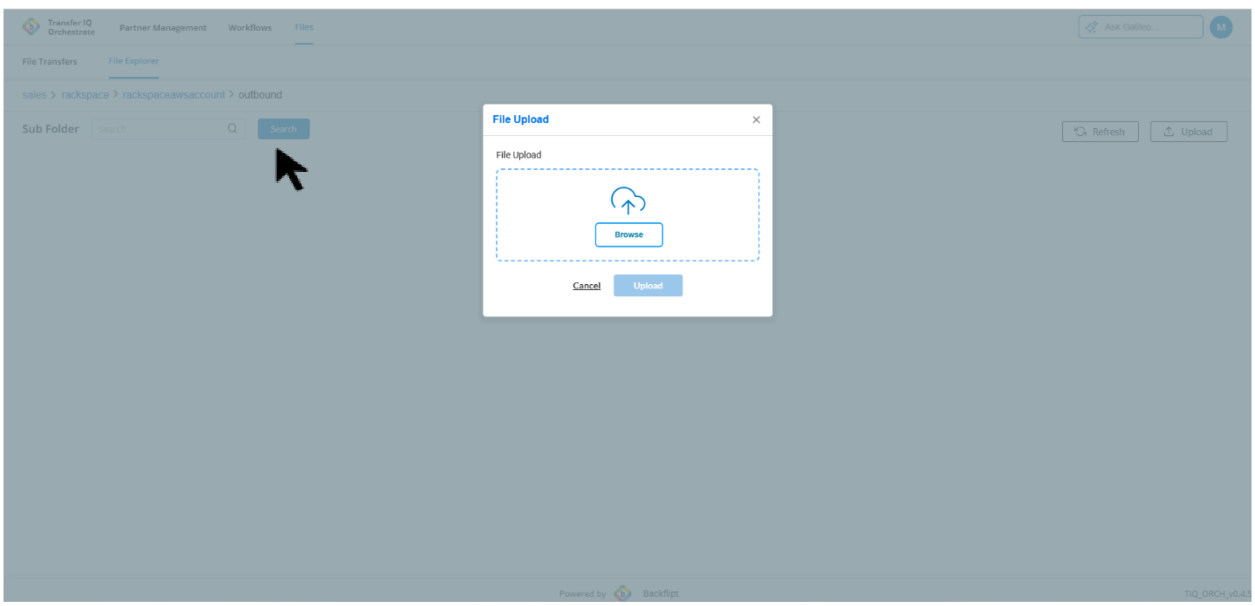
File Transfers Using the File Explorer Tab

To initiate a file transfer using the **File Explorer** tab, follow the steps below:

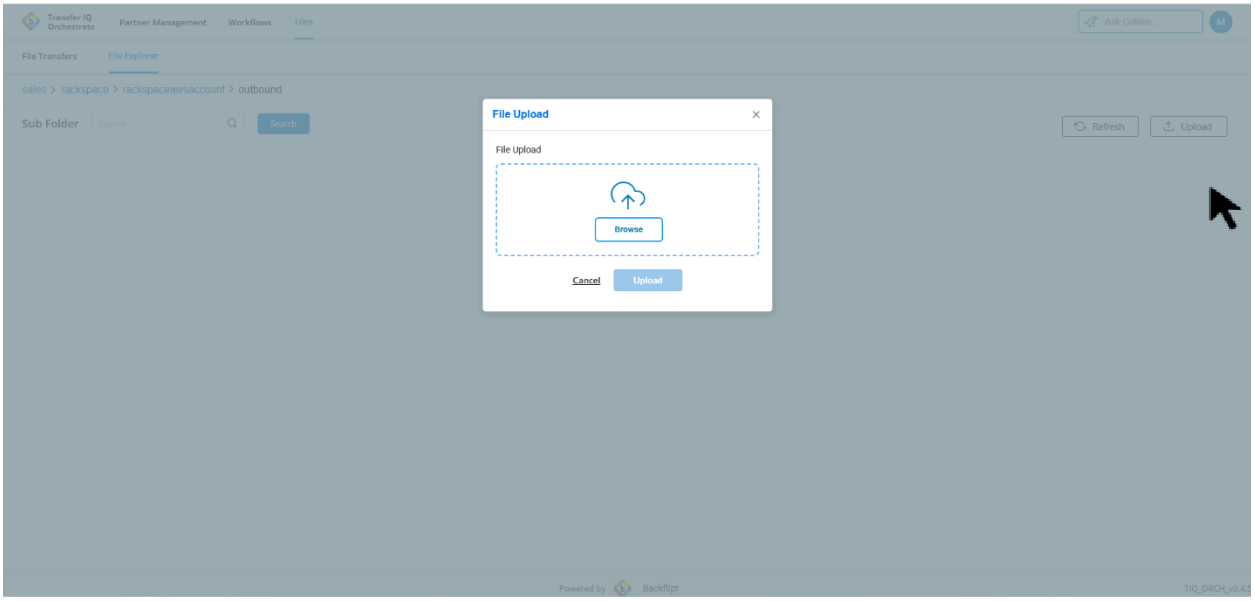
1. **Navigate to the Source Folder Path**
    a. Open the File Explorer tab.



