Management Portal

Sftp Gateway Deployments

The UI provides a Sftp Gateway deployment menu that enables users to create a new SFTP gateway. The page shows a list of all deployments, including both active and deleted ones.

To add a new Sftp Gateway, users are required to provide the following information:

- Instance Name: Users can enter a name for the Sftp deployment. This name helps identify and distinguish the deployment from others.

- Version: User can change the version of the sftp gateway. We always improve and add new features to our sftp gateway. Use the latest recommended version.

- Ingress external Port: User can change the port where the sftp gateway will be accepting requests. We recommend to use port 22, 80 or 8080.

- Username and password: User can define the username and password to authenticate to the sftp gateway.

- Public Port: Users can provide a public port for the SFTP gateway deployment. This port allows external access to the SFTP gateway.

- Keys: Users can specify the keys associated with the SFTP deployment. These keys are used for authentication and secure file transfer.

- Upload Destination: Users can define the destination for the SFTP deployment. These destinations determine where the files will be transferred.

Api Gateway Uploader Deployments

The UI provides an Api Gateway Uploader deployment menu that enables users to create a new Api Gateway. The page shows a list of all deployments, including both active and deleted ones.

To add a new Api Gateway Uploader, users are required to provide the following information:

- Instance Name: Users can enter a name for the Api Gateway deployment. This name helps identify and distinguish the deployment from others.

- Upload Destination: Users can define the destination for the Api Gateway deployment. These destinations determine where the files will be transferred.

Destinations

The Destination page in the UI allows users to view and manage destinations. Users can see a list of defined destinations and have the option to add a new destination.

To add a new destination, users are required to provide the following information:

- Alias: Users can specify an alias for the destination. This alias helps identify and label the destination for easy reference.

- Destination Type: Users need to select the type of destination, which could be a specific protocol or service used for file transfer or storage.

- Host and IP: Users are required to provide the hostname or the IP address of the destination. This information helps establish a secure connection to the destination.

- Credentials: Users have the choice to provide either a username and password or SSH public keys as credentials for the upload system to be able to access the destination securely.

Keys

The Keys page in the UI allows users to manage and view all the keys stored in the system. Users can see a list of existing keys and have the ability to add a new key.

To add a new key, users are required to provide the following information:

- Alias: Users need to provide an alias for the key. This alias helps identify and label the key for easy reference and management.

- Public SSH Key: Users are required to input the public SSH key itself (eg: cat ~/.ssh/id_rsa.pub"pbcopy). This key is used for authentication and secure access to SFTP gateway.

API

The Public API Endpoints provide a set of interfaces that enable automation of tasks within the system. These endpoints are designed to be accessible by external systems such as Jenkins pipelines or Azure DevOps pipelines, allowing seamless integration and automation capabilities.

Users can interact with the endpoints to perform various tasks, such as initiating deployments, retrieving deployment status, managing configurations, and more.

Connectors

The Connectors page provides a set of interfaces to various services to send notifications. In case of failed data transfer, the user can receive a notification message via the configured connector using webhooks.

Notifications

The Notifications page serves as a central hub for users to access a consolidated stream of events dispatched by our notification system.

Within this interface, each notification gives a thorough and detailed explanation of why a data transfer didn't work as expected.

Users

The User Management page provides a comprehensive interface for managing users within the system. Users with the appropriate permissions can access this page to view and manage the list of existing users.

Based on the subscription type, the owner has the ability to invite additional users and extend the system's capabilities to a broader team. Invited users will have similar privileges and be able to perform various tasks, including creating deployments, managing destinations, and more.

To invite a new user, the system requires certain information for user identification and access.

- login name.

- the user's name and surname.

-email address.

- job title.

By providing these details, the system can generate an invitation and grant the invited user access to the system's functionalities.

Subscriptions

The subscription page allows the owner of the application to manage the subscription settings.

