

AutomationEdge

User Guide

(Release 7.0.0)

© 2021, AutomationEdge Technologies Inc All rights reserved

Information used in this document is subject to change without notice. Companies, names, and data used in the examples herein are fictitious unless otherwise noted. No part of this document can be reproduced or transmitted in any format, by any means, electronic or mechanical, for any purpose without permission of AutomationEdge Technologies.

Contents

1	Introduction	7
1.1	Users Roles	7
1.2	Users & Access Permissions.....	8
1.3	About This Document	9
2	AutomationEdge Post-Installation tasks	10
3	Getting Started	11
3.1	Login	11
3.2	User Icon	16
4	Home	25
4.1	Introduction	25
4.2	Upload License	25
4.3	Home: Components on home page	38
5	Users	40
5.1	Tenant Users	40
5.2	User Groups	69
5.3	User Groups: Features/Permissions for other users	76
6	Workflows	76
6.1	Publishing Workflows: General Flow	77
6.2	Publish to Development Instance	77
6.3	Setup, Execute Sales Revenue on Development Instance.....	97
6.4	Workflows: Export from Development Instance	108
6.5	Workflows: Import to UAT Instance	110
6.6	Workflows: Export from UAT Instance	115
6.7	Workflows: Import to Production Instance	117
6.8	Workflows: Maintain	124
6.9	Workflows: Features/Permissions for other Users	150
6.10	Workflow Categories	150
6.11	Credentials.....	169
6.12	Workflow Scheduler.....	190

6.13	Scheduler: Transfer Schedules	205
6.14	Scheduler: Features/Permissions for other users	211
7	Agents	212
7.1	Tab: Agents	212
7.2	Agents: Memory Settings	228
7.3	Agents vs. Assisted Agents	228
7.4	Tab: Assisted Agents.....	229
7.5	Tab: Controller Agents.....	239
7.6	Agents: Workflow Assignment.....	257
7.7	Agents: Controller Assignment.....	263
7.8	Agents: IP Whitelisting.....	266
7.9	Agent Settings	267
7.10	Agents: Features/Permissions for other users	269
8	Catalogue	270
8.1	Submit Request	270
8.2	Request details	271
8.3	Catalogue: Features/Permissions for other users	274
8.4	Features to improve efficiency of Requests	274
9	Requests	275
9.1	Viewing Request Details.....	275
9.2	Searching Requests	280
9.3	Download Requests	282
9.4	Requests: Features/Permissions for other users	282
10	Logs.....	283
10.1	Agent Logs.....	283
10.2	Audit Logs.....	295
11	Reports.....	303
11.1	Dashboards	303
11.2	Maintain Reports on Dashboard.....	323
11.3	Out of the box Reports	345
11.4	Custom Reports.....	347

11.5	Datasources (for custom reports).....	347
11.6	Templates (for custom reports)	355
11.7	Email Reports	389
11.8	Reports: Features/Permissions for other users.....	403
12	Plugins	404
12.1	Plugin Steps.....	405
12.2	Plugin Utilization	406
12.3	Plugin Properties Configuration.....	407
13	Purging.....	411
13.1	Purge Policy.....	411
13.2	Purge Schedule	414
13.3	Archived.....	415
14	Process Studio	418
14.1	Process Studio: Download	418
14.2	Process Studio: Assign License	419
14.3	Process Studio Registration	421
14.4	Process Studio Registrations: View	423
14.5	Process Studio Registration: Delete.....	424
15	Integration.....	426
15.1	Integration: Services	426
15.2	Integration: Types	427
15.3	Integration: Type Configuration	427
15.4	Integration Services: Features/Permissions for other users	435
16	File Management	436
16.1	Workflows	436
16.2	Agents.....	441
17	Settings	445
17.1	SMTP.....	445
17.2	LDAP	451
17.3	Tenant Policy.....	454
17.4	Email Notification.....	463

17.5	Proxy Settings.....	478
17.6	Single Sign-On	506
Appendices		523
1	Appendix 1: Integration with Type Remedforce.....	524
1.1	Setup on Remedforce.....	524
1.2	Setup on AutomationEdge.....	526
2	Appendix 2: SSO – Identity Providers	527
2.1	AE initiated SSO with Okta using OAuth/OpenID	527
2.2	Okta(IDP) initiated SSO to AE using OAuth/OpenID	544
2.3	AE initiated SSO with Okta using SAML	561
2.4	Okta(IDP) initiated SSO for AE using SAML	577
2.5	AE initiated SSO with Keycloak using OAuth/OpenID	597
2.6	AE initiated SSO with Keycloak using SAML	610
2.7	AE initiated SSO with ADFS using OAuth/OpenID	629
2.8	AE initiated SSO with ADFS using SAML	639
2.9	Keystore and Certificate Generation	674
Contact		675

1 Introduction

AutomationEdge (version 7.0.0)

AutomationEdge is an automation platform for Digital initiatives in a company. AutomationEdge helps in Robotic business process automation, IT automation, Rapid API integrations, ChatBot Automation etc.

AutomationEdge can help automate activities in different departments including Front office, Middle office, Back office, IT operations, security operations etc. The software robots of AutomationEdge helps relieve humans from repetitive work so that they can focus on work which is fulfilling and which can add value to the organization. AutomationEdge can help in providing hassle free, frictionless, rapid service to internal and external customers of the organization with reduced errors, increased compliance and reduced cost.

1.1 Users Roles

1.1.1 System Administrator

System Administrator is a user who can manage the AE server across tenants. All the global settings, tenant creation etc. are handled by System Administrator.

1.1.2 Tenant Administrator

Tenant Administrator is responsible for maintaining the system for a specific tenant. Tenant Administrator creates user, workflows etc. for the tenant. Tenant Administrator is a super user having all the permissions of Workflow Administrator, User Administrator and Tenant User.

1.1.3 Workflow Administrator

Workflow Administrator is responsible for maintaining all the workflows for a specific tenant.

1.1.4 User Administrator

User Administrator is responsible for maintaining the Tenant Users and User Administrators for a specific tenant. They can also manage the Tenant Policy.

1.1.5 Agent Administrator

Agent Administrator is responsible for controlling or managing agents.

1.1.6 Tenant User

Tenant Users have the lowest level of access to the system. These users can run the workflows and see the results

1.1.7 Activity Monitor

Activity Monitor is responsible for AutomationEdge monitoring. It has access to the following menus, Home (Dashboard view only), Reports, Agent Monitoring (view only) and Requests (view only).

1.2 Users & Access Permissions

The following table is a ready reference to the complete list of permissions for different roles.

Table 1: Users Roles & Access Permissions Summary

Menu options/Features	System Administrator	Tenant Administrator	Workflow Administrator	User Administrator	Agent Administrator	Tenant User ¹	Activity Monitor
Home, Licence Details	-	✓	✓ ²	-	-	-	✓ ³
Add, Edit Tenant	✓	-	-	-	-	-	-
Add, Edit, Search, System User	✓	-	-	-	-	-	-
Add, Edit, Upload Tenant Users	✓	✓	-	✓ ⁴	-	-	-
Add, Edit, Delete User Groups	-	✓	-	✓	-	-	-
Add, Edit, Delete workflows	-	✓	✓	-	-	✓ ⁵	-
Workflows: Scheduler	-	✓	✓	-	-	-	-
Create, Edit, Delete Workflow Categories	-	✓	✓	-	-	-	-
Workflows: Credentials	-	✓	✓	-	-	-	-
Assign permission to Workflows, Categories	-	✓	-	✓	-	-	-
Move Workflows to other Categories	-	✓	✓	-	-	-	-
View, Edit and Execute workflows (if granted permission)	-	✓	✓	-	-	✓	-
Agent Monitoring, Download Agent, Edit, Stop, Restart Agents, Assisted Agents and Controller Agents. Start Agent if Agent controller is enabled. Assign Workflow to Agents	-	✓	-	-	✓	-	✓ ⁶
Agent Settings	✓	✓	-	-	✓	-	-
Working with Catalogue	-	✓	✓	-	-	✓	-
Working with Requests	-	✓	✓	-	-	✓	✓
Download Agent Logs	-	✓	✓	-	-	-	-
Download Audit Logs	✓	✓	-	-	-	-	-
Artifacts	✓	-	-	-	-	-	-
Reports	-	✓ ⁷	✓	-	-	✓	✓
Plugins: View	✓	✓	✓	-	✓	-	-
Plugins: Upload, Assignment	✓	-	-	-	-	-	-
Purge Policy, Schedule	✓	✓	-	-	-	-	-
Purging: Archived	-	✓	-	-	-	-	-

Menu options/Features	System Administrator	Tenant Administrator	Workflow Administrator	User Administrator	Agent Administrator	Tenant User ¹	Activity Monitor
View/Add and Download Process Studio Registrations	-	✓	✓ ⁸	-	-	✓ ⁹	-
Integration: Services, Types and Type Configurations	✓	✓ ¹⁰	-	-	-	-	-
Settings: System Setting Add, Edit Server URL; Security Questions	✓	-	-	-	-	-	-
File Management	✓	✓	-	-	-	-	-
Settings: SMTP, LDAP, Email Notification, Tenant Policy, Proxy Settings, Single Sign-On	✓ ¹¹	✓	-	✓ ¹²	-	-	-

¹ Tenant User can use the AutomationEdge features depending on Read, Edit or Write permissions granted to them on workflows.

² Workflow Administrator can only view the dashboard on Home menu

³ Activity Monitor can only view the dashboard on Home menu.

⁴ User Administrators can add, edit or upload Tenant Users with role 'Tenant User'. They can also manage User Administrators.

⁵ Tenant Users can only View, Edit workflows depending on permissions.

⁶ Activity Monitor can only perform Agent Monitoring

⁷ Tenant Administrators additionally have access to Custom Reports (Datasources and Template) and Email Reports.

⁸ Workflow Administrators and Tenant Users can only view Process Studio Registrations

⁹ Tenant Users can only view their Process Studio Registrations

¹⁰ System Administrator can create Integration Services and Types. Integration menu is visible to a Tenant Administrator if enabled for the Tenant by System Administrator. Tenant Administrator can create a number of Integration Type configurations as set by System Administrator in Allowed Number of configurations. Type configuration is only for Tenant Administrator.

¹¹ System Administrator has options for SMTP and Tenant Policy only.

¹² User Administrators can modify the Tenant Policy.

1.3 About This Document

Guides are available for System Administrator and a combined guide for Tenant Administrator, Workflow Administrator, User Administrator, Agent Administrator, Tenant User and Activity Monitor known as User Guide. This document is a combined guide for Tenant Administrator, Workflow Administrator, User Administrator, Agent Administrator and Tenant User named as User Guide.

In this guide all explanations in all sections are for Tenant Administrator. Tenant Administrator is the super user among Tenant Administrator, Workflow Administrator, User Administrator, Agent

Administrator and Tenant User. At the end of most sections there is a table listing the feature availability to the rest of the users.

2 AutomationEdge Post-Installation tasks

Perform the following AutomationEdge post-installation steps.

- Login as a Tenant Administrator. Refer [Login](#).
- Change your password for security reasons as discussed in section [Change Password](#)

Required steps:

- Upload AutomationEdge License – Refer to section [Upload License](#).
- Assign Process Studio license to one or more Tenant users. – Refer to section [Process Studio: Assign License](#).
- Purging policy and schedule – Refer to section [Purging](#).
- SMTP at Tenant level – Refer to section [SMTP](#).
- At least one Tenant Administrator should have an email assigned – Refer to section [Tenant Users: Add New](#).

Recommended steps:

- Tenant Policy – Refer to section [Tenant Policy](#).
- It is recommended to enable Email Notifications – Refer to section [Email Notification](#)
- Agent Setting – Refer to section [Agents](#).

3 Getting Started

3.1 Login

To log on to the AutomationEdge:

1. Go to the AutomationEdge URL.
2. The login page is displayed. It has two options to Sign In with an AutomationEdge user or Sign In with SSO.

3.1.1 Sign In with AutomatonEdge User

Provide user credentials as seen below,

1. To login with AutomationEdge user, enter the Username and Password (Figure 1). The Password should be alphanumeric. It should be a combination of lowercase letters, uppercase letters, numerals, and special characters. The minimum password length recommended is about 6 characters.
2. Click Sign in.

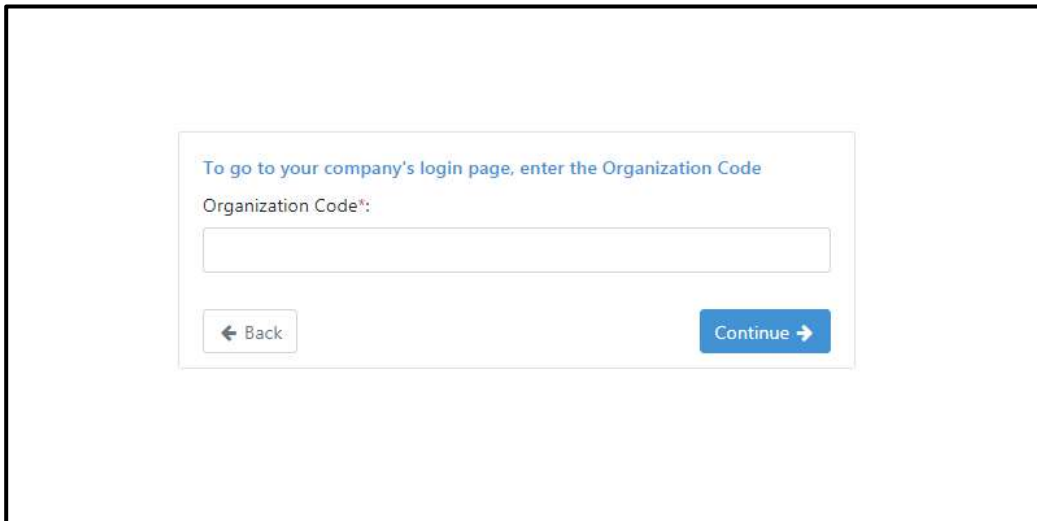


Figure 1a: Login Screen

3.1.2 Sign In with SSO

Following are the steps for Single Sign-On with an AutomationEdge SSO user linked to an Identity Provider user.

1. Click on the Sign In with SSO link below the Sign In button.
2. A screen to enter the Organization Code appears. Every Organization/Tenant can have one unique AutomationEdge SSO user linked to a particular Identity Provider user.

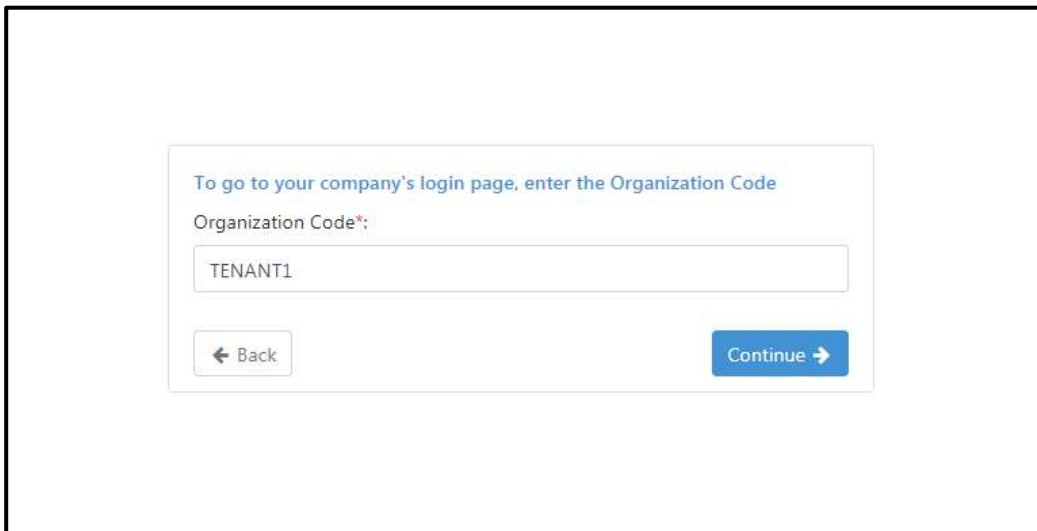


The screenshot shows a web form with the following elements:

- Header text: "To go to your company's login page, enter the Organization Code"
- Label: "Organization Code*:"
- Input field: An empty text box for entering the Organization Code.
- Buttons: A "Back" button with a left arrow and a "Continue" button with a right arrow.

Figure 1b: Provide Organization code for SSO user

3. Provide the Organization Code (Tenant) of the AutomationEdge SSO user.
4. Click Continue.



The screenshot shows the same web form as Figure 1b, but with the following changes:

- Input field: The text "TENANT1" is entered into the Organization Code field.
- Buttons: The "Back" and "Continue" buttons remain visible.

Figure 1c: Organization code/Tenant

5. In case you provide an invalid organization code it gives an error: Single Sign-On is not configured for this client.

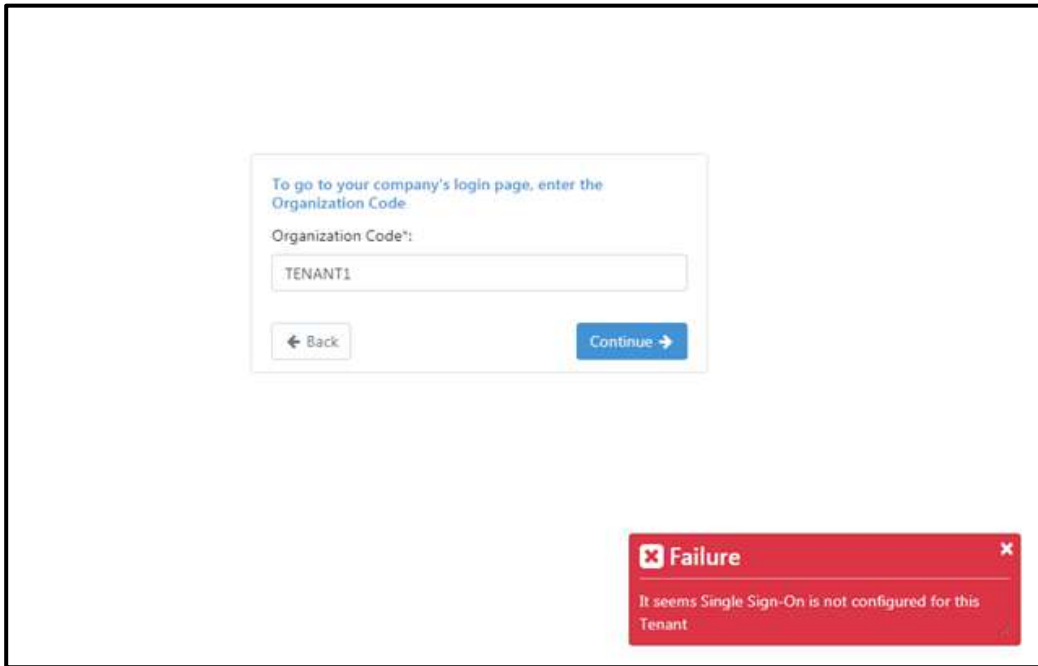


Figure 1d: No SSO user in the Organization code

6. Provide a valid Organization/Tenant Code that has SSO user configured for the desired Identity Provider user.

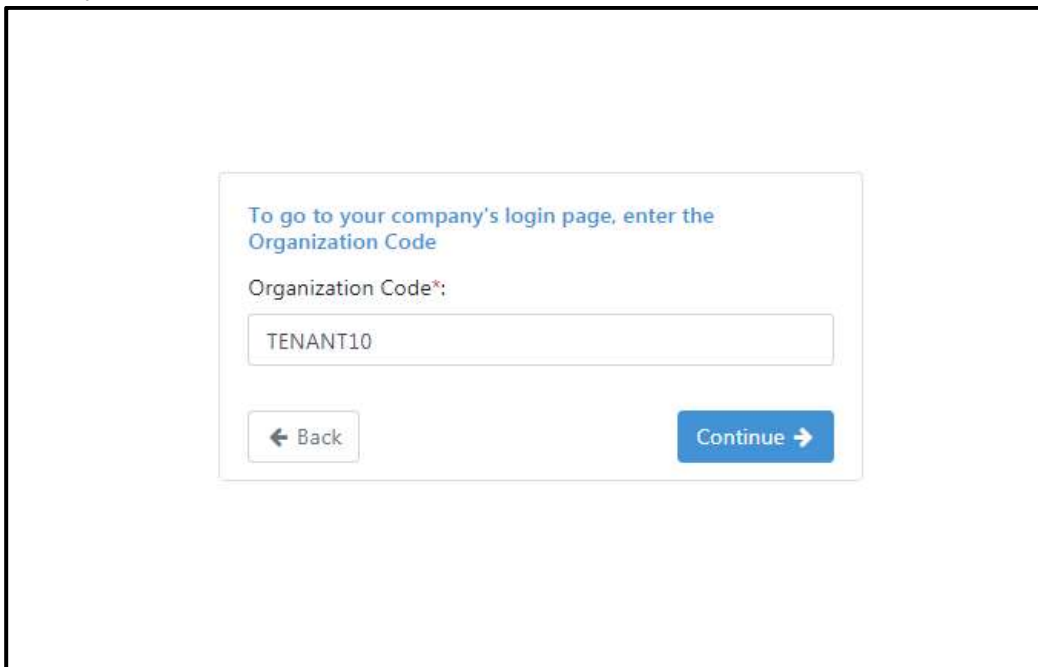


Figure 1e: Valid Organization code with SSO user

7. The Identity Provider login page appears. The Identity Provider login displayed depends on the configurations under Settings→Single Sign-On done by the Tenant.

8. In this case Okta Identity Provider login page is displayed. AutomationEdge also supports SSO with other Identity Providers like Keycloak and ADFS.

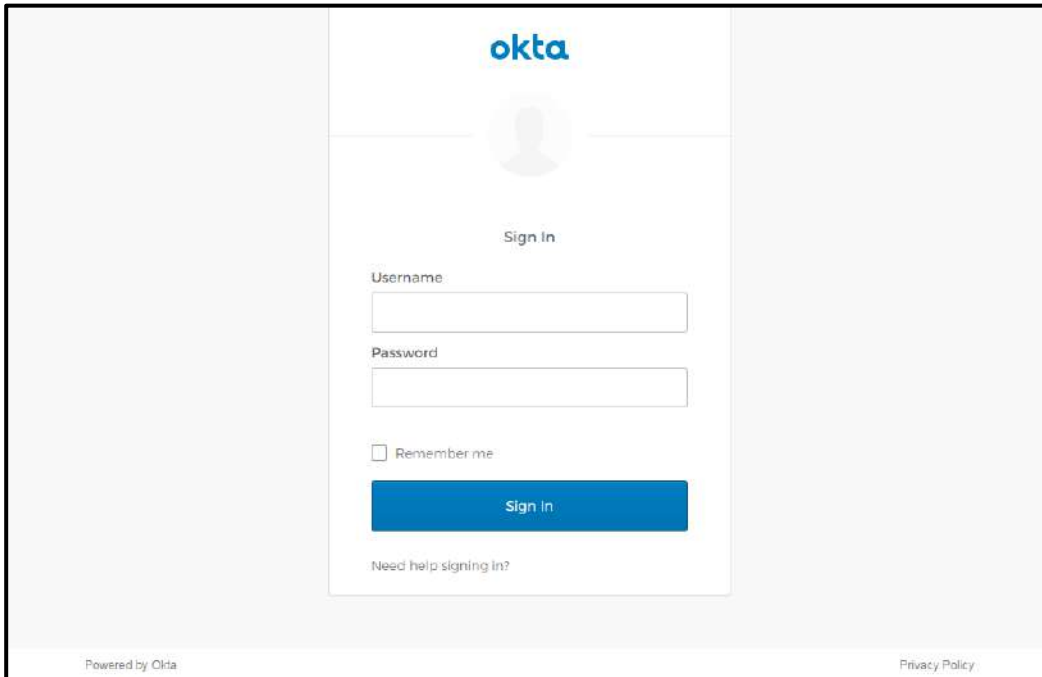


Figure 1f: Identity Provider Login

9. Provide an Okta Username and Password linked to the AutomationEdge SSO user. Click Sign In.

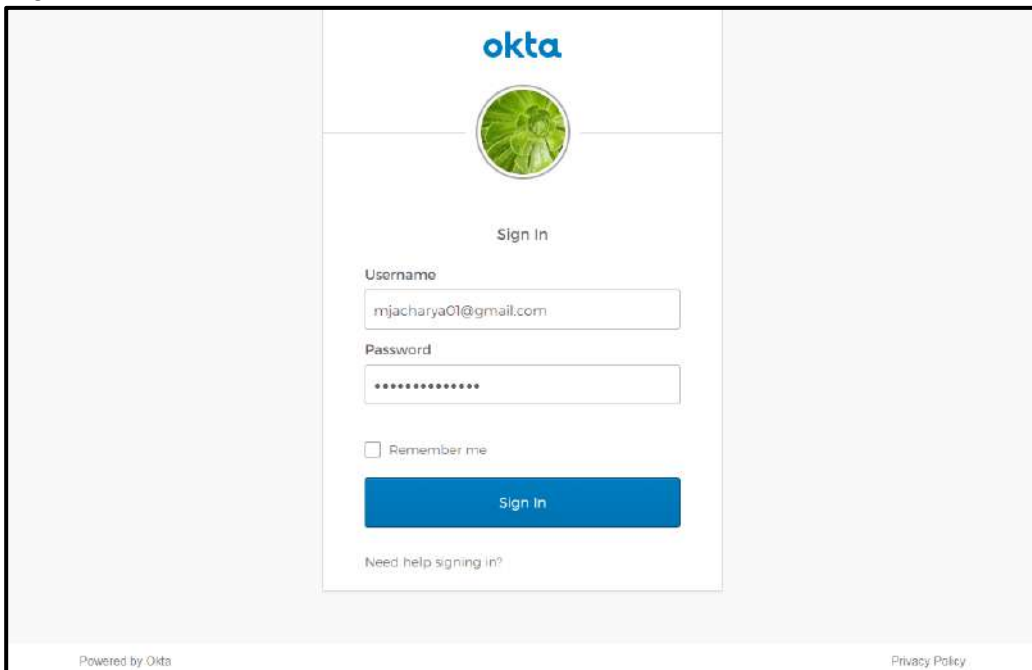


Figure 1g: Identity Provider Login Credentials

10. You are automatically taken to the AutomationEdge home Page. You are logged in with the AutomationEdge SSO user configured with this Identity Provider user while creating AutomationEdge SSO user.

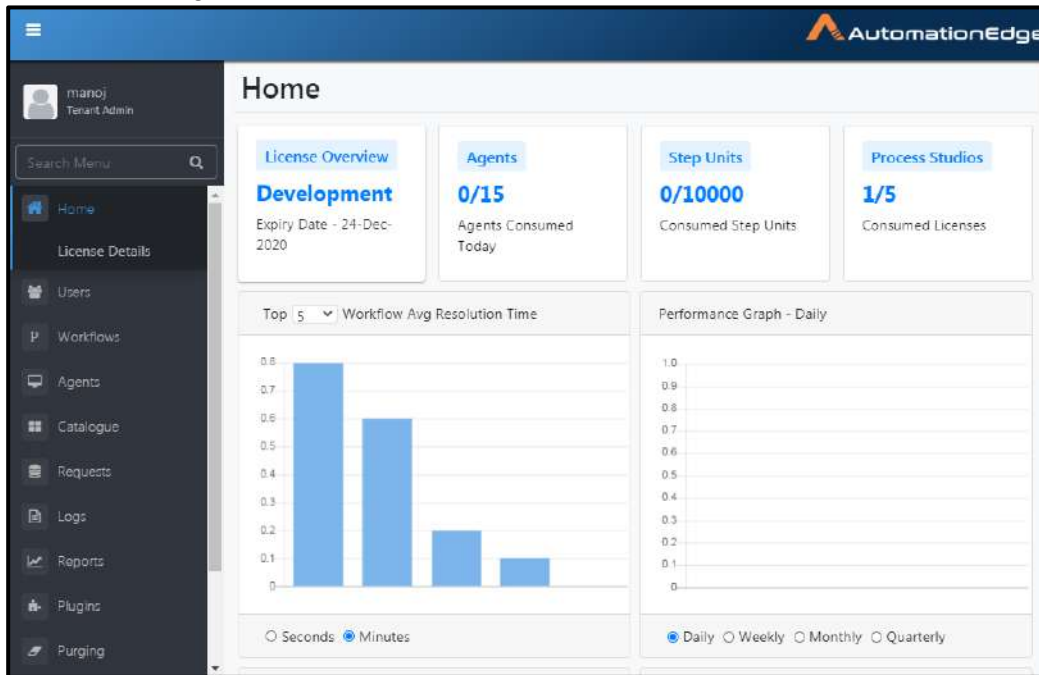


Figure 1h: successful Login of SSO user

11. This completes the Service Provider (in this case AutomationEdge) initiated flow of Sign In with Single Sign-On.

3.1.3 Concurrent Login

AutomationEdge users can log in concurrently and have multiple active sessions. However, some organizations/tenants may want to prevent concurrent login of users. Hence, concurrent login of user feature is configurable. Refer 'AutomationEdge Installation Guide' on how to configure Concurrent Login options. Following are the possible options,

- Multiple Sessions Allowed**
 This is the default option. With this option, users can login concurrently and can have multiple active sessions at the same time.
- Disallow New Session**
 With this option, a second user login is not allowed if the user's session is already in progress. If the user's session is active and he tries to login again then an error message is displayed to the user.
- Invalidate Old Session**
 With this option, if a user already has an active session and tries to login again then the user's old active session is logged out. The user's new login will be successful and a new session will be created.

3.2 User Icon

A user icon along with username is visible on the bottom left corner of the expanded menu. On clicking the user icon, you can view the last login time as well as others options as seen in the screenshot below and listed in the sections below.

The screenshot displays the AutomationEdge user interface. On the left, a dark sidebar contains a user profile menu. A red arrow points to the user icon at the top of this menu. The menu items include: Tenant Admin (Tenant Admin), Last Login: 11-Aug-2020 20:40:51, View Profile, About, Change Password, Set Tenant Logo, and Sign Out. Below the menu are navigation options: Requests, Logs, Reports, and Plugins. The main dashboard area shows a 'Home' section with four cards: License Overview (Trial, License Expiring in 57 Days), Agents (0/5 Consumed Today), Step Units (0/1000 Consumed Step Units), and Process Studios (1/5 Consumed Licenses). There are also two performance graphs: 'Workflow Avg Resolution Time' (bar chart) and 'Performance Graph - Weekly' (bar chart).

Figure 2a: User Icon

3.2.1 View Profile

On clicking View Profile, you can see user details as seen below.

The screenshot shows a 'User Profile' dialog box with a close button (X) in the top right corner. The dialog contains the following user details:

Name	Tenant Admin
Email Id	tenant.admin@ae.com
Username	tenantadmin
Role	Tenant Admin
Organization Code	TENANT10
Language	English (United States) ▼

At the bottom of the dialog, there are two buttons: 'Save' and 'Cancel'.

Figure 2b: User Profile

3.2.2 About

Clicking About to see the About pop-up. It shows the released version details.

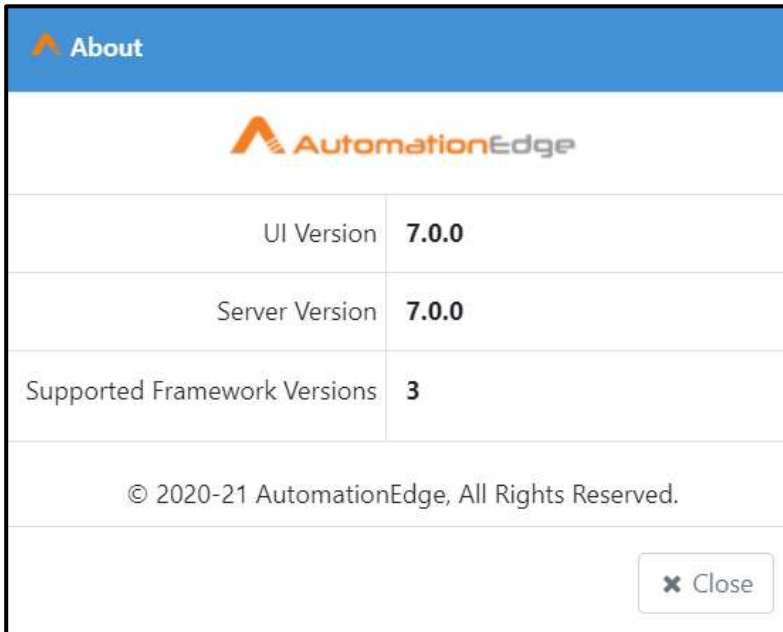


Figure 2c: About AutomationEdge

3.2.3 Change Password

On the first login, the user will be requested to change the password if “Force Change Password” is enabled during user creation or update.

To reset the password:

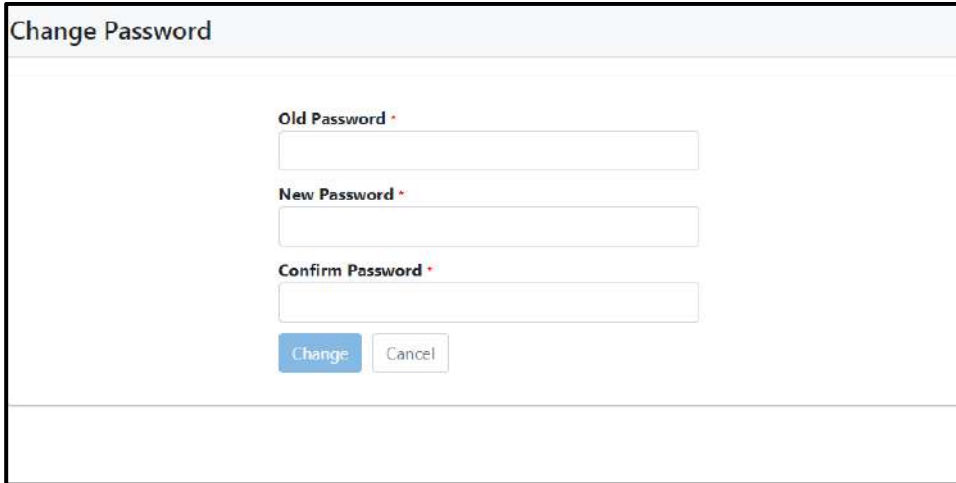
1. Click the User Icon on the bottom left corner of the Home screen (Figure 2a).
2. Select Change Password.



Figure 2d: Changing Password for Tenant Users

(Tenant Administrator, Workflow Administrator, User Administrator Agent Administrator & Tenant User)

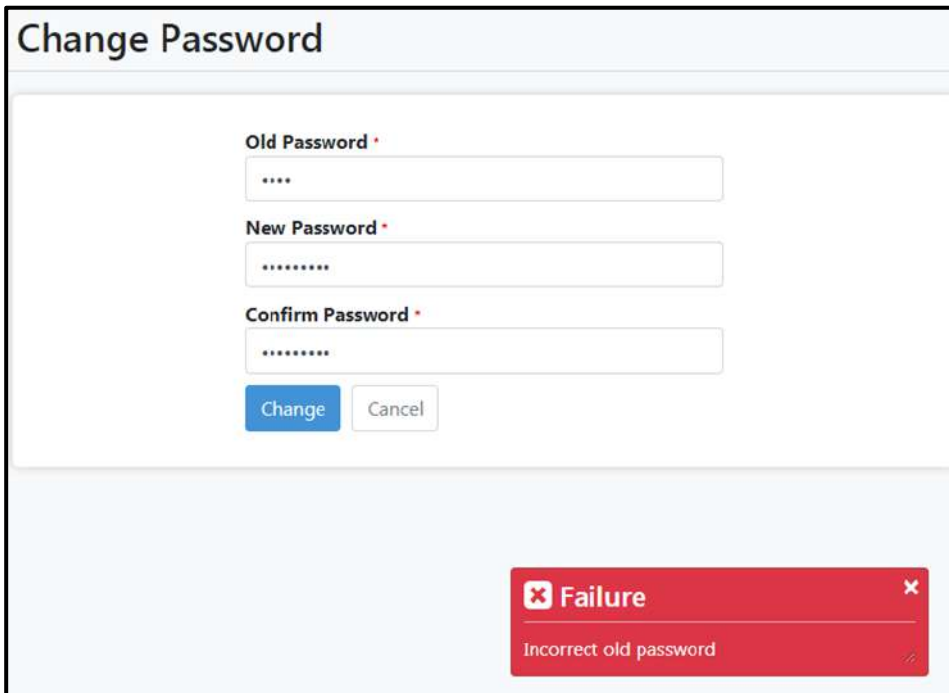
3. Enter the Old Password (Figure 6).
4. Enter the New Password. Re-enter the new password in Confirm Password field.
5. Click change button. Your password will be reset.



The image shows a 'Change Password' form with three input fields: 'Old Password', 'New Password', and 'Confirm Password'. Each field has a red asterisk to its right. Below the fields are two buttons: 'Change' (blue) and 'Cancel' (white with grey border).

Figure 2e: Resetting Password

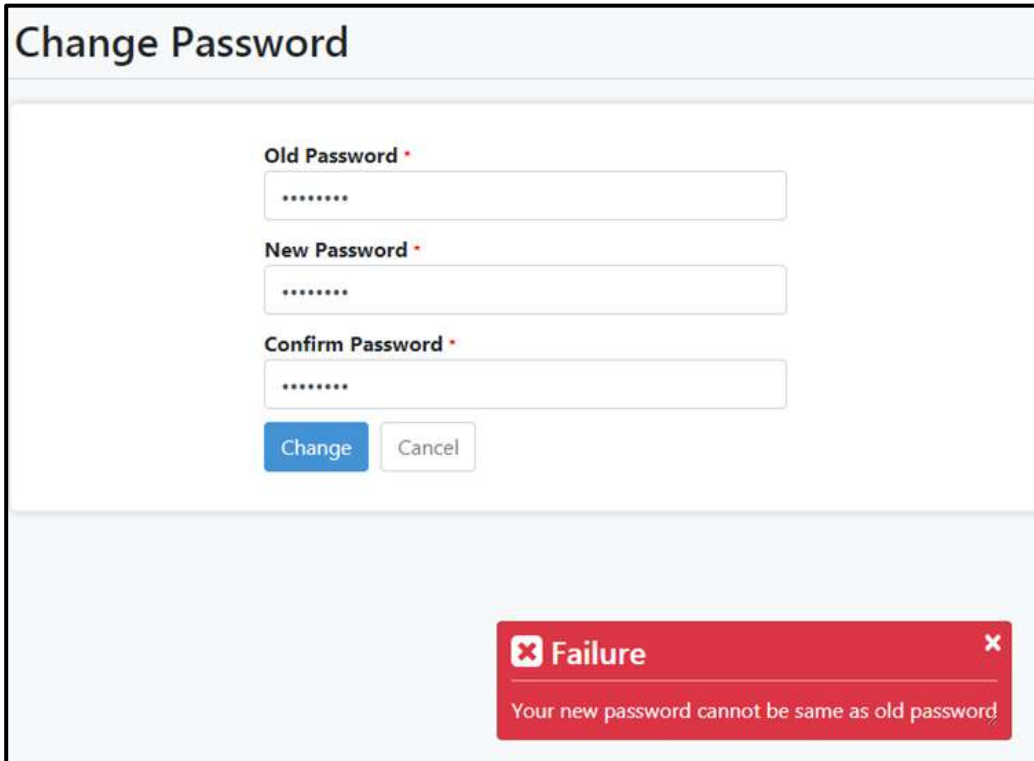
6. Password is updated successfully and you are taken to the home page.
7. In case you provide an incorrect current password you get an Incorrect old password error.



The image shows the same 'Change Password' form as in Figure 2e, but with the 'Old Password' field filled with four asterisks. A red error message box is displayed at the bottom right of the form, containing a white 'x' icon, the word 'Failure', and the text 'Incorrect old password'.

Figure 2f: Incorrect old password

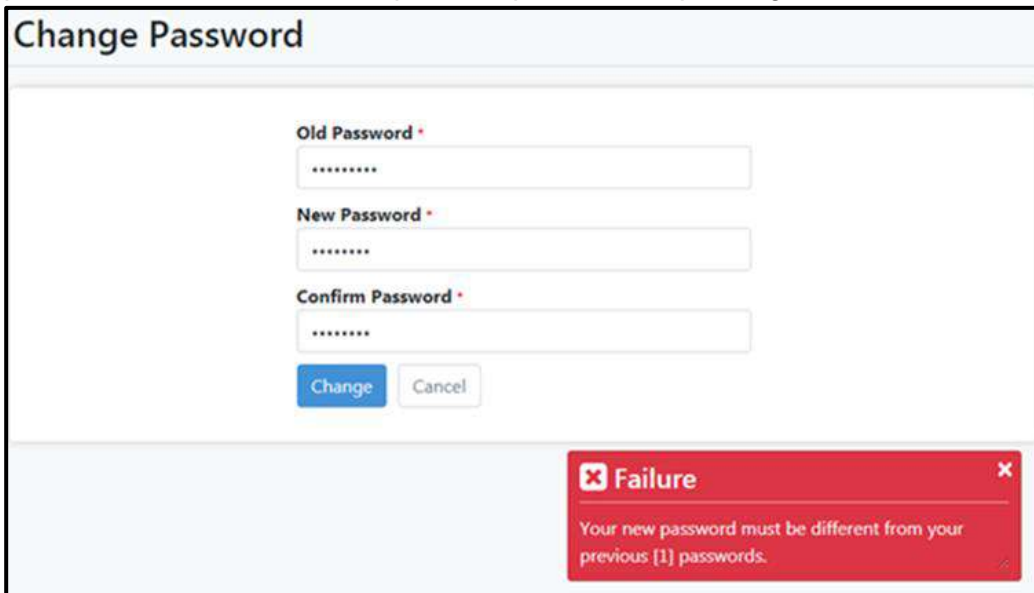
8. In case you provide a password same as your old password you get an error that password cannot be same as old password.



The screenshot shows a 'Change Password' form with three input fields: 'Old Password', 'New Password', and 'Confirm Password'. Each field contains a series of dots representing masked text. Below the fields are two buttons: 'Change' (blue) and 'Cancel' (grey). A red error message box is displayed at the bottom right, containing a close button (X), the word 'Failure', and the text 'Your new password cannot be same as old password!'.

Figure 2g: Password same as old password

9. In case you provide a password same as a previous password it gives an error that password cannot be same as previous password depending on Password Policy.



The screenshot shows a 'Change Password' form with three input fields: 'Old Password', 'New Password', and 'Confirm Password'. Each field contains a series of dots representing masked text. Below the fields are two buttons: 'Change' (blue) and 'Cancel' (grey). A red error message box is displayed at the bottom right, containing a close button (X), the word 'Failure', and the text 'Your new password must be different from your previous [1] passwords.'.

Figure 2h: Password same as previous password

3.2.4 Set Tenant Logo (Branding)

You can have your own branding by setting a logo at the Tenant level. The logo appears on the top left corner on AutomationEdge UI.

Following are the steps to Set Tenant Logo.

1. Click User icon at the top left corner.

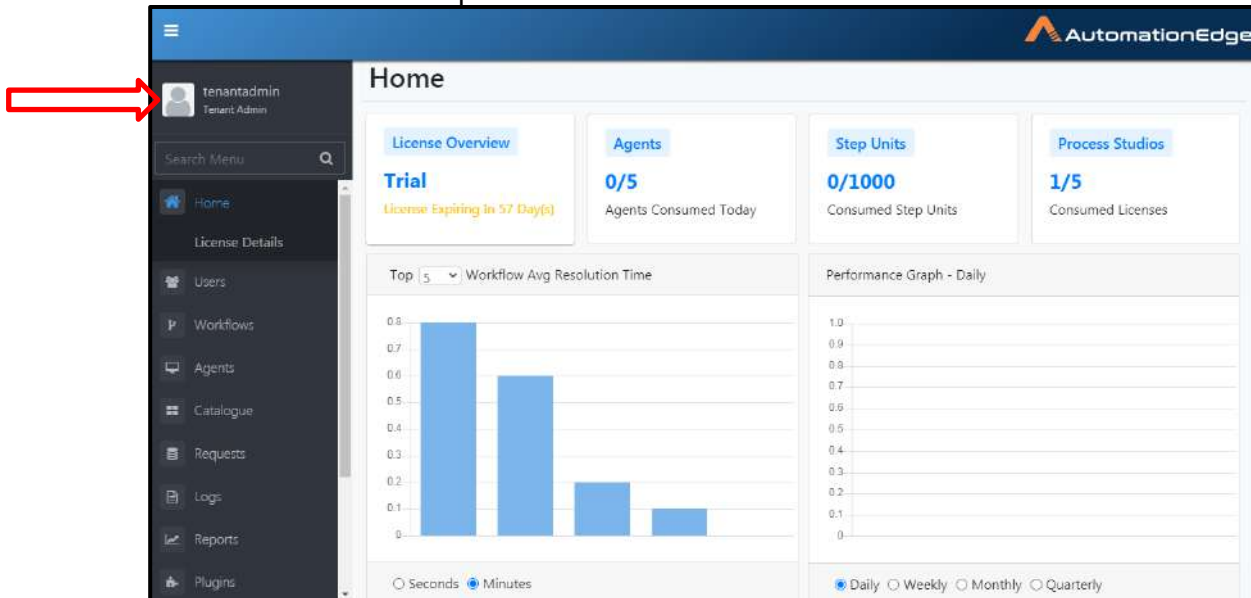


Figure 2i: Click User Icon

2. A pop-up appears. Click Set Tenant Logo from the pop-up.

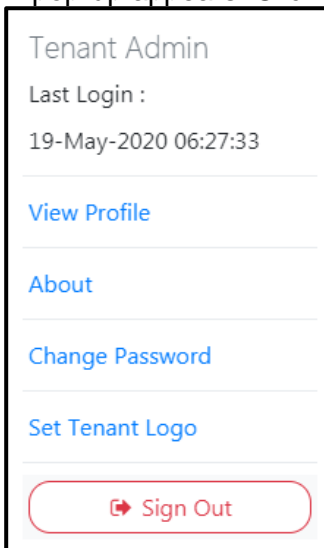


Figure 2j: Setting a Tenant Logo

3. Browse for a logo in .jpg or .png formats.

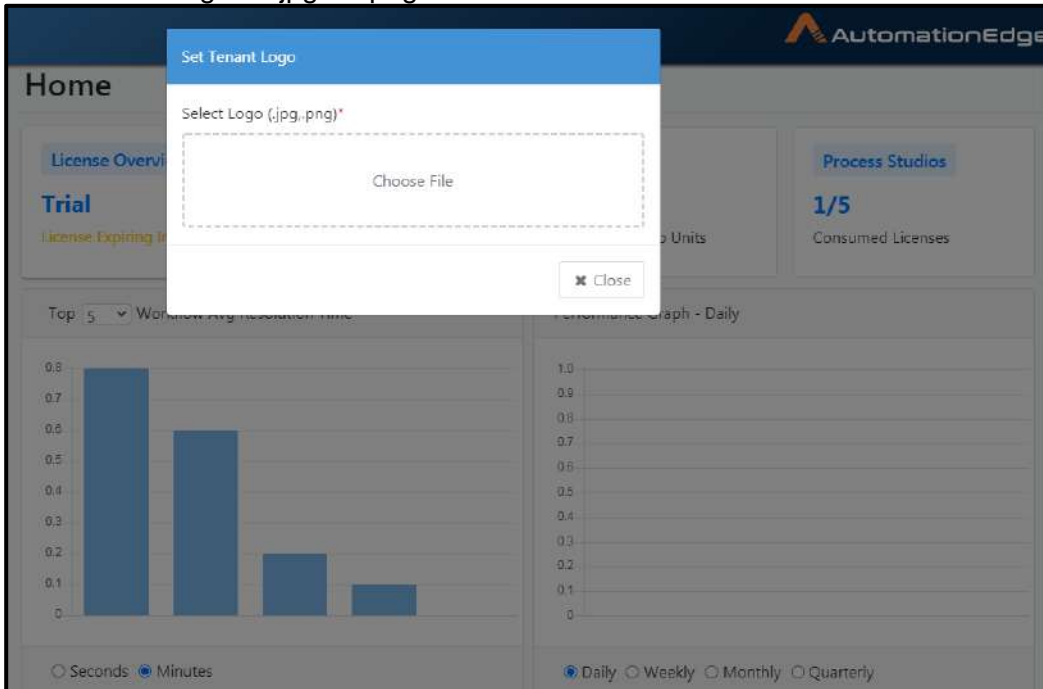


Figure 2k: Choose a logo image file

4. A logo is chosen as shown below. Maximize the coverage area. Click Save.

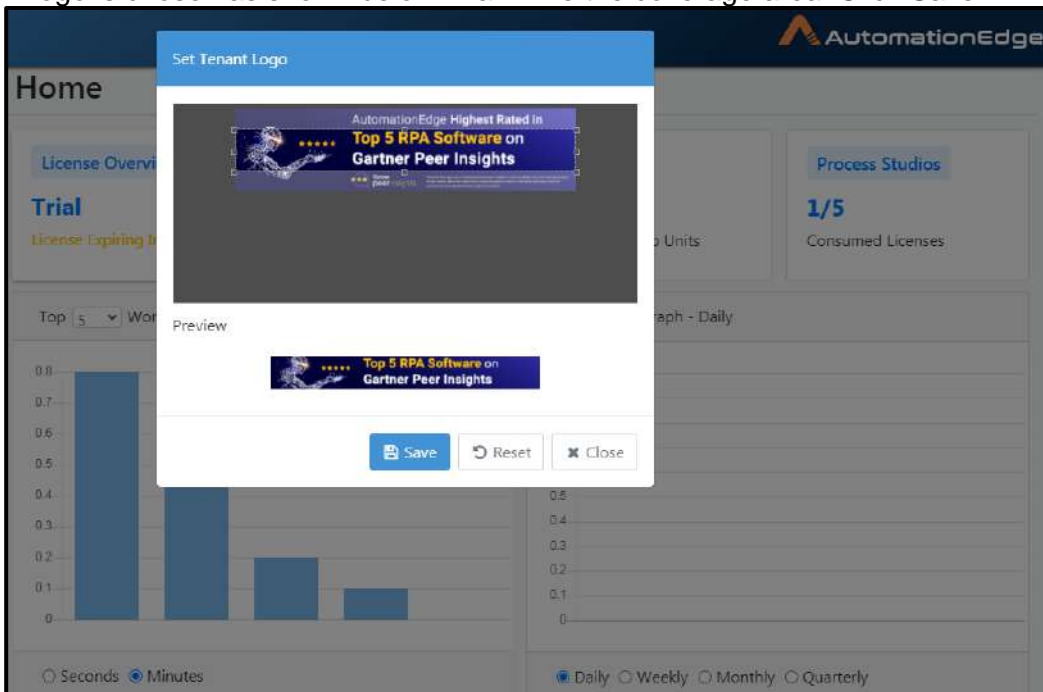


Figure 2l: Save the logo

5. Logo uploaded successfully message is displayed.
6. The newly uploaded logo is visible on the top left corner.

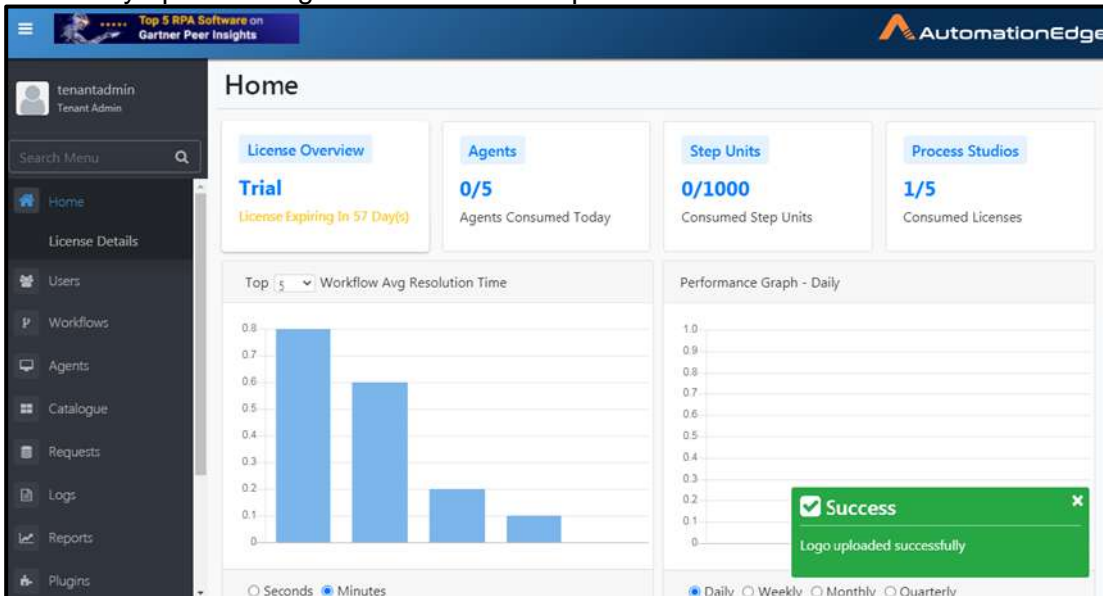


Figure 2m: Logo updated successfully

3.2.5 Remove Tenant Logo

Folowing are the steps to remove Tenant logo,

1. Click on User Icon on the bottom left corner. The pop-up has an additional link Remove Tenant logo.
2. Click on Remove Tenant logo to remove the logo.

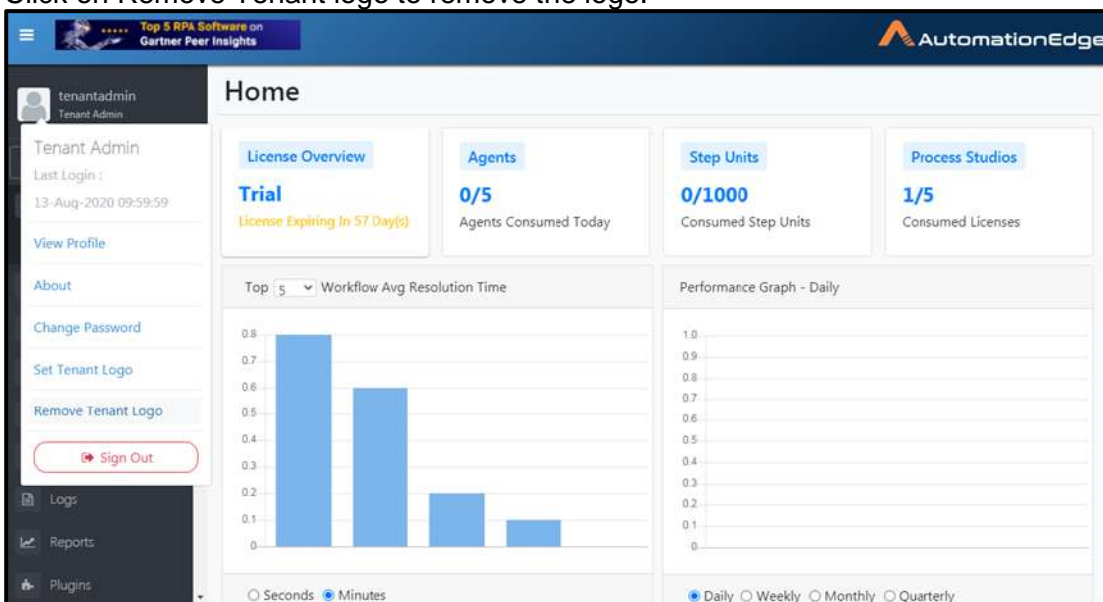


Figure 2n: Remove Tenant logo

- The logo is removed and Logo updated successfully message is displayed.

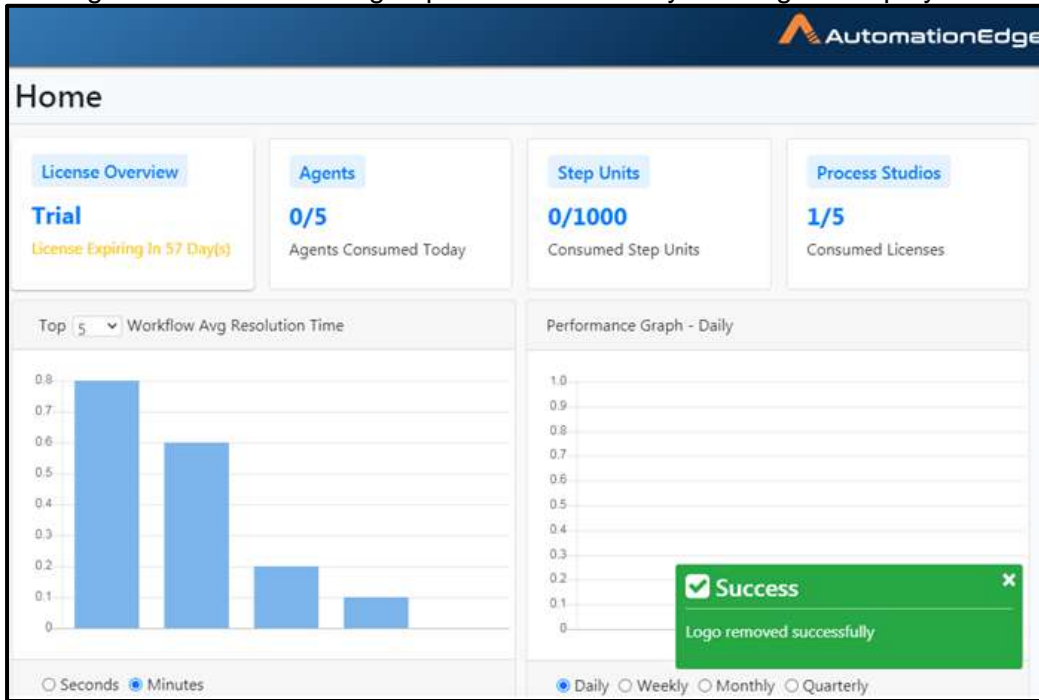


Figure 2o: Logo (removed) uploaded successfully.

3.2.6 Sign Out

To sign out from AutomationEdge user can,

1. Click the user icon on the bottom of the menu.
2. Click Sign Out.

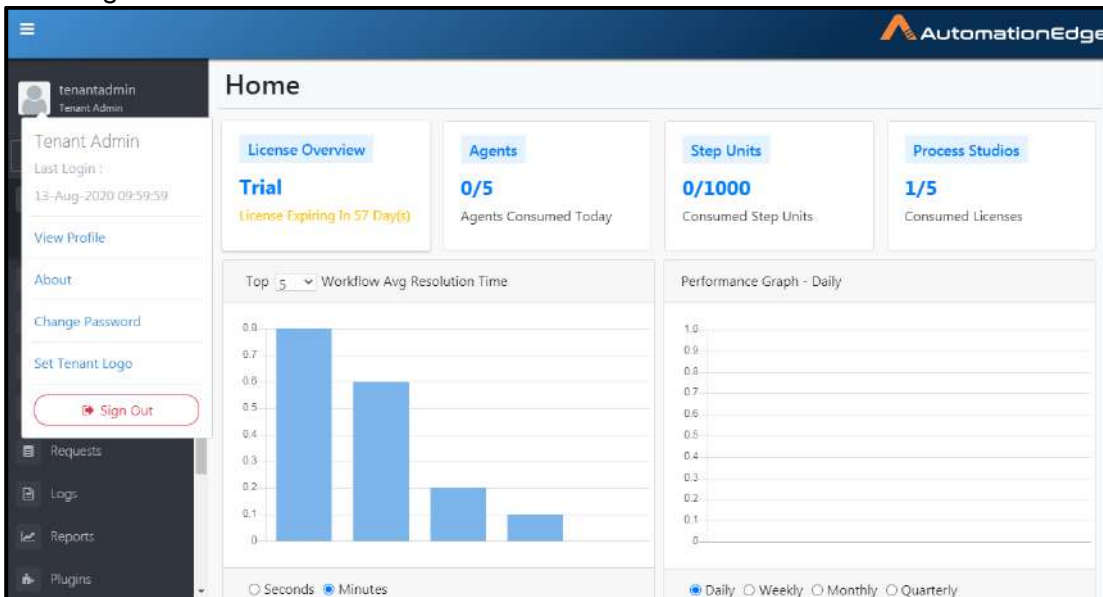


Figure 2p: Sign Out

4 Home

4.1 Introduction

AutomationEdge runs on subscription based licensing. A license authorizes,

1. The total number of Agents/Robots that can be deployed and the breakup for each of the Agent types i.e. Standard, Advanced or Turbo. By default, all Agents are deployed as Standard Agents. The Agent mode can be changed after Agent registration if the license limit permits. Agents can be downgraded to a lower mode such as from Turbo to Advanced or Standard but cannot be upgraded to a higher mode such as from Standard to Advanced or Turbo or Advanced to Turbo without any change in license.
2. The number of workflow/process step units that can be used in active workflows.

4.2 Upload License

After logging on to AutomationEdge for the first time, following screen appears for Tenant Administrator.

The top bar has sections as follows,

1. License Overview: Upload your license and activate your subscription to AutomationEdge. The license status such as expiry date is not set is not visible.
2. Agents Consumed: Currently there are no Agents/Robots consumed or available (0/0) licensed for workflow/process automation.
3. Consumed Step Units: Currently no workflow/process step units are consumed and no step units are available (0/0) or licensed for workflow/process automation.
4. To activate the license, click anywhere over the 'Activate Upload Your License' region.

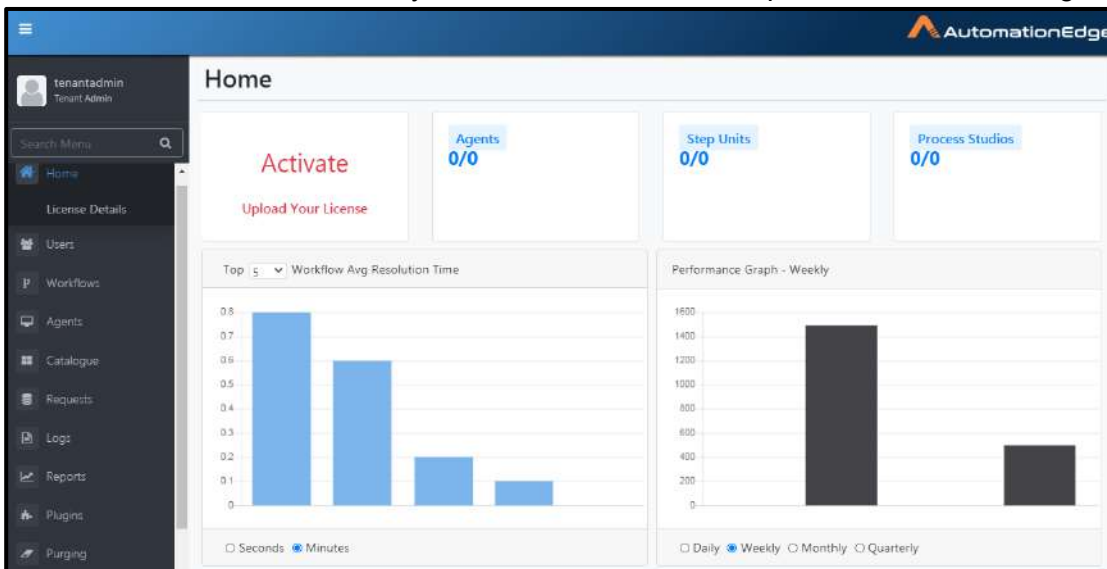


Figure 3a: Home page with License status

- An Upload License pop-up window appears as shown below. Click Choose File.

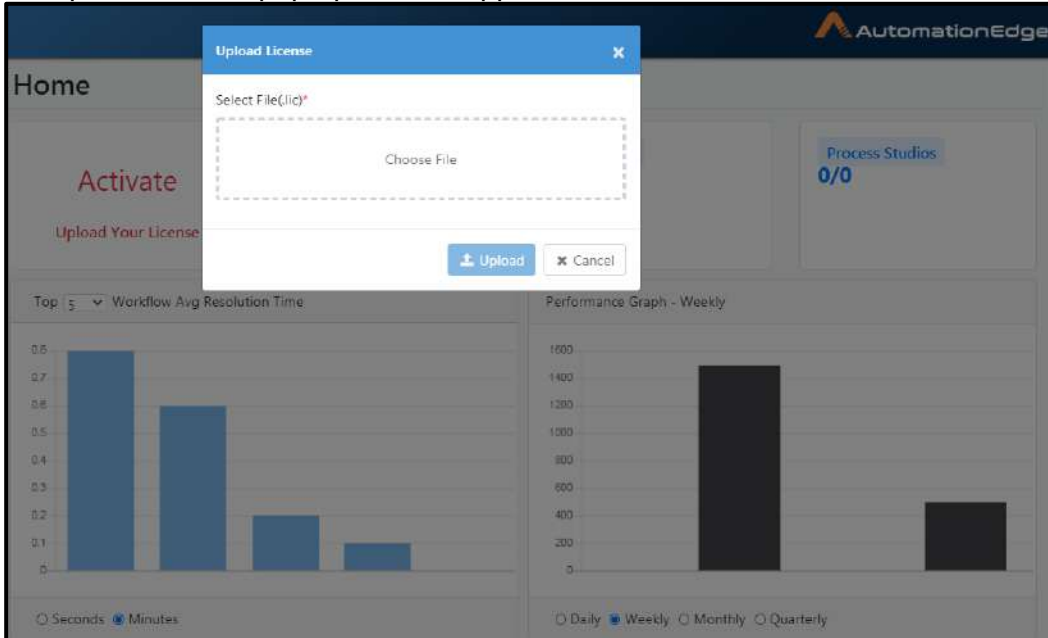


Figure 3b: Choose License file

- Navigate file explorer to choose a license file with extension .lic. Once the license file is chosen as shown below click Upload button.

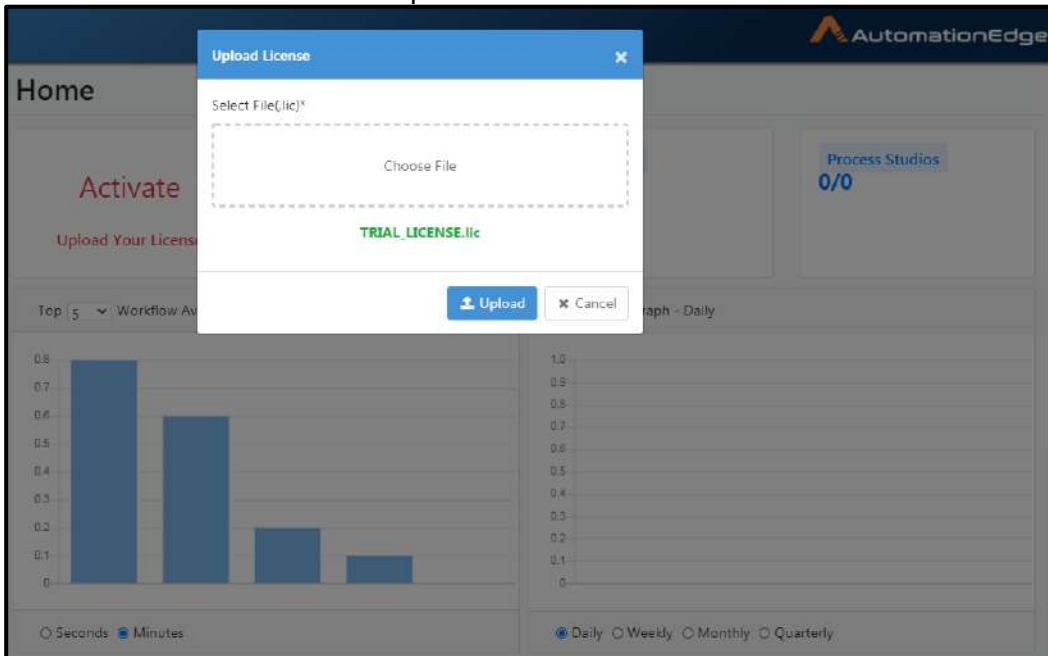


Figure 3c: Search License File to Upload

- The screen now shows license details as per the license file uploaded. Since the license file was a Trial license it shows license type as Trial. It also shows the license expiry date, the number of Agents consumed today (i.e. maximum number of Agents that ran today) and total number of Agents allowed, the consumed step units and total step units available.

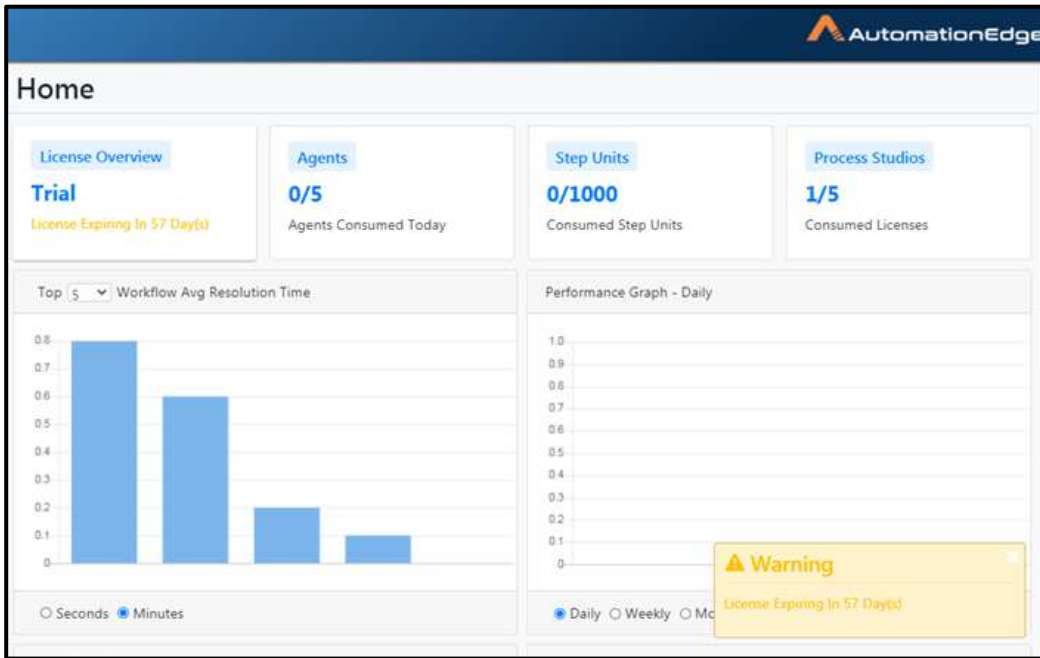


Figure 3d: License uploaded successfully

- Click anywhere on the license overview section to see History table.

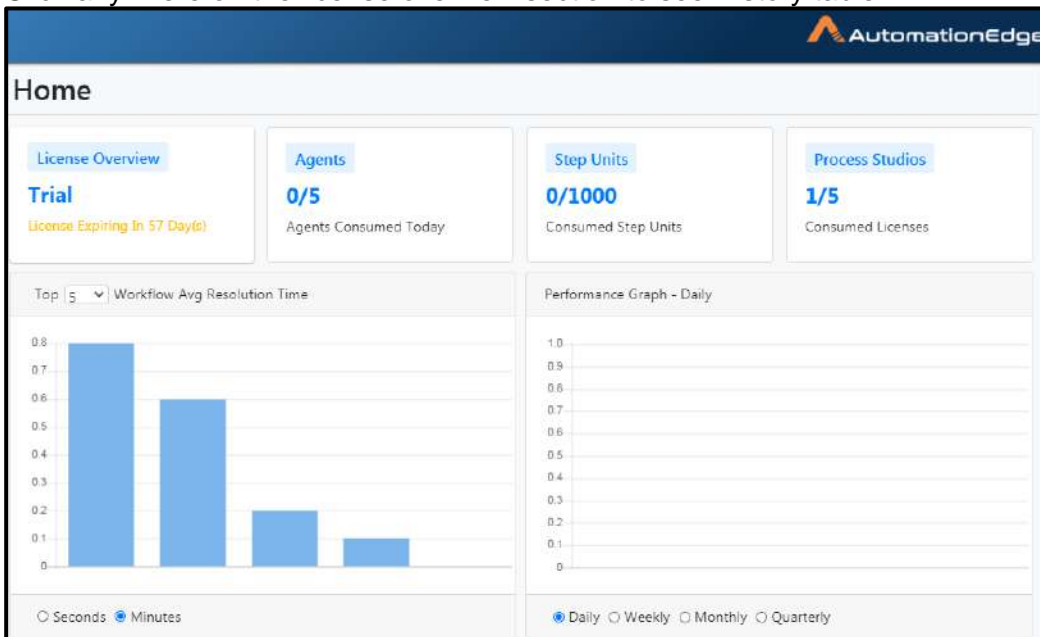


Figure 3e: Home page: License

9. You can see the License Details as below. You may select more columns from the Show columns drop down.

License Type	Process Studios	Standard Agents	Advanced Agents	Turbo Agents	Assisted Agents	Step Units	Grace Period (In Days)	Expiry Date
UAT	5	5	5	5	5	10000	5	23-Dec-2020

Figure 3f: License History

The table below describes each of the possible license options that are available.

Table 2: License Options

AutomationEdge License Options	Description
License Type	AutomationEdge offers the following types licenses, <ul style="list-style-type: none"> • TRIAL • Enterprise • Subscription • UAT • Development Each of the license types are explained in the following sections.
Process Studios	This specifies the maximum number of Process Studios that can be assigned to users and registered.
Standard Agents	This specifies the number of subscribed Standard Agents. Standard Agents execute one workflow at a time.
Advanced Agents	This specifies the number of subscribed Advanced Agents. Advanced Agents can execute one sequential and one non-sequential workflow at a time or two non-sequential workflows at a time. Note: Two instances of a sequential workflow will execute one after the other and not in parallel.
Turbo Agent	This specifies the number of subscribed Turbo Agents. Turbo Agents can execute one sequential and three non-sequential workflows at a time or four non-sequential workflows at a time.
Assisted Agents	This specifies the number of subscribed Assisted Agents. Assisted Agents are personal Agents or Attended Bots and run on the users' machine. Assisted Agents can execute one workflow at a time. For more details on Assisted Agents, refer to section Tab: Assisted Agents
Assisted Agent Working Hours	It is the number of subscribed Assisted Agent Working Hours per day that an assisted Agent can be up or run for.
Step Units	Steps in a plugin have associated step units. When these steps are used in an active workflow in AutomationEdge, each instance of the step consumes associated step units. The total number of consumed steps units of all active workflows deployed on AutomationEdge at any time should not exceed the number of overall Step Units specified in the license.

AutomationEdge License Options	Description
Grace period (In Days)	This shows the Grace period of the license over the expiry date.
Start Date	This shows the Start Date of the license.
Expiry Date	This shows the Expiry Date of the license.

10. Here we uploaded a Trial license. Similarly, other license types can be uploaded. A snapshot of all license types is shown in the sections that follow.

4.2.1 Types of License

4.2.1.1 Trial License

This license type is meant for trial instances. This license has a validity of X (say 60) days from the day it's generated. Trial license does not have any limitation concerning features provided, just that, after X days, workflow execution will cease to function. A new trial license can be requested to renew and extend the trial period or. The default number of total Agents is one and it is of type Standard. By default, number of Advanced or Turbo Agents is zero.

It also shows the license expiry period (in this figure license expiring in 37 days), the number of Agents consumed today (i.e. maximum number of Agents that ran today) and total number of Agents allowed, the consumed step units and total step units available.

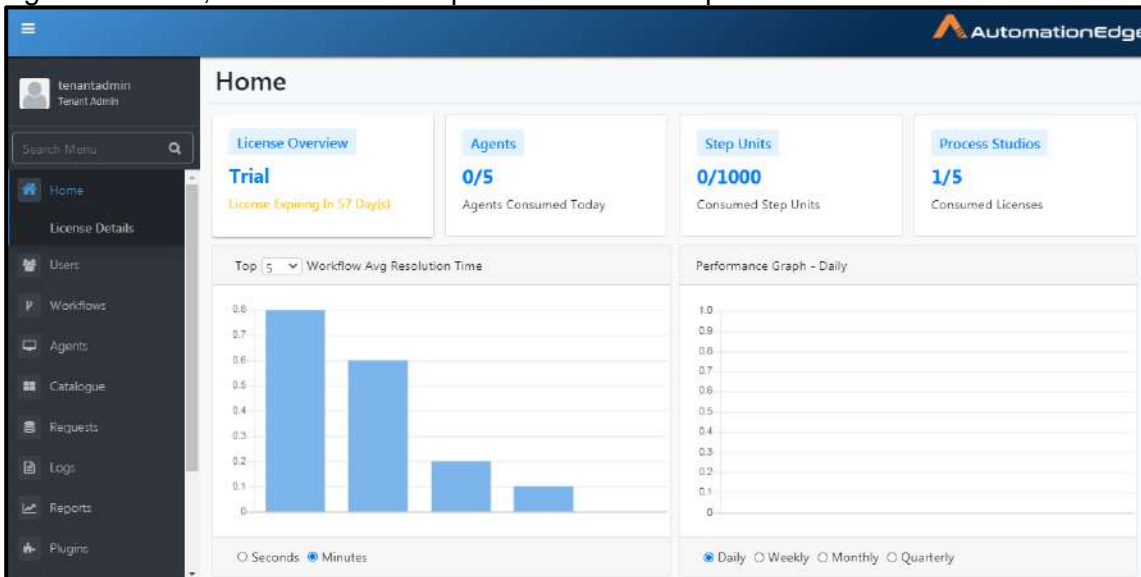


Figure 4a: Trial License

The screenshot shows the 'License Details' page for a license with Customer ID C680518. It includes an 'Update' button and a 'Show Columns' dropdown. The license details are as follows:

License Type	Process Studios	Standard Agents	Advanced Agents	Turbo Agents	Assisted Agents	Step Units	Grace Period (In Days)	Expiry Date
UAT	5	5	5	5	5	10000	5	23-Dec-2020

Figure 4b: Trial License Details

4.2.1.2 Production License

Production license are of two types: Enterprise and Subscription.

4.2.1.2.1 Enterprise

This license type allows a customer to use any number of Agents (this includes any number of Standard, Advanced and Turbo Agents) and Step Units. The license will have expiry date after which (and the grace period) workflows execution will stop.

The following figure shows a valid Enterprise license with expiry date. It also shows unlimited agents and unlimited step units.

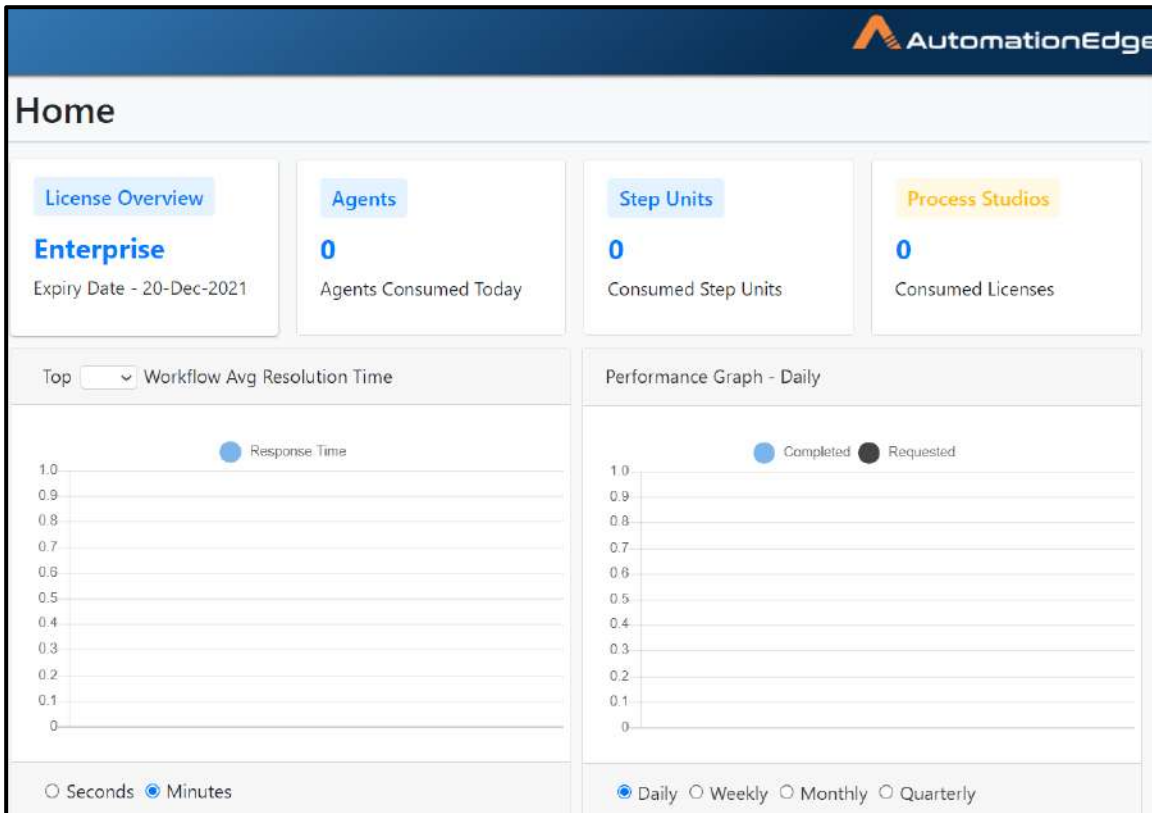


Figure 4c: Enterprise license

The screenshot shows the 'License Details' page for Customer ID: C768560. It includes an 'Update' button and a 'Show Columns' dropdown set to 9. The table below lists the license specifications:

License Type	Process Studios	Standard Agents	Advanced Agents	Turbo Agents	Assisted Agents	Step Units	Grace Period (In Days)	Expiry Date
ENTERPRISE	0	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	1	20-Dec-2021

Figure 4d: Enterprise License Details

4.2.1.2.2 Subscription

This license type allows a customer to use Agents and Step Units subscribed for. The subscription for Agents is broken down by number of Standard, Advanced or Turbo Agents. Customers should renew the license before the expiration date. Customer will not be able to add new workflows/enable workflows or add new agents, if the license limit is reached. After expiry of license and grace period, the workflow execution will stop.