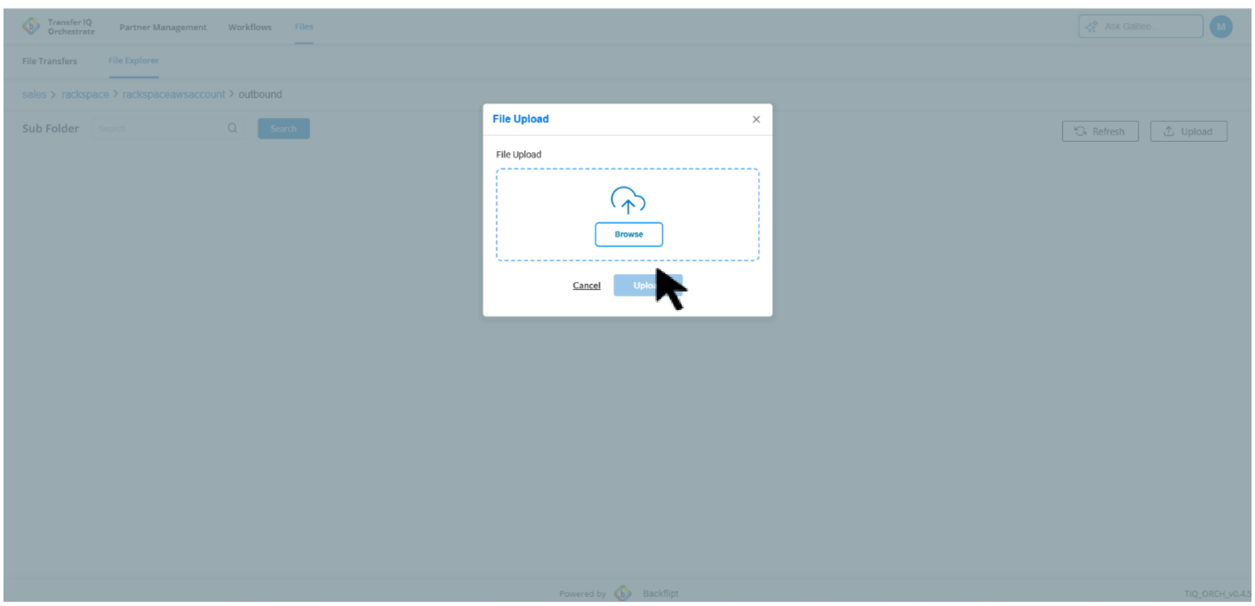
b. Navigate to the folder where the file transfer should begin. This is usually the **outbound folder** under a specific **partner account folder** within the assigned **Business Unit**.