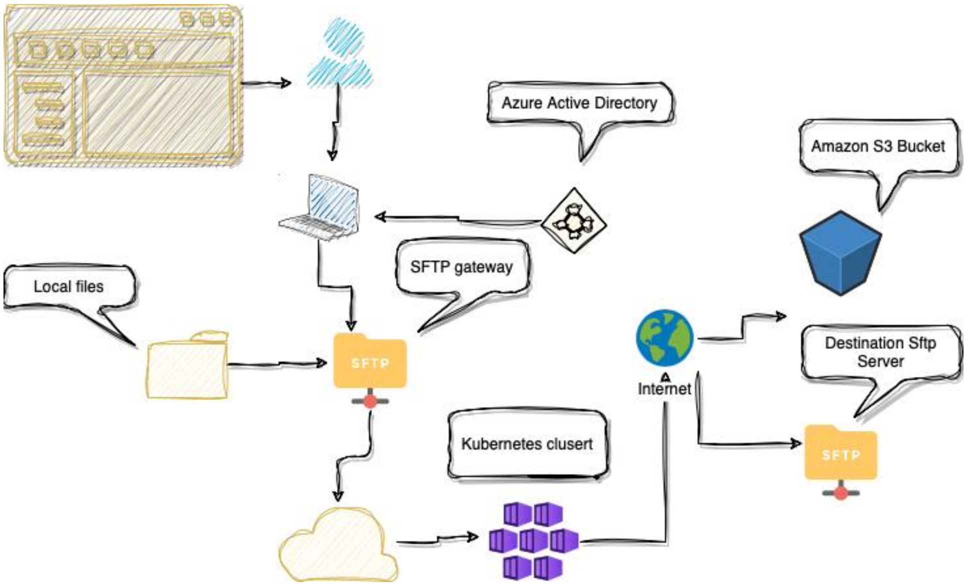
Upon the user's initial login, the application's functionality will be restricted until a subscription is purchased.

To complete the subscription process, the user will need to provide necessary information such as their address and VAT number.

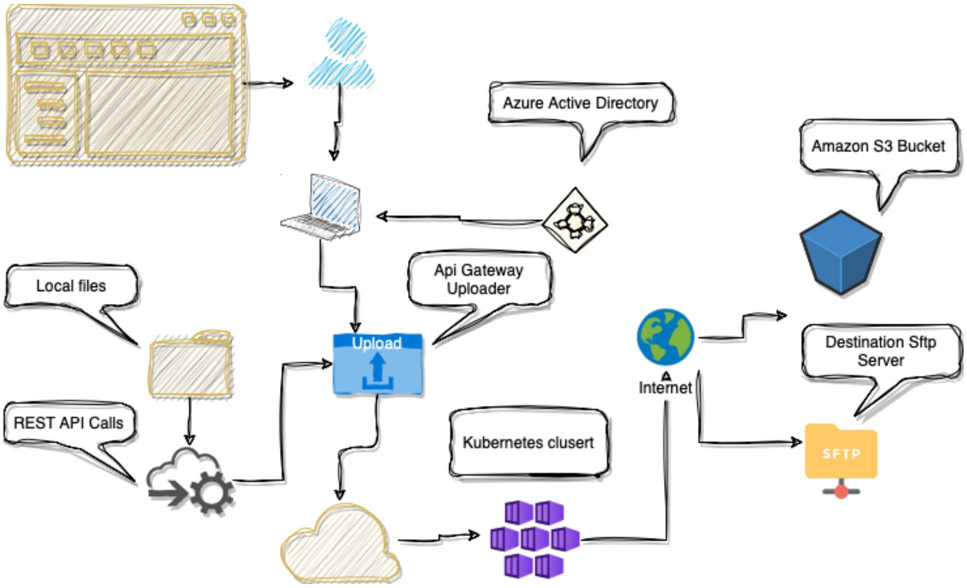
The subscription information can be managed by the user at any time, allowing them to update or modify their details as needed.

Additionally, the subscription page provides access to a history of invoices and receipts, enabling users to review past transactions and obtain relevant financial records.

SFTP Gateway diagram



Api Gateway uploader diagram



Scenario:

Local-to-External Vendor Document Transfer via SFTP Gateway

Alex works as an IT administrator in a manufacturing company that deals with sensitive document transfers on a regular basis. Recently, the company has partnered with an external vendor who requires them to securely transfer various documents.

To facilitate this transfer, Alex decides to leverage the Almeria Industries SFTP gateway system within their organization.

Here's how he proceeds:

-Configuration:

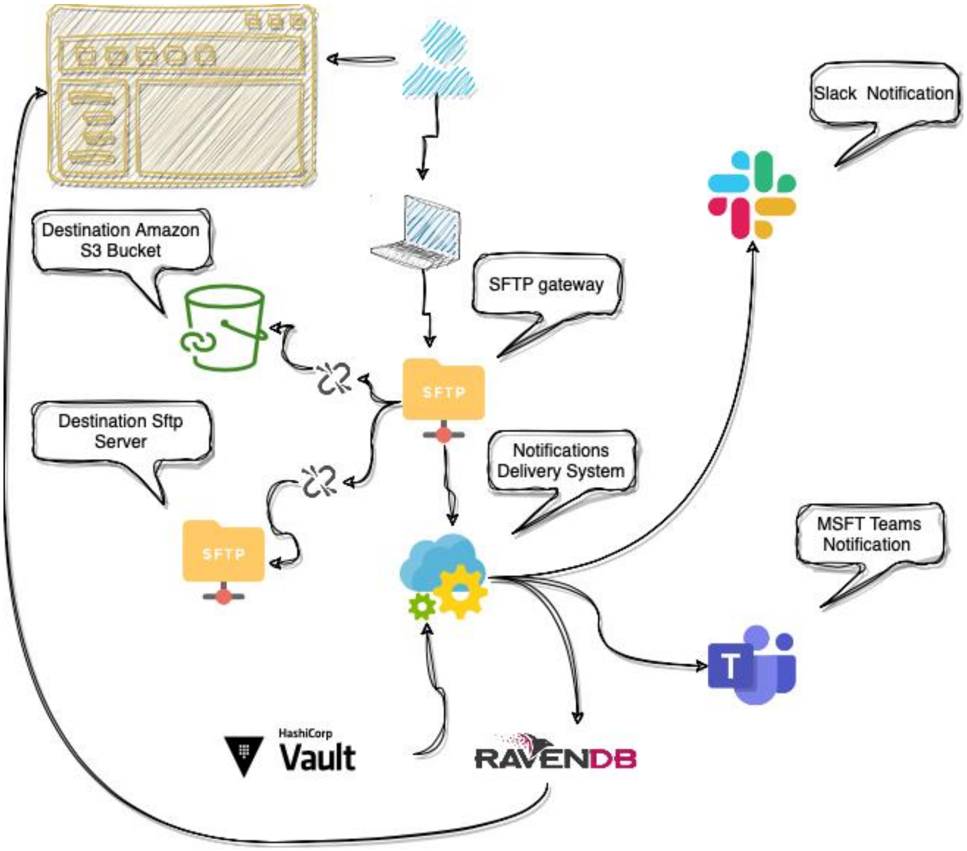
Alex accesses the Almeria Industries user interface and navigates to the "Sftp Gateway" section. He creates a new SFTP gateway configuration, specifying the necessary parameters such as hostname, port, and authentication method. Additionally, Alex sets up the required security measures, including encrypting the files, to ensure secure document transfers.

-Document Transfer:

Alex locates the documents in the local directory that need to be transferred to the external vendor. He initiates the document transfer process through the local sftp client that will be connecting to the SFTP gateway. The SFTP gateway system establishes a secure channel with the external vendor's SFTP server. Using the established connection, the documents are securely transferred from the local directory to the external vendor's server, ensuring confidentiality and integrity throughout the process.

-Notifications:

Alex wants to stay in the loop when data transfer encounter issues at the destination due network connectivity or incorrect credentials. To make sure he's always notified, he sets up a new Connector. This Connector acts like a bridge and links up with his chosen channel on MSFT Teams, using incoming Webhook.


Slack Notification
Destination Amazon S3 Bucket
SFTP gateway
SFTP
Destination Sftp Server
Notifications Delivery System
SFTP
MSFT Teams Notification
HashiCorp Vault
RAVENDB