For example, a subscription license may be obtained for a number of days of peak activity. User can spawn the agents above the capacity provided by license for each individual agent's category but within the limit expiry date.

The following figure shows a valid Subscription license with expiry date, the number of Agents consumed today (i.e. maximum number of Agents that ran today) and total number of Agents allowed, the consumed step units and total step units available as well expiry date.

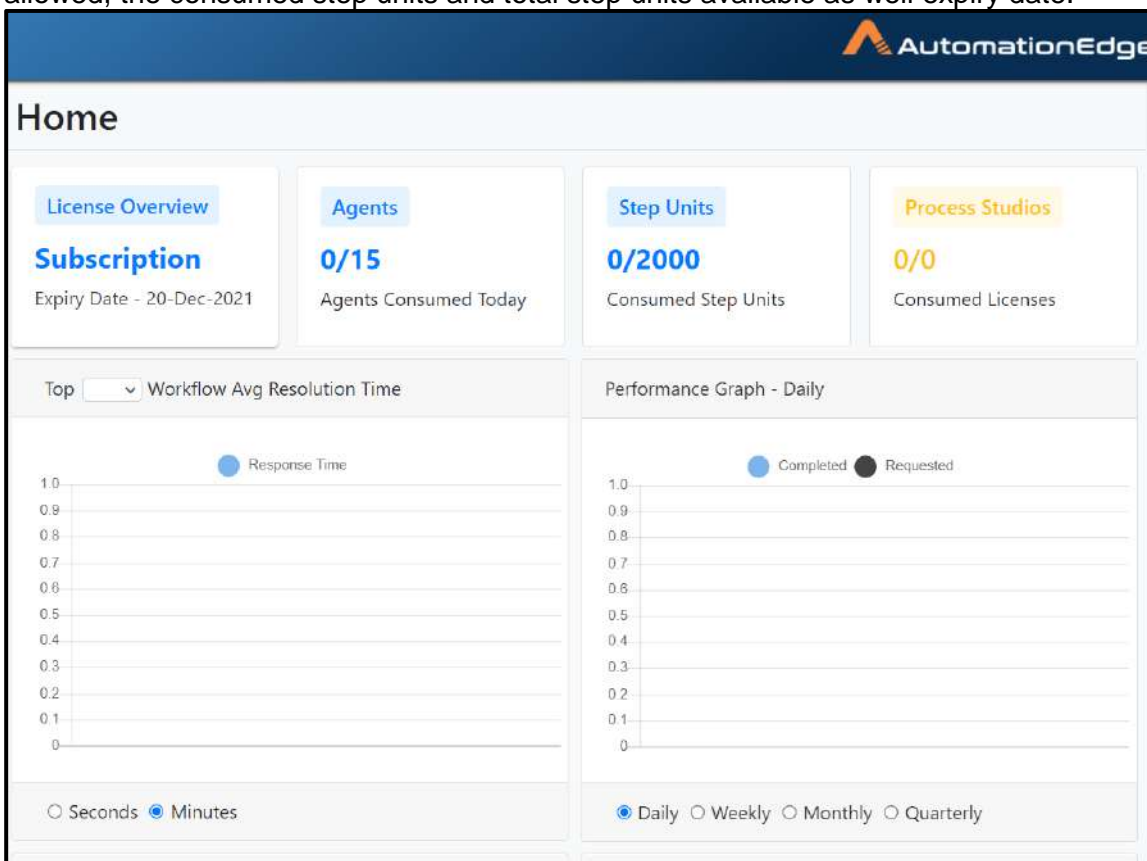


Figure 4e: Subscription license

License Details Update								
Customer ID: C455200							Show Columns: 9	
License Type	Process Studios	Standard Agents	Advanced Agents	Turbo Agents	Assisted Agents	Step Units	Grace Period (In Days)	Expiry Date
SUBSCRIPTION	0	5	5	5	5	2000	1	20-Dec-2021

Figure 4f: Subscription License Details

4.2.1.3 UAT

UAT license has the number of agent(s) as per request. Customer's get this license only if they have purchased either Enterprise or Subscription license. The number of agents is set in the license. If a customer wants more agents in UAT, they have to request for additional agents. The yearly number of Standard, Advanced or Turbo Agents is less than the number of Agents in the corresponding Production license. The license has an expiry date same as the parent Enterprise license after which (and the grace period) the workflow execution stops. The following figure shows a valid UAT license with expiry date, the number of Agents consumed today (i.e. the maximum number of Agents that ran today) and total number of Agents allowed, the consumed step units and total step units available.

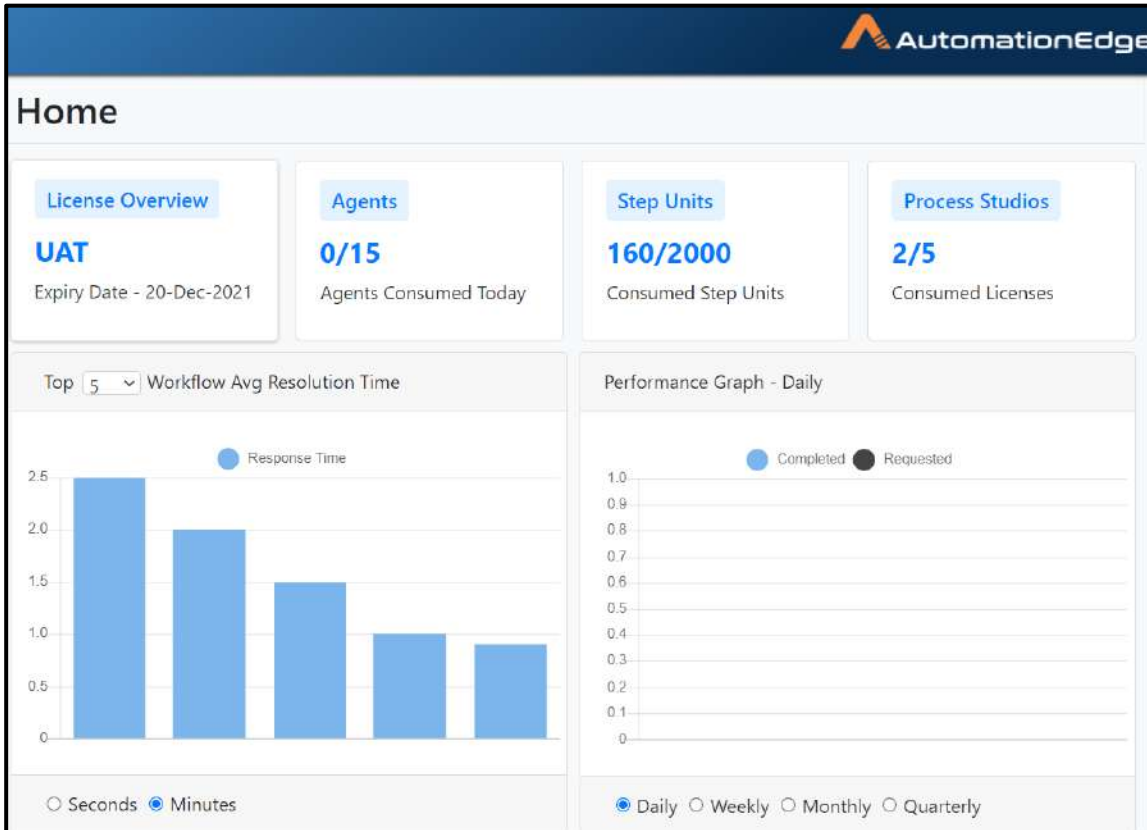


Figure 4g: UAT License

The screenshot shows the 'License Details' page for Customer ID: C768560. The table below lists the license specifications:

License Type	Process Studios	Standard Agents	Advanced Agents	Turbo Agents	Assisted Agents	Step Units	Grace Period (In Days)	Expiry Date
UAT	5	5	5	5	5	2000	1	20-Dec-2021

Figure 4h: UAT License Details

4.2.1.4 Development

Development license is used for development purposes. Process Studio can connect to an AutomationEdge server with development license. It can be used for developing workflows at customer sites. The license has an expiry date same as the parent Production license after which (and the grace period) the workflow execution will stop.

The following figure shows a valid Development license with expiry date, the number of Agents consumed today (i.e. maximum number of Agents that ran today) and total number of Agents allowed, the consumed step units and total step units available.

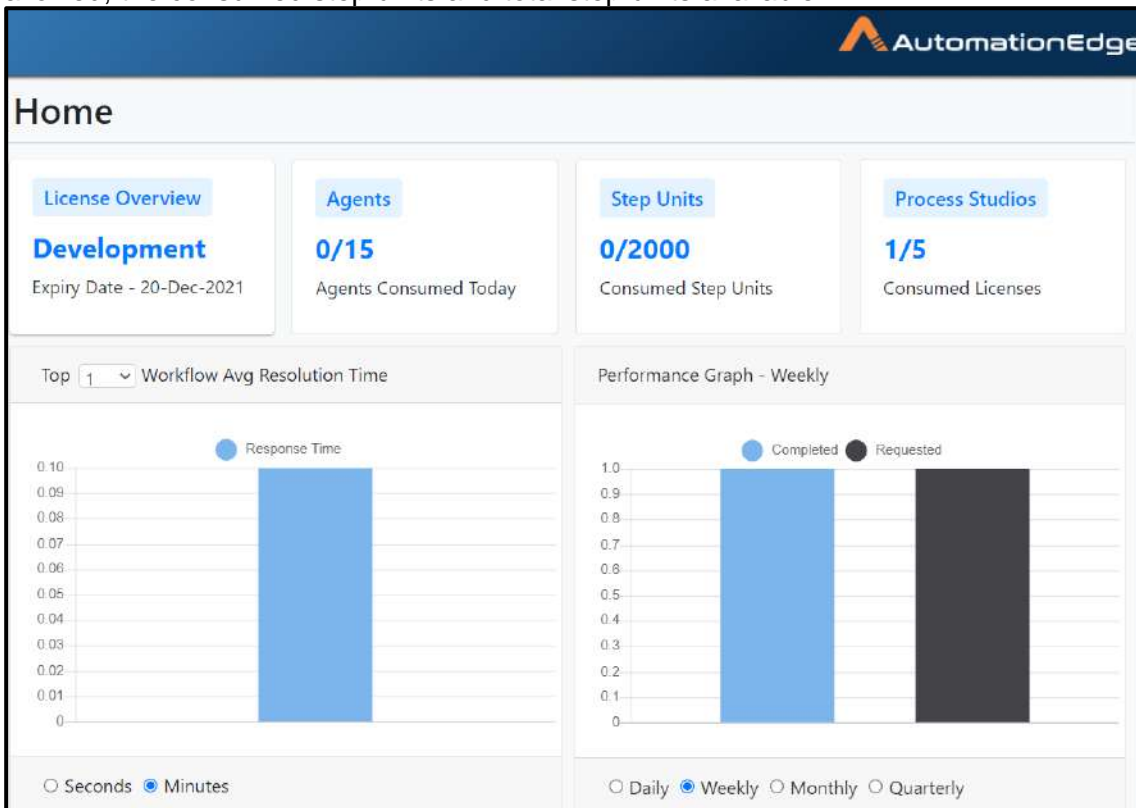


Figure 4i: Development license

The screenshot shows the 'License Details' page in AutomationEdge. It includes a table with the following data:

License Type	Process Studios	Standard Agents	Advanced Agents	Turbo Agents	Assisted Agents	Step Units	Grace Period (In Days)	Expiry Date
DEVELOPMENT	5	5	5	5	5	2000	1	20-Dec-2021

Additional details visible: Customer ID: C768560, Show Columns: 9, and an Update button.

Figure 4j: Development license Details

4.2.1.5 Licensing for Assisted Agents

As the assisted Agents have limited capabilities as compared to unassisted Agents, they do not consume regular Agent's license. AE license has an additional field for counting/regulating number of uses of assisted Agents.

The License of Assisted Agent mentions the number of hours the Assisted Agents can run per day. This number of hours worked can be between 6 and 23 hours.

A user can start or stop any number of times from the first time of start; up to the number of hours it has been licensed. In case an Agent is started very late on a particular it is allowed to spill the working hours to the next day if it is in continuity of an existing session and within the number of licensed hours. Any new start after this is considered as the first start of the next day and the user is again allowed to start or stop Assisted Agent any number of times until the completion of license hours.

Assisted Agents can run one Assisted Workflow at a time.

4.2.1.5.1 Granting Assisted Agents to Users

The License limits the number of Assisted Agents that can be used by a particular Tenant. Tenant Administrator has UI access to allow those many users to download Assisted Agents. At any given time only those many users can download and install Assisted Agents.

4.2.1.5.2 Controlling Assisted Agent Usage

Tenant Administrators can give permissions to users to download Assisted Agents. Depending on number of Assisted Agent licenses, the Tenant Administrator can select those many users for using Assisted Agents.

Following are the steps for a Tenant Administrator to give permission to download and use Assisted Agents,

1. Go to Agents menu. Click Assisted Agents button.
2. Click Assign to Users button on the right.

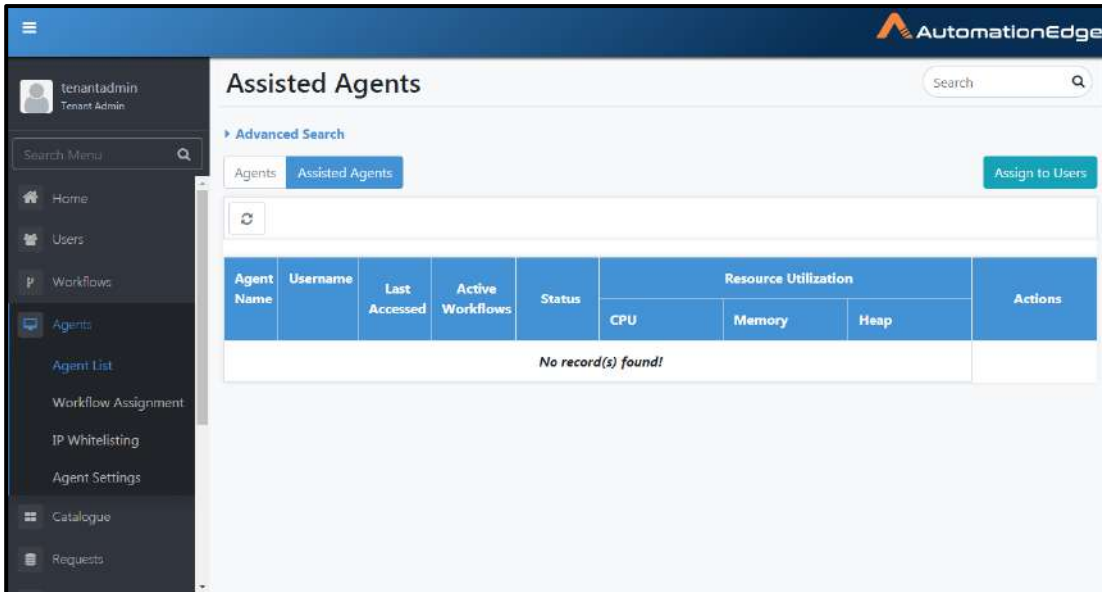


Figure 5a: Assign to Users Button

3. Select the checkbox against the users to be given permission to download Assisted Agents.

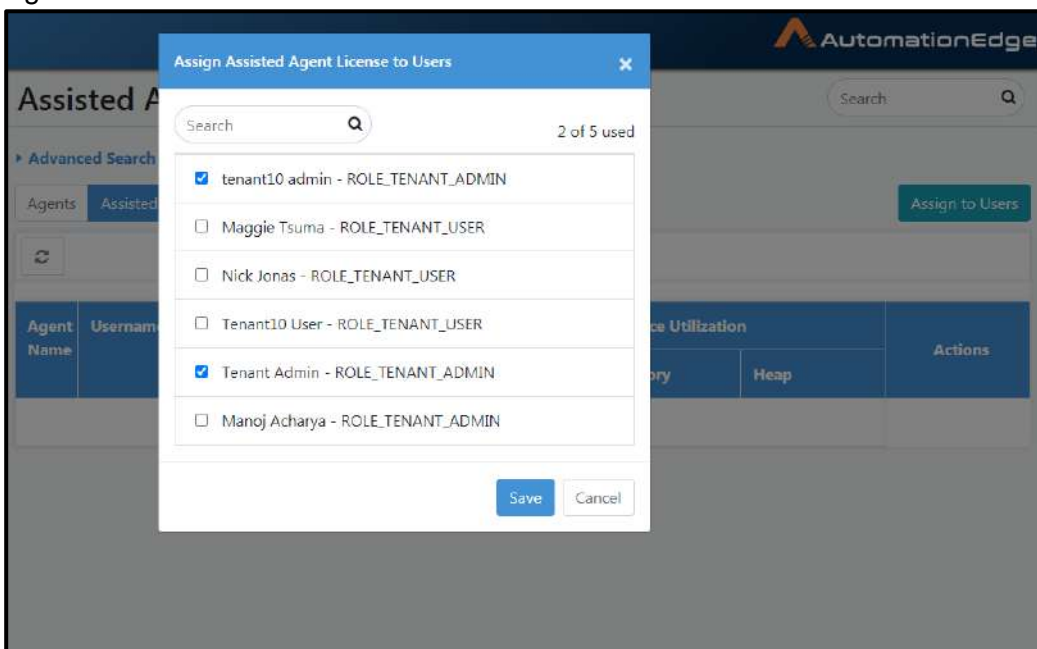


Figure 5b: Assign Assistant Agent to Users

- Assignment is updated successfully and the selected users can now download and use Assisted Agents

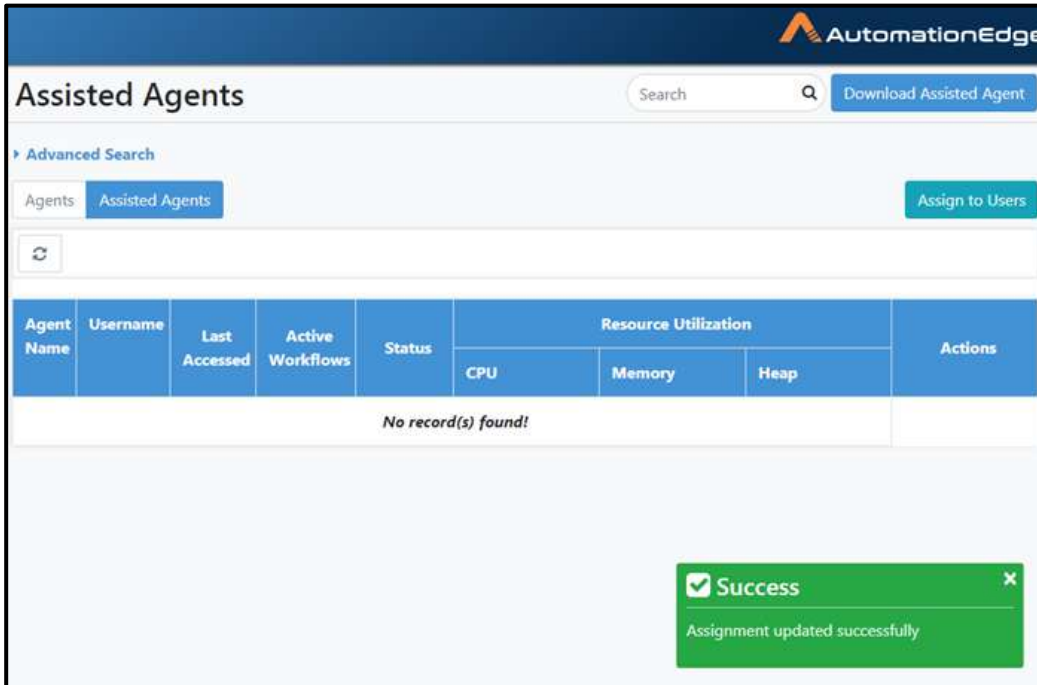


Figure 5c: Agent Assignment to Users successful

4.2.2 License Expiry Notification

Expiry related notifications will be sent to the Tenant Administrator if an SMTP server is configured on AutomationEdge server and an email address is configured for the Tenant Administrator.

Notifications will be sent on the following occasions:

4.2.2.1 Notifications related to License dates

Following are the Notifications related to license dates,

- If the license is about to expire very soon, an email will be sent mentioning the expiry date.
- If the license is expiring today, an email will be sent mentioning, your license is expiring today.
- If license has expired, an email will be sent with a message to renew the license and the expired date.

4.2.2.2 Notifications related to Number of Assisted Agents

Following are the Notifications related number of Assisted Agents,

1. If the license is to be renewed and the renewal license is already uploaded for a near future date, such that the renewed license has less number of Assisted Agents; the Tenant Administrator will get an Email notification about stopping and removing some of the Assisted Agents depending on the new license. Else all the Assisted Agents will be stopped.
2. If the license is renewed with a reduction in Assisted Agent count, the system will check how many assisted agents have been reduced in the renewed license. If number assisted agents in the renewed license are less than assisted agents being currently used, then all the assisted agents are stopped. Tenant Administrator has to reassign the Grant and then Agents can be restarted. Tenant Administrator will get an Email notification in this regard.

4.3 Home: Components on home page

This section discusses the components on AutomationEdge home page. After logging on to AutomationEdge, following screen appears for Tenant Administrator. In this case AutomationEdge Server instance has UAT license.

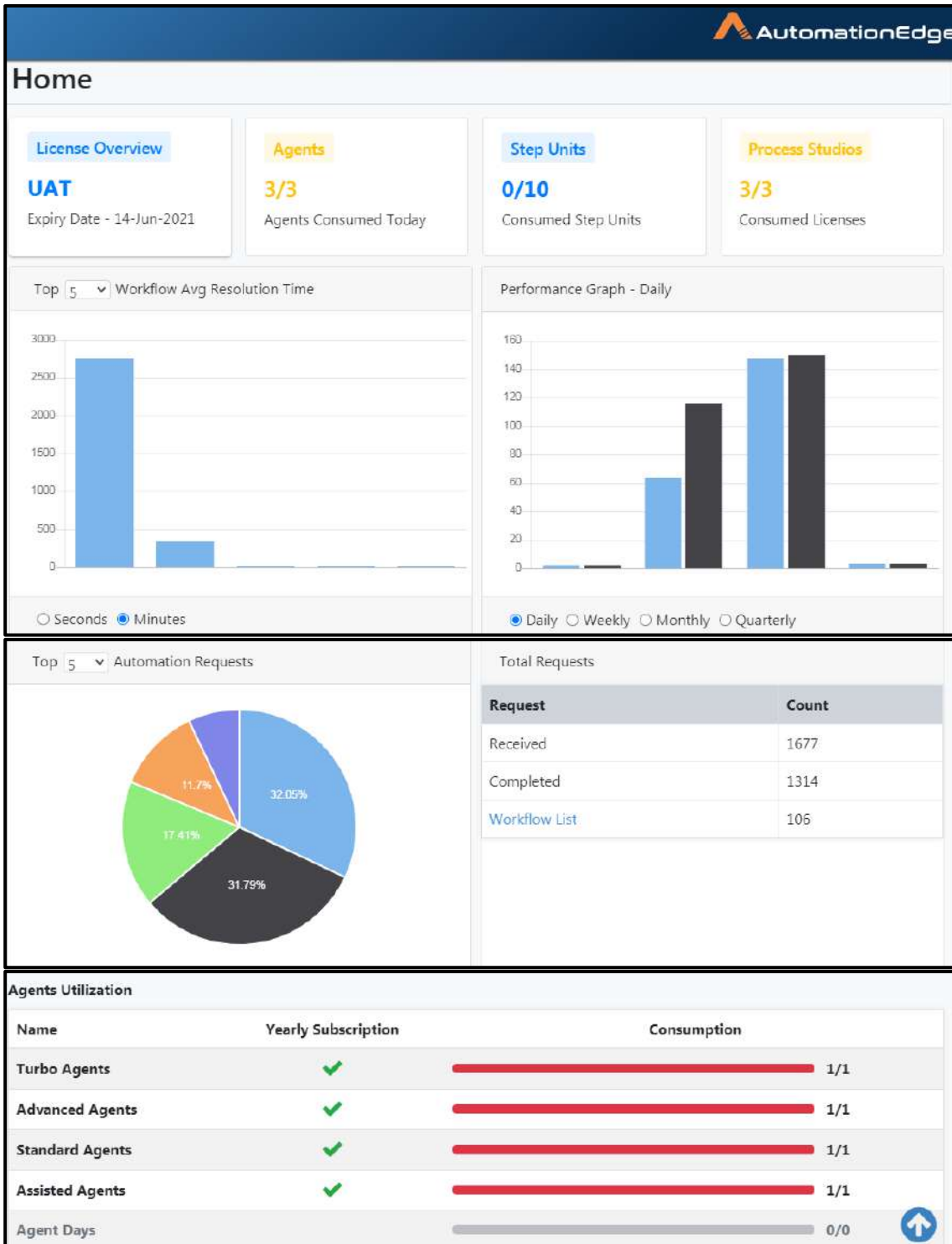


Figure 6: Home Screen for Tenant Administrator

Note: The home page dashboard data is refreshed every five minutes.

Table 3: Tenant Administrator Home Screen Menu

Section	Name	Description
Menu	Home	Displays Organization information, License details, and various charts describing the current status of AE engine. And charts for Agent Utilization by Agent type i.e. Turbo, Advanced and Standard.
	Users	Edit/add tenant users, create user groups, upload users in bulk and you can assign roles to the tenant users and user groups.
	Workflows	Configure, edit, view workflows and create workflow categories, assign permissions to workflow, can view and add new workflow scheduler.
	Agents	Download agent and assign a workflow to agents.
	Catalogue	To view and execute the workflows that have agents assigned
	Requests	To view all the requests submitted by the users and their result.
	Logs	To view Audit logs and Agent logs.
	Reports	To Create custom dashboards with out of the box reports or custom reports.
	Plugins	To view plugins and plugin steps
	Purging	To purge and archive data on four tables with large volume of data.
	Process Studio	To assign Process Studio licenses.
	Integration	To setup Integration Services, Types and Type configurations.
	Settings	To setup commonly used services.
Icon	User Icon	You can view your login details; change your password, logout from AE.
Table	Tenant Details table	The Table 6 below Add New Tenant displays a list of all tenants. The table provides details such as Organization code, tenant license type, start, and end date, and so on.

5 Users

5.1 Tenant Users

Tenant Users sub-menu, is used to add a new user, upload users, edit and delete users.

Table 6: Tenant User Options

Buttons/Text Box	Description
Search Users (Search Text Box)	Enter search string to filter Tenant Users.
Advanced Search	Enter advanced search criteria to filter Tenant Users.
Add New User	Used to add new user
Upload users	Used to upload the users in bulk.

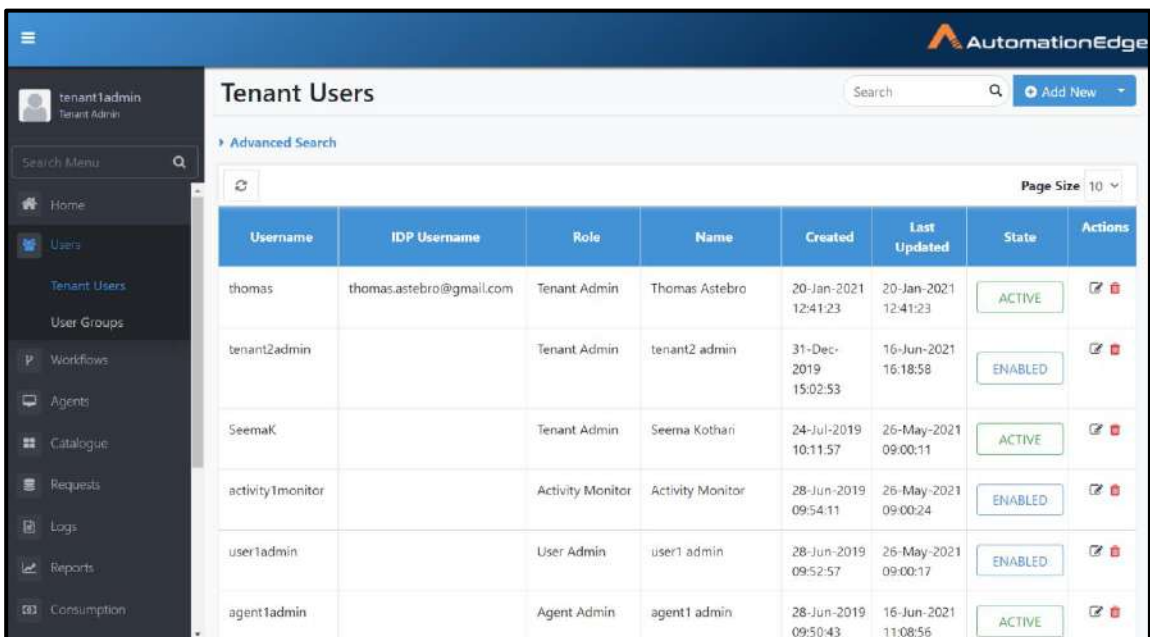
5.1.1 Tenant Users: View

To view Tenant Users,

1. Use the Menu Toggle to expand the main menu.
2. Click on Users menu item. Click Tenant Users sub-menu.
3. A list of all tenants appears in tabular format as shown below.

To search for Tenant Users,

1. Use the Menu Toggle to expand the main menu.
2. Click on Tenant Users menu item
3. Enter search string to filter the records real time.















Username	IDP Username	Role	Name	Created	Last Updated	State	Actions
thomas	thomas.astebro@gmail.com	Tenant Admin	Thomas Astebro	20-Jan-2021 12:41:23	20-Jan-2021 12:41:23	ACTIVE	 
tenant2admin		Tenant Admin	tenant2 admin	31-Dec-2019 15:02:53	16-Jun-2021 16:18:58	ENABLED	 
SeemaK		Tenant Admin	Seema Kothari	24-Jul-2019 10:11:57	26-May-2021 09:00:11	ACTIVE	 
activity1monitor		Activity Monitor	Activity Monitor	28-Jun-2019 09:54:11	26-May-2021 09:00:24	ENABLED	 
user1admin		User Admin	user1 admin	28-Jun-2019 09:52:57	26-May-2021 09:00:17	ENABLED	 
agent1admin		Agent Admin	agent1 admin	28-Jun-2019 09:50:43	16-Jun-2021 11:08:56	ACTIVE	 

Figure 7: Viewing Tenant Users

Table 7: Tenant User Tabular List Column Description

Field Name	Description
Username	Displays tenant user username.
IDP Username	In case of SSO user, IDP username is also displayed in addition to the username.
Role	Displays tenant user role.
Name	Displays tenant user first name & Last Name
Created	Displays tenant user creation date.
Last Updated Date	Displays tenant user last updated date.
State	Displays the State of the User. The possible states are Unverified, Active, Locked, Dormant, Disabled, Deleted and Enabled. The Details about User State are discussed in a following section Tenant Users: State.
Actions:	
Edit (✎)	Click to edit tenant user details.
Delete (🗑)	Click to delete tenant user.

5.1.2 Tenant Users: Search

To search for plugins,

1. Use the Menu Toggle to expand the main menu. Click on Users menu item
2. Enter search string to filter the records real time.

The screenshot shows the AutomationEdge Tenant Users management interface. A search bar is located at the top right of the main content area, highlighted with a red box and a red arrow. The interface includes a sidebar menu on the left with options like Home, Users, Tenant Users, User Groups, Workflows, Agents, Catalogue, Requests, Logs, Reports, Plugins, and Purging. The main content area displays a table of tenant users with columns for Username, Role, Name, Created, Last Updated, State, and Actions. The table contains 8 records, and the page size is set to 10. A red arrow points to the search bar, indicating the search functionality.

Figure 8: Search Free Text Box

5.1.3 Tenant Users: Advanced Search

For Advanced Search on tenant users:

1. Click Users.
2. Click Tenant Users.
3. Click Advanced Search.

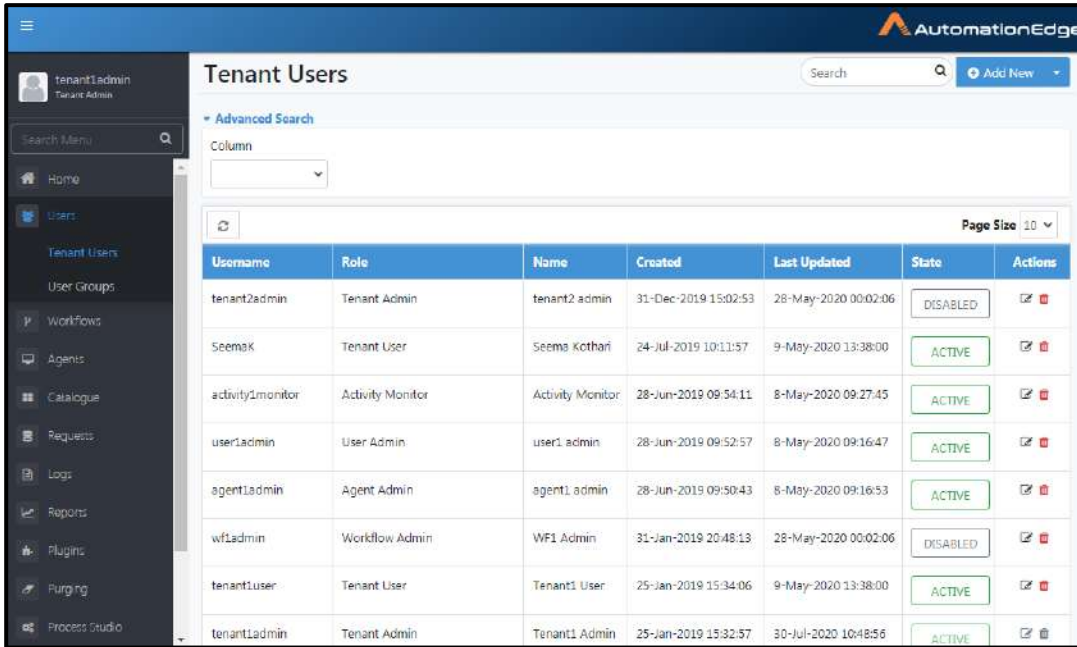


Figure 9a: Advanced Search

4. You can select the column on which you wish to base your search.

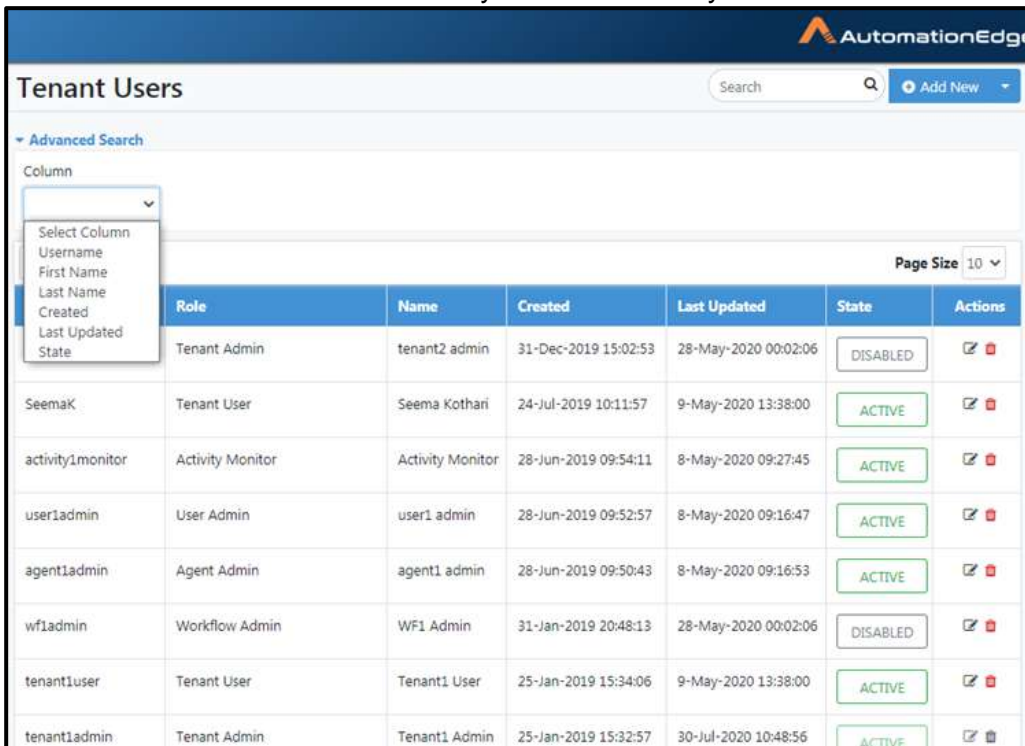


Figure 9b: Advanced Search Select Column

- Once you select column the Comparator field appears. Choose your comparator.

Username	Role	Name	Created	Last Updated	State	Actions
tenant2admin	Tenant Admin	tenant2 admin	31-Dec-2019 15:02:53	28-May-2020 00:02:06	DISABLED	[Edit] [Delete]
SeemaK	Tenant User	Seema Kothari	24-Jul-2019 10:11:57	9-May-2020 13:38:00	ACTIVE	[Edit] [Delete]
activity1monitor	Activity Monitor	Activity Monitor	28-Jun-2019 09:54:11	8-May-2020 09:27:45	ACTIVE	[Edit] [Delete]
user1admin	User Admin	user1 admin	28-Jun-2019 09:52:57	8-May-2020 09:16:47	ACTIVE	[Edit] [Delete]
agent1admin	Agent Admin	agent1 admin	28-Jun-2019 09:50:43	8-May-2020 09:16:53	ACTIVE	[Edit] [Delete]
wf1admin	Workflow Admin	WF1 Admin	31-Jan-2019 20:48:13	28-May-2020 00:02:06	DISABLED	[Edit] [Delete]
tenant1user	Tenant User	Tenant1 User	25-Jan-2019 15:34:06	9-May-2020 13:38:00	ACTIVE	[Edit] [Delete]
tenant1admin	Tenant Admin	Tenant1 Admin	25-Jan-2019 15:32:57	30-Jul-2020 10:48:56	ACTIVE	[Edit] [Delete]

Figure 9c: Advanced Search on Select Comparator

- Provide a value for the column.
- Click Add Filter.

Username	Role	Name	Created	Last Updated	State	Actions
tenant2admin	Tenant Admin	tenant2 admin	31-Dec-2019 15:02:53	28-May-2020 00:02:06	DISABLED	[Edit] [Delete]
SeemaK	Tenant User	Seema Kothari	24-Jul-2019 10:11:57	9-May-2020 13:38:00	ACTIVE	[Edit] [Delete]
activity1monitor	Activity Monitor	Activity Monitor	28-Jun-2019 09:54:11	8-May-2020 09:27:45	ACTIVE	[Edit] [Delete]
user1admin	User Admin	user1 admin	28-Jun-2019 09:52:57	8-May-2020 09:16:47	ACTIVE	[Edit] [Delete]
agent1admin	Agent Admin	agent1 admin	28-Jun-2019 09:50:43	8-May-2020 09:16:53	ACTIVE	[Edit] [Delete]
wf1admin	Workflow Admin	WF1 Admin	31-Jan-2019 20:48:13	28-May-2020 00:02:06	DISABLED	[Edit] [Delete]

Figure 9d: Value for Comparator

8. You can see the Added Filter. You also have the option to Clear Filters. Similarly, you can also add more filters. You can see the filtered list below.

The screenshot shows the 'Tenant Users' management interface. At the top, there is a search bar and an 'Add New' button. Below that, an 'Advanced Search' section is visible with a filter applied: 'Username like tenant'. A table below the filter shows the results of the search. The table has columns for Username, Role, Name, Created, Last Updated, State, and Actions. There are three rows of data. The first row is for 'tenant2admin' with a role of 'Tenant Admin' and a state of 'DISABLED'. The second row is for 'tenant1user' with a role of 'Tenant User' and a state of 'ACTIVE'. The third row is for 'tenant1admin' with a role of 'Tenant Admin' and a state of 'ACTIVE'. At the bottom of the table, it indicates 'Page 1 of 1 (Total 3 Record(s))' and a 'Page Size' of 10.

Username	Role	Name	Created	Last Updated	State	Actions
tenant2admin	Tenant Admin	tenant2 admin	31-Dec-2019 15:02:53	28-May-2020 00:02:06	DISABLED	
tenant1user	Tenant User	Tenant1 User	25-Jan-2019 15:34:06	9-May-2020 13:38:00	ACTIVE	
tenant1admin	Tenant Admin	Tenant1 Admin	25-Jan-2019 15:32:57	30-Jul-2020 10:48:56	ACTIVE	

Figure 9e: Added Filter

Following is the comparator descriptions for advanced search options are as follows.

Table 8: Advanced Search Options by Username, First Name, Last Name

Field	Description
Equal To	To search entries by the exact entered text.
Not Equal To	To search entries not matching the entered text.
Like	To search entries containing the entered text
Begins With	To search entries that begins with the entered text.
Ends With	To search entries that ends with the entered text.

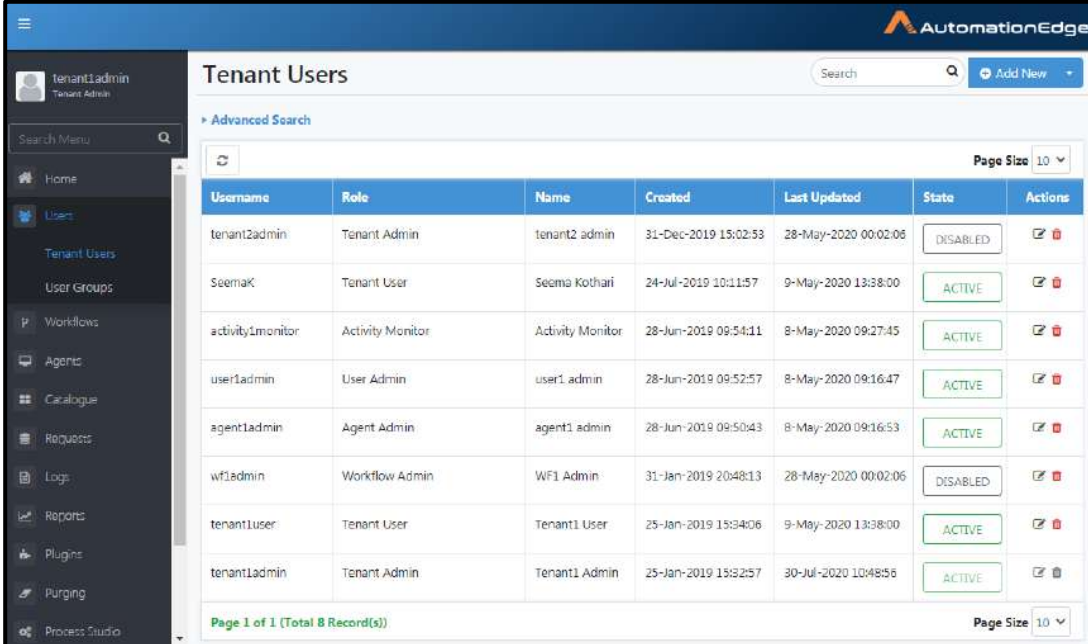
Table 9: Advanced Search Options by Created and Last Updated Date

Field	Description
Exact Date	To search entries by the exact entered date.
Before	To search entries before the entered date.
After	To search entries after the entered date.
In Between	To search entries in between the entered dates.
Not In Between	To search entries not in between the entered dates.

5.1.4 Tenant Users: Add New

To add a Tenant user,

1. Navigate to Users → Tenant Users.



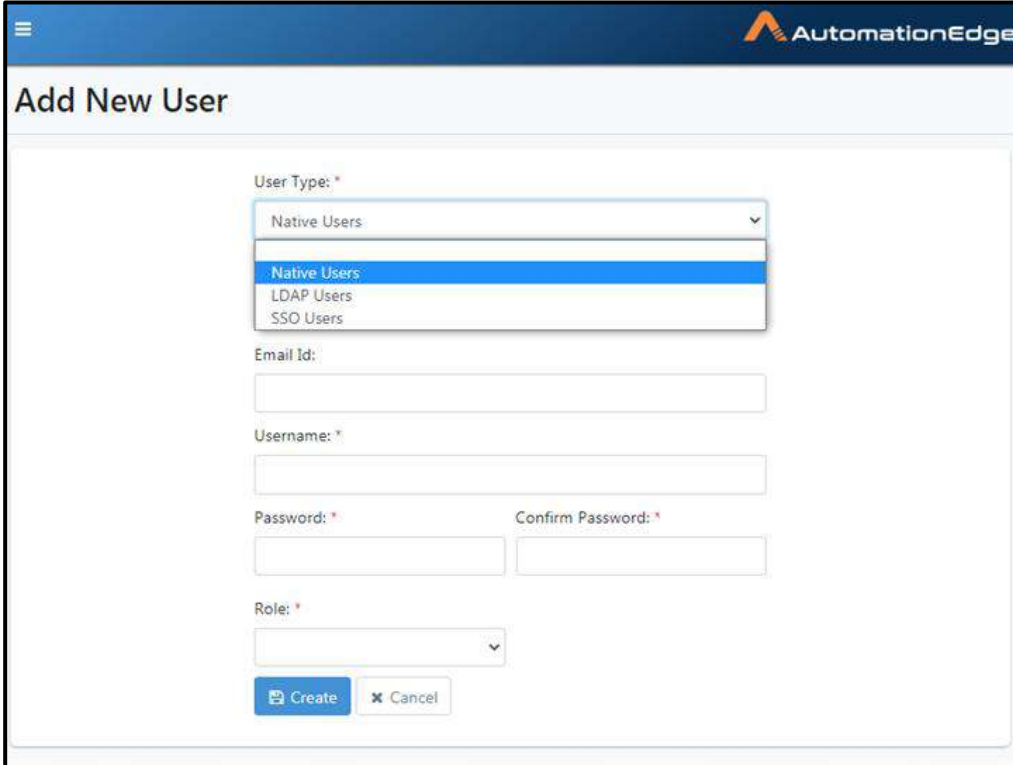
The screenshot shows the 'Tenant Users' page in the AutomationEdge application. The page features a search bar, an 'Add New' button, and a table of users. The table has columns for Username, Role, Name, Created, Last Updated, State, and Actions. The current page shows 8 records out of a total of 8.

Username	Role	Name	Created	Last Updated	State	Actions
tenant2admin	Tenant Admin	tenant2 admin	31-Dec-2019 15:02:53	28-May-2020 00:02:06	DISABLED	[Edit] [Delete]
SeemaK	Tenant User	Seema Kothari	24-Jul-2019 10:11:57	9-May-2020 13:38:00	ACTIVE	[Edit] [Delete]
activityMonitor	Activity Monitor	Activity Monitor	28-Jun-2019 09:54:11	8-May-2020 09:27:45	ACTIVE	[Edit] [Delete]
user1admin	User Admin	user1 admin	28-Jun-2019 09:52:57	8-May-2020 09:16:47	ACTIVE	[Edit] [Delete]
agent1admin	Agent Admin	agent1 admin	28-Jun-2019 09:50:43	8-May-2020 09:16:53	ACTIVE	[Edit] [Delete]
wf1admin	Workflow Admin	WF1 Admin	31-Jan-2019 20:48:13	28-May-2020 00:02:06	DISABLED	[Edit] [Delete]
tenant1user	Tenant User	Tenant1 User	25-Jan-2019 15:34:06	9-May-2020 13:38:00	ACTIVE	[Edit] [Delete]
tenant1admin	Tenant Admin	Tenant1 Admin	25-Jan-2019 15:32:57	30-Jul-2020 10:48:56	ACTIVE	[Edit] [Delete]

Figure 10a: Adding Tenant User

3. Click Add New User.
Refer to [Table 10: Add New User – Details](#). towards the end of this section for a description of the User creation fields.

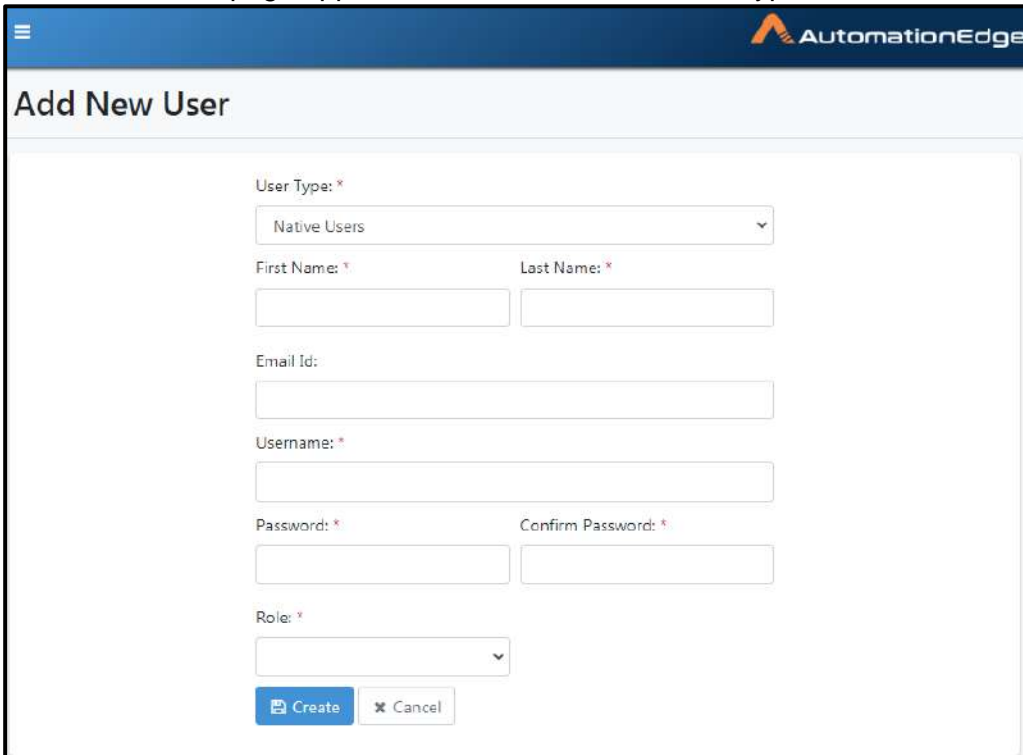
5. Select user Type from the drop down list.



The screenshot shows the 'Add New User' form in the AutomationEdge interface. The 'User Type' dropdown menu is open, displaying three options: 'Native Users' (which is highlighted in blue), 'LDAP Users', and 'SSO Users'. Below the dropdown, there are input fields for 'Email Id', 'Username', 'Password', and 'Confirm Password'. There is also a 'Role' dropdown menu. At the bottom of the form, there are two buttons: 'Create' and 'Cancel'.

Figure 10b: User Type

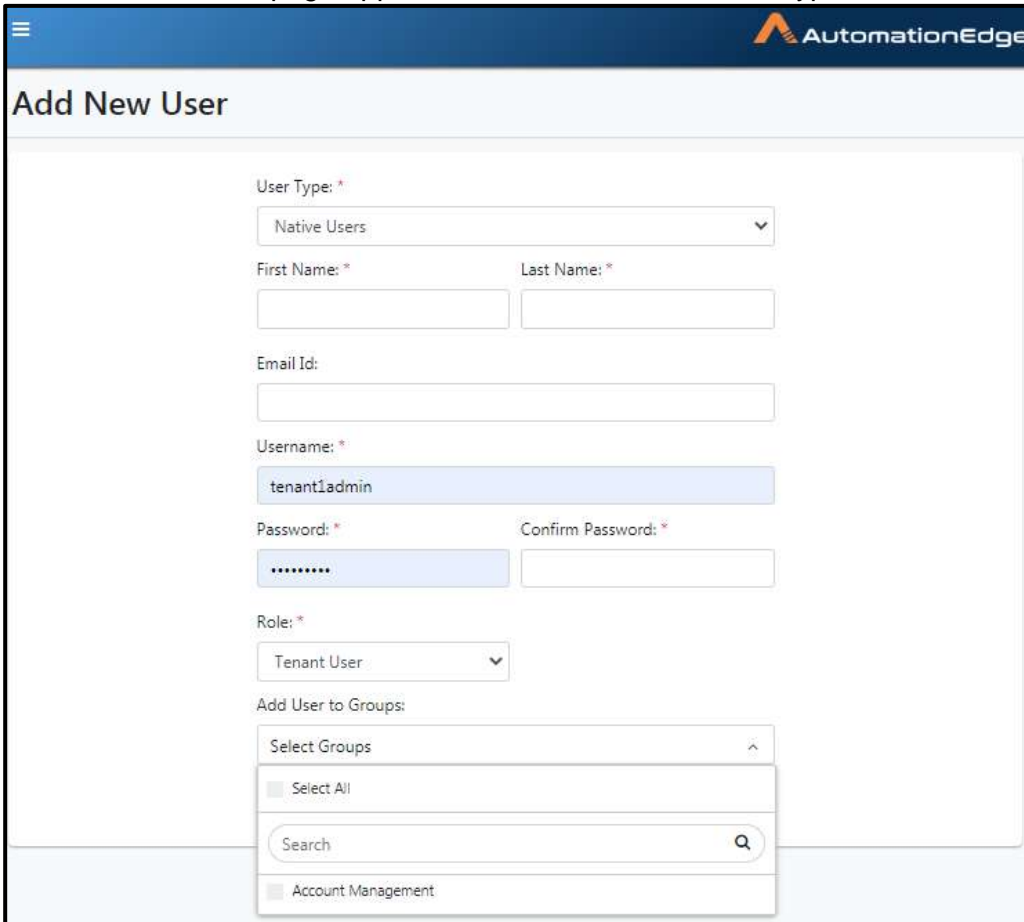
4. The User Details page appears as shown below for User type: Native User.



The screenshot shows the 'Add New User' form in the AutomationEdge interface. The 'User Type' dropdown menu is set to 'Native Users'. Below it, there are input fields for 'First Name' and 'Last Name', followed by 'Email Id', 'Username', 'Password', and 'Confirm Password'. There is also a 'Role' dropdown menu. At the bottom of the form, there are two buttons: 'Create' and 'Cancel'.

Figure 10c: Create Native User

6. In case the role chosen is Tenant User, an option to add User to Groups is available. The Tenant User Details page appears as shown below for User type: Native User

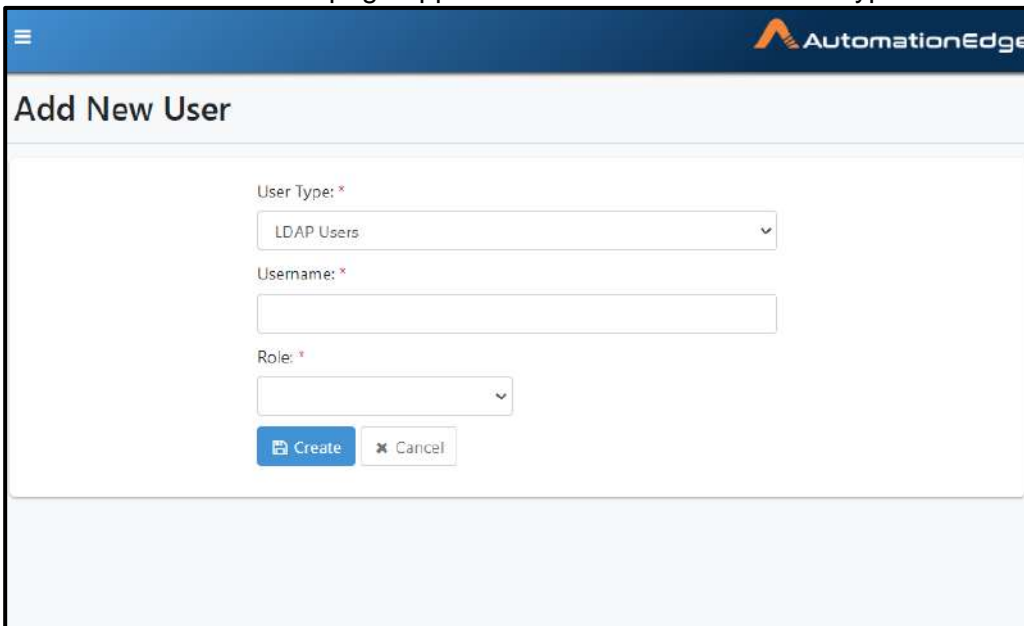


The screenshot shows the 'Add New User' form in the AutomationEdge interface. The form is titled 'Add New User' and includes the following fields and options:

- User Type:** A dropdown menu set to 'Native Users'.
- First Name:** and **Last Name:** text input fields.
- Email Id:** text input field.
- Username:** text input field containing 'tenant1admin'.
- Password:** and **Confirm Password:** text input fields, both masked with dots.
- Role:** A dropdown menu set to 'Tenant User'.
- Add User to Groups:** A section with a 'Select Groups' dropdown, a 'Select All' checkbox, a search input field, and a list of groups including 'Account Management'.

Figure 10d: Native User with role Tenant User

7. The Tenant User Details page appears as shown below for User type: LDAP User.

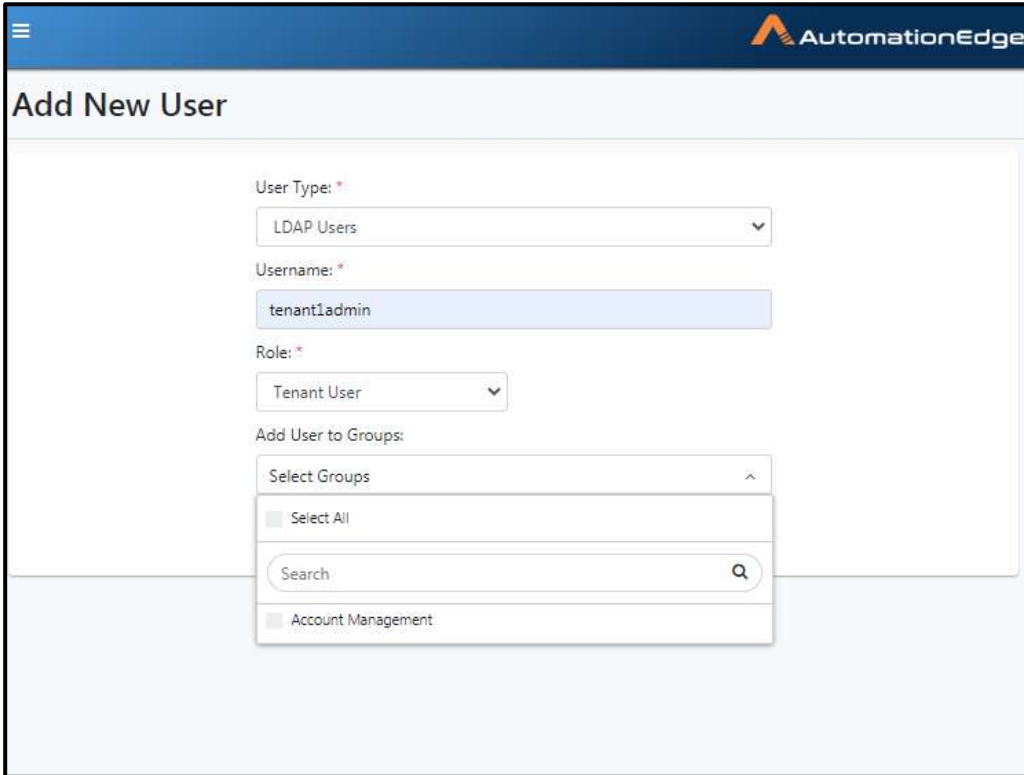


The screenshot shows the 'Add New User' form in the AutomationEdge interface for an LDAP User. The form is titled 'Add New User' and includes the following fields and options:

- User Type:** A dropdown menu set to 'LDAP Users'.
- Username:** text input field.
- Role:** A dropdown menu.
- Buttons:** 'Create' and 'Cancel' buttons at the bottom.

Figure 10e: Create LDAP user

8. In case the role chosen is Tenant User, an option to add User to Groups is available. The Tenant User Details page appears as shown below for User type: LDAP User

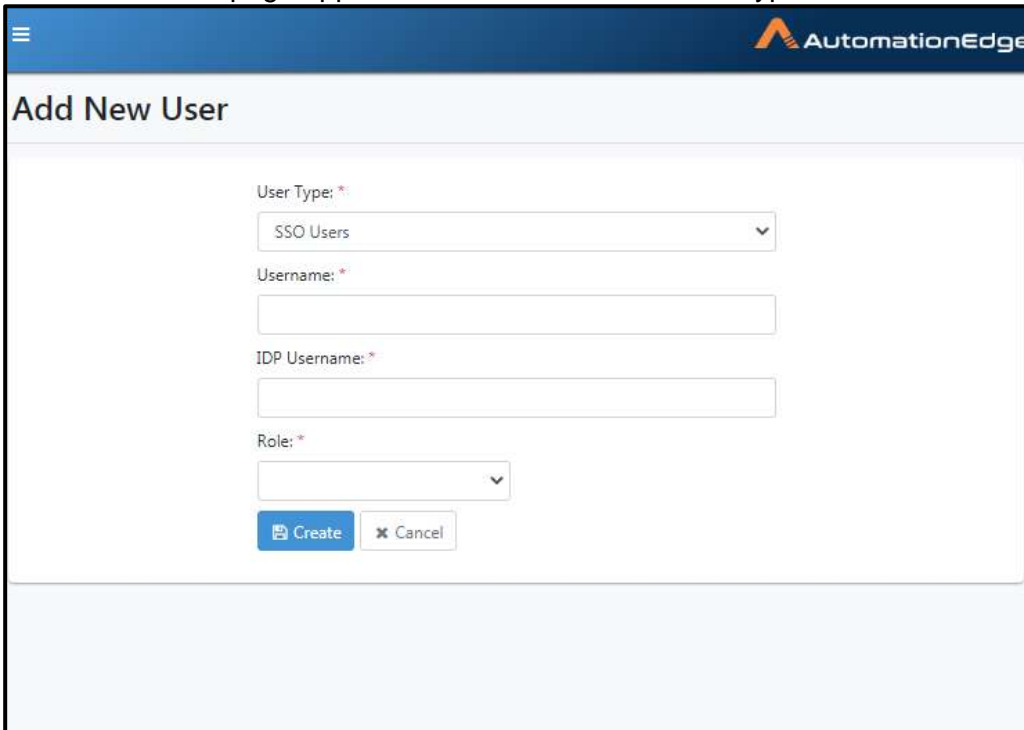


The screenshot shows the 'Add New User' form in the AutomationEdge interface. The form is titled 'Add New User' and has a blue header with the AutomationEdge logo. The form fields are as follows:

- User Type:** A dropdown menu with 'LDAP Users' selected.
- Username:** A text input field containing 'tenant1admin'.
- Role:** A dropdown menu with 'Tenant User' selected.
- Add User to Groups:** A section with a 'Select Groups' dropdown menu, a 'Select All' checkbox, a search bar with the text 'Search' and a magnifying glass icon, and a list of groups with 'Account Management' selected.

Figure 10f: LDAP User with role Tenant User

5. The User Details page appears as shown below for User type: SSO Users.

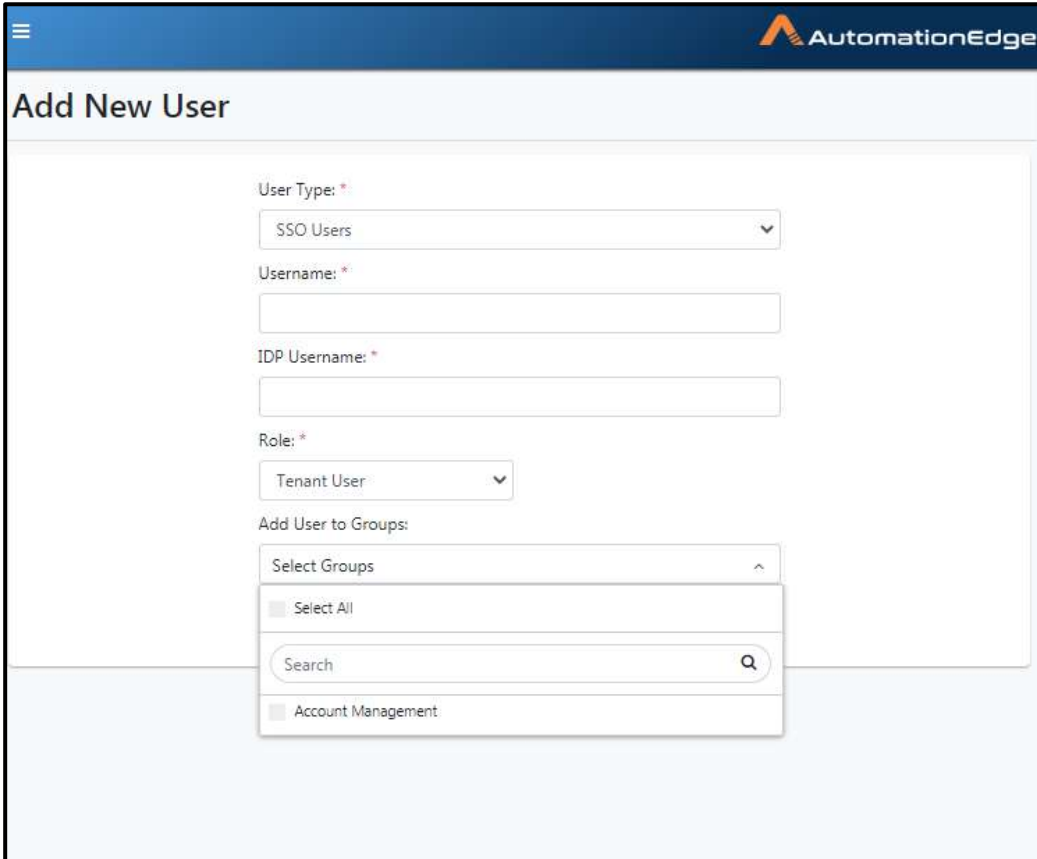


The screenshot shows the 'Add New User' form in the AutomationEdge interface for an SSO User. The form is titled 'Add New User' and has a blue header with the AutomationEdge logo. The form fields are as follows:

- User Type:** A dropdown menu with 'SSO Users' selected.
- Username:** An empty text input field.
- IDP Username:** An empty text input field.
- Role:** A dropdown menu with an empty selection.
- Buttons:** Two buttons at the bottom: 'Create' (with a plus icon) and 'Cancel' (with an X icon).

Figure 10g: Create SSO user

9. In case the role chosen is Tenant User, an option to add User to Groups is available. The Tenant User Details page appears as shown below for User type: SSO User.



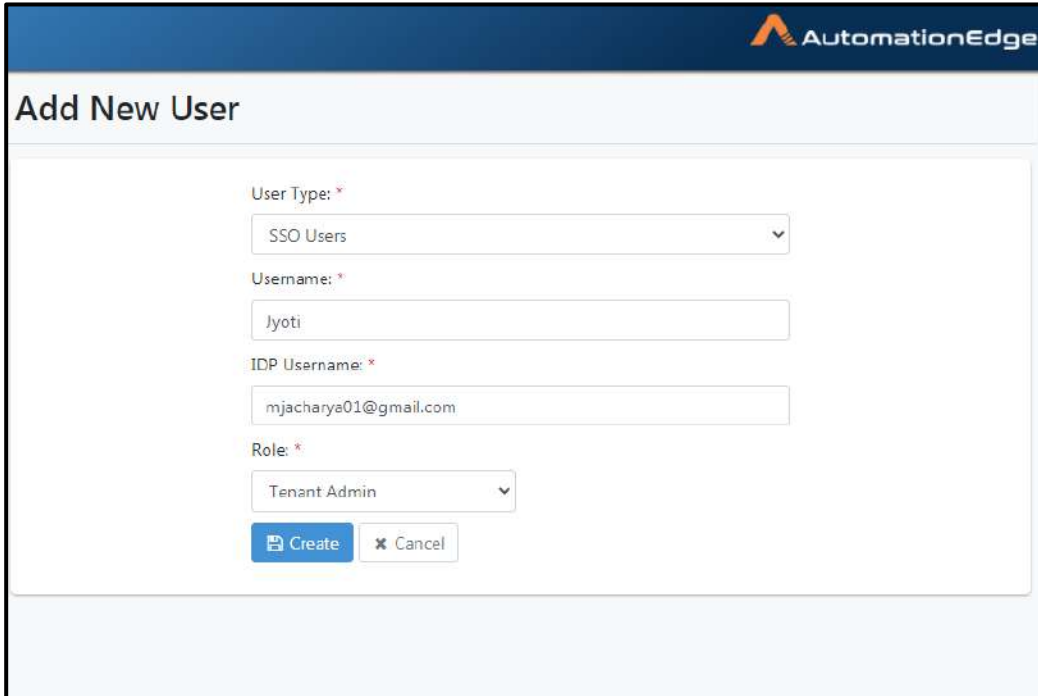
The screenshot shows the 'Add New User' form in the AutomationEdge interface. The form is titled 'Add New User' and is located within a blue header bar that contains the AutomationEdge logo. The form fields are as follows:

- User Type:** A dropdown menu with 'SSO Users' selected.
- Username:** A text input field.
- IDP Username:** A text input field.
- Role:** A dropdown menu with 'Tenant User' selected.
- Add User to Groups:** A section with a search bar and a list of groups. The search bar contains the text 'Select Groups'. Below the search bar, there is a checkbox labeled 'Select All' and a search input field with the text 'Search' and a magnifying glass icon. Below the search input, there is a checkbox labeled 'Account Management'.

Figure 10h: SSO User with role Tenant User

10. Complete the user creation process of User Type SSO Users.
11. Provide an AutomationEdge SSO Username to be created.
12. Provide an IDP Username to link to this AutomationEdge SSO User.

13. Select a Role and Click Create button.



Add New User

User Type: *
SSO Users

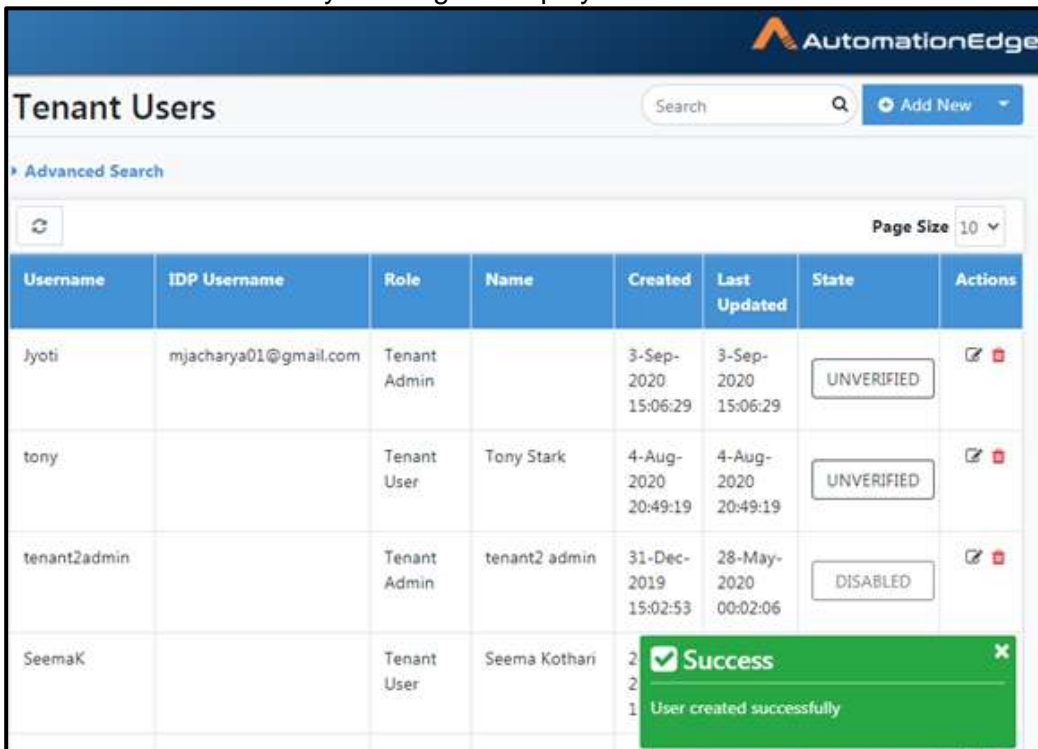
Username: *
Jyoti

IDP Username: *
mjacharya01@gmail.com

Role: *
Tenant Admin

Figure 10i: Create SSO Users Type

14. User created successfully message is displayed as seen below.



Tenant Users

Search

Advanced Search

Page Size 10

Username	IDP Username	Role	Name	Created	Last Updated	State	Actions
Jyoti	mjacharya01@gmail.com	Tenant Admin		3-Sep-2020 15:06:29	3-Sep-2020 15:06:29	UNVERIFIED	<input type="checkbox"/> <input type="checkbox"/>
tony		Tenant User	Tony Stark	4-Aug-2020 20:49:19	4-Aug-2020 20:49:19	UNVERIFIED	<input type="checkbox"/> <input type="checkbox"/>
tenant2admin		Tenant Admin	tenant2 admin	31-Dec-2019 15:02:53	28-May-2020 00:02:06	DISABLED	<input type="checkbox"/> <input type="checkbox"/>
SeemaK		Tenant User	Seema Kothari	2020-08-04 20:49:19	2020-08-04 20:49:19		<input type="checkbox"/> <input type="checkbox"/>

Success
User created successfully

Figure 10j: SSO User Created Successfully

15. You may now use this SSO User to 'Sign In with SSO' on AutomationEdge Login screen as described in the section Sign In with SSO.

16. Similarly, you may use Native and LDAP users for Sign In on AutomationEdge Login screen

A description of the User Details page fields for all the User Types is provided in the table below.

Table 10: Add New User – Details

Field Name	Description
User Details:	
User Type	<p>Select from the following,</p> <ul style="list-style-type: none"> • Native User: Details of the users are kept in AE-DB. User authentication done by AE. • LDAP User: <ul style="list-style-type: none"> - LDAP user type is available in the dropdown list only if LDAP has been configured in the settings menu. - Details about the user are fetched from LDAP. User authentication done using LDAP authentication. • SSO User: AutomationEdge SSO User Authentication is done by Identity Provider. The supported protocols are OpenID Connect and OAuth 2.0. Every Organization/Tenant can have one unique AutomationEdge SSO user linked to a particular Identity Provider user. <p>You must Setup Single Sign-On under Settings→ Single Sign-On menu to be able to add SSO Users. Refer section - Single Sign-On for the setups.</p> <p>Note:</p> <ul style="list-style-type: none"> - SSO Users cannot be created for Sysadmin role. - SSO Users cannot use Process Studio.
First Name	Specify user's first name. Tenant Administrator cannot add, remove, and delete tenants. Only Users can be added or deleted. This field is Mandatory.
Last Name	Specify user's last name. This field is Mandatory.
Email Id	Specify user's email Id. This field is Mandatory.
Username	Specify user's AutomationEdge username. This field is Mandatory.
IDP Username	Specify the Identity Provider (IDP) username to be linked to the AutomationEdge username. <ul style="list-style-type: none"> ➤ Only one AutomationEdge username from an Organization/Tenant can be linked to an IDP username. ➤ AutomationEdge Username be linked to an IDP username should be unique across Tenants.

Password	Specify user's password. This field is Mandatory.
Force Change Password	When, the system forces the user to change the password on next login.
Role	Select from the following: <ul style="list-style-type: none"> • ROLE_TENANT_ADMIN • ROLE_TENANT_USER • ROLE_USER_ADMIN • ROLE_WORKFLOW_ADMIN • ROLE_AGENT_ADMIN
Add User to Groups	If Role selected is Tenant User an option to Add User to Groups is available. A Tenant user can be assigned to one or more Groups.
Buttons:	
Create button	Click to create a Tenant User.
Cancel button	Click to cancel the process of adding new tenant

Note: In case of LDAP users only user name and role need to be entered, other details are fetched from LDAP during first login.

17. In this section we have demonstrated end to end User creation for user type SSO user.
18. For other User Types also, enter users' details (First Name, Last Name, Email Id, Username, password etc.) as per User Type.
19. For other user Types you can use 'Sign In' option on AutomationEdge Login screen.
20. You will have to change the password on First Login for Native Users.
21. Click Create.
22. After first Login the users are activated.

Note: While Tenant Administrator can create users with roles as above, User Administrator can create/update users having Tenant user role only.

23. This completes the process of Tenant User creation.

5.1.5 Tenant Users Add: Upload Users

The Upload Users feature can be used when users are to be created in bulk at a time. Only Tenant Users (with role Tenant user) can be created using this feature.

A description of the fields is given in the table below.

Table 11: Button “Upload Users”: Bulk User Upload Field/Button Description

Field Name	Description
User Type	Select User Type: LDAP User/Native User SSO User
Download sample template link	Reference format for entering user details.
Buttons:	
Choose File	To select the .csv file that contains the list of users.
Upload Users	To upload the selected user list file
Cancel button	To cancel bulk user upload.

To create users in bulk:

1. Navigate to Users menu.
2. Click the arrow next to Add New button. Click Upload Users.

The screenshot displays the 'Tenant Users' management page in the AutomationEdge application. The interface includes a sidebar with navigation options like Home, Users, Workflows, Agents, Catalogue, Requests, Logs, Reports, Plugins, Purging, Process Studio, and Integration. The main content area shows a table of existing users with columns for Username, Role, Name, Created, Last Updated, State, and Actions. The 'Add New' button is visible, and the 'Upload Users' option is highlighted in the dropdown menu.

Username	Role	Name	Created	Last Updated	State	Actions
tenant2admin	Tenant Admin	tenant2 admin	31-Dec-2019 15:02:53	28-May-2020 00:02:06	DISABLED	[Edit] [Delete]
SeemaK	Tenant User	Seema Kothari	24-Jul-2019 10:11:57	9-May-2020 13:38:00	ACTIVE	[Edit] [Delete]
activity1monitor	Activity Monitor	Activity Monitor	28-Jun-2019 09:54:11	8-May-2020 09:27:45	ACTIVE	[Edit] [Delete]
user1admin	User Admin	user1 admin	28-Jun-2019 09:52:57	8-May-2020 09:16:47	ACTIVE	[Edit] [Delete]
agent1admin	Agent Admin	agent1 admin	28-Jun-2019 09:50:43	8-May-2020 09:16:53	ACTIVE	[Edit] [Delete]
wf1admin	Workflow Admin	WF1 Admin	31-Jan-2019 20:48:13	28-May-2020 00:02:06	DISABLED	[Edit] [Delete]
tenant1user	Tenant User	Tenant1 User	25-Jan-2019 15:34:06	9-May-2020 13:38:00	ACTIVE	[Edit] [Delete]
tenant1admin	Tenant Admin	Tenant1 Admin	25-Jan-2019 15:32:57	30-Jul-2020 10:48:56	ACTIVE	[Edit] [Delete]

Figure 11a: Selecting Upload Users Button

3. Select User Type
4. Click Sample Template button on top right hand corner to download a sample file template to upload users.

Template for native users has firstname, lastname, email and username.

L17					
	A	B	C	D	E
1	firstname	lastname	email	username	
2	Peter	Parker	pete@abc.com	peter	
3	Tony	Stark	tony@abc.com	tony	
4					

Figure 11b: Template of Native Users

Template for LDAP users has only username.