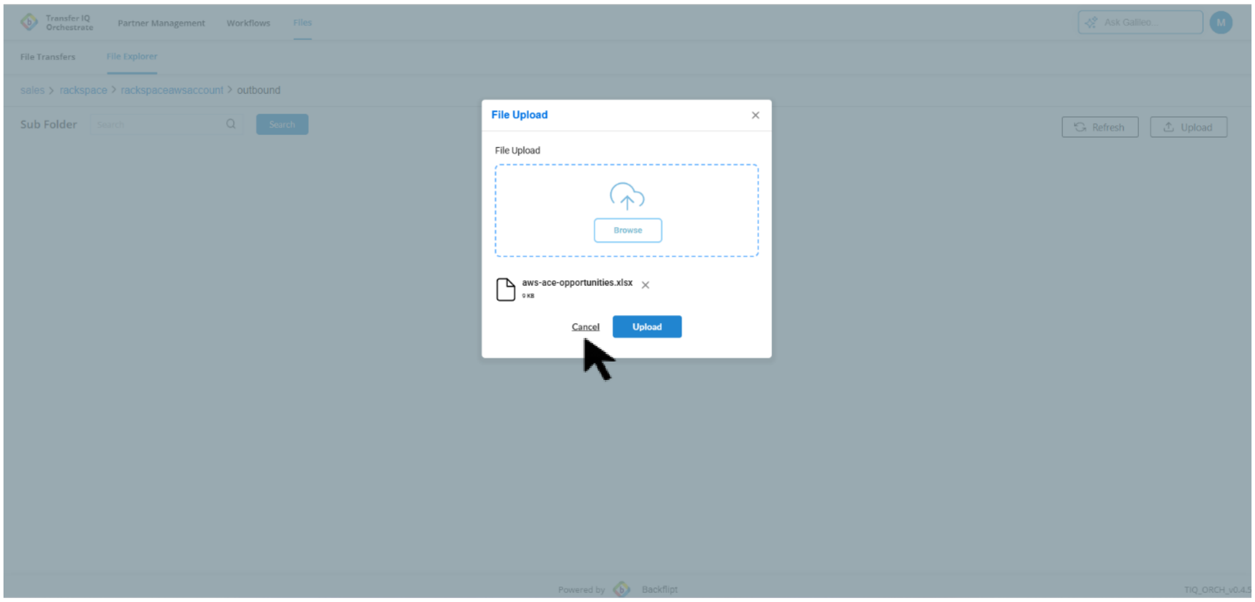
2. **Click the Upload Button**
   a. Inside the selected folder, click the **Upload** button to begin the process.



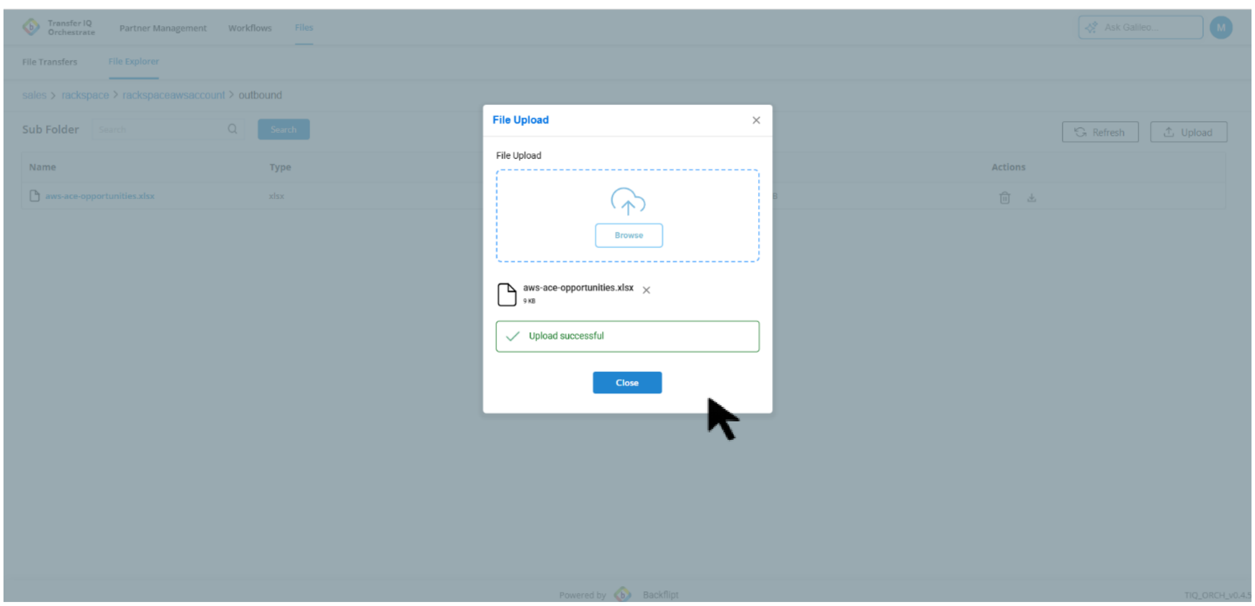
3. **Select a File to Upload**
    a. A popup window will appear with a **Browse** button.



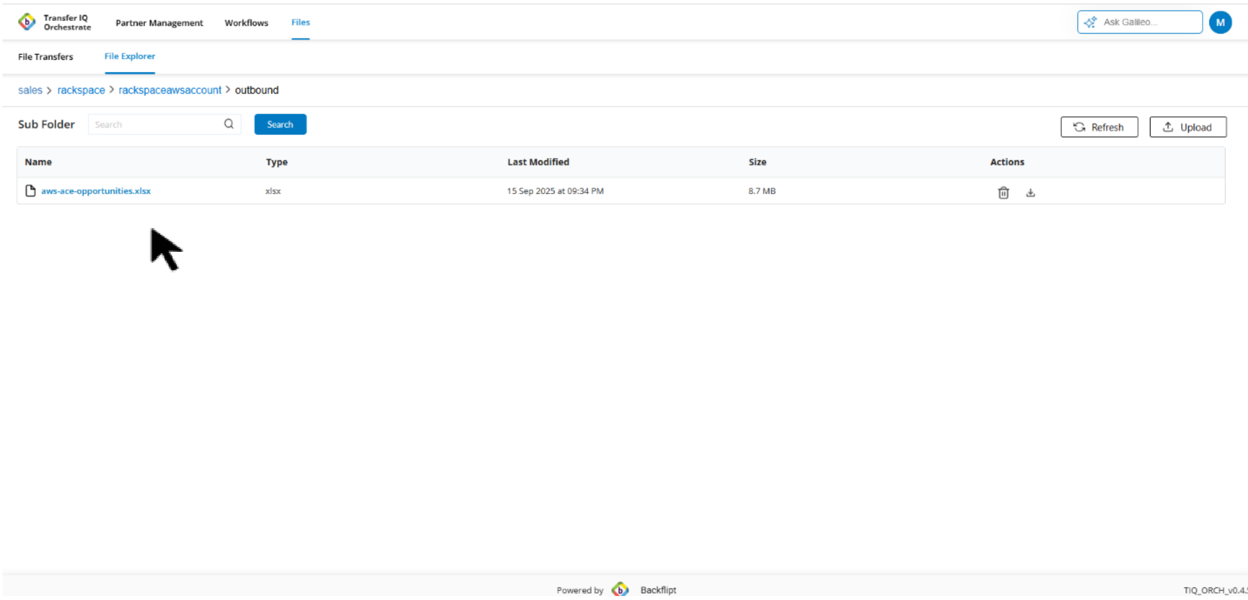
    b. Click the **Browse** button to open the file selection dialog from the local system.
4. **Preview the Selected File**
    a. After selecting a file, the file name will appear **below the browse card** in the popup.
    b. This shows that the file is ready for upload.



5. **Start the File Transfer**
    a. Click the **Upload** button within the popup to begin transferring the file to the selected folder path.

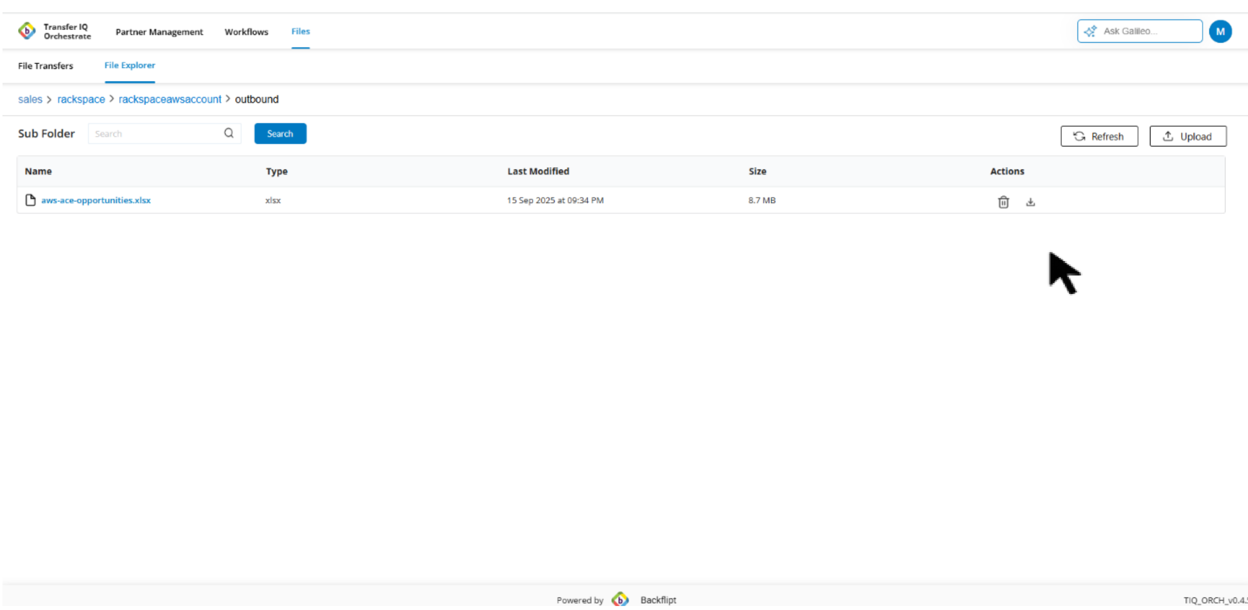


    b. Once the file is uploaded, if there is **only one workflow** created for the partner account, that workflow will be triggered automatically. If **multiple workflows** exist, the application will identify and trigger the **best-matching workflow** based on the uploaded file.



After a file is successfully uploaded using the File Explorer tab, the following actions can be performed:

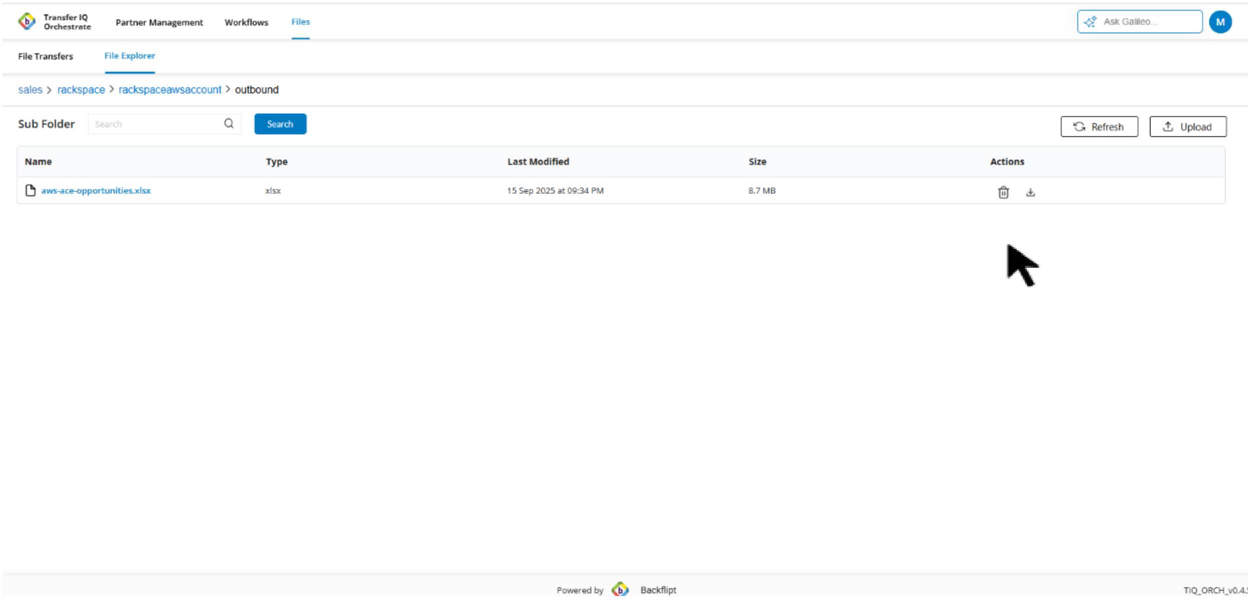
6. **Download the Uploaded File**
   a. Locate the uploaded file in the folder view.
   b. Click the **Download** button next to the file name.
   c. The file will be downloaded to the local system.

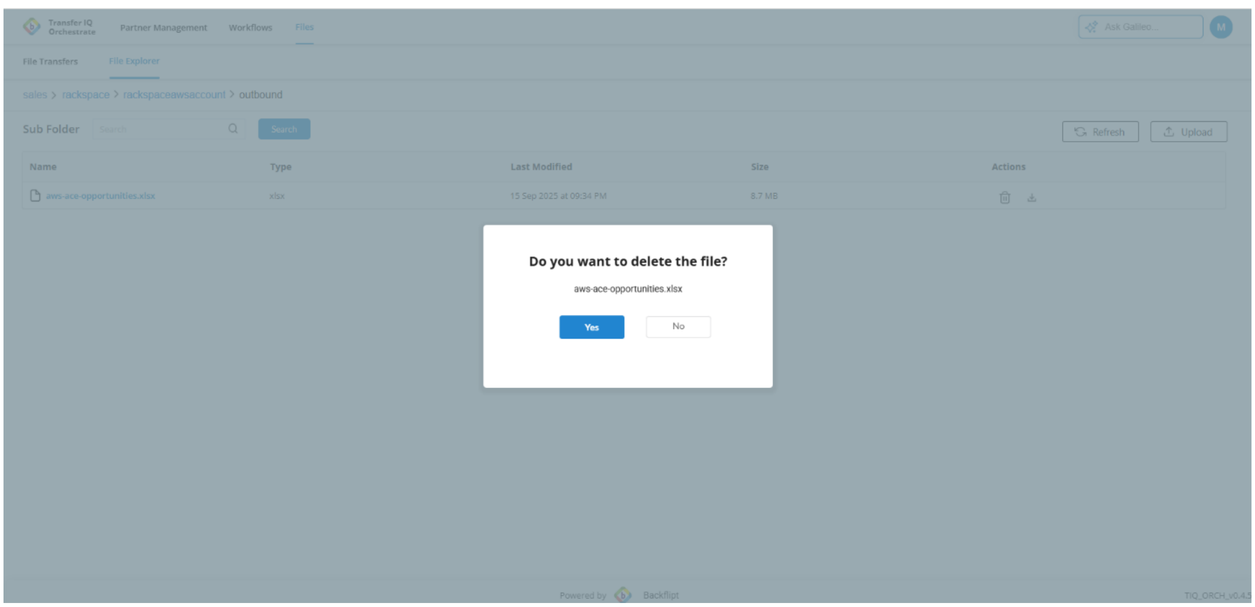


7. **Delete the Uploaded File**
   d. To remove an uploaded file, click the **Delete** button next to the file name.
   e. A **confirmation popup** will appear with **"Yes"** and **"No"** options.

f. Click **"Yes"** to confirm and delete the file.

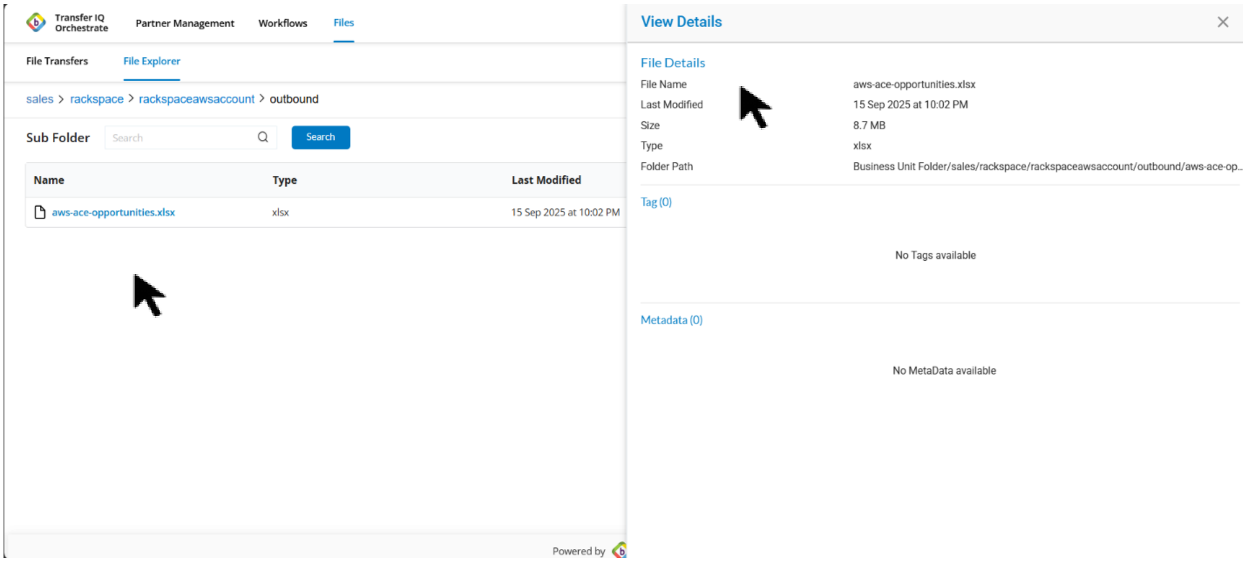
g. Clicking **"No"** will cancel the deletion and keep the file intact.





8. View details of the uploaded file

a. To view the details of the uploaded file, click on the file and sidebar will open which contains details associated to the uploaded file



So, in the above way, business user/ Admin can upload files in file explorer for only outbound EFS/PFTS workflows from the system itself instead of logging into AWS to upload the files.