SFTP Connector Guide

> **Note: Publisher** - Professional Services, Saviynt
>
> **Contributors** - Rajesh Gaddam

Disclaimer

The integration was either created by Saviynt or by Saviynt community users and verified by Saviynt. The integration is available “as is” and fall under standard connectors support for REST, SOAP, JDBC, LDAP, PowerShell, Jar and Saviynt Connector Framework.

> **Note:** It is highly recommended to use OOTB EIC features available for file import/export.
>
> 1. Files can be imported to EIC by using API’s i.e. schema import and data import
> 2. All reports are available through API’s i.e. Runtime analytics

Contents

Preface

This guide describes the integration between Saviynt **Enterprise Identity Cloud (EIC)** and SFTP location for transferring the files.

Audience

This guide is intended for administrators and target application integration teams responsible for implementing a secure integration service with SFTP based on SFTP file location.

Introduction

In Saviynt EIC solution there is a need for periodic and automated transfer of files into and out of Saviynt EIC solution based on customer requirements. For example, schema-based import jobs for different objects expect the data files to be available in Datafiles directory and schema files to be available in SAV directory. And sometimes data needs to be sent from Saviynt EIC solution to customer target systems for further consumption and processing by the target applications. To address these requirements Saviynt Professional Services COE team has developed a File Transfer Utility (aka SFTP Connector based on JarConnector) to automate transfer of files between customer SFTP location and Saviynt environment.

Note: This guide provides information about using the File Transfer Utility for only transferring files in to and out of EIC. This utility does not import the data in the files into EIC tables as such.

Supported Features

The SFTP integration supports the following features:

File Transfer	
File Import	**File Export**
Support transfer of files (.csv and .sav files) from a customer SFTP location to Saviynt EIC platform	Support export of files (.csv, .xls, .xlsx, .txt and .sav files) from Saviynt EIC solution to customer SFTP location.

Supported Software Versions

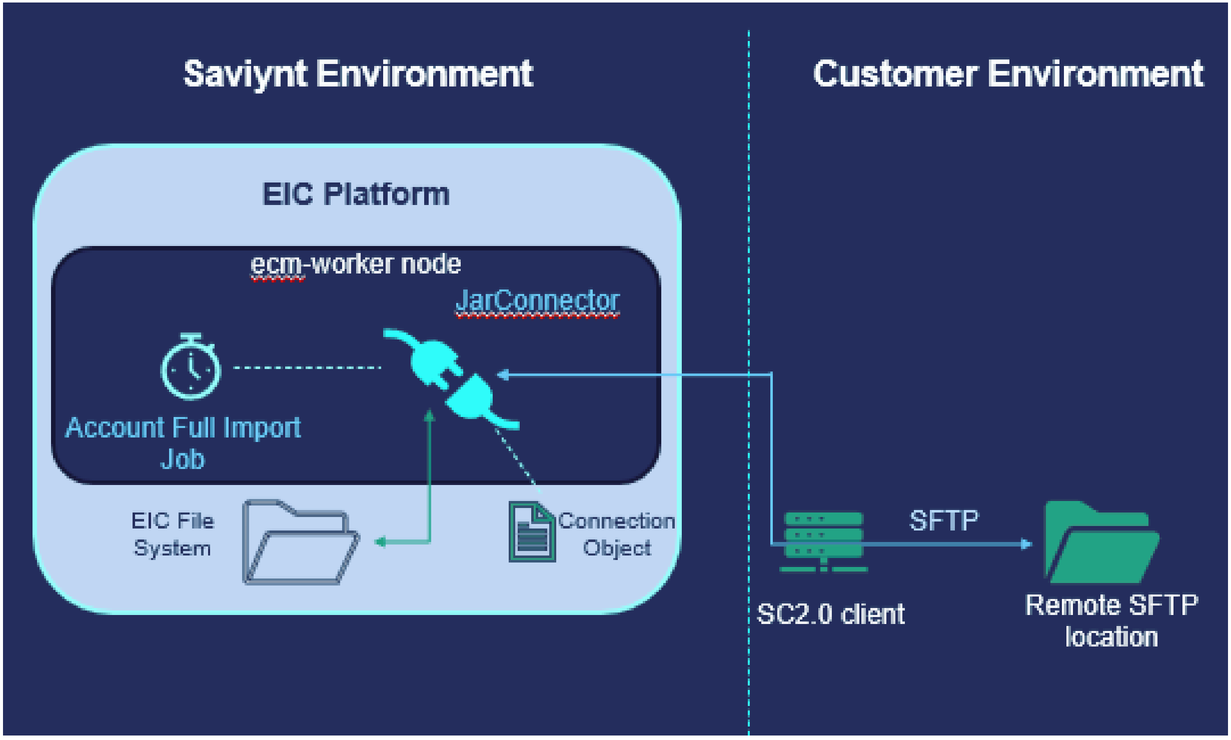
Software	Version
EIC	v5.5 sp3.x, v2020.x and v2021.x

Integration Architecture

Utility is a **JarConnector** type connector for transferring data using SFTP protocol .

- The SFTP Utility (JarConnector) is deployed as an extension jar in EIC
- Input params are stored in connection object in the ImportAccountsJSON
- It supports supports transfer of .csv and .sav files into EIC to **Datafiles** and **SAV** directories respectively under Admin->Settings->File Directory
- It supports transfer of .txt, .csv, .xls, .xlsx files from **Reports** directory of EIC to a SFTP location

The following diagram depicts the high-level architecture:

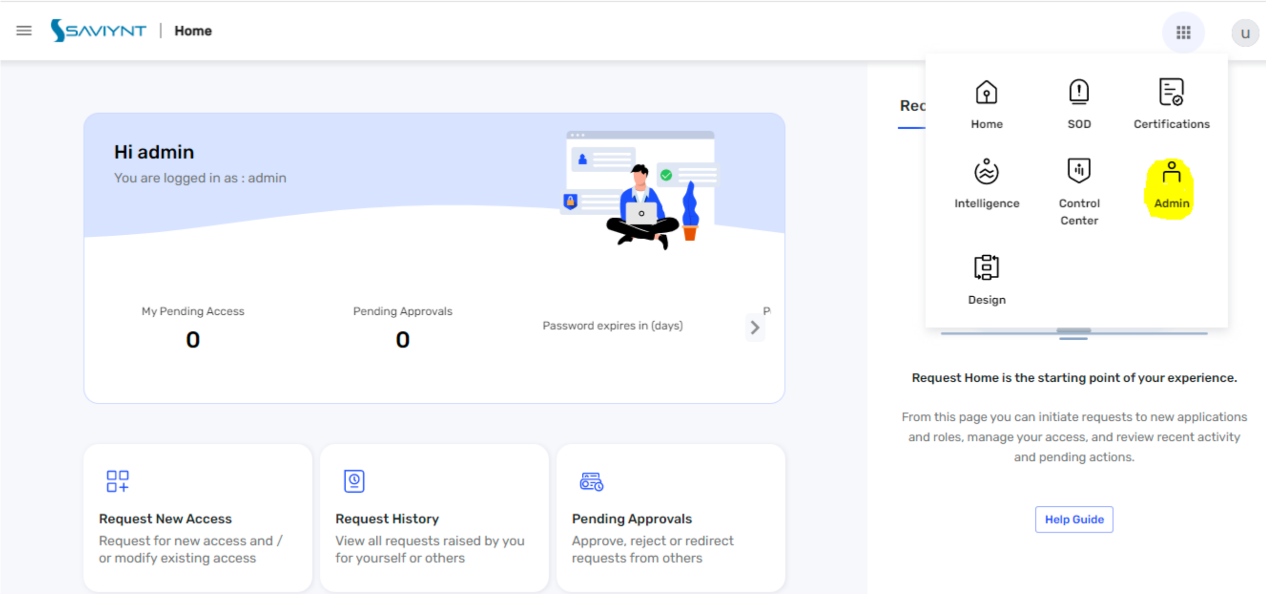


Setting Up the Integration

Prerequisites

Setting up the SFTP connector on your tenant

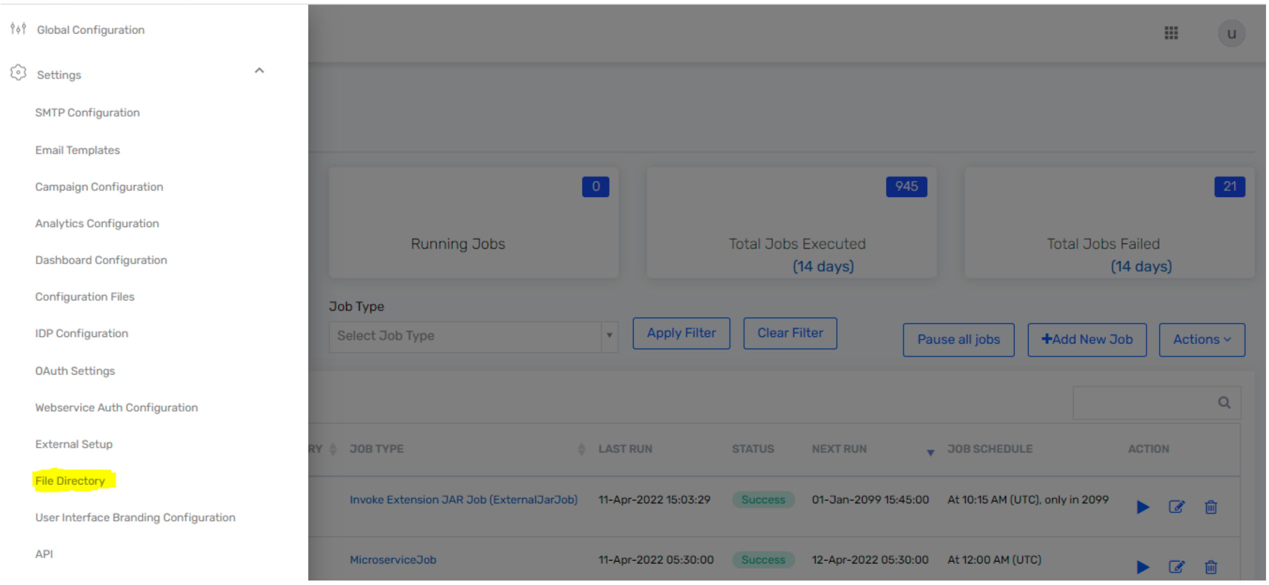
1. Download the utility jar to your local machine (Download SFTP Jar Connector source code)
2. Login to EIC using the Admin credentials.
3. Go to admin page


SAVIYNT
Home
u
Req
Home
SOD
Certifications
Intelligence
Control Center
Admin
Design
Hi admin
You are logged in as : admin
My Pending Access
0
Pending Approvals
0
Password expires in (days)
P
Request New Access
Request for new access and / or modify existing access
Request History
View all requests raised by you for yourself or others
Pending Approvals
Approve, reject or redirect requests from others
Help Guide

Request Home is the starting point of your experience.

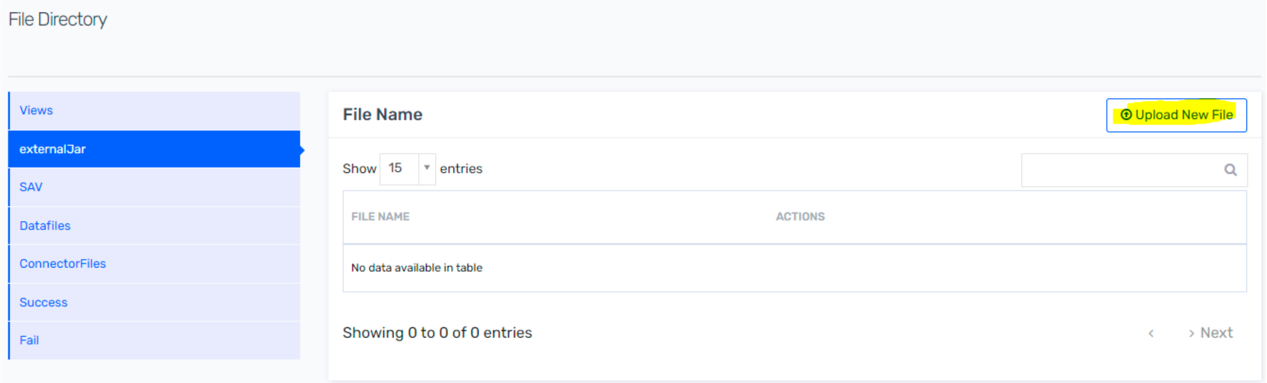
From this page you can initiate requests to new applications and roles, manage your access, and review recent activity and pending actions.

4. Go to Settings and File Directory



RY	JOB TYPE	LAST RUN	STATUS	NEXT RUN	JOB SCHEDULE	ACTION
	Invoke Extension JAR Job (ExternalJarJob)	11-Apr-2022 15:03:29	Success	01-Jan-2099 15:45:00	At 10:15 AM (UTC), only in 2099	
	MicroserviceJob	11-Apr-2022 05:30:00	Success	12-Apr-2022 05:30:00	At 12:00 AM (UTC)	

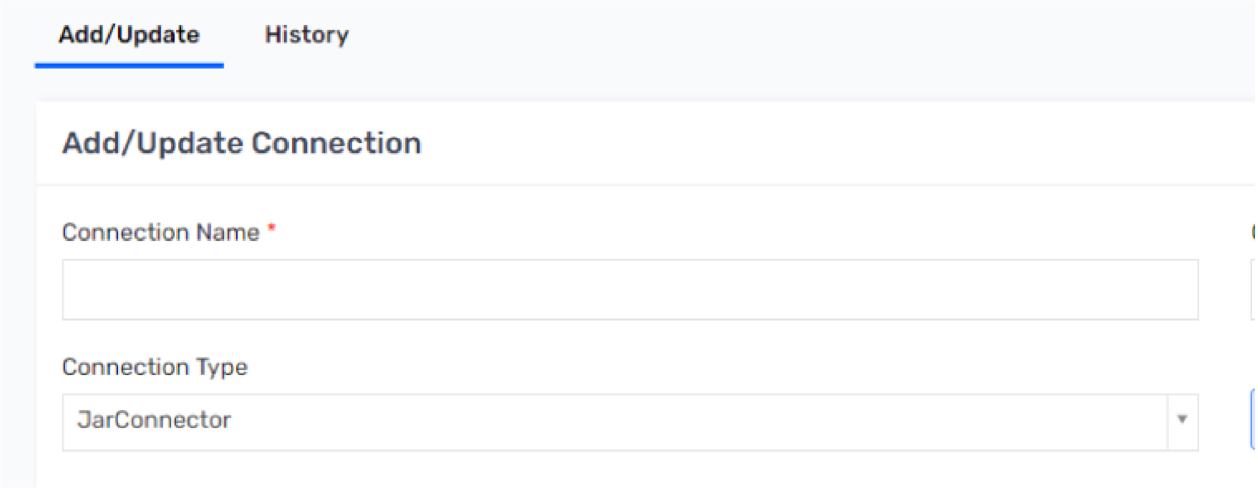
5. Go to **externalJar** and upload the jar file by clicking on Upload New File



FILE NAME	ACTIONS
No data available in table	

Showing 0 to 0 of 0 entries

6. Select the downloaded jar file and deploy it by clicking on Upload button
7. After deploying the jar file restart the application (Admin -> Admin Functions -> Application Restart) Note: The input parameters to the connector are driven via a JarConnector type of Connection in Saviynt EIC Solution from the UI.



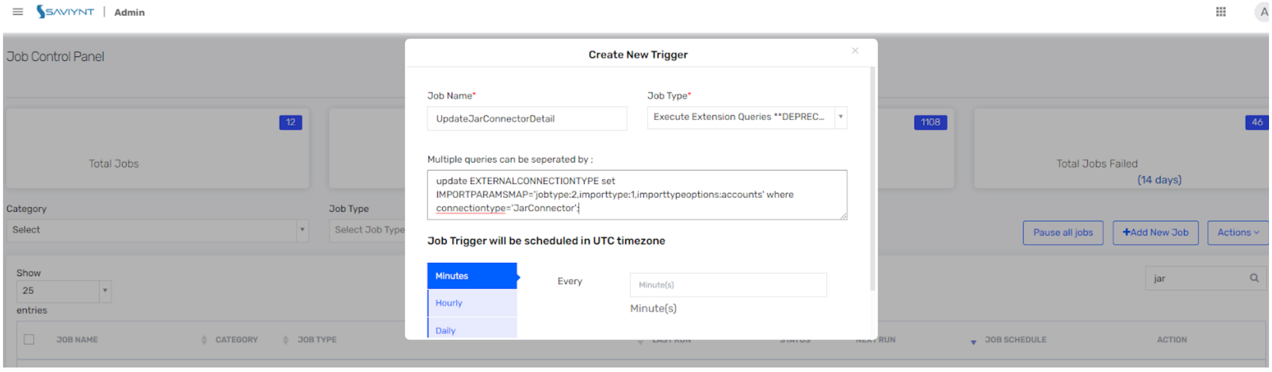
Add/Update Connection

Connection Name *

Connection Type

JarConnector

8. Create a Custom Query Job or Execute Extension Queries type of job trigger



Create New Trigger

Job Name*: UpdateJarConnectorDetail

Job Type*: Execute Extension Queries **DEPREC...

Multiple queries can be seperated by ;

update EXTERNALCONNECTIONTYPE set IMPORTPARAMSMAP='jobtype:2,importtype:1,importtypeoptions:accounts' where connectiontype='JarConnector';

Job Trigger will be scheduled in UTC timezone

Every Minute(s)

9. Use the following query in the job trigger
   update EXTERNALCONNECTIONTYPE set IMPORTPARAMSMAP='jobtype:2,importtype:1,importtypeoptions:accounts' where connectiontype='JarConnector';
10. Click on Save to save the job trigger and execute the newly created Custom Query Job (This is a one-time activity).

Establish a network connectivity with SFTP by opening a firewall port.

If the SFTP location that you are trying to connect is behind the firewall then make sure that the firewall rules to allow connectivity are in place from your SC 2.0 servers.

Identify the authentication method

The connector supports below authentication methods for connecting to SFTP location:

- **Username and Password** : For this the username and password values are stored in the ConnectionJSON of the connection. The ConnectionJSON is encrypted automatically by the Saviynt EIC Solution when the connection is saved. (Please note that once the ConnectionJSON is encrypted, it cannot be decrypted.)
- **Private key file (.pem file)** : For this the .pem file needs to be saved as .csv file and uploaded to the Datafiles directory of Saviynt EIC from UI. Once the key file is uploaded to Datafiles directory as .csv file and a job is triggered to execute this file, the connector automatically takes the file from the Datafiles directory, converts it into .pem file and transfers it to a secure location within Saviynt EIC which is not accessible by users. This way .pem file is secured from unauthorized access by users. If you want to change the key file, then upload the new .pem file to Datafiles directory which will be picked up by the next job run using this connector. *Please refer to APPENDIX section below in this document on how to deploy a private key file (.pem file)*

Understanding the Configuration Parameters

First, we need to create a connection of type JarConnector. In the connection we need to configure configure ConnectionJSON and ImportAccountJSON

Connection Parameters

The connector uses the following parameters for connecting to SFTP location

Parameter	Description	Example Configuration	Mandatory?
Connection Name	Specify the name to identify the connection.	-	Yes
Connection Description	Specify the description for the connection.	-	No

ConnectionJSON	Specify this parameter to create a connection.	Use the following format to connect to the SFTP :
		`{`
		`"SFTPHOST": "111.22.02.56",`
		`"SFTPPORT": "22",`
		`"SFTPUSER": "sftpuser",`
		`"SFTPPASS": "P7686kkjhd"`
		`}`
			Yes

Description of the attributes used in the ConnectionJSON

Property Name	Description	Note
SFTPHOST	IP address or the hostname of the SFTP server on the client side	The names of the properties indicated here may vary. However, these properties are being referred in the ImportAccountsJSON as well. Hence, the same needs to be updated into the ImportAccountsJSON as well.
SFTPPORT	Port number to connect to the SFTP server on the client side	
SFTPUSER	Username for the SFTP user to login to the SFTP server	
SFTPPASS	Password for the SFTP user to login to the SFTP server (Note – Password not required if private key type of authentication is being used. Hence this property needs to be kept blank)	

Please note that once you save the connection, the ConnectionJSON content is encrypted and saved in database. Once encrypted, it cannot be decrypted. So, if you want to change anything in the ConnectionJSON in future, you will have to replace the entire ConnectionJSON in the UI by editing the connection, you will not be able to change a specific line in the ConnectionJSON)

Import Parameters (for transferring the files)

The connector uses the following parameters for transferring files

Parameter	Description	Recommended Configuration	Mandatory?

AccountEntImport JSON	Specify this parameter to import the accounts and entitlements	Use the following format to import accounts and entitlements using the SFTP:
		`{`
		`"fullyQualifiedClassName": "com.saviynt.connector.SFTPConnector.FileTransferUtilitywithargs",`
		`"methodName": "saviyntFileTransfer_SFTP",`
			Yes

```
        "arguments": {

                "SFTPHOST":
"${connectionJSON.SFTPHOST}",

                "SFTPPORT":
"${connectionJSON.SFTPPORT}",

                "SFTPUSER":
"${connectionJSON.SFTPUSER}",

                "SFTPPASS":
"${connectionJSON.SFTPPASS}",

                "ACTION":
"download",


"SFTP_DIRECTORY":"/upload/",


"SAVIYNT_DIRECTORY":"
/saviynt_shared/saviynt/Import
/",


"FILE_NAME_LIST":"AWS_TEST.
csv",


"SFTP_LOGFILE_DIRECTORY":"
/saviynt_shared/saviynt/Import
/Success/",


"DELETE_SOURCE_FILE_AFTER_DOWNL
OAD":"no",


"SFTP_KEY_PATH":"
/saviynt_shared/saviynt/Import
/Datafiles/",

"SFTP_KEYFILE_NAME":"sftp_key.
csv",
                "SFTP_ CERT
_DEFAULT_PATH":"/saviynt_shared
/saviynt/Import/Datafiles/",


"LOG_FILE_AGE":"2"
        }
}
```

Description of the attributes used in the ImportAccountsJSON

Property Name	Description	Note
fullyQualifiedClassName	This is the class name which is invoked in the utility and the value must always be “com.saviynt.connector.SFTPConnector. FileTransferUtilitywithargs”.	The key and the value for this property must NOT be changed
methodName	Method name in the utility to be invoked for performing download and upload actions and the value must always be “saviyntFileTransfer_SFTP”.	The key and the value for this property must NOT be changed
arguments	These are the arguments which are required by the utility to be executed. The value for this property will always be a JSON.	The key for this property must NOT be changed
SFTPHOST	This property should point to the property which defines the SFTP host/server in the ConnectionJSON. ‘connectionJSON’ is the object which points to the ConnectionJSON and any attribute from the ConnectionJSON can be accessed as the following ${connectionJSON.<<propertyName>>}	The key for this property must NOT be changed. The value for this must point to the property in ConnectionJSON which holds the value of the SFTP server on client side.
SFTPPORT	This property should point to the property which defines the SFTP host/server Port in the ConnectionJSON. ‘connectionJSON’ is the object which points to the ConnectionJSON and any attribute from the ConnectionJSON can be accessed as the following ${connectionJSON.<<propertyName>>}	The key for this property must NOT be changed. The value for this must point to the property in ConnectionJSON which holds the value of the SFTP server Port on client side.
SFTPUSER	This property should point to the property which defines the SFTP host/server username in the ConnectionJSON. connectionJSON is the object which points to the ConnectionJSON and any attribute from the ConnectionJSON can be accessed as the following ${connectionJSON.<<propertyName>>}	The key for this property must NOT be changed. The value for this must point to the property in ConnectionJSON which holds the value of the SFTP server username on client side.
SFTPPASS	This property should point to the property which defines the SFTP host/server user’s password in the ConnectionJSON. connectionJSON is the object which points to the ConnectionJSON and any attribute from the ConnectionJSON can be accessed as the following ${connectionJSON.<<propertyName>>}	The key for this property must NOT be changed. The value for this must point to the property in ConnectionJSON which holds the value of the SFTP server user’s password on client side.

Property Name	Description
ACTION	Allowed values are DOWNLOAD or UPLOAD • Use ‘DOWNLOAD as the value if you intend to transfer files from SFTP location to Saviynt EIC’s Datafiles or SAV directories • Use ‘UPLOAD as the value if you intend to transfer files from /Reports directory of Saviynt EIC to SFTP location

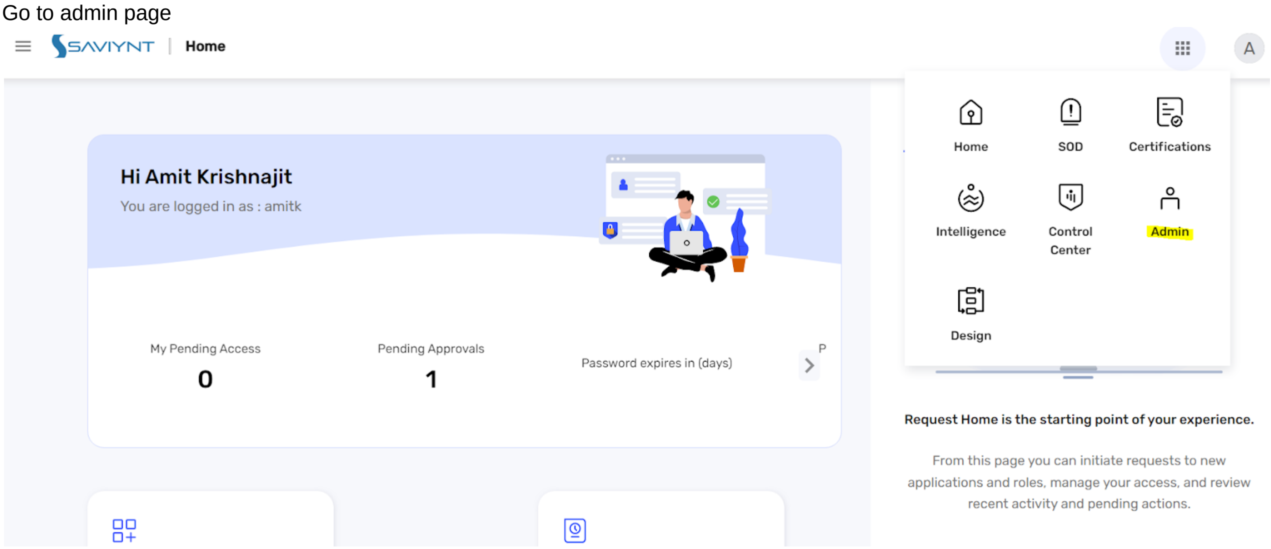
SFTP_DIRECTORY	Directory path on the SFTP server to/from which files need to be transferred. This path is given by customer's team who provides the SFTP location details. This path is not given by Saviynt team. Note: Please ensure that the directory path given for this always ends with a forward slash (/). Please see below example e.g.: /upload/
SAVIYNT_DIRECTORY	This is the directory path on the Saviynt EIC solution from/to which files need to be transferred. The path value differs on the value of the ACTION property: - When ACTION property is DOWNLOAD, provide Saviynt file system directory path until the **Import** directory (just one level above Datafiles directory). e.g:*/saviynt_shared/saviynt/Import/* - When ACTION property is UPLOAD, provide Saviynt file system directory path until the **Reports** directory e.g:*/saviynt_shared/saviynt/Reports/* **Note:** - Please ensure that the directory path given for this always ends with a forward slash (/). Please see below example: */saviynt_shared/saviynt/Import/* */saviynt_shared/saviynt/Reports/* - Please note that this directory path value differs based on the version of Saviynt EIC solution the customer is using. For example, for v2021 version of EIC, the path will be */saviynt_shared/saviynt/Import/* (for DOWNLOAD) *and /saviynt_shared/saviynt/Reports/* (for UPLOAD) And for v5.5 sp3.x and v2020.x versions of EIC, the path will be */opt/sharedappdrive/saviynt/Import/* (for DOWNLOAD) and */opt/sharedappdrive/saviynt/Reports/* (for UPLOAD) - The above only are examples. Please open a Fresh Desk ticket with Saviynt support to get the exact path for the Saviynt EIC version the customer is using
FILE_NAME_LIST	Comma separated values of the file names that you intend to transfer. Utility supports transferring multiple files at a time. Below are the file types that are supported from transfer: - For DOWNLOAD action only .csv and .sav file types are supported by the utility - For UPLOAD action only .csv, .txt, .xls and .xlsx files are supported by the utility **Note:** - Please include the file extension in the file name - Do not include space before or after comma in the comma separated list. See below example e.g.: Employee_users.csv, Schema_USERS.sav

FILE_NAME_REGEX	If you want to transfer files matching a specific pattern, please use this property to capture the regex (regular expression) for the file name pattern. The regex should comply with standard regex syntax. e.g.: =^.*Test?[-_. A-Za-z0-9]* Below are the file types that are supported from transfer: • For DOWNLOAD action only .csv and .sav file types are supported by the utility • For UPLOAD action only .csv, .txt, .xls and .xlsx files are supported by the utility **Note:** • Do NOT include file extensions in the regular expression. Just mention the regex for name of the file • In case of UPLOAD action, if multiple files are found matching the regular expression in the /Reports directory. Only the file with latest timestamp will be transferred from Saviynt EIC to SFTP location • In case of REGEX, please add four slash(\\\\) for every slash which is present in the REGEX, e.g., when using \d in the expression, it should be added to the REGEX as \\\\d.
FILE_EXTENSION	This is an optional property. By design below are the file types that are supported for transfer by the utiity: • For DOWNLOAD action only .csv and .sav file types are supported by the utility • For UPLOAD action only .csv, .txt, .xls and .xlsx files are supported by the utility If you want to restrict the utility to transfer only specific file types from the above file types, then you can mention the comma separated values of the extensions as shown in the below example. Please note that if you provide any file extensions that are outside of the supported file extensions above, they will be ignored e.g: *.csv,.txt*
SFTP_KEY_PATH	This property is used when a private key file (.pem file) based authentication is used for connecting to SFTP server. Utility will first check if this property and SFTP_KEYFILE_NAME properties are not blank. If so, it will use private key file (.pem file) based authentication else the utility will check for SFTPUSER and SFTPPASS properties and uses username /password based authentication By design the private key (.pem file) needs to be uploaded to Datafiles directory from Saviynt EIC UI. Please refer to section 3.2.5 on how to upload the private key file. Use this property to capture the Saviynt file system directory path where the private key file for SFTP authentication is stored, which is the path to the Datafiles directory. Please note that this path value differs based on the version of Saviynt EIC solution the customer is using. For example, for v2021 version of EIC, the path will be */saviynt_shared/saviynt/Import/Datafiles/* and for v5.5 sp3.x and v2020.x versions of EIC, the path will be */opt/sharedappdrive/saviynt/Import/Datafiles/*
SFTP_KEYFILE_NAME	Provide the name of the private key file that was uploaded to Datafiles Directory e.g.: sftp_key.csv
SFTP_ CERT _DEFAULT_PATH	This is the folder where the utility will look for the key file. Please keep the path until Datafiles directory e.g.: /saviynt_shared/saviynt/Import/Datafiles/

SFTP_LOGFILE_DIRECTORY	This is an optional parameter By default, the log statements of the utility are written to Saviynt debug logs which are visible under *Application Logs* in UI. Additionally, the utility can be configured to write the log file statements to a custom log file under /Datafiles/Success so that the log file can be viewed from the UI under Success directory e.g.: */saviynt_shared/saviynt/Import/* **Note:** - Please ensure that the directory path given for this always ends with a forward slash (/). Please see below example: */saviynt_shared/saviynt/Import/* - Please note that this directory path value differs based on the version of Saviynt EIC solution the customer is using. For example, for v2021 version of EIC, the path will be */saviynt_shared/saviynt/Import/* and for v5.5 sp3.x and v2020.x versions of EIC, the path will be */opt/sharedappdrive/saviynt/Import/*
LOG_FILE_AGE	Number of days to retain the custom log file. Please note that max allowed days are 30 and default days are 7 e.g. 5
DELETE_SOURCE_FILE_AFTER_DOWNLOAD	Allowed values: Yes or No If Yes, utility will delete the source file from SFTP location after successfully downloading the file on to Saviynt side If No, utility will NOT delete the source file from SFTP location after successfully downloading the file on to Saviynt side This is applicable only for DOWNLOAD action

Creating a Connection

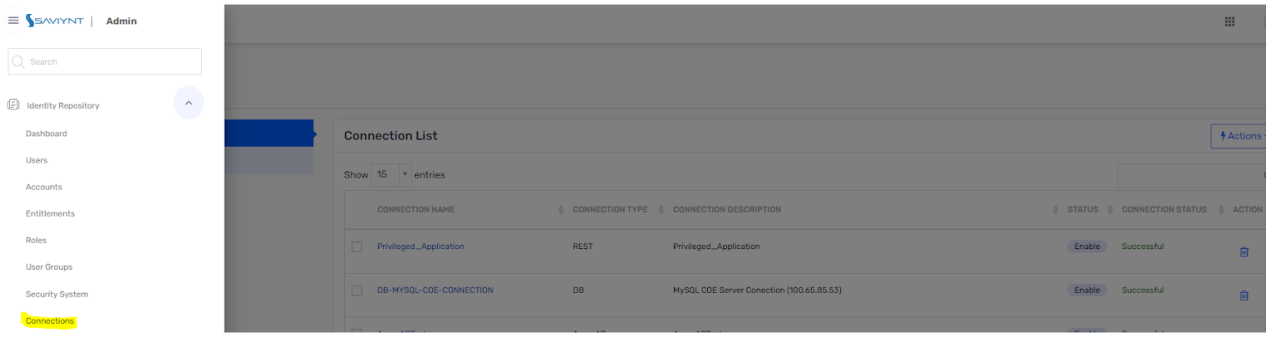
First, we need to create a connection of type JarConnector. In the connectionJSON we need to configure configure ConnectionJSON and ImportAccountJSON. Follow the below steps for the configuration:

1. Login to EIC as an admin user with required privileges
2. Go to admin page
3. 

Request Home is the starting point of your experience.

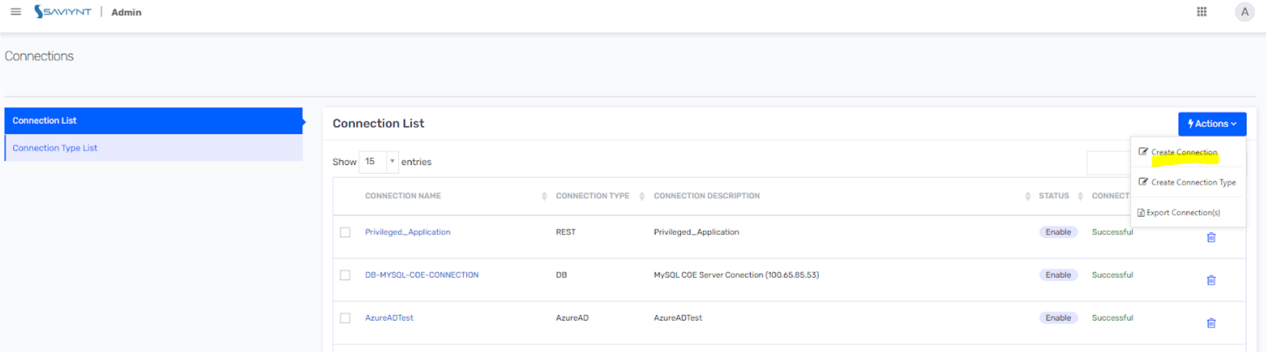
From this page you can initiate requests to new applications and roles, manage your access, and review recent activity and pending actions.

4. Go to Identity Repository -> Connections



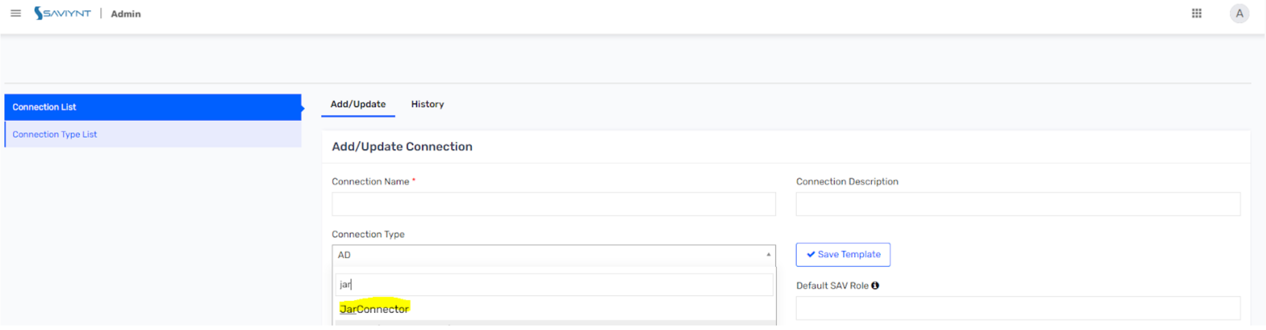
CONNECTION NAME	CONNECTION TYPE	CONNECTION DESCRIPTION	STATUS	CONNECTION STATUS	ACTION
Privileged_Application	REST	Privileged_Application	Enable	Successful	
DB-MYSQL-COE-CONNECTION	DB	MySQL COE Server Conection (100.65.85.53)	Enable	Successful	

5. Click on Actions -> Create Connection



CONNECTION NAME	CONNECTION TYPE	CONNECTION DESCRIPTION	STATUS	CONNECT
Privileged_Application	REST	Privileged_Application	Enable	Successful
DB-MYSQL-COE-CONNECTION	DB	MySQL COE Server Conection (100.65.85.53)	Enable	Successful
AzureADTest	AzureAD	AzureADTest	Enable	Successful

6. Select Connection Type as JarConnector



Connection Name *

Connection Description

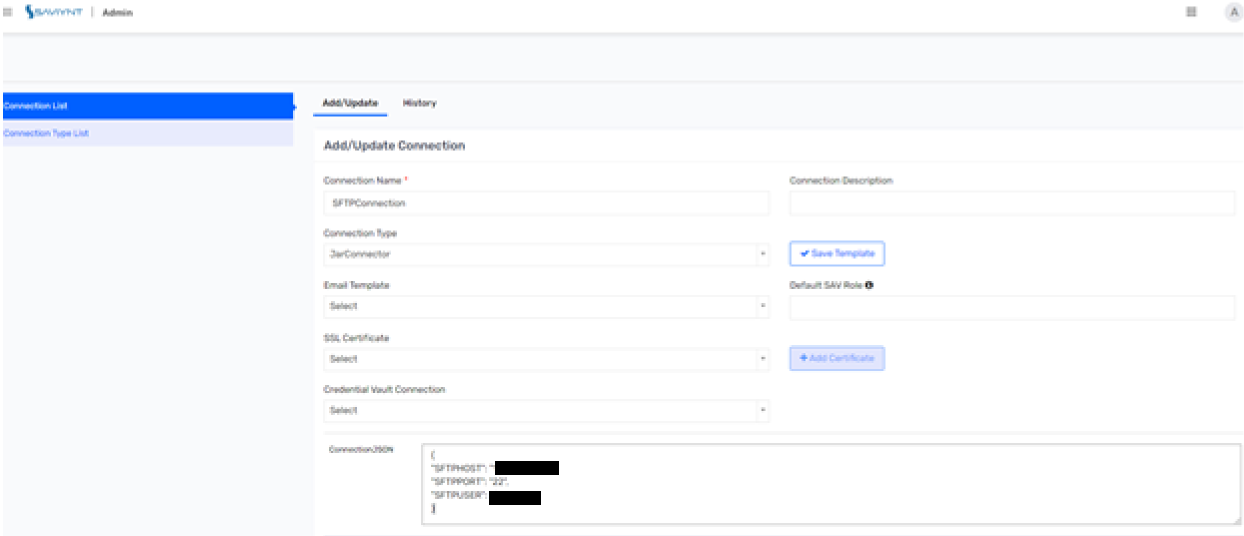
Connection Type: AD

jar

JarConnector

Default SAV Role

7. Provide a Connection Name, ConnectionJSON and ImportAccountsJSON and click on Save connection



Connection Name *: SFTPConnection

Connection Description

Connection Type: JarConnector

Email Template: Select

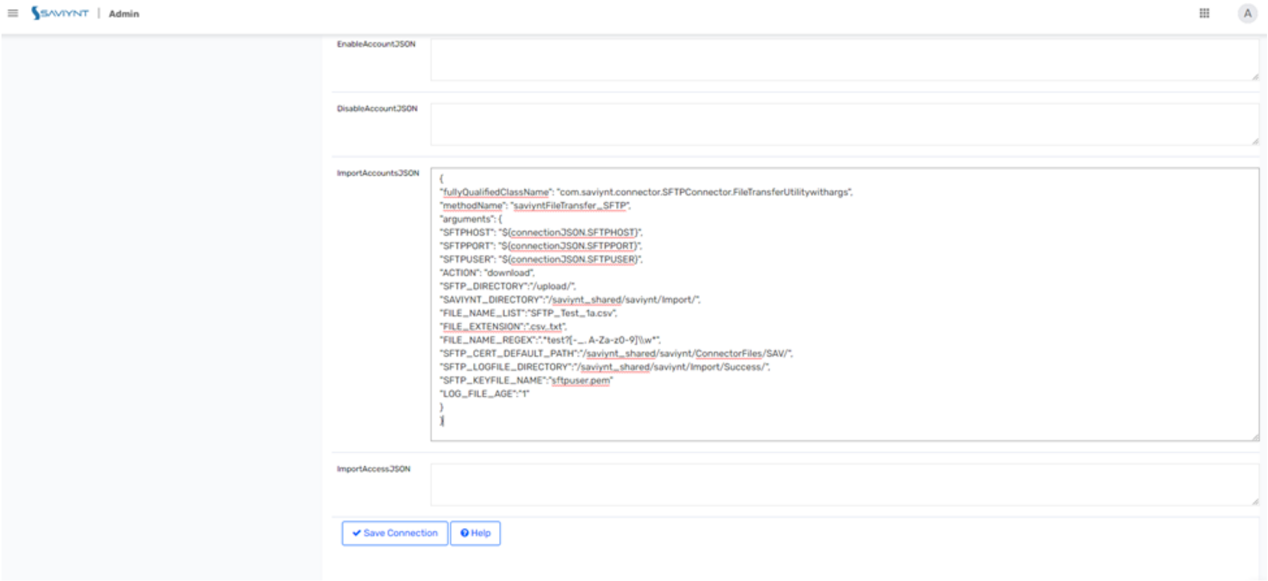
Default SAV Role

SSL Certificate: Select

Credential Vault Connection: Select

ConnectionJSON

```
{
"SFTPHOST": "[redacted]
"SFTPPORT": "22",
"SFTPUSER": [redacted]
}
```



EnableAccountJSON

DisableAccountJSON

ImportAccountsJSON

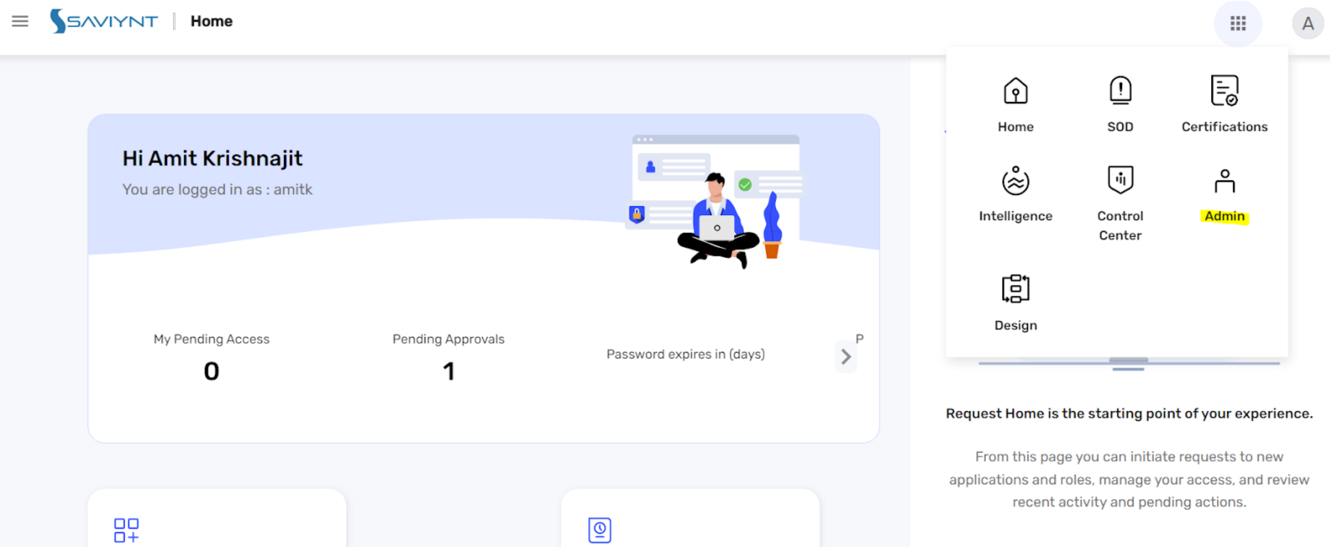
```
{
"fullyQualifiedClassName": "com.saviynt.connector.SFTPConnector.FileTransferUtilitywithargs",
"methodName": "saviyntFileTransfer_SFTP",
"arguments": {
"SFTPHOST": "${connectionJSON.SFTPHOST}",
"SFTPPORT": "${connectionJSON.SFTPPORT}",
"SFTPUSER": "${connectionJSON.SFTPUSER}",
"ACTION": "download",
"SFTP_DIRECTORY":"/upload/",
"SAVIYNT_DIRECTORY":"/saviynt_shared/saviynt/Import/",
"FILE_NAME_LIST":"SFTP_Test_1a.csv",
"FILE_EXTENSION":".csv,.txt",
"FILE_NAME_REGEX":"."test?[-_. A-Za-z0-9]\\.w*",
"SFTP_CERT_DEFAULT_PATH":"/saviynt_shared/saviynt/ConnectorFiles/SAV/",
"SFTP_LOGFILE_DIRECTORY":"/saviynt_shared/saviynt/Import/Success/",
"SFTP_KEYFILE_NAME":"sftpuser.pem"
"LOG_FILE_AGE":"1"
}
}
```

ImportAccessJSON

Creating a Security System and Endpoint

A security system and endpoint need to be created so that the Jar connection can be mapped to it.

1. Login to EIC as an admin user with required privileges
2. Go to admin page



Hi Amit Krishnajit

You are logged in as : amitk

My Pending Access 0

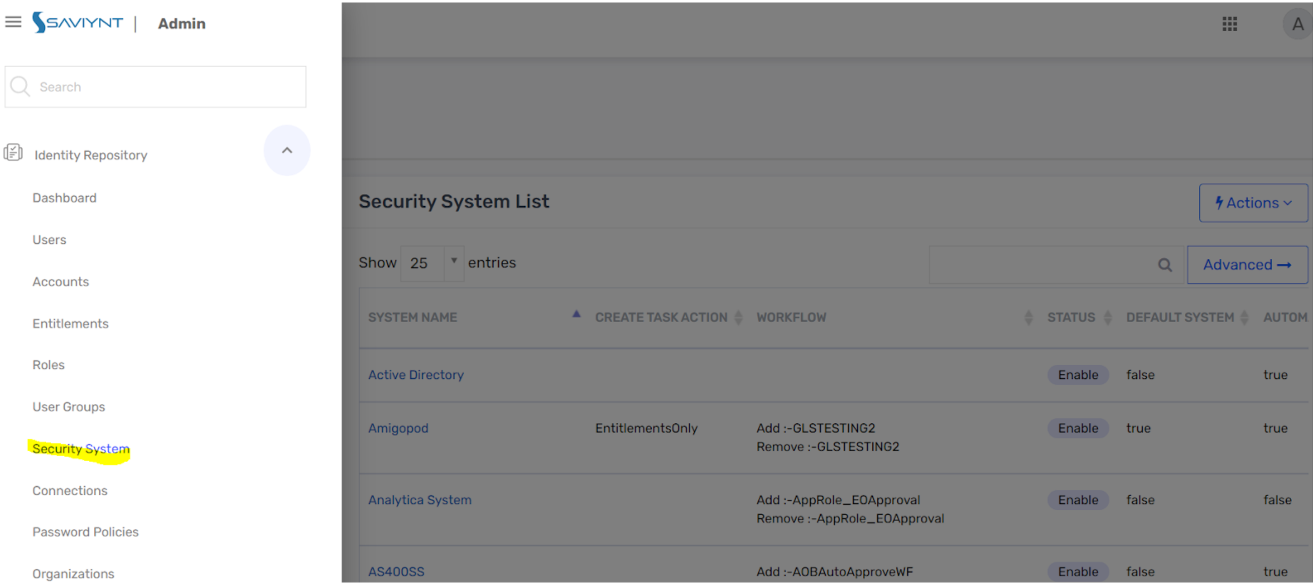
Pending Approvals 1

Password expires in (days)

Request Home is the starting point of your experience.

From this page you can initiate requests to new applications and roles, manage your access, and review recent activity and pending actions.

3. Go to Identity Repository -> Security System

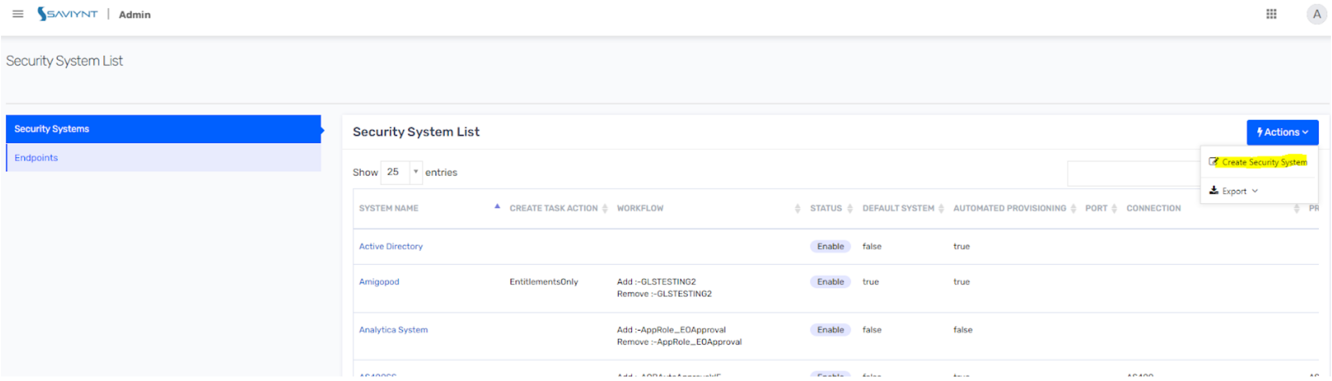


Security System List

Show 25 entries

SYSTEM NAME	CREATE TASK ACTION	WORKFLOW	STATUS	DEFAULT SYSTEM	AUTOM
Active Directory			Enable	false	true
Amigopod	EntitlementsOnly	Add :-GLSTESTING2 Remove :-GLSTESTING2	Enable	true	true
Analytica System		Add :-AppRole_EOApproval Remove :-AppRole_EOApproval	Enable	false	false
AS400SS		Add :-AOBAutoApproveWF	Enable	false	true

4. Click on Actions -> Create Security System

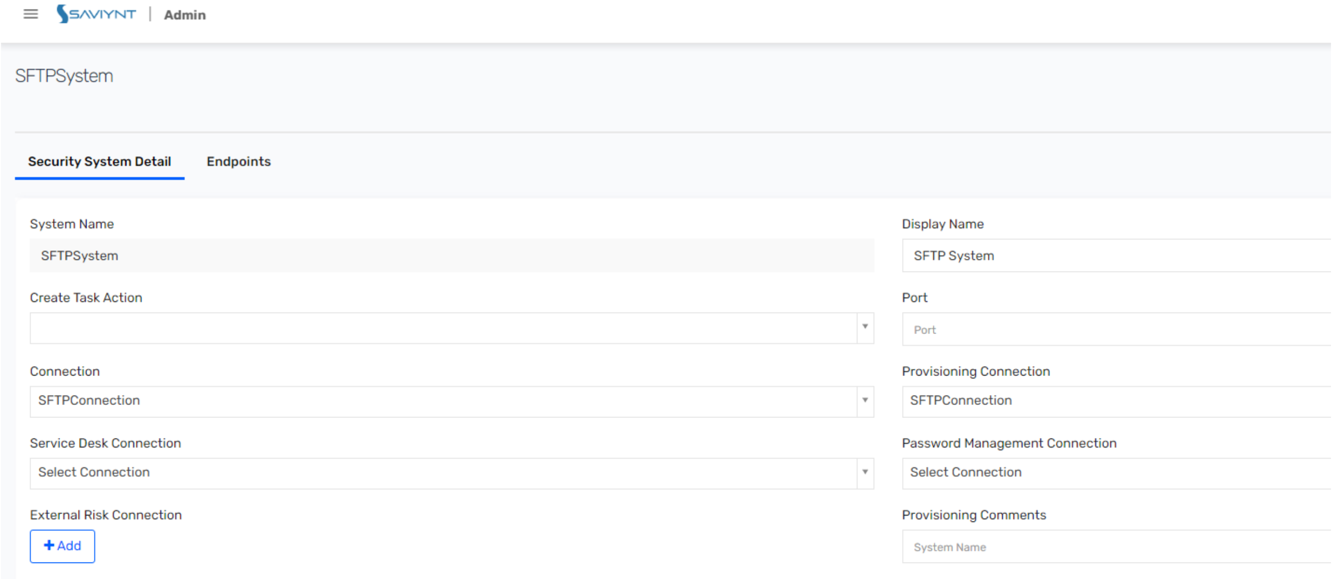


Security System List

Show 25 entries

SYSTEM NAME	CREATE TASK ACTION	WORKFLOW	STATUS	DEFAULT SYSTEM	AUTOMATED PROVISIONING	PORT	CONNECTION	PR
Active Directory			Enable	false	true			
Amigopod	EntitlementsOnly	Add :-GLSTESTING2 Remove :-GLSTESTING2	Enable	true	true			
Analytica System		Add :-AppRole_EOApproval Remove :-AppRole_EOApproval	Enable	false	false			

5. Input the System Name, display name, select the Connection and Provisioning Connection as the JarConnector connection created above.



System Name: SFTPSystem

Display Name: SFTP System

Create Task Action:

Port: Port

Connection: SFTPConnection

Provisioning Connection: SFTPConnection

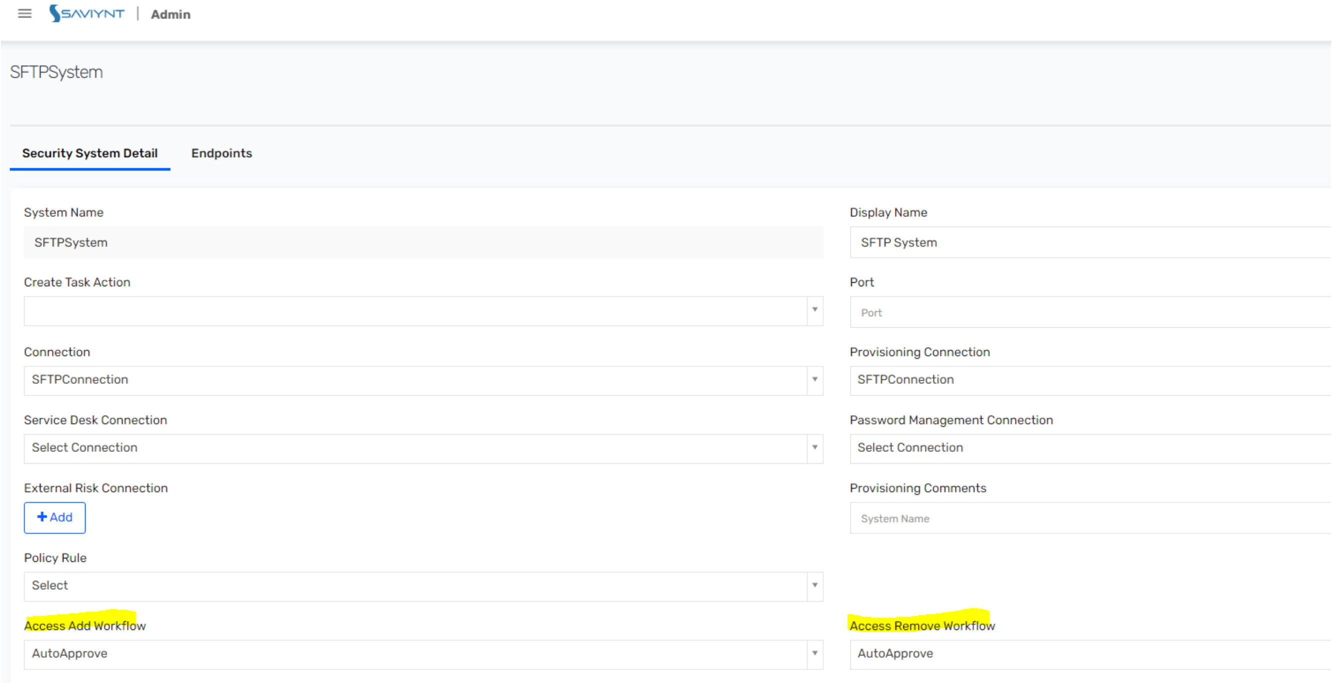
Service Desk Connection: Select Connection

Password Management Connection: Select Connection

External Risk Connection

Provisioning Comments: System Name

6. Select an Auto Approve workflow in the Access Add Workflow and Access Remove Workflow in the Security System (Refer to APPENDIX section on how to create an Auto Approve Workflow)



System Name: SFTPSystem

Display Name: SFTP System

Create Task Action:

Port: Port

Connection: SFTPConnection

Provisioning Connection: SFTPConnection

Service Desk Connection: Select Connection

Password Management Connection: Select Connection

External Risk Connection

Provisioning Comments: System Name

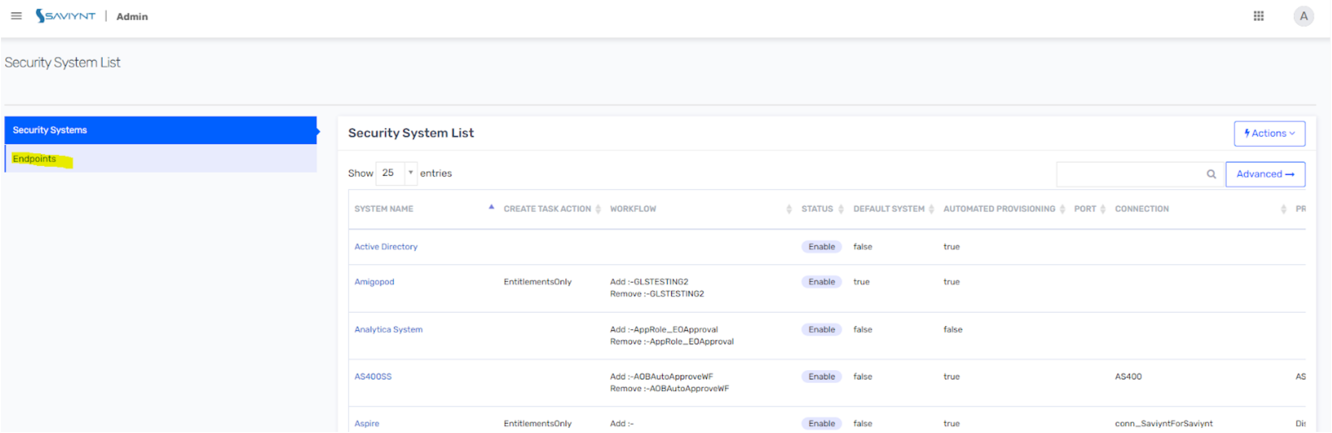
Policy Rule: Select

Access Add Workflow: AutoApprove

Access Remove Workflow: AutoApprove

7. After the Security System is created, go to Identity Repository -> Security System

8. Go to Endpoints section



Security System List

Security Systems

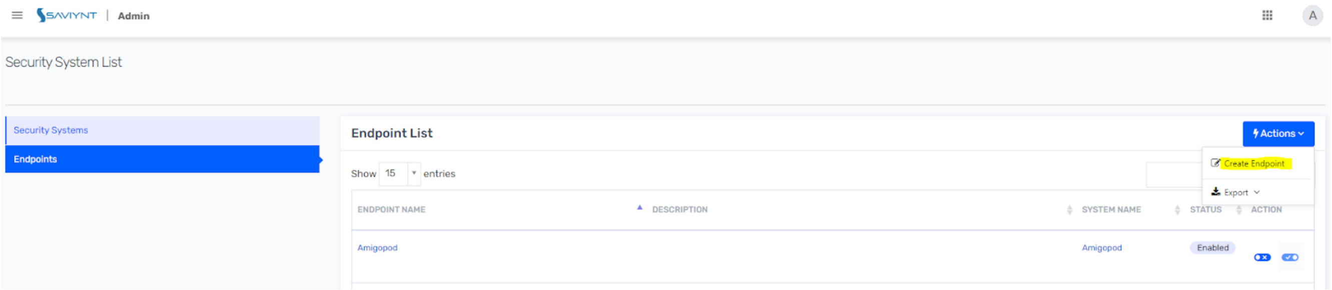
Endpoints

Security System List

Show 25 entries

SYSTEM NAME	CREATE TASK ACTION	WORKFLOW	STATUS	DEFAULT SYSTEM	AUTOMATED PROVISIONING	PORT	CONNECTION	PR
Active Directory			Enable	false	true			
Amigopod	EntitlementsOnly	Add :-GLSTESTING2 Remove :-GLSTESTING2	Enable	true	true			
Analytica System		Add :-AppRole_EOApproval Remove :-AppRole_EOApproval	Enable	false	false			
AS400SS		Add :-AOBAutoApproveWF Remove :-AOBAutoApproveWF	Enable	false	true		AS400	AS
Aspire	EntitlementsOnly	Add :-	Enable	false	true		conn_SaviyntForSaviynt	Di

9. Click on Actions -> Create Endpoint



Security System List

Security Systems

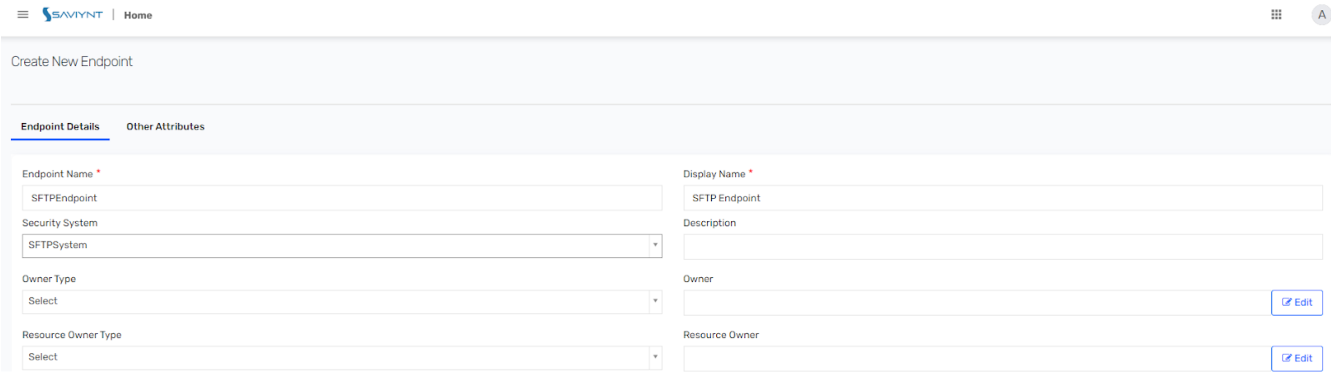
Endpoints

Endpoint List

Show 15 entries

ENDPOINT NAME	DESCRIPTION	SYSTEM NAME	STATUS	ACTION
Amigopod		Amigopod	Enabled	

10. Provide the Endpoint name, display name and select the Security system which was created in the previous step



Create New Endpoint

Endpoint Details | Other Attributes

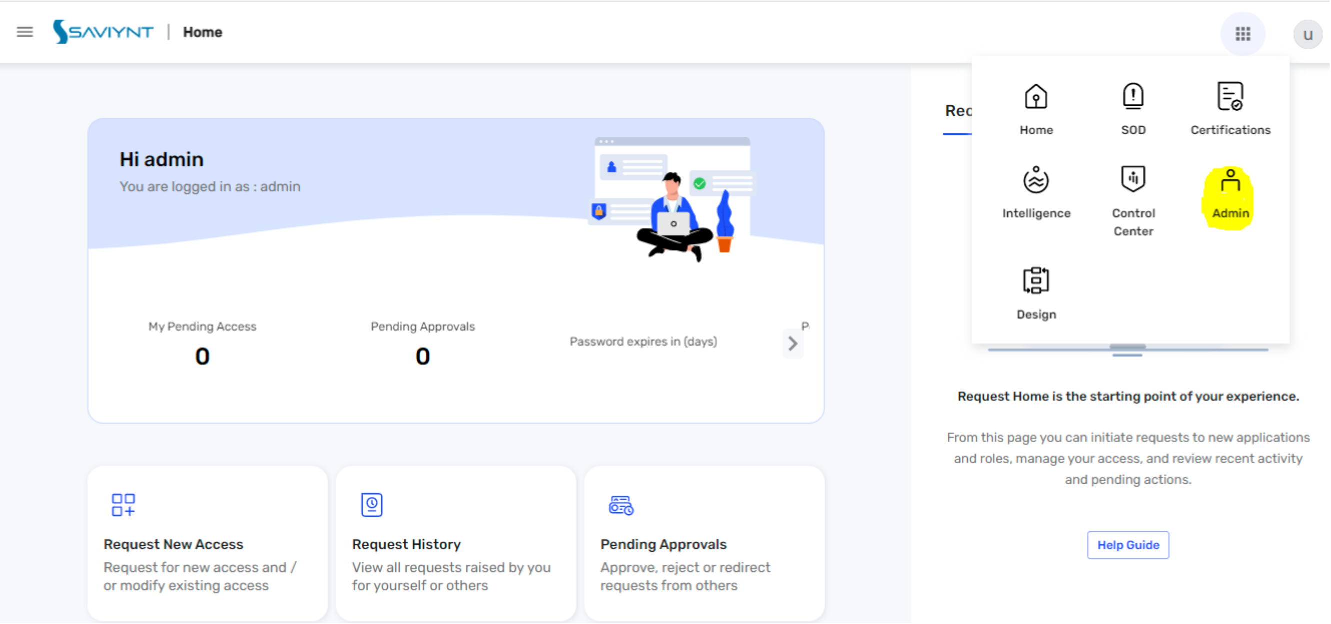
Endpoint Name *	Display Name *
SFTPEndpoint	SFTP Endpoint
Security System	Description
SFTPSystem	
Owner Type	Owner
Select	
Resource Owner Type	Resource Owner
Select	

11. Click on Create button to create the endpoint

Using the SFTP File Transfer Utility for Transferring the files

Once the deployment and configuration steps mentioned above are complete, perform the transfer of files by following the below steps:

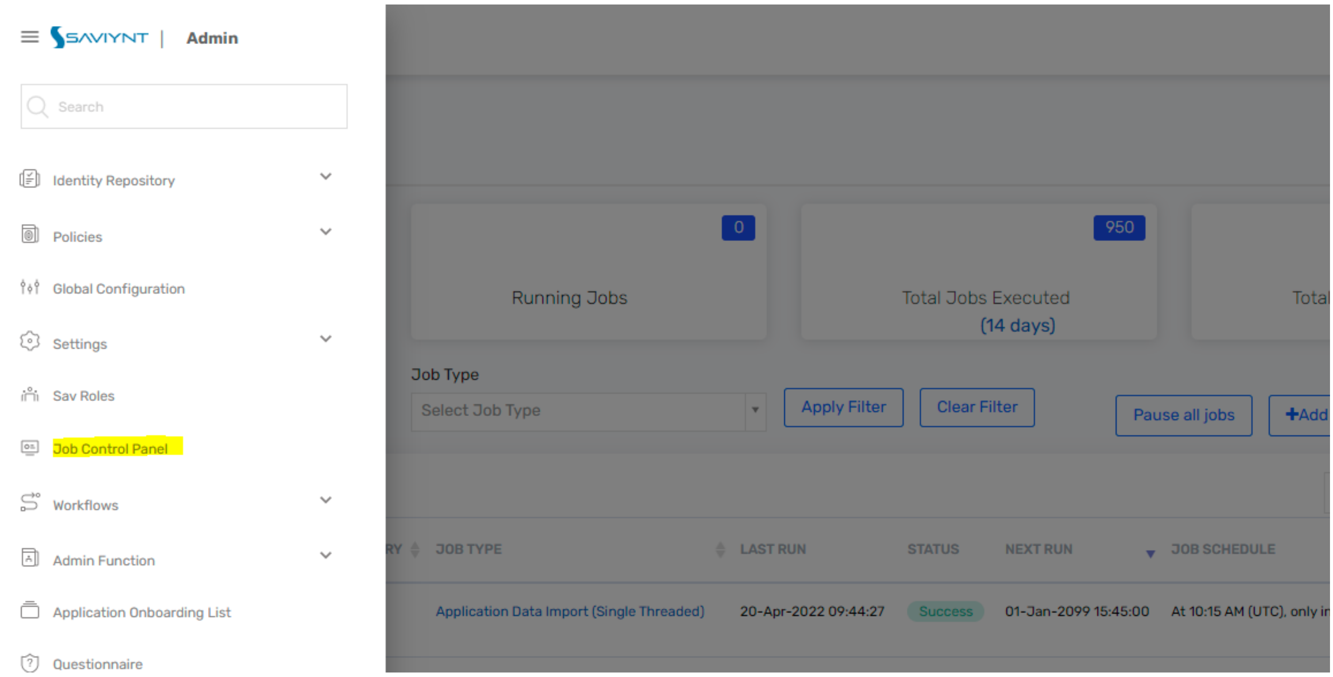
1. Login to EIC as an admin user with required privileges
2. Go to admin page


SAVIYNT | Home
u
Rec
Home
SOD
Certifications
Intelligence
Control Center
Admin
Design
Hi admin
You are logged in as : admin
My Pending Access
0
Pending Approvals
0
Password expires in (days)
P
Request New Access
Request for new access and / or modify existing access
Request History
View all requests raised by you for yourself or others
Pending Approvals
Approve, reject or redirect requests from others
Help Guide

Request Home is the starting point of your experience.

From this page you can initiate requests to new applications and roles, manage your access, and review recent activity and pending actions.

3. Go to Job Control Panel

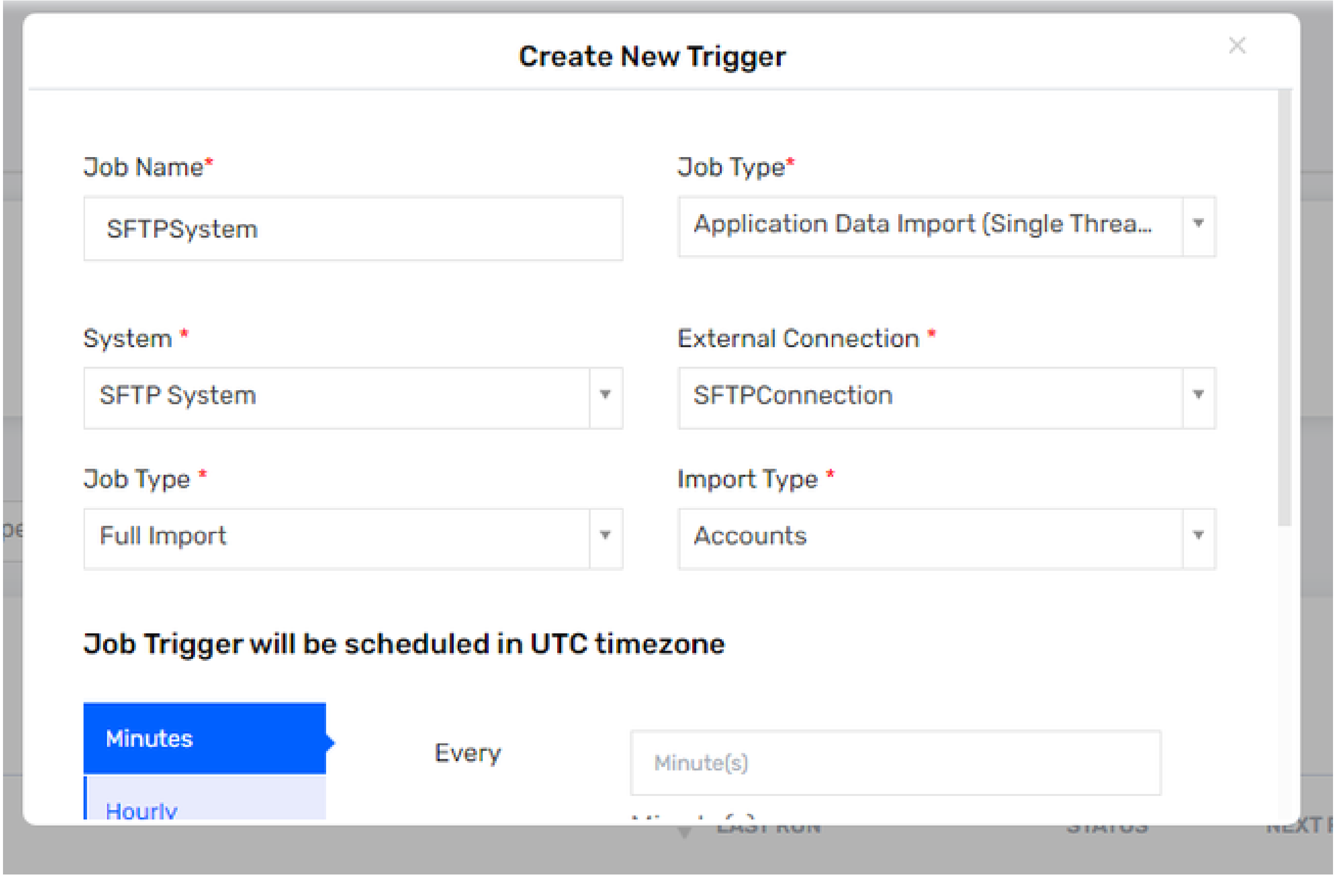


RY	JOB TYPE	LAST RUN	STATUS	NEXT RUN	JOB SCHEDULE
	Application Data Import (Single Threaded)	20-Apr-2022 09:44:27	Success	01-Jan-2099 15:45:00	At 10:15 AM (UTC), only ir

4. Click on Add New Job button on the screen

5. It will open a create new trigger pop-up. Fill in the details as shown below.

Parameter	Value	Notes
Job Name	A meaning ful job name of your choice (e.g SFTPFileTransfer)	
Job Type	Application Data Import (Single Threaded)	Use the value as-is
System	e.g: SFTP System	Select from the dropdown the Security System where the Jar Connection was mapped to.
External Connection	e.g: SFTPConnection	This will auto-populate on selection of the System. The value would be the name of the Jar Connection which was created.
Job Type	Full Import	Select the value from the dropdown
Import Type	Accounts	Select the value from the dropdown



Create New Trigger

Job Name* SFTPSystem

Job Type* Application Data Import (Single Threa...

System * SFTP System

External Connection * SFTPConnection

Job Type * Full Import

Import Type * Accounts

Job Trigger will be scheduled in UTC timezone

Minutes

Hourly

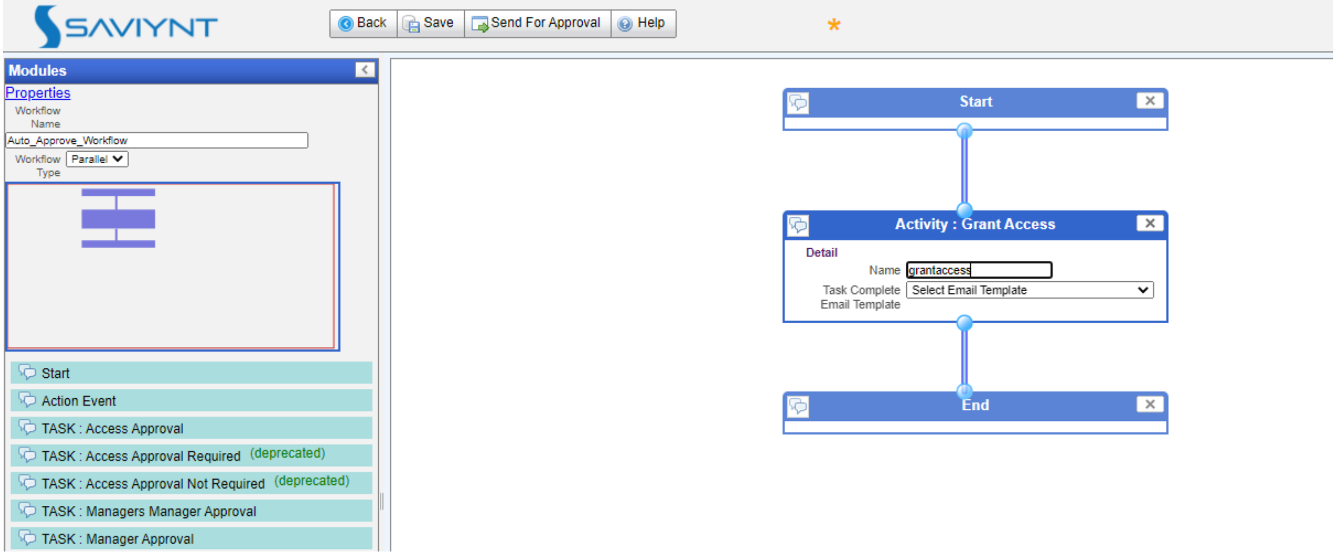
Every Minute(s)

APPENDIX

1.Question: How to create an auto-approve workflow?

Answer: Please create a workflow by following the below steps

1. Go to Admin -> Workflows -> Workflow List
2. Click on Actions -> Create New Workflow
3. Create a workflow in the following way:



Workflow Name Auto_Approve_Workflow

Workflow Type Parallel

- Start
- Action Event
- TASK : Access Approval
- TASK : Access Approval Required (deprecated)
- TASK : Access Approval Not Required (deprecated)
- TASK : Managers Manager Approval
- TASK : Manager Approval

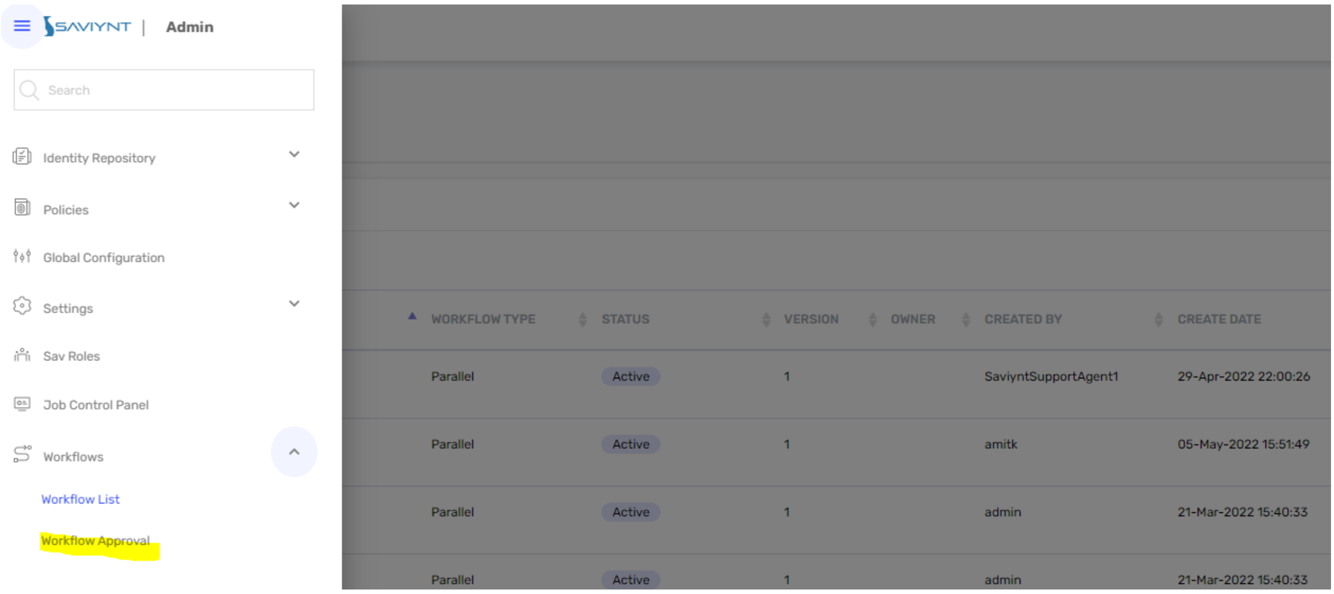
Detail

Name grantaccess

Task Complete Email Template Select Email Template

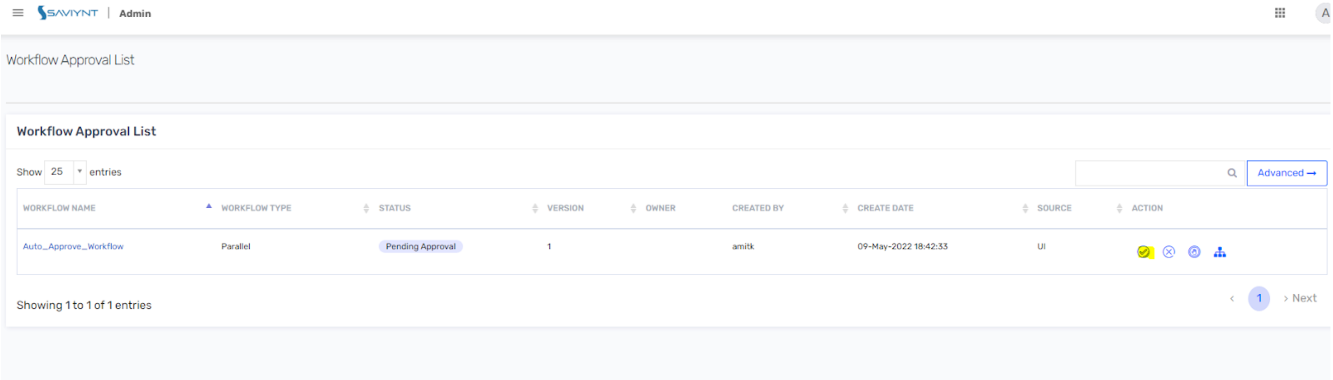
3. Click on Save and then click on Send for Approval

4. Go to Admin -> Workflows -> Workflow Approval



WORKFLOW TYPE	STATUS	VERSION	OWNER	CREATED BY	CREATE DATE
Parallel	Active	1		SaviyntSupportAgent1	29-Apr-2022 22:00:26
Parallel	Active	1		amitk	05-May-2022 15:51:49
Parallel	Active	1		admin	21-Mar-2022 15:40:33
Parallel	Active	1		admin	21-Mar-2022 15:40:33

5. Click on Accept

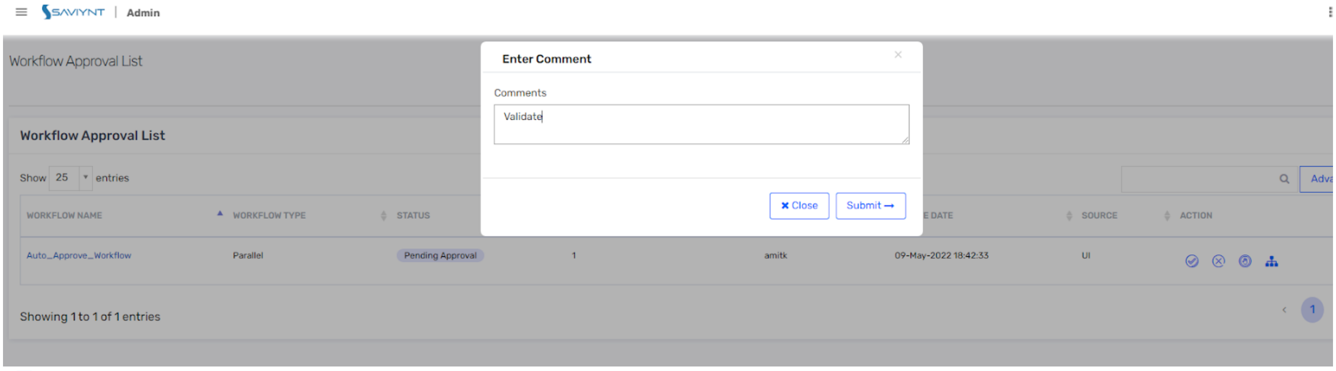


Workflow Approval List

WORKFLOW NAME	WORKFLOW TYPE	STATUS	VERSION	OWNER	CREATED BY	CREATE DATE	SOURCE	ACTION
Auto_Approve_Workflow	Parallel	Pending Approval	1		amitk	09-May-2022 18:42:33	UI	

Showing 1 to 1 of 1 entries

6. Provide some comments and submit

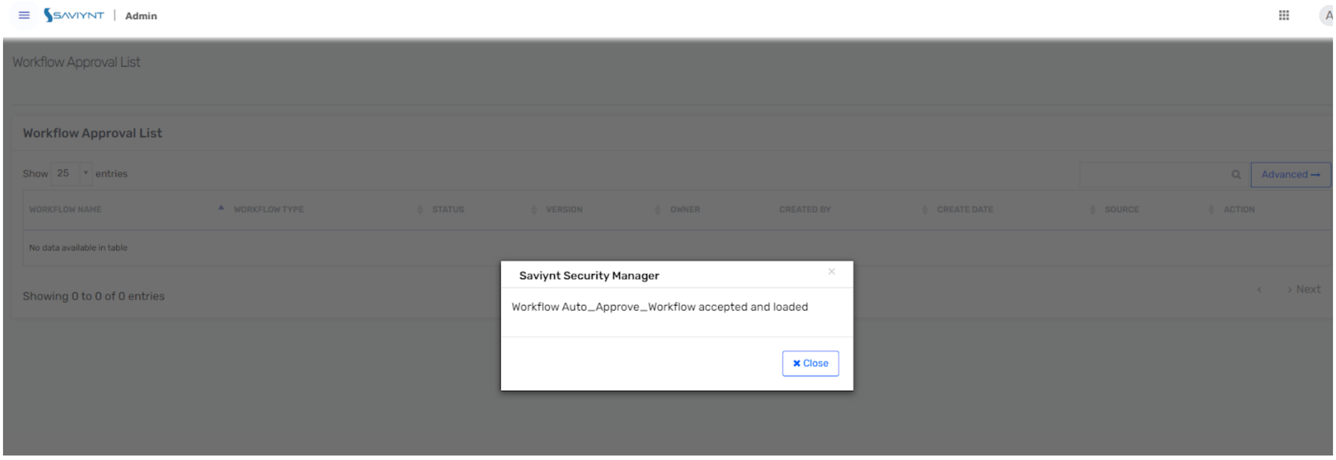


Enter Comment

Comments: Validate

WORKFLOW NAME	WORKFLOW TYPE	STATUS				E DATE	SOURCE	ACTION
Auto_Approve_Workflow	Parallel	Pending Approval	1		amitk	09-May-2022 18:42:33	UI	

Showing 1 to 1 of 1 entries



Workflow Approval List

WORKFLOW NAME	WORKFLOW TYPE	STATUS	VERSION	OWNER	CREATED BY	CREATE DATE	SOURCE	ACTION
No data available in table								

Showing 0 to 0 of 0 entries

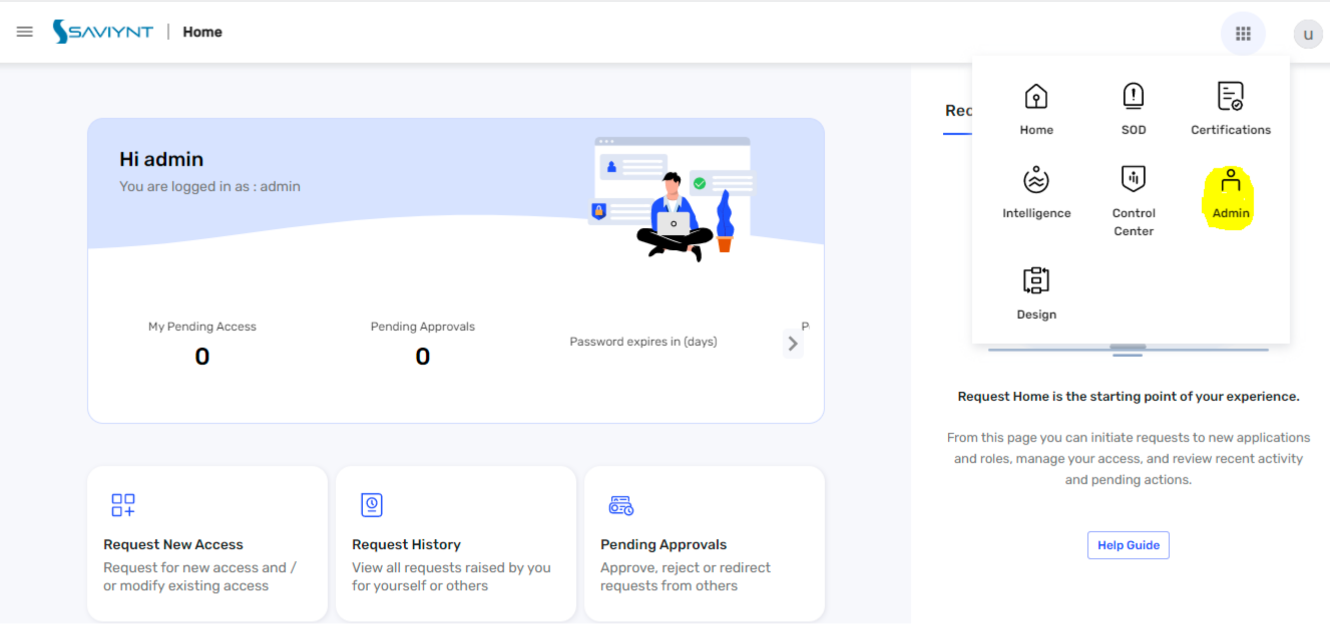
Saviynt Security Manager

Workflow Auto_Approve_Workflow accepted and loaded

2. Question: How do I transfer the private key (.pem) file for SFTP authentication ?

Answer:

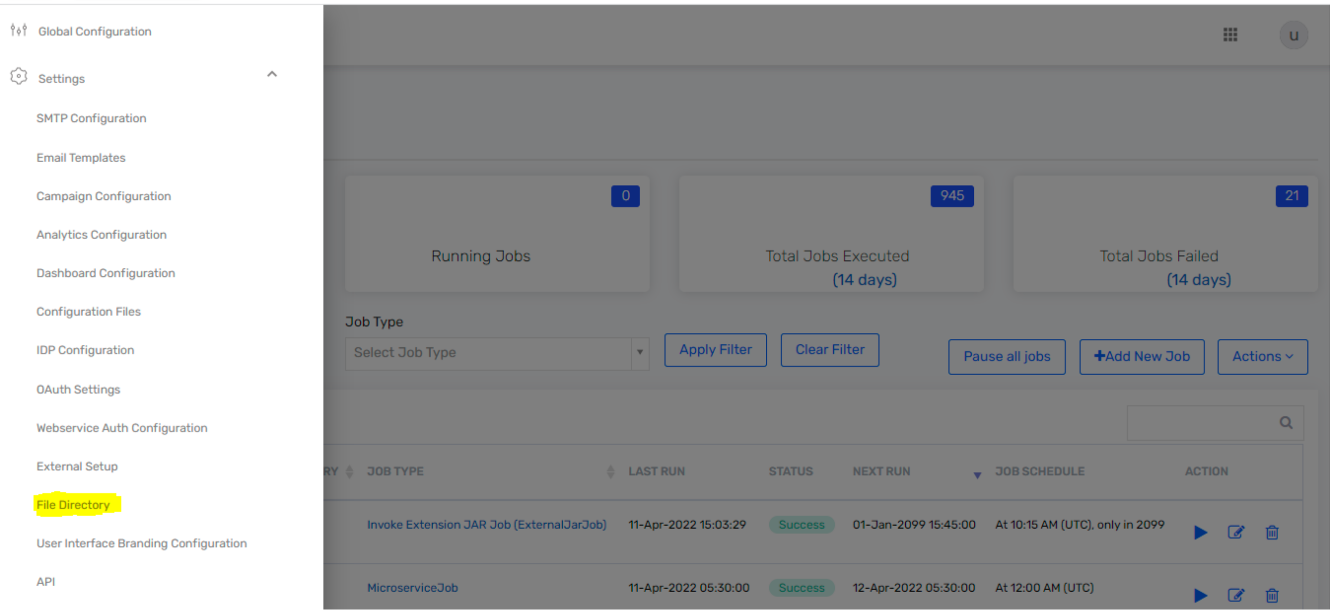
1. Procure the .pem file from the customer team
2. Save the file on local system as .csv file
3. Login to EIC as an admin user with required privileges
4. Go to admin page


SAVIYNT
Home
u
Hi admin
You are logged in as : admin
My Pending Access
0
Pending Approvals
0
Password expires in (days)
P
Request New Access
Request for new access and / or modify existing access
Request History
View all requests raised by you for yourself or others
Pending Approvals
Approve, reject or redirect requests from others
Rec
Home
SOD
Certifications
Intelligence
Control Center
Admin
Design
Help Guide

Request Home is the starting point of your experience.

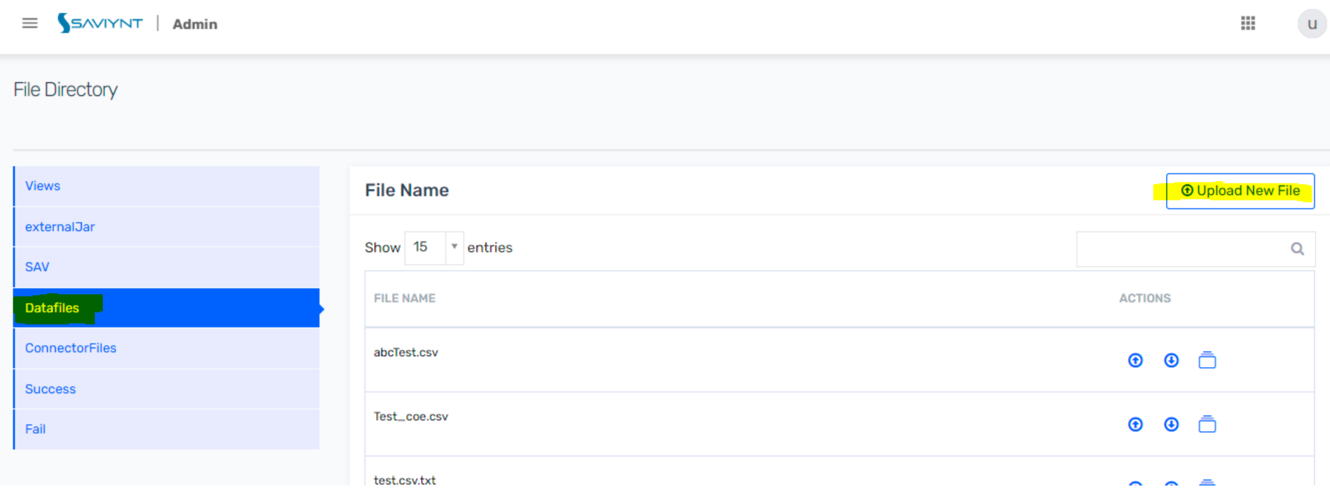
From this page you can initiate requests to new applications and roles, manage your access, and review recent activity and pending actions.

5. Go to Settings and File Directory



RY	JOB TYPE	LAST RUN	STATUS	NEXT RUN	JOB SCHEDULE	ACTION
	Invoke Extension JAR Job (ExternalJarJob)	11-Apr-2022 15:03:29	Success	01-Jan-2099 15:45:00	At 10:15 AM (UTC), only in 2099	
	MicroserviceJob	11-Apr-2022 05:30:00	Success	12-Apr-2022 05:30:00	At 12:00 AM (UTC)	

6. Click on the Datafile section and click on the Upload New File button to upload the file



FILE NAME	ACTIONS
abcTest.csv	
Test_coe.csv	
test.csv.txt	

3. Question: How do I download/upload the files from/to multiple directories on SFTP location ?

Answer: Utility supports download/upload the files from/to one directory per execution of the utility. To download files from multiple directories, create multiple connections, security systems, endpoints, and job triggers. Each trigger has to be executed in sequence.

4. Question: Can we both download and upload the files at the same time?

Answer: Utility supports only one action (download or upload) at a time per execution of the utility. You can create separate jobs for download and upload and each job with a property file corresponding to the action you want to perform download / upload and configure those jobs to run in sequence.

Troubleshooting

To troubleshoot common problems with connectors, answer frequently asked questions, and provide solutions to a few common issues you might encounter while configuring or working with connectors, see Common Troubleshooting Guide for Connectors.