A4					
	A	B	C	D	E
1	username				
2	peter				
3	tony				
4					

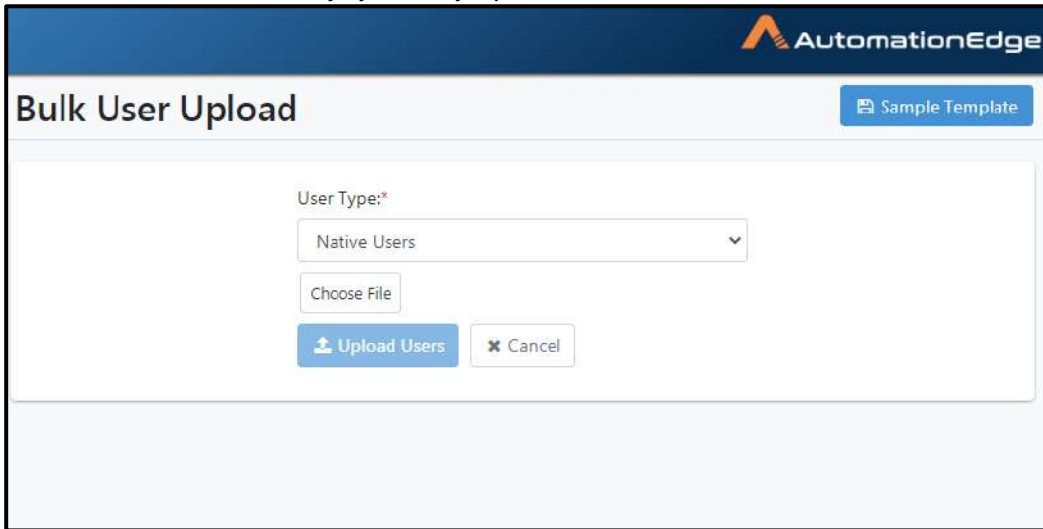
Figure 11c: Template for LDAP Users

Template for SSO users has username and idpusername.

B5				
	A	B	C	D
1	username	idpusername		
2	peter	tom		
3	tony	robert		
4				

Figure 11d: Template for LDAP Users

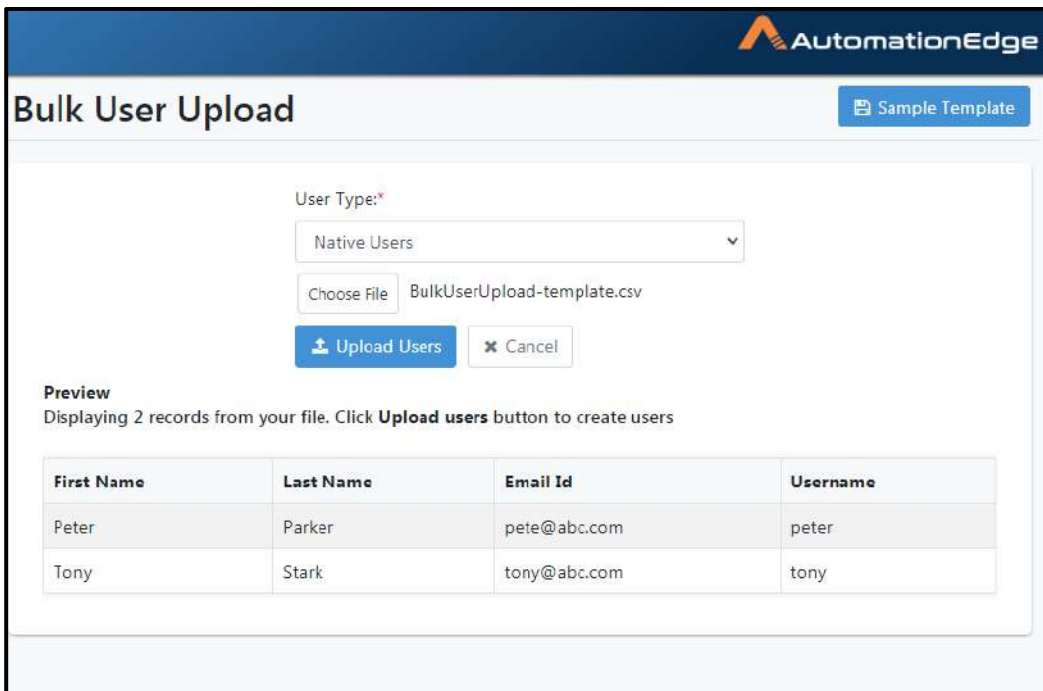
5. Edit the downloaded template with user details and save the .csv file.
6. Click Choose File and select the created user detail file. In this case we shall upload file for Native Users. Similarly, you may upload files for LDAP or SSO users.



The screenshot shows the 'Bulk User Upload' interface. At the top right, there is a 'Sample Template' button. Below it, the 'User Type:' dropdown menu is set to 'Native Users'. A 'Choose File' button is visible, and below it are 'Upload Users' and 'Cancel' buttons.

Figure 11e: User Details Sample Template

7. Preview of selected user file displays. Click Upload Users to upload the selected user detail file.



The screenshot shows the 'Bulk User Upload' interface with a preview of the selected user file. The 'User Type:' dropdown is still set to 'Native Users'. The 'Choose File' button now shows the filename 'BulkUserUpload-template.csv'. Below the 'Upload Users' and 'Cancel' buttons, there is a 'Preview' section with the text 'Displaying 2 records from your file. Click Upload users button to create users'. A table displays the following data:

First Name	Last Name	Email Id	Username
Peter	Parker	pete@abc.com	peter
Tony	Stark	tony@abc.com	tony

Figure 11f: Preview of Selected User File

8. The Result of upload is displayed as shown below. The uploaded information is also available in a downloaded file.

The screenshot displays the 'Bulk User Upload' interface. At the top right, there is a 'Sample Template' button. The main form area includes a 'User Type:*' dropdown menu currently set to 'Native Users'. Below this is a 'Choose File' button next to the filename 'BulkUserUpload-template.csv'. There are two buttons: 'Upload Users' (with an upload icon) and 'Cancel' (with an 'x' icon). A 'Result' section is shown below the form, containing a table with the following data:

Total users uploaded - 2
Users created - 2
Errors - 0

Below the table, a note states: 'Refer downloaded [BulkUserUpload-result.csv](#) for more information'.

Figure 11g: Uploading Users

In case of partial failures, the file BulkUseUpload-result.csv file adds reason of failure against each failed user.

5.1.6 Tenant Users: State

State is useful for Tenant User monitoring. Following is the complete list of User States possible.

1. **UNVERIFIED**<Unverified User> - As soon as a user account is created it goes into UNVERIFIED state. When user try to login for the first time dormancy check will be applied and if account happens to be dormant, then account state changes to DISABLED otherwise ACTIVE and logs in.
2. **ACTIVE** - User logs in and performs normally when in this state.
3. **LOCKED** - A user may be locked on crossing the max number of Attempts for unsuccessful login. The schedules configured by the locked user may continue to run. On login a locked user gives a generic error message.
4. **DORMANT** - If an account has had no activity for a long period of time, then the account is marked as dormant. A dormant account is automatically disabled. On login a dormant user gives a generic error message. The dormancy period can be set in the Tenant Policy menu under Settings. A dormant account can also be enabled or disabled by the System or Tenant Administrator.

5. **DISABLED** – A user can be manually disabled from Active, Enabled or Locked states. If a user is disabled, their schedules get automatically disabled. A display message to show this warning is shown in the confirmation box for disabling user. On login a disabled user gives a generic error message.
6. **DELETED**– A User Account is in DELETED state when an Administrator deletes the account. This state is not displayed on the UI. On login a deleted user gives a generic error message.
7. **ENABLED** – A user is enabled from disabled, dormant or locked state; but user is yet to login. On login an enabled user is marked as Active and logs in.

The following snapshot shows the different user states and their interrelationships.

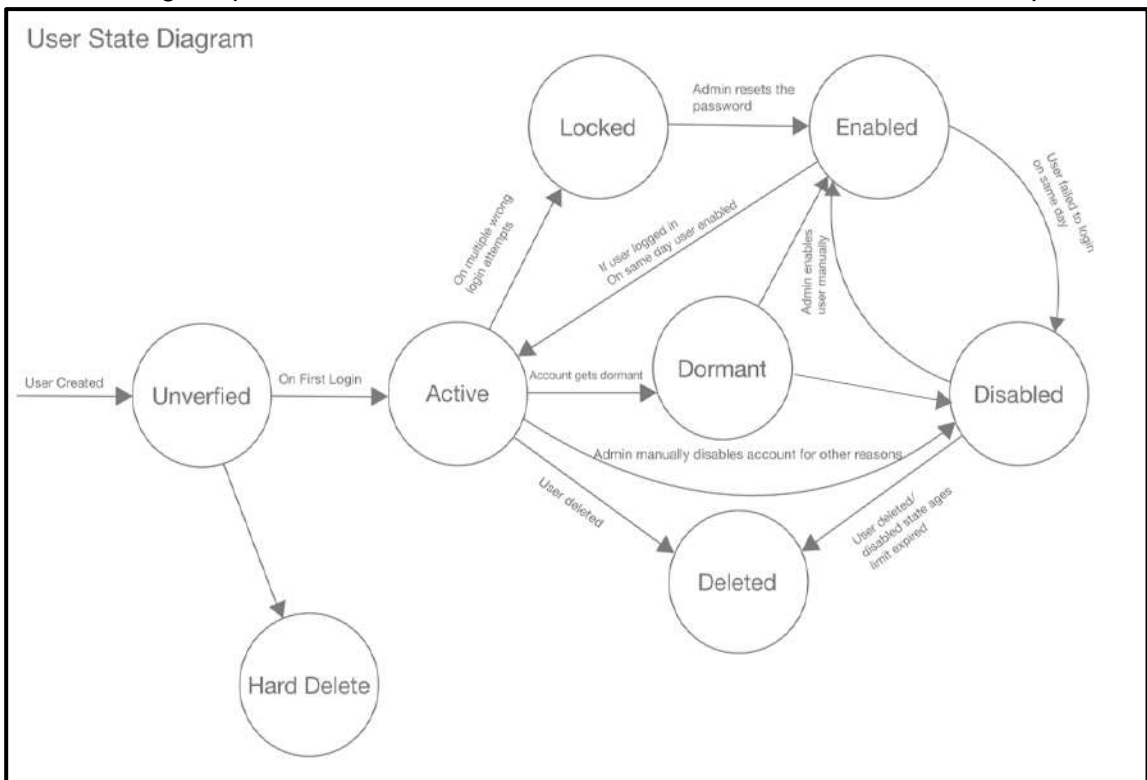
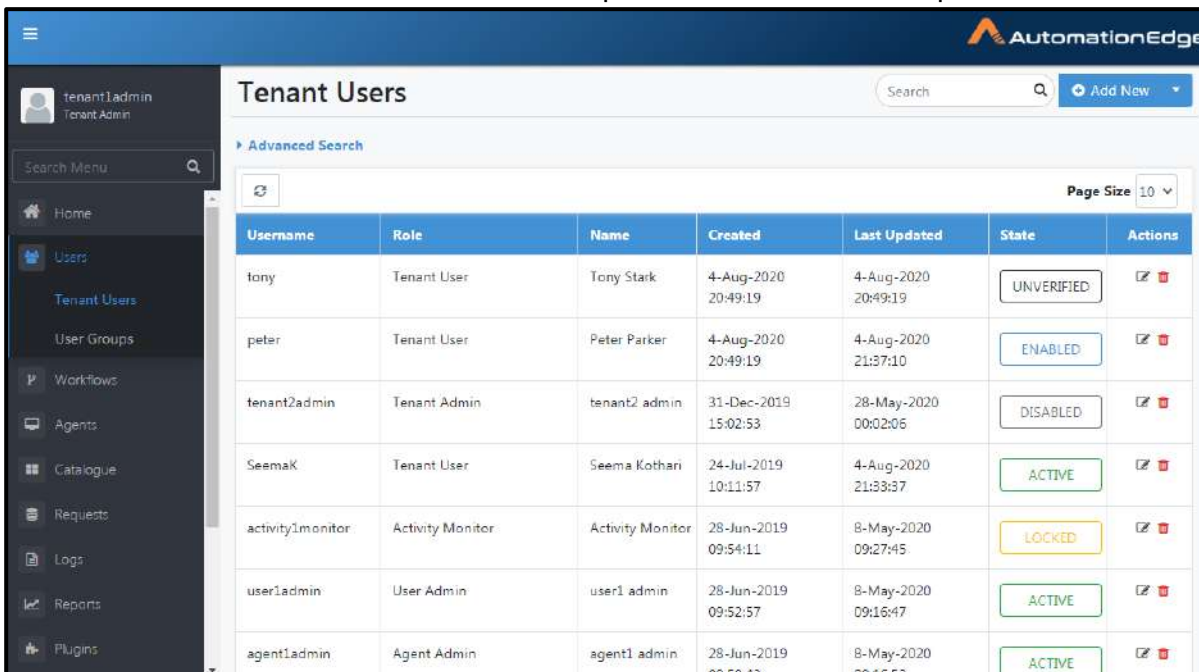


Figure 11h: User states and Interrelationships

5.1.6.1 Tenant Users: Change State

AE Tenant Users menu is shown with several possible States in the snapshot below.

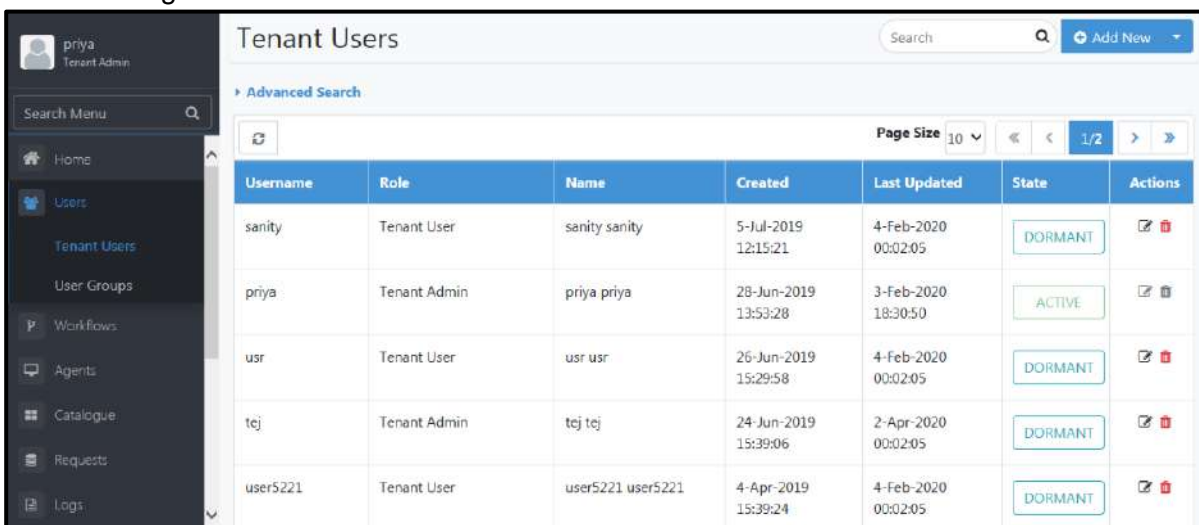


The screenshot shows the 'Tenant Users' page in the AutomationEdge interface. The page includes a search bar, an 'Add New' button, and a table of users. The table has columns for Username, Role, Name, Created, Last Updated, State, and Actions. The users listed are:

Username	Role	Name	Created	Last Updated	State	Actions
tony	Tenant User	Tony Stark	4-Aug-2020 20:49:19	4-Aug-2020 20:49:19	UNVERIFIED	[Edit] [Delete]
peter	Tenant User	Peter Parker	4-Aug-2020 20:49:19	4-Aug-2020 21:37:10	ENABLED	[Edit] [Delete]
tenant2admin	Tenant Admin	tenant2 admin	31-Dec-2019 15:02:53	28-May-2020 00:02:06	DISABLED	[Edit] [Delete]
SeemaK	Tenant User	Seema Kothari	24-Jul-2019 10:11:57	4-Aug-2020 21:33:37	ACTIVE	[Edit] [Delete]
activity1monitor	Activity Monitor	Activity Monitor	28-Jun-2019 09:54:11	8-May-2020 09:27:45	LOCKED	[Edit] [Delete]
user1admin	User Admin	user1 admin	28-Jun-2019 09:52:57	8-May-2020 09:16:47	ACTIVE	[Edit] [Delete]
agent1admin	Agent Admin	agent1 admin	28-Jun-2019 09:50:43	8-May-2020 09:16:53	ACTIVE	[Edit] [Delete]

Figure 11i: Snapshot depicting several User States

The following screenshot shows some dormant accounts.



The screenshot shows the 'Tenant Users' page in the AutomationEdge interface, displaying dormant accounts. The page includes a search bar, an 'Add New' button, and a table of users. The users listed are:

Username	Role	Name	Created	Last Updated	State	Actions
sanity	Tenant User	sanity sanity	5-Jul-2019 12:15:21	4-Feb-2020 00:02:05	DORMANT	[Edit] [Delete]
priya	Tenant Admin	priya priya	28-Jun-2019 13:53:28	3-Feb-2020 18:30:50	ACTIVE	[Edit] [Delete]
usr	Tenant User	usr usr	26-Jun-2019 15:29:58	4-Feb-2020 00:02:05	DORMANT	[Edit] [Delete]
tej	Tenant Admin	tej tej	24-Jun-2019 15:39:06	2-Apr-2020 00:02:05	DORMANT	[Edit] [Delete]
user5221	Tenant User	user5221 user5221	4-Apr-2019 15:39:24	4-Feb-2020 00:02:05	DORMANT	[Edit] [Delete]

Figure 11j: Snapshot depicting Dormant State

The state of an Active, Locked, Disabled or Dormant user can be changed by clicking on the state link.

The use case below demonstrates how to change the state of a user in LOCKED state. Tenant Administrator Users can be unlocked by the System Administrators. Tenant Users can be unlocked by System Administrators or Tenant Administrators.

Login AE UI. If a user is locked you get a message that account is inaccessible.

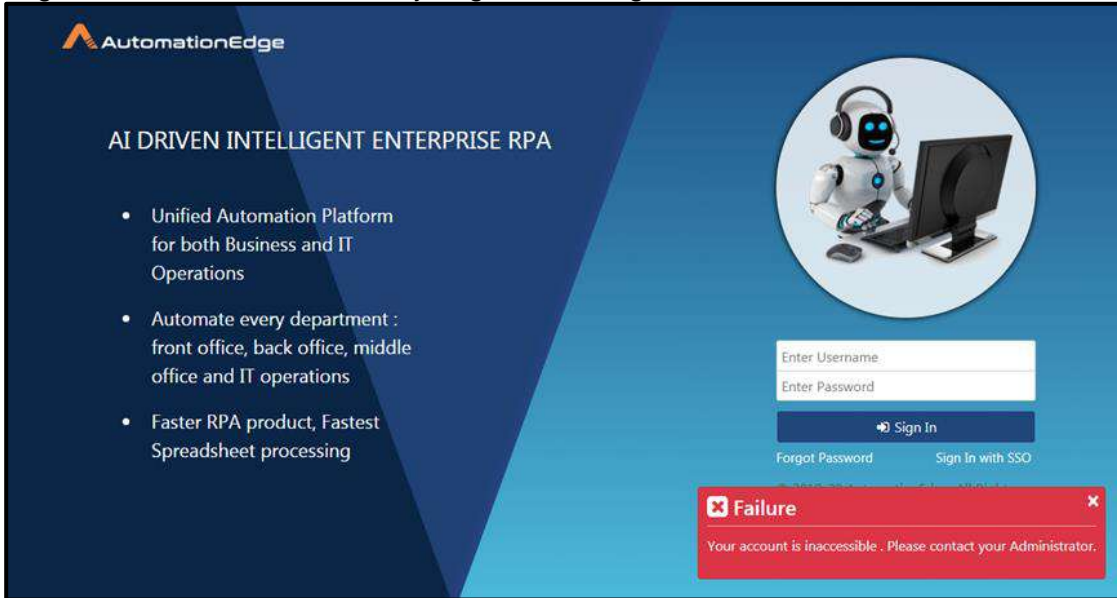


Figure 11k: Locked User Login error message

Following are the steps to change user state from Locked to Unverified and then Active on first login.

1. Navigate to Users → Tenant Users menu.
2. The State of a user is visible in the state column.
3. If a user is locked its state is locked.
4. Click the LOCKED link corresponding to the tenant user you wish to unlock. In this case we wish to unlock tenant12user.

The screenshot shows the 'Tenant Users' management interface in AutomationEdge. The interface includes a sidebar with navigation options like 'Users', 'Tenant Users', 'User Groups', 'Workflows', 'Agents', 'Catalogue', 'Requests', 'Logs', 'Reports', and 'Plugins'. The main content area displays a table of users. The table has columns for Username, Role, Name, Created, Last Updated, State, and Actions. The user 'tenant12user' is listed with a 'LOCKED' state, while 'tenant12admin' is 'ACTIVE'. There are also search and pagination controls at the top of the table.

Username	Role	Name	Created	Last Updated	State	Actions
tenant12user	Tenant User	Tenant12 User	1-Jul-2021 21:05:02	1-Jul-2021 21:07:49	LOCKED	🔗 🗑️
tenant12admin	Tenant Admin	tenant12 admin	16-Jun-2021 16:40:30	1-Jul-2021 20:58:44	ACTIVE	🔗 🗑️

Figure 11l: Tenant User is locked

- You can see a popup window to Select an Action as seen below. From Locked state you can use Unlock User option to Enable the user or Disable User to disable the user.

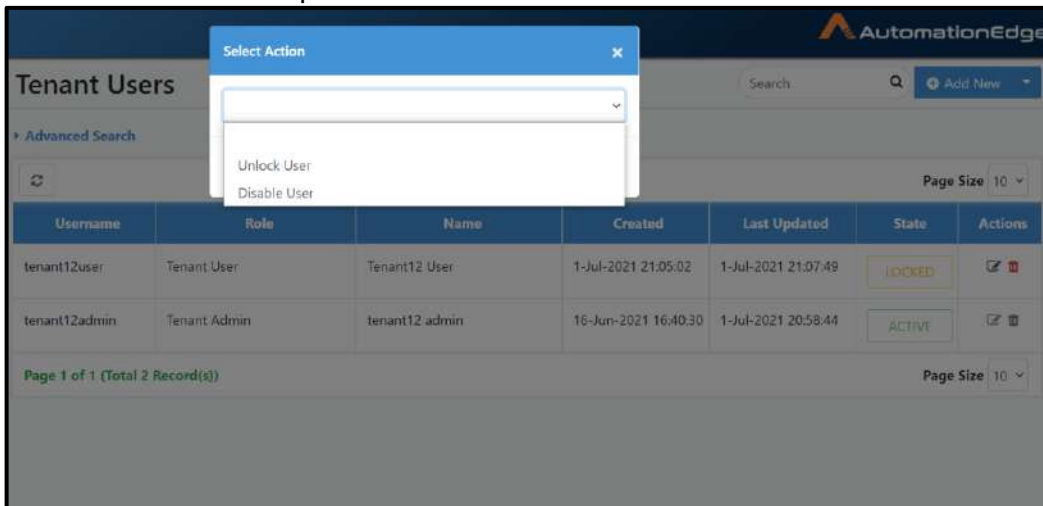


Figure 11m: Actions for Locked User

- In this case we have chosen Unlock tenant12user User.

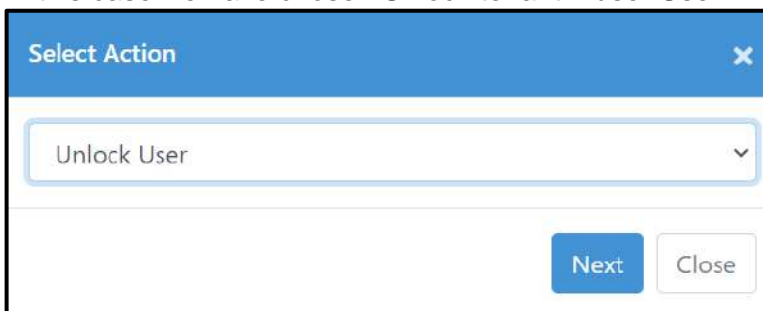


Figure 11n: Unlock Locked User

- An Unlock User pop-up appears. Set and confirm a new password for the user.

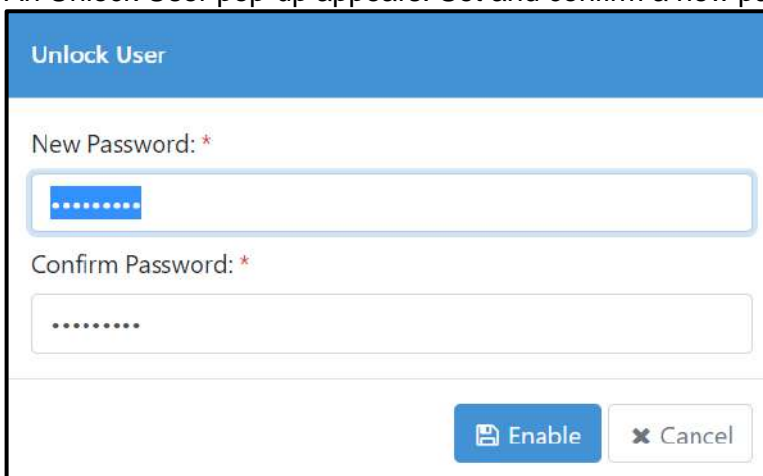
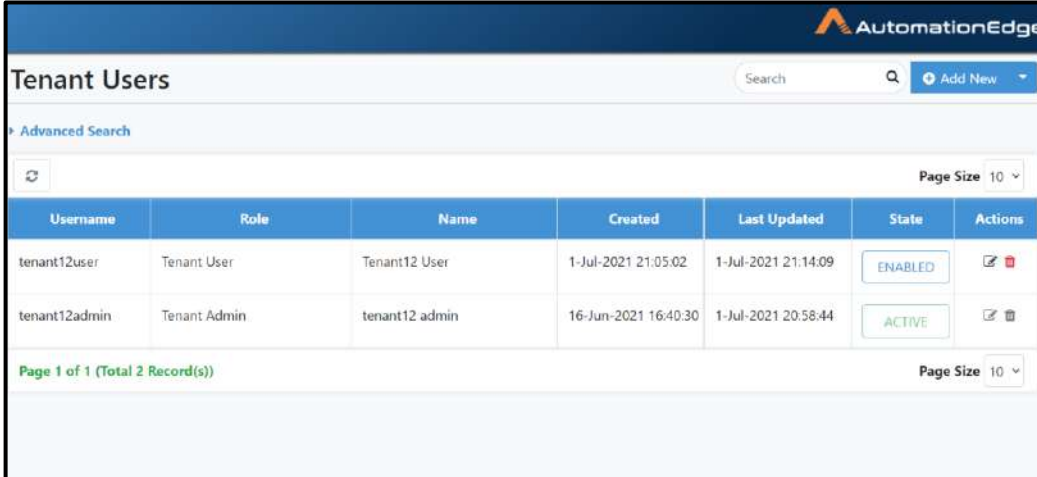


Figure 11o: Unlock Tenant User - Reset Password

- A User [Enabled] successfully message appears.

9. Once unlocked the state of the Tenant user (tenant12user in this case) goes to Enabled.







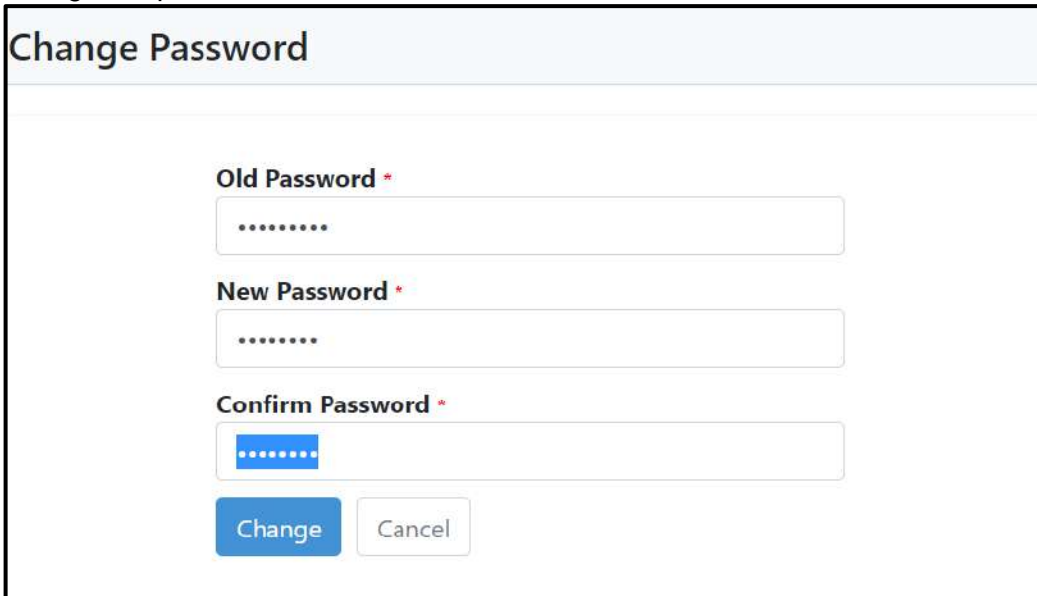
Username	Role	Name	Created	Last Updated	State	Actions
tenant12user	Tenant User	Tenant12 User	1-Jul-2021 21:05:02	1-Jul-2021 21:14:09	ENABLED	 
tenant12admin	Tenant Admin	tenant12 admin	16-Jun-2021 16:40:30	1-Jul-2021 20:58:44	ACTIVE	 

Figure 11p: Unlocked User in Enabled State

10. You may now login with tenant12user with the newly set password for the enabled user.
11. The first time login it forces you to change the password.
12. A Change Password screen appears. Provide the password you set as part of unlocking the user account in the Old Password field. Provide the new password to set in the New Password and Confirm Password fields.
13. The screen below shows the passwords provided in encrypted format. Click Change to change the password.



Change Password

Old Password *

.....

New Password *

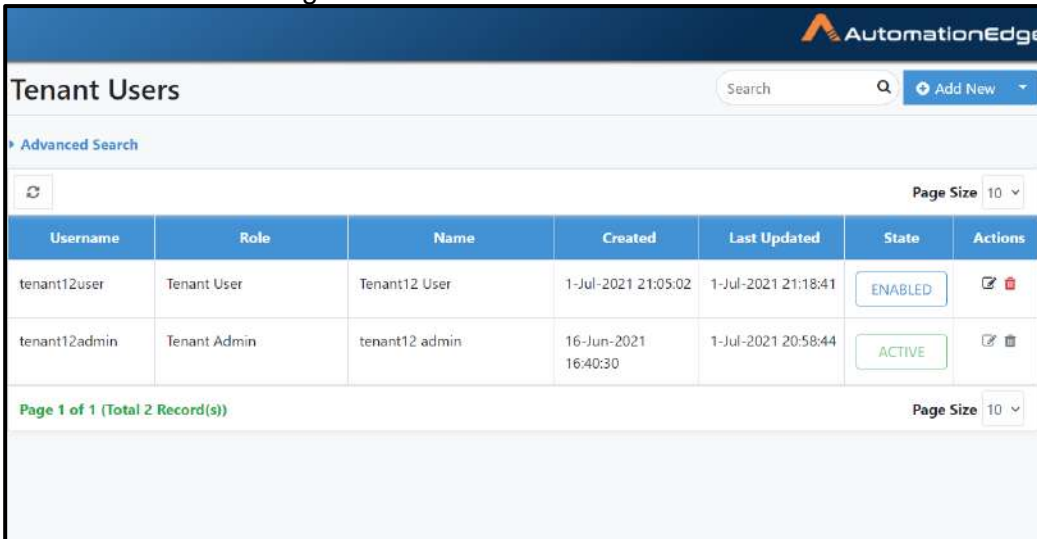
.....

Confirm Password *





.....

Figure 11q: Force Change Password

14. Password reset can give an error in the following scenarios,
 - In same password as the old password it gives an error - “Your new password cannot be same as old password”
 - In case you provide a password same as an old password, depending on the Password History set in the Tenant policy you get an error message –“New password must be different from your previous passwords”
 - case you provide an incorrect password you get an error message – “Incorrect old password”.
15. With the correct old password and a valid new password, once the password is changed it takes you back to the login screen. Login with the new password set on first login.
16. Once you login you land on the Landing page. In case of Tenant Administrators the landing page is the Home Page while in case of tenant Users the landing page is the Catalogue page.
17. Navigate to the Tenant Users menu. You see that the Enabled user state for user tenant12user has changed to Active.



The screenshot shows the 'Tenant Users' management interface. At the top, there is a search bar and an 'Add New' button. Below the search bar is an 'Advanced Search' section with a refresh icon and a 'Page Size' dropdown set to 10. The main content is a table with the following data:

Username	Role	Name	Created	Last Updated	State	Actions
tenant12user	Tenant User	Tenant12 User	1-Jul-2021 21:05:02	1-Jul-2021 21:18:41	ENABLED	 
tenant12admin	Tenant Admin	tenant12 admin	16-Jun-2021 16:40:30	1-Jul-2021 20:58:44	ACTIVE	 

At the bottom of the table, it shows 'Page 1 of 1 (Total 2 Record(s))' and another 'Page Size' dropdown set to 10.

Figure 11r: Unlocked User is Active

18. This completes the process of unlocking the user account.
19. The same process can be followed to enable as well as disable/delete users. Depending on the current user state the options to unlock, enable or disable/delete are displayed upon clicking the current state. The unlock, enable or disable/delete are also demonstrated step by step in the AutomationEdge_R7.0.0_System_Administrator_Guide.

5.1.7 Tenant Users: Edit

To edit a tenant user details:

1. Click Users.
2. Click Tenant Users
3. Click the Edit icon (✎) corresponding to the tenant user you wish to edit.

Username	Role	Name	Created	Last Updated	State	Actions
tony	Tenant User	Tony Stark	4-Aug-2020 20:49:19	4-Aug-2020 20:49:19	UNVERIFIED	✎ ✖
peter	Tenant User	Peter Parker	4-Aug-2020 20:49:19	4-Aug-2020 21:37:10	ENABLED	✎ ✖
tenant2admin	Tenant Admin	tenant2 admin	31-Dec-2019 15:02:53	28-May-2020 00:02:06	DISABLED	✎ ✖
SeemaK	Tenant User	Seema Kothari	24-Jul-2019 10:11:57	4-Aug-2020 21:33:37	ACTIVE	✎ ✖
activity1monitor	Activity Monitor	Activity Monitor	28-Jun-2019 09:54:11	8-May-2020 09:27:45	LOCKED	✎ ✖
user1admin	User Admin	user1 admin	28-Jun-2019 09:52:57	8-May-2020 09:16:47	ACTIVE	✎ ✖
agent1admin	Agent Admin	agent1 admin	28-Jun-2019 09:50:42	8-May-2020 09:15:53	ACTIVE	✎ ✖

Figure 12a: Selecting Tenant User to Edit

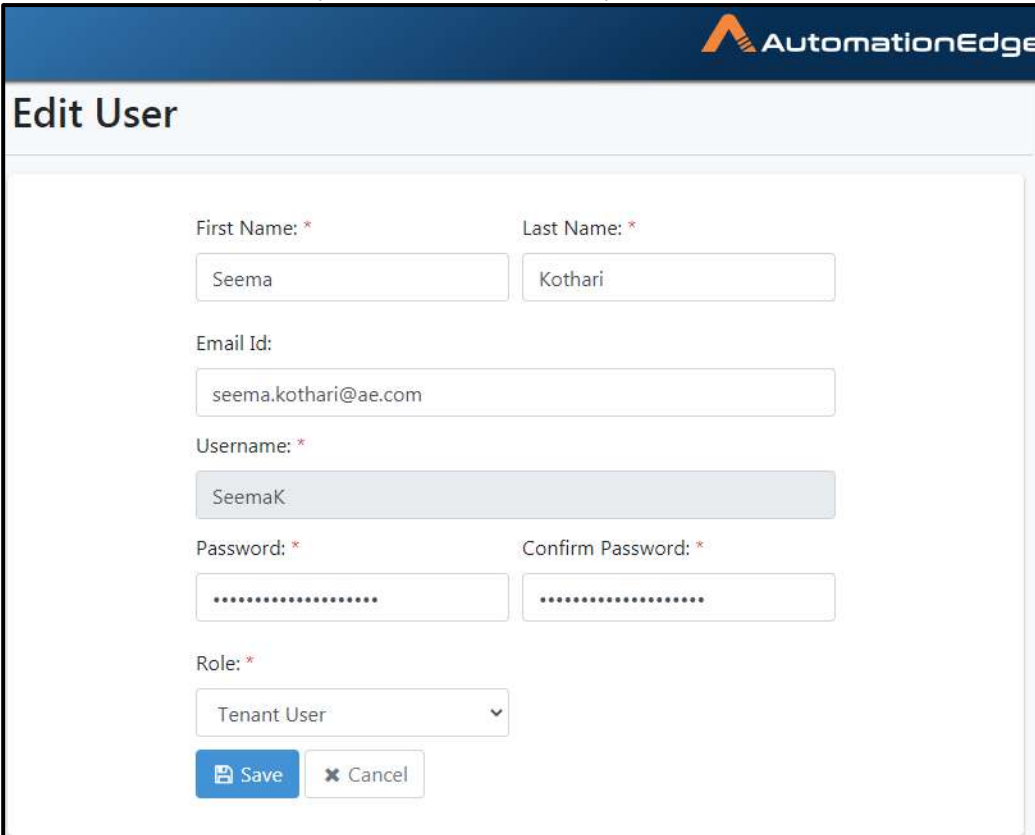
4. Edit the details. For Native user's first name, last name, email Id, password and role can be edited. For LDAP users only role can be edited. However, User Administrator cannot modify role for Native Users as well as LDAP users. Add User to Groups is also not editable.
5. If you want the user to change the password after the first login, check the Force Change Password checkbox.

6. You can select the role for Tenant User. There are four Roles for Tenant Users (Refer 3 above)
 - a. ROLE_TENANT_ADMIN
 - b. ROLE_TENANT_USER
 - c. ROLE_USER_ADMIN
 - d. ROLE_WORKFLOW_ADMIN.
 - e. ROLE_AGENT_ADMIN
 - f. ROLE_ACTIVITY_MONITOR

 **Note:** User Administrators cannot edit Tenant role.

User Administrators cannot edit LDAP Users.

7. Select a new role which you want to select for your tenant.



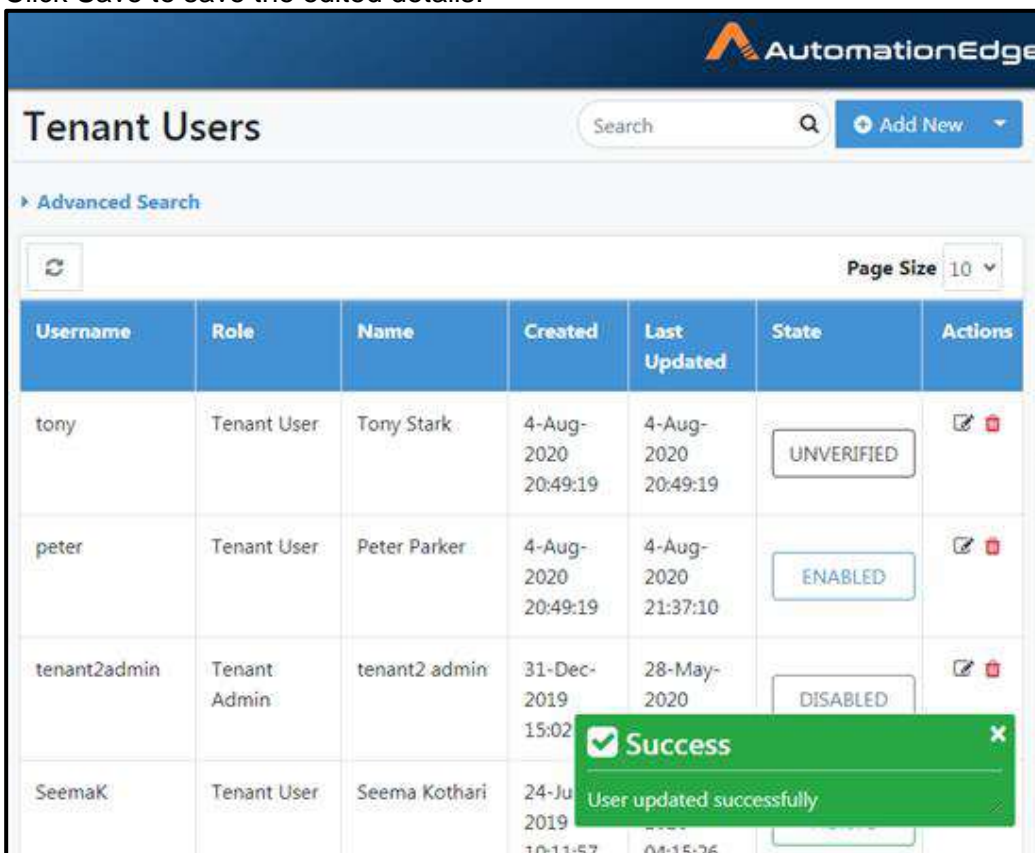
The screenshot shows the 'Edit User' interface in AutomationEdge. The form contains the following fields and values:

- First Name: * Seema
- Last Name: * Kothari
- Email Id: seema.kothari@ae.com
- Username: * SeemaK
- Password: *
- Confirm Password: *
- Role: * Tenant User

At the bottom of the form, there are two buttons: 'Save' and 'Cancel'.

Figure 12b: Editing Tenant Users Details

8. Click Save to save the edited details.



The screenshot displays the 'Tenant Users' management interface. At the top, there is a search bar and an 'Add New' button. Below this is an 'Advanced Search' section with a refresh icon and a 'Page Size' dropdown set to 10. The main content is a table with columns: Username, Role, Name, Created, Last Updated, State, and Actions. The table lists four users: 'tony' (Tenant User, Tony Stark, 4-Aug-2020 20:49:19, UNVERIFIED), 'peter' (Tenant User, Peter Parker, 4-Aug-2020 21:37:10, ENABLED), 'tenant2admin' (Tenant Admin, tenant2 admin, 31-Dec-2019 15:02, DISABLED), and 'SeemaK' (Tenant User, Seema Kothari, 24-Jul-2019 10:11:57, State partially visible). A green success message overlay is present, stating 'Success' and 'User updated successfully'.







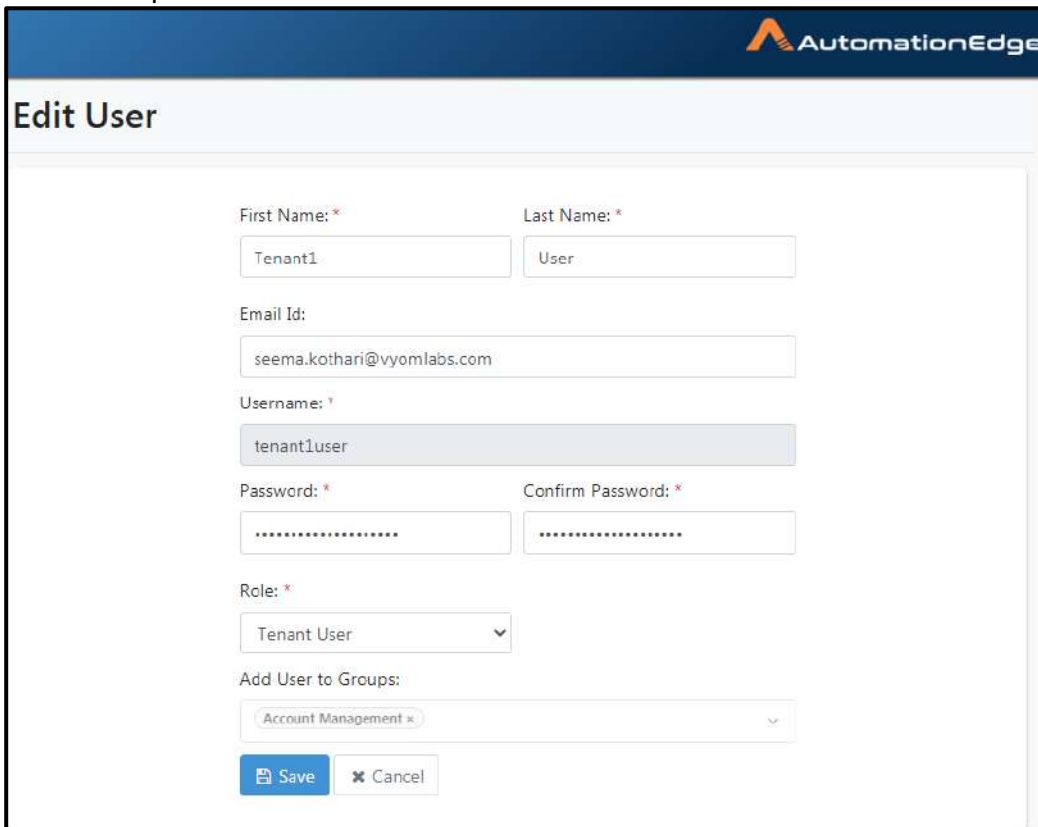
Username	Role	Name	Created	Last Updated	State	Actions
tony	Tenant User	Tony Stark	4-Aug-2020 20:49:19	4-Aug-2020 20:49:19	UNVERIFIED	 
peter	Tenant User	Peter Parker	4-Aug-2020 20:49:19	4-Aug-2020 21:37:10	ENABLED	 
tenant2admin	Tenant Admin	tenant2 admin	31-Dec-2019 15:02	28-May-2020	DISABLED	 
SeemaK	Tenant User	Seema Kothari	24-Jul-2019 10:11:57	04-15-26		

Figure 12c: User updated successfully message

9. If a Tenant User was assigned a Group at the time of creation the edit screen appears as below. You can see the Add User to Groups field, however it is not editable. Please note that a Group cannot be added to a Tenant User at the time of edit.



The screenshot shows the 'Edit User' interface. At the top right is the AutomationEdge logo. The title 'Edit User' is on the left. The form fields are as follows:

- First Name: * (text input: Tenant1)
- Last Name: * (text input: User)
- Email Id: (text input: seema.kothari@vyomlabs.com)
- Username: * (text input: tenant1user)
- Password: * (password input:)
- Confirm Password: * (password input:)
- Role: * (dropdown menu: Tenant User)
- Add User to Groups: (disabled dropdown menu: Account Management)

At the bottom are 'Save' and 'Cancel' buttons.

Figure 12d: Add User to Group is not editable

5.1.8 Tenant Users: Delete

To delete the tenant user:

1. User the Menu Toggle to expand the main menu.
2. Click on Users menu item. Click Tenant Users sub-menu
3. Click the Delete icon (🗑️) corresponding to the tenant user you wish to delete.

Username	Role	Name	Created	Last Updated	State	Actions
tony	Tenant User	Tony Stark	4-Aug-2020 20:49:19	4-Aug-2020 20:49:19	UNVERIFIED	🗑️
peter	Tenant User	Peter Parker	4-Aug-2020 20:49:19	4-Aug-2020 21:37:10	ENABLED	🗑️
tenant2admin	Tenant Admin	tenant2 admin	31-Dec-2019 15:02:53	28-May-2020 00:02:06	DISABLED	🗑️
SeemaK	Tenant User	Seema Kothari	24-Jul-2019 10:11:57	4-Aug-2020 21:33:37	ACTIVE	🗑️
activity1monitor	Activity Monitor	Activity Monitor	28-Jun-2019 09:54:11	8-May-2020 09:27:45	LOCKED	🗑️
user1admin	User Admin	user1 admin	28-Jun-2019 09:52:57	8-May-2020 09:16:47	ACTIVE	🗑️
agent1admin	Agent Admin	agent1 admin	28-Jun-2019 09:52:57	8-May-2020 09:16:47	ACTIVE	🗑️

Figure 13a: Deleting Tenant User

4. Click OK to confirm user deletion.

Confirm User Deletion

Are you sure you want to delete this user?

Delete
Cancel

Figure 13b: Confirming User Deletion

5. User deleted successfully message appears.

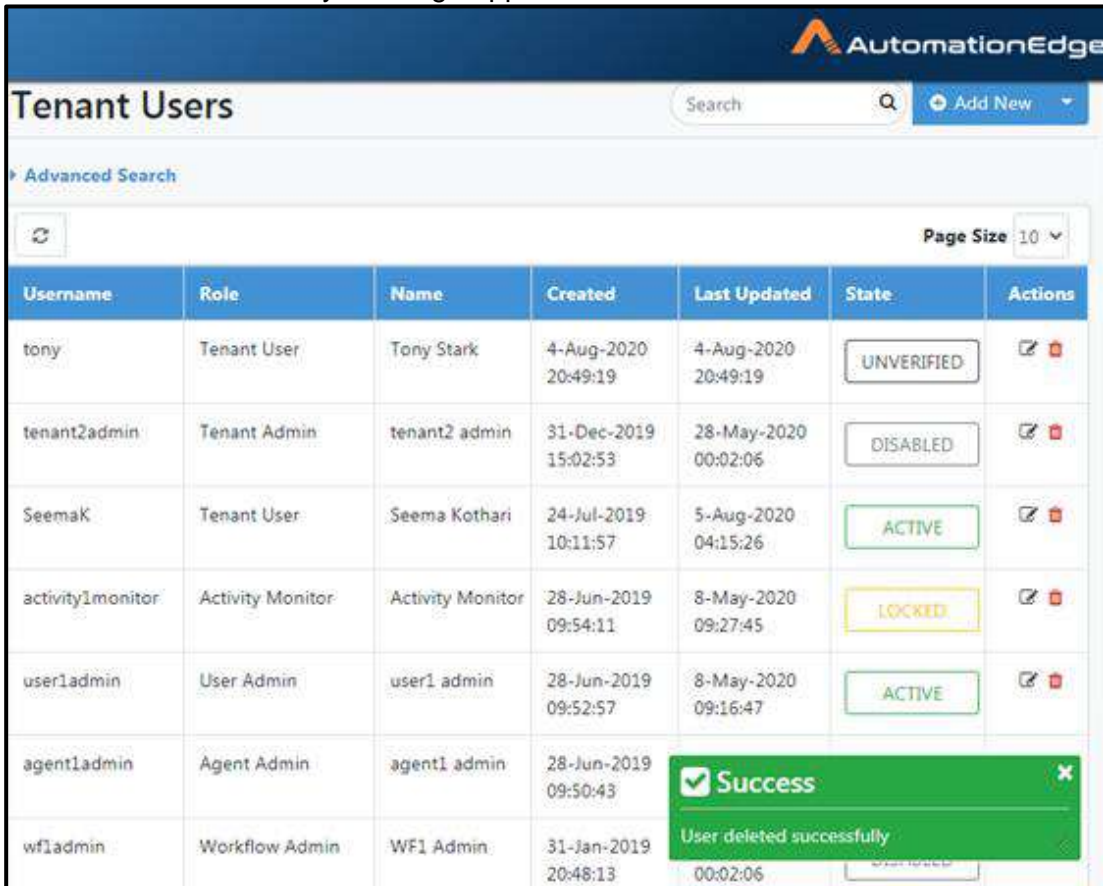


Figure 13c: User deleted successfully message

5.1.9 Tenant Users: Features/Permissions for other users

Table 12: Tenant Users Features

Feature/Role	Tenant Administrator	Workflow Administrator	User Administrator	Agent Administrator	Tenant User	Activity Monitor
Add New User Feature*	✓	-	✓	-	-	-
Upload Users	✓	-	✓	-	-	-
Advanced Search for Users	✓	-	✓	-	-	-
Edit/Delete	✓	-	-	-	-	-

Note: While Tenant Admin can create LDAP users with all roles, User Administrator can create LDAP users having Tenant user role only.

5.2 User Groups

5.2.1 Create New Group

Tenant users can be grouped together to form groups of users. These groups can then be used for assigning workflow permissions. A user can be present in more than one group.

To add user group:

1. Click Users.
2. Click User Groups.

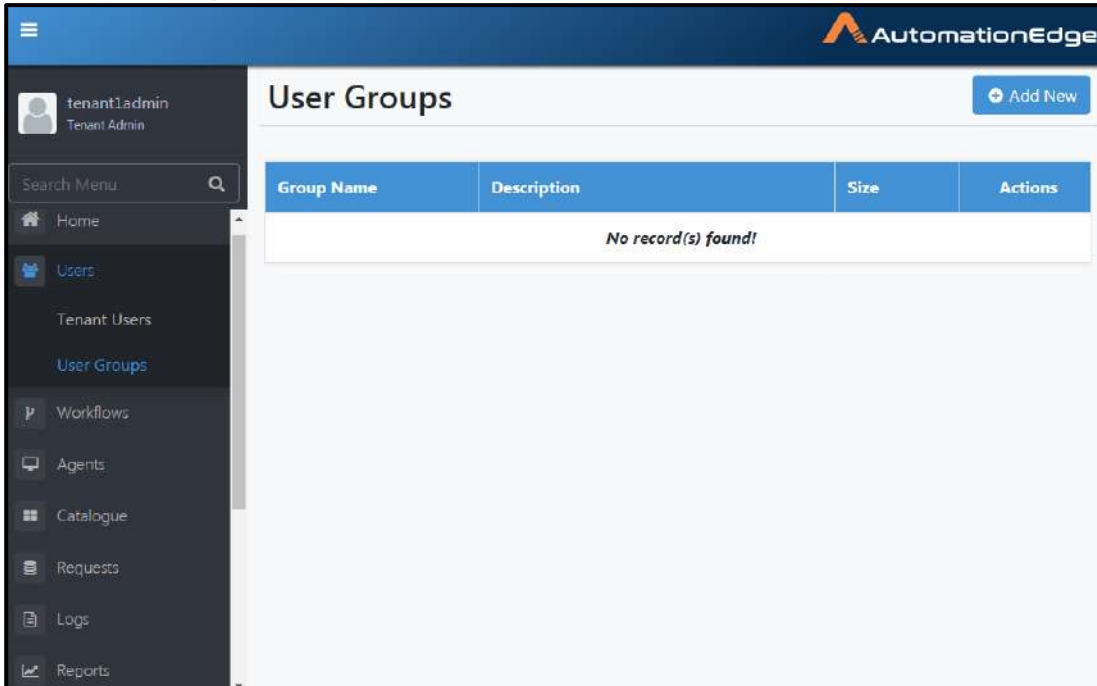
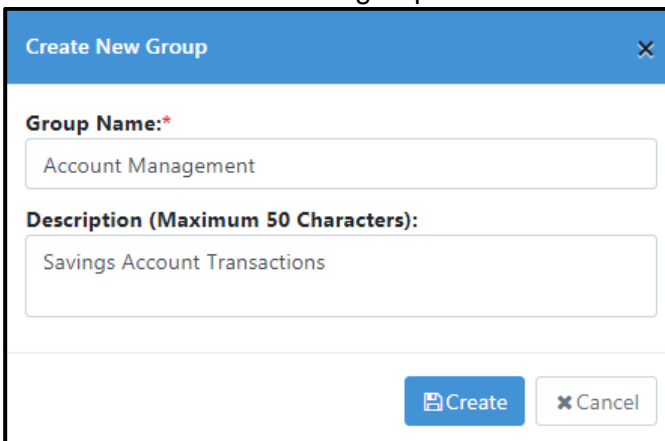


Figure 14a: Adding User Groups

3. Click Create New Group. Create New Group screen displays as shown below.
4. Enter Group Name and provide a description of the created group.
5. Click Create to create new group.



The "Create New Group" dialog box is shown. It has a blue header with the title "Create New Group" and a close button (X). The form contains two text input fields: "Group Name:" with the value "Account Management" and "Description (Maximum 50 Characters):" with the value "Savings Account Transactions". At the bottom right, there are two buttons: "Create" and "Cancel".

Figure 14b: Entering User Group Details

6. The new group is created as displayed below.

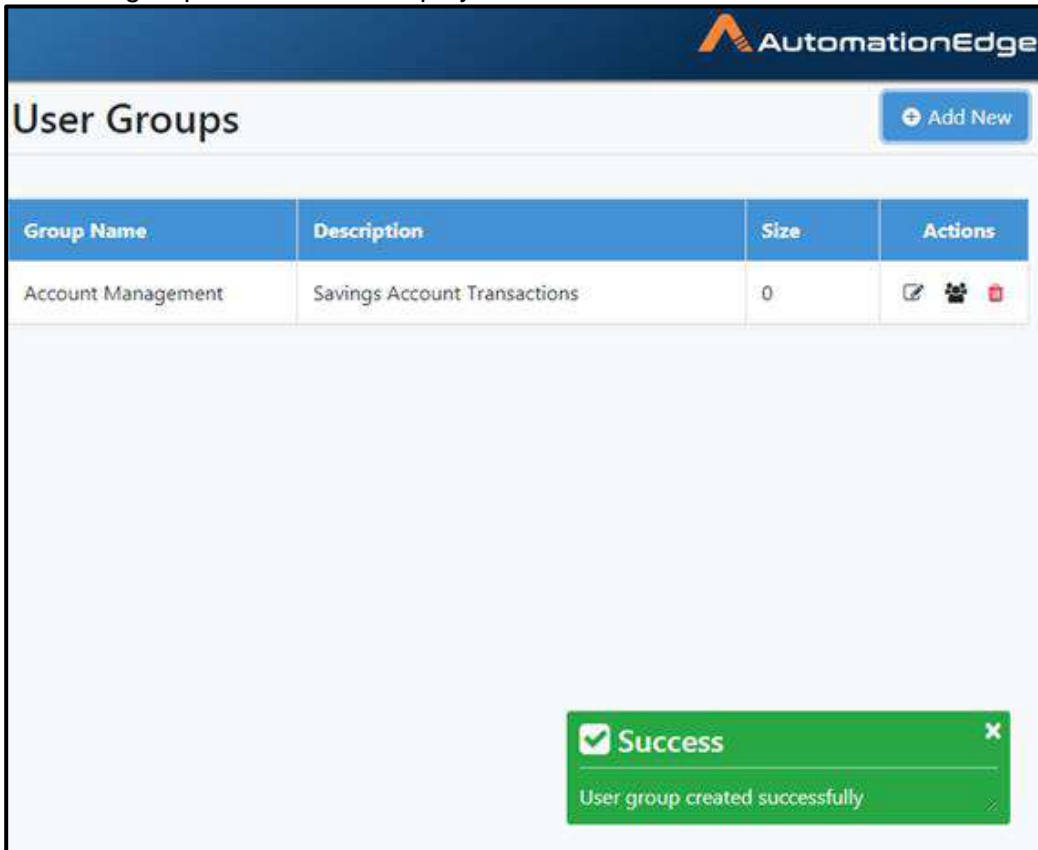


Figure 14c: User Group Creation Success message

A description of the fields is provided in the table below.

Table 13: Create New Group: Field/Button Description

Field Name	Description
Create New Group:	
Group Name	To specify user group name.
Description	To specify user group description.
Buttons:	
Create	To create a user group.
Cancel	To cancel creating a user group.

5.2.2 Search User Group

A list of all user Groups is available as a tabular display. There is no separate search field.

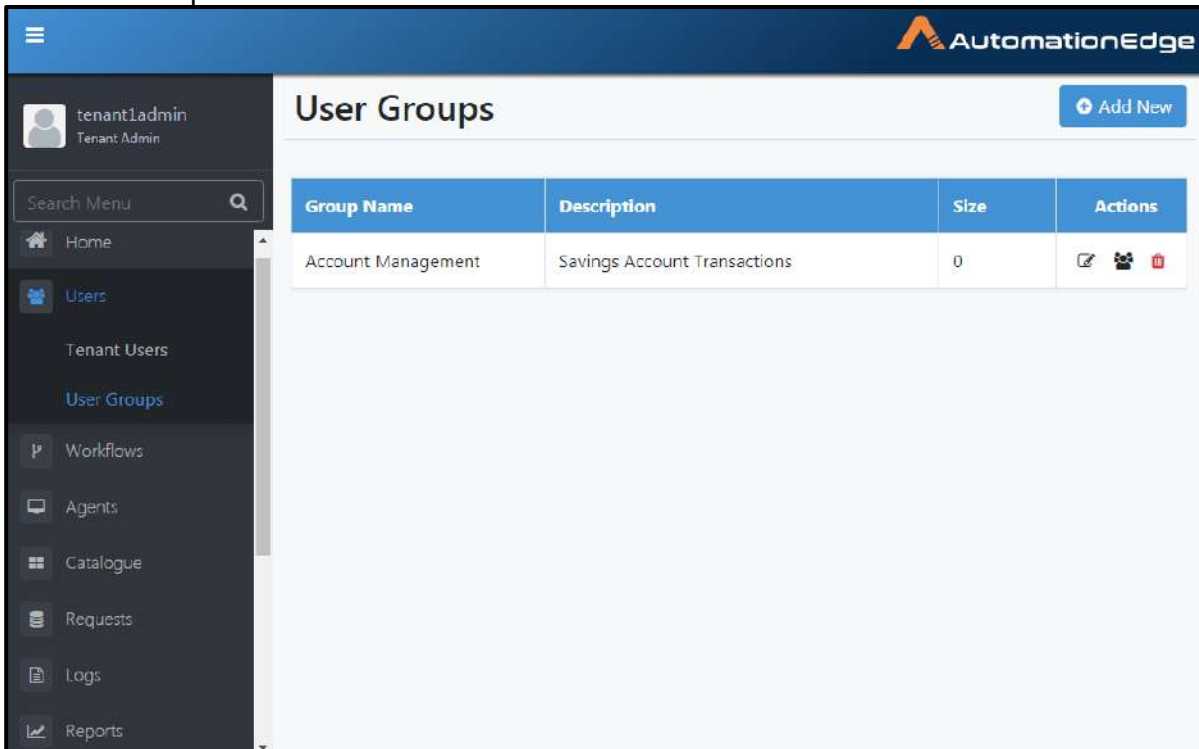


Figure 15: Search User Group

Table 14: Available User Groups Tabular Display

Name	Description
Group Name	Displays name of the user group.
Description	Displays user group description.
Size	Displays size of the group.
Actions:	Displays actions that can be performed on the user group.
Edit Group (✎)	To edit group.
Show Members (👥)	To view members of a group.
Delete Group (🗑)	To delete the group.

5.2.3 Edit User Group

To edit user group:

1. Click Users.
2. Click Users Groups.
3. Click the Edit icon (✎) corresponding to the user group you wish to edit.

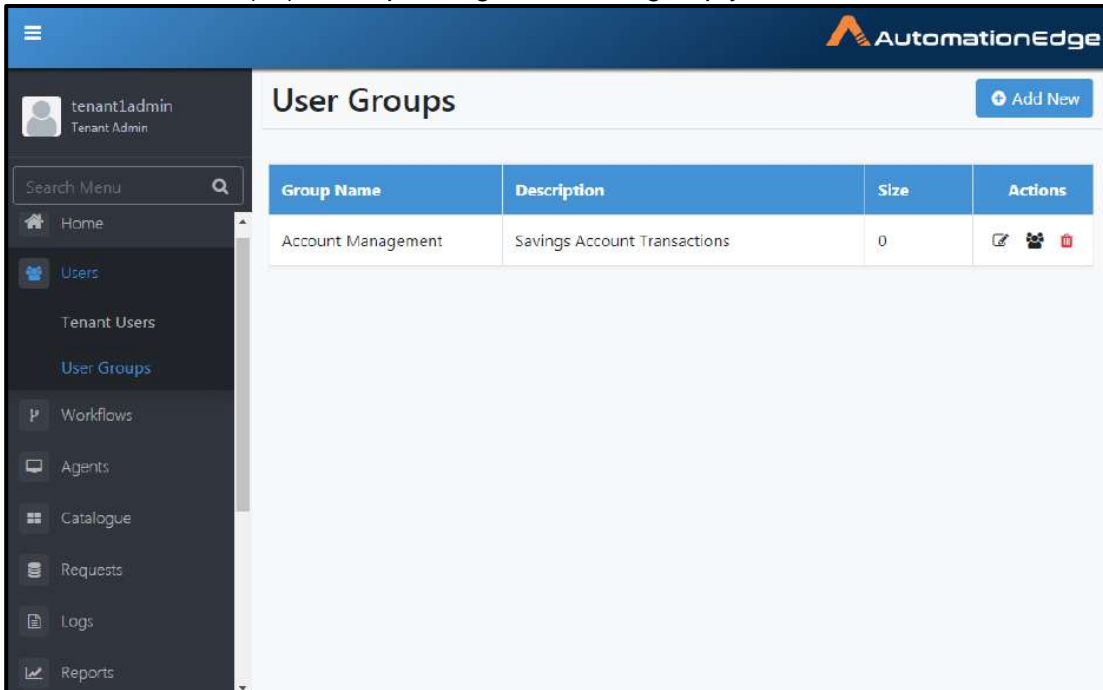
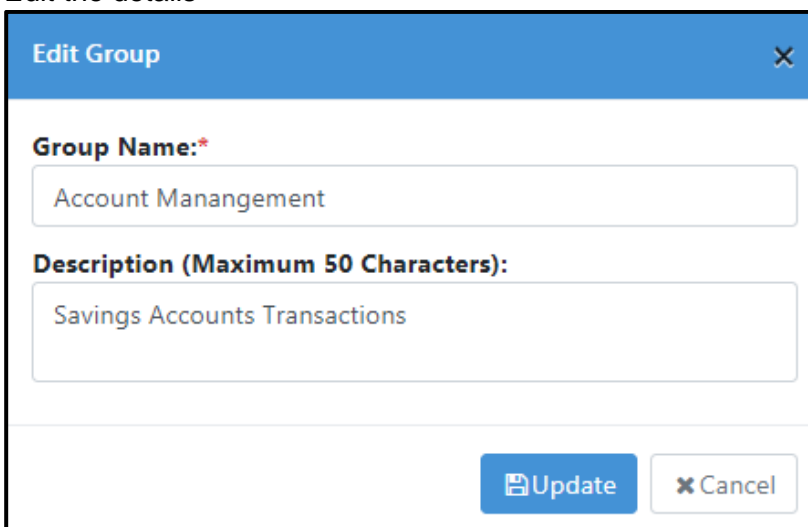


Figure 16a: Editing User Details

4. Edit the details



The "Edit Group" modal form contains the following fields and buttons:

- Group Name:** A text input field containing "Account Management".
- Description (Maximum 50 Characters):** A text input field containing "Savings Accounts Transactions".
- Update:** A blue button with a document icon.
- Cancel:** A button with an 'x' icon.

Figure 16b: Saving Edited User Group Details

5. Click Save to save the edited details.

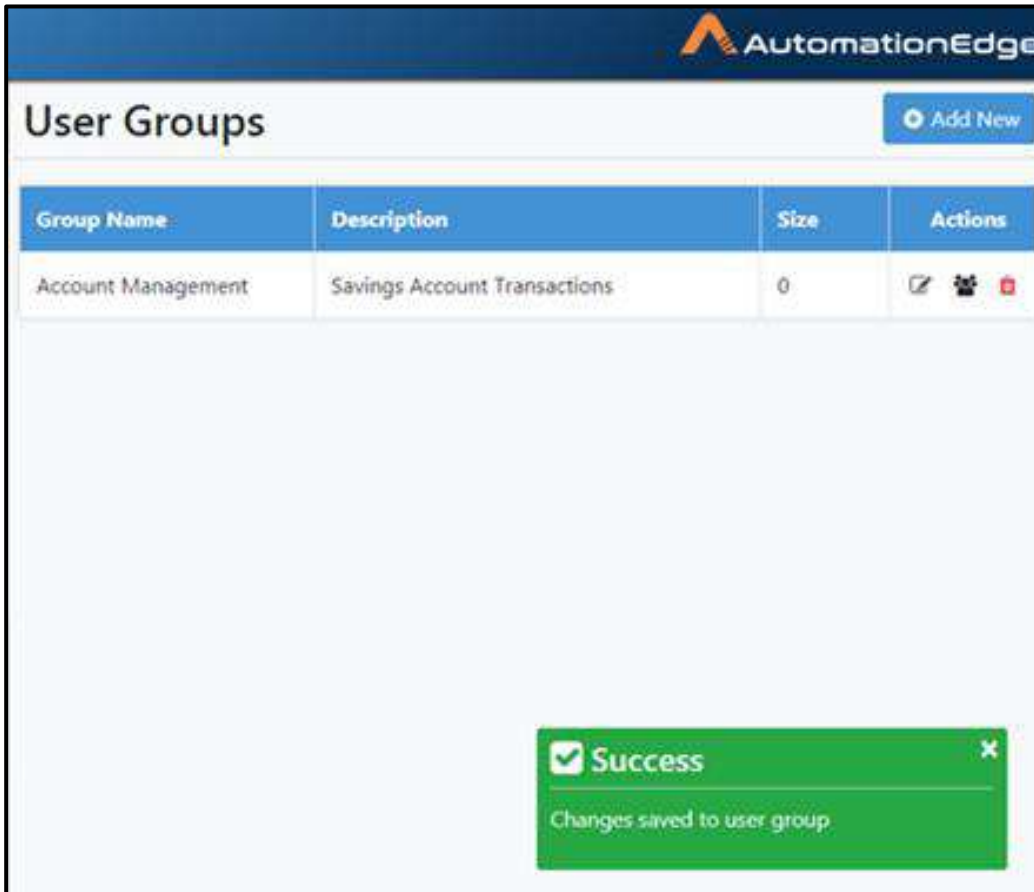


Figure 16c: User Group Edited Success Message

5.2.4 User Groups: Delete

Use this option to delete User Groups. However, if a user group is deleted all the user's loose membership of that group.

Following are the steps to delete a user group:

1. Navigate to the Users menu and User Groups sub-menu.
Click the Delete icon (🗑️) corresponding to the specific tenant user group you wish to delete, from the list.
2. Click Delete to confirm deletion of the user group.

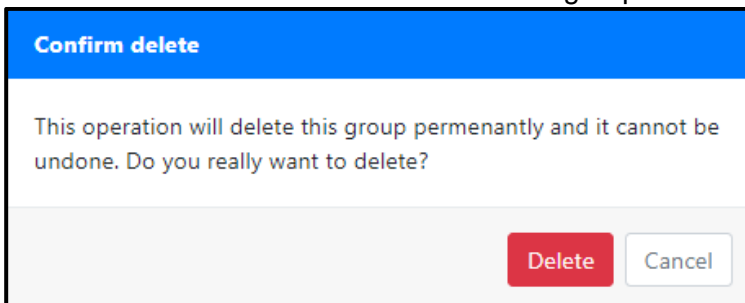



Figure 17a: Confirming User Group Deletion

3. A success message is displayed showing Group deleted successfully.

5.2.5 Adding User to a Group

To add a user to a group:

1. Navigate to the Users → User Groups menu.
2. Click show members () icon for a group.
3. Select the user in All Users list to add into Existing Members group.

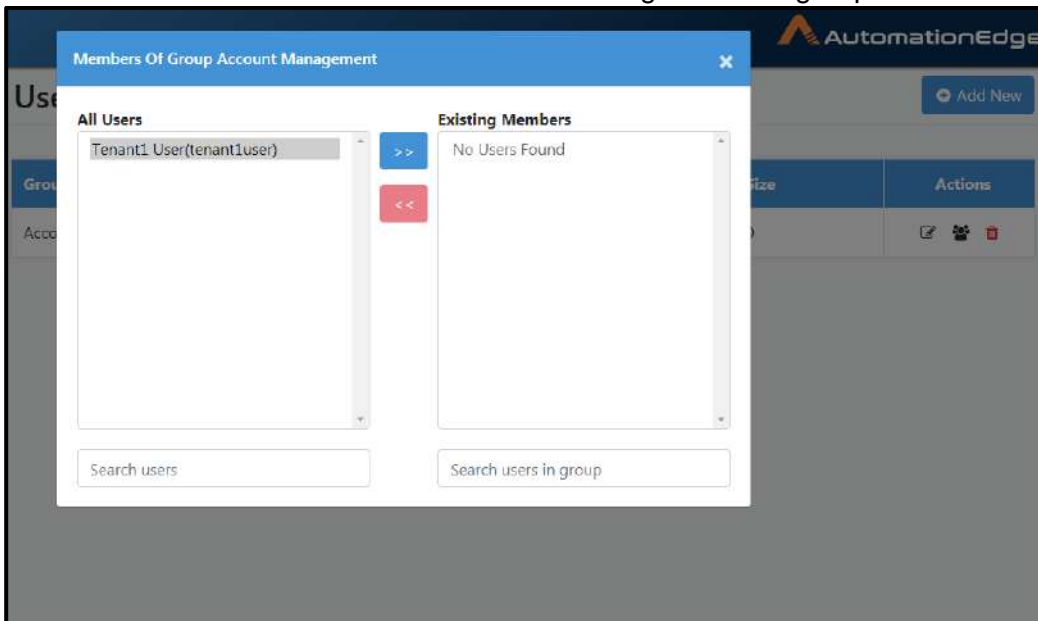


Figure 18a: Adding Users to a Group

4. Click Add. Selected user will be added to existing members group.

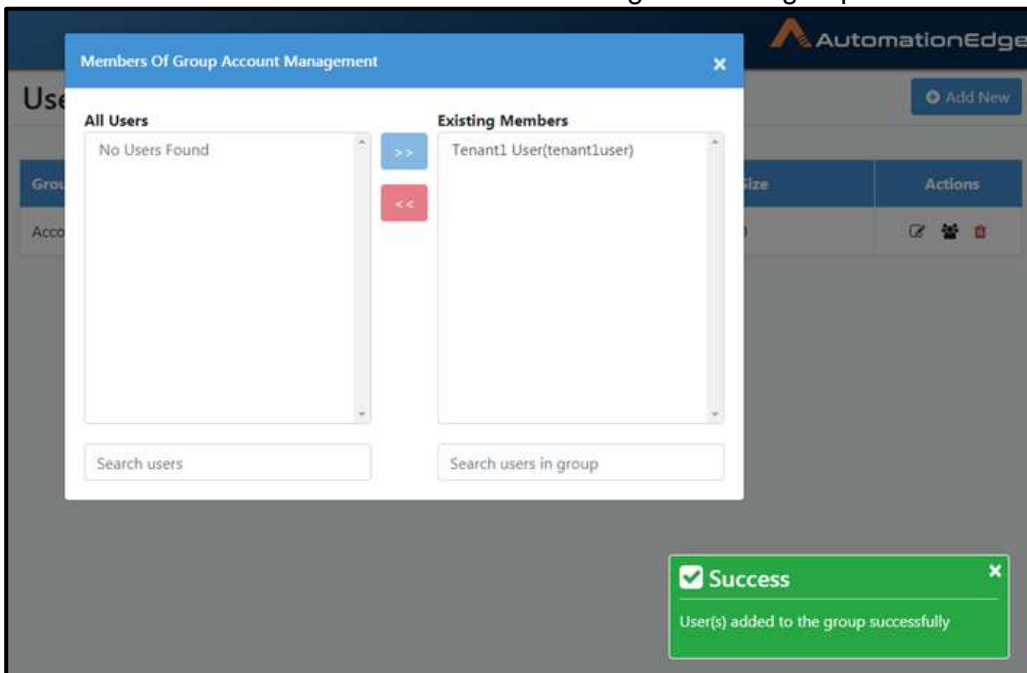



Figure 18b: User Added to the Existing Members Group

5.2.6 Removing User from a Group

To remove a user from a group:

1. Navigate to Users → User Groups. Click show members () icon for a group.
2. Select the user in Existing Members list to remove. Click on the red arrows to remove the user from the group.

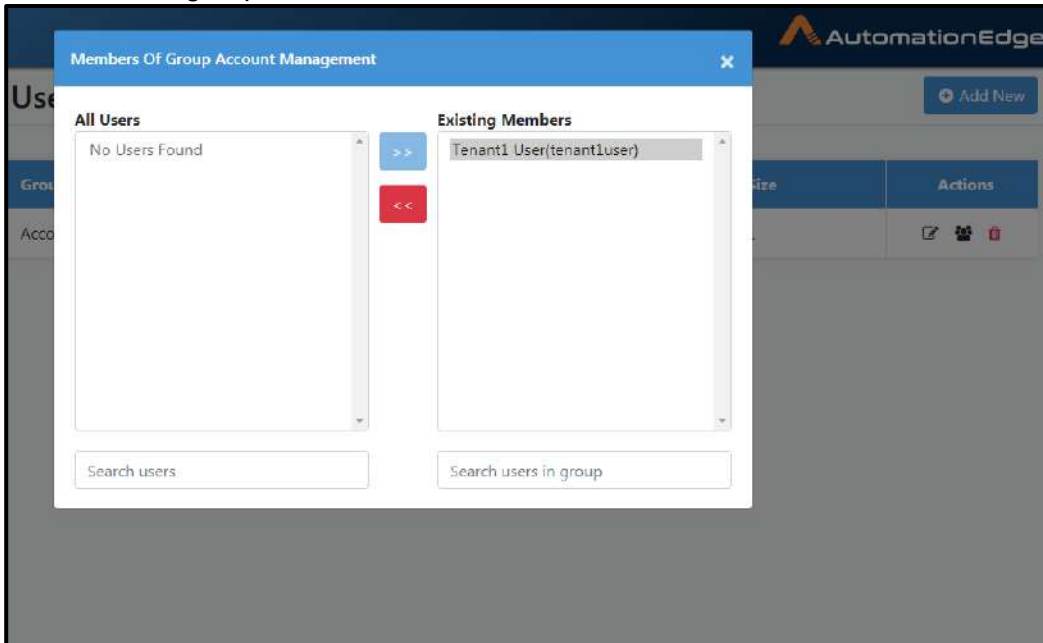


Figure 19a: Select members to remove

3. Selected user is removed from the group and a success message is seen.

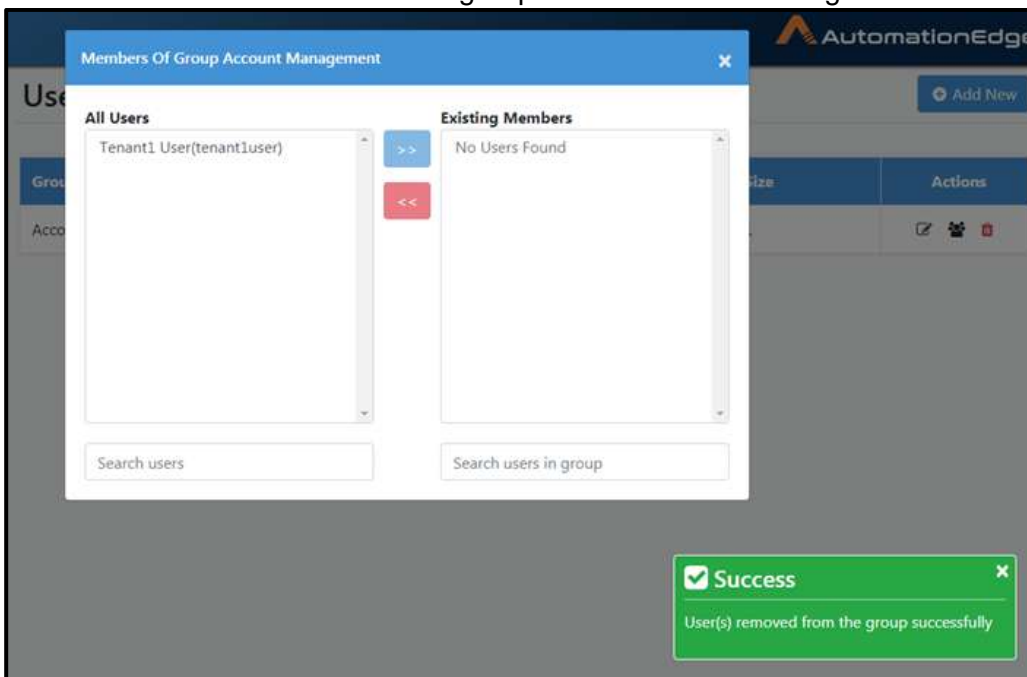


Figure 19b: User Removed from a Group

5.3 User Groups: Features/Permissions for other users

Table 15: User Groups Features

Feature/Role	Tenant Administrator	Workflow Administrator	User Administrator	Agent Administrator	Tenant User	Activity Monitor
Create User Group	✓	-	✓	-	-	-
Edit User Group	✓	-	✓	-	-	-
Delete User Group	✓	-	✓	-	-	-
Add User to Group	✓	-	✓	-	-	-
Delete User from Group	✓	-	✓	-	-	-

6 Workflows

Workflows are automation processes that can be invoked. Workflows automate real-life processes by automating the execution of tasks. A workflow consists of steps which help in designing or customizing a workflow.

Table 16: Workflow Menu Description

Sub-Menus	Description
Workflow List	Using this sub-menu, you can add new workflow, search, edit, delete, activate, and deactivate workflow.
Scheduler	Using this sub-menu, you can add, search, edit, delete, activate, deactivate and transfer workflow schedules.
Categories	Using this sub-menu, you can create workflow categories and move workflows to different categories.
Credentials	Using this sub-menu, you can create, edit and delete credential pools and credentials. You can also move credentials to credential pools.

6.1 Publishing Workflows: General Flow

Following is the general flow to publish Process Studio Processes/Workflows to AutomationEdge.

1. Publish to Development Instance
2. Export from Development Instance
3. Import to UAT Instance
4. Export from UAT instance
5. Import to Production (Enterprise or Subscription) instance

6.2 Publish to Development Instance

Workflows: Publish Project from Process Studio

Process Studio projects can be published to AutomationEdge using the following options,

- Process Studio Publish → Create or
- Process Studio Publish → Update

The following sections discuss Process Studio Publish (Create & Update) options to publish AutomationEdge workflow on a Development instance.

6.2.1.1 Publish: Create

In this exercise, we will publish a project (Sales Revenue) for the first time using Process Studio Publish→Create option. Following are the steps to publish an AutomationEdge workflow using Process Studio Publish option,

1. Open Sales Revenue Project in Process Studio.
2. Select File menu and click Publish and then on Create option.
3. Alternately, right-click on the project to be published, as seen below.

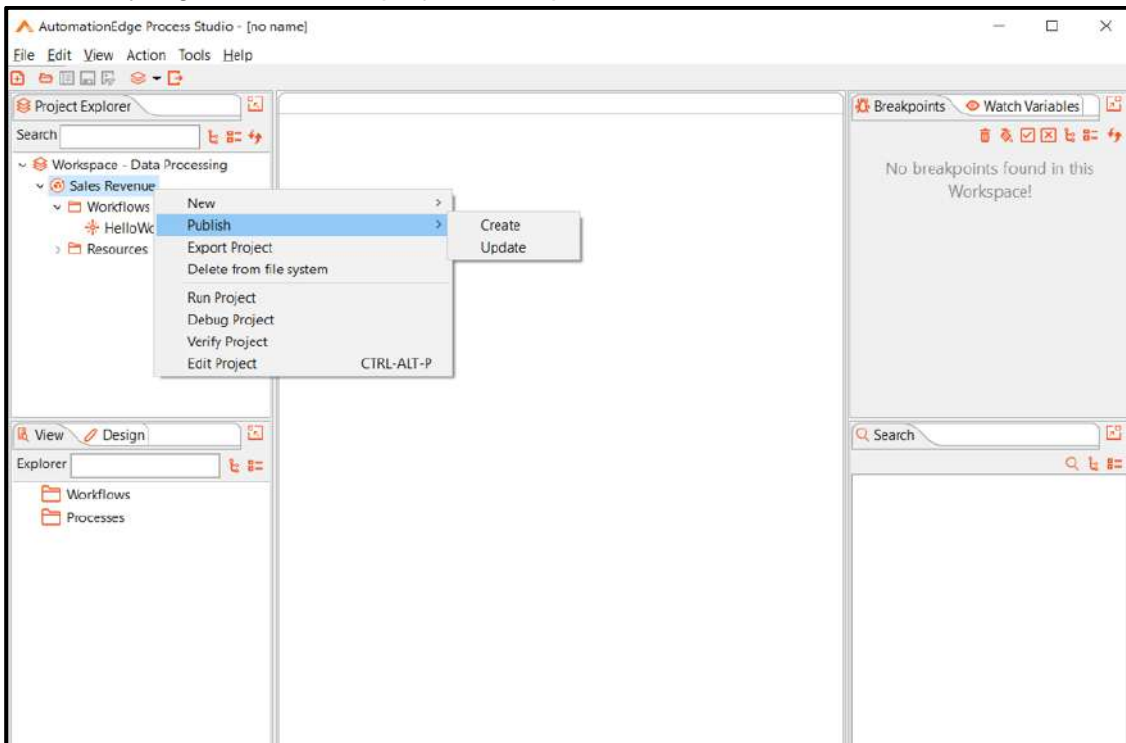


Figure 20a: Publish Sales Revenue Project

4. However, we receive an error message popup with a message - Main file is not specified for the project.
5. When you publish a project, you need to set the main file by editing the project. It is self-evident when the project has multiple processes/workflows, where you need to select the parent process/workflow as the main workflow/process by editing the project.

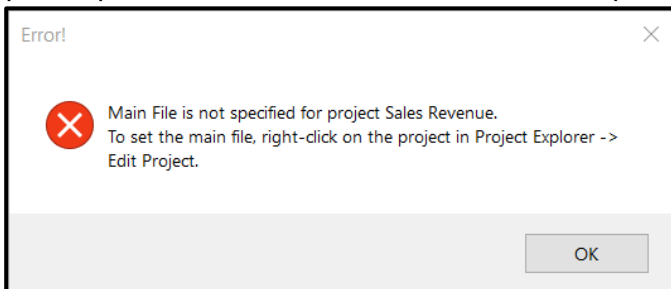


Figure 20b: Main File for Project not specified

6. To set the Main workflow/process right click the project and select Edit Project.

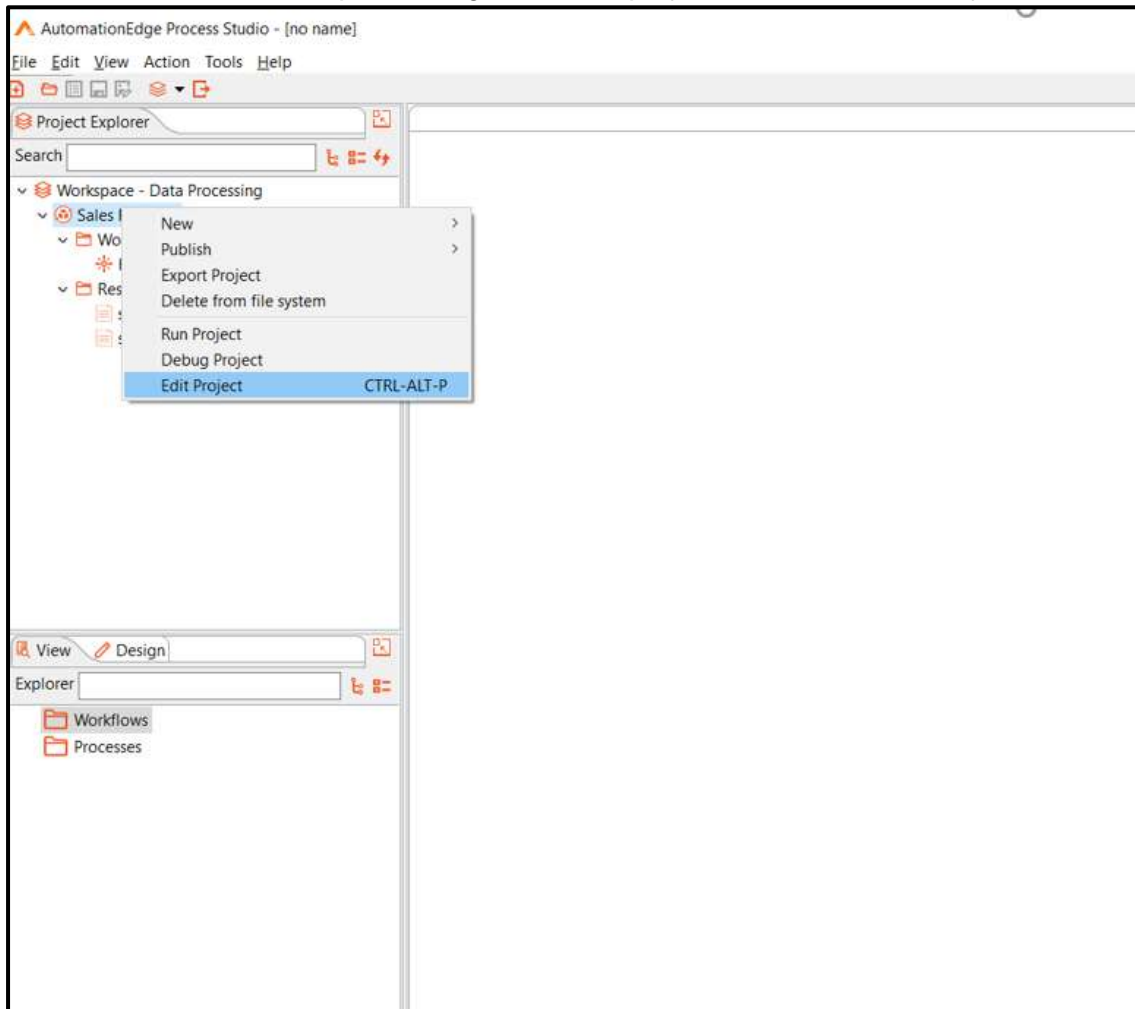


Figure 20c: Edit Project

- In the Main workflow/process field Browse your main workflow/process as seen below.

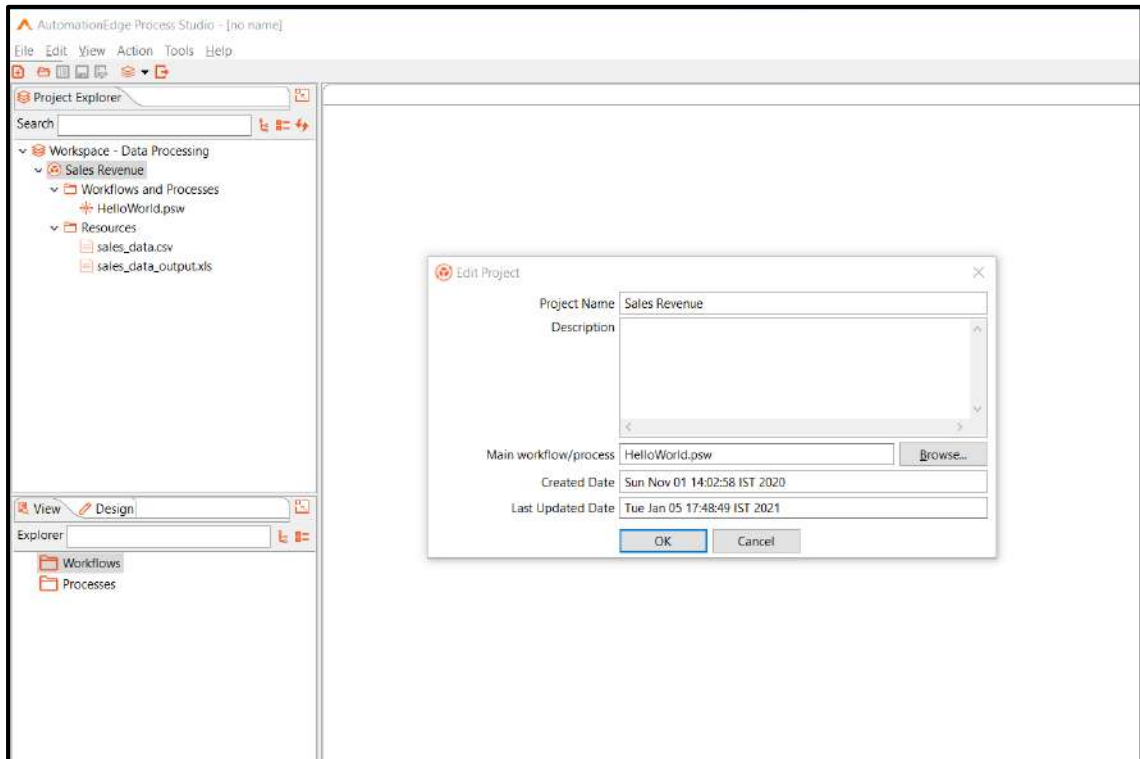


Figure 20d: Set Main workflow/process

- If you have a Process and multiple workflows, then open the parent Process or parent Workflow and go to the respective tab.
- Once again, go back to the Publish→Create option under the File menu.
- If you have not saved the password, the AutomationEdge connection Details dialog appears. Provide the password.

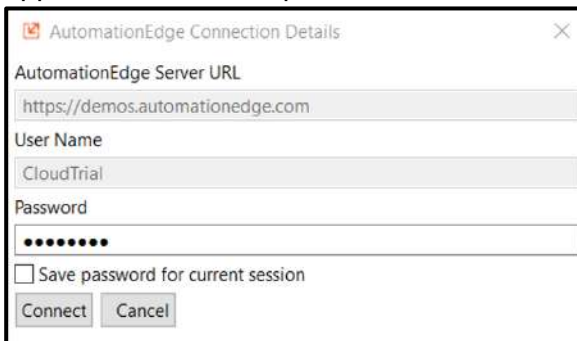


Figure 20e: AutomationEdge Connection

11. A pop-up message appears warning that you must select a parent process(psp) or workflow(psw) as the case may be so that all the linked psp/psw files are exported into a zip. Acknowledge the message.

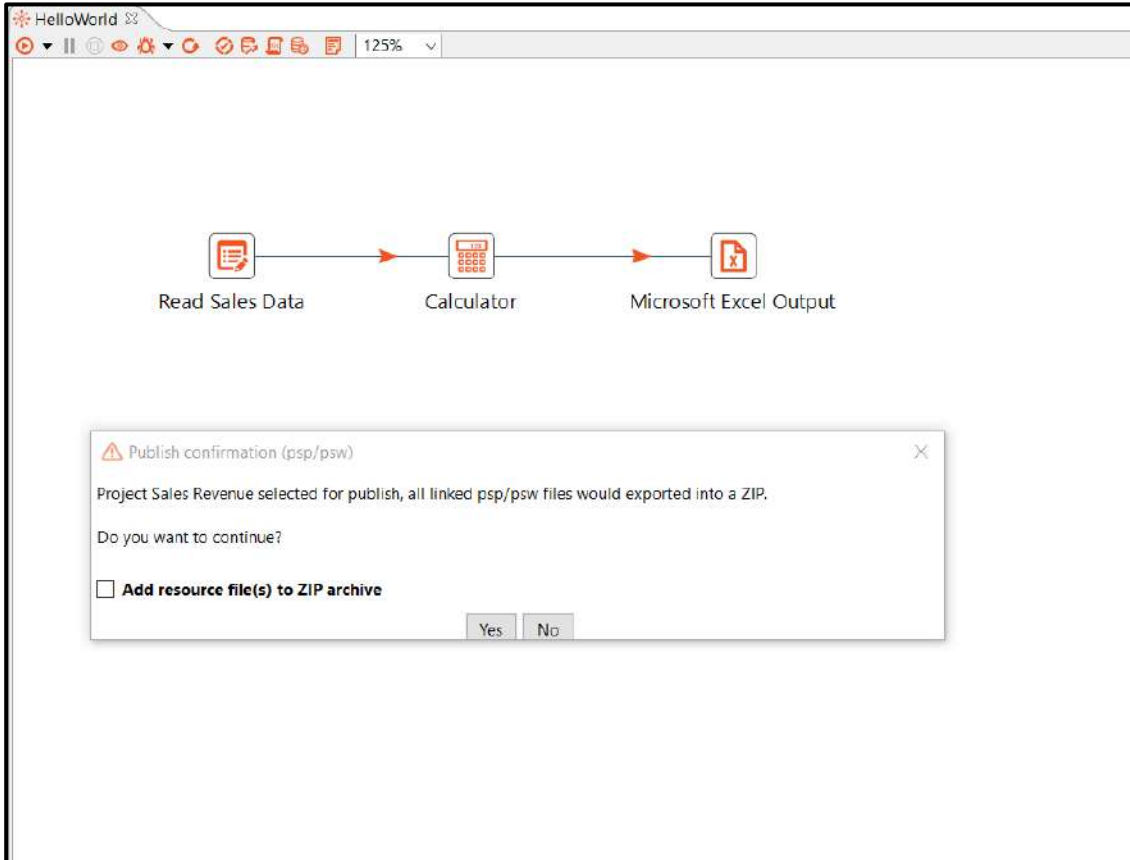


Figure 20f: Publish Confirmation

12. In case you check 'Add supporting files to zip archive,' a corresponding popup appears. In this case, there are no supporting .csv, .txt, .xlsx or other files. Leave 'Add supporting files to zip archive' unchecked and click Yes.

13. A Workflow Details pop up appears with details as seen below.
 - Enable Assisted for Attended workflows
 - Enable RDP enabled if working on Controller Agent machine.
 - If you wish to Set default values as Configuration parameter values, enable the check box.
 - Note:
 - Workflows which need to be executed sequentially are automatically detected as *Sequential*, (else if one of the sequential automation workflows is running as non-sequential, and the workflow is terminated, then all the subsequent requests remain in New state). This workflow is not sequential.
14. Click Create.

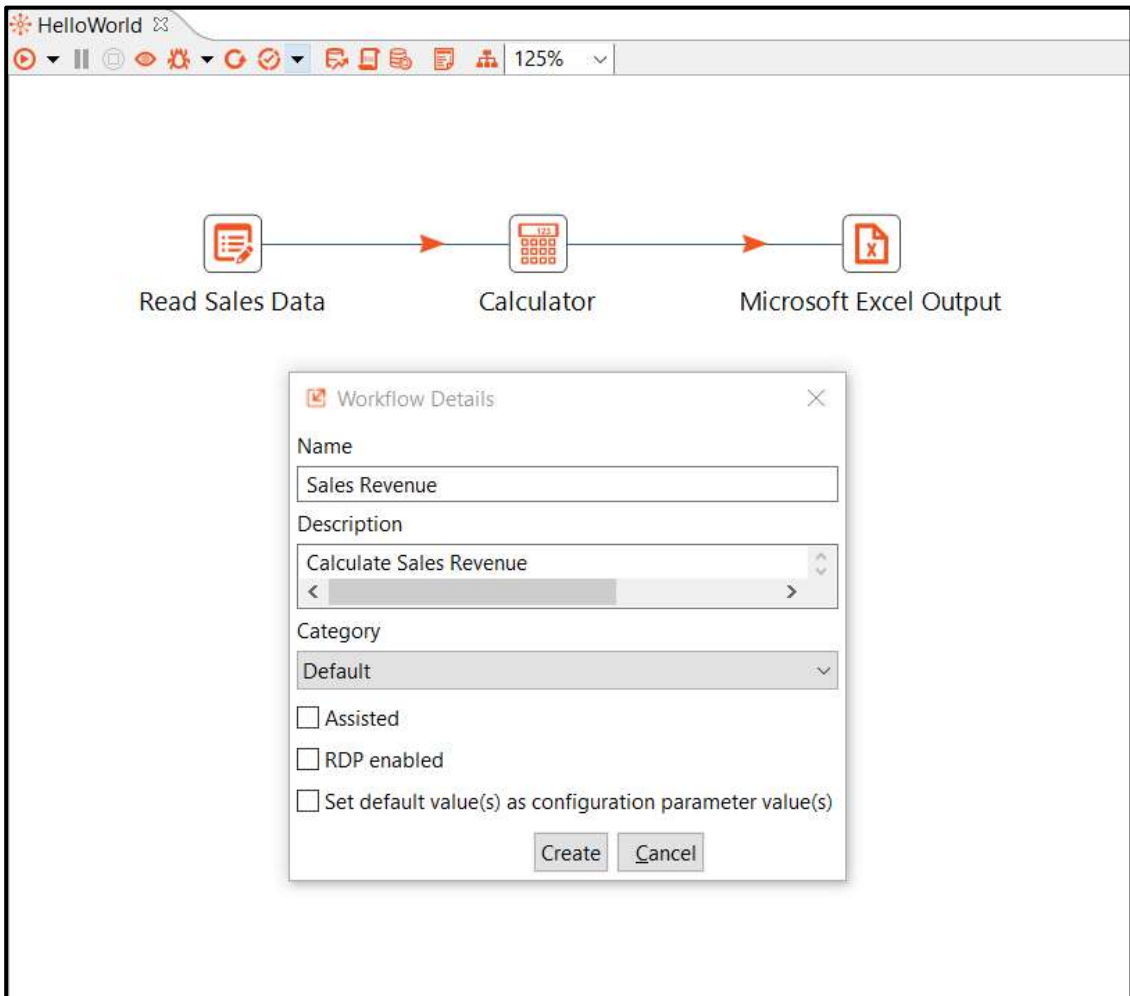


Figure 20g: Workflow Configurations

 **Note:** For a detailed description of Workflow configuration fields refer to [Table 17: Add Workflow Details Field Description](#)

15. A pop-up message appears showing Workflow created successfully, and publish operation is completes.

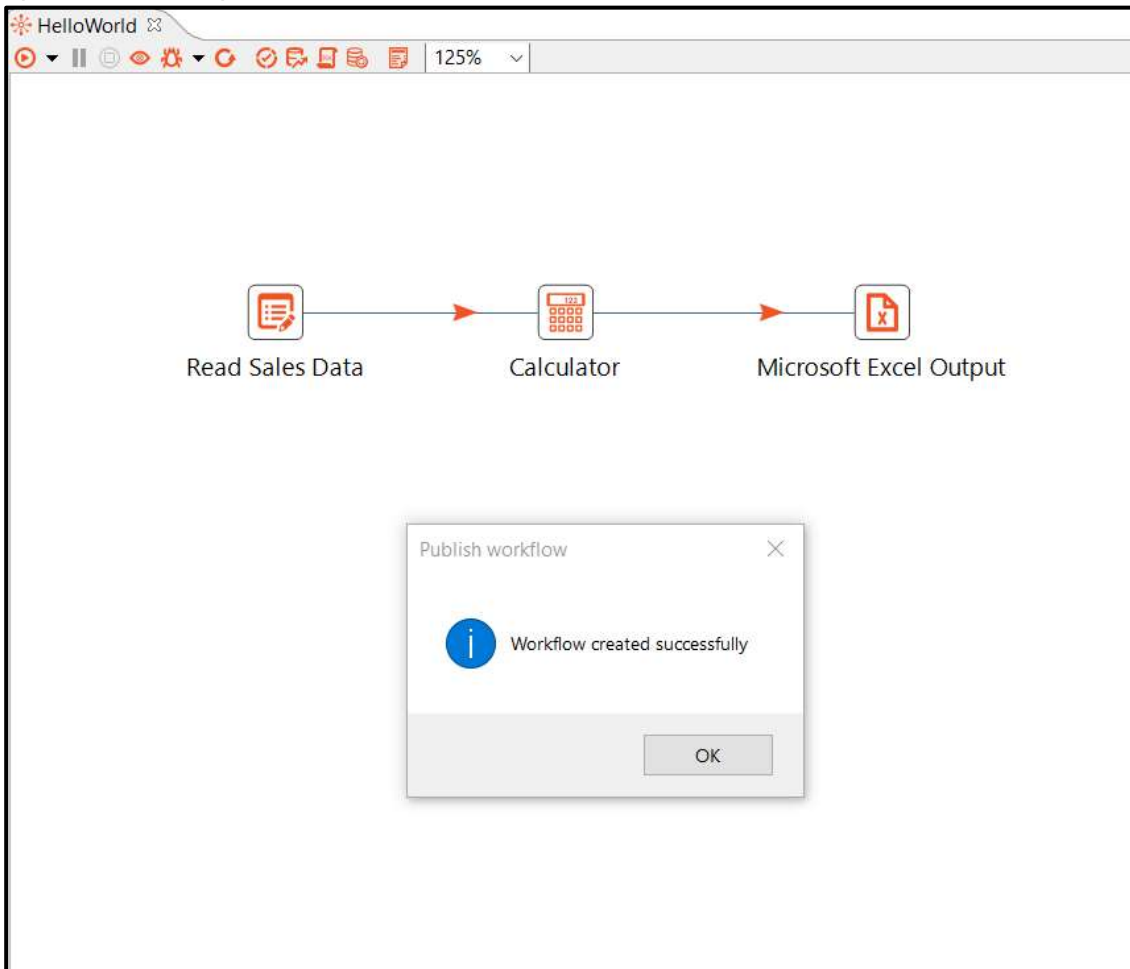


Figure 20h: Workflow created pop-up message

16. Now log on to the AutomationEdge instance on which you created the workflow. In the Workflow List menu, you can see the newly published Sales Revenue workflow.
17. At this point, you cannot yet activate the workflow. Hover over the Activate toggle switch to see the message Workflow not configured yet.

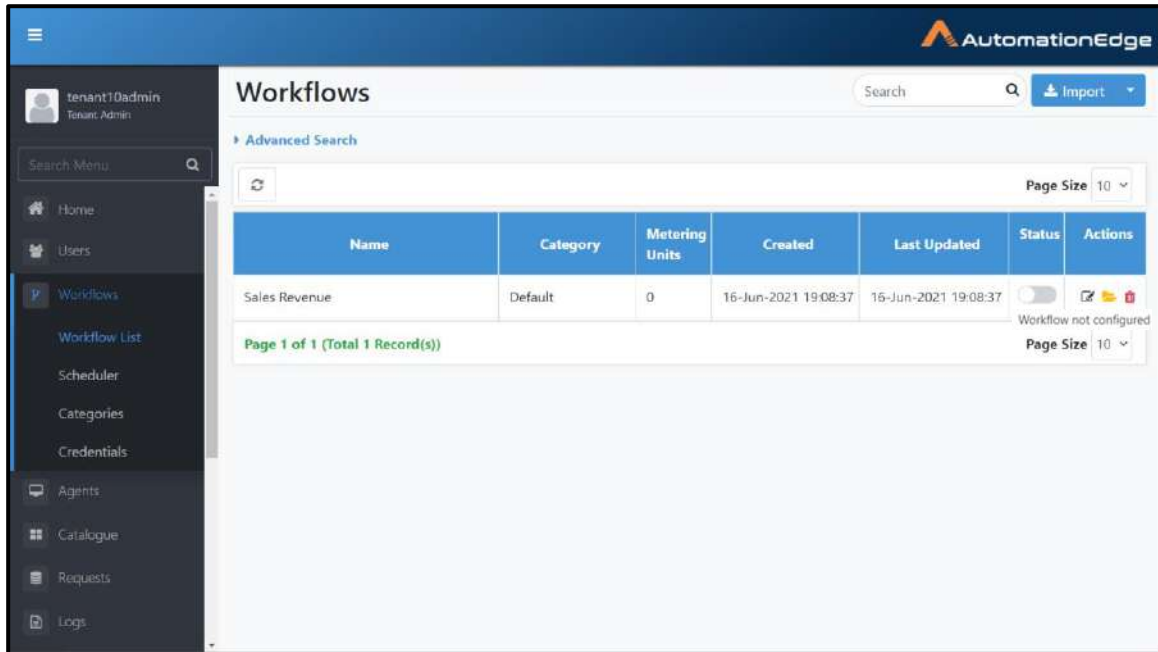


Figure 20i: View newly published workflow

18. Click the edit icon in the Actions column to complete workflow configuration. As seen below, most of the basic details are present. Unlike Process Studio the Enable Sequential Execution checkbox is visible in workflow configurations. Since this is not a GUI Automation workflow the checkbox is unchecked.
19. Additionally, configure Expected Completion Time, Maximum Completion Time, Cleanup Requests older than and Manual Execution time.


Configure Workflow Details

Workflow Name: **Sales Revenue**

Workflow Description (Maximum 128 Characters): *

Workflow Category:

Default ▼

Workflow Icon: 

Assisted Workflow : **false**

Enable Sequential Execution

Enable RDP

Enable Input Attributes

Workflow Priority:

Default ▼

Expected Completion Time(Seconds): *

Maximum Completion Time(Seconds): *

Cleanup Requests older than(Hours):

Manual Execution Time:

 Minutes ▼

[▶ Email Notification Setting](#)

No Configuration Parameters




Figure 20j: Configure workflow basic details

20. Configure Email Notification Setting as seen below.
21. Click Save.

Configure Workflow Details

▼ Email Notification Setting

Notify On Workflow Failure

Notify On Exceeding Time Limit

Select Users*:

By Role: Tenant Admin Workflow Admin

By Username:

By Email:

Request Creator

Failure Message:

No Configuration Parameters




Figure 20k: Configure email notification

Table 17: Add Workflow Details Field Description

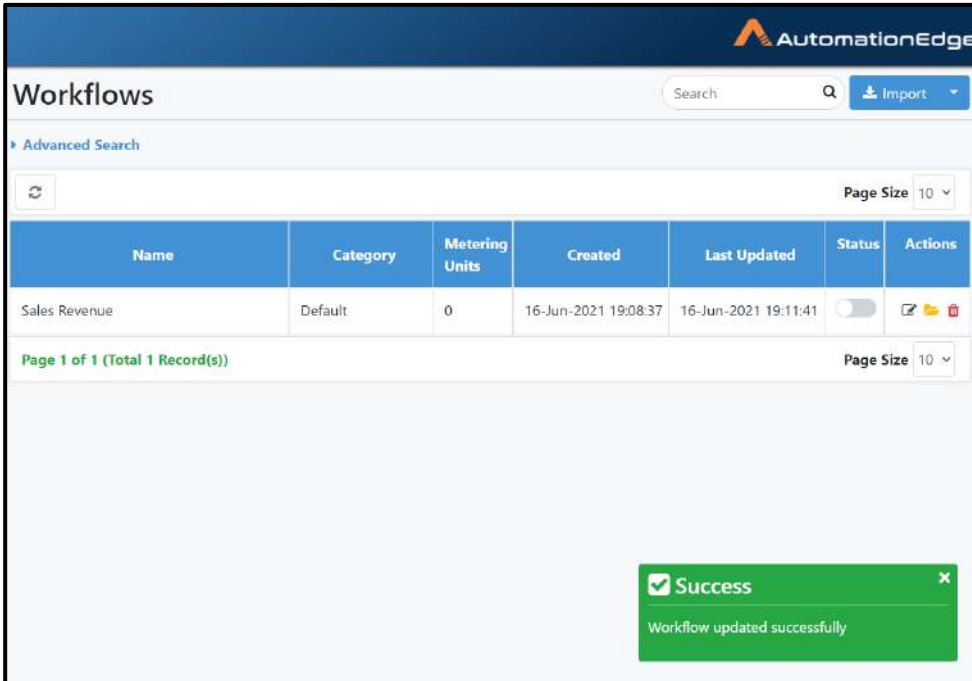
Field Name	Description
Basic Details:	
Workflow Name	Specify workflow name. This field is Mandatory.
Workflow Description	Specify workflow description. This field is Mandatory.
Workflow Category	Select the workflow category from the drop-down list.
Workflow Icon	Browse to upload icon for workflow.
Assisted Workflow	<p>Enable this checkbox to execute this workflow as an assisted workflow only. The workflow will not be available to run on regular Agents. While updating a Workflow, one will not have the option to switch between assisted and unassisted Workflows. Also, when a Workflow is marked as assisted, it automatically becomes sequential.</p>
Enable Sequential Execution	<p>Enable the checkbox for the workflow's sequential execution.</p> <p>At any given time, only one sequential workflow can run on an agent (If one of the automation workflows with these steps is running as non-sequential, and the workflow is terminated, then all the subsequent requests remain in New state).</p> <p>During Publish, Process Studio marks workflows with the following steps as sequential.</p> <p>(Mainly UI workflows are marked as sequential workflows. The non-UI workflows can run in parallel). The Enable Sequential Execution checkbox is automatically checked on the AutomationEdge UI workflow edit page. The workflow can be considered auto-sequential otherwise, uncheck it.</p> <ul style="list-style-type: none"> • Robot Handling step • Capture Screenshot step • Desktop steps • GUI Automation Windows steps • Surface Automation steps • AS400 • Auto IT <p>In this example, the workflow does not have one of these steps; hence it will not be sequential.</p>

<p>Enable RDP</p>	<p>Enable checkbox to start an RDP session of Agent machine to which workflow is assigned on the Controller Agent machine.</p> <p>When 'Is RDP Enabled' is checked 'Is Sequential Execution' is automatically checked, since RDP is generally required for sequential workflows that need an active screen.</p> <p>Agent must be running to request RDP for RDP Enabled workflows and execute the workflows. However, make sure no console session or RDP session is active.</p> <p>For requisite Windows Policy Changes for Is RDP Enabled workflows refer section: Windows Remote Desktop policies for RDP enabled workflows</p> <p>Use cases for Is RDP enabled workflows</p> <ul style="list-style-type: none"> • Idle Timeout Since RDP Session is taken only for workflow execution, the idle timeout on the Agent machine should match the max execution of the workflow. • Reconnect RDP Session will try to reconnect to the Agent VM during workflow execution in case the reason for disconnect is other than normal disconnect event initiated from the Agent VM. • Controller Shutdown When the controller is shutdown, it won't close the Active RDP sessions, since workflow execution is active. • Workflow Hangs/Infinite execution In case a Desktop Workflow hangs, it needs to be terminated manually and then RDP session is closed by Agent. Till this happens No other RDP based workflow will be able to run on the Agent. • Workflow execution initiation timeout In case the RDP session does not get connected within a specific time period (2 mins), the workflow request fails with this reason. • Banners Usually there are banners when a user logs in to a machine, (e.g. This Server is Property of)These banners will need to be disabled to use Automatic login.
-------------------	--

Enable Input Attributes	<p>Enable checkbox to display Additional Input Attributes in the Parameter Form displayed during workflow execution from AutomationEdge Catalogue. These are used to capture additional information.</p>
Workflow Priority	<p>Workflow priority is visible after the workflow is created in Edit mode.</p> <p>With this feature workflow requests can be prioritized. Priority can be set on workflows so that workflow requests are executed according to the priority.</p> <p>The field for priority supports three priorities Low, Default and High. Workflow editor can set its value to Low, Default or High. The value can be set while creating or updating workflow configuration.</p> <p>Once the priority is set, all the requests submitted after that will run with specified priority. Once the request is submitted, its priority cannot be changed.</p> <p>High priority workflow requests will be processed before low and default priority requests. Default priority requests will be processed before low priority requests. Among the requests with the same priority; requests will be processed in 'First In First Out' manner.</p> <p>To enable this feature, some configuration changes are required in ActiveMQ configuration. To enable priority following changes need to be done in activemq.xml present in activemq's conf folder.</p> <p>Add prioritizedMessages="true" property for policyEntry queue=">" tag</p> <pre data-bbox="662 1459 1302 1774"> <destinationPolicy> <policyMap> <policyEntries> <policyEntry queue=">" prioritizedMessages="true"/> </policyEntry> ... </policyMap> </destinationPolicy> </pre> <p>ActiveMQ and server needs to be restarted after this change.</p>

Expected Completion Time (seconds)	Specify expected time to complete a workflow from the time it is triggered. This field is Mandatory.
Maximum Completion Time (seconds)	Specify maximum time to complete a workflow from the time it is triggered. This field is Mandatory.
Clean-up Requests older than(Hours)	Requests in 'New' status older than number of hours provided will be marked as "Expired".
Email Notification Setting:	If SMTP not configured for the tenant, email notifications cannot be enabled. If SMTP is configured Email Notification can be setup as follows.
Notify On Workflow Failure	Enable checkbox to notify selected users on workflow failure.
Notify On Exceeding Time Limit	Enable checkbox to notify selected users on workflow exceeding time limit.
Select user:	
By Role:	All users with a particular role can be notified
Tenant Administrator	Enable checkbox to notify all Tenant Administrators.
Workflow Administrator	Enable checkbox to notify all Workflow Administrators.
By Username:	Provide a list of usernames to be notified.
By Email:	Provide a list of email addresses to be notified.
Request Creator	Enable checkbox to notify request creator.
Failure Message	Write a free text Failure Message for the notification.
Configuration Parameters	<p>Configuration Parameters are the workflow parameters that are set while defining workflow. The same values of configuration parameters are supplied to the workflow every time it is run. Typically, configuration parameters contain details for connecting to the external servers.</p> <p>Configuration parameters can be of the type String, File, Boolean, Number, Integer, Date and Credential. For date a Boolean Picker is provided in the UI while for other types, the corresponding type validation is provided.</p>
Buttons:	
Save	Save configured workflow details.
Cancel	Cancel configuring workflow.

22. Workflow updated successfully message appears.



The screenshot shows the AutomationEdge Workflows interface. At the top, there is a search bar and an 'Import' button. Below that is an 'Advanced Search' section with a refresh icon and a 'Page Size' dropdown set to 10. A table lists workflow records with columns: Name, Category, Metering Units, Created, Last Updated, Status, and Actions. The first row shows 'Sales Revenue' with a status of 'Off'. Below the table, a green success message box displays a checkmark, the word 'Success', and the text 'Workflow updated successfully'.




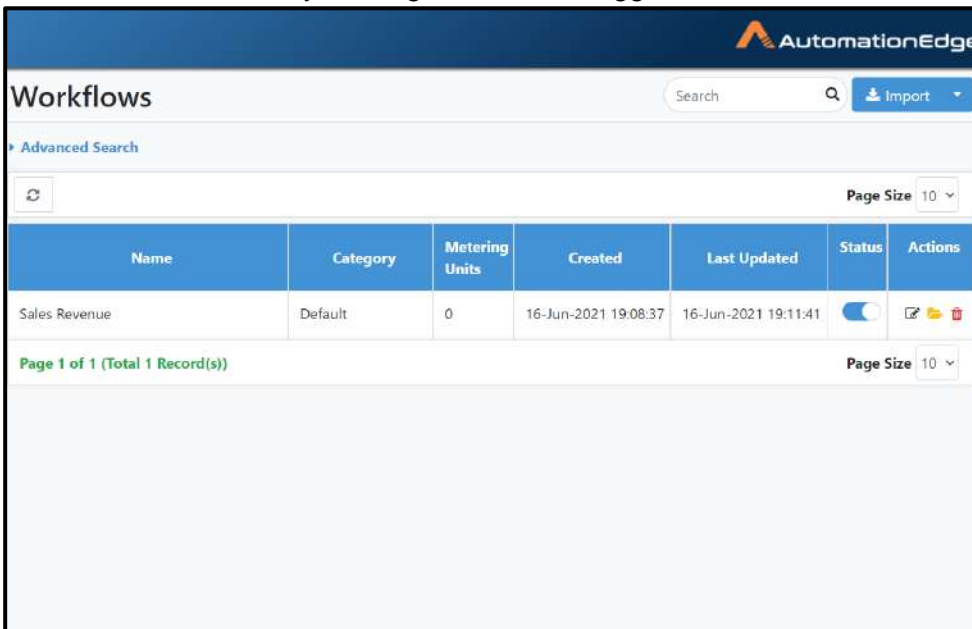
Name	Category	Metering Units	Created	Last Updated	Status	Actions
Sales Revenue	Default	0	16-Jun-2021 19:08:37	16-Jun-2021 19:11:41	Off	  

Figure 20l: Workflow updated with configurations

23. Activate the workflow by clicking the activate toggle switch.



The screenshot shows the AutomationEdge Workflows interface. The table from the previous screenshot is shown again, but the 'Status' for 'Sales Revenue' is now 'On', indicated by a blue toggle switch. The success message box is no longer present.




Name	Category	Metering Units	Created	Last Updated	Status	Actions
Sales Revenue	Default	0	16-Jun-2021 19:08:37	16-Jun-2021 19:11:41	On	  

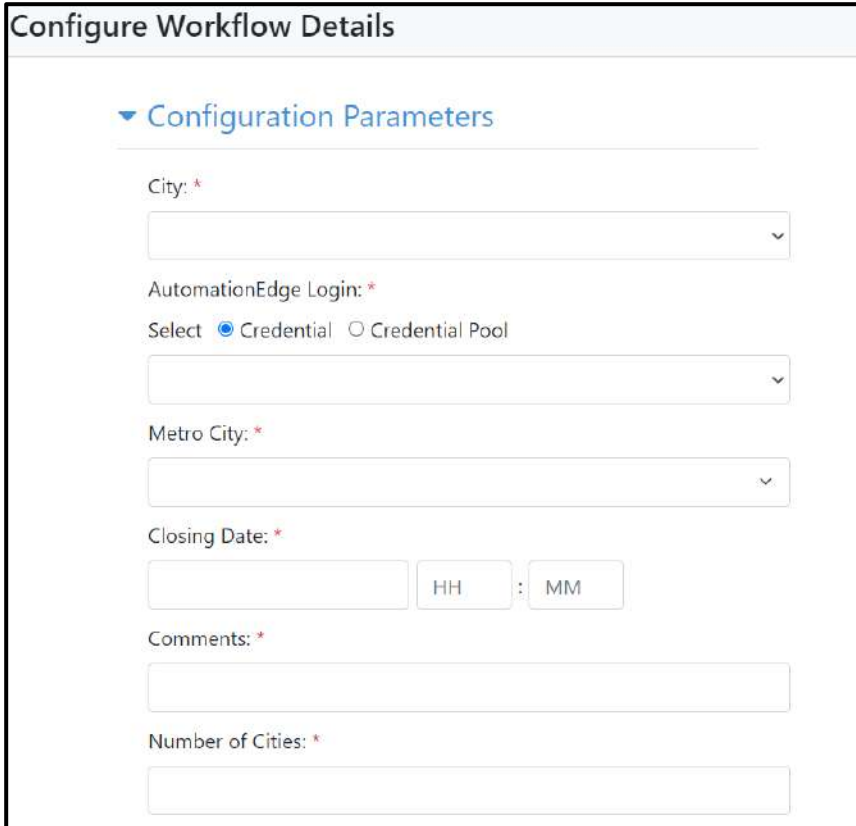
Figure 20m: Activate workflow

24. The process of publishing workflow to AutomationEdge (Development instance) using the Publish→Create option in Process Studio is complete.

6.2.1.2 Parameter data types on UI

This section discusses the supported data types for workflow parameters and the corresponding UI Control types. These are applicable to configuration and runtime parameters except File data type which is for runtime parameters only.

Following is a sample Configuration Parameters section in the Workflow configuration.



The screenshot shows a web form titled "Configure Workflow Details". Under the "Configuration Parameters" section, there are several fields:

- City:** A dropdown menu with a red asterisk indicating it is required.
- AutomationEdge Login:** A dropdown menu with a red asterisk. Below it are radio buttons for "Credential" (selected) and "Credential Pool".
- Metro City:** A dropdown menu with a red asterisk.
- Closing Date:** A date selection field with "HH" and "MM" input boxes and a colon separator, with a red asterisk.
- Comments:** A text input field with a red asterisk.
- Number of Cities:** A text input field with a red asterisk.

Figure 20n: Configuration Parameters

Following are the UI controls for configuration and runtime parameter data types (except File which is available only for runtime parameters).

1. Checkbox (Boolean)

If a configuration parameter is of type Boolean, it appears as a checkbox to enable or disable. The following is a screenshot of a sample Boolean data as a checkbox.

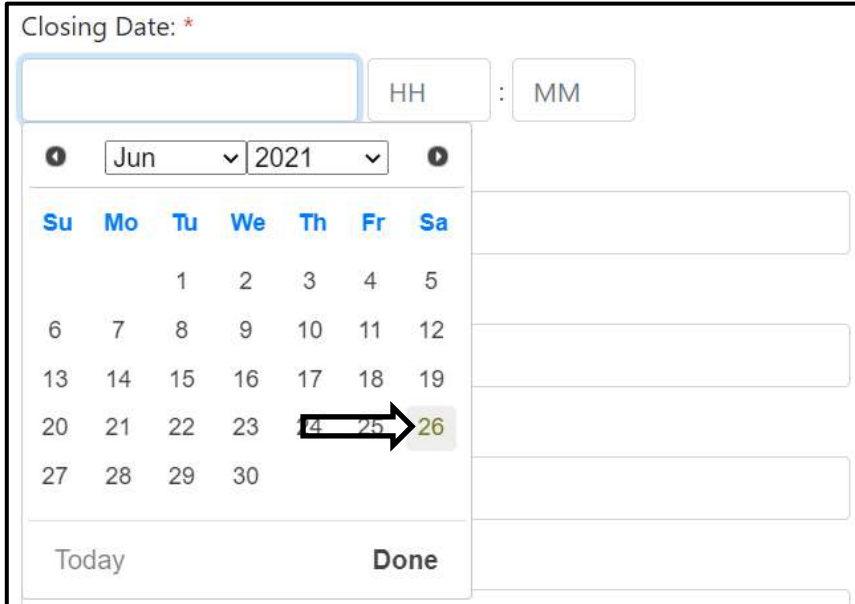


The screenshot shows a single checkbox control with the text "Local Office Available" next to it. The checkbox is currently unchecked.

Figure 20o: Checkbox for Boolean (True/False)

2. Text Box (Date)

Date value can be selected from picker for date time as shown below.



Closing Date: *

HH : MM

Jun 2021

Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

Today Done

Figure 20p: Picker for date time

3. Text Box (String)

Provide a string value in a Text Box.



Comments: *

Figure 20q: Text box for string

4. Text Box (Integer, Number)

Provide an Integer or Number in a Text Box.



Number of Cities: *

9

Figure 20r: Text box for Integer and Number

5. Text Box (File)

Click Choose File button to browse a file at runtime and click the Upload button.

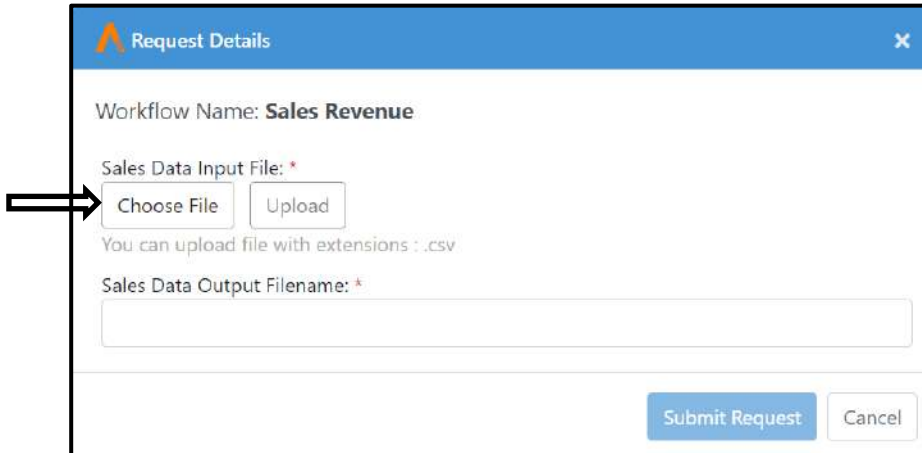


Figure 20s: Choose file at runtime

6. Single Selection List (List)

Select a single value from a Single Selection List.

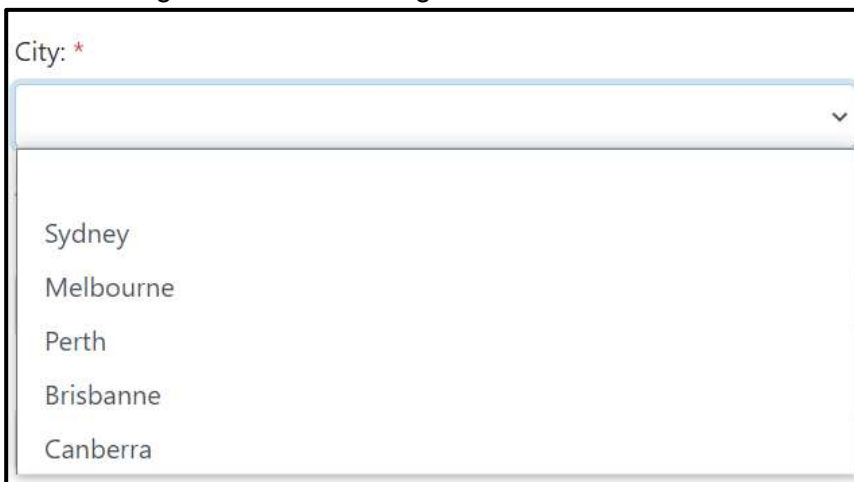


Figure 20t: Single Selection List

7. Single Selection List (Credential)

If a configuration parameter is of type Credential, it shows radio buttons for Credential and Credential Pool as shown below. Once a radio button is selected for Credential or Credential Pool the corresponding dropdown list appears. If a Credential belongs to a Credential Pool, it does not appear in the Credential drop down list.

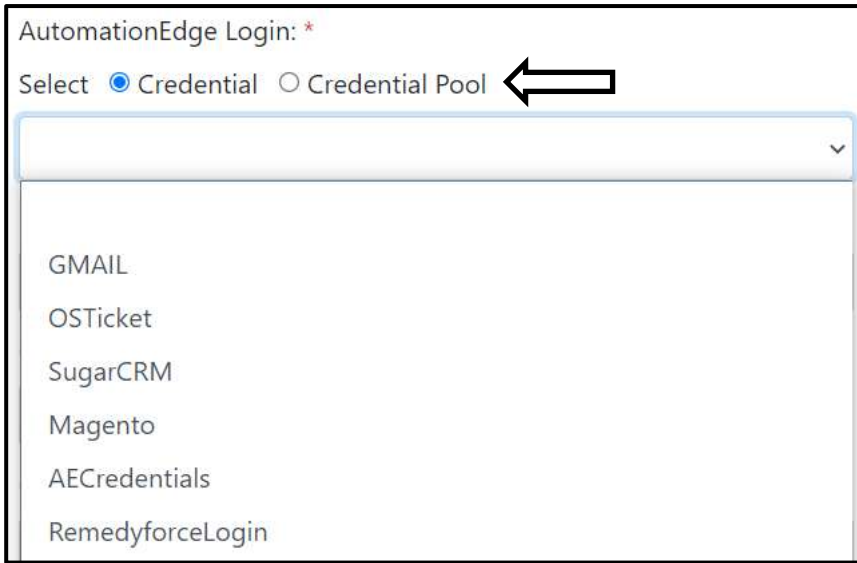


Figure 20u: Radio Buttons for Credential and Credential Pool

8. Combo Box (List)

On AEUI select a single Checkbox or enter a custom value in the field.

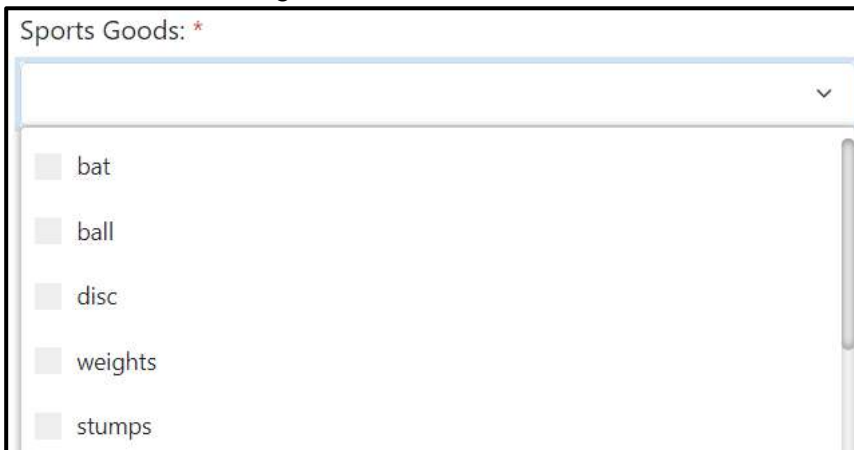


Figure 20v: Select a single value or provide a custom value in the field

9. Radio Button (List)

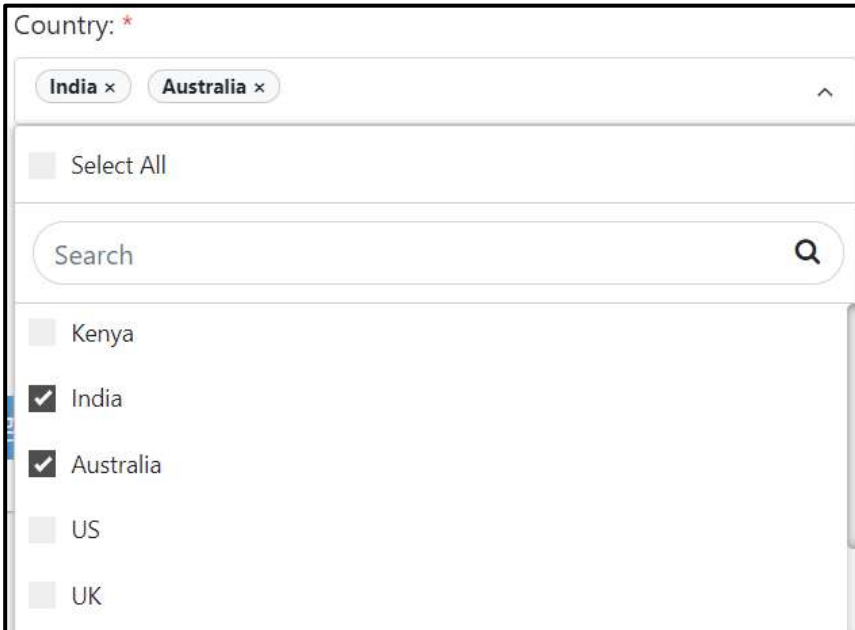
Select a radio button from the radio button list.



Figure 20w: Select a Radio Button

10. Multiple Selection List (List)

Enable checkboxes to select multiple values.



The screenshot shows a form field labeled "Country: *". The field contains two selected items: "India" and "Australia", each with a small 'x' icon to its right. Below the field, there is a "Select All" option with an unchecked checkbox. A search bar with the text "Search" and a magnifying glass icon is positioned below the "Select All" option. The list of countries is displayed below the search bar, with checkboxes next to each name: Kenya (unchecked), India (checked), Australia (checked), US (unchecked), and UK (unchecked).

Figure 20x: Select multiple values

Also refer to the section Parameters in the AutomationEdge_R7.0.0_ProcessStudio_User_Guide for more details.

We used the Publish → Create option to create workflow (Sales Revenue) on the Development instance. Now, complete the life cycle of exporting from Development instance, importing to UAT instance, exporting from UAT and finally importing to a Production instance.

6.3 Setup, Execute Sales Revenue on Development Instance

6.3.1 Workflows: Workflow Assignment to Agent

1. Click Agents menu. Click Workflow Assignment sub-menu.

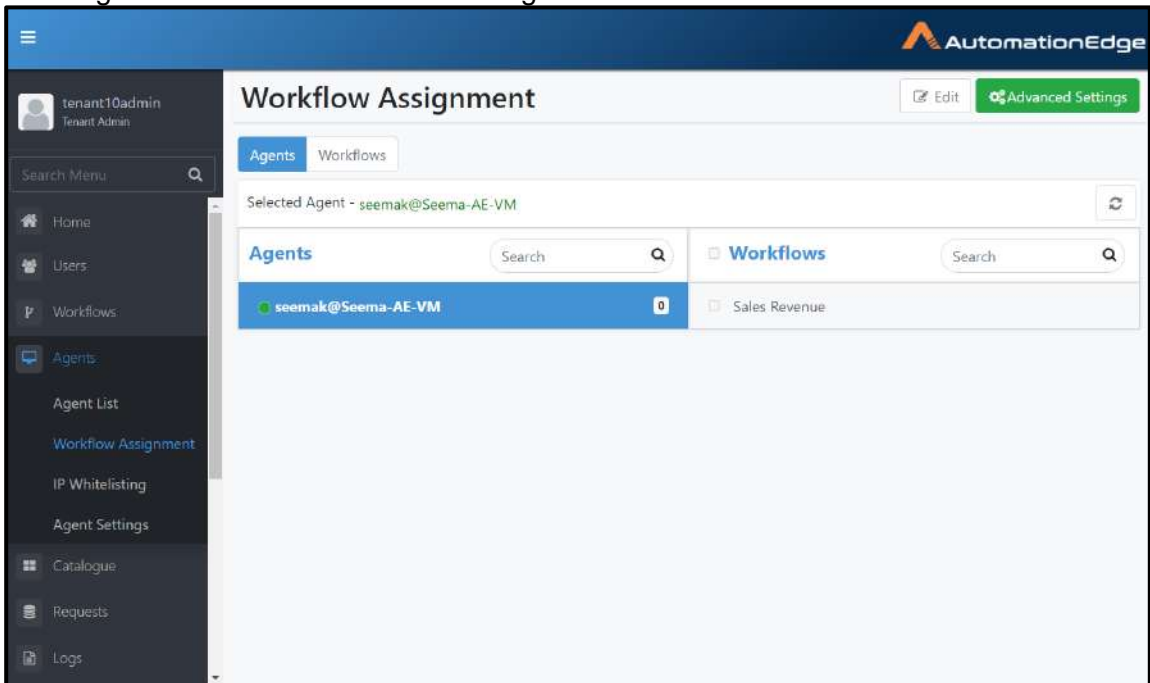


Figure 22a: Assign Workflow to Agent

2. Select an Agent. Click the arrow key on the right for the Agent.
3. You can now see the list of available workflows.
4. Click Edit to modify the workflow assignments to Agent.
5. Now you may enable checkbox next to Sales Revenue. Click Save.

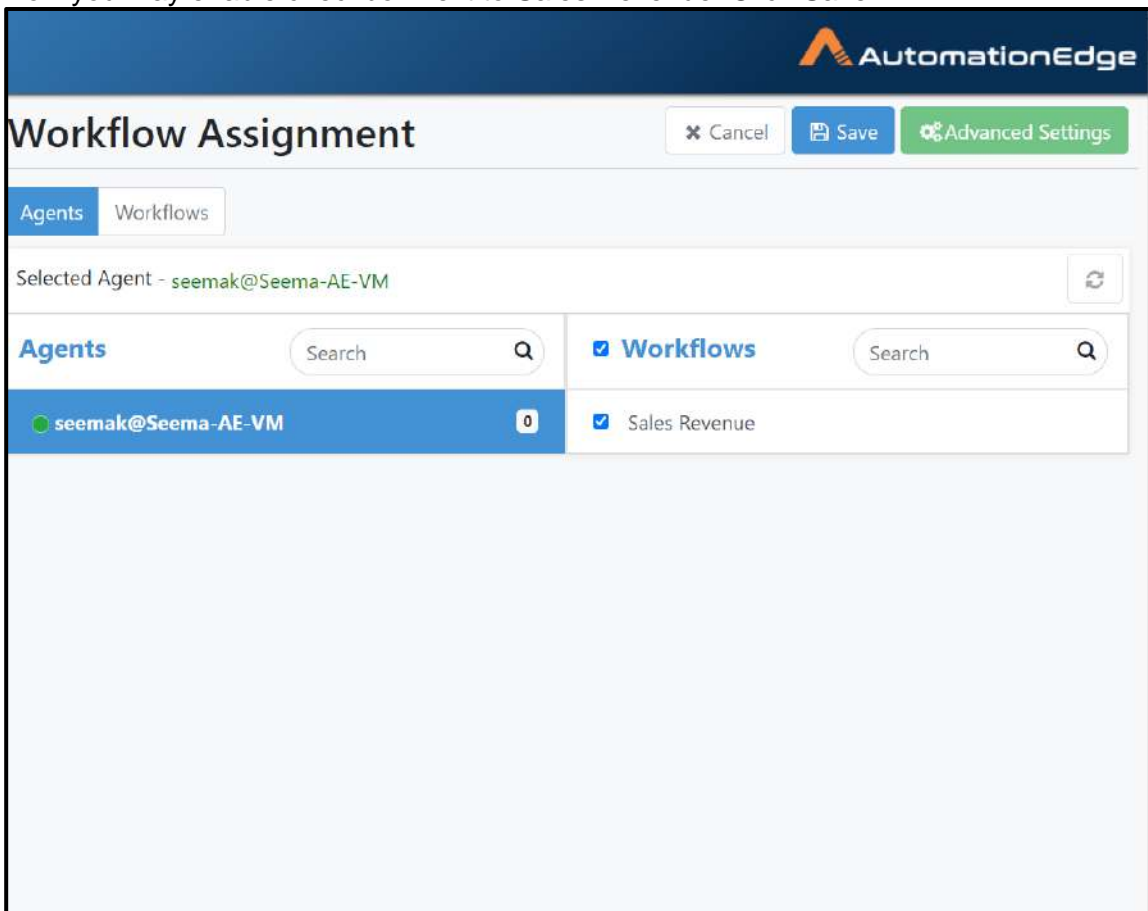


Figure 22b: Click Edit and Enable workflows to assign to Agent

6. A pop-up appears to Confirm Assignment. Acknowledge the message.

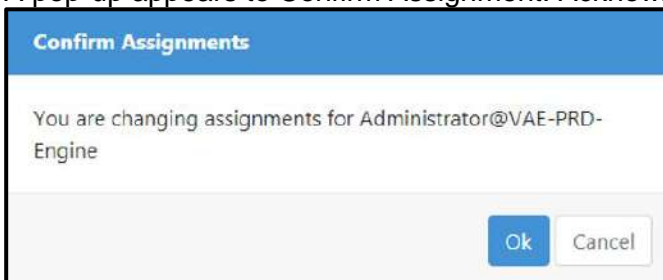
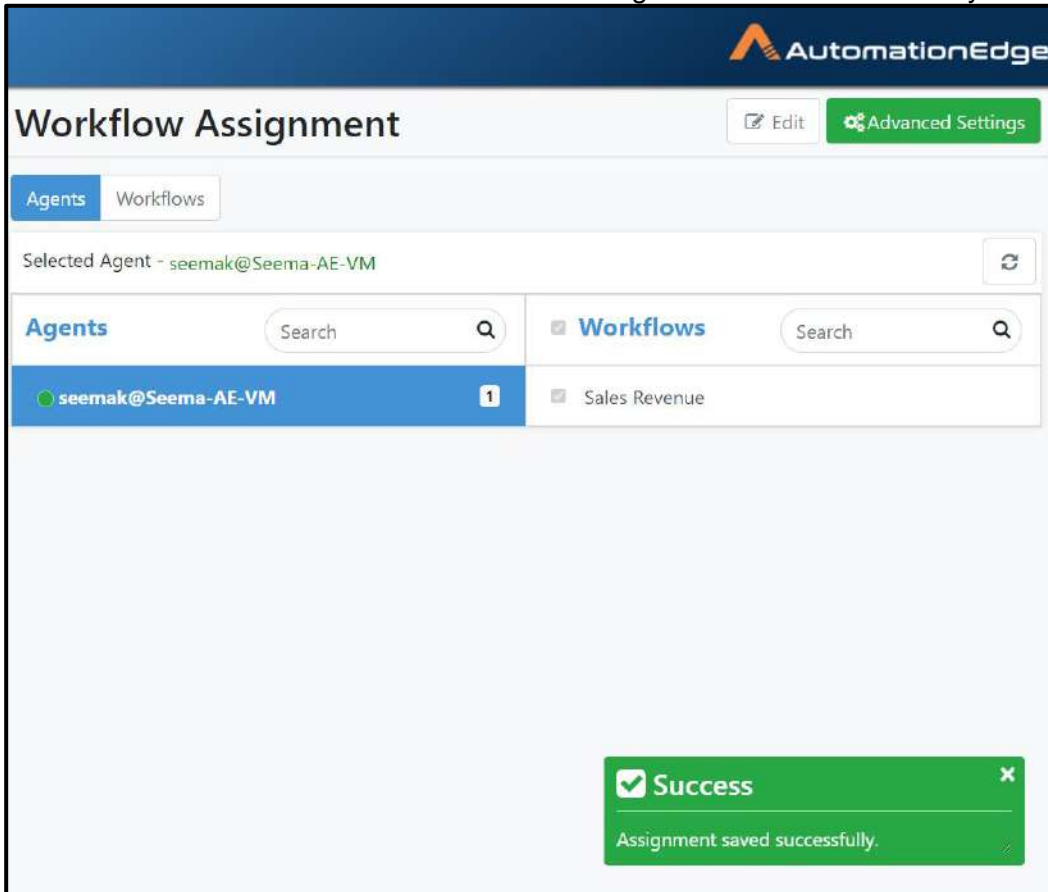


Figure 22c: Acknowledge Assignment

7. The screenshot below shows that Workflow Assignment saved successfully.



The screenshot displays the AutomationEdge 'Workflow Assignment' page. At the top, there is a dark blue header with the AutomationEdge logo. Below the header, the page title 'Workflow Assignment' is shown in a light blue bar, accompanied by 'Edit' and 'Advanced Settings' buttons. The main content area features two tabs: 'Agents' (active) and 'Workflows'. Under the 'Agents' tab, the 'Selected Agent' is 'seemak@Seema-AE-VM'. Below this, there are two searchable lists: 'Agents' and 'Workflows'. The 'Agents' list shows 'seemak@Seema-AE-VM' with a count of '1'. The 'Workflows' list shows 'Sales Revenue'. A green success message box is visible in the bottom right corner, stating 'Success' and 'Assignment saved successfully.'.

Figure 22d: Assignment saved successfully

8. Go to Catalogue menu. The workflow is now visible in the catalogue.
9. Click Sales Revenue workflow icon.

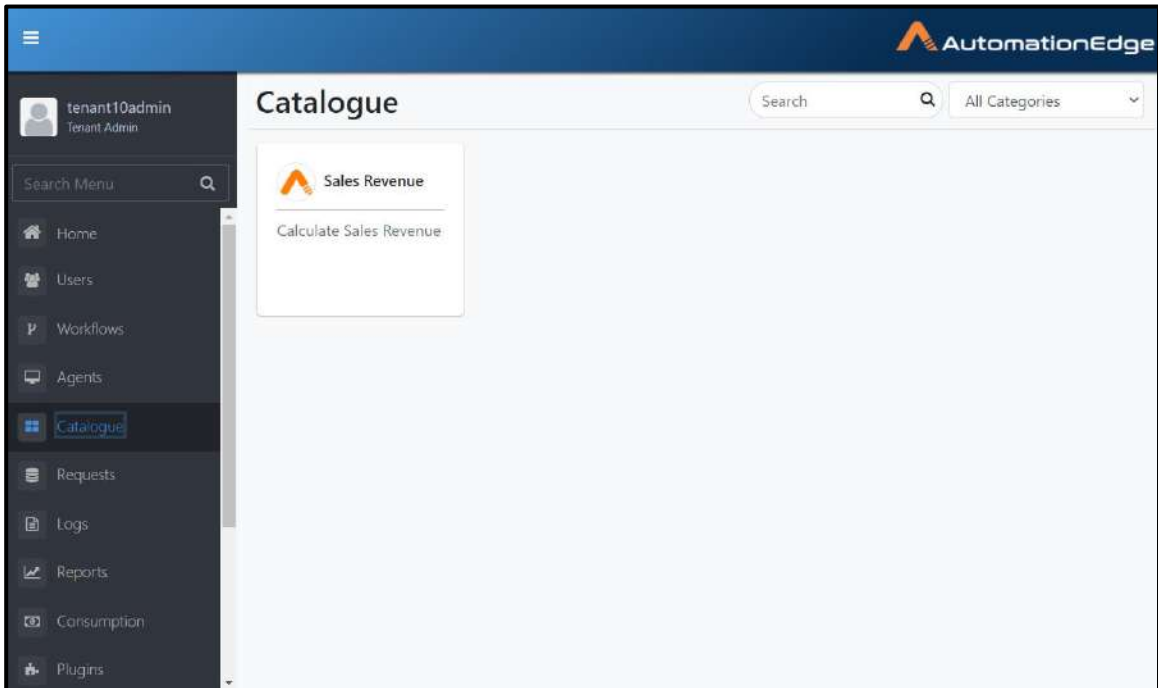


Figure 23a: Workflow on Catalogue

- Along with other Workflows, assisted Workflows will also appear on User's catalogue page, if User has execution permissions on them and User has at least one assisted Agent registered.

Note: Along with other Workflows, assisted Workflows will also appear on User's catalogue page, if User has execution permissions on them and User has at least one assisted Agent registered.

6.3.2 Assigning permissions to workflow

1. To see the workflow as a catalogue item for other users provide necessary Read/Write/Execute permissions to Users/Groups under Workflows menu and Category sub-menu.

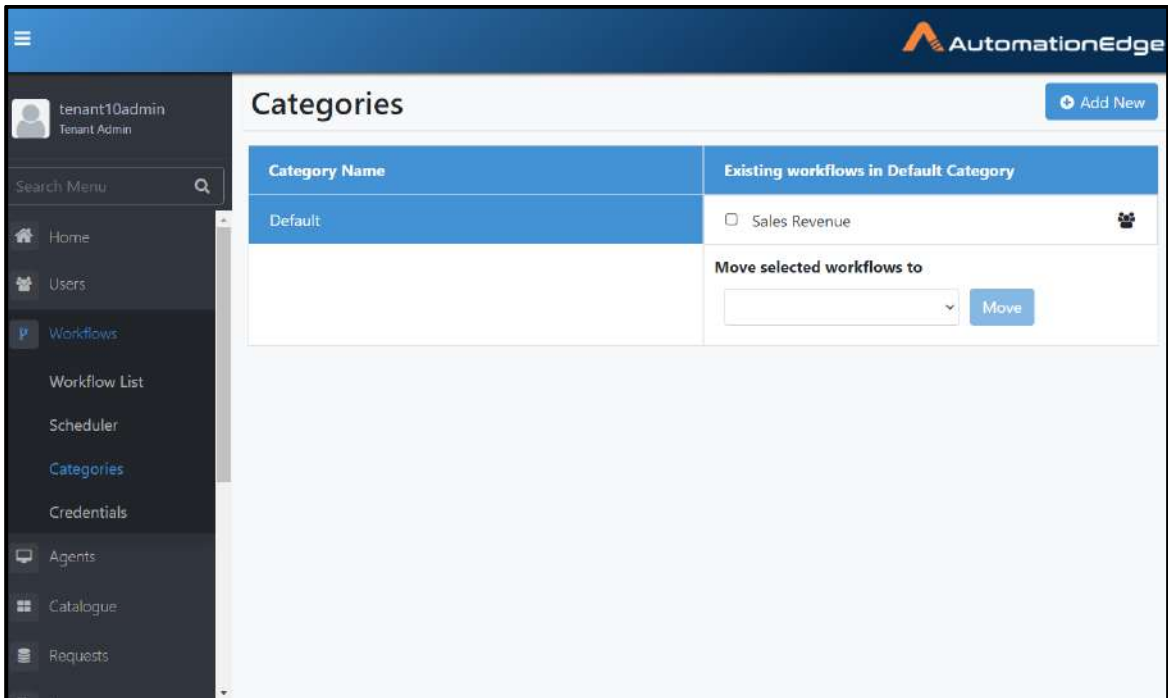


Figure 24a: Workflow Category Menu-Permissions icon

2. Select the Type from the drop down list.

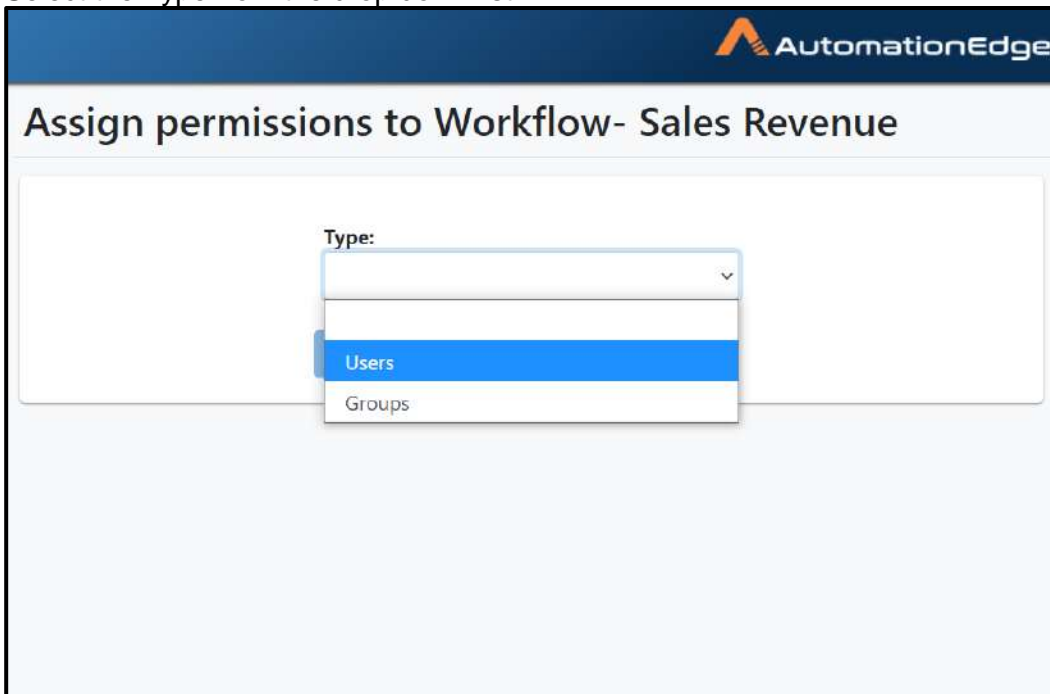
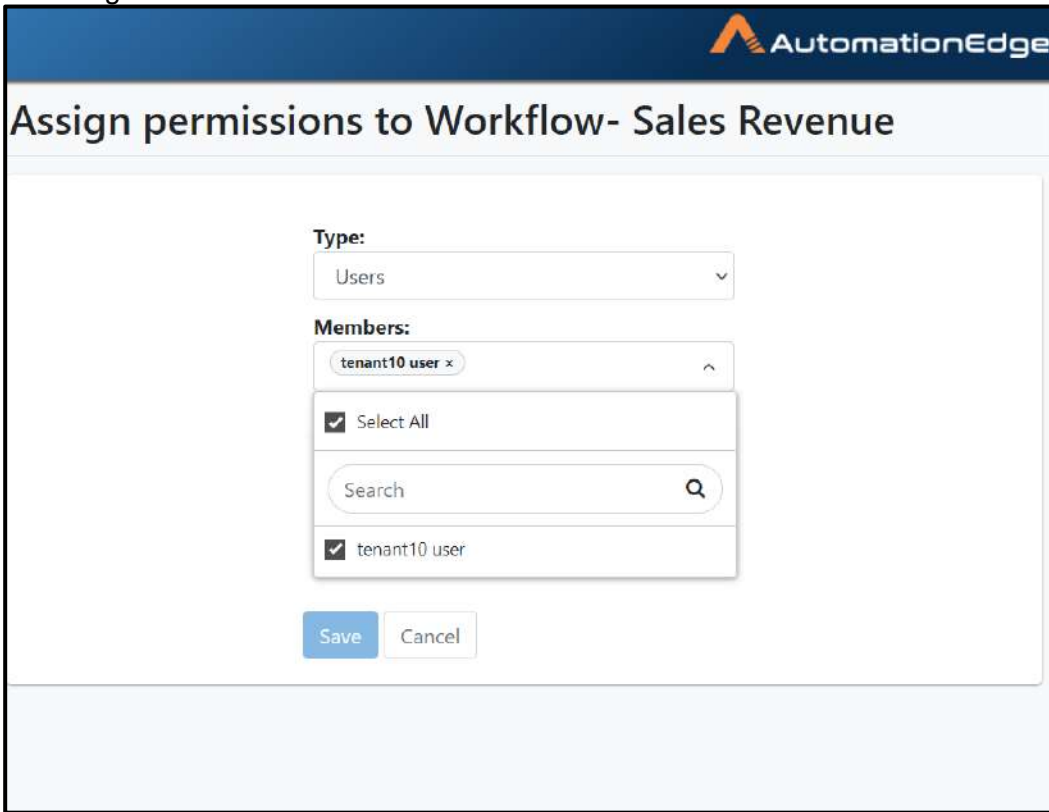


Figure 24b: Assign Workflow Permissions to users

3. Select the Users or Groups and the corresponding members.
4. In this figure below Users is chosen and member Tenant 10 User is selected.

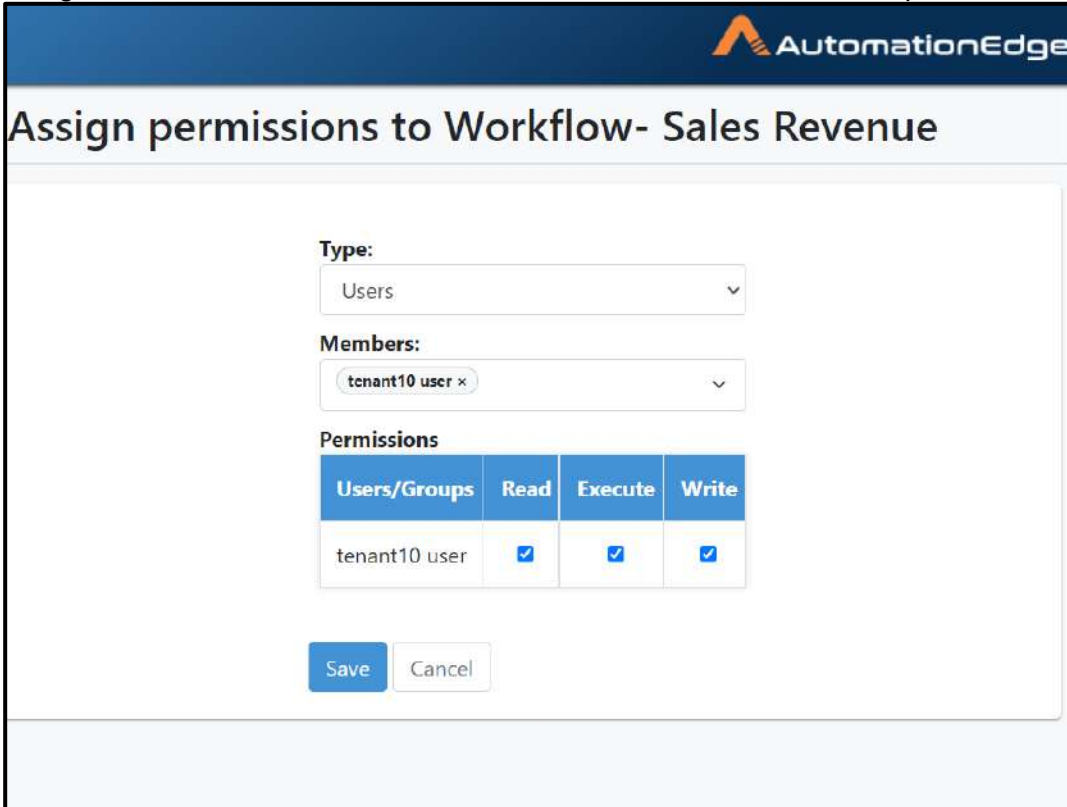


The screenshot shows a dialog box titled "Assign permissions to Workflow- Sales Revenue" with the AutomationEdge logo at the top right. The dialog contains the following elements:

- Type:** A dropdown menu currently showing "Users".
- Members:** A list of members with "tenant10 user" selected and displayed as a tag with an "x" icon.
- Select All
- A search input field with the placeholder text "Search" and a magnifying glass icon.
- tenant10 user
- Two buttons at the bottom: "Save" (highlighted in blue) and "Cancel".

Figure 24c: Select Users to assign permissions

5. Assign Read, Write and/or Execute Permissions Tenant 1 User as required. Click Save.



AutomationEdge

Assign permissions to Workflow- Sales Revenue

Type:
Users

Members:
tenant10 user

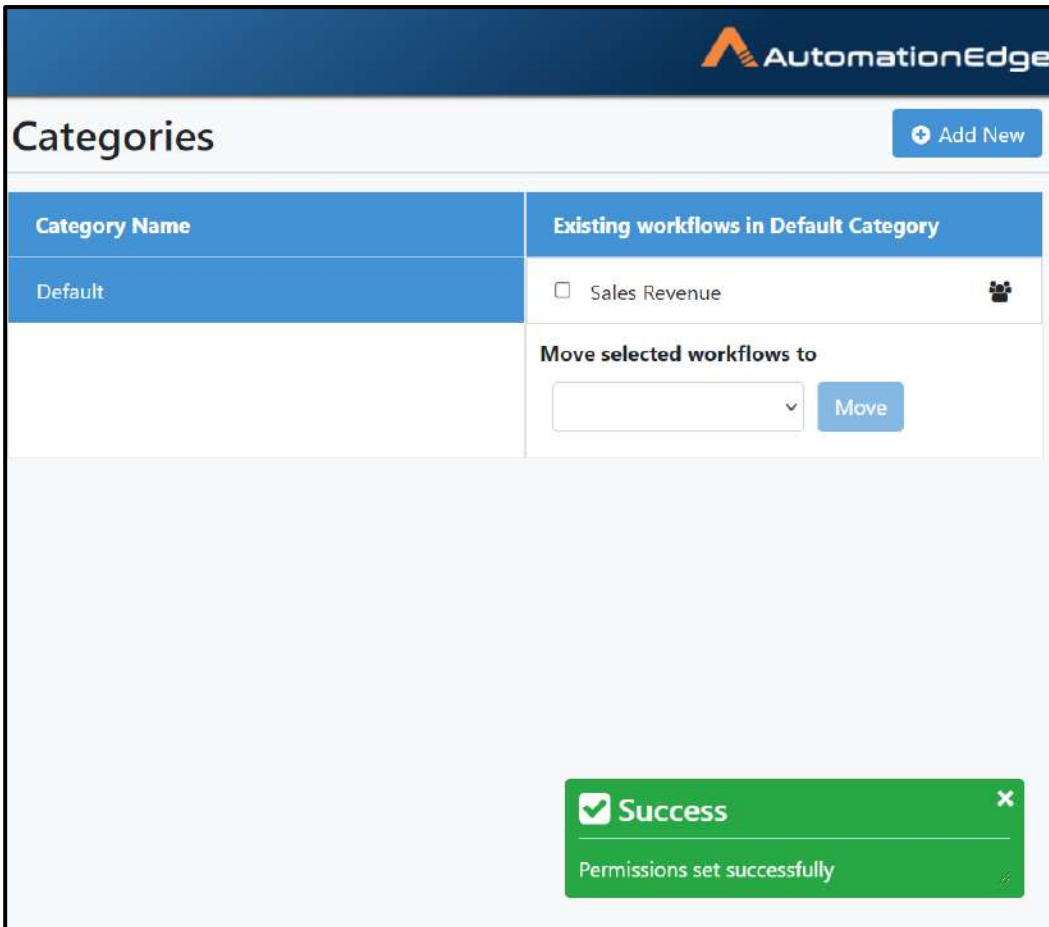
Permissions

Users/Groups	Read	Execute	Write
tenant10 user	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Save Cancel

Figure 24d: Select Permission check boxes

6. Note the Permissions set successfully message.



The screenshot shows the 'Categories' management interface. At the top right, there is an 'Add New' button. The main content is a table with two columns: 'Category Name' and 'Existing workflows in Default Category'. The 'Default' category is selected, and it contains one workflow, 'Sales Revenue', which has a checkbox and a user icon next to it. Below the table, there is a section titled 'Move selected workflows to' with a dropdown menu and a 'Move' button. At the bottom right, a green success message box displays a checkmark, the word 'Success', and the text 'Permissions set successfully'.

Figure 24e: Permissions Set

6.3.3 Executing Workflows

The workflow can now be executed from the Catalogue.

1. Navigate to the Catalogue menu. Click on the Sales Revenue tile.

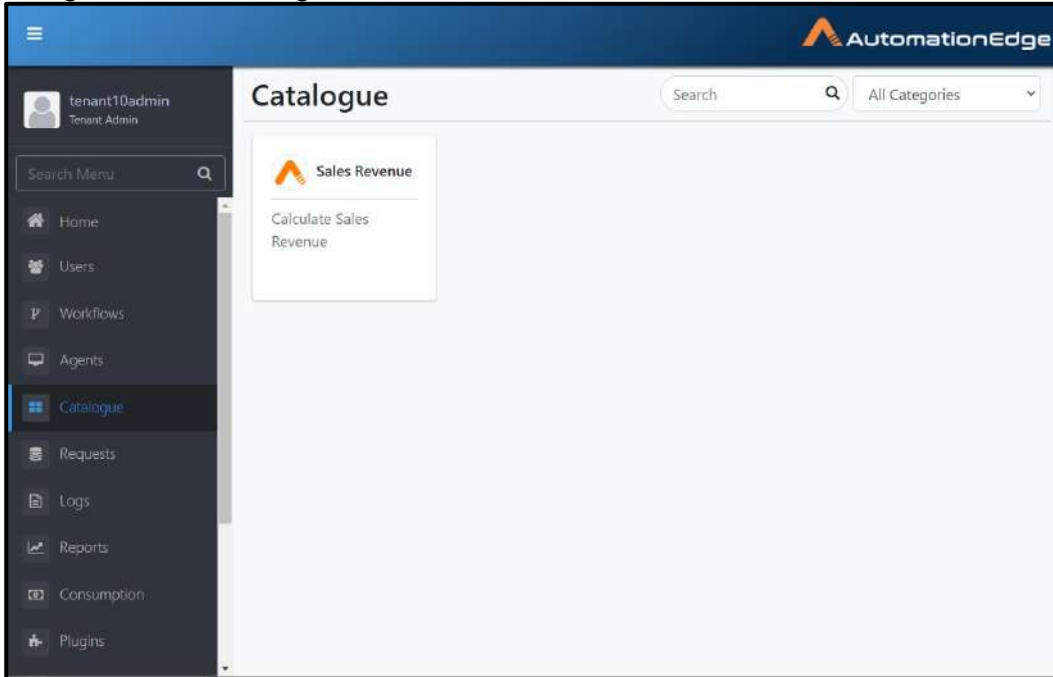


Figure 25a: Catalogue

2. Calculate Sales Revenue Request Details Parameters form appears.
3. Sales Data Input file is a parameter of type file. Click Choose File button to browse and select the file. As per process studio process parameters file extensions allowed are .csv for this file.
4. Click Upload button.
5. Provide a name for the Sales Data Output file. Click Submit Request.

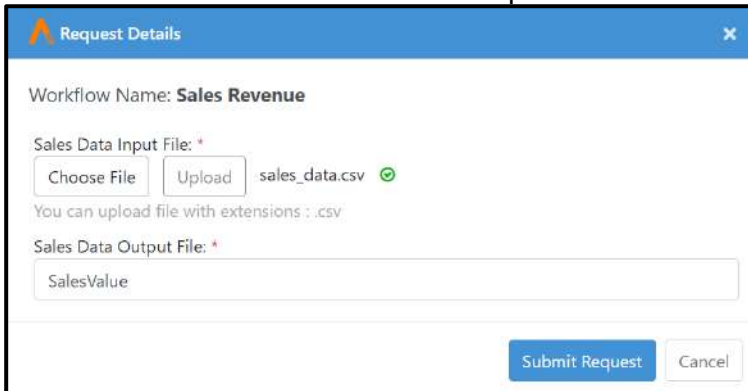


Figure 25b: Choose and Upload input file

6. Acknowledge the pop-up for successful request submission. Note the Request ID.

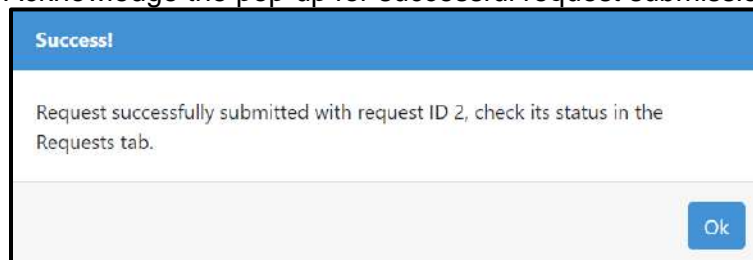


Figure 25c: Submit Request from Catalogue

6.3.4 Monitor Requests

The workflow execution can now be monitored from the Requests menu.

1. Click Requests menu. Identify your workflow.
2. The screen shot below shows Sales Revenue completed successfully.
3. You may download the output file sales_output.xls.
4. The screenshot below shows the downloaded file in the bottom left corner.

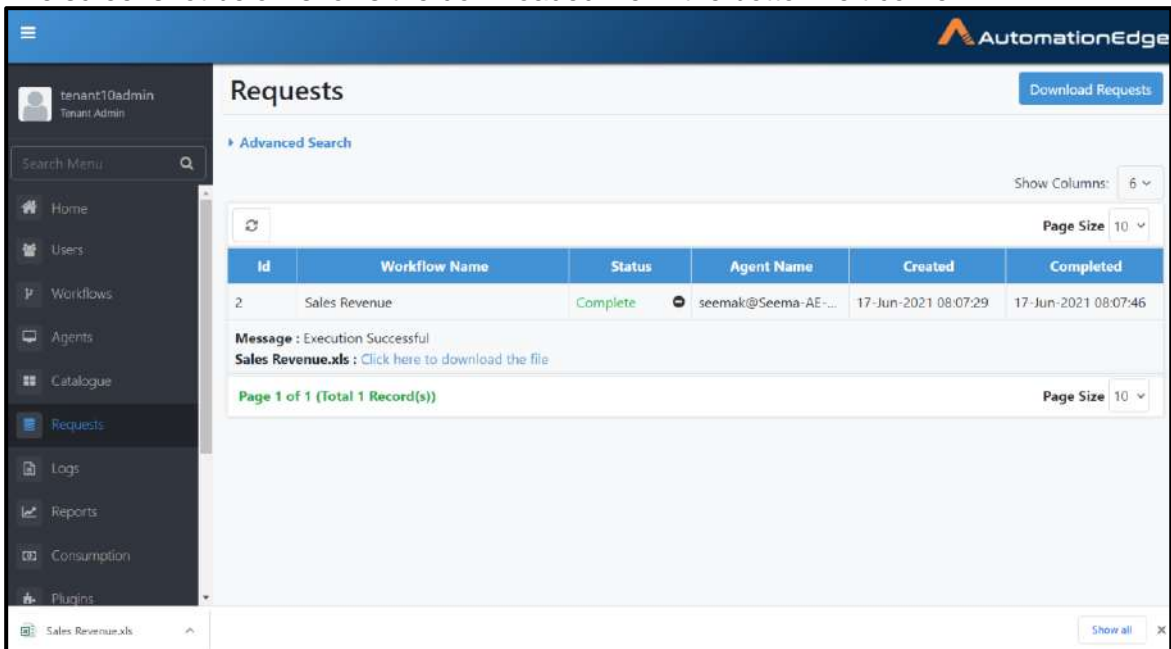


Figure 26a: Downloaded output file

5. Following is a screenshot of the output file.

	A	B	C	D	E
1	customer	quantity	unitprice	totalprice	
2	Thunderboltz FC	20	1000	20000.	
3	Genpact	15	900	13500.	
4	iWareLogic	10	500	5000.	
5					

Figure 26b: Output file

- The following is a screenshot showing the file was received by email.

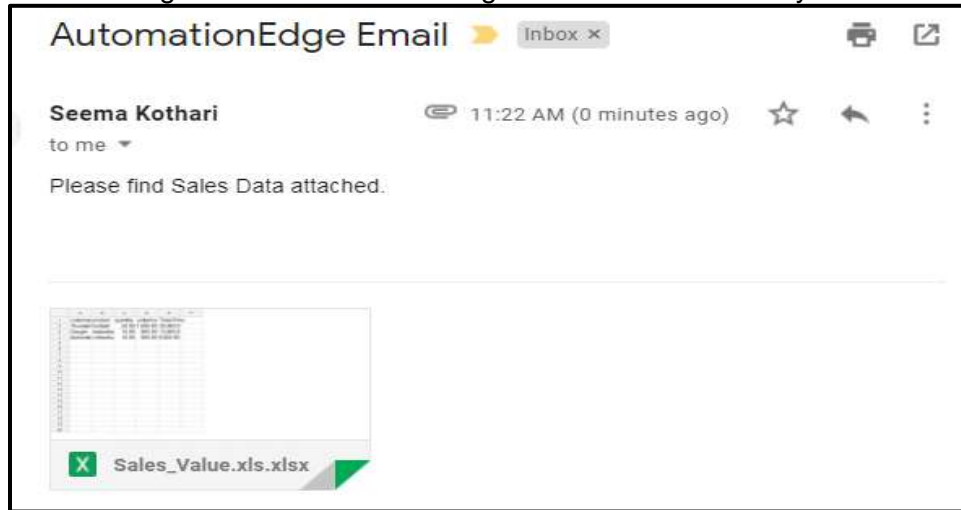


Figure 26c: File attached to email

- This completes publishing and executing Sales Revenue Workflow on AutomationEdge server.

6.4 Workflows: Export from Development Instance

Once workflow is found to be working satisfactorily on Development instance, it's usually exported and then uploaded on UAT. A workflow can be exported from development instance and then imported to UAT or Production (Enterprise/Subscription) instances, although it is recommended to import it to a UAT server.

The exported workflow is self-contained i.e. it has all the .psp and .psw it needs, and all the supporting files that are required for execution.

Following are the steps to export one or more Workflows,

1. Go to the Workflows menu. Workflow List sub-menu is selected by default.
2. Click the arrow next to the Import button on the top right corner. From the drop down list click Export.
3. You may view the file structure and contents of the workflow zip being exported by clicking the folders icon in the Actions column. Users can see and verify if the zip being exported contains valid files.

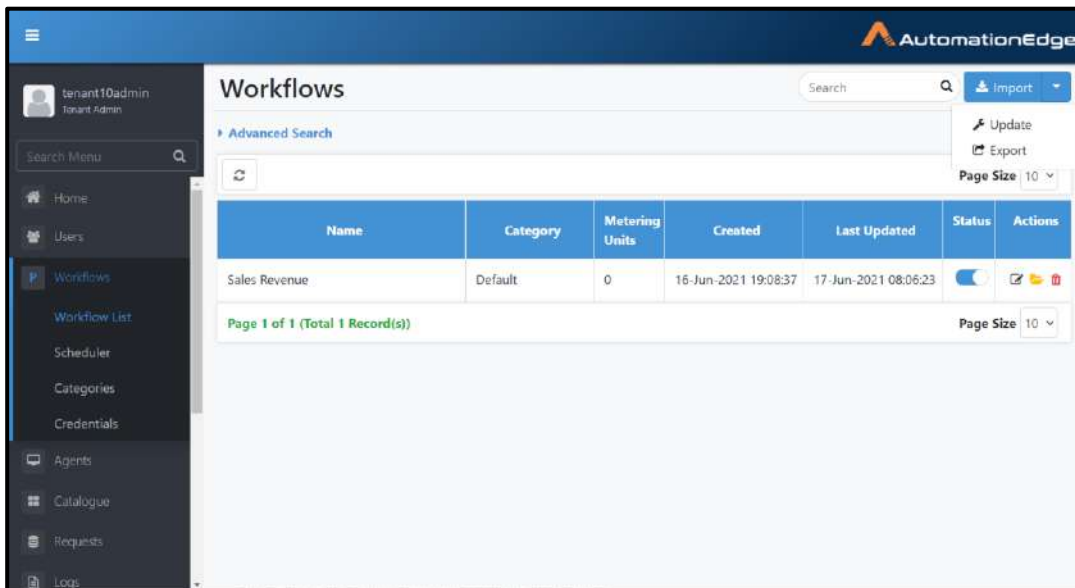


Figure 27a: Export Process Studio Workflow

4. Select a workflow or workflows to export.
5. Enable check boxes next to workflows to be exported.



Figure 27b: Export Workflow Window

6. The chosen workflows are now visible in the selected workflows.

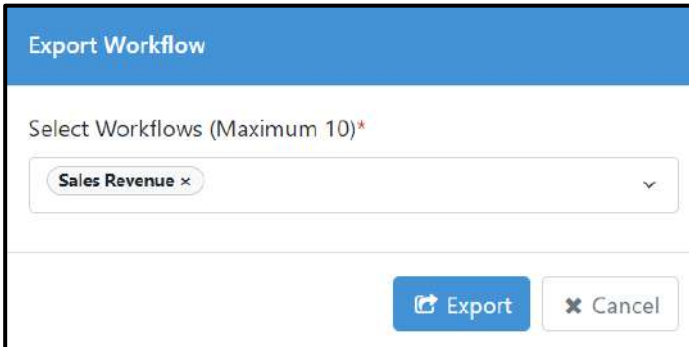


Figure 27c: Choose Workflow to Export

7. The below snapshot shows the exported zip file at the bottom left corner. Figure 27e: Message for Workflow exported successfully.

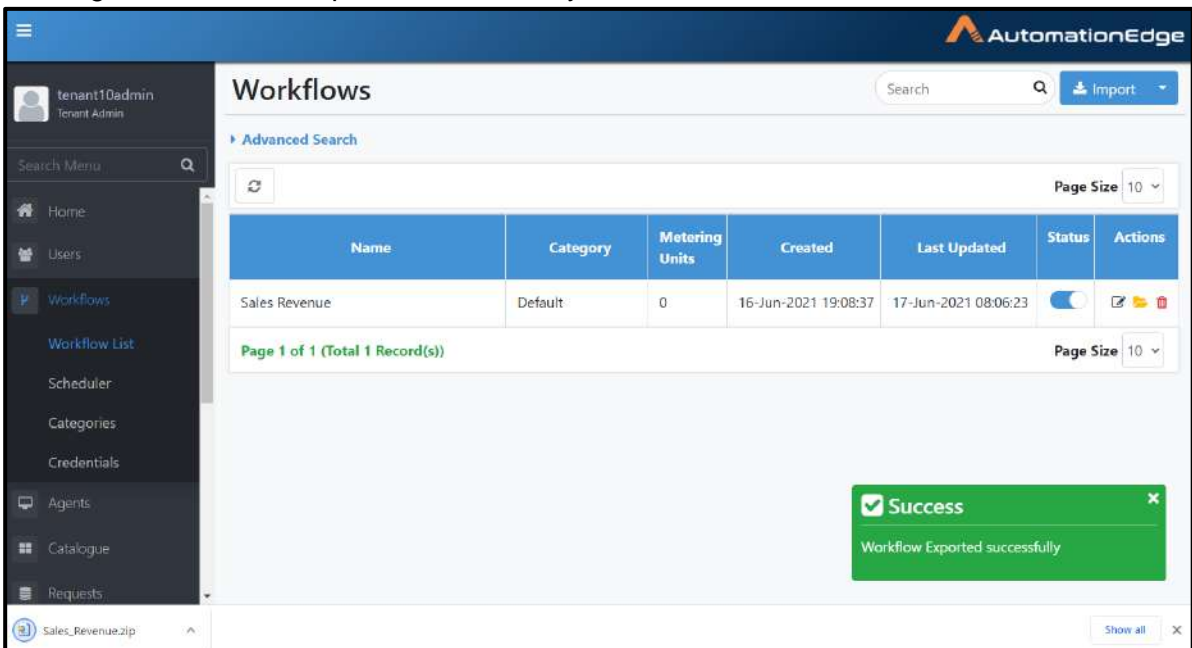


Figure 27d: Workflow exported successfully

6.5 Workflows: Import to UAT Instance

Import button on Workflow menu supports import of a zip file exported from DEV instance or other instances of AutomationEdge.

Note: A project exported from Process Studio cannot be imported or updated directly on an AutomationEdge instance.

Once workflow is found to be working satisfactorily on Development instance, it's usually uploaded on UAT. A workflow can be exported from development instance and then imported to UAT or Production (Enterprise/Subscription) instances, although it is usually imported to UAT server. Only one workflow can be imported at a time.

Import the workflow as exported from Development Instance. Following are the steps to import the workflow on the UAT instance.

1. Login to UAT instance

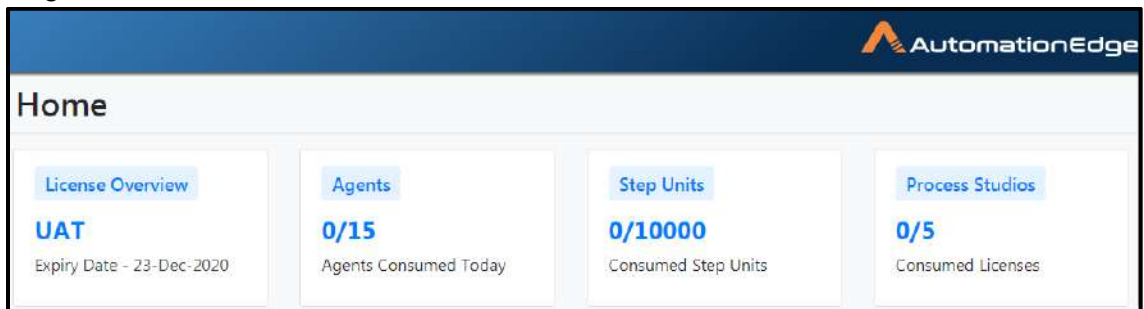


Figure 28a: UAT instance

2. Navigate to the Workflows menu. Workflow list menu is chosen by default. Click Import button.

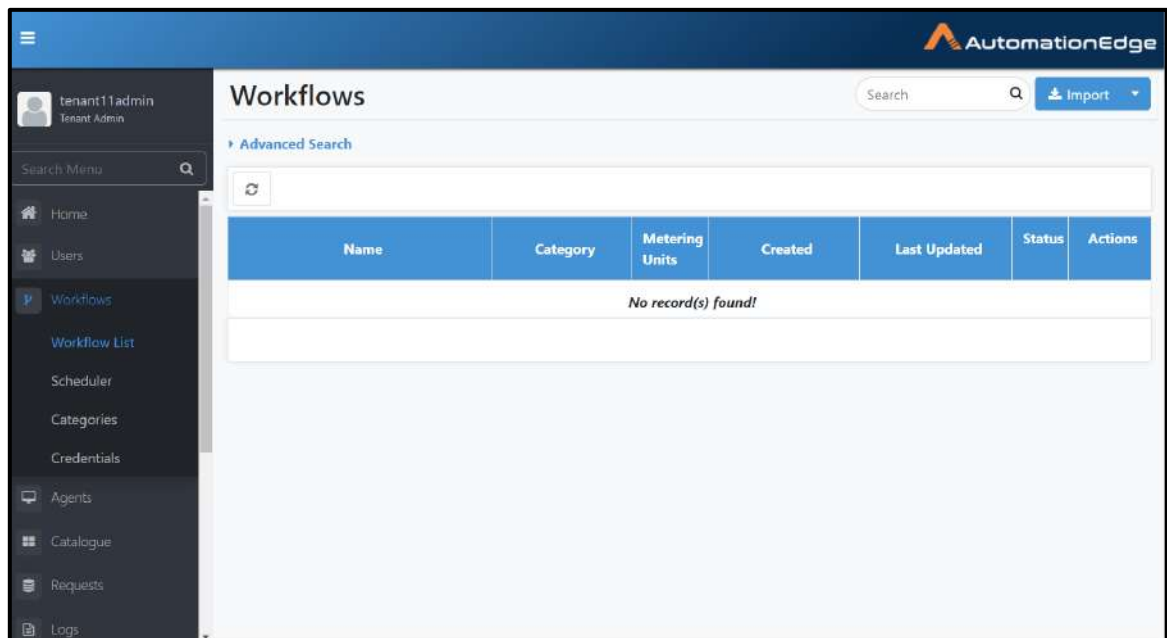


Figure 28b: Import Workflow

3. The Create New Workflow page appears as seen below. Provide configuration details. Browse and upload the exported zip file from Development instance under Select Workflow file (.zip).

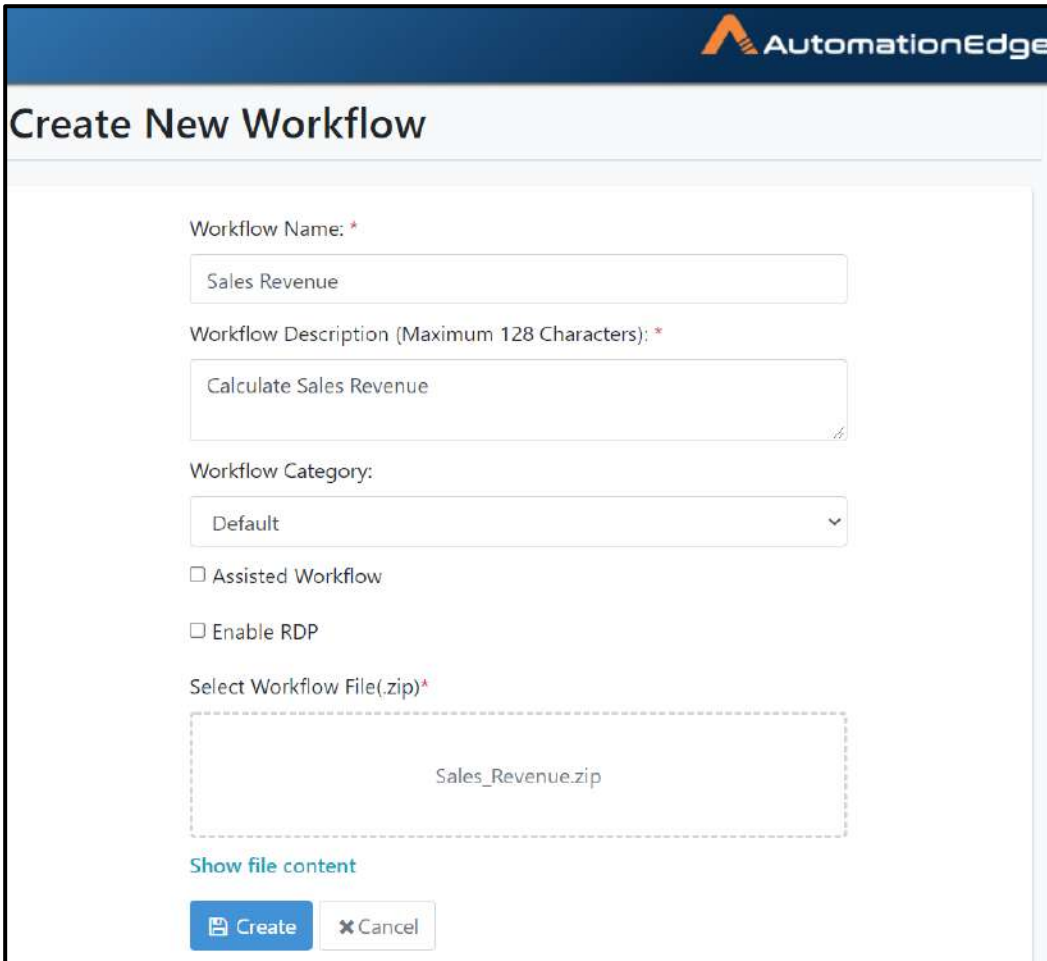


Figure 28c: Create New Workflow Configurations

4. Click Show file content above to see the contents of the zip file being imported. Click Create.

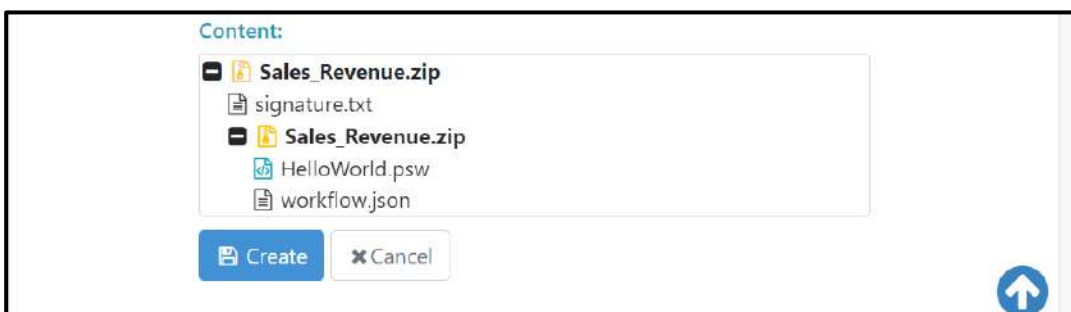


Figure 28d: Workflow zip file content

5. Fill in the basic workflow configuration details.

Configure Workflow Details

▼ Basic Details


Workflow Name: **Sales Revenue**

Workflow Description (Maximum 128 Characters): *

Calculate Sales Revenue

Workflow Category:

Default

Workflow Icon: 

Assisted Workflow : **false**

Enable Sequential Execution

Enable RDP

Enable Input Attributes

Workflow Priority:

Default

Expected Completion Time(Seconds): *

10

Maximum Completion Time(Seconds): *

20

Cleanup Requests older than(Hours):

36

Manual Execution Time:

5

Figure 28e: Workflow Basic Configuration

- Fill in the email notifications configuration settings. Click Save.

▼ Email Notification Setting

Notify On Workflow Failure

Notify On Exceeding Time Limit

Select Users*:

By Role: Tenant Admin Workflow Admin

By Username:

By Email:

Request Creator

Failure Message:

No Configuration Parameters

Figure 28f: Workflow Email Notification configuration

- Workflow updated successfully message appears.

Workflows

▶ Advanced Search

Page Size 10

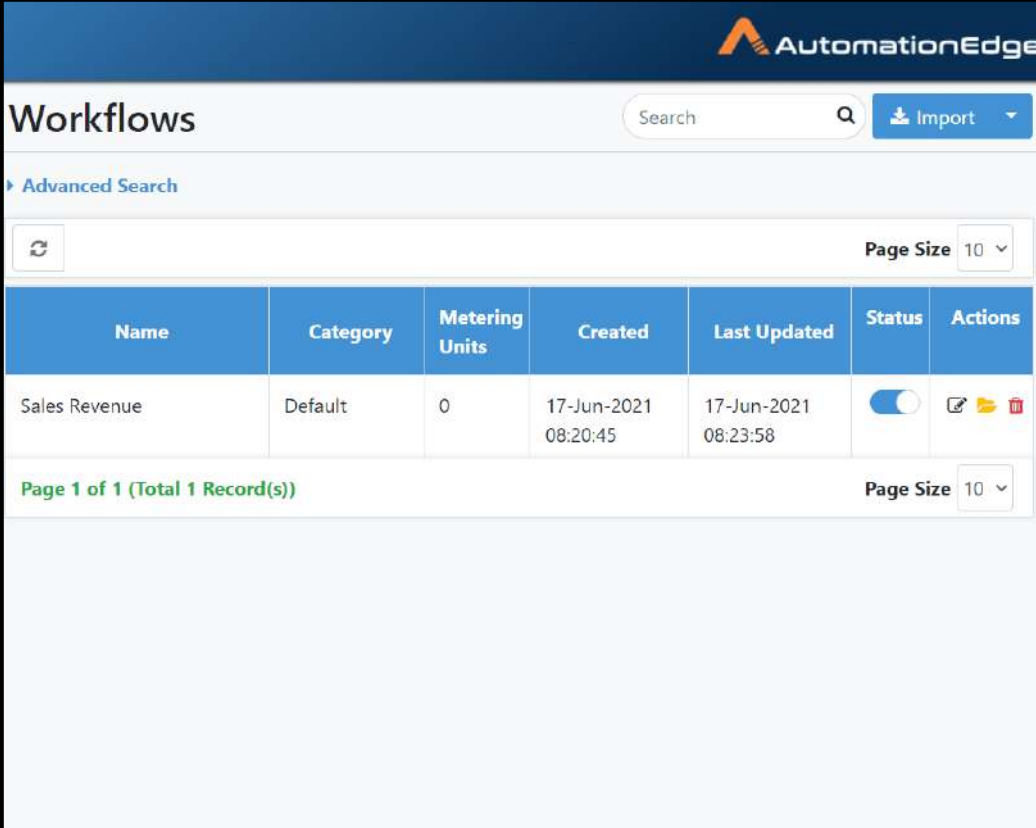
Name	Category	Metering Units	Created	Last Updated	Status	Actions
Sales Revenue	Default	0	17-Jun-2021 08:20:45	17-Jun-2021 08:23:58	<input type="checkbox"/>	

Page 1 of 1 (Total 1 Record(s))
Page Size 10




Success ×
 Workflow updated successfully

Figure 28g: Workflow Added Successfully

- You may now Activate the workflow.



The screenshot shows the AutomationEdge interface for managing workflows. At the top, there is a search bar and an 'Import' button. Below this is an 'Advanced Search' section with a refresh icon and a 'Page Size' dropdown set to 10. The main content is a table with the following data:

Name	Category	Metering Units	Created	Last Updated	Status	Actions
Sales Revenue	Default	0	17-Jun-2021 08:20:45	17-Jun-2021 08:23:58	<input checked="" type="checkbox"/>	  

Below the table, it indicates 'Page 1 of 1 (Total 1 Record(s))' and another 'Page Size' dropdown set to 10.

Figure 28h: Newly imported Sales Revenue on UAT instance

- This completes the process of workflow import to UAT instance.

6.6 Workflows: Export from UAT Instance

Once workflow is found to be working satisfactorily on UAT instance, it's usually uploaded on Production instance. A workflow can be exported from UAT instance and imported to Production (Enterprise/Subscription) instances. Only workflows present on UAT instance can be exported as 'Verified' workflows. This signifies that workflow has been thoroughly tested on UAT instance.

The exported workflow is self-contained. i.e. it has all the .psp and .psw it needs, and all the supporting files that are required for execution. The steps to export the workflow from UAT are discussed here.

1. Login to a UAT instance.

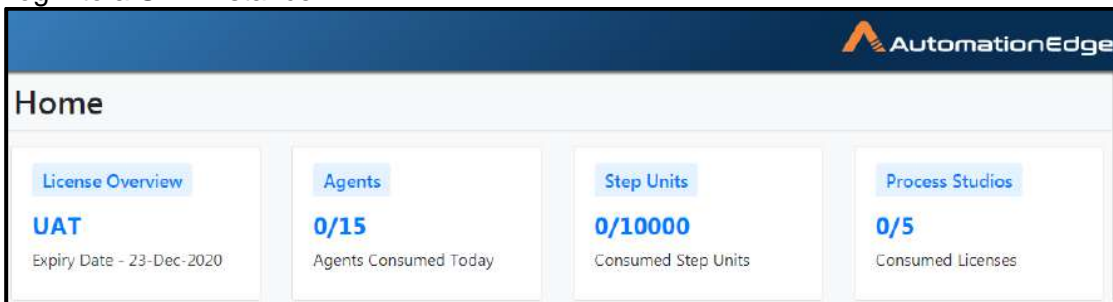


Figure 29a: UAT instance

2. Click Workflows menu. Workflows List menu is selected by default.
3. Click arrow next to Import button. Click Export.

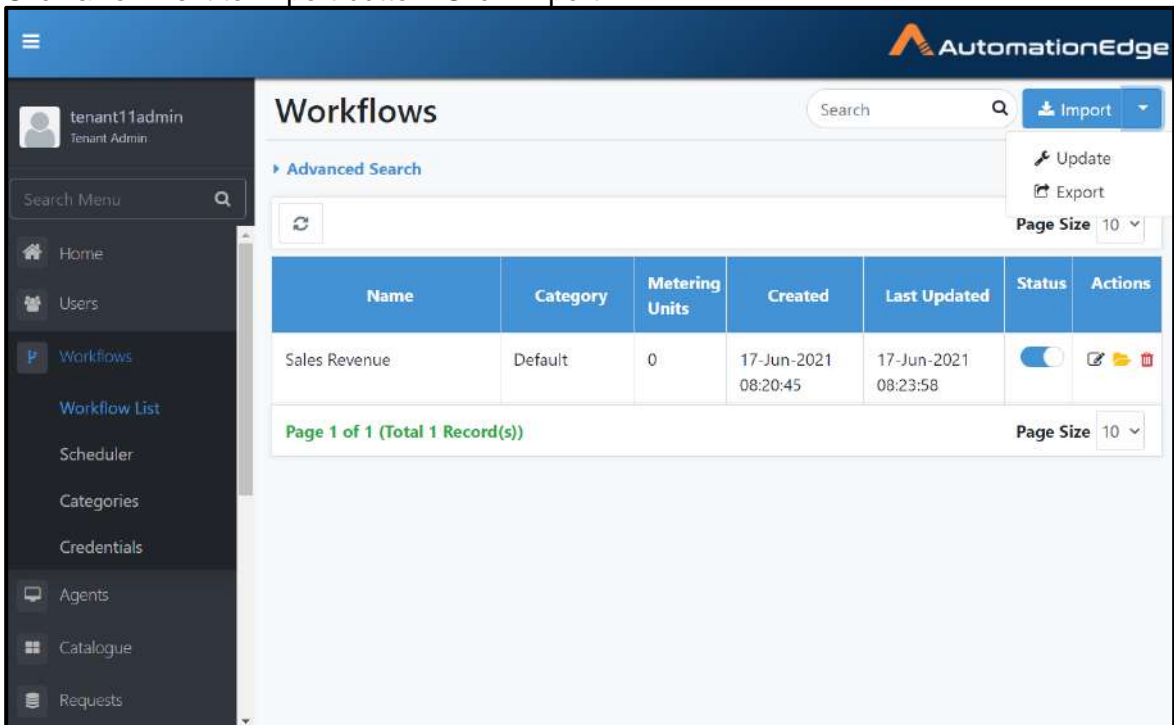


Figure 29b: Export Option

4. Select workflows from the dropdown menu.

5. You have the option to enable Export as Verified checkbox. If Export as verified checkbox is enabled the exported workflow will be marked as verified. This Export as Verified checkbox option is only available on a UAT instance. Hence, workflows present in UAT instance only can be exported as 'Verified' workflows. Users should use this option only if a workflow has been appropriately tested on a UAT instance.
6. Once marked as verified the workflow will be imported as a verified workflow in Production instance.
7. Select the workflows you wish to export by clicking on the check boxes. In this case we have selected Sales Revenue .
8. In this case we have enabled the Export as Verified checkbox. Click Export.

Figure 29c: Workflow to Export as Verified

9. Workflow Exported Successfully message appears.

Name	Category	Metering Units	Created	Last Updated	Status	Actions
Sales Revenue	Default	0	17-Jun-2021 08:20:45	17-Jun-2021 08:23:58	On	✎ 📄 🗑️

Figure 29d: Workflow exported successfully

10. This completes the process of exporting workflow from UAT instance.

6.7 Workflows: Import to Production Instance

Import button on Workflow menu supports import of a zip file exported from an instance of AutomationEdge.

 **Note:** A project exported from Process Studio cannot be imported or updated directly on an AutomationEdge instance.

Once a workflow is found to be working satisfactorily on UAT instance, it is exported from UAT and imported on Production (Enterprise/Subscription) instance. Usually workflows exported as verified from UAT instance are imported on Production Instance. These workflows are marked as verified Workflows on a Production instance. Only one workflow can be imported at a time.

Import the workflow zip exported from UAT Instance. The process to import the workflow is the same as discussed for Import to UAT instances. Following are the steps to import the workflow on the Production instance.

1. Logon to a production instance (Enterprise or Subscription)

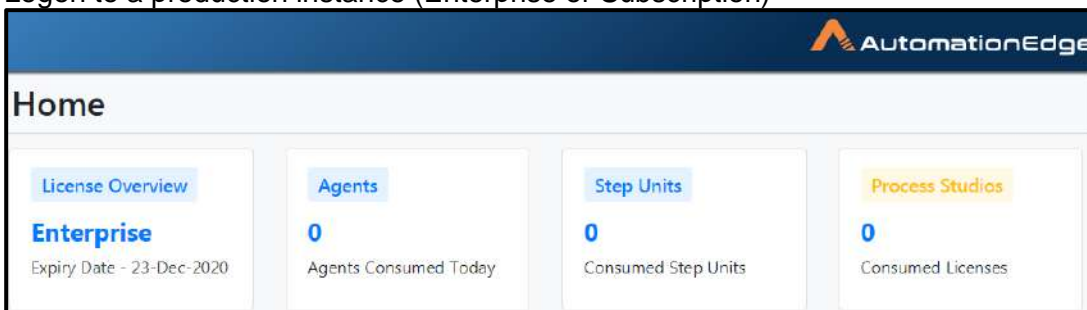


Figure 30a: Login to Enterprise or Subscription server

2. Click Workflows menu. Workflows List menu is selected by default.

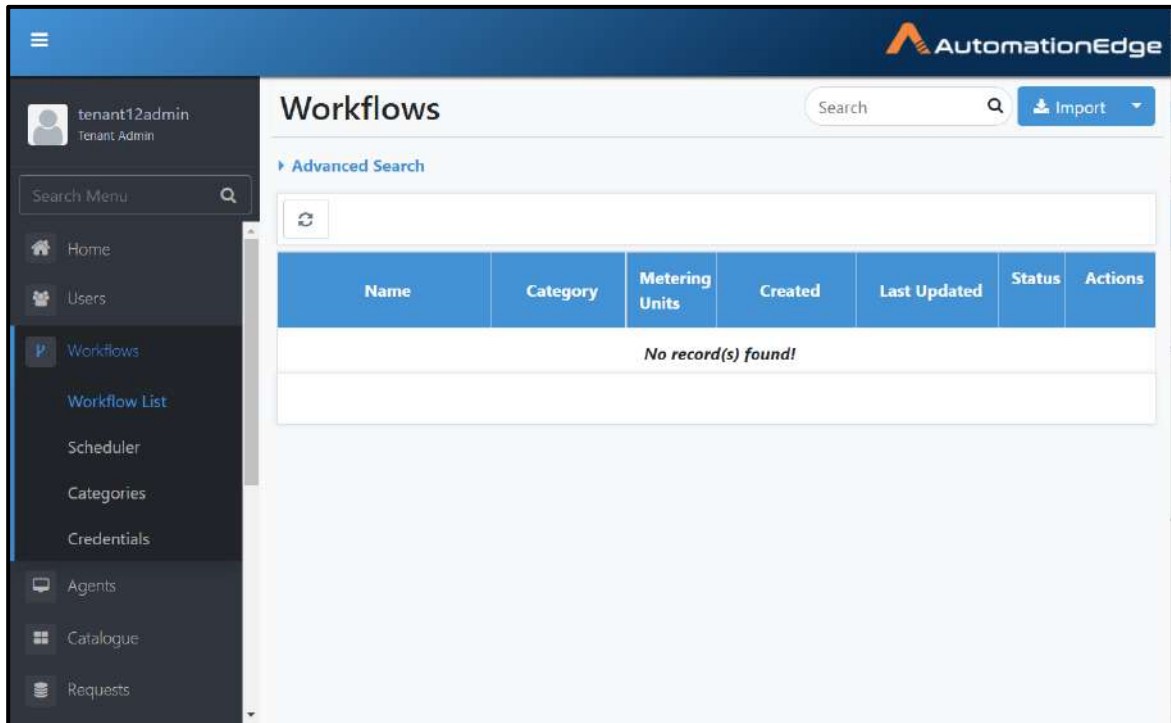


Figure 30b: Workflow Menu

3. Click the Import button. The Create New Workflow page appears.
4. Provide desired details. Browse the exported zip file from UAT instance. You can see the file contents by clicking the Show file content link. Click Create.

Create New Workflow

Workflow Name: *

Workflow Description (Maximum 128 Characters): *

Workflow Category:

Assisted Workflow

Enable RDP

Select Workflow File(.zip)*

Sales_Revenue.zip

[Show file content](#)

Content:

- [-] **Sales_Revenue.zip**
 - signature.txt
- [-] **Sales_Revenue.zip**
 - HelloWorld.psw
 - license.json
 - workflow.json

Figure 30c: Import and Configure Process Studio Workflow

5. The Configure workflow details page appears. Provide basic details as shown below.

Configure Workflow Details

▼ Basic Details


Workflow Name: **Sales Revenue**

Workflow Description (Maximum 128 Characters): *

Calculate Sales Revenue

Workflow Category:

Default

Workflow Icon: 

Assisted Workflow : **false**

Enable Sequential Execution

Enable RDP

Enable Input Attributes

Workflow Priority:

Default

Expected Completion Time(Seconds): *

5

Maximum Completion Time(Seconds): *

20

Cleanup Requests older than(Hours):

3

Manual Execution Time:

5 Hours




Figure 30d: Workflow Basic Details

6. Provide Email Notification Setting as shown below.
7. Provide values appropriately as shown below for Email Notification Settings. Click Save.

▼ Email Notification Setting

Notify On Workflow Failure

Notify On Exceeding Time Limit

Select Users*:

By Role: Tenant Admin Workflow Admin

By Username:

By Email:

Request Creator

Failure Message:

No Configuration Parameters


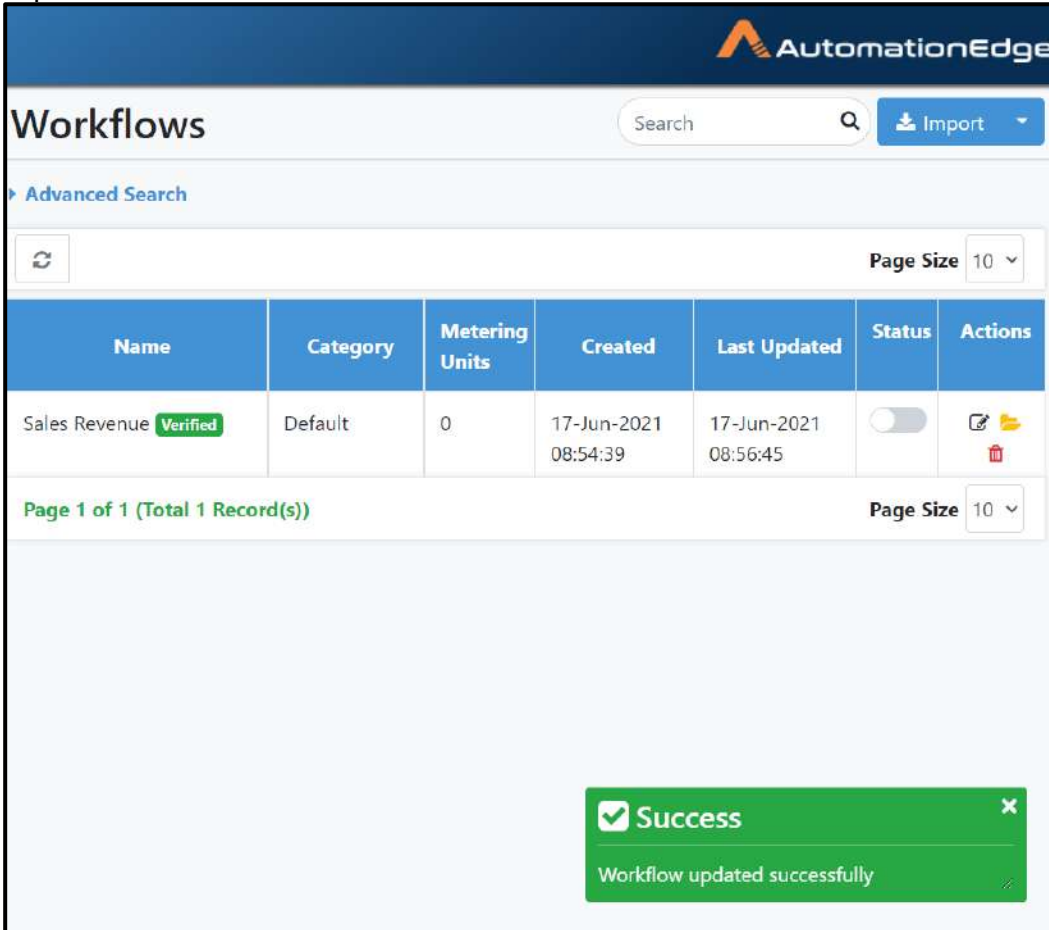


Figure 30e: Configure Workflow Email Notification Settings

8. Workflow updated successfully message appears as shown below. The workflow is now visible in the workflow list as a verified workflow since the workflow zip imported was exported as a verified workflow from UAT.



The screenshot displays the AutomationEdge interface for managing workflows. At the top, there is a search bar and an 'Import' button. Below this is an 'Advanced Search' section with a refresh icon and a 'Page Size' dropdown set to 10. The main content is a table with the following columns: Name, Category, Metering Units, Created, Last Updated, Status, and Actions. A single record is shown with the name 'Sales Revenue', which has a green 'Verified' badge. The 'Status' column for this record shows a toggle switch that is currently turned off. Below the table, there is a pagination bar indicating 'Page 1 of 1 (Total 1 Record(s))' and another 'Page Size' dropdown set to 10. A green success message box is overlaid at the bottom right, stating 'Success' and 'Workflow updated successfully'.




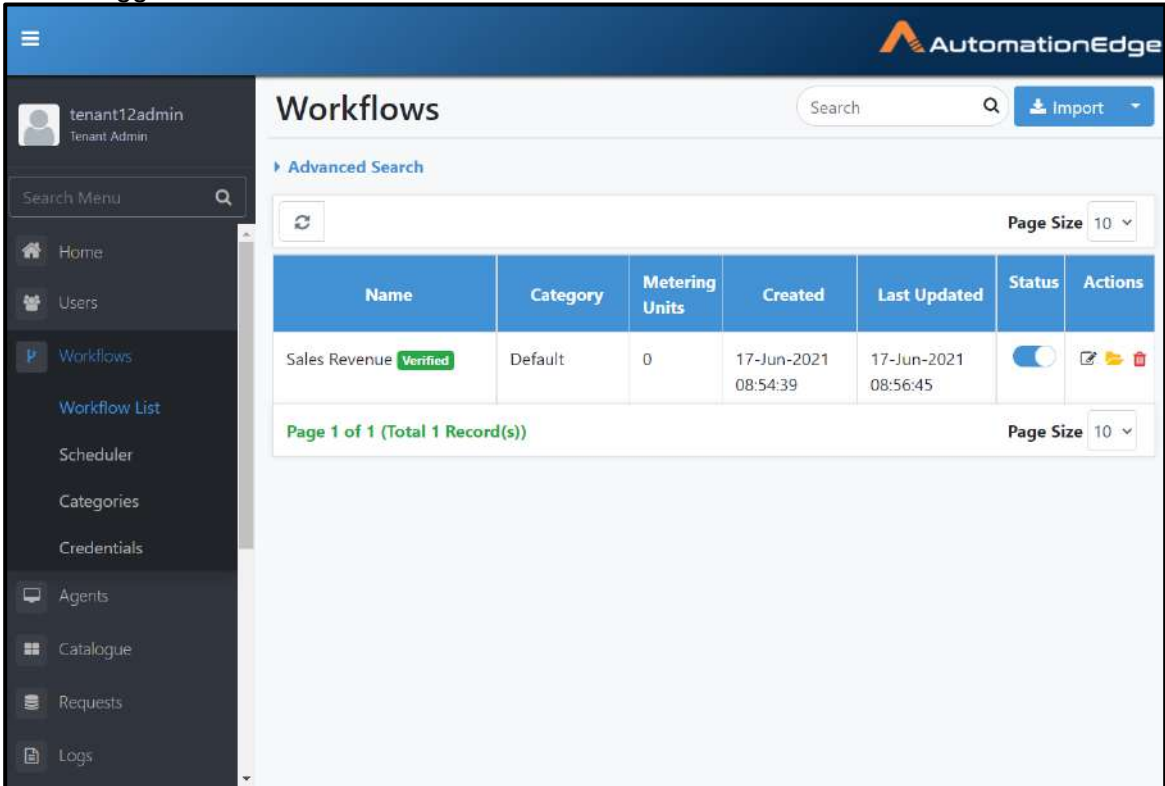



Name	Category	Metering Units	Created	Last Updated	Status	Actions
Sales Revenue Verified	Default	0	17-Jun-2021 08:54:39	17-Jun-2021 08:56:45	<input type="checkbox"/>	  

Figure 30f: Workflow Updated Success message

9. The workflow is now visible in the workflow list. Activate the workflow by clicking on the Active toggle.



The screenshot displays the AutomationEdge interface for the 'Workflows' section. The user is logged in as 'tenant12admin' (Tenant Admin). The page shows a table with one workflow record:

Name	Category	Metering Units	Created	Last Updated	Status	Actions
Sales Revenue Verified	Default	0	17-Jun-2021 08:54:39	17-Jun-2021 08:56:45	<input checked="" type="checkbox"/>	  

Page 1 of 1 (Total 1 Record(s))

Figure 30g: Verified workflow imported to Production instance

The workflow can now be assigned to an Agent. Once assigned the workflow is visible in the catalogue. Permissions can be given to users or user groups for the workflow. The workflow can now be executed from the Catalogue and monitored from the Requests menu. This is the same as was done on the UAT server in the previous sections.

6.8 Workflows: Maintain

6.8.1 Workflows: Update

Process Studio workflows can be updated. There are two ways to update workflows,

- Update Workflows from Process Studio using Publish option
- Update Workflows with Update option on Workflows List Menu

Both of these ways to update AutomationEdge workflows are discussed in the sections below.

6.8.1.1 Update Workflows from Process Studio using Publish option

In the previous section, we completed publishing a workflow for the first time with Publish→Create option, to AutomationEdge. To make updates to the workflow, use the Publish→Update option.

Following are the steps to update AutomationEdge Workflows directly from Process Studio using Publish→Update option.

1. Open Sales Revenue process in Process Studio as seen below.

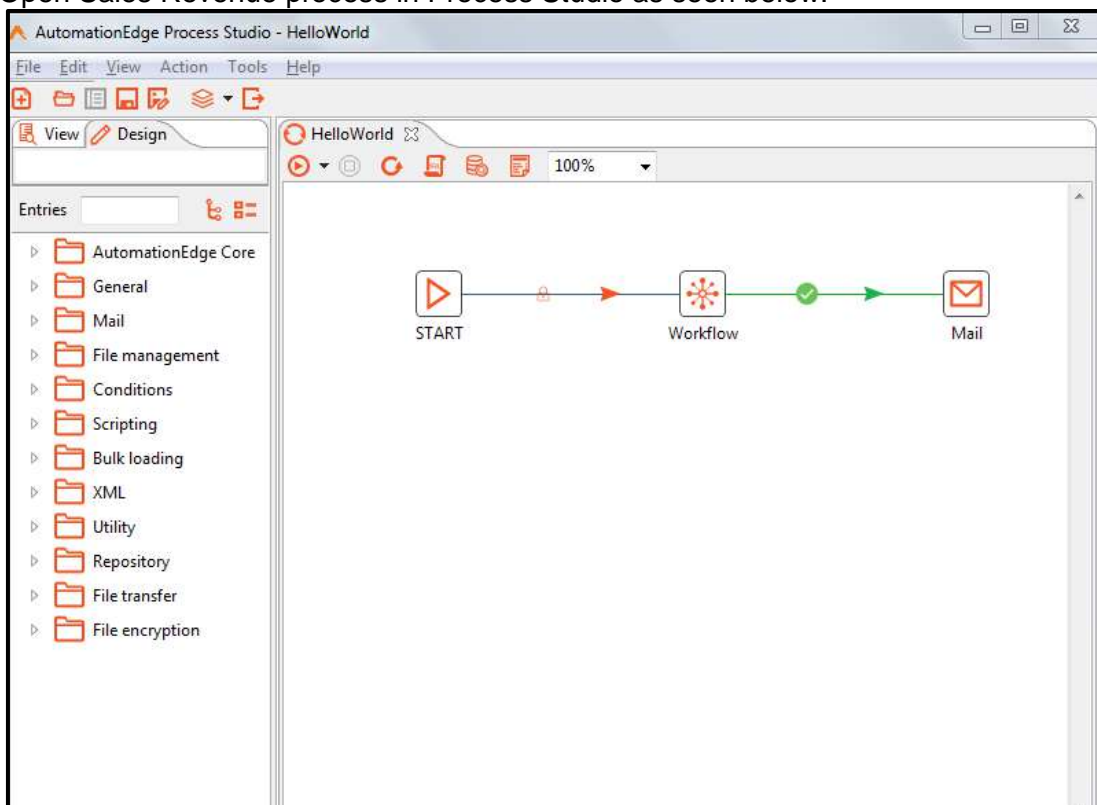


Figure 31a: Open workflow in Process Studio

2. In case you have a Process and multiple workflows then open the parent Process or parent Workflow and go to the respective tab.
3. In this case we have only one workflow hence we have selected the HelloWorld workflow.
4. Select File menu and click Publish and choose Update option.

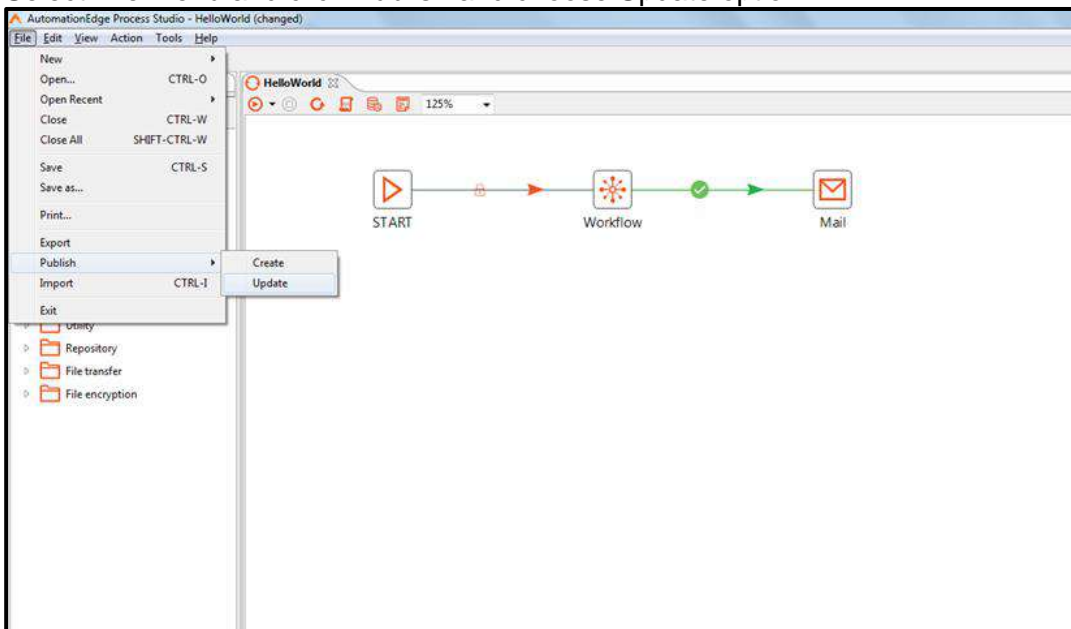


Figure 31b: Update workflow using Publish Update option

5. If you have not saved the password AutomationEdge connection Details dialog appears. Provide the password.

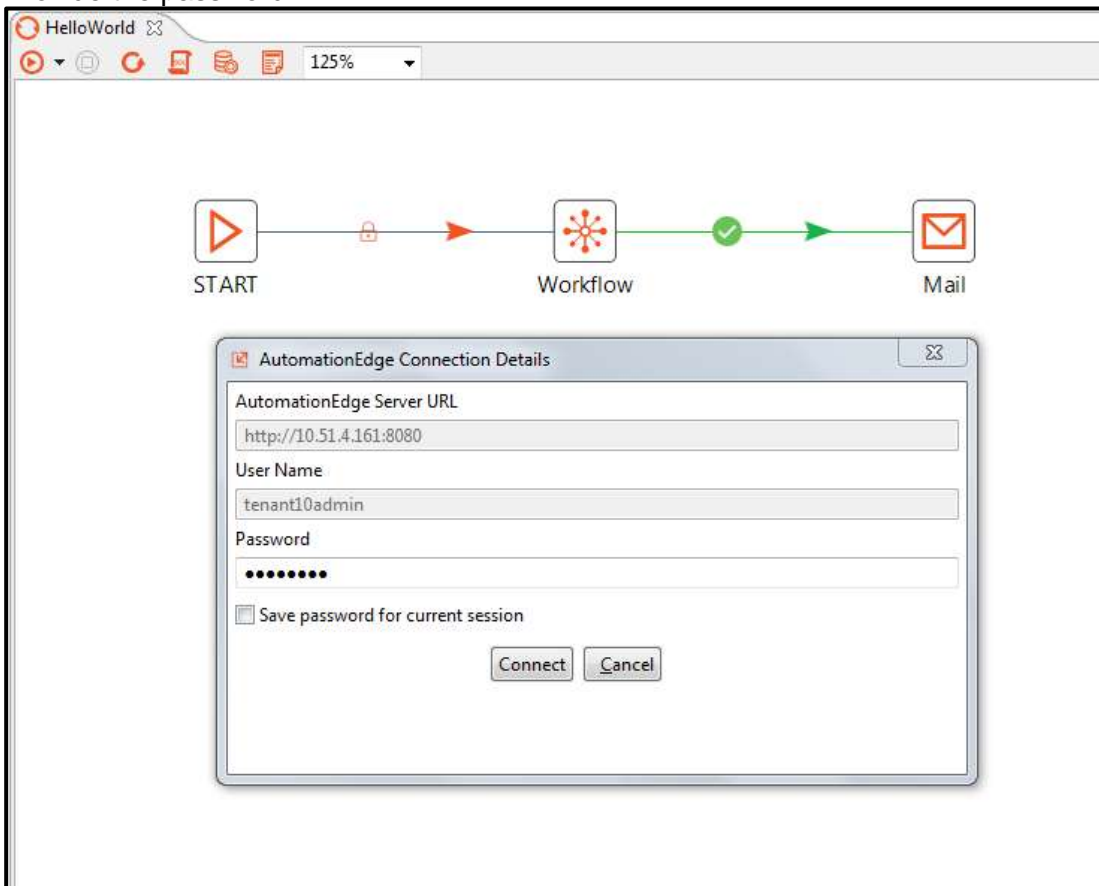


Figure 31c: Connect to AutomationEdge Server

6. A pop-up message appears warning that you must select a parent process(psp) or workflow(psw) as the case may be so that all the linked psp/psw files are exported as a zip. Acknowledge the message.
7. In this case, there are no supporting .csv, .txt, .xlsx or other files. Leave 'Add supporting files to zip archive' unchecked and click Yes.

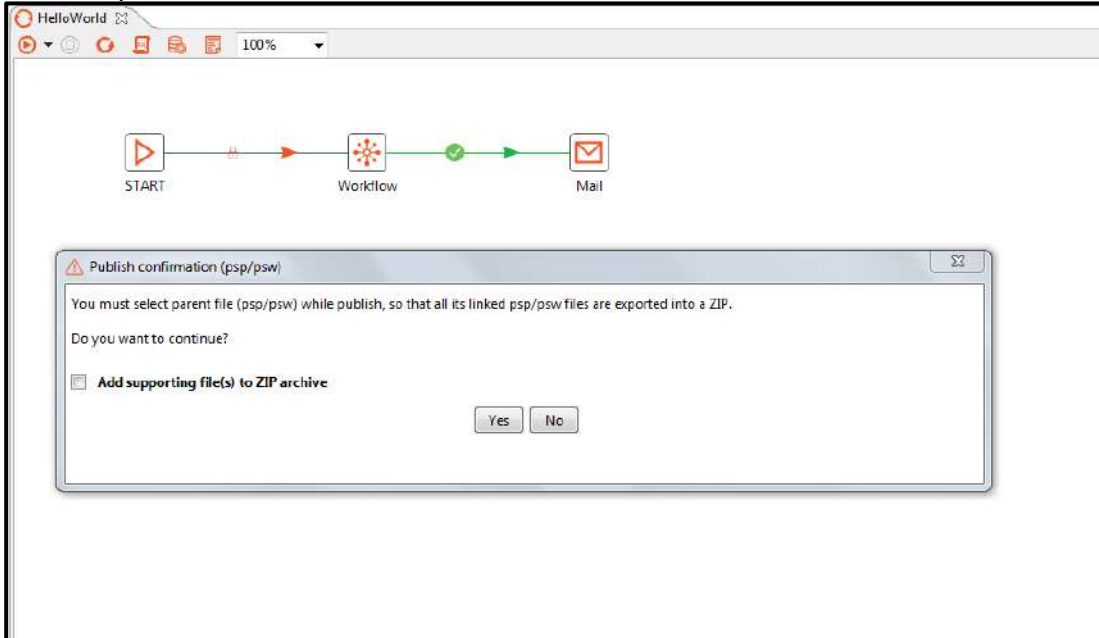


Figure 31d: Optionally Add supporting files

8. Else you may check the Add Supporting files to Zip archive to add additional or supporting files to the zip.

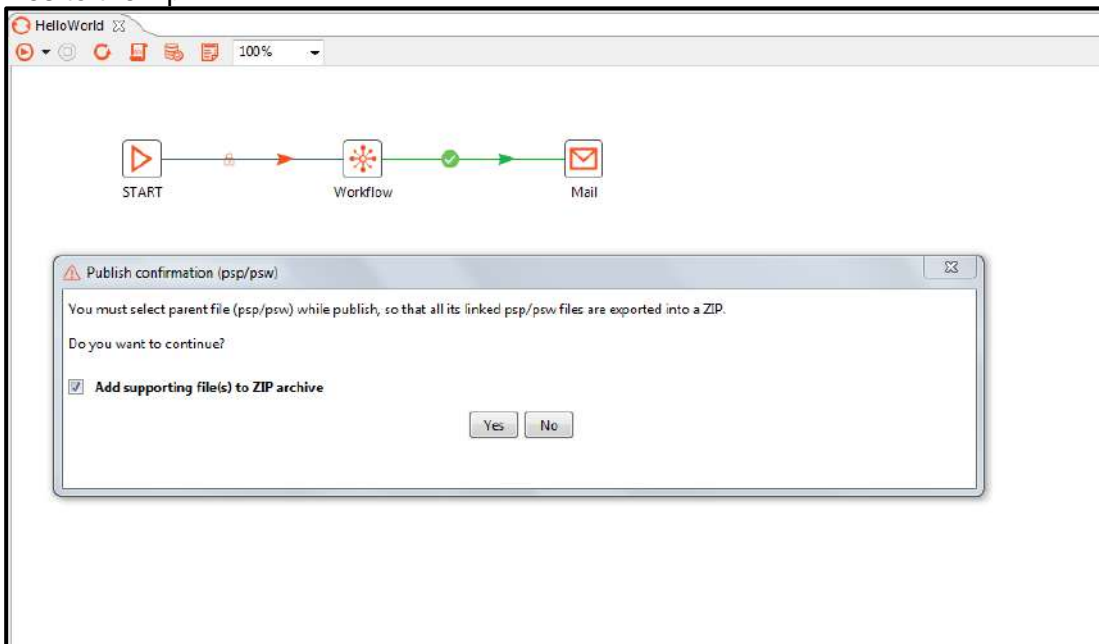


Figure 31e: Check to add supporting files to zip

9. In case you check 'Add supporting files to zip archive' a corresponding popup appears.
10. In this case we have selected the input file sales_data.csv. Click Add to Destination and then the Add button below. However, this is for demonstration purposes only. sales_data.csv is only an input file and not a supporting file, hence optional.

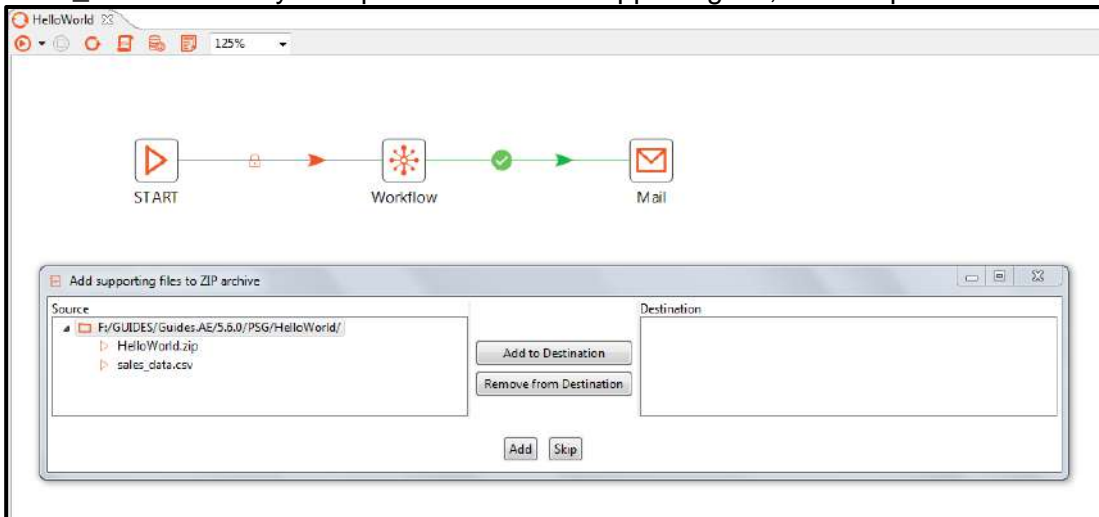


Figure 31f: choose the files to add to zip

11. A Workflow Details pop up appears with details as seen below.

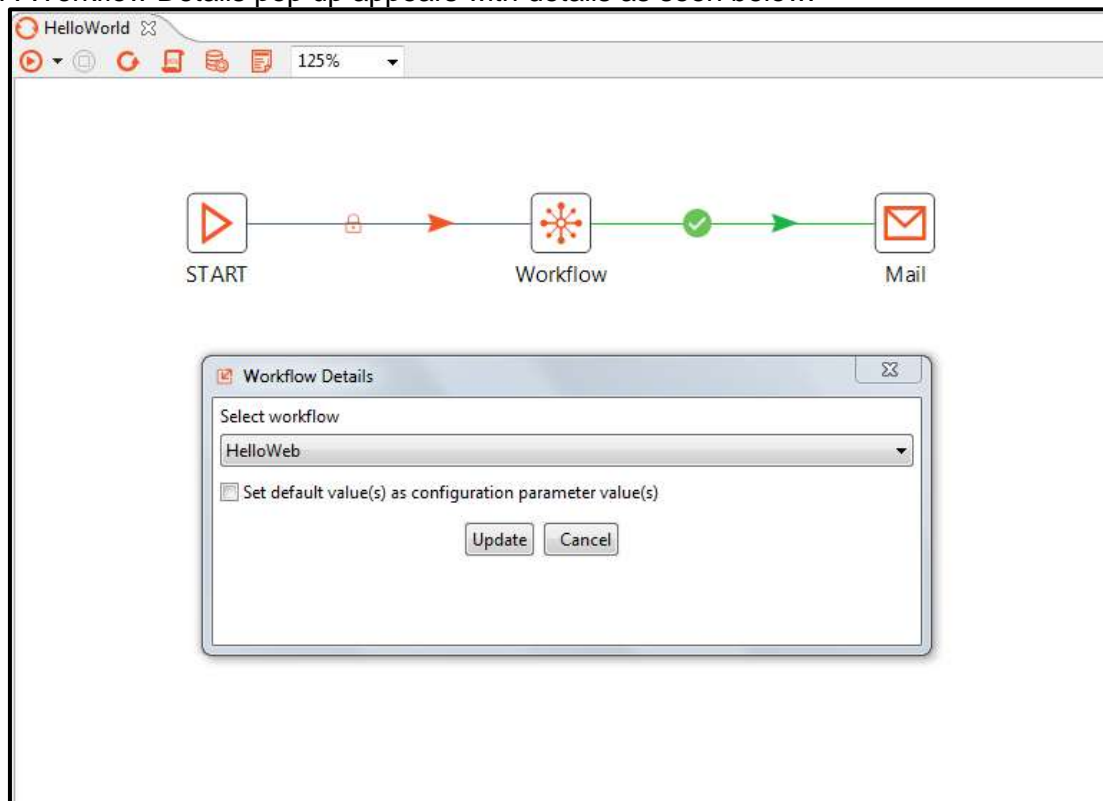


Figure 31g: Workflow configurations

12. Select the workflow to be updated from the drop down list.
13. If you do not see the workflow in this list, click More... in the drop-down list, and locate your workflow. You may use the Filter box to search narrow the list. Click OK.

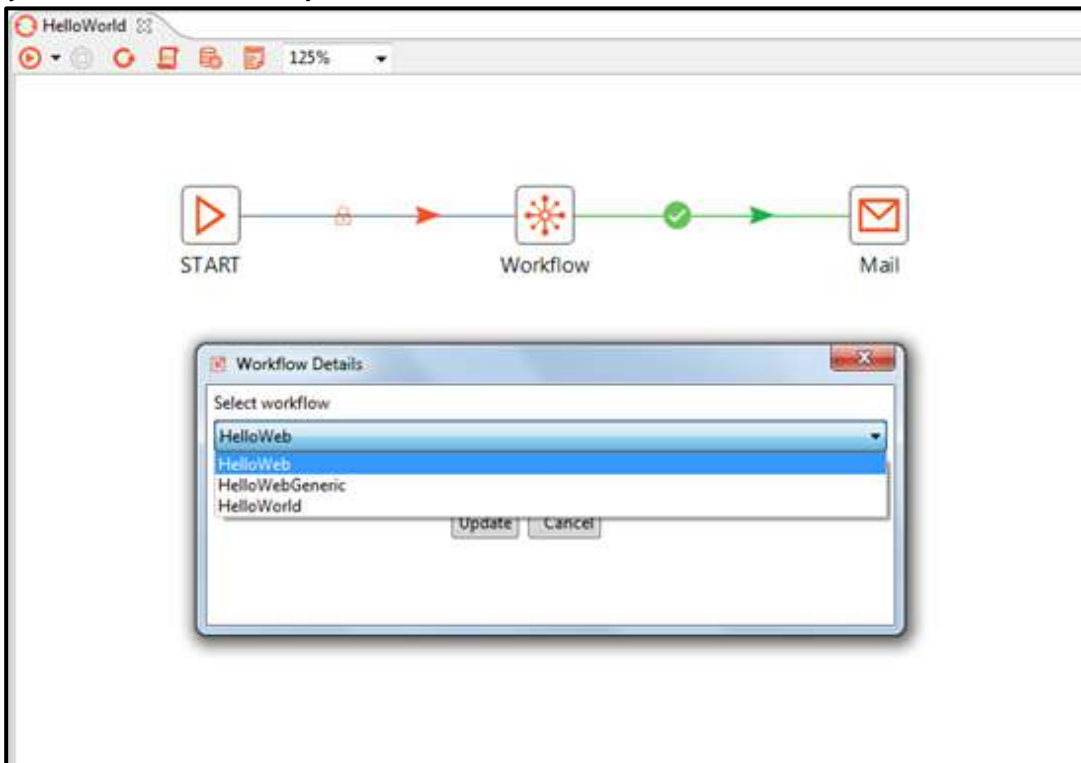


Figure 31h: Select workflow to update

14. You may check optional parameters as desired. Parameters such as Assisted, Sequential and RDP enabled are inherited from the published workflow, and not visible here.
15. If you wish to 'Set default value(s) as configuration parameter value(s) enable check box.
16. Click Update.

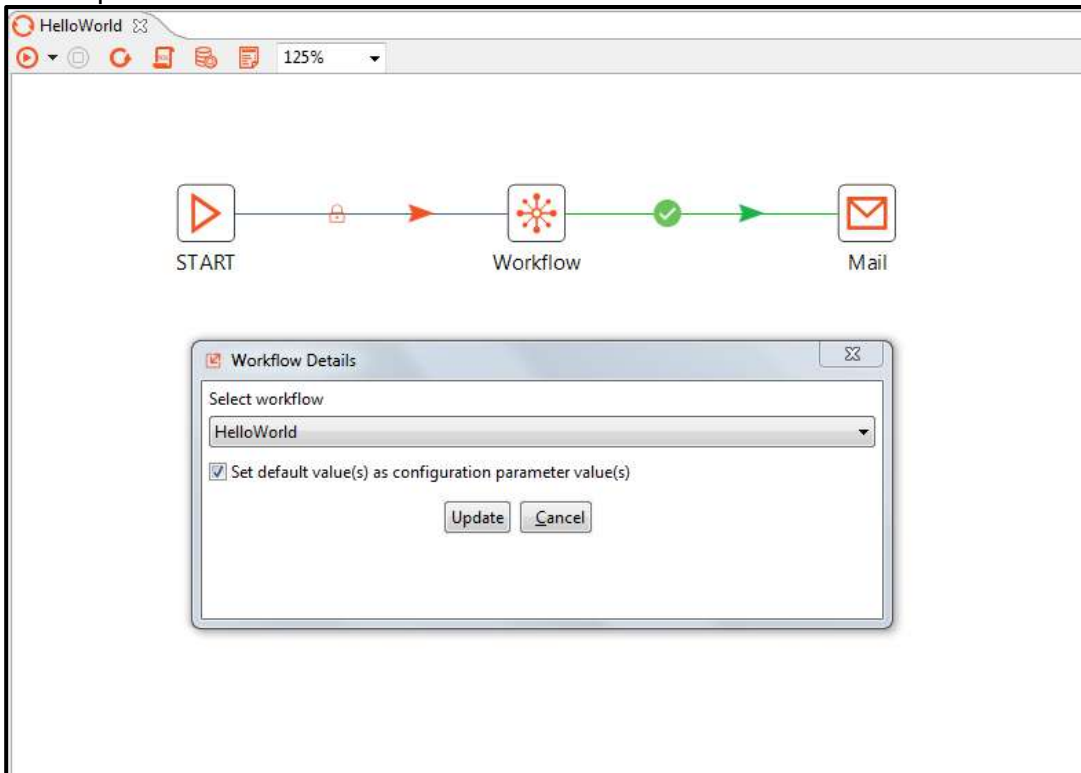


Figure 31i: set configuration parameters default values

17. A pop-up message appears showing Workflow updated successfully.

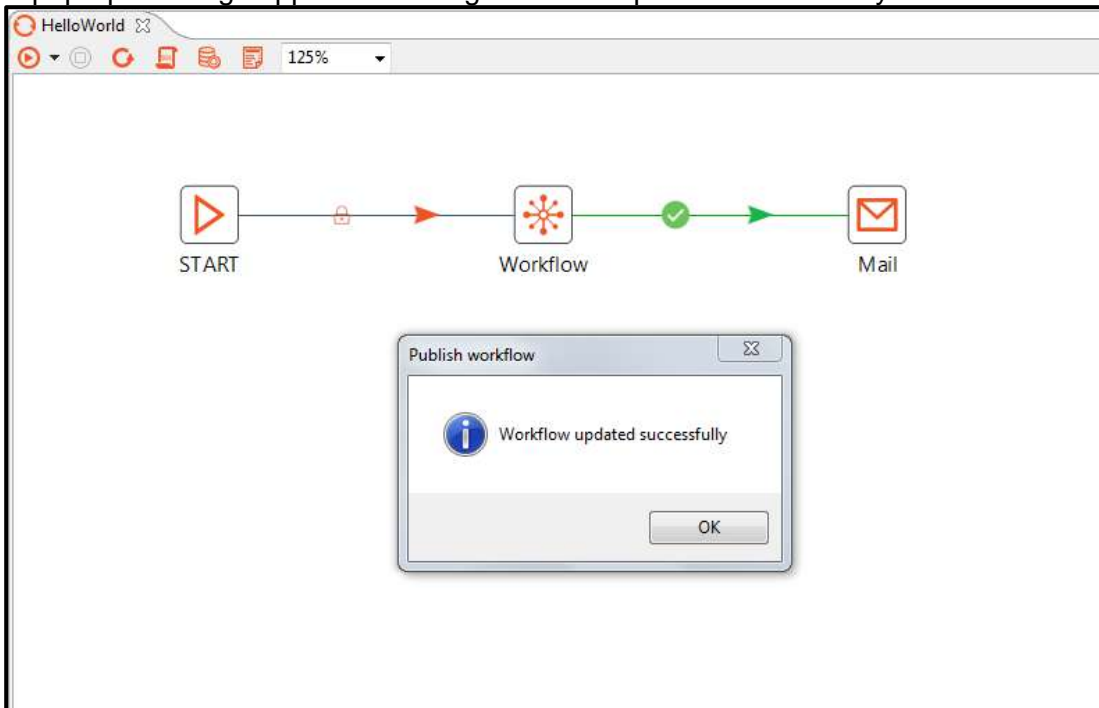
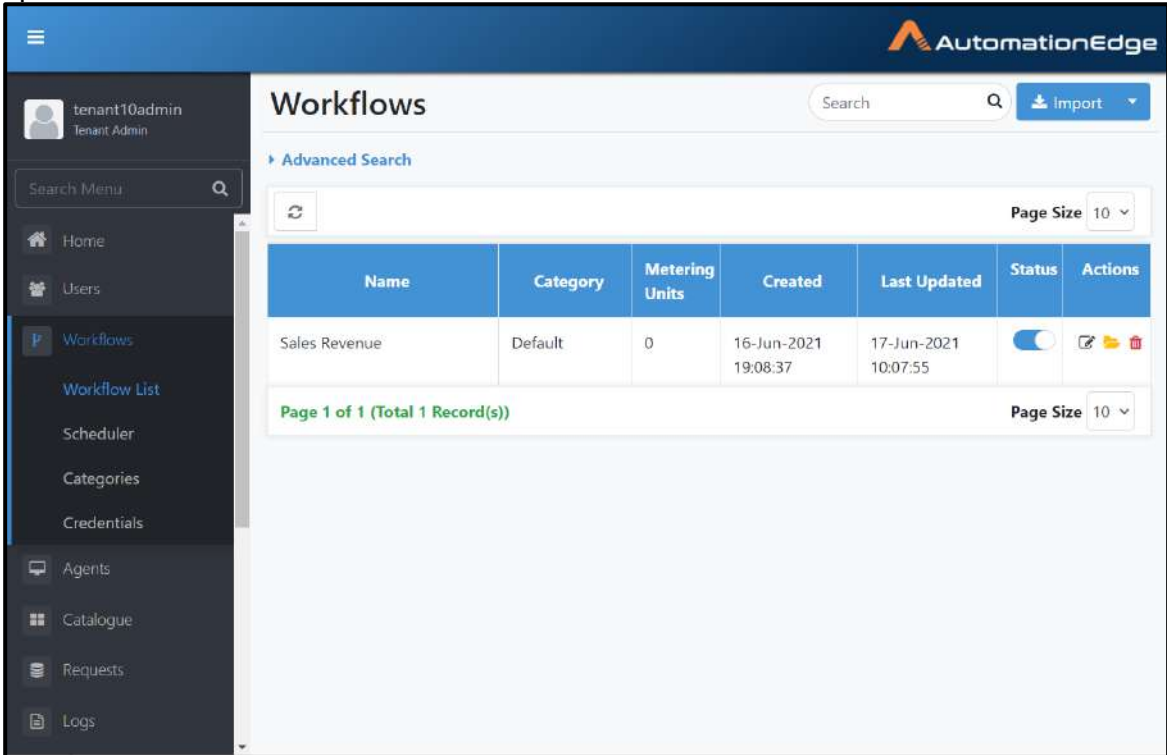





Figure 31j: Workflow updated successfully

18. This completes the update of an AutomationEdge workflow from Process Studio.
19. Now logon to AutomationEdge instance. In the Workflow List menu, you can see the updated Sales Revenue workflow.



The screenshot shows the AutomationEdge UI. The top navigation bar includes the AutomationEdge logo and a search bar. The left sidebar shows the user profile 'tenant10admin' and a menu with options: Home, Users, Workflows (selected), Workflow List, Scheduler, Categories, Credentials, Agents, Catalogue, Requests, and Logs. The main content area is titled 'Workflows' and features a search bar, an 'Import' button, and an 'Advanced Search' section. Below this is a table with the following data:

Name	Category	Metering Units	Created	Last Updated	Status	Actions
Sales Revenue	Default	0	16-Jun-2021 19:08:37	17-Jun-2021 10:07:55	On	  

Below the table, it indicates 'Page 1 of 1 (Total 1 Record(s))' and a 'Page Size' dropdown set to 10.

Figure 31k: Updated workflow on AutomationEdge UI

20. If you wish to update workflow configuration click the edit icon in the Actions column. As seen the basic details are retained as before update. Make any desired changes.

Configure Workflow Details


▼ Basic Details

Workflow Name: **HelloWorld**

Workflow Description (Maximum 128 Characters): *

Workflow Category:

Default ▼

Workflow Icon: 

Assisted Workflow : **false**

Enable Sequential Execution

Enable RDP

Enable Input Attributes

Workflow Priority:

Default ▼

Expected Completion Time(Seconds): *

Maximum Completion Time(Seconds): *

Cleanup Requests older than(Hours):

Manual Execution Time:

 Minutes ▼

► Email Notification Setting

No Configuration Parameters




Figure 311: Edit to Configure workflow details

21. Configure Email Notification Setting as seen below. Click Save.

Configure Workflow Details

▼ Email Notification Setting

Notify On Workflow Failure

Notify On Exceeding Time Limit

Select Users*:

By Role: Tenant Admin Workflow Admin

By Username:

By Email:

Request Creator

Failure Message:

No Configuration Parameters

Figure 31m: Configure Notification Settings

22. Workflow updated successfully message appears.

Workflows

Advanced Search

Page Size 10

Name	Category	Metering Units	Created	Last Updated	Status	Actions
Sales Revenue	Default	0	16-Jun-2021 19:08:37	17-Jun-2021 12:05:27	<input checked="" type="checkbox"/>	

Page 1 of 1 (Total 1 Record(s))
Page Size 10

✔ **Success** ✕

Workflow updated successfully

Figure 31n: Workflow updated successfully

23. We have seen the Process of updating AutomationEdge workflow using the publish option in Process Studio.

6.8.1.2 Update Workflows with Update option on Workflows List Menu

Following are the steps to update AutomationEdge Workflows using Update option on Workflows List menu.

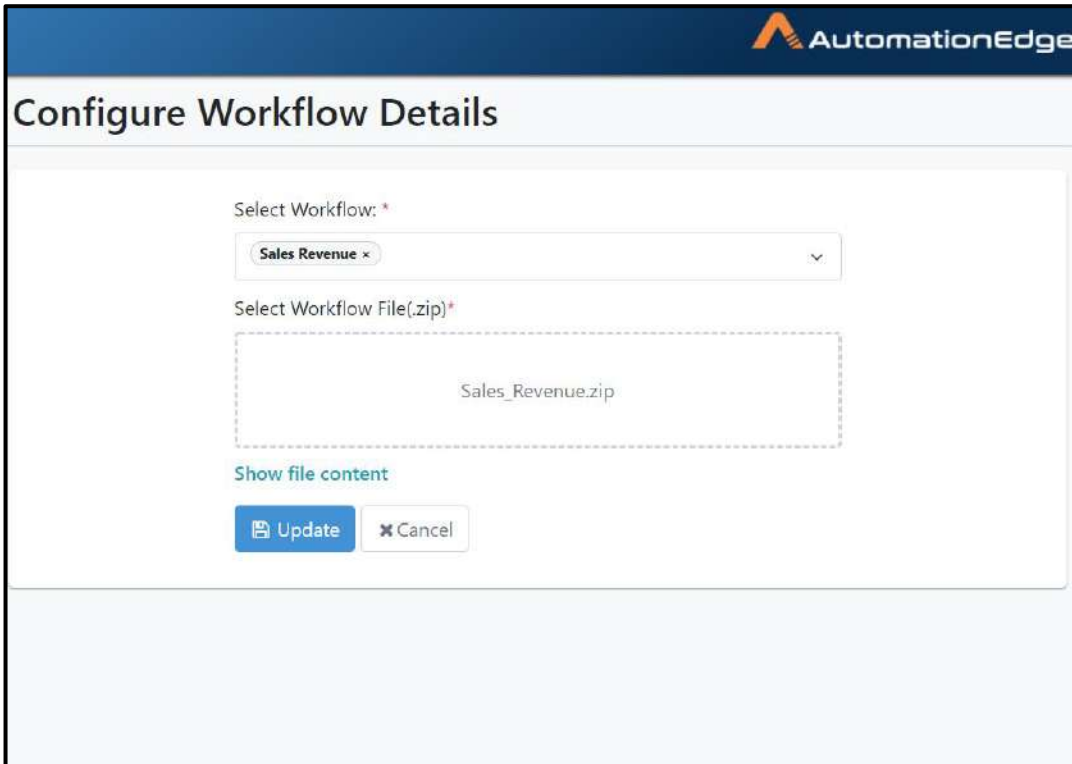
1. Login to AutomationEdge as a Tenant Administrator or Workflow Administrator user. Go to the workflows menu. Click the arrow on the 'Import' button. Select Update.

The screenshot displays the AutomationEdge Workflows management interface. The left sidebar shows the user 'tenant10admin' and a navigation menu with options like Home, Users, Workflows, Scheduler, Categories, Credentials, Agents, Catalogue, Requests, and Logs. The main content area is titled 'Workflows' and features a search bar, an 'Import' button with a dropdown menu (showing 'Update' and 'Export'), and a 'Page Size' selector set to 10. Below this is an 'Advanced Search' section with a refresh icon. The main table lists workflow records with columns for Name, Category, Metering Units, Created, Last Updated, Status, and Actions. One record is visible: 'Sales Revenue' (Category: Default, Metering Units: 0, Created: 16-Jun-2021 19:08:37, Last Updated: 17-Jun-2021 12:05:27, Status: On). The table footer indicates 'Page 1 of 1 (Total 1 Record(s))' and another 'Page Size' selector set to 10.

Name	Category	Metering Units	Created	Last Updated	Status	Actions
Sales Revenue	Default	0	16-Jun-2021 19:08:37	17-Jun-2021 12:05:27	On	[Edit] [Update] [Delete]

Figure 31o: Update Process Studio Workflow

2. The following screen appears. Click Select Workflow. Search for the workflow or enable checkbox next to the workflow you wish to update. Sales Revenue is selected as shown below.
3. Browse for a workflow zip file, exported from an AutomationEdge instance. Click Update.



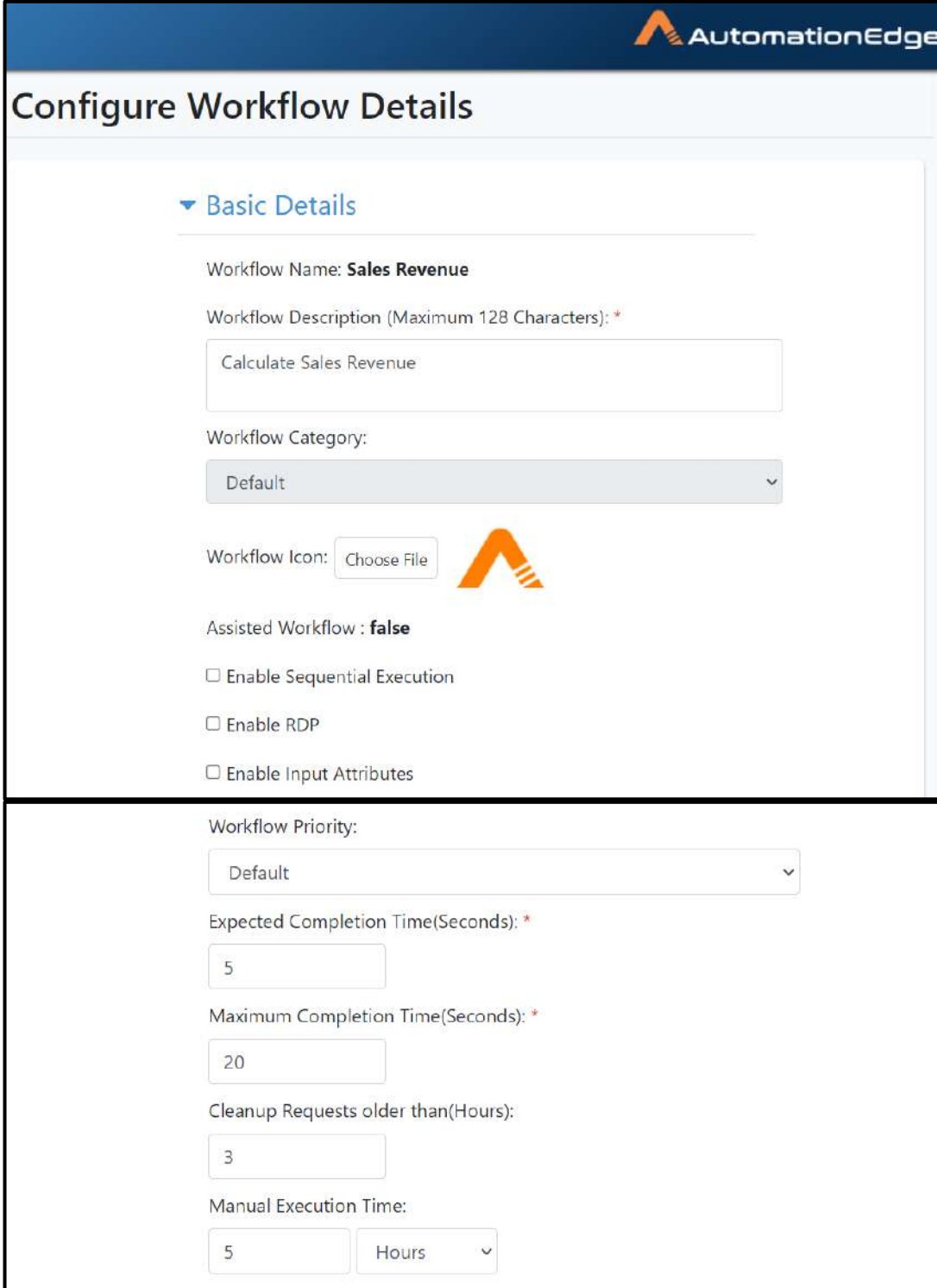
The screenshot displays the 'Configure Workflow Details' page. At the top, the AutomationEdge logo is visible. The main heading is 'Configure Workflow Details'. Below this, there are two main sections:

- Select Workflow: ***: A dropdown menu with 'Sales Revenue' selected and a close button (x).
- Select Workflow File(.zip): ***: A dashed box representing a file upload area, containing the text 'Sales_Revenue.zip'. Below this box is a link labeled 'Show file content'.

At the bottom of the form, there are two buttons: a blue 'Update' button with a document icon and a white 'Cancel' button with an 'x' icon.

Figure 31p: Select Workflow and the Workflow zip

4. Make changes to the Configure Workflow Details page as desired.



AutomationEdge

Configure Workflow Details

▼ Basic Details


Workflow Name: **Sales Revenue**

Workflow Description (Maximum 128 Characters): *

Calculate Sales Revenue

Workflow Category:

Default

Workflow Icon: 

Assisted Workflow : **false**

Enable Sequential Execution

Enable RDP

Enable Input Attributes

Workflow Priority:

Default

Expected Completion Time(Seconds): *

5

Maximum Completion Time(Seconds): *

20

Cleanup Requests older than(Hours):

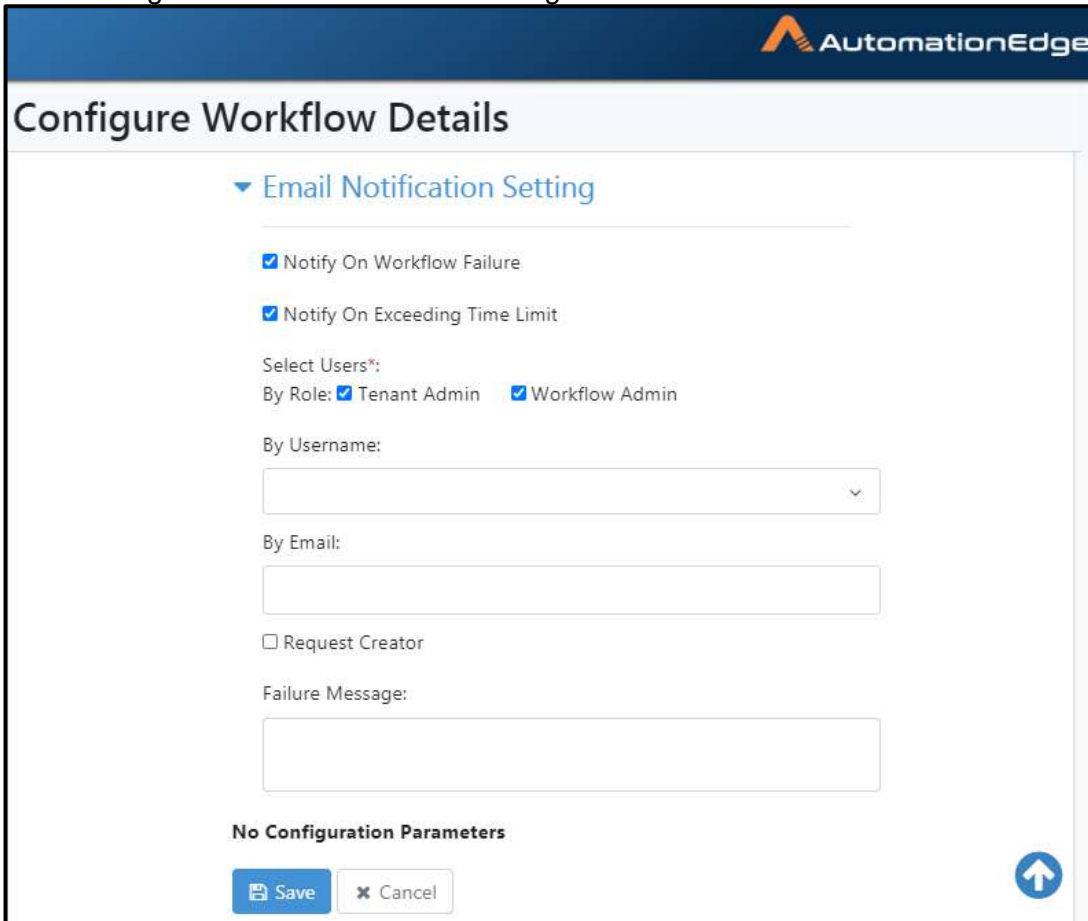
3

Manual Execution Time:

5

Figure 31q: Configure Workflow Basic Details

5. Make changes to Email Notification Setting as desired. Click Save.



The screenshot shows the 'Configure Workflow Details' interface. At the top, there is a blue header with the AutomationEdge logo. Below the header, the title 'Configure Workflow Details' is displayed. The main content area is titled 'Email Notification Setting' and contains the following options:

- Notify On Workflow Failure
- Notify On Exceeding Time Limit
- Select Users*:
 - By Role: Tenant Admin Workflow Admin
 - By Username:
 - By Email:
 - Request Creator
 - Failure Message:

At the bottom of the form, there is a section labeled 'No Configuration Parameters' with two buttons: 'Save' and 'Cancel'. A blue circular arrow icon is located in the bottom right corner of the form area.

Figure 31r: Configure Workflow Notification Setting

- Workflow updated successfully message appears.

The screenshot shows the AutomationEdge interface for managing workflows. At the top, there is a search bar and an 'Import' button. Below this is an 'Advanced Search' section with a refresh icon and a 'Page Size' dropdown set to 10. The main content is a table with the following data:

Name	Category	Metering Units	Created	Last Updated	Status	Actions
Sales Revenue	Default	0	16-Jun-2021 19:08:37	17-Jun-2021 12:14:47	<input checked="" type="checkbox"/>	

Below the table, it indicates 'Page 1 of 1 (Total 1 Record(s))' and another 'Page Size' dropdown set to 10. At the bottom right, a green success message box is displayed with the text: 'Success Workflow updated successfully'.

Figure 31s: Update Success message

6.8.2 Workflows: View

To view the workflows created on AutomationEdge server,

1. Click Workflow menu. Workflow List sub-menu is selected by default.
2. View the complete list of workflows on this Workflows Page.

Name	Category	Metering Units	Created	Last Updated	Active	Actions
HelloWorld	Default	0	21-Jul-2020 20:15:21	5-Aug-2020 09:39:50	<input checked="" type="checkbox"/>	
HelloWebGeneric	Default	0	21-Jul-2020 15:43:21	21-Jul-2020 15:50:56	<input checked="" type="checkbox"/>	
HelloWeb	Default	0	21-Jul-2020 09:08:51	21-Jul-2020 09:12:22	<input checked="" type="checkbox"/>	

Page 1 of 1 (Total 3 Record(s))

Figure 32a: View Workflow List

Table 18: Configured Workflow Field Description

Field Name	Description
Name	Displays workflow name.
Category	Displays workflow category.
Metering Units	Displays the number of step metering units consumed by the workflow.
Created	Displays workflow creation date & time
Last Updated	Displays the last updated date of the workflow.
Active	Toggle to activate or deactivate workflows.
Actions:	
<input type="checkbox"/> Edit ()	Click to edit workflow configurations.
<input type="checkbox"/> Show workflow files()	Click to display workflow files.
<input type="checkbox"/> Delete()	Click to delete the workflow.

6.8.3 Workflows: Search

1. Type a string in the Search Box to filter workflow list.

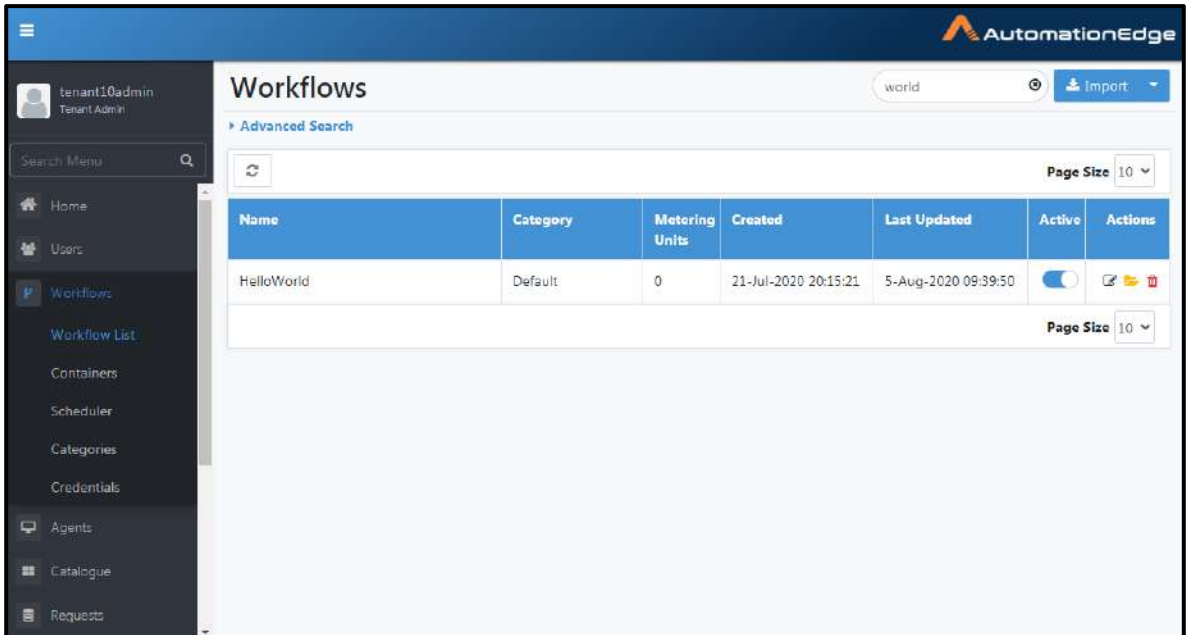


Figure 32b: Search String

6.8.4 Workflows: Advanced Search

To search workflows using Advanced Search:

1. Navigate to Workflows→ Workflow List.
2. Click Advanced Search. Choose a column to set a filter condition.

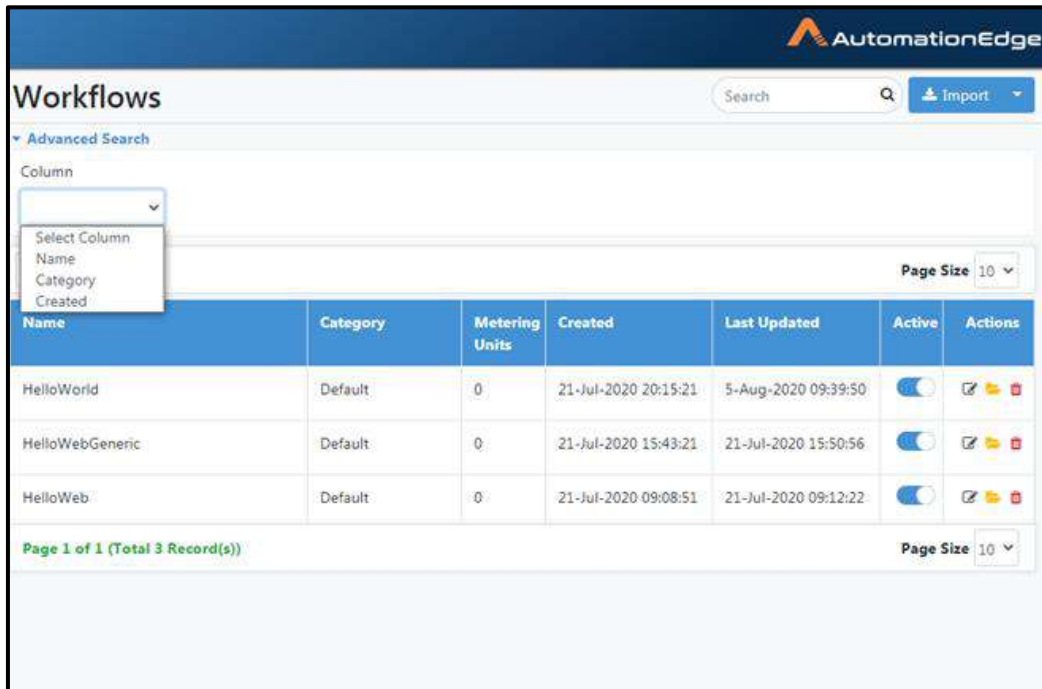


Figure 32c: Workflows Advanced Search

- The search options for Name and Category are the same as shown for Category below.
- Select a comparator from the drop down list.

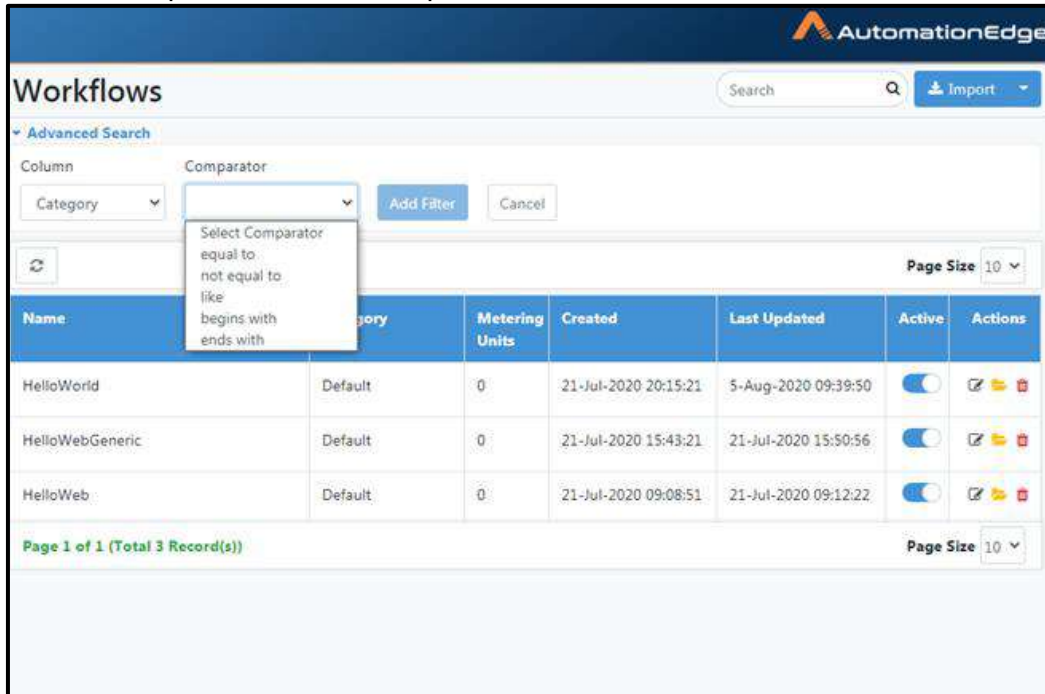


Figure 32d: Search Filters by Name

- Provide a desired Value. Click Add Filter.

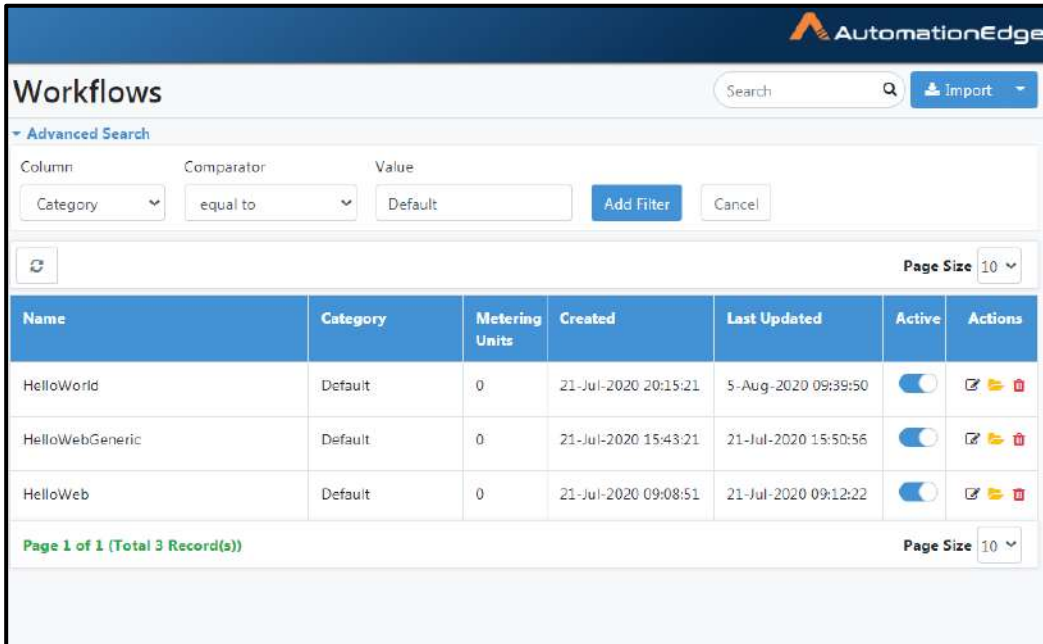


Figure 32e: Search Filters by Date

6. The first filter is added with Category value default. You can now see a filtered list of workflows.
7. You may delete individual filters or clear the entire list of filters by clicking Clear Filters.

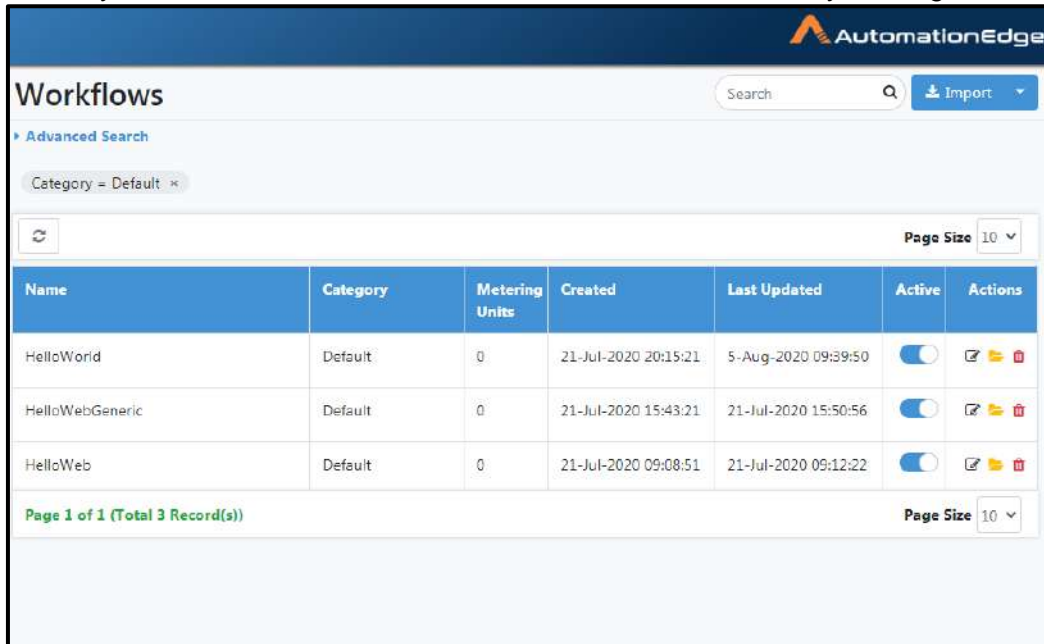


Figure 32f: Added Filter

8. This completes the Advanced Search process.

Advanced search options for workflows are explained below. They are available for Name, Category and Created date.

Table 19: Advanced Search Options by Name

Advanced Search Comparators by name(for Name, Category):	
Drop down list Field	Description
Equal To	To search entries matching the entered text.
Not Equal To	To search entries not matching the entered text.
Like	To search entries containing the entered text
Begins With	To search entries that begin with the entered text.
Ends With	To search entries that end with the entered text.

Table 20: Advanced Search Options by Date

Advanced Search Comparators by date(for created date)	
Drop down list Field	Description
Exact Date	To search entries by the exact entered date.
Before	To search entries before the entered date.
After	To search entries after the entered date.
In Between	To search entries in between the entered dates.
Not In Between	To search entries not in between the entered dates.

Table 21: Advanced Search Options by Status

Field	Description
Equal To	To search entries by the exact entered text.
Not Equal To	To search entries not matching the entered text.

6.8.5 Workflows: Actions

Perform actions on AutomationEdge workflows,

1. Navigate to the Workflows→Workflow List sub-menu.
2. The workflow list is displayed, the Actions column displays icons for four actions, discussed in the sections below.
 - Version History (📄)
 - Edit (✎)
 - Open File (📁)
 - Delete (🗑)

6.8.5.1 Workflow: Edit

Edit Process Studio workflows. Following are the steps to edit workflows,

1. Click the Edit icon (✎) corresponding to the workflow you wish to edit.

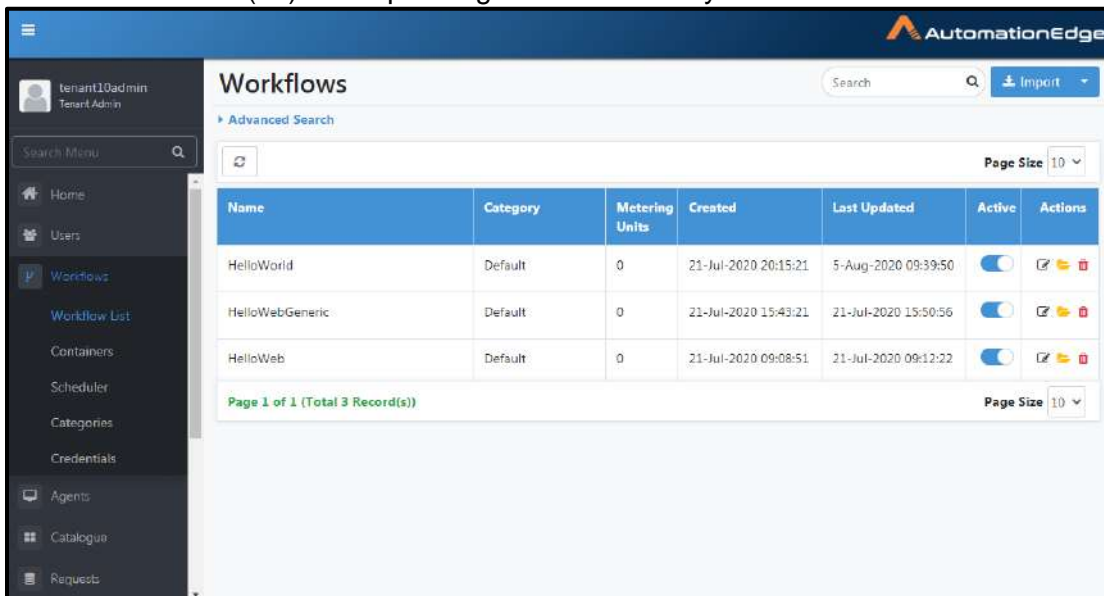


Figure 33a: Selecting Workflow to Configure

2. Update the details. The editable fields are Workflow Description, Workflow Icon, Is Sequential Execution, Expected Completion Time (seconds), Maximum Completion Time (seconds) and Configuration Parameters

3. Click Save to save the updated workflow details.

Configure Workflow Details


▼ Basic Details

Workflow Name: **HelloWorld**

Workflow Description (Maximum 128 Characters): *

Workflow Category:

Default ▼

Workflow Icon: 

Assisted Workflow : **false**

Enable Sequential Execution

Enable RDP

Enable Input Attributes

Workflow Priority:

Default ▼

Expected Completion Time(Seconds): *

Maximum Completion Time(Seconds): *

Cleanup Requests older than(Hours):

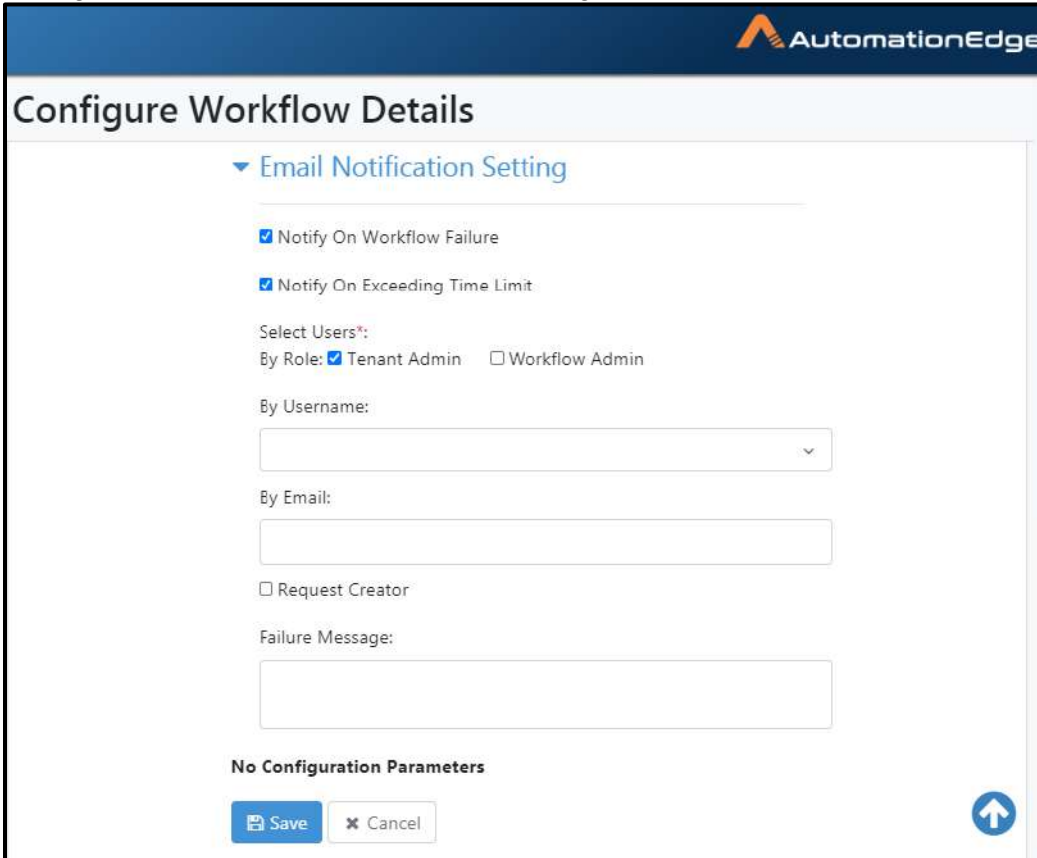
Manual Execution Time:

 ▼

Figure 33b: Configure Workflow Basic Details

4. Email notification settings Notify on Workflow Failure and Notify On Exceeding Time Limit can be enabled. Once enabled additional fields are visible as shown below.
5. Users can be notified by role such as enabling Tenant Admin and Workflow Admin roles. A list of usernames can be provided in the By Username field, a list of email addresses can be provided in the By Email field or Request Creator can be notified by enabling the Request Creator check box. Failure message can be provided in the text box.
6. The process parameters can be seen in the Configuration Parameters section.
7. Note: While creating input/output process parameters please use the internal parameter `'${Internal.Entry.Current.Directory}'` to assign the current working directory of the 'Process Studio process' as the directory containing the input and output files. Click Save.

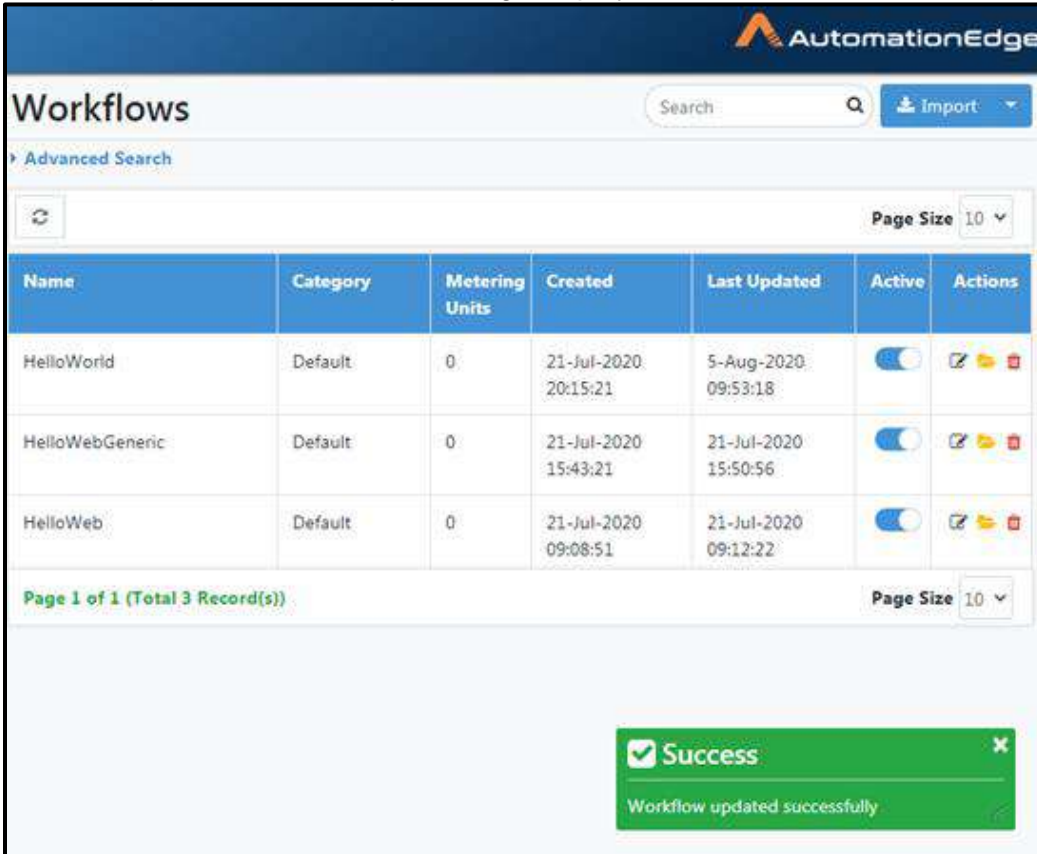
8. Configure Workflow Email Notification Setting as below.












The screenshot shows a web interface titled "Configure Workflow Details" with the AutomationEdge logo in the top right. The main section is "Email Notification Setting" with a dropdown arrow. It contains two checked checkboxes: "Notify On Workflow Failure" and "Notify On Exceeding Time Limit". Below these is the "Select Users*" section with "By Role:" and two options: "Tenant Admin" (checked) and "Workflow Admin" (unchecked). There are three input fields: "By Username:" (a dropdown menu), "By Email:" (a text box), and "Request Creator" (a checkbox). A "Failure Message:" text box is at the bottom. A "No Configuration Parameters" message is displayed above the "Save" and "Cancel" buttons. A blue circular button with an upward arrow is in the bottom right corner.

Figure 33b: Configure Workflow Notification Settings

9. Workflow updated successfully message displays as shown below.



The screenshot displays the AutomationEdge Workflows management interface. At the top, there is a search bar and an 'Import' button. Below this is an 'Advanced Search' section with a refresh icon and a 'Page Size' dropdown set to 10. The main content is a table with the following data:

Name	Category	Metering Units	Created	Last Updated	Active	Actions
HelloWorld	Default	0	21-Jul-2020 20:15:21	5-Aug-2020 09:53:18	<input checked="" type="checkbox"/>	  
HelloWebGeneric	Default	0	21-Jul-2020 15:43:21	21-Jul-2020 15:50:56	<input checked="" type="checkbox"/>	  
HelloWeb	Default	0	21-Jul-2020 09:08:51	21-Jul-2020 09:12:22	<input checked="" type="checkbox"/>	  

Below the table, it shows 'Page 1 of 1 (Total 3 Record(s))' and another 'Page Size' dropdown set to 10. A green success message box is visible in the bottom right corner, containing a checkmark icon, the text 'Success', and 'Workflow updated successfully'.

Figure 33c: Workflow Update Message

6.8.5.2 Workflows: View File Structure

To view a workflow file structure,

1. Navigate to the Workflows→Workflow List
2. Click on the Show workflow files in the Actions column.

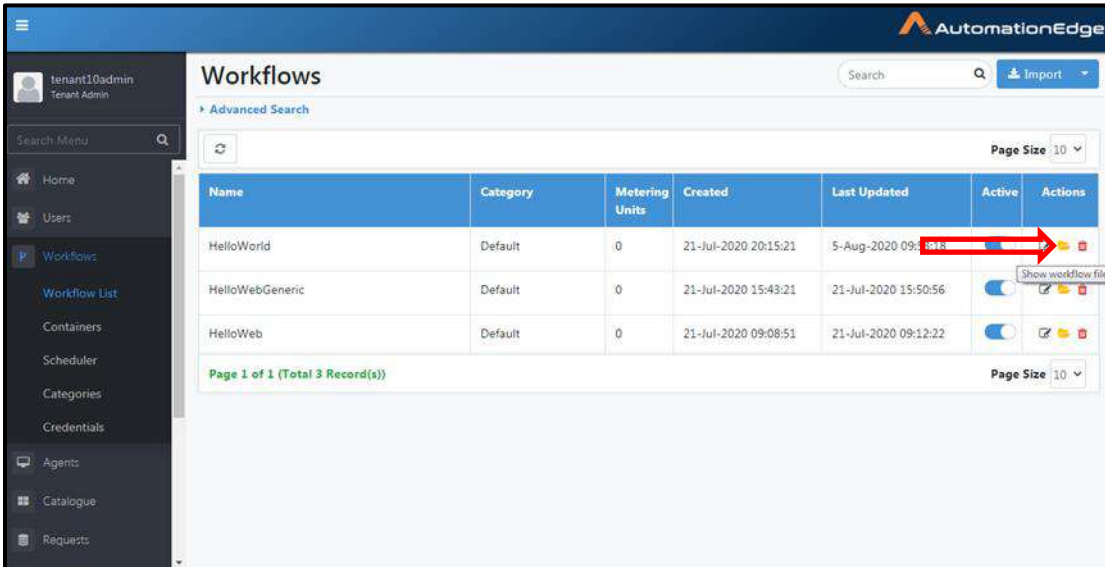


Figure 33d: Show Workflow files

3. A pop-up showing the contents of the workflow zip can be seen as below.

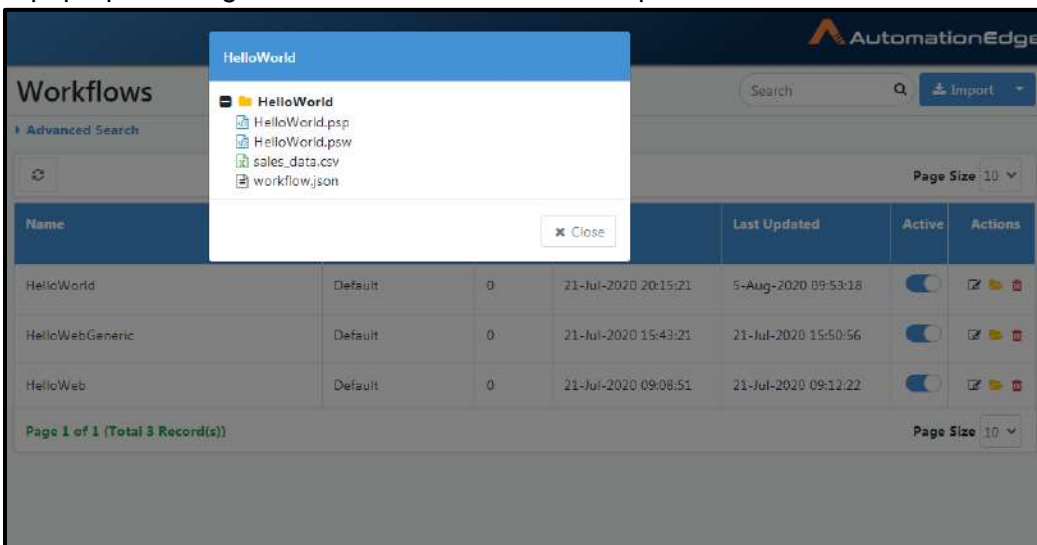


Figure 33e: Workflow zip files

6.8.5.3 Workflows: Delete

To delete workflow:

1. Click Workflows.
2. Click Configured Workflows.
3. Click the delete icon (🗑️) corresponding to the workflow to be deleted

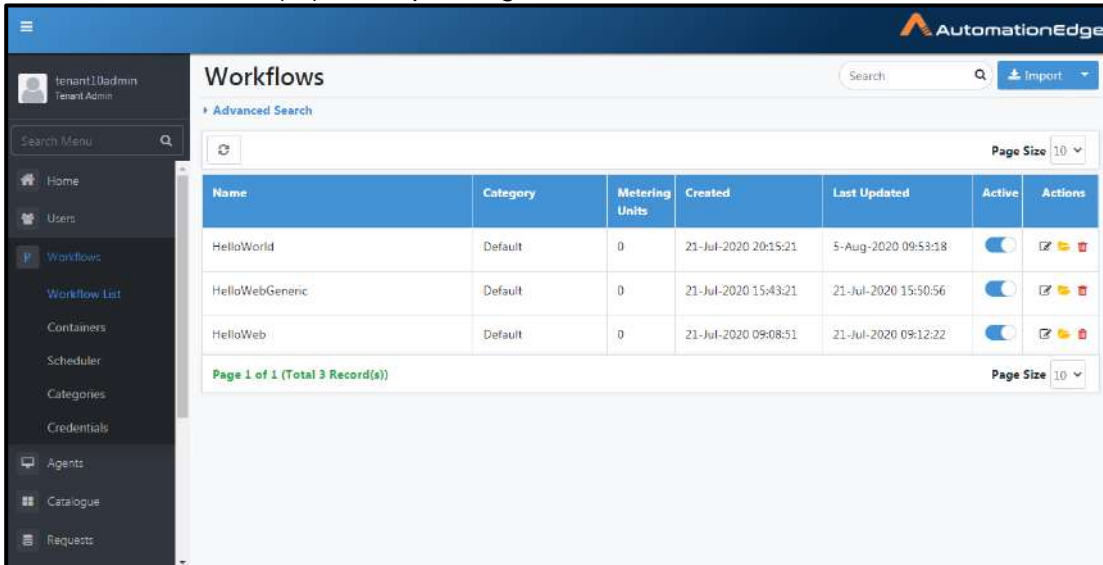


Figure 34a: Select Workflow to be deleted

4. Click Delete to confirm deletion of the workflow

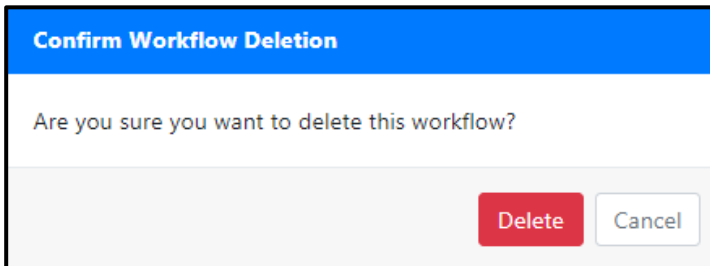


Figure 34b: Confirmation of Deletion of Workflow

5. If requests have been submitted for the workflow, then a message appears – Cannot delete workflow as requests have been submitted for the workflow.

The screenshot shows the AutomationEdge Workflows interface. At the top, there is a search bar and an 'Import' button. Below the search bar is an 'Advanced Search' section. The main content is a table with the following columns: Name, Category, Metering Units, Created, Last Updated, Active, and Actions. The table contains three rows of workflow data:

Name	Category	Metering Units	Created	Last Updated	Active	Actions
HelloWorld	Default	0	21-Jul-2020 20:15:21	5-Aug-2020 09:53:18	<input checked="" type="checkbox"/>	
HelloWebGeneric	Default	0	21-Jul-2020 15:43:21	21-Jul-2020 15:50:56	<input checked="" type="checkbox"/>	
HelloWeb	Default	0	21-Jul-2020 09:08:51	21-Jul-2020 09:12:22	<input checked="" type="checkbox"/>	

Below the table, there is a pagination bar showing 'Page 1 of 1 (Total 3 Record(s))' and a 'Page Size' dropdown set to 10. A red error message box is displayed at the bottom right of the page, containing the text: 'Failure: Cannot delete workflow as requests have been submitted of this workflow'.

Figure 34c: Cannot Delete workflows with Submitted Requests

6. If no requests have been submitted for the workflow, then it can be deleted. Workflow deleted successfully message displays.

The screenshot shows the AutomationEdge Workflows interface. At the top, there is a search bar and an 'Import' button. Below the search bar is an 'Advanced Search' section. The main content is a table with the following columns: Name, Category, Metering Units, Created, Last Updated, Active, and Actions. The table contains two rows of workflow data:

Name	Category	Metering Units	Created	Last Updated	Active	Actions
HelloWebGeneric	Default	0	21-Jul-2020 15:43:21	21-Jul-2020 15:50:56	<input checked="" type="checkbox"/>	
HelloWeb	Default	0	21-Jul-2020 09:08:51	21-Jul-2020 09:12:22	<input checked="" type="checkbox"/>	

Below the table, there is a pagination bar showing 'Page 1 of 1 (Total 2 Record(s))' and a 'Page Size' dropdown set to 10. A green success message box is displayed at the bottom right of the page, containing the text: 'Success: Workflow [HelloWorld] deleted successfully'.

Figure 34d: Workflow Delete Message

6.9 Workflows: Features/Permissions for other Users

Table 21: Workflows Features

Feature/Role	Tenant Administrator	Workflow Administrator	User Administrator	Agent Administrator	Tenant User*	Activity Monitor
Add New Workflow	✓	✓	-	-	-	-
Process Studio Workflow	✓	✓	-	-	-	-
Advanced Search	✓	✓	-	-	✓	-
Activate Workflow	✓	✓	-	-	-	-
Edit Workflow	✓	✓	-	-	-	-
Delete Workflow	✓	✓	-	-	-	-
Create/Edit/Delete Category	✓	✓	-	-	-	-
Move workflow to other categories	✓	✓	-	-	✓	-
Assign Permissions to Workflows	✓	-	✓	-	-	-
Scheduler: Add/Activate/Edit/Delete	✓	✓	-	-	✓	-

*Tenant users can use the AutomationEdge features depending on Read, Write or Execute permissions granted to the users or their user group on workflows.

Edit icon is enabled only if tenant user has effective write permissions on the workflow.

6.10 Workflow Categories

The Workflows: Categories submenu has contents as described in the table below and shown in the figure below. These will be discussed in detail in the following sub-sections.

Table 22: Description of sections on Workflow categories sub-menu

No.	Artefact	Description
	“Add New Button”	Displays the category selected in the table in the left columnar section
	Left columnar section displays all Categories	It has Actions to Edit, Assign Permissions and delete Category
	Right columnar section displays all workflows in the Category selected on the left.	It has Actions to Assign Permissions to Workflows. It has a checkbox to be selected if the workflow need to be moved from one category to another
	Move Button	Enable checkbox for workflows to be moved in the right columnar section. Select the Category to which the selected workflows need to be moved from the drop down

		list next to the move button. Then select the move button.
--	--	--

6.10.1 Add New Category

Workflows can be grouped in workflow categories. A workflow can be present in only one category at a time.

A category named 'Default' is always present.

To create a new workflow category:

1. Click Workflows.
2. Click Workflow categories.
3. Click Add New button.

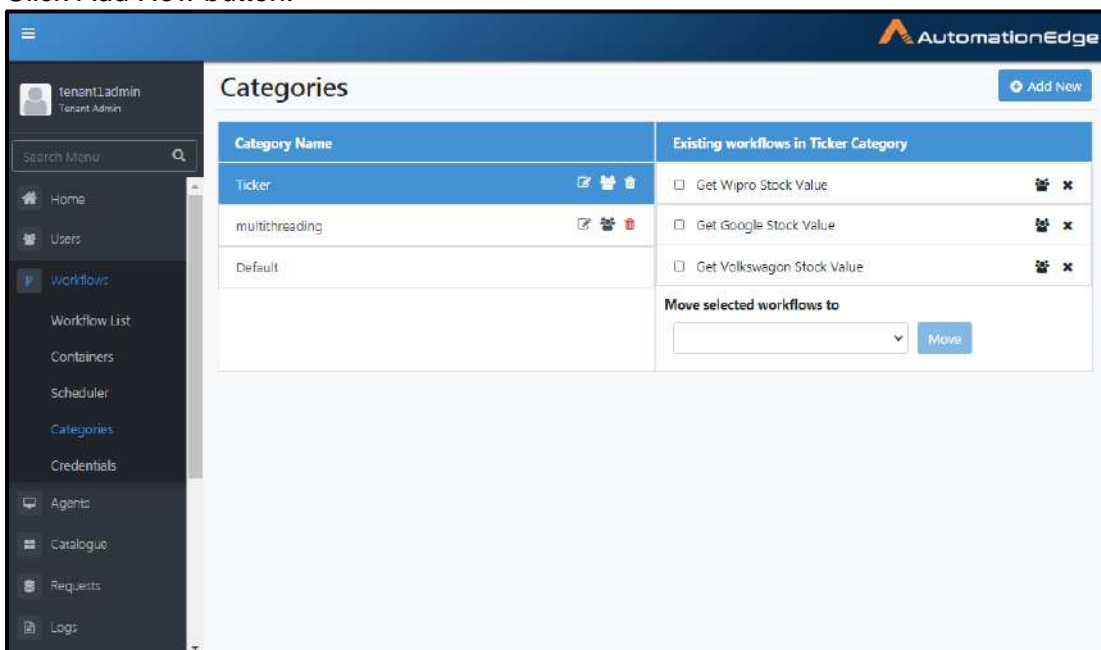


Figure 35a: Workflow Category

- Enter the details of the new workflow (category name and description). Click Create to create new workflow category.

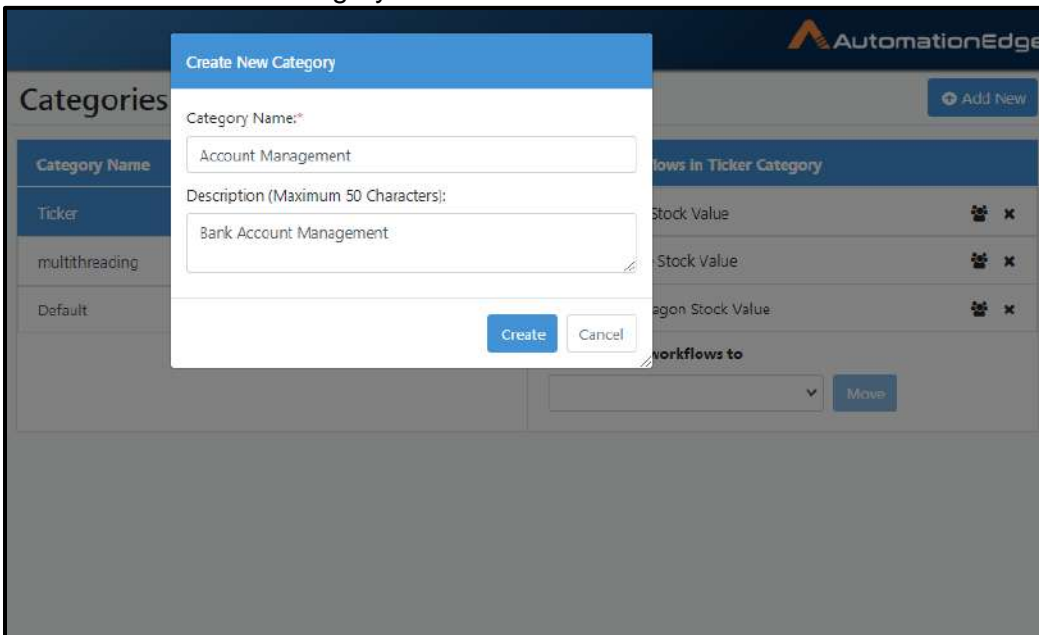


Figure 35b: Entering New Workflow Category Details

- Workflow category created successfully message appears.

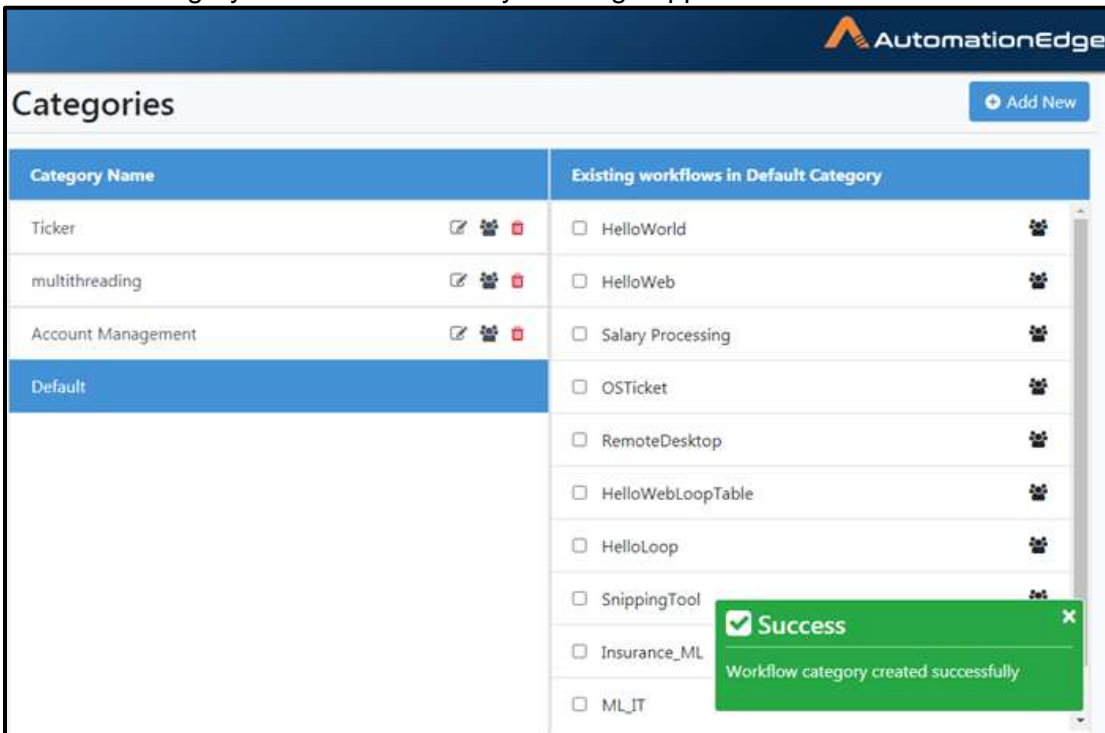


Figure 35c: Workflow category created successfully

Table 23: Add New Category Field Description

Field	Description
Category Name	Specify workflow category name.
Description	Specify workflow category description.
Buttons:	
Create	Click to create new workflow category.
Cancel	Click to cancel creating new workflow category.

6.10.2 Search Workflow Category

A tabular list of all categories appears as seen in left columnar section as shown below.

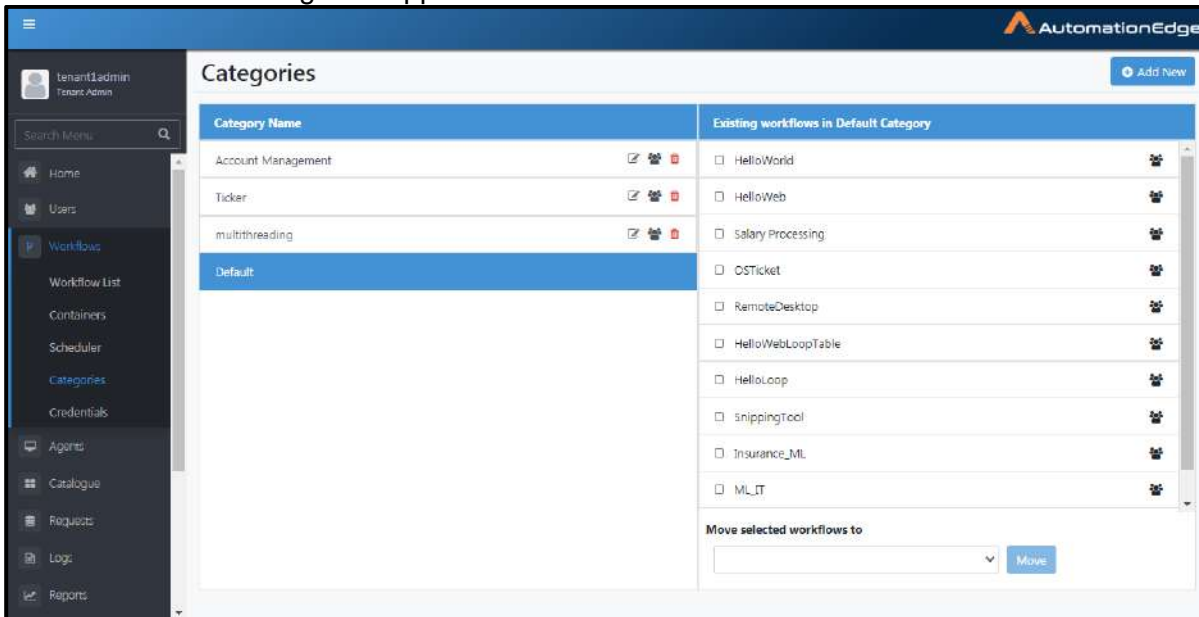


Figure 36a: Workflow Category


Columns descriptions are as shown in the Table below.

Table 24: Workflow Category Tabular List Field Description

Field Name	Description
Create New Category	To create new workflow category.
Category Name	Displays workflow category name
Description	Displays workflow category description.
Actions:	Displays actions that can be performed on workflow category.
Edit (✎)	To edit workflow category.
Assign Permissions (👤)	To assign permission to workflow category.
Delete (🗑)	To delete workflow category.

6.10.3 Editing Workflow Category

To edit workflow category:

1. Click Workflows
2. Click Workflow Categories.
3. Click Settings icon in Actions column.
4. Click Edit ()

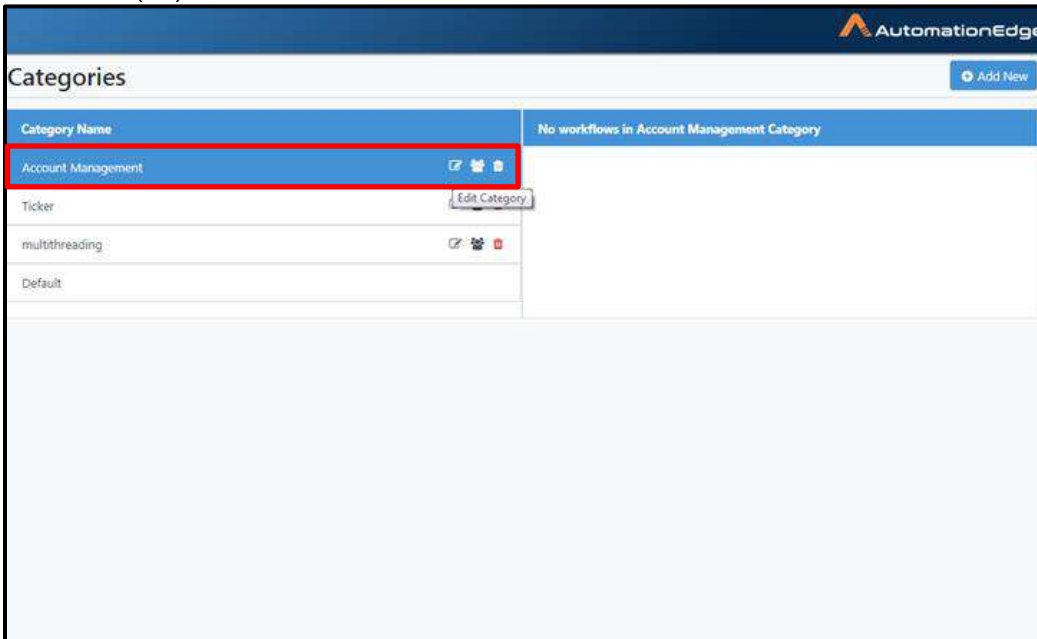


Figure 37a: Selecting Edit Option

5. Click Edit the workflow category (category name and description)
6. Click to save the edited details.

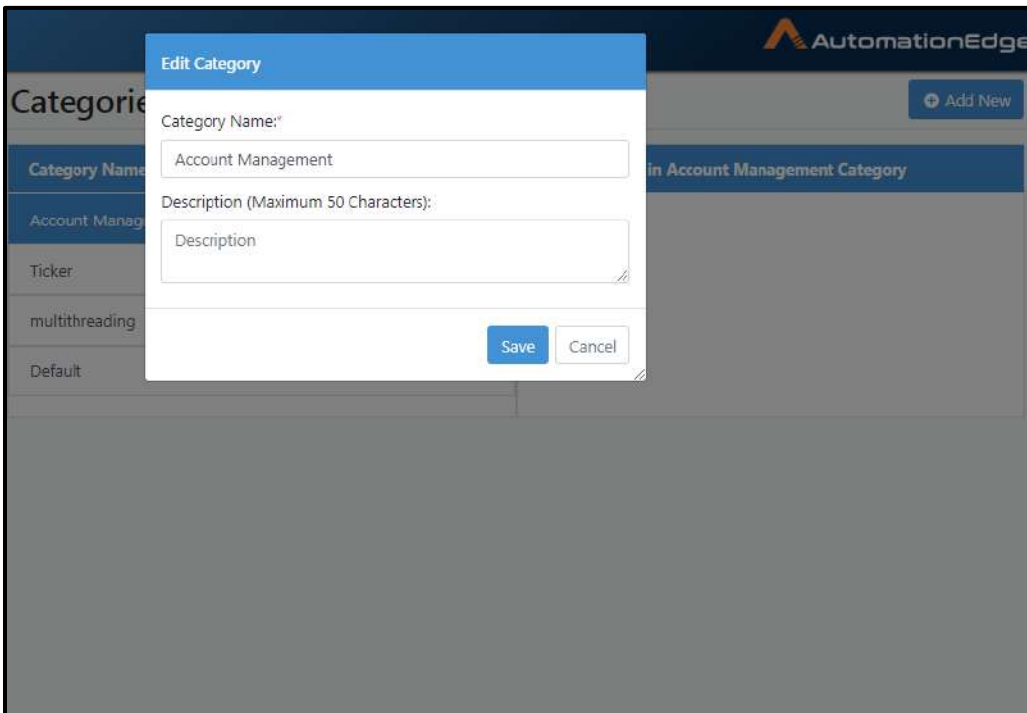


Figure 37b: Editing Workflow Category

7. Workflow category updated successfully message appears.

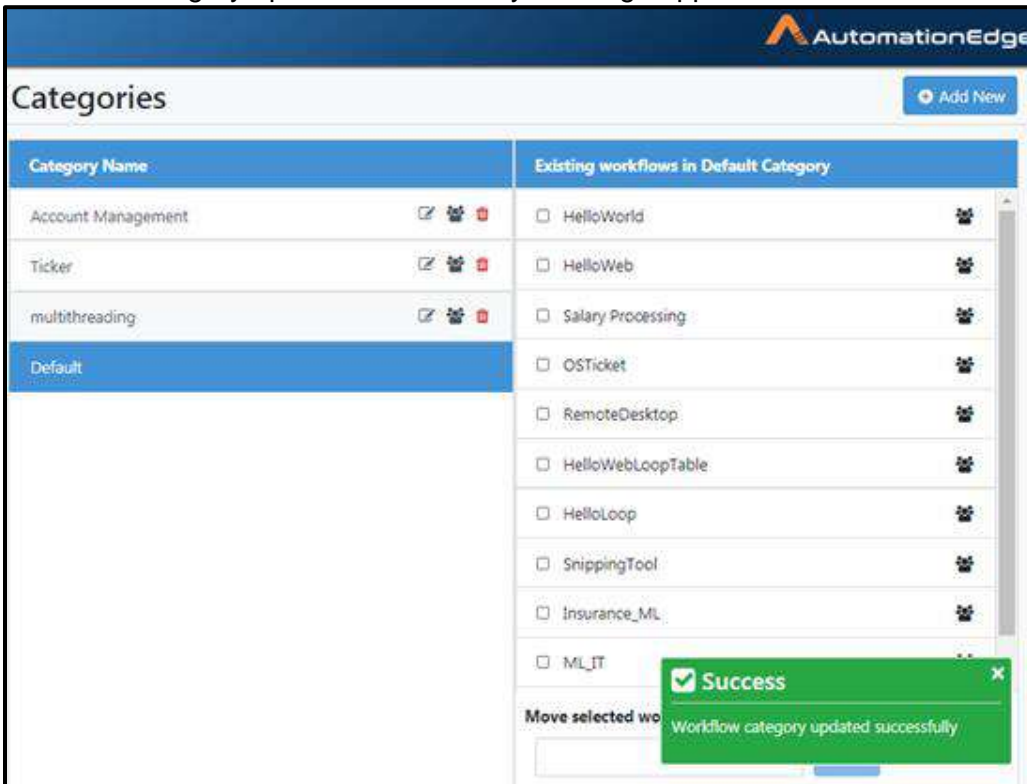


Figure 37c: Edited workflow updated successfully

6.10.4 Assigning Permissions to Workflow Category or Workflow

To assign permissions to category:

1. Navigate to Workflows→Workflows Category.
2. Highlight the Category to assign permissions.
3. Click Assign Permissions icon (👤) corresponding to the category to assign permission.

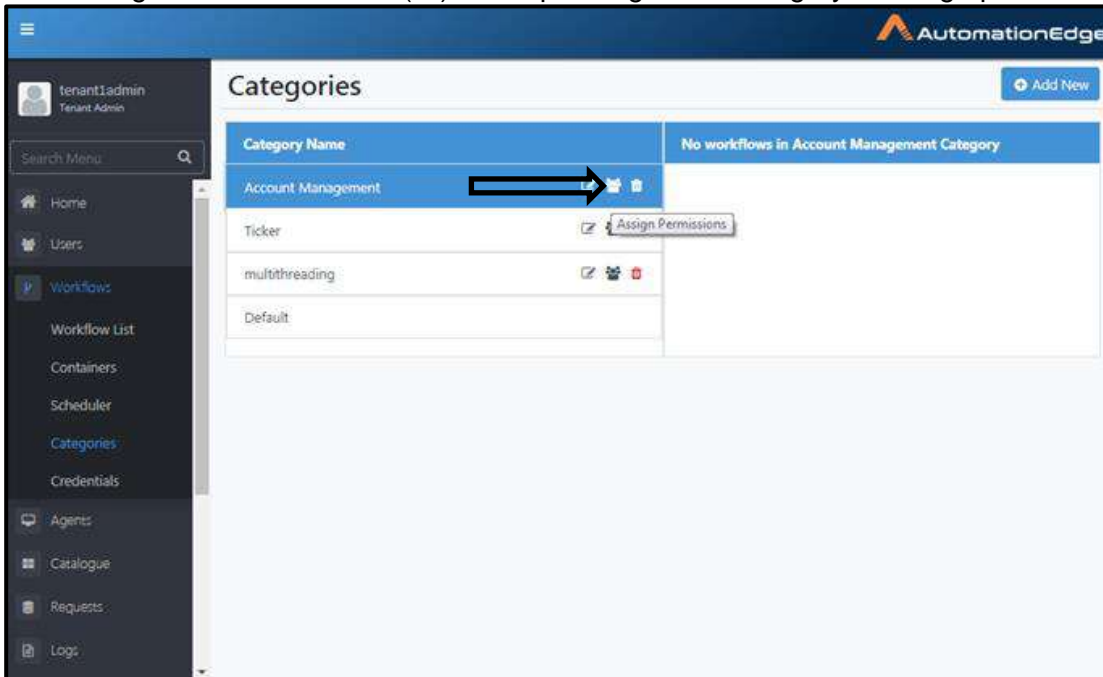


Figure 38a: Selecting Category to Assign Permissions

4. Alternatively, if you wish to assign granular permissions at the Workflow level click Assign Permissions icon (👤) next to the workflow.

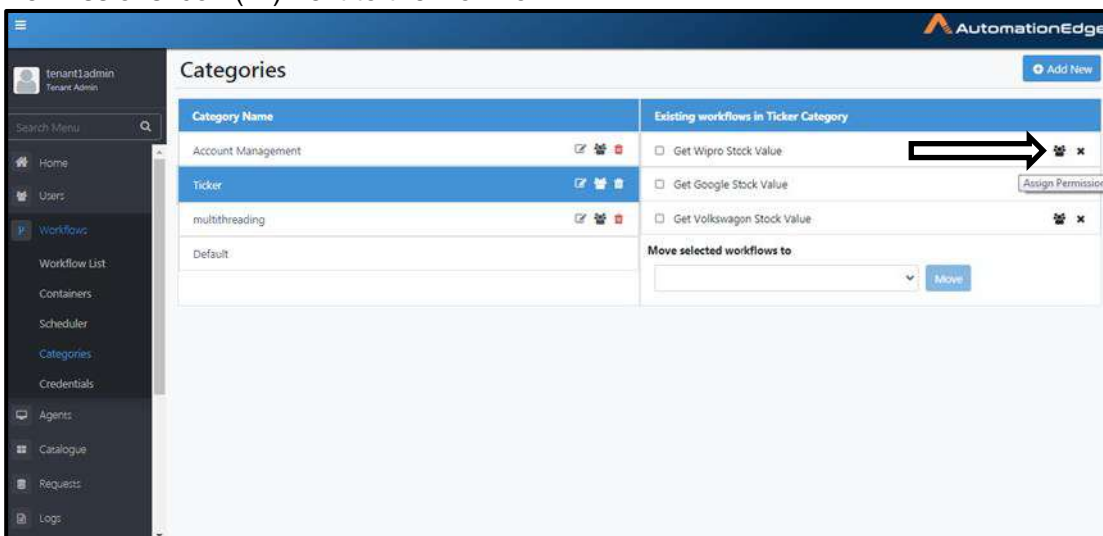


Figure 38b: Select Workflow to assign permissions

5. In the next steps we will assign permissions to a workflow category. The steps to assign permissions to a workflow are the same.

6. Once you click Assign Permissions icon (👤) for the category the following screen appears.

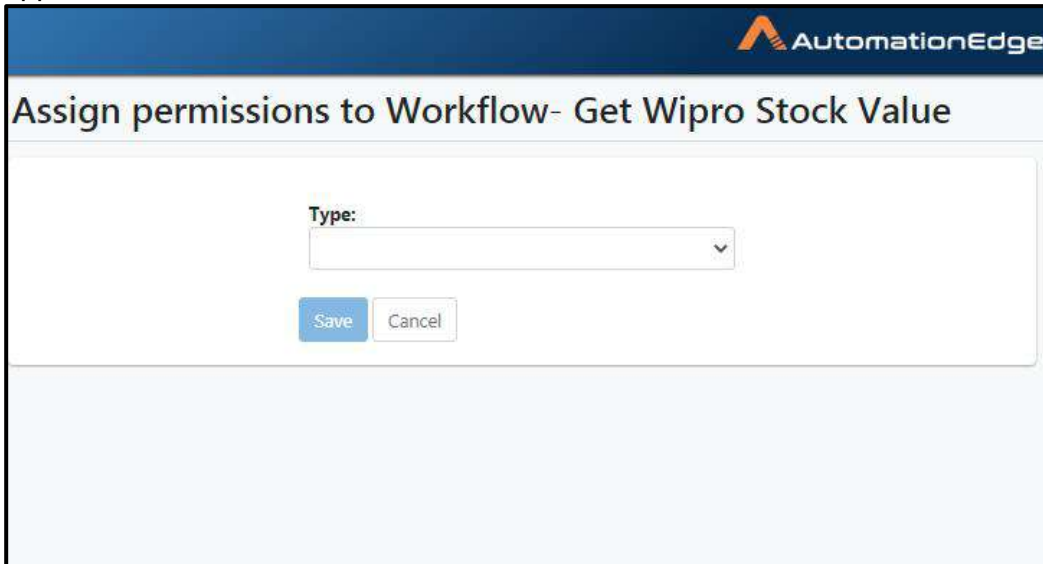


Figure 38c: Select Type

7. Select type i.e. user or group from the drop-down of Select type field.

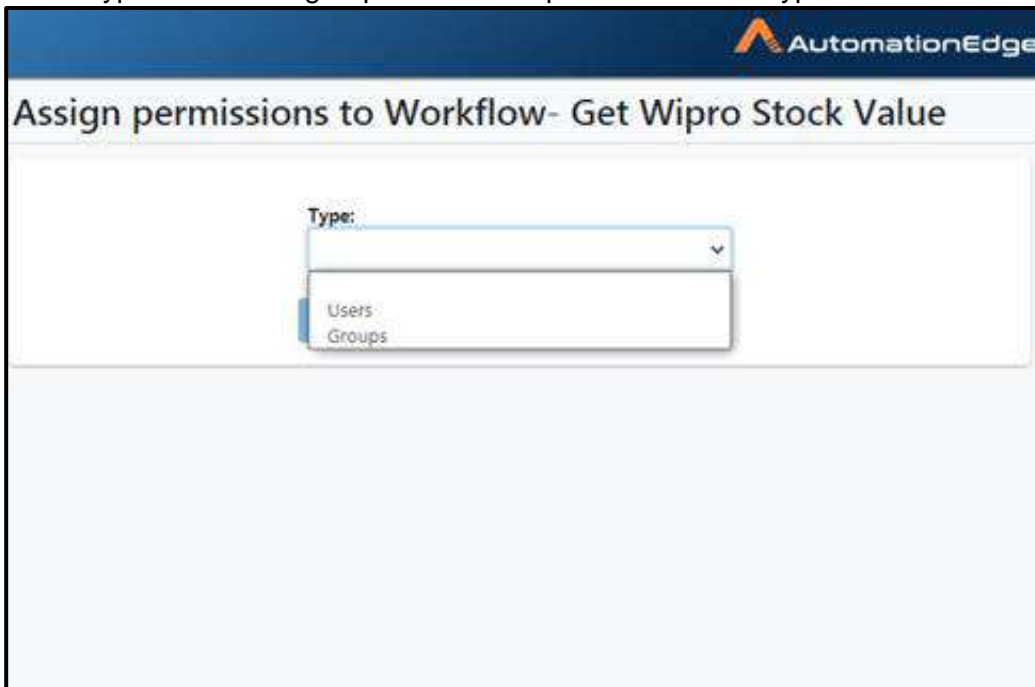


Figure 38d: Assign Permission-Type drop down list

8. Select members from Select Members drop-down.

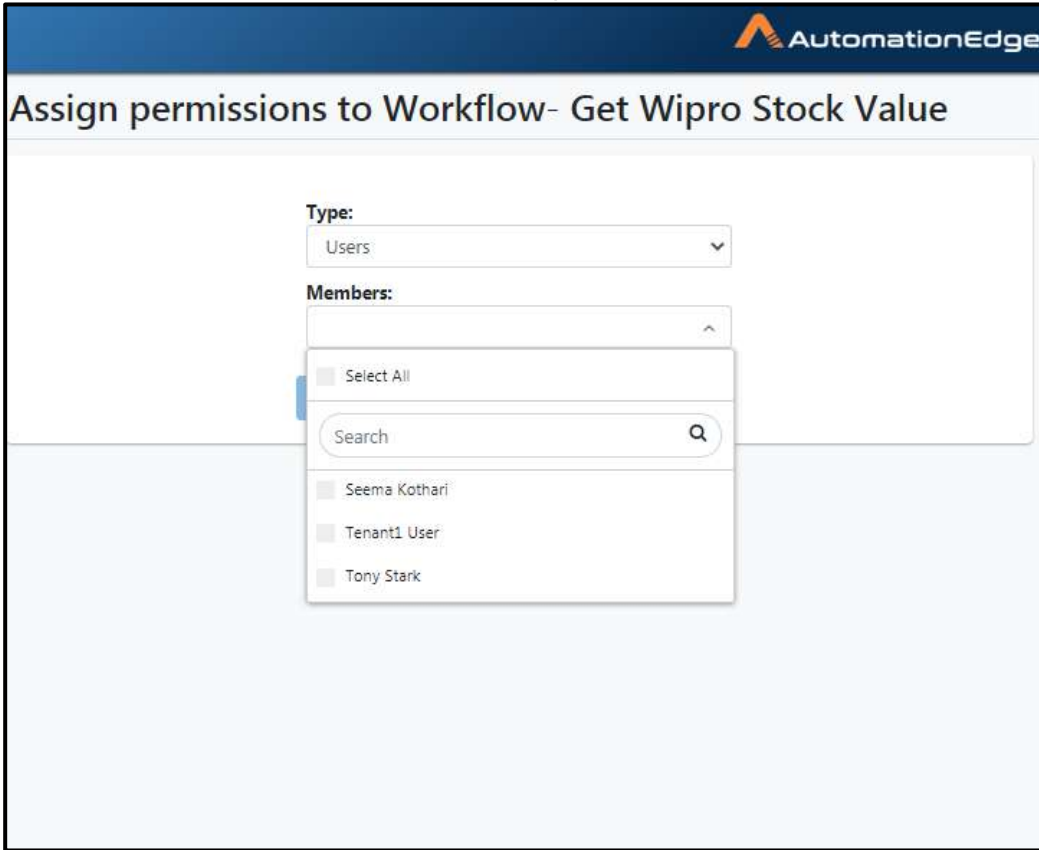
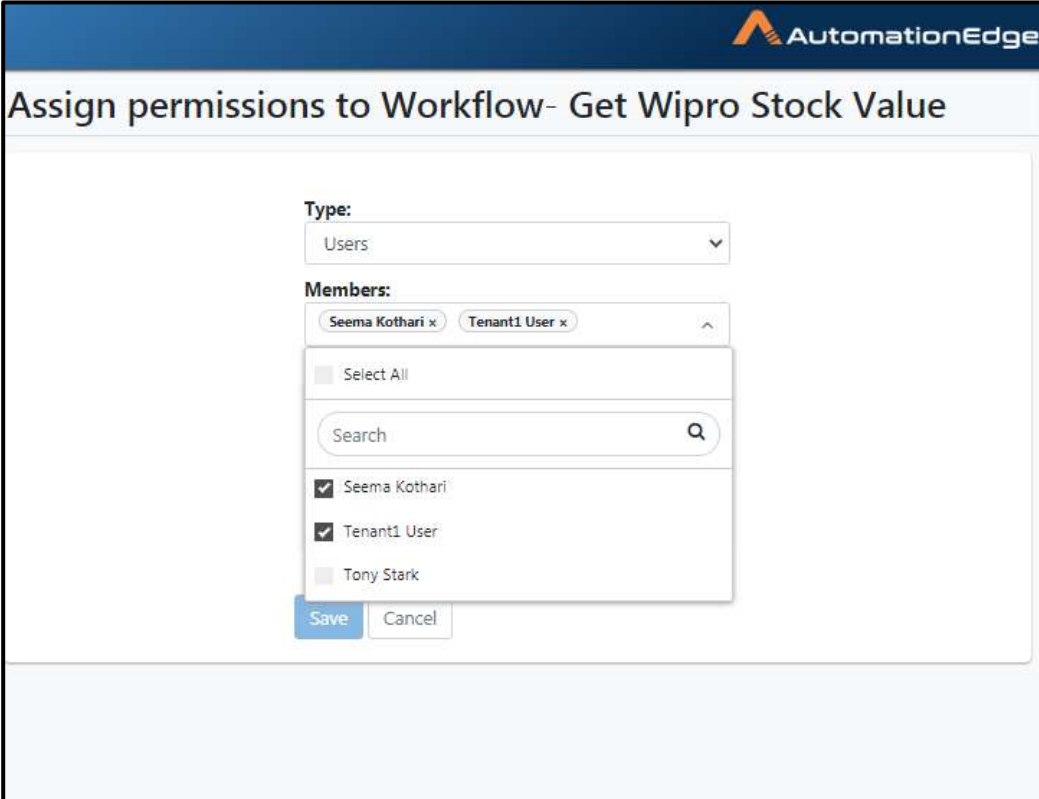


Figure 38e: Select Users

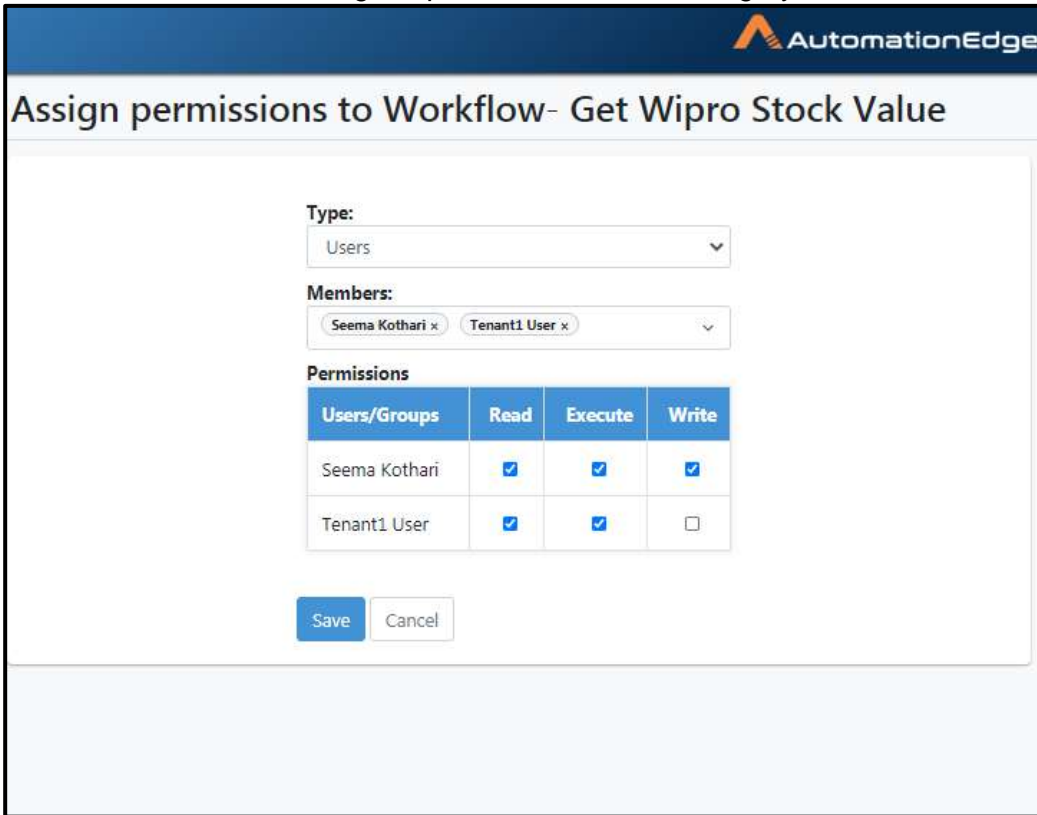
9. Enable checkbox next to the members to assign workflow permissions.



The screenshot displays the AutomationEdge interface for assigning permissions to a workflow. The title is "Assign permissions to Workflow- Get Wipro Stock Value". The "Type" dropdown is set to "Users". The "Members" section shows a list of users: Seema Kothari, Tenant1 User, and Tony Stark. The checkboxes for Seema Kothari and Tenant1 User are checked, while Tony Stark is unchecked. The "Save" button is highlighted in blue.

Figure 38f: Assign Permissions to users

10. Assign Read/Write/Execute permissions to the users for the workflow as shown below.
11. Click Save to save the assigned permissions for the category to the users.



AutomationEdge

Assign permissions to Workflow- Get Wipro Stock Value

Type:
Users

Members:
Seema Kothari x Tenant1 User x

Permissions

Users/Groups	Read	Execute	Write
Seema Kothari	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Tenant1 User	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Save Cancel

Figure 38g: Assigning Permissions to a Category

12. Upon Save you are taken back to Category page.
13. You may optionally select the Category permission for the users.

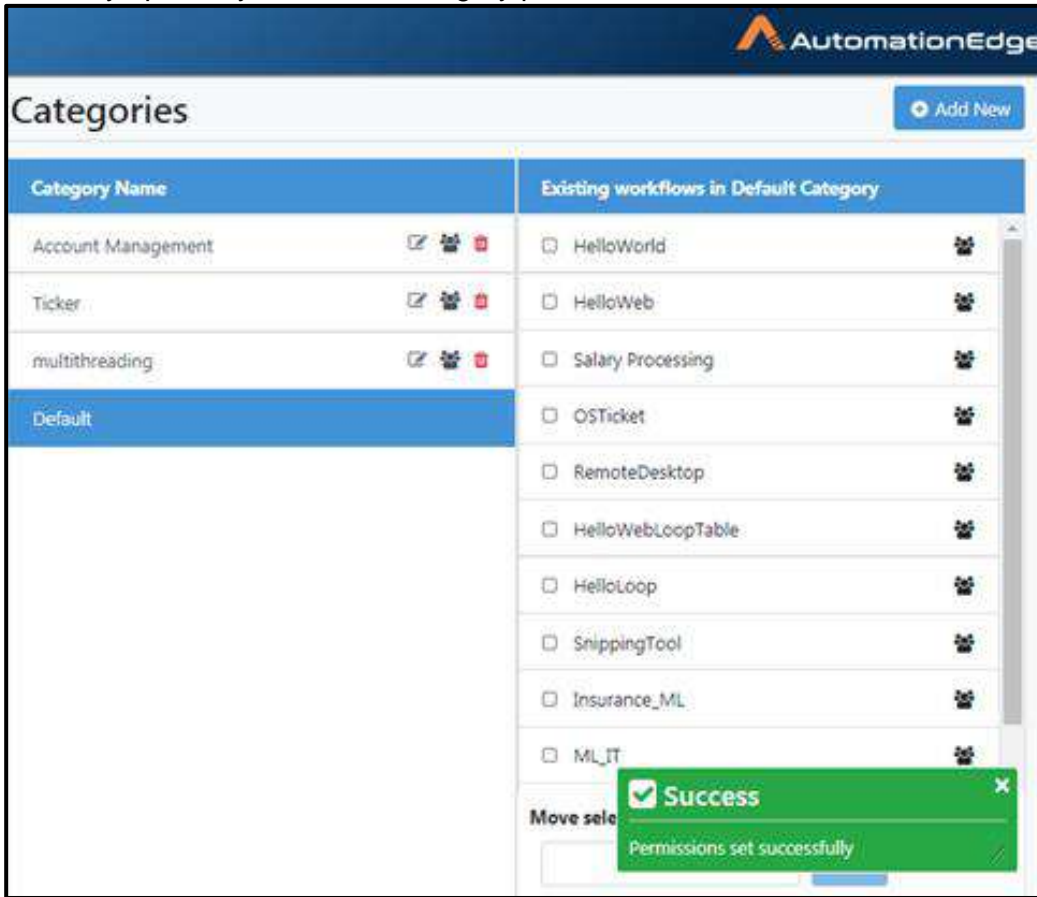


Figure 38h: Permissions set successfully message


Table 25: Assigning Permissions to Workflow Category Field Description

Field	Description
Select Type	Select type: users/groups for assigning permission.
Select Members	To select members for assigning permission.
Permissions	To assign read/write/execute permission to workflow category.
Buttons:	
Save	To save assigned permissions to workflow.
Cancel	To cancel assigning permissions to workflow

6.10.5 Changing Permissions to Workflow Category

Change permissions to category

To change permissions to category:

1. Navigate to Workflows → Workflows Category.
2. Click Assign Permissions icon () corresponding to the category to change assigned permission.

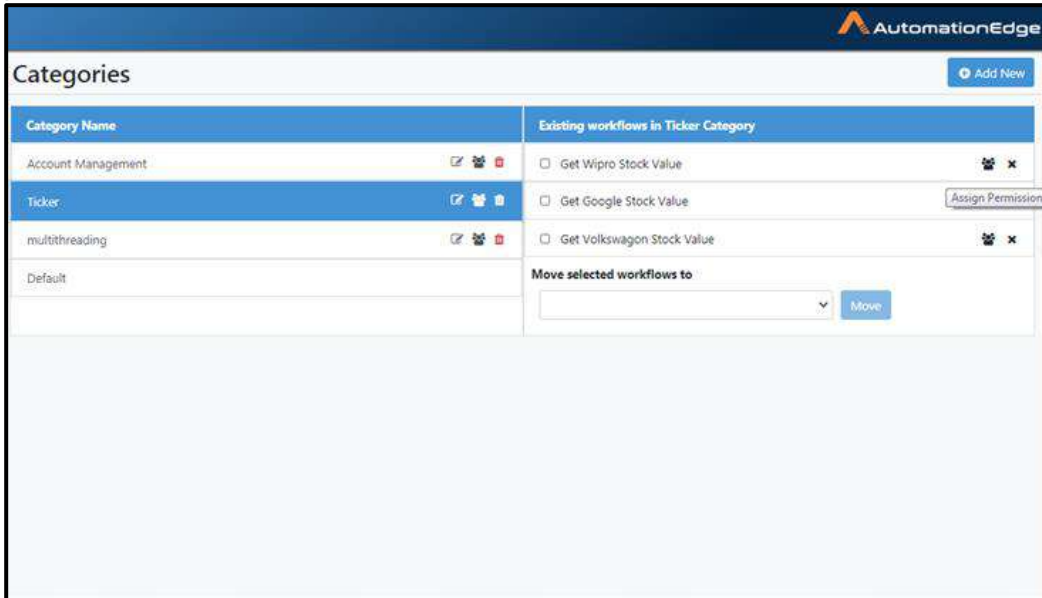


Figure 39a: Selecting Category to Change Assigned Permissions

3. The process to change the assigned permissions is same as that of assigning permissions.
4. Select type of permission from the drop-down of Select type field.
5. Select members and change permissions as desired.
6. Click Save to save the newly assigned permissions to the category.

6.10.6 Deleting Workflow Category

To delete the workflow:

1. Navigate to Workflows→ Workflow Categories.
2. Click and highlight the Category to be deleted.
3. Click delete icon (🗑️) corresponding to the workflow category in the Actions column

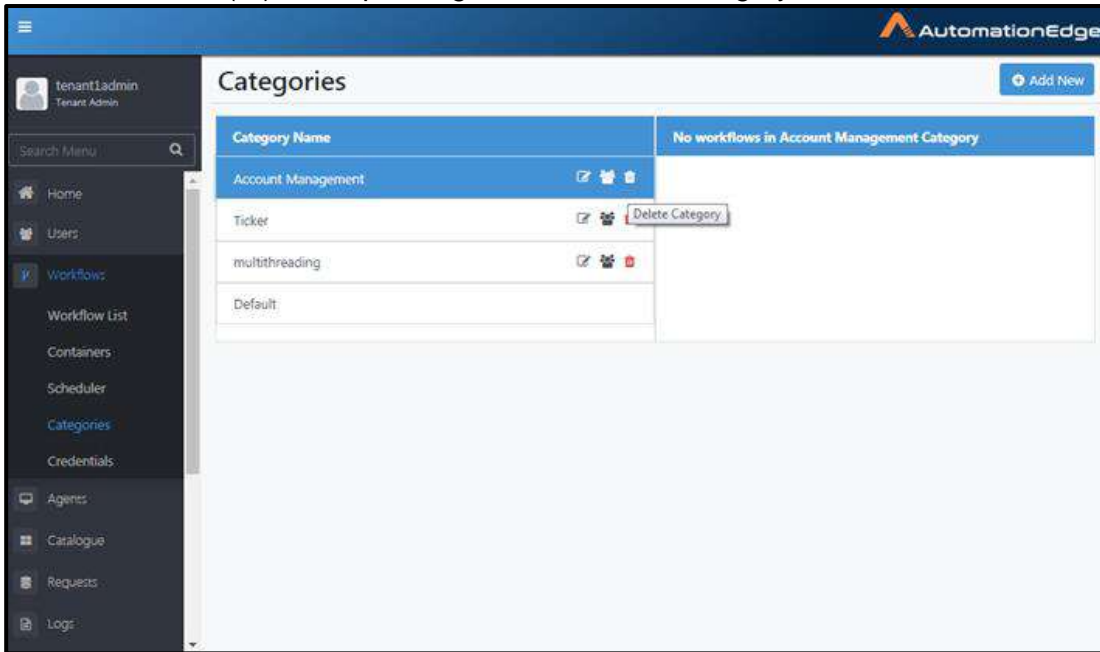


Figure 40a: Deleting Workflow Category

4. Click Delete to confirm deletion of workflow category

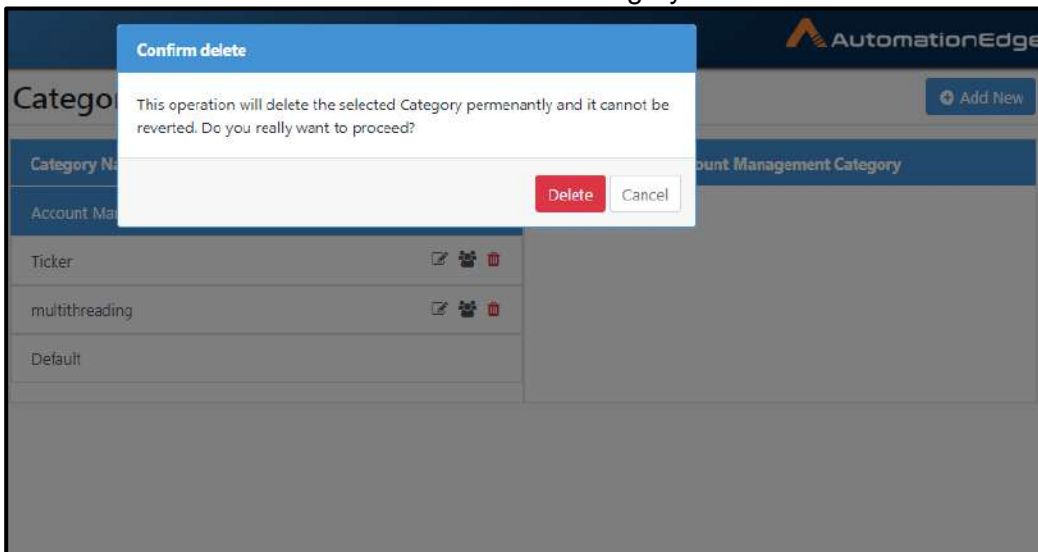


Figure 40b: Confirmation of Deletion of Workflow Category

Note: All the workflows in the deleted category will be moved to the default category.

- Workflow category deleted successfully message appears.

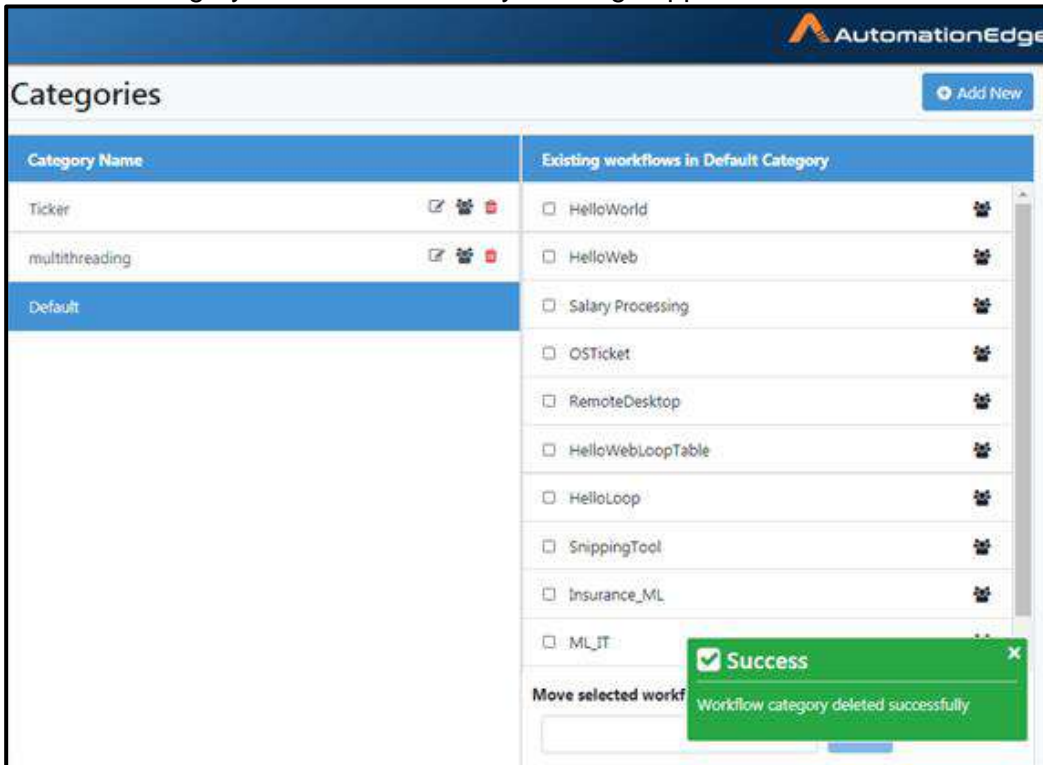


Figure 40c: Workflow Category Deleted successfully message

6.10.7 Existing Workflows in Category

Following are the steps to view workflows in an existing category.

- Navigate to Workflows→Categories menu.
- Categories are visible on the left hand pane and the corresponding workflows are on the right hand pane.
- An explanation of the fields is in the table that follows
- Select a category on the left pane.
- A list of Workflows under the selected category is visible in the right hand pane.

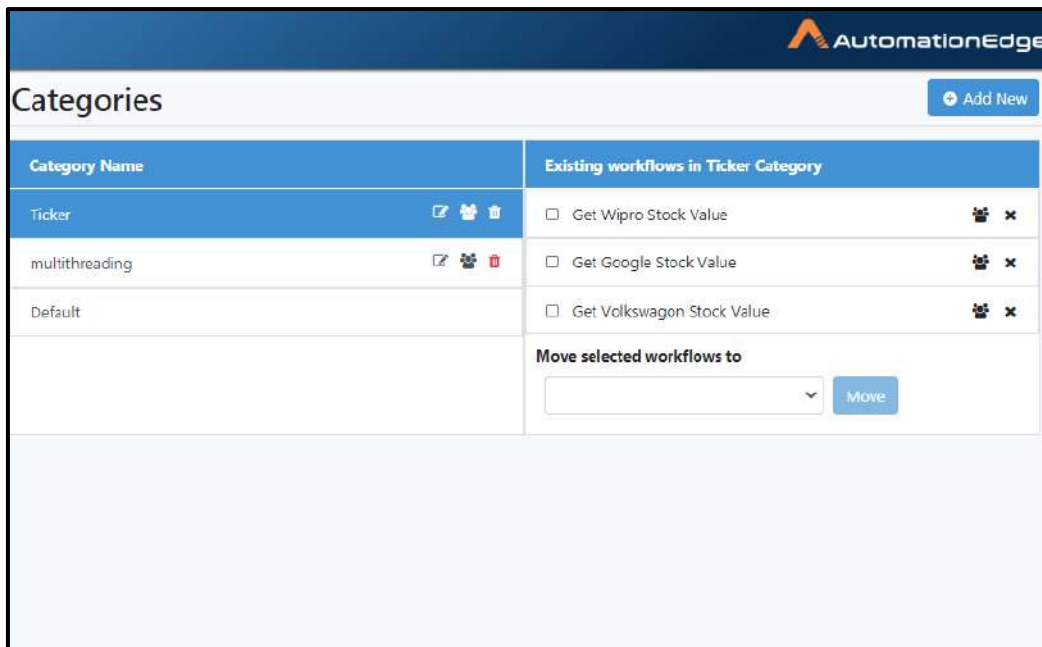




Figure 41a: Workflow Categories

- You may click and highlight any other category to expand the category and see the workflows in the category.

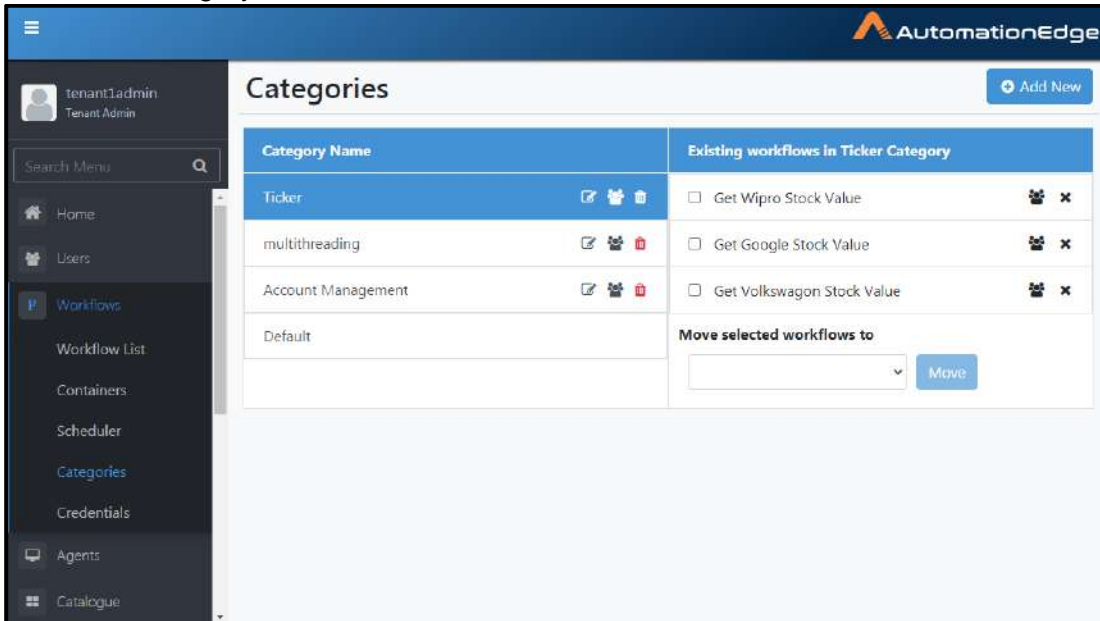
Table 26: Existing Workflows in a Category chosen on the left hand section.

Field	Description
Category	Displays the Category Name
Tabular List:	
	Use this icon to drag and drop workflows to any category on the left hand side.
Check Box	Enable check box for all workflows to be moved.
Assign Permissions ()	To assign permission to the workflow of a category. It can be used for assigning permissions for tenant users and user groups.
Move selected workflows to	Choose a workflow category from the drop down list. It is the category where you want to move the selected workflows.
Move Button	Click Move button to move selected workflows to the category chosen above.




6.10.8 Moving Workflows

To move workflows to another category:

1. Navigate to Workflows → Workflow Categories.
2. Select the category that has workflows to be moved.



The screenshot shows the 'Categories' page in the AutomationEdge interface. The page has a dark blue header with the AutomationEdge logo and a user profile for 'tenant1admin'. A sidebar on the left contains a search menu and navigation links for Home, Users, Workflows, Workflow List, Containers, Scheduler, Categories, Credentials, Agents, and Catalogue. The main content area is titled 'Categories' and features an 'Add New' button. It contains a table with two columns: 'Category Name' and 'Existing workflows in Ticker Category'. The 'Ticker' category is selected and highlighted in blue. The table lists three categories: 'Ticker', 'multithreading', and 'Account Management'. The 'Default' category is also listed. The 'Existing workflows in Ticker Category' column shows three workflows: 'Get Wipro Stock Value', 'Get Google Stock Value', and 'Get Volkswagon Stock Value'. Each workflow has a checkbox and a delete icon. Below the table, there is a section titled 'Move selected workflows to' with a dropdown menu and a 'Move' button.

Category Name	Existing workflows in Ticker Category
Ticker	<input type="checkbox"/> Get Wipro Stock Value 
multithreading	<input type="checkbox"/> Get Google Stock Value 
Account Management	<input type="checkbox"/> Get Volkswagon Stock Value 
Default	

Move selected workflows to:

Figure 42a: Workflow Categories with workflows

3. Select the category whose workflows you wish to move to another category. In this case the selected category is Ticker.
4. Existing workflows in the selected category will display in the right side.
4. Enable the checkbox next to the workflows to be moved, in this case enable the checkbox for Get Wipro Stock Value
5. Move selected workflows to field with a drop down, is now visible as seen below.

The screenshot shows the 'Categories' page in AutomationEdge. The page has a header with the AutomationEdge logo and an 'Add New' button. Below the header is a table with two columns: 'Category Name' and 'Existing workflows in Ticker Category'. The 'Category Name' column lists 'Ticker', 'multithreading', 'Account Management', and 'Default'. The 'Existing workflows in Ticker Category' column lists three workflows: 'Get Wipro Stock Value' (checked), 'Get Google Stock Value', and 'Get Volkswagon Stock Value'. Below the table, there is a 'Move selected workflows to' section with a dropdown menu and a 'Move' button. The dropdown menu is open, showing the following options: 'Ticker', 'multithreading', 'Account Management', and 'Default'.

Figure 42b: Check Workflow to be moved

6. Select the category to move to from the drop-down list next to the Move button. Click Move. Workflows will move to the selected category.

The screenshot shows the 'Categories' page in AutomationEdge. The page has a header with the AutomationEdge logo and an 'Add New' button. Below the header is a table with two columns: 'Category Name' and 'Existing workflows in Ticker Category'. The 'Category Name' column lists 'Ticker', 'multithreading', 'Account Management', and 'Default'. The 'Existing workflows in Ticker Category' column lists three workflows: 'Get Wipro Stock Value' (checked), 'Get Google Stock Value', and 'Get Volkswagon Stock Value'. Below the table, there is a 'Move selected workflows to' section with a dropdown menu and a 'Move' button. The dropdown menu is open, and 'multithreading' is selected.

Figure 42c: Select Target category

7. Workflows category changed successfully message appears. Get Wipro Stock Value is removed from the Ticker Category.

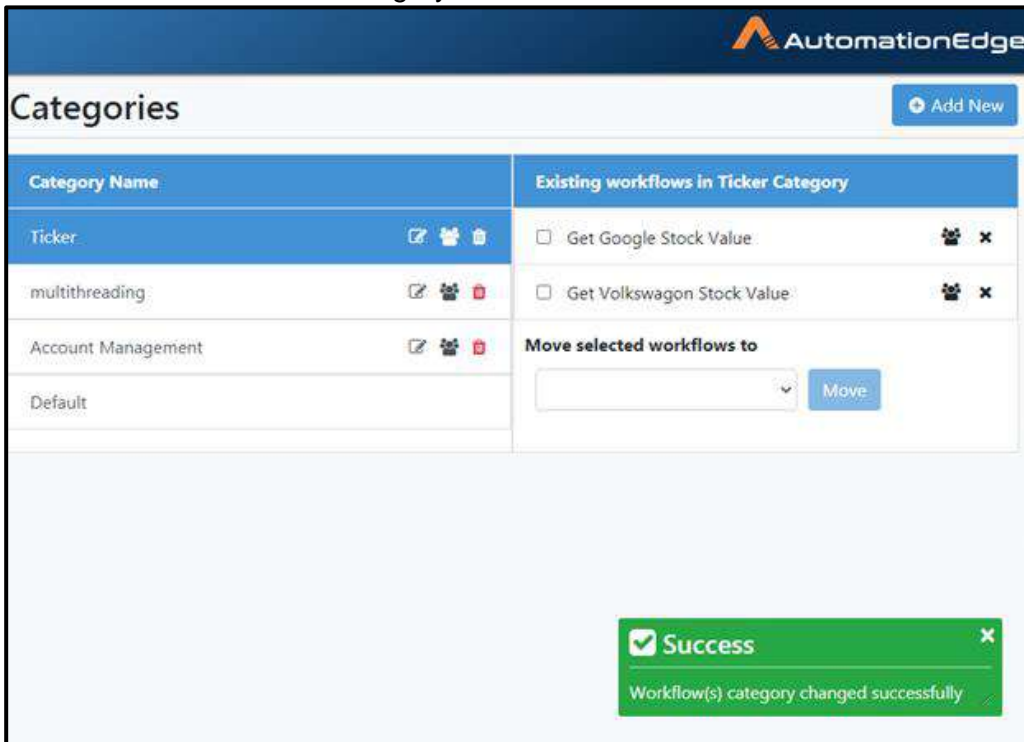


Figure 42d: Workflow Category changed successfully message

8. You can now see Get Wipro Stock Value in the new category.

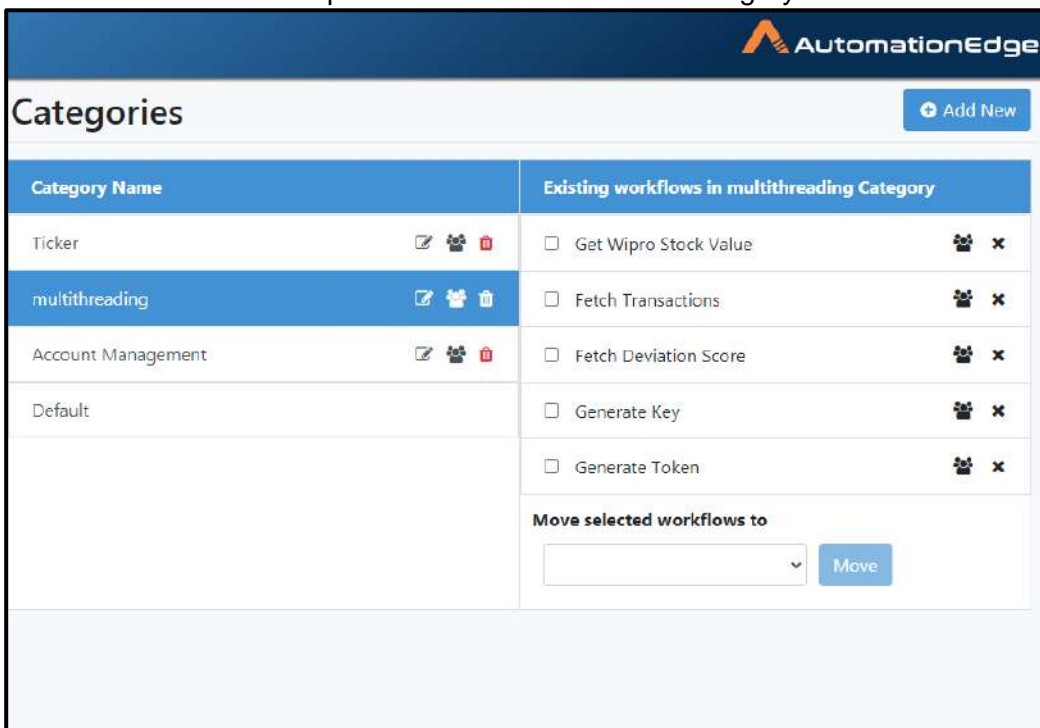


Figure 42e: See the Workflow in the new Category

6.10.9 Workflow Categories: Features/Permissions for other users

Table 27: Add New User for other Tenant Users

Feature/Role	Tenant Administrator	Workflow Administrator	User Administrator	Agent Administrator	Tenant User*	Activity Monitor
Create/Edit/Delete Category	✓	✓	-		-	-
Move workflow to other categories	✓	✓	-		-	-
Assign Permissions to Workflows	✓	-	✓		-	-

*Tenant users can use the AutomationEdge features depending on Read, Write or Execute permissions granted to them on workflows.

6.11 Credentials

Credential provides two features: Credentials and Credential Pools.

Credential: AutomationEdge may connect to external systems for getting automation work done. Credentials of the external systems can be stored in the workflow definitions. However, many organizations want separation of responsibilities between the process owners and credential managers. Credentials can change over time (e.g. password expiry) in such cases the workflow configuration parameters need to be altered.

This feature makes it easy to manage the credentials of external systems. The credentials are created and managed separately. Credential Management is done by a relevant authority. Workflow owners cannot see or alter user credentials. Workflow owners can use credentials in workflow or process parameters.

Process Studio process parameters or workflow parameters offer credential as a data type. The parameters are then available as AutomationEdge workflow configuration or runtime parameters.

Credential Pool: A Credential Pool is a collection of credentials. Some external systems (target) allow only one active session per user at a time. For such external systems, a Credential Pool can be created, that would hold all the available credentials for that external system. Each workflow instance acquires a single credential from a pool at any given time. Hence, if a user wants to run multiple Workflow instances the user can acquire multiple credentials from a credential pool.

Note: If a credential belongs to a Credential Pool it cannot be used in a workflow directly, it can be used via pool only.

The Workflow Credentials menu has two columnar sections as shown in the figure and described in the table below.

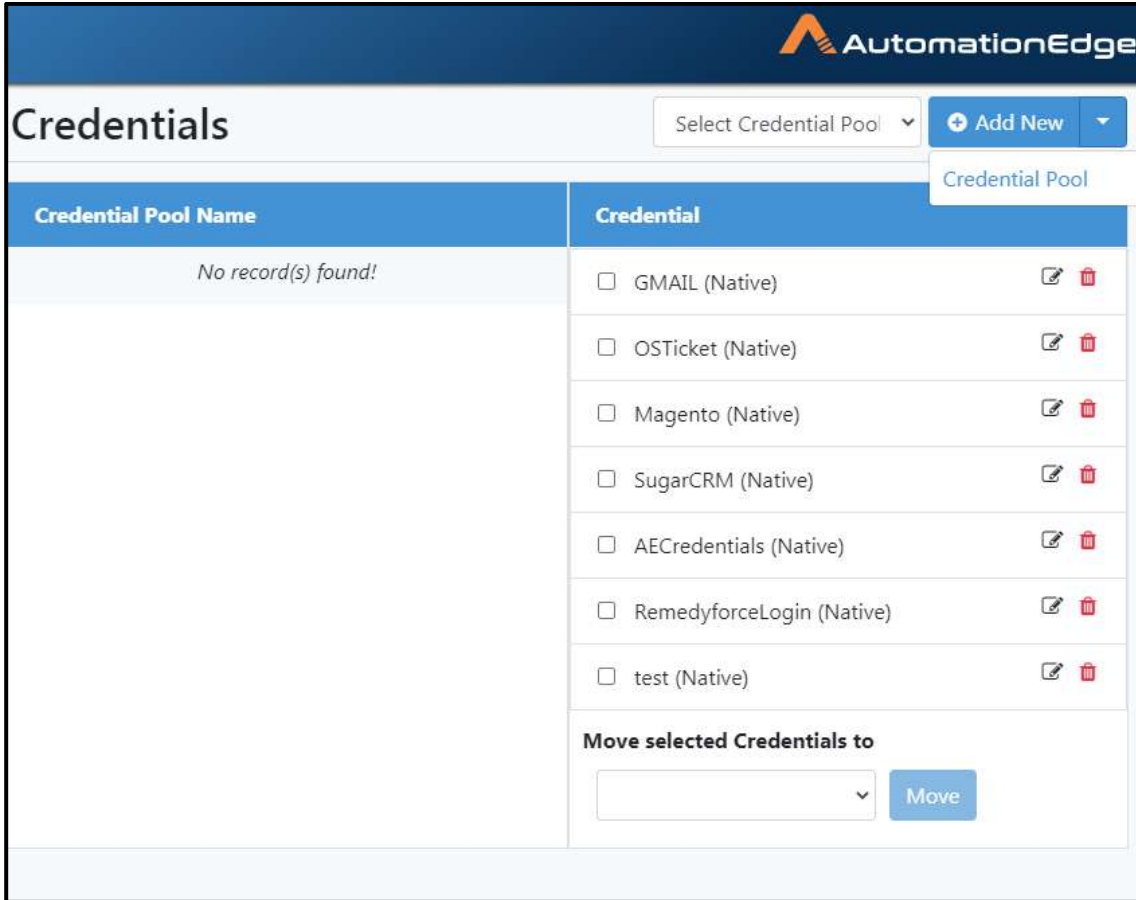


Figure 49a: Credentials

Table 31: Description of sections on Credentials menu

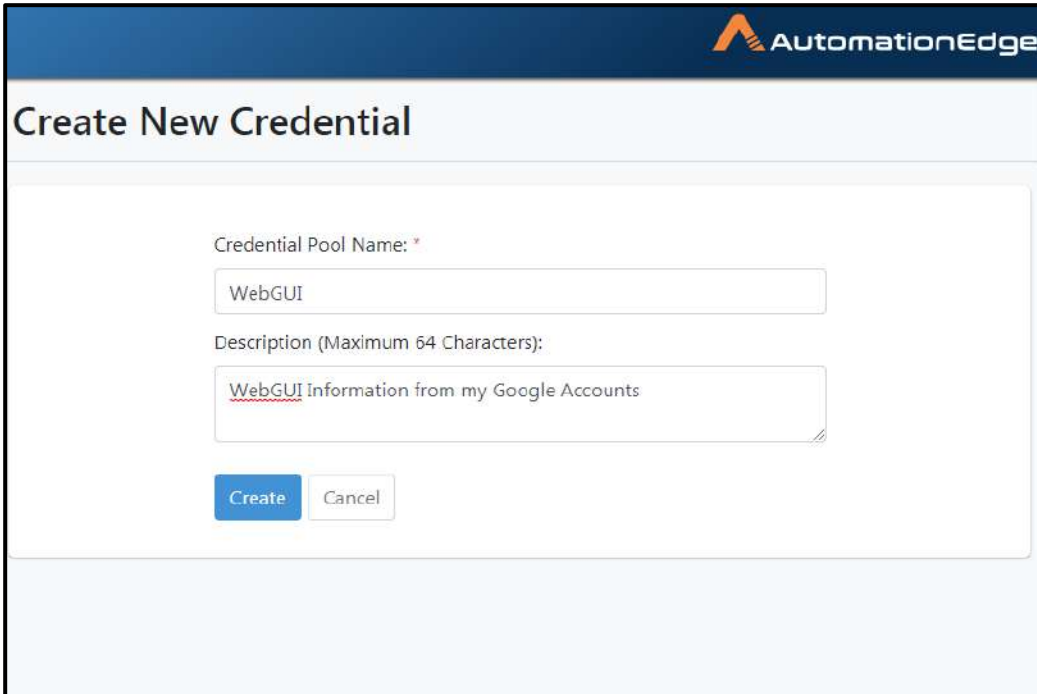
Left Columnar Section	Right Columnar Section
1. New Credential Pool	1. New Credential
2. A table listing all Credential Pools	2. A drop down list to choose a Credential Pool. It acts a filter for the list of Credential Pools below.
	3. A table listing all Credentials if no particular Credential Pool is selected above.
	4. 'Move selected Credential to' is used to move Credentials to a Credential Pool.

6.11.1 Credential Pool

6.11.1.1 New Credential Pool

To create a Credential Pool,

1. Click Credentials sub-menu
2. Click 'New Credential Pool'
3. Provide details as shown below. Click Create.



The screenshot shows a web interface for creating a new credential pool. The header is dark blue with the AutomationEdge logo. The main content area is white with a light blue border. The title 'Create New Credential' is in bold. Below the title is a form with two input fields. The first field is labeled 'Credential Pool Name: *' and contains the text 'WebGUI'. The second field is labeled 'Description (Maximum 64 Characters):' and contains the text 'WebGUI Information from my Google Accounts'. At the bottom of the form are two buttons: 'Create' (blue) and 'Cancel' (white).

Figure 50a: Create Credential Pool

- You are taken to the Credentials page. You can now see the newly created Credential Pool WebGUI.

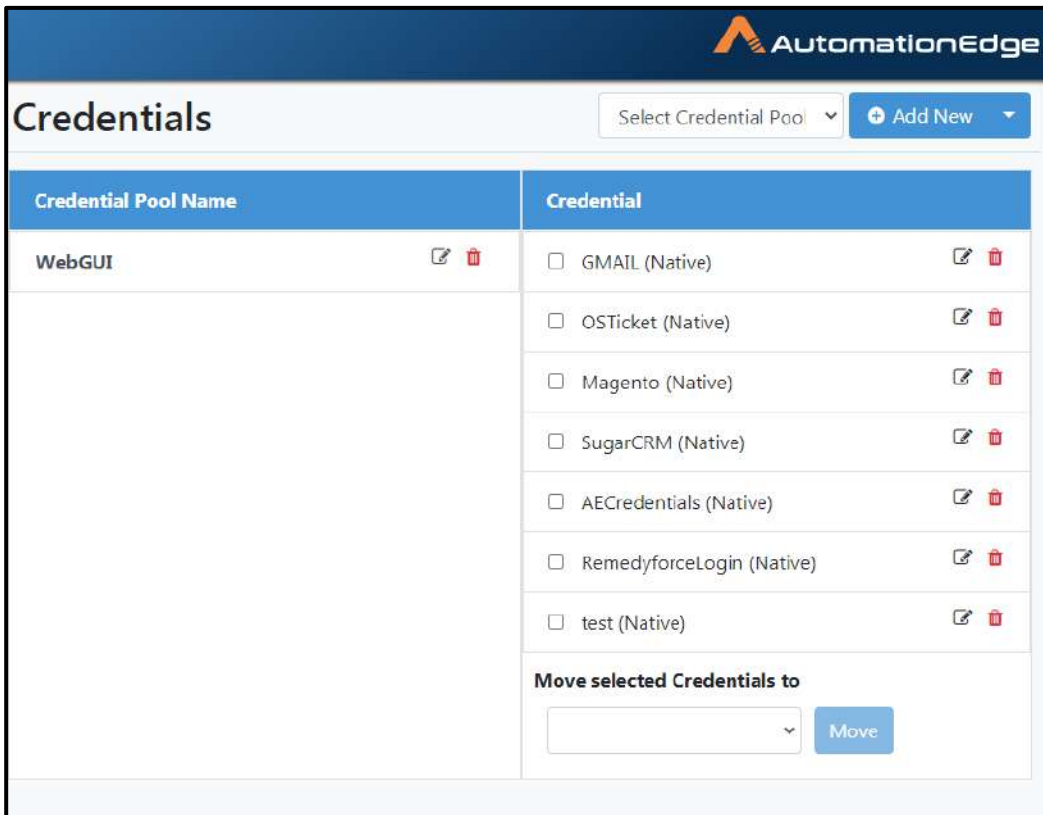


Figure 50b: WebGUI Credential Pool is created

- A description of the fields is shown in the table below.

Table 32: Create Credential Pool

Field Name	Description
Credential Pool Name	Specify a name for the Credential Pool.
Description	Provide a description for the Credential Pool.
Buttons:	
Create	Click Create to create the credential pool
Cancel	Click Cancel to cancel Creation.

6.11.1.2 Edit Credential Pool

To edit Credential Pool:

- Click Credential sub-menu.

2. Click the Edit icon (✎) corresponding to the Credential Pool you wish to edit.

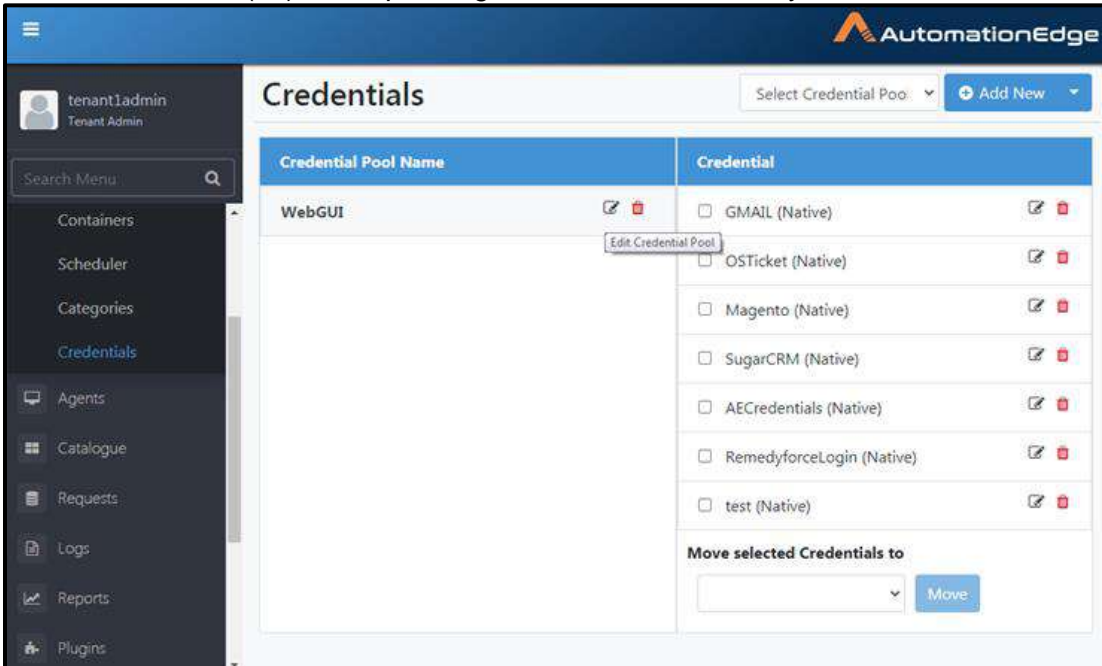


Figure 51a: Edit Credential Pool

3. Click Save to update the Credential Pool.

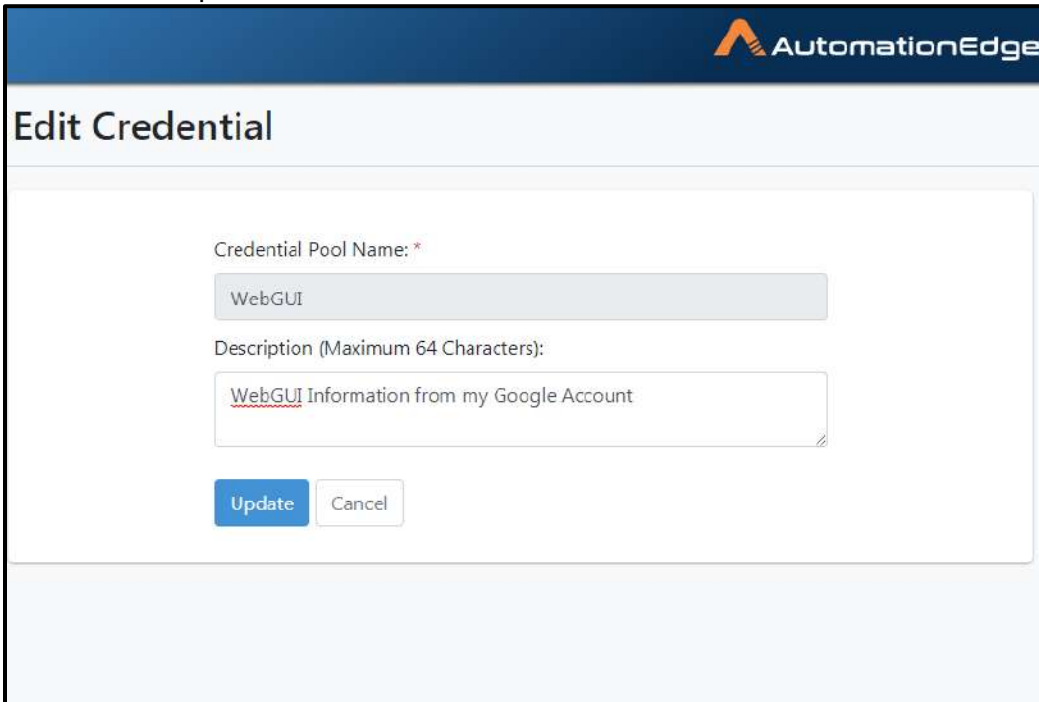
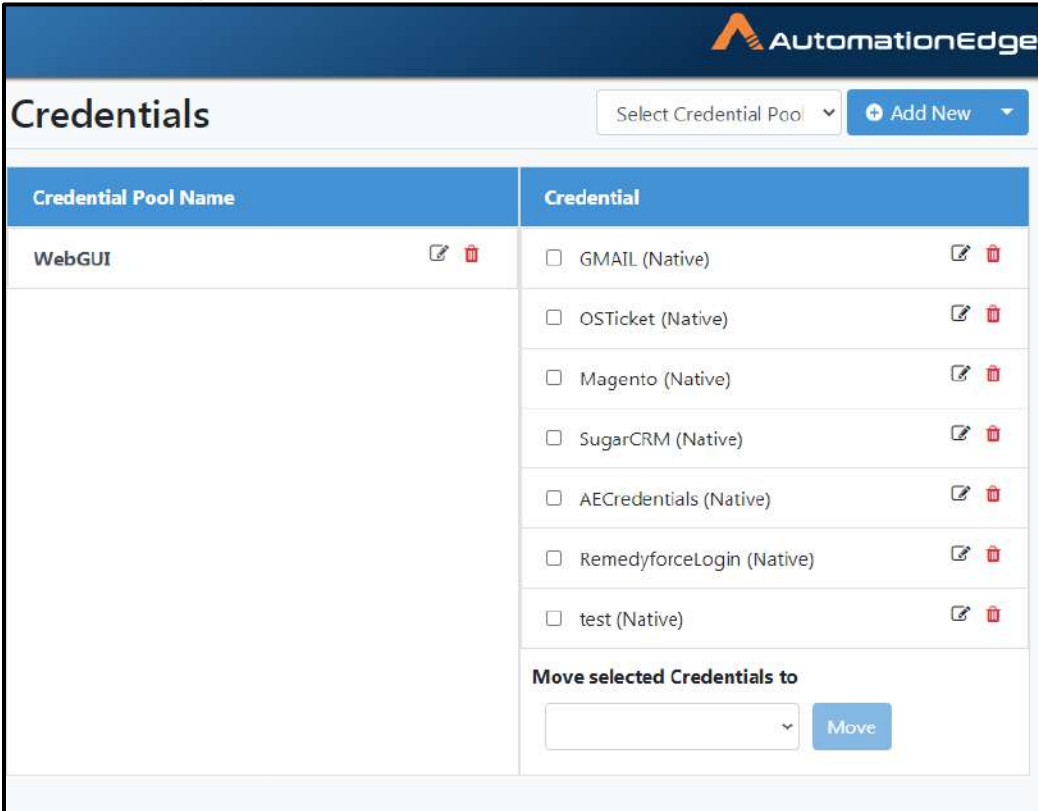


Figure 51b: Edit Credential Pool

4. Click Save to update the Credential Pool.



Credential Pool Name	Credential
WebGUI	<input type="checkbox"/> GMAIL (Native)
	<input type="checkbox"/> OSTicket (Native)
	<input type="checkbox"/> Magento (Native)
	<input type="checkbox"/> SugarCRM (Native)
	<input type="checkbox"/> AECredentials (Native)
	<input type="checkbox"/> RemedyforceLogin (Native)
	<input type="checkbox"/> test (Native)

Move selected Credentials to

Move

Figure 51c: Credential pool saved successfully

6.11.1.3 Delete Credential Pool

To delete Credential Pool:

1. Click Credential sub-menu.
2. Click the Delete icon (🗑️) corresponding to the Credential Pool you wish to delete.

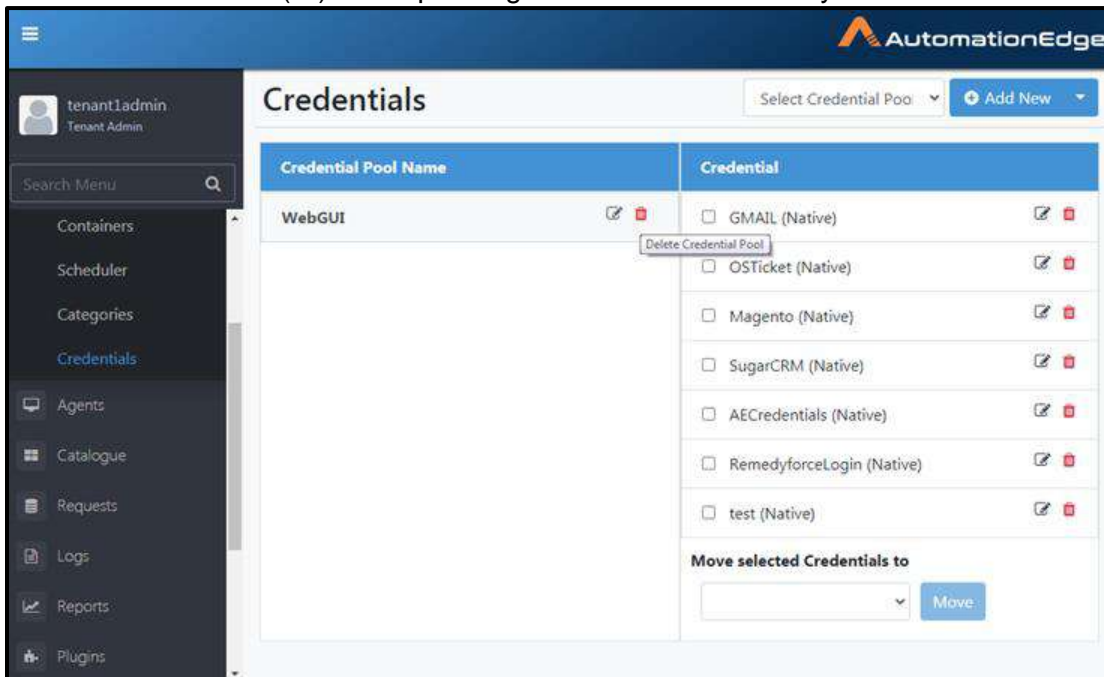


Figure 52a: Deleting Credential Pool

3. A Confirm delete popup appears. Click Delete to confirm user deletion. Note that in the background the Credential pool is expanded and you can see the included workflows.

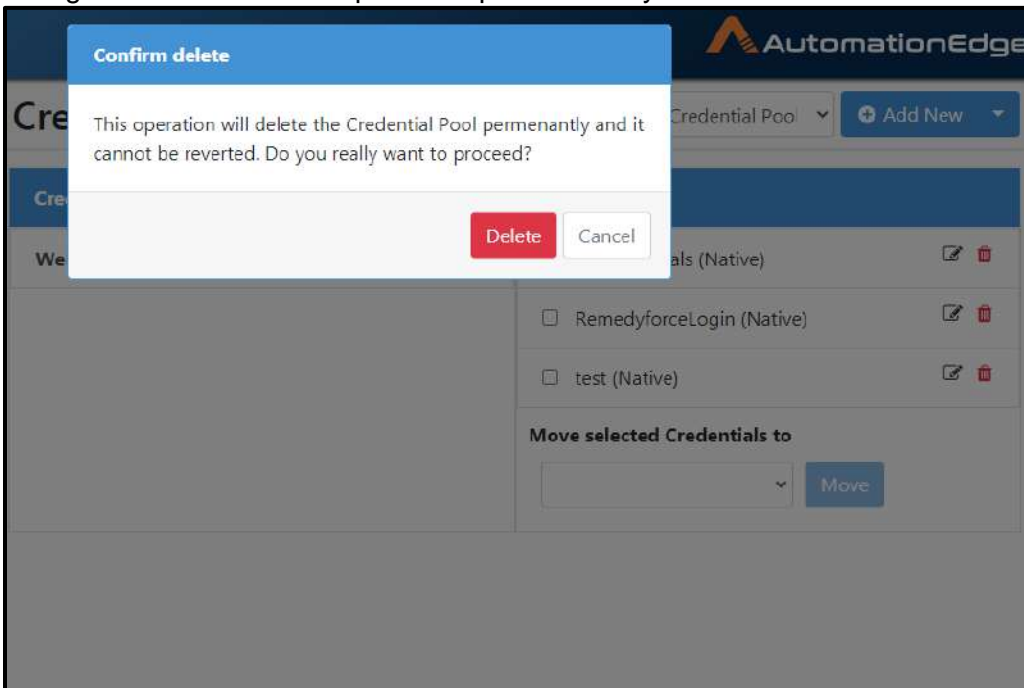


Figure 52b: Confirming User Deletion

4. Credential pool [WebGUI] deleted successfully message appears.

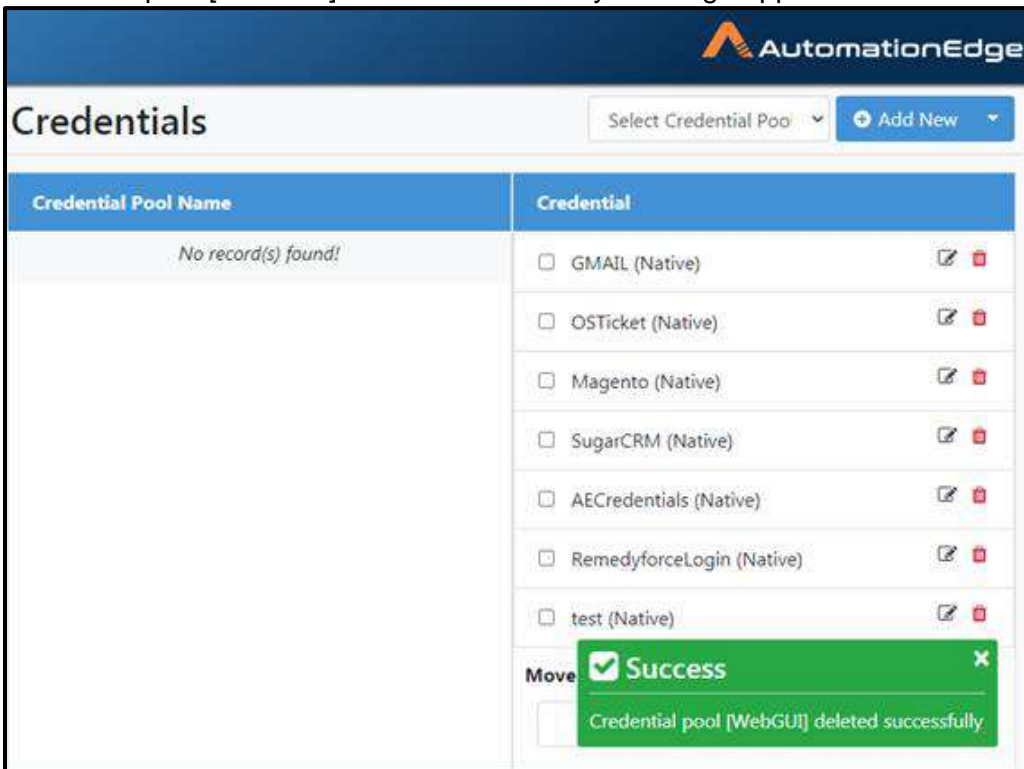


Figure 52c: Credential pool deleted successfully

6.11.1.4 Credential Pool: Features/Permissions for other users

Table 33: Credential Pool Features/Permissions for other users

Feature/Role	Tenant Administrator	Workflow Administrator	User Administrator	Tenant User
Create New Credential Pool	✓	✓	-	-
Edit Credential Pool	✓	✓	-	-
Delete Credential Pool	✓	✓	-	-

6.11.2 Credential

6.11.2.1 Add New Credential

To add a new Credential,

1. Click Credential sub-menu. On the left hand section click Add New button.

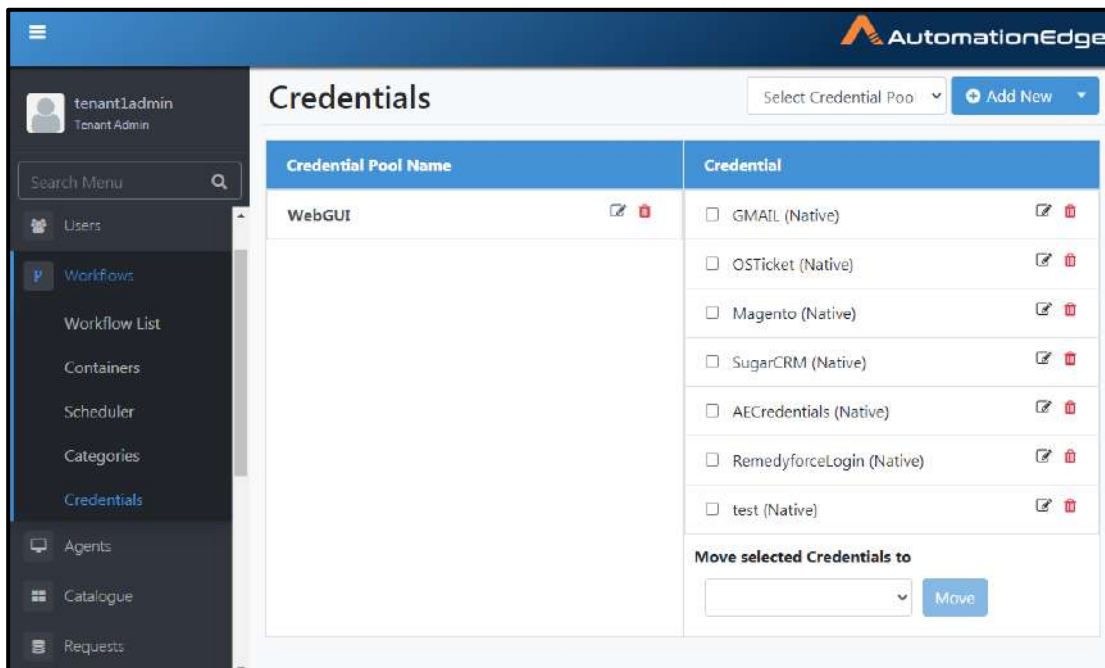
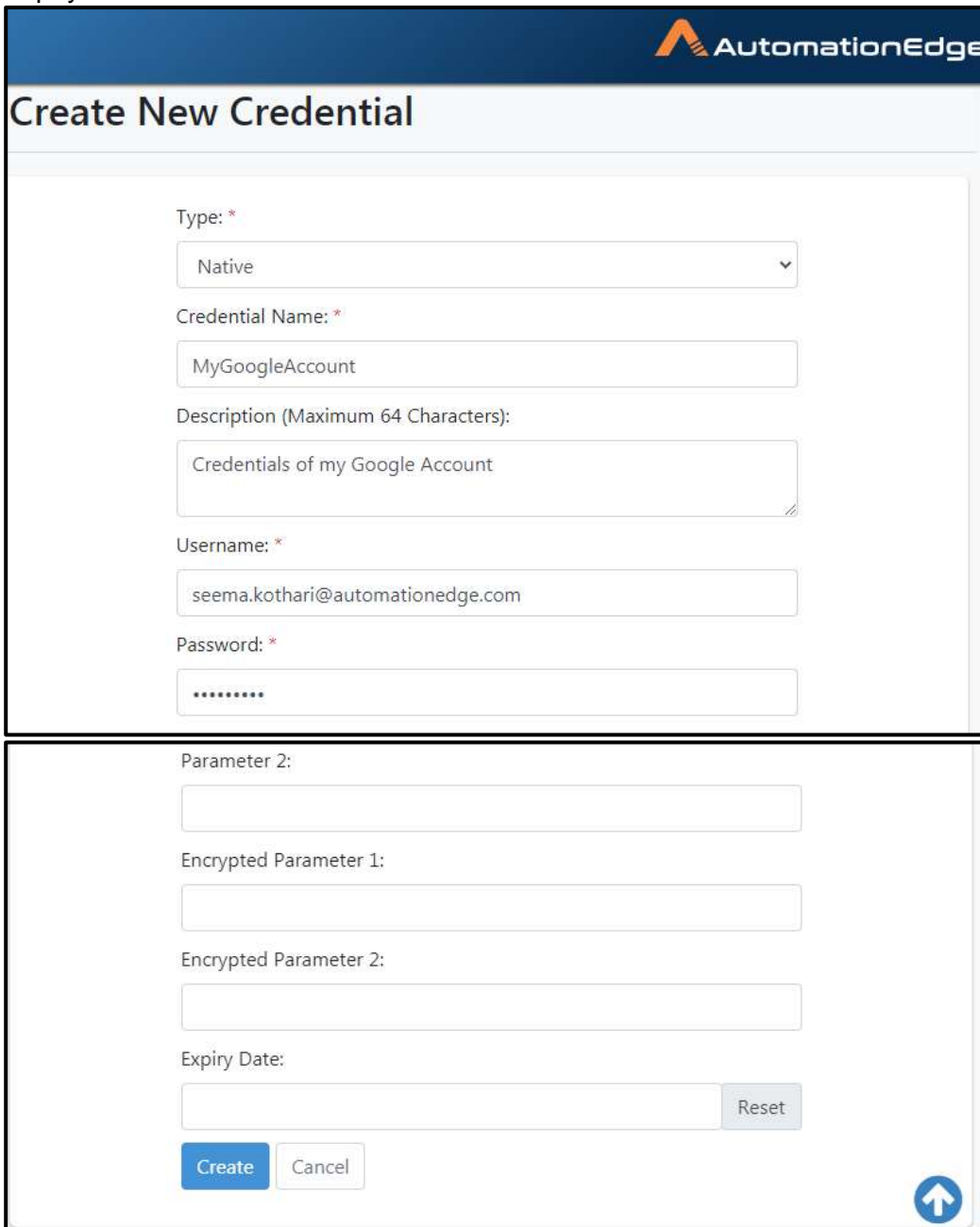


Figure 53a: Add Credential

2. Create New Credential pop-up window appears. Enter details as shown below. Click on Expiry Date.



Create New Credential

Type: *
Native

Credential Name: *
MyGoogleAccount

Description (Maximum 64 Characters):
Credentials of my Google Account

Username: *
seema.kothari@automationedge.com

Password: *

Parameter 2:

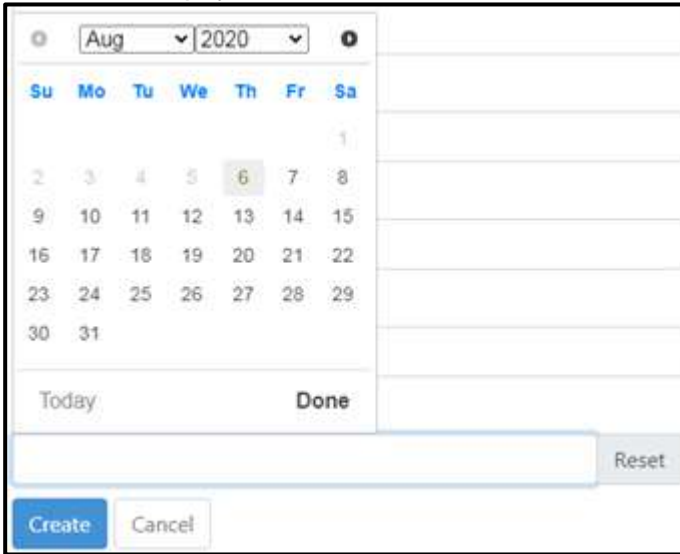
Encrypted Parameter 1:

Encrypted Parameter 2:

Expiry Date:

Figure 53b: New Credential configurations

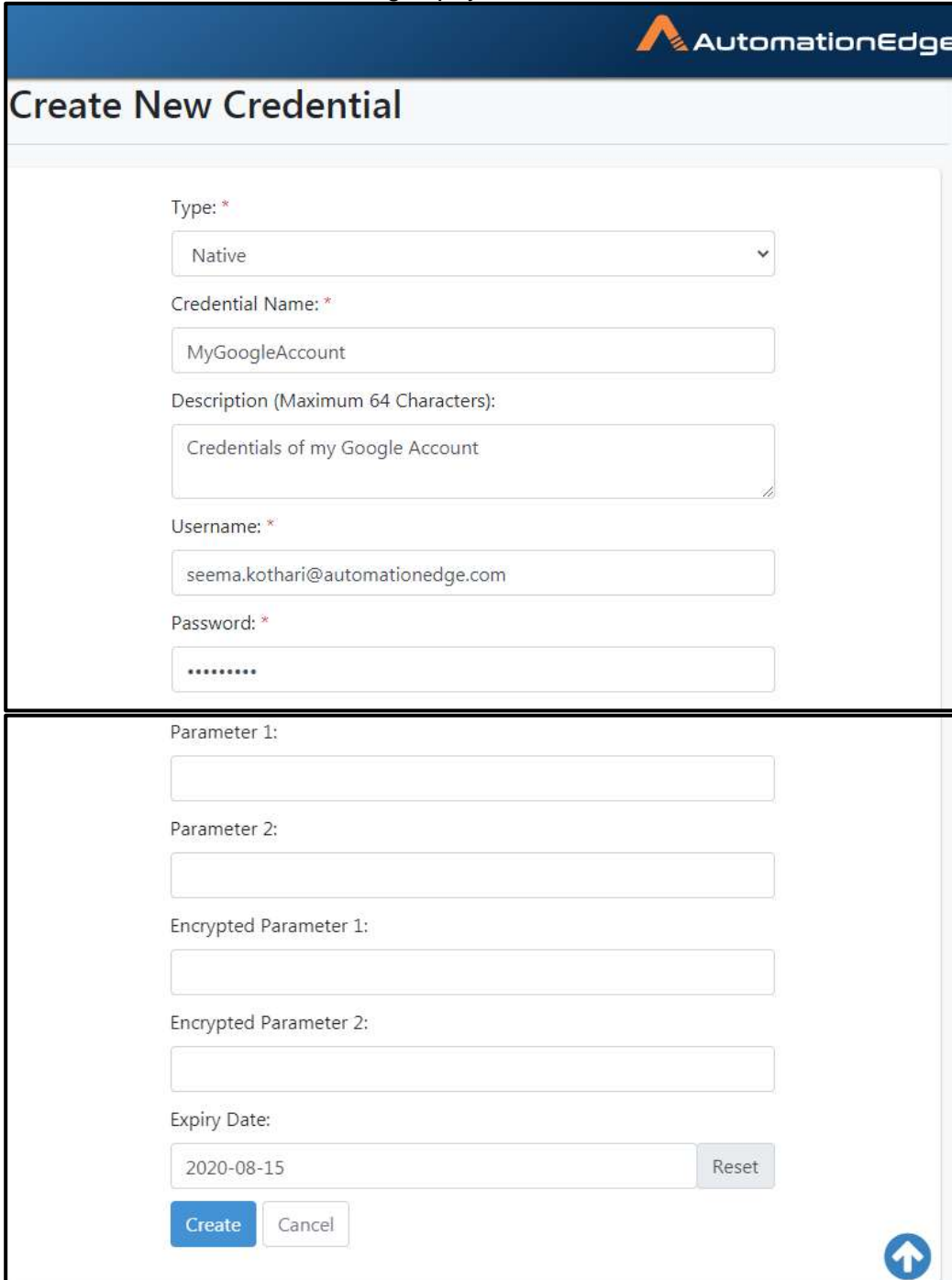
3. Choose an expiry date.



The image shows a date selection interface. At the top, there are dropdown menus for the month (Aug) and year (2020). Below this is a calendar grid for August 2020. The days of the week are labeled: Su, Mo, Tu, We, Th, Fr, Sa. The date '6' is highlighted in a grey box. To the right of the calendar is a vertical stack of empty input fields. Below the calendar, there are 'Today' and 'Done' buttons. At the bottom of the interface, there is a 'Reset' button, and further down, 'Create' and 'Cancel' buttons.

Figure 53c: Choose expiry date from calendar

4. All details for Credential including expiry date are seen below. Click Create.



Create New Credential

Type: *
Native

Credential Name: *
MyGoogleAccount

Description (Maximum 64 Characters):
Credentials of my Google Account

Username: *
seema.kothari@automationedge.com

Password: *
.....

Parameter 1:

Parameter 2:

Encrypted Parameter 1:

Encrypted Parameter 2:

Expiry Date:
2020-08-15


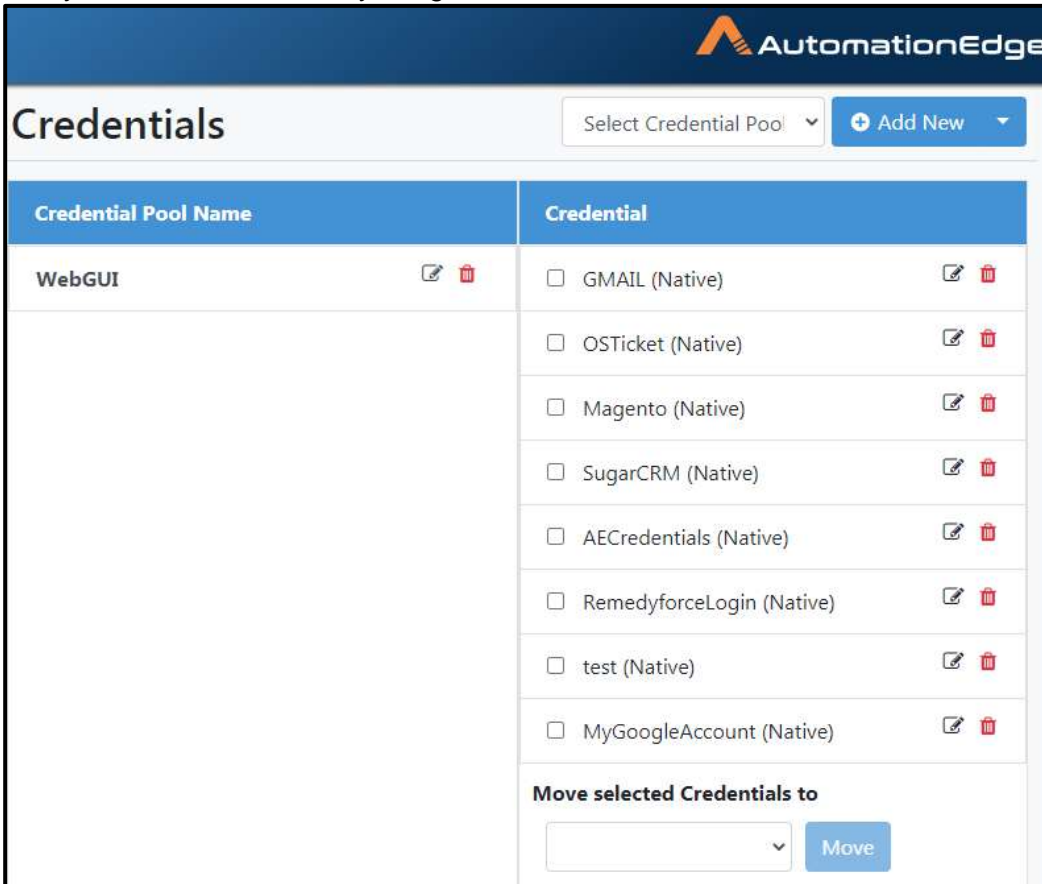


Figure 53d: Create Credential

- The Credential is created and you are taken back to the credentials page. Notice the newly created Credential MyGoogleAccount in the list.



The screenshot displays the AutomationEdge interface for managing credentials. At the top, there is a header with the AutomationEdge logo and a title 'Credentials'. Below the header, there is a search bar labeled 'Select Credential Pool' and a button labeled '+ Add New'. The main content area is a table with two columns: 'Credential Pool Name' and 'Credential'. The 'Credential Pool Name' column contains the text 'WebGUI' and two icons (edit and delete). The 'Credential' column contains a list of credentials, each with a checkbox, the name, and two icons (edit and delete). The credentials listed are: GMAIL (Native), OSTicket (Native), Magento (Native), SugarCRM (Native), AECredentials (Native), RemedyforceLogin (Native), test (Native), and MyGoogleAccount (Native). At the bottom of the table, there is a section titled 'Move selected Credentials to' with a dropdown menu and a 'Move' button.

Credential Pool Name	Credential
WebGUI	<input type="checkbox"/> GMAIL (Native)
	<input type="checkbox"/> OSTicket (Native)
	<input type="checkbox"/> Magento (Native)
	<input type="checkbox"/> SugarCRM (Native)
	<input type="checkbox"/> AECredentials (Native)
	<input type="checkbox"/> RemedyforceLogin (Native)
	<input type="checkbox"/> test (Native)
	<input type="checkbox"/> MyGoogleAccount (Native)

Move selected Credentials to

Figure 53e: Credential Creation Success Message

5. A description of the fields is provided in the table below.

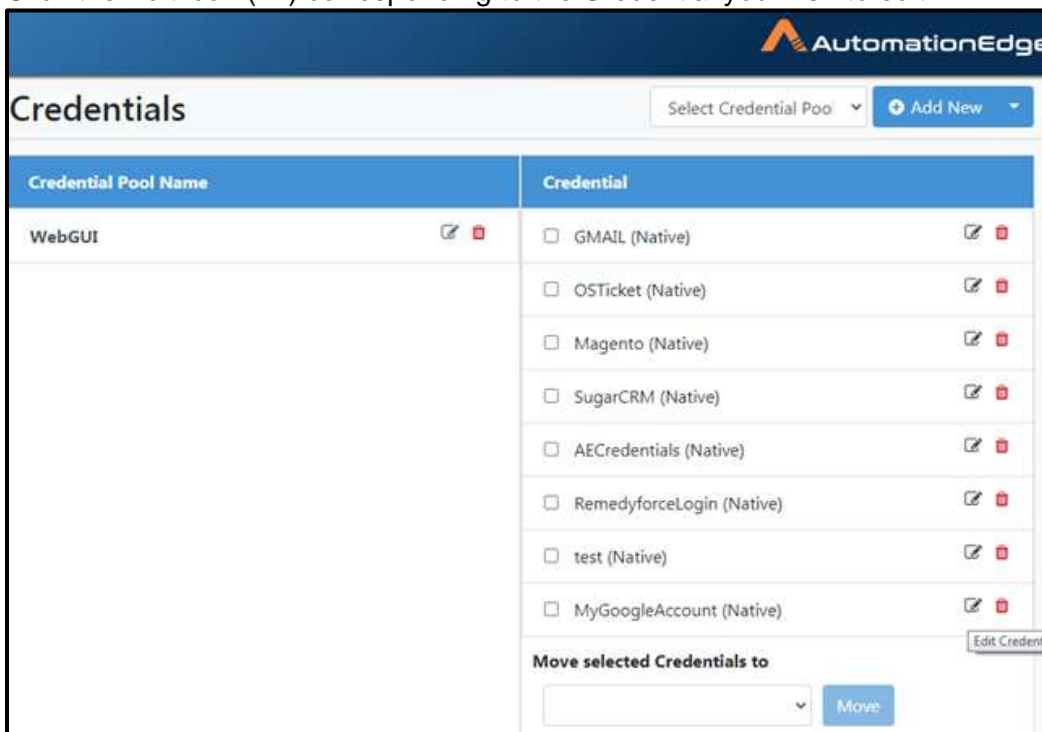
Table 34: Create New Credential Field Descriptions

Field Name	Description
Credential Name	Specify a name for the Credential.
Description	Provide a description for the Credential.
Username	Provide a Username for the Credential.
Password	Provide a password for the username. Password is stored in encrypted format.
Parameter 1	Provide an optional Parameter 1.
Parameter 2	Provide an optional Parameter 2
Encrypted Parameter 1	Provide an optional Encrypted Parameter 1. You may use encrypted parameters to store sensitive fields (e.g. Access Token, Security Key) that you do not wish to expose to users. It is stored in encrypted format.
Encrypted Parameter 2	Provide an optional Encrypted Parameter 2. It is stored in encrypted format, like Encrypted Parameter 1.
Expiry Date	Provide an expiry date for the credential from the picker.
Buttons:	
Create	Click Create button to save the Credential
Cancel	Click Cancel button to Cancel the operation.

6.11.2.2 Edit Credential

To edit credential,

1. Click Credential sub-menu.
2. Click the Edit icon (✎) corresponding to the Credential you wish to edit.



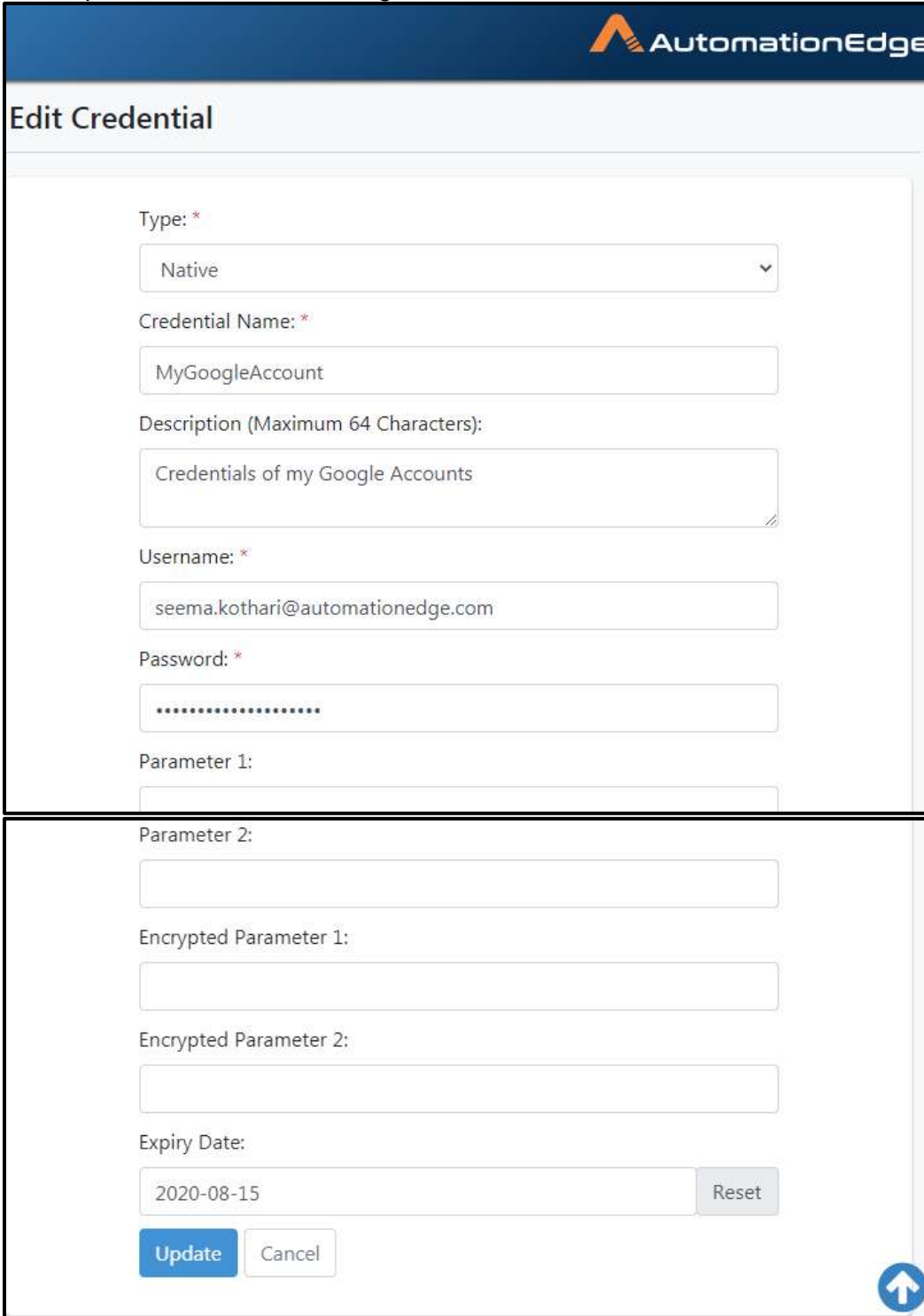
Credential Pool Name	Credential
WebGUI	<input type="checkbox"/> GMAIL (Native)
	<input type="checkbox"/> OSTicket (Native)
	<input type="checkbox"/> Magento (Native)
	<input type="checkbox"/> SugarCRM (Native)
	<input type="checkbox"/> AECredentials (Native)
	<input type="checkbox"/> RemedyforceLogin (Native)
	<input type="checkbox"/> test (Native)
	<input type="checkbox"/> MyGoogleAccount (Native)

Move selected Credentials to

Move

Figure 54a: Select Credential to Edit

3. Click Update to confirm the changes.



The screenshot shows the 'Edit Credential' interface. At the top, there is the AutomationEdge logo. Below it, the title 'Edit Credential' is displayed. The form contains the following fields and controls:

- Type:** A dropdown menu with 'Native' selected.
- Credential Name:** A text input field containing 'MyGoogleAccount'.
- Description (Maximum 64 Characters):** A text area containing 'Credentials of my Google Accounts'.
- Username:** A text input field containing 'seema.kothari@automationedge.com'.
- Password:** A password input field with masked characters.
- Parameter 1:** An empty text input field.
- Parameter 2:** An empty text input field.
- Encrypted Parameter 1:** An empty text input field.
- Encrypted Parameter 2:** An empty text input field.
- Expiry Date:** A date input field showing '2020-08-15' and a 'Reset' button.
- Buttons:** 'Update' (blue), 'Cancel' (grey), and 'Reset' (grey).
- Navigation:** A blue circular button with an upward arrow in the bottom right corner.

Figure 54b: Edit Credential

4. You are taken back to the Credentials page. This completes the process of editing a Credential.

6.11.2.3 Delete Credential

To delete Credential,

1. Click Credential sub-menu.
2. Look in the right section for the credential to be deleted. Click the Delete icon (🗑️) corresponding to the credential you wish to delete.
3. Click Delete to confirm Credential deletion

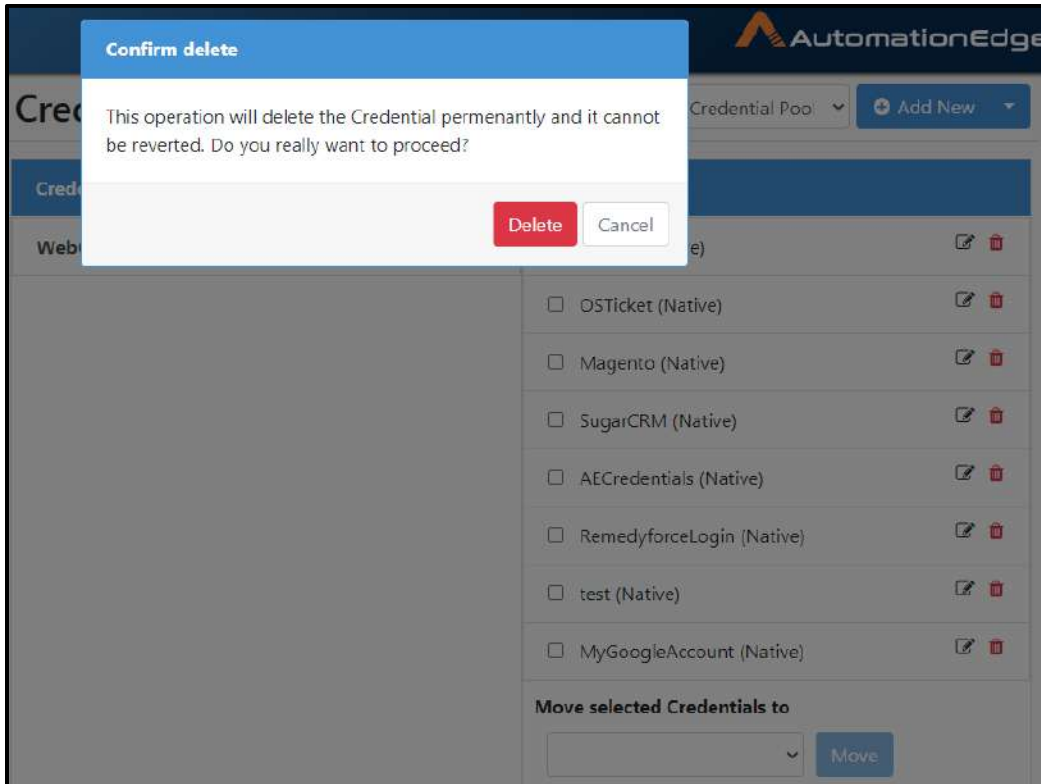


Figure 55a: Confirming Credential Deletion

- Credential deleted successfully message appears.

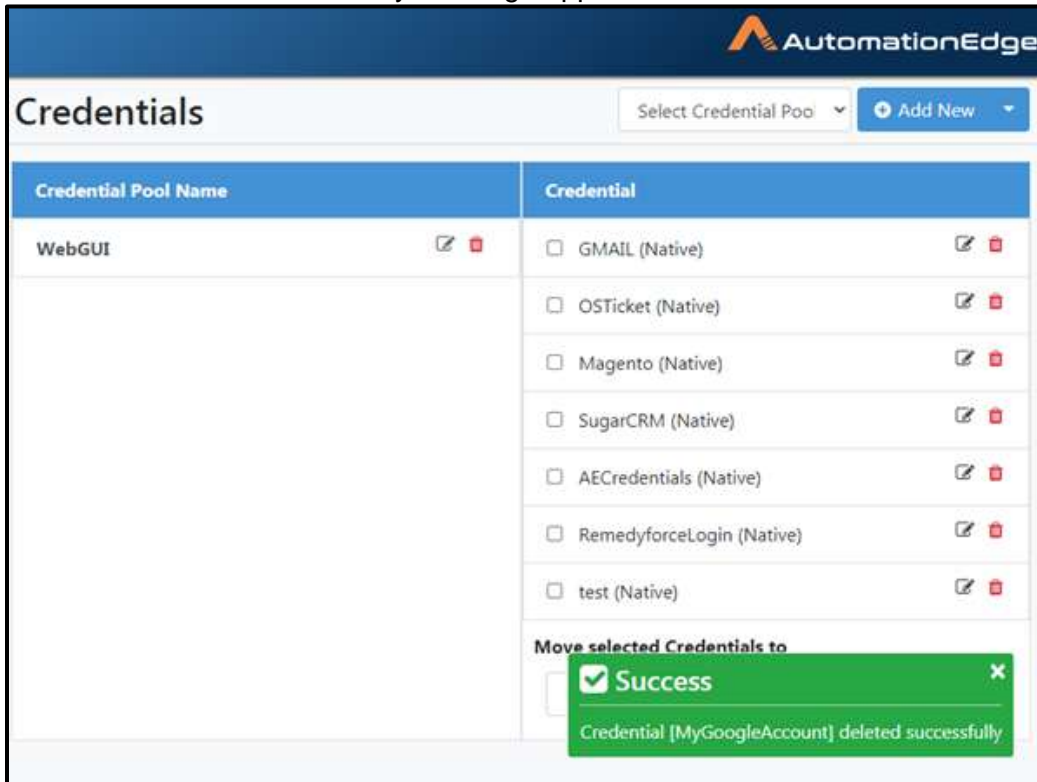


Figure 55b: Credential deleted successfully message

6.11.2.4 Move Credential

Use Move Credentials functionality to Move Credential to a Credential pool.

Follow the steps below,

- Go to the Workflow menu and Credential Sub-menu.
- Select the checkbox next to the Credentials you wish to move as shown below.

3. Select the Credential Pool to move to from the drop down list as seen below. Click Move.

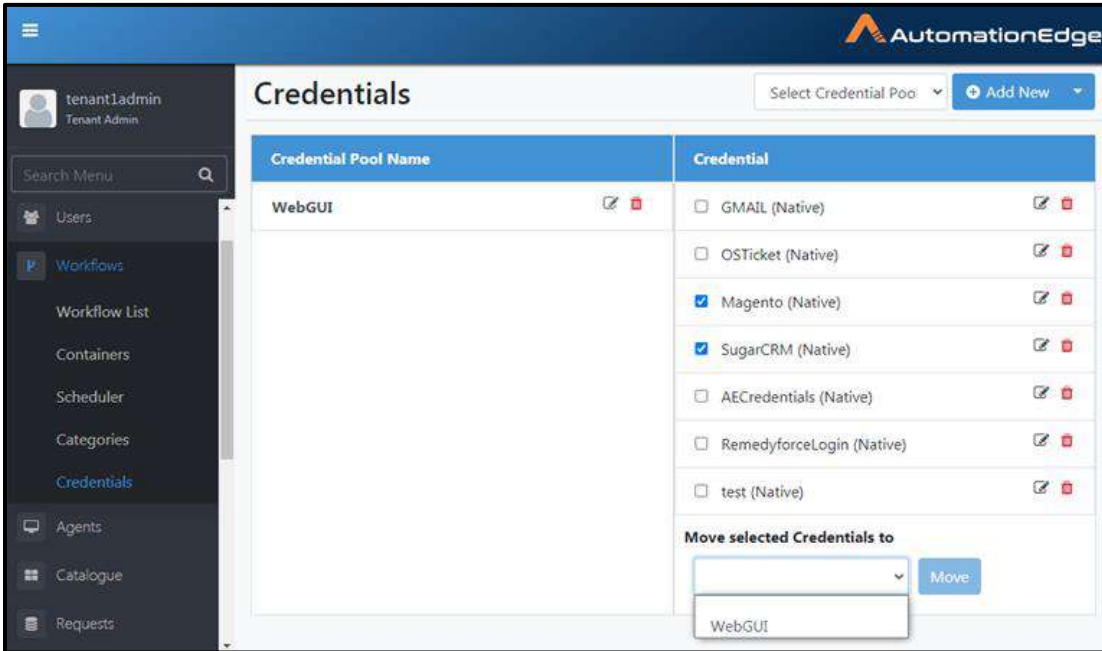


Figure 56a: Move Selected Credentials to a Credential Pool

4. The Credential has been moved successfully to the chosen Credential Pool WebGUI.
5. Expand WebGUI Credential Pool to see the Credentials.

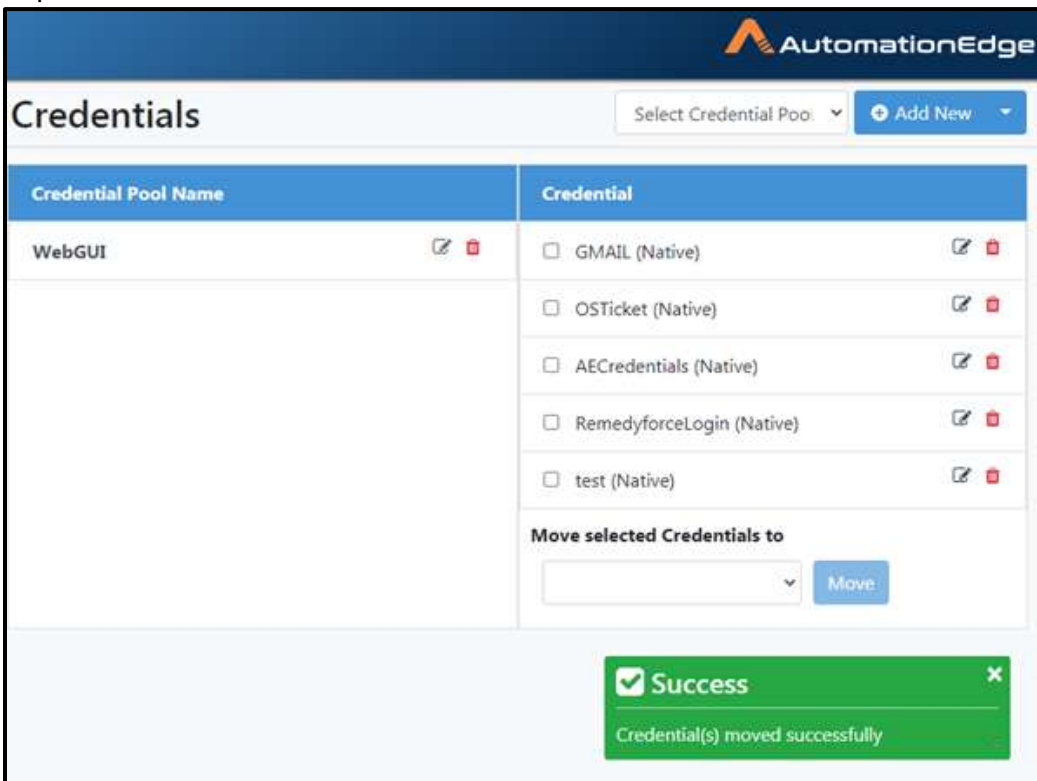


Figure 56b: Credential Moved Success Message

- Select WebGUI Credential pool from the drop down list.

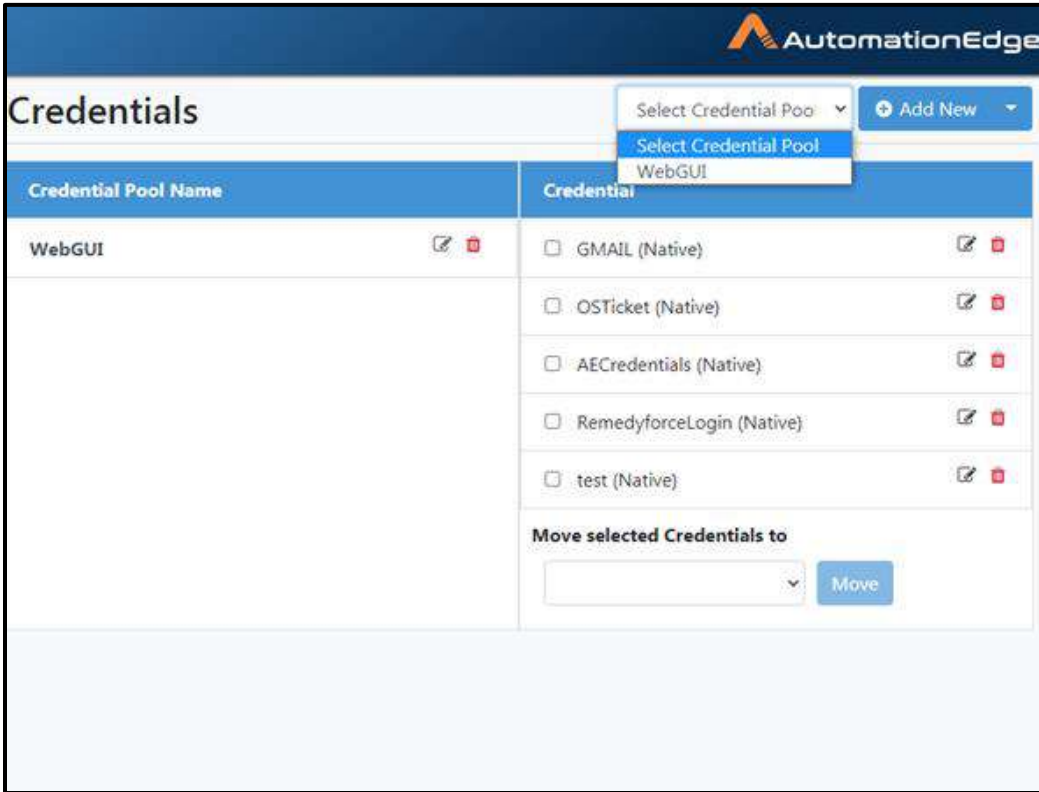


Figure 56c: Select Credential Pool

- Moved Credentials are now visible in WebGUI Credential pool.

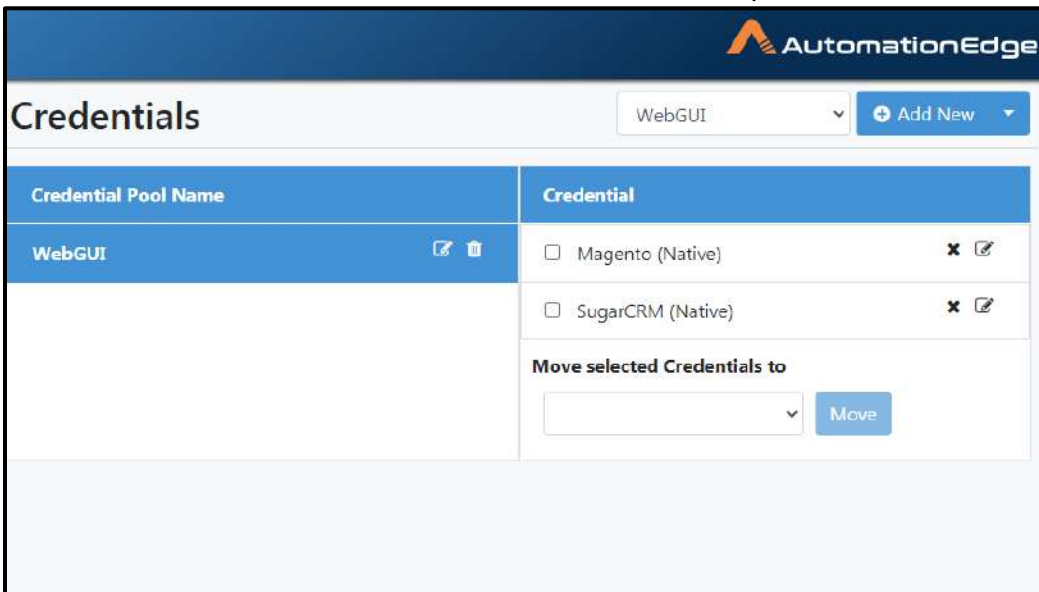


Figure 56d: View Credentials in Selected Credential Pool

6.11.2.5 Credential: Features/Permissions for other users

Table 35: Credentials Features/Permissions for other users

Feature/Role	Tenant Administrator	Workflow Administrator	User Administrator	Tenant User	Activity Monitor
Create New Credential	✓	✓	-	-	-
Edit Credential	✓	✓	-	-	-
Delete Credential	✓	✓	-	-	-
Move Credential to Credential Pool	✓	✓	-	-	-

6.12 Workflow Scheduler

Workflow Scheduler is used for scheduling workflow execution automatically at specified times. However, assisted workflows cannot be scheduled.

6.12.1 Add New Schedule

To add a new schedule:

1. Click Workflows menu. Click Scheduler sub-menu.
2. Add New Schedule

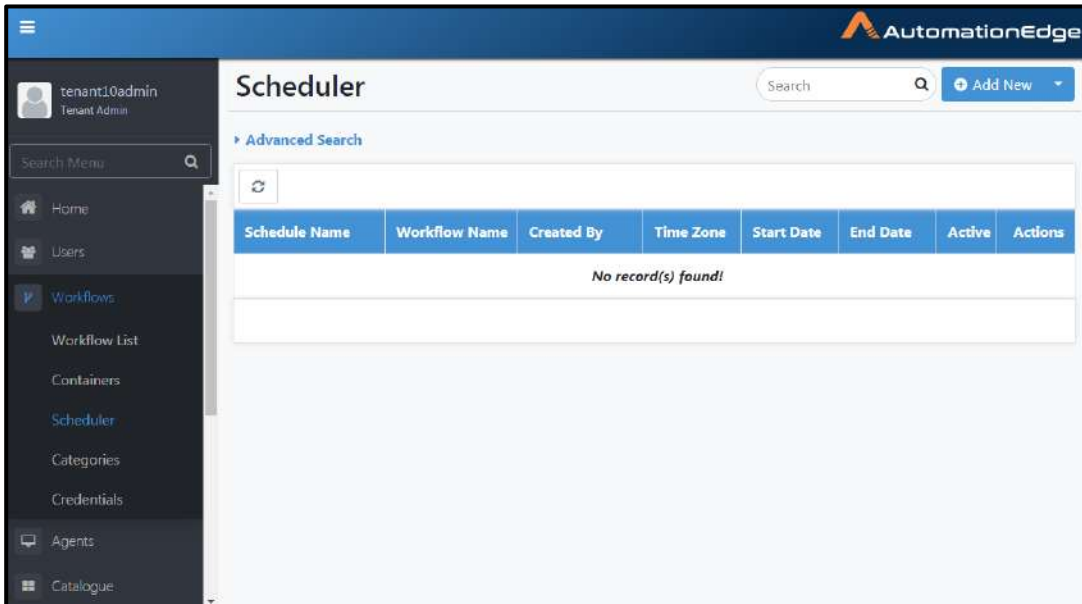


Figure 57a: Adding New Schedule

3. Workflow scheduler screen appears. It has two sections, Workflow Details and Schedule Details.

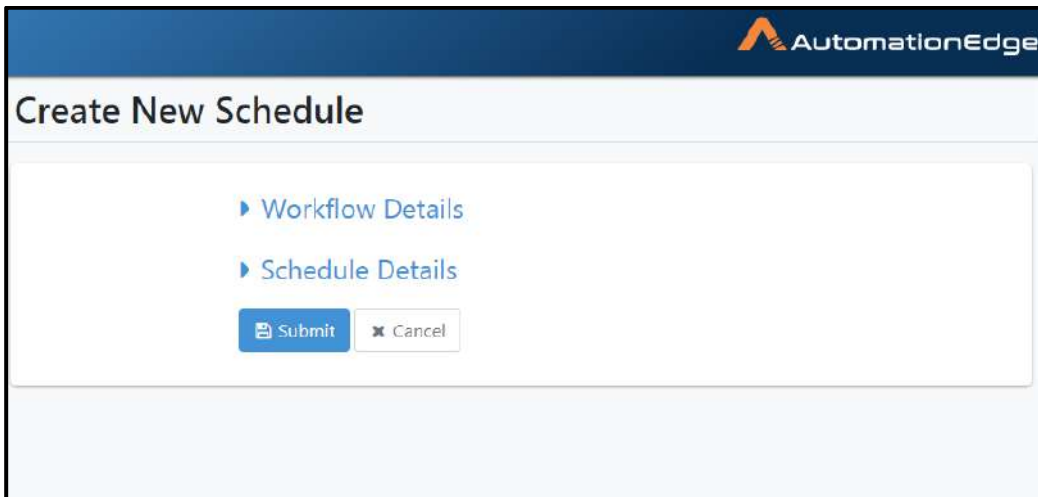


Figure 57b: Create new Schedule sections

4. Enter Workflow Details. First choose the workflow to be scheduled by enabling checkbox next to the workflow. Alternatively type a workflow name in the search region as seen below. It will filter the list of workflows and then you may enable checkbox next to the workflow desired.

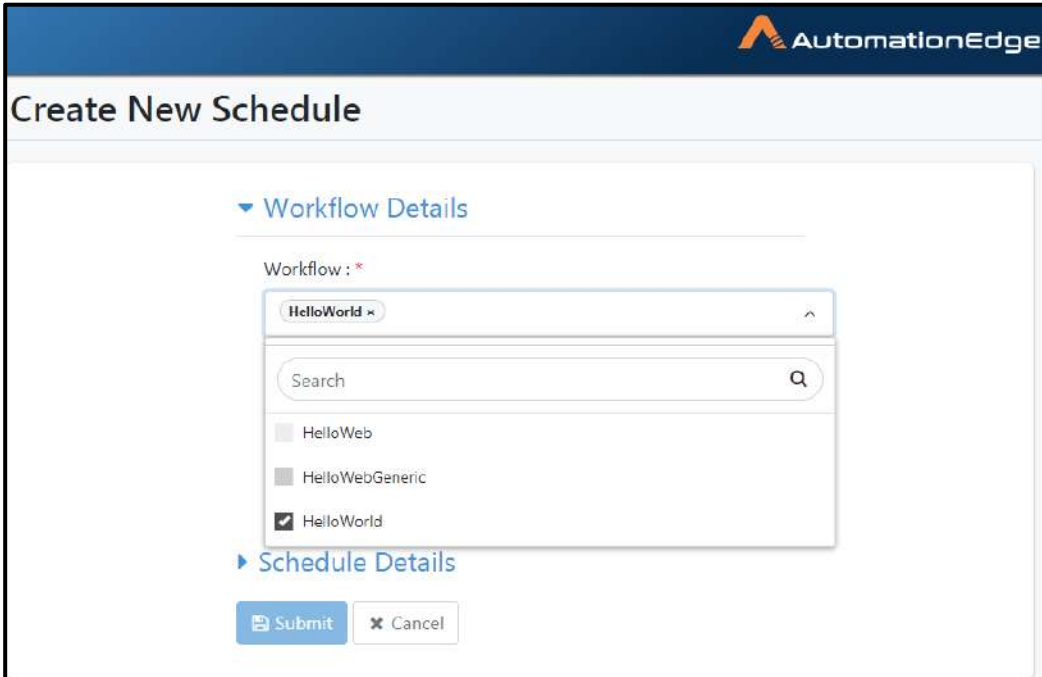


Figure 57c: Choose workflow to be scheduled

5. Once the workflow is chosen, the associated runtime parameters are displayed. Provide desired values.

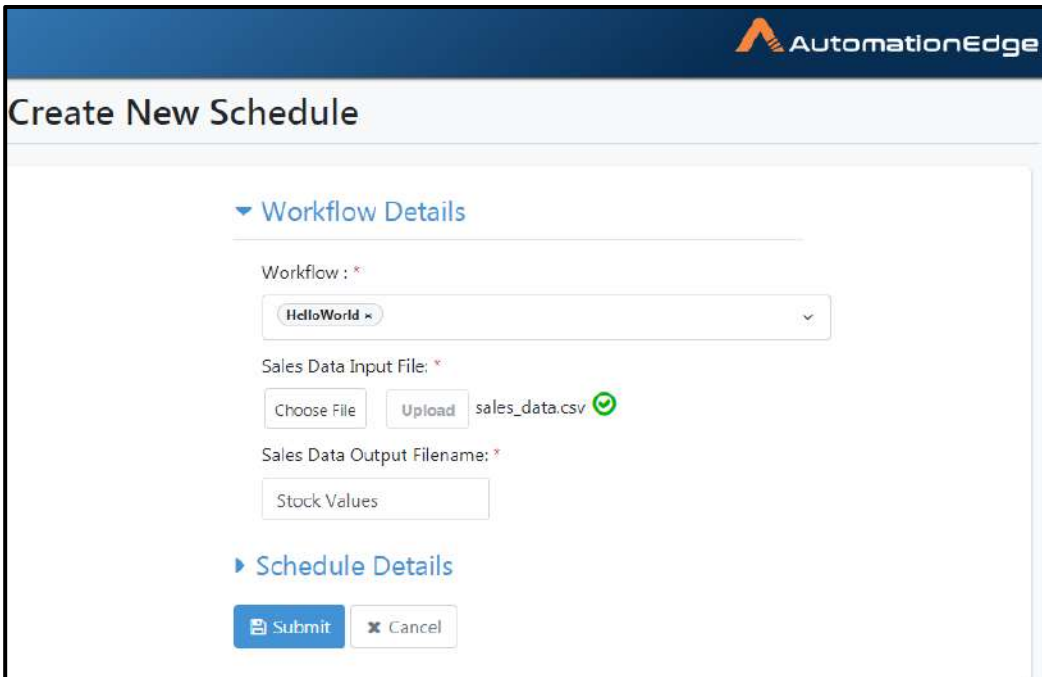


Figure 57d: Provide values for runtime parameters

6. Now populate Schedule Details as shown below. Click Submit.

Create New Schedule

▶ Workflow Details

▼ Schedule Details

Schedule Name *

Description (Maximum 150 Characters) *

Run Schedule Infinitely

Start Date: * End Date: *

Schedule Type: *

Time Zone: *

Start Time: *
 :

Repeat Every *

End Time: *
 :




Figure 57e: Entering Workflow Schedule Details

- The schedule is saved successfully message appears.

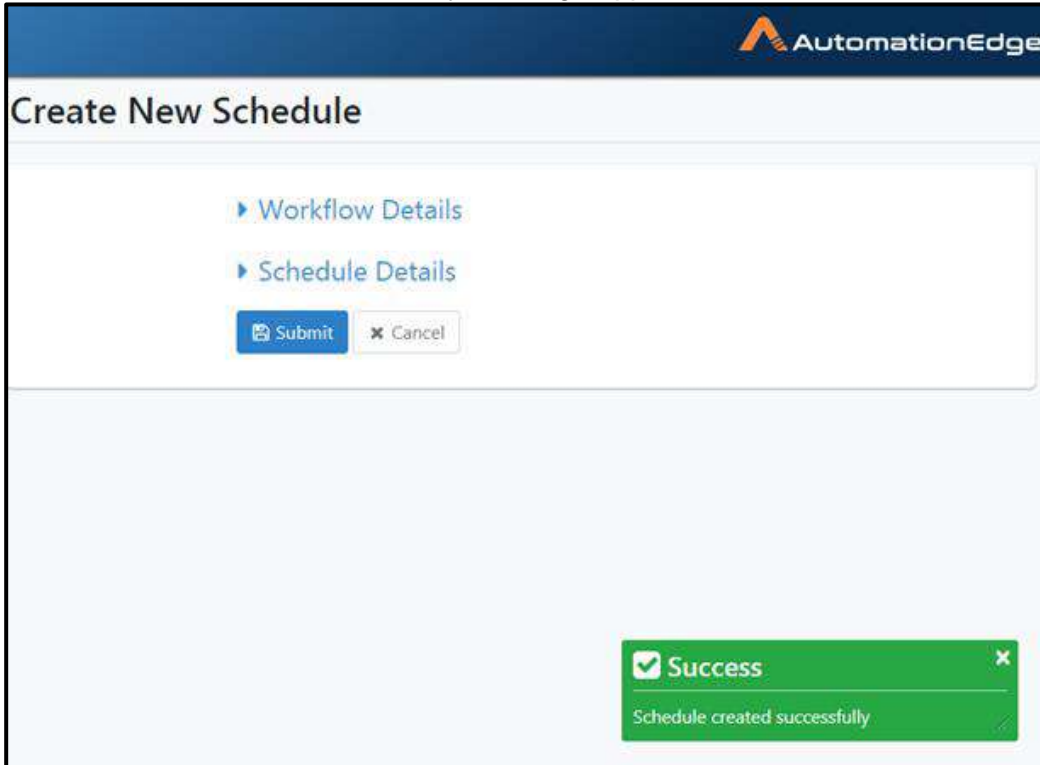


Figure 57f: Schedule Saved Successfully

- The Schedule is now visible under Scheduler sub-menu

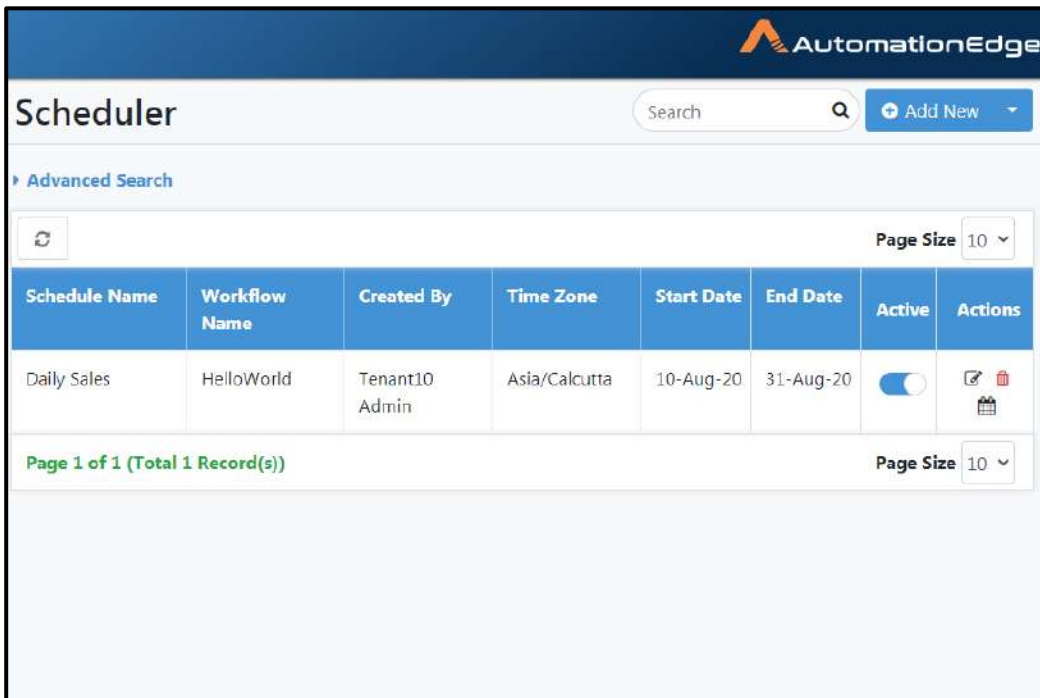


Figure 57g: Schedule List

The field descriptions are shown in the table below.

Table 36: Add New Schedule: Workflow Scheduler Field/Button Description

Field Name	Description
Workflow	Select workflow from the drop-down list. This field is Mandatory.
Workflow Runtime Parameters	Provide values for runtime parameters of the workflow as per workflow definition.
Schedule Details:	
Schedule Description	To specify schedule description. This field is Mandatory.
Schedule Start Date	To specify scheduler, start date. This field is Mandatory.
Run Schedule Infinitely	Select this to run schedule forever. If enabled Schedule End Date becomes invisible. Else, Schedule End has to be specified.
Schedule End Date	Option Available only if "Run Schedule infinitely" is not selected. When visible this field is Mandatory.
Schedule Type	It displays different options for daily, monthly and weekly. This field is Mandatory.
Time Zone	The user's (browser) time zone is populated by default. User can change the time zone if needed. Once a schedule is created time zone is not editable.
Schedule Execution Time/ Schedule Start Time	Specify the start time in hours and minutes. The schedule will start execution at a time greater than or equal to Start time specified. If 'Repeat Every' is enabled, then Schedule Execution Time is labelled as Schedule Start Time. This field is Mandatory. <ul style="list-style-type: none"> • If schedule type is Daily the schedule starts running at this time every day. • If schedule type is Weekly the schedule starts running at this time on the weekdays selected. • If schedule type is Monthly the schedule starts running at this time for selected months and selected days.
Repeat Every	Check this box to add repeat instructions. If not selected schedule runs once per day. If checked it enables repeat by hour or minute. <ul style="list-style-type: none"> • If Hours is selected 1-24 values are available in the drop down list. • If Minutes are selected 1, 2, 3, 4, 5, 10, 15, 20, 30, 45 values are available in the dropdown list.
Schedule End Time	Specify the end time in hours and minutes. The schedule will execute until a time less than the end time specified. This field is enabled if 'Repeat Every' is enabled. When visible this field is Mandatory.

	<ul style="list-style-type: none"> • If schedule type is Daily the schedule stops running at this time every day. • If schedule type is Weekly the schedule stops running at this time on the weekdays selected. • If schedule type is Monthly the schedule stops running at this time for selected months and selected days.
Buttons:	
Submit	To submit workflow scheduler details.
Cancel	To cancel adding new workflow scheduler.

6.12.2 Search Schedule

Following are the steps to search for a schedule.

1. Click Workflows menu and Scheduler sub-menu.
2. Type a search string for schedule description in the Search Schedule free text box.
3. The Schedule list gets filtered automatically as per text entered or click the search icon.

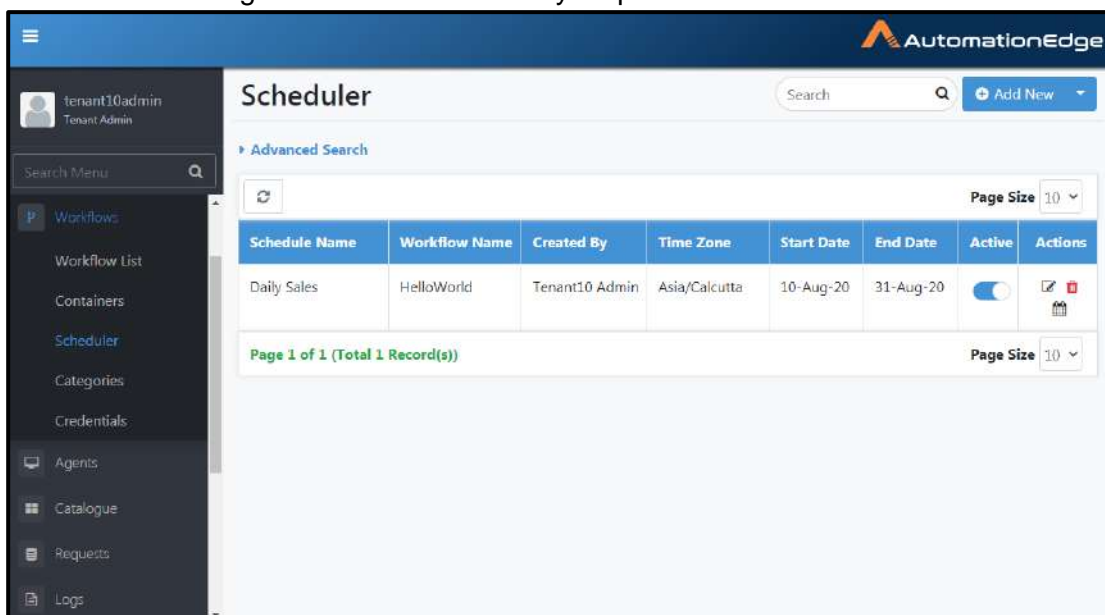





Figure 58a: Search Schedule

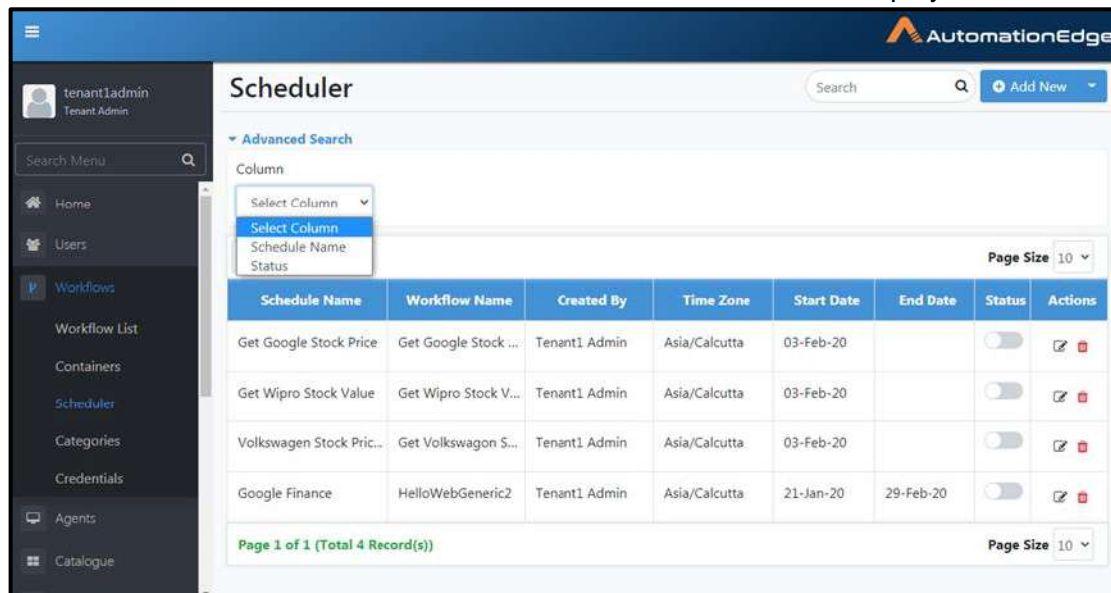
Table 37: List of Schedulers

Field Name	Description
Schedule Description	Displays schedule description.
Workflow Name	Select workflow from the drop-down list.
Created By	Displays username that created the Schedule.
Start Date	Displays scheduled start date.
End Date	Displays scheduled end date.
Actions:	
Active (<input checked="" type="checkbox"/>)	Select checkbox to activate the schedule. User can select or de-select the check box to enable or disable the Scheduler.
Edit ()	Click Edit Pencil icon to edit schedule details.
Delete Button ()	Click Delete icon to delete the schedule.
View upcoming fire times()	Click to view the list of upcoming fire times for the schedule.

6.12.2.1 Scheduler Advanced Search

Following are the steps for Scheduler Advanced Search.

1. Click on the arrow beside Advanced Search. The Column field is displayed as below.



The screenshot shows the AutomationEdge Scheduler interface. The 'Advanced Search' dropdown menu is open, displaying a 'Column' field with a dropdown menu. The dropdown menu is currently open, showing 'Select Column' as the selected option. Below the dropdown menu, there is a table with the following columns: Schedule Name, Workflow Name, Created By, Time Zone, Start Date, End Date, Status, and Actions. The table contains four rows of data. The page size is set to 10, and the page number is 1 of 1 (Total 4 Record(s)).









Schedule Name	Workflow Name	Created By	Time Zone	Start Date	End Date	Status	Actions
Get Google Stock Price	Get Google Stock ...	Tenant1 Admin	Asia/Calcutta	03-Feb-20		<input type="checkbox"/>	 
Get Wipro Stock Value	Get Wipro Stock V...	Tenant1 Admin	Asia/Calcutta	03-Feb-20		<input type="checkbox"/>	 
Volkswagen Stock Pric...	Get Volkswagon S...	Tenant1 Admin	Asia/Calcutta	03-Feb-20		<input type="checkbox"/>	 
Google Finance	HelloWebGeneric2	Tenant1 Admin	Asia/Calcutta	21-Jan-20	29-Feb-20	<input type="checkbox"/>	 

Figure 58b: Select a column to search

- Once a Column value is chosen the Comparator field is enabled. Select from the drop down list.

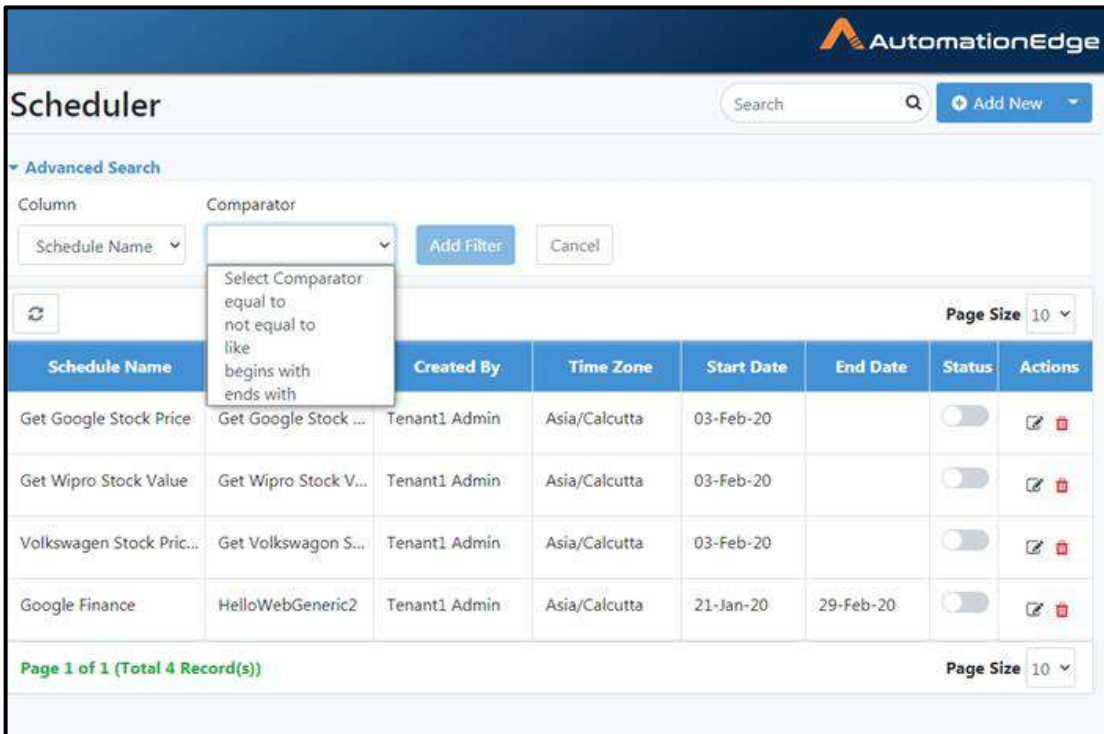


Figure 58c: Select Comparator

- Next the Value field is displayed. Provide a Value for Advanced Search. Click Add Filter.

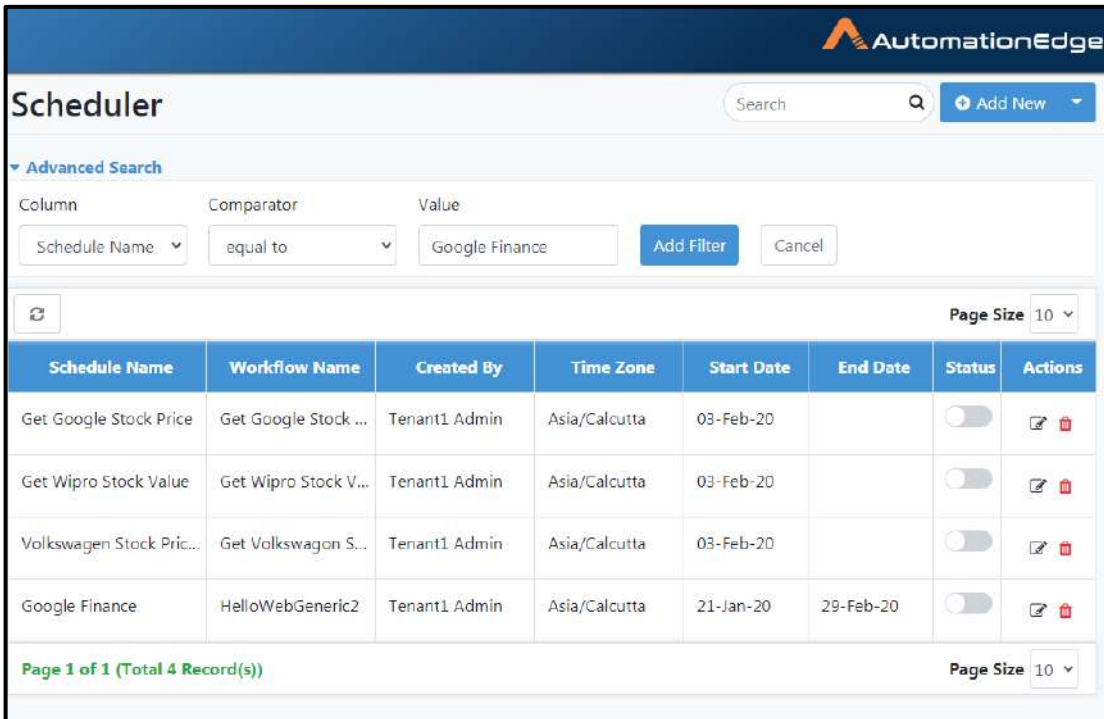


Figure 58d: Provide Value

4. You can now see the filter and results of Advanced Search.

The screenshot shows the AutomationEdge Scheduler interface. At the top, there is a search bar with the text 'Search' and a magnifying glass icon, and a blue button labeled 'Add New'. Below the search bar, there is a section for 'Advanced Search' with a filter applied: 'Schedule Name = Google Finance'. A refresh icon is visible to the left of the table. The table has columns: Schedule Name, Workflow Name, Created By, Time Zone, Start Date, End Date, Status, and Actions. The first row shows 'Google Finance', 'HelloWebGeneric2', 'Tenant1 Admin', 'Asia/Calcutta', '21-Jan-20', '29-Feb-20', and a status toggle. Below the table, it says 'Page 1 of 1 (Total 1 Record(s))' and 'Page Size 10'.

Figure 58e: Search Results with filter applied

Comparator descriptions for advanced search options are as follows.

Table: Advanced Search Options by Schedule Name

Field	Description
Equal To	To search entries by the exact entered text.
Not Equal To	To search entries not matching the entered text.
Like	To search entries containing the entered text
Begins With	To search entries that begins with the entered text.
Ends With	To search entries that ends with the entered text.

Table: Advanced Search Options by Status

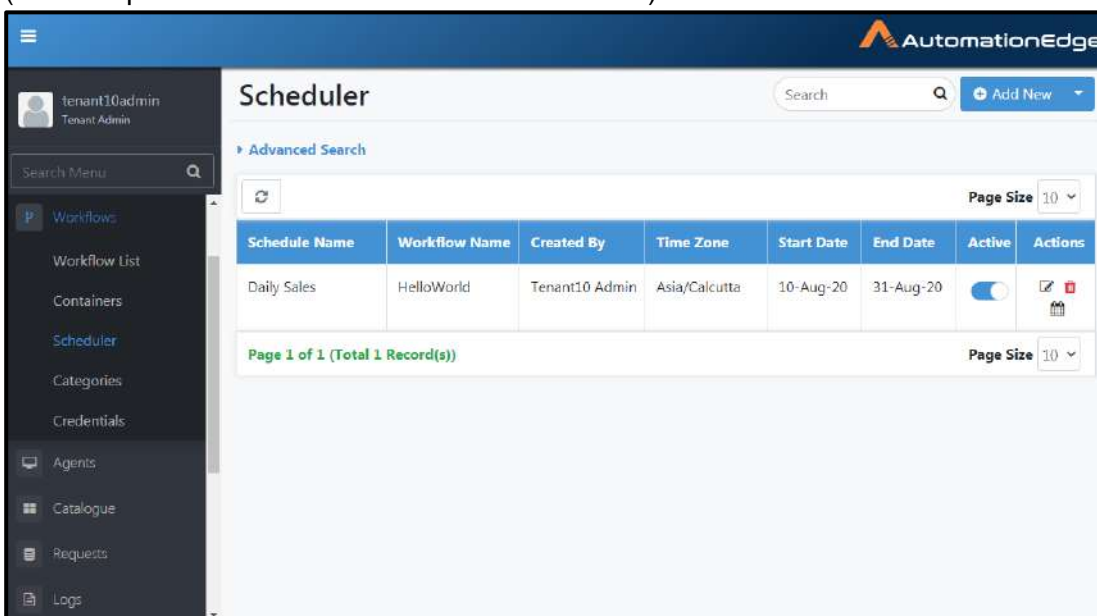
Field	Description
Equal To	To search entries by the exact entered text.
Not Equal To	To search entries not matching the entered text.

6.12.3 Deactivate Schedule



Following are the steps to deactivate a schedule,

1. Click Workflows menu and Scheduler sub-menu.
2. Search a Scheduler to edit from the list.
3. Under Active column click toggle to make the schedule inactive.

(Note: Expired schedules can also be deactivated).



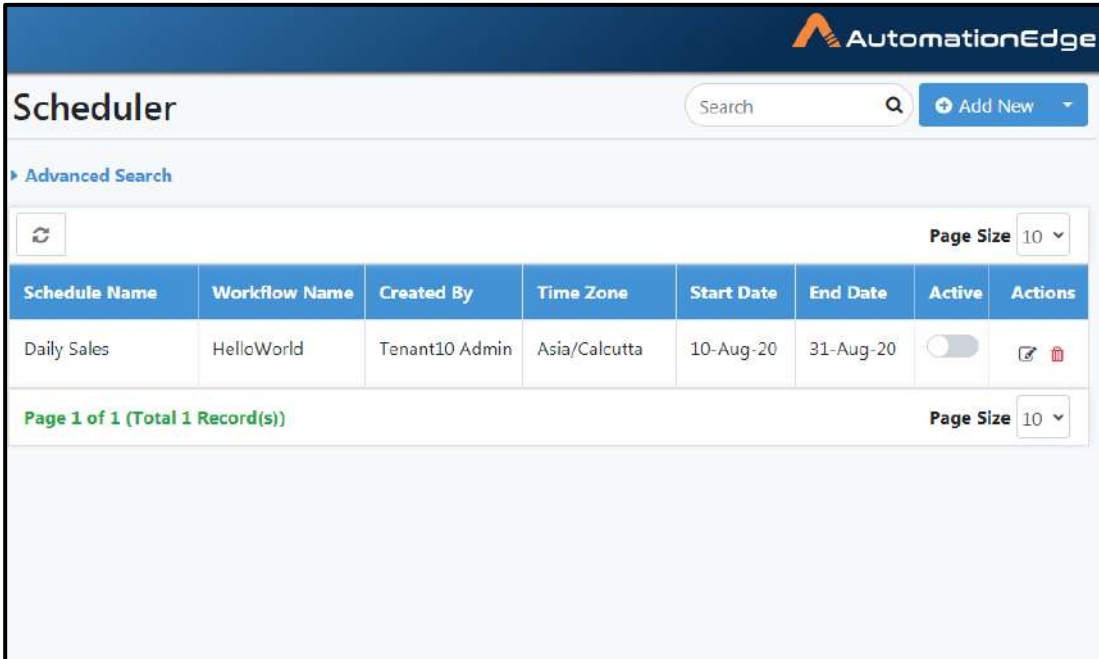
The screenshot displays the AutomationEdge Scheduler interface. The left sidebar shows the navigation menu with 'Scheduler' selected. The main content area shows a table with the following data:

Schedule Name	Workflow Name	Created By	Time Zone	Start Date	End Date	Active	Actions
Daily Sales	HelloWorld	Tenant10 Admin	Asia/Calcutta	10-Aug-20	31-Aug-20	<input checked="" type="checkbox"/>	 

Page 1 of 1 (Total 1 Record(s))

Figure 59a: Deactivate Schedule

- The schedule is now deactivated as seen below.



The screenshot shows the AutomationEdge Scheduler interface. At the top, there is a search bar and an 'Add New' button. Below that is an 'Advanced Search' section with a refresh icon and a 'Page Size' dropdown set to 10. The main content is a table with the following data:

Schedule Name	Workflow Name	Created By	Time Zone	Start Date	End Date	Active	Actions
Daily Sales	HelloWorld	Tenant10 Admin	Asia/Calcutta	10-Aug-20	31-Aug-20	<input type="checkbox"/>	Edit Delete

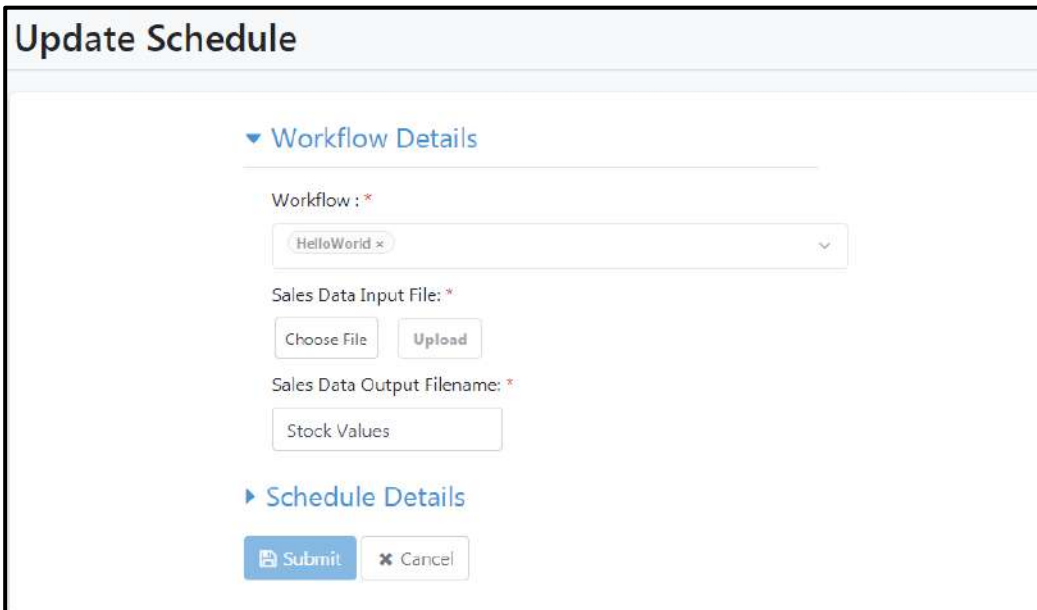
Below the table, it indicates 'Page 1 of 1 (Total 1 Record(s))' and another 'Page Size' dropdown set to 10.

Figure 59b: Schedule Deactivated

6.12.4 Edit Schedule

Following are the steps to edit a schedule.

- Click Workflows menu and Scheduler sub-menu.
- Search a Scheduler to edit from the list and under Actions column click edit. Edit Schedule details as shown below and Click Submit.



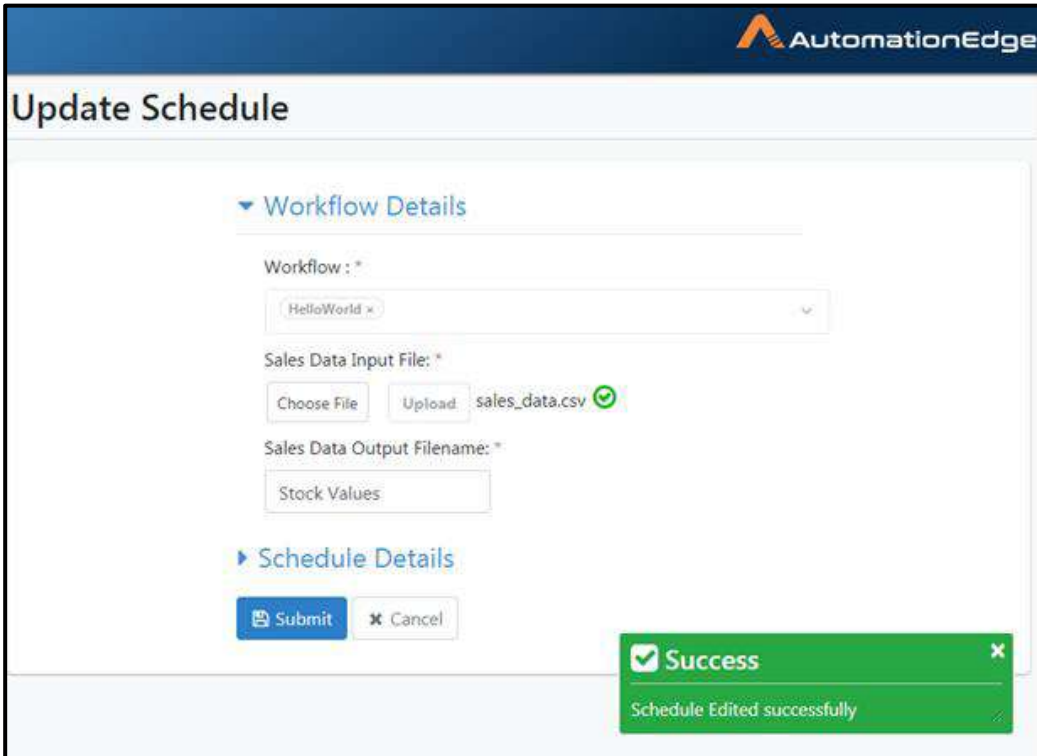
The screenshot shows the 'Update Schedule' form. It has a 'Workflow Details' section with the following fields:

- Workflow:** A dropdown menu with 'HelloWorld' selected.
- Sales Data Input File:** A field with 'Choose File' and 'Upload' buttons.
- Sales Data Output Filename:** A text input field containing 'Stock Values'.

Below the 'Workflow Details' section is a 'Schedule Details' section with 'Submit' and 'Cancel' buttons.

Figure 60a: Edit Schedule

3. Choose File and upload a file as part of edit. Click Submit
4. Schedule edited successfully message appears.



The screenshot displays the 'Update Schedule' interface in the AutomationEdge application. The page title is 'Update Schedule'. Under the 'Workflow Details' section, the 'Workflow' dropdown is set to 'HelloWorld'. The 'Sales Data Input File' field shows an uploaded file named 'sales_data.csv' with a green checkmark icon. The 'Sales Data Output Filename' field is set to 'Stock Values'. Below these fields, there are 'Submit' and 'Cancel' buttons. A green success message box is visible in the bottom right corner, stating 'Success' and 'Schedule Edited successfully'.

Figure 60b: Schedule edited successfully

6.12.5 Delete Schedule

Following are the steps to delete a schedule.

1. Click Workflows menu and Scheduler sub-menu.
2. Search a Scheduler to edit from the list.
3. Under Active column click toggle to make the schedule inactive.
4. Under Actions column click delete icon.
5. Acknowledge Schedule delete confirmation pop-up message.

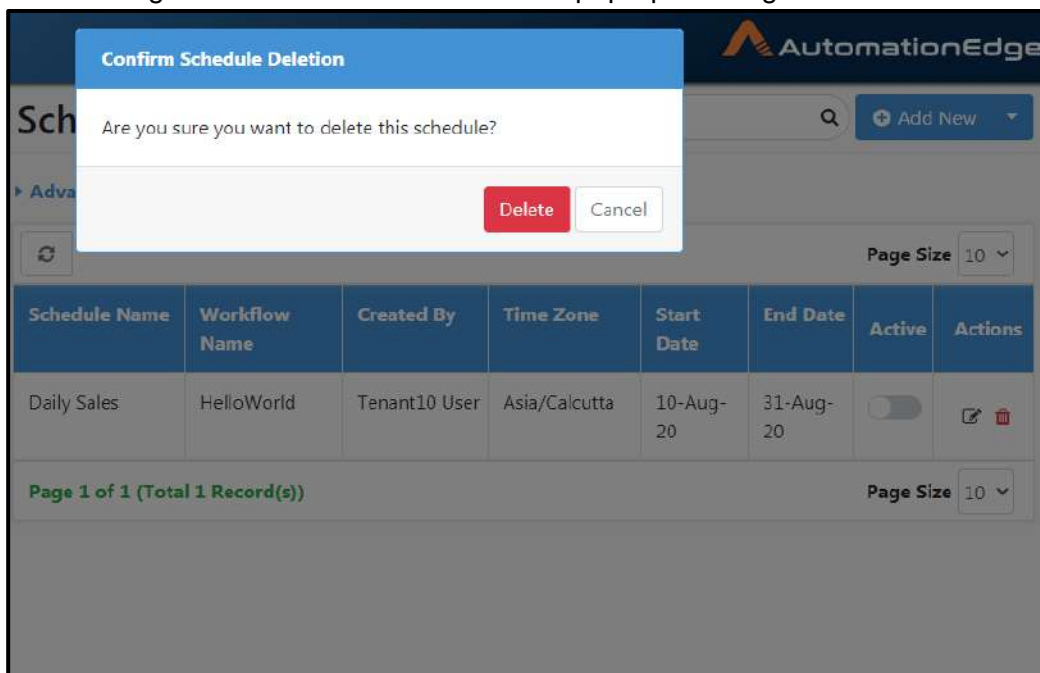


Figure 61a: Delete Schedule

- Schedule Deleted successfully message appears.

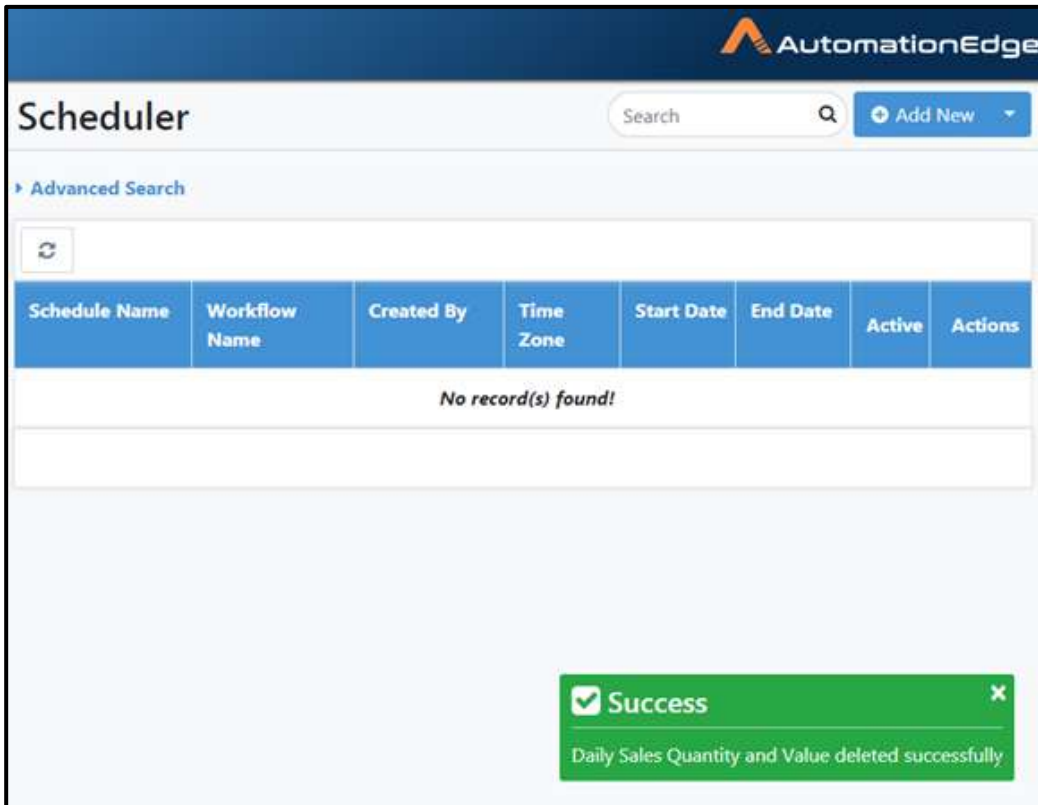


Figure 61b: Schedule deleted successfully

6.12.6 View upcoming fire times

Following are the steps to view upcoming fire times.

- Navigate to WorkflowsàScheduler
- Click on View upcoming fire times icon.

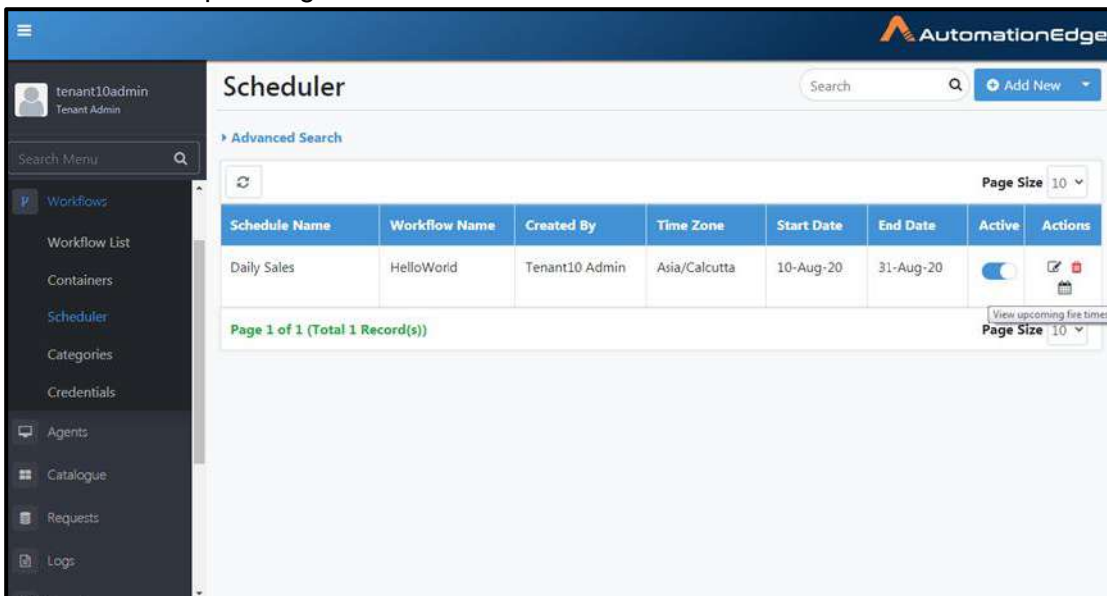


Figure 61c: Upcoming Fire times icon

- The upcoming fire times are displayed as seen below. Click Show More.

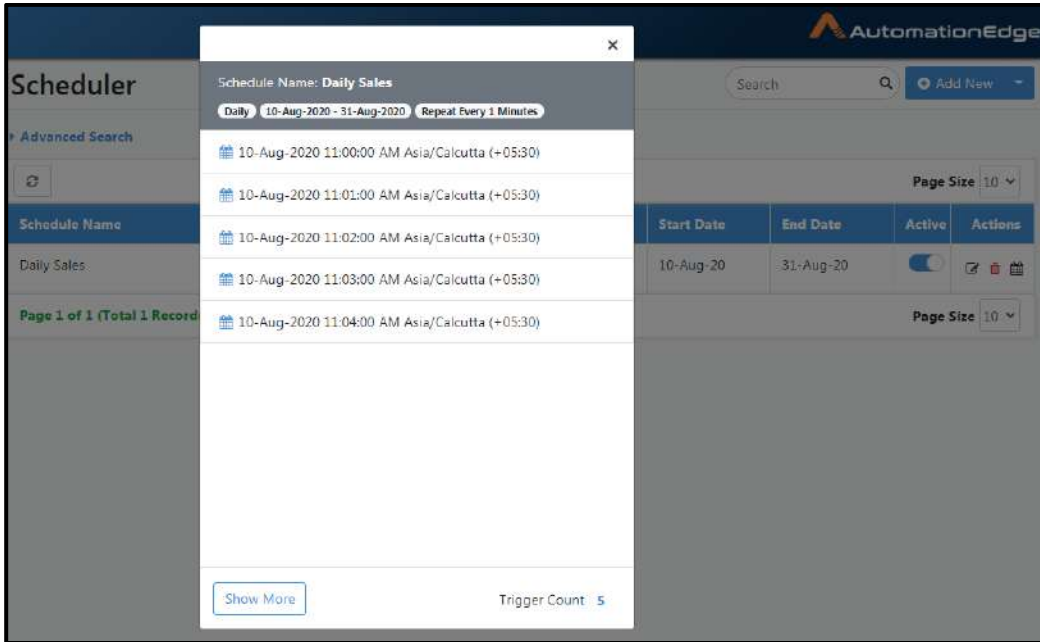


Figure 61d: View Upcoming Fire Times

- On click Show More more fire times are displayed as below.
- You may also click on Trigger Count to change the number of schedules triggered when you click 'View Upcoming fire times' or click Show More button.

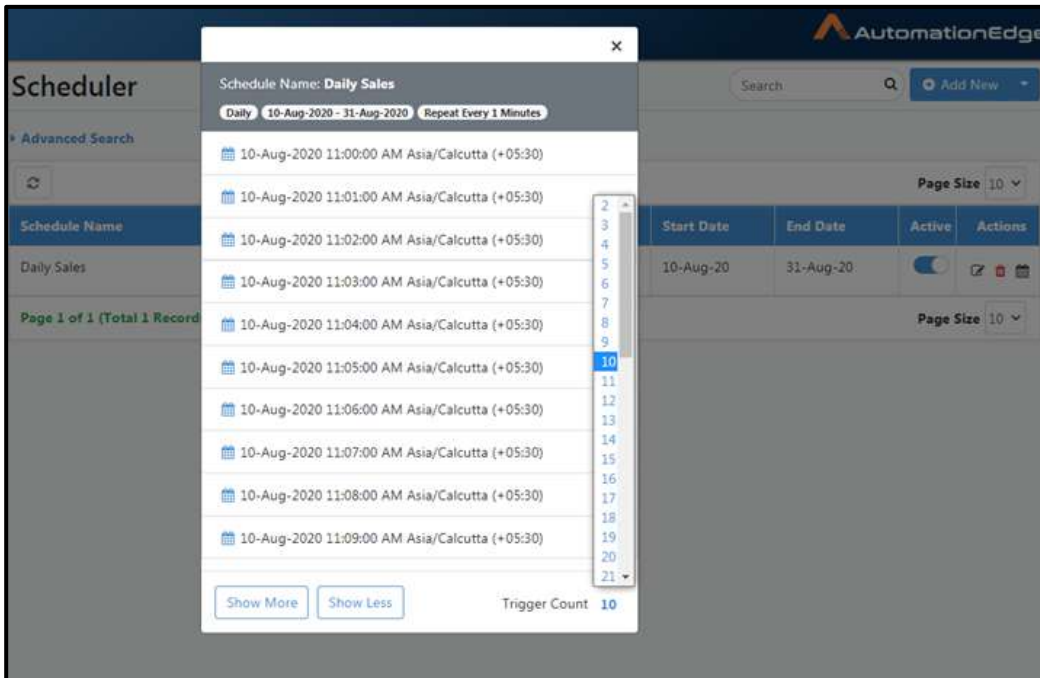


Figure 61e: See or Trigger more schedules on Scheduler list

- This completes the description of View upcoming fire times.

6.13 Scheduler: Transfer Schedules

6.13.1 Introduction

This section describes how to transfer the ownership of schedules.

When a user is to be deleted, it may be assumed that all his/her artefacts including schedules also have to be deleted prior to user deletion. However, there might be cases when those schedules are still valid and schedules need to be retained even if the user who created the schedules is deleted.

6.13.2 Who can transfer ownership of schedules

Only Tenant Administrators have access to Schedule Ownership Transfer.

Transfer ownership of any user's (including itself) schedule to any other user who has WRITE access to the scheduled workflow. Ownership transfer won't be available in case the target user does not have WRITE access to the scheduled workflow.

Table 38: Transfer ownership of schedules Use Cases

User Case	Conditions	UI	API
Schedule Transfer is invoked	Target User has Write access to Scheduled Workflows	Success Message will be displayed	200 Ok will be returned
Schedule Transfer is invoked	Target User does not have Write access to Scheduled Workflows	Not possible through UI	API will return error and no schedules will be transferred.
Schedule Transfer is invoked	Any User other than Tenant Administrator	Not possible through UI	API will throw Access denied error

6.13.3 Steps to transfer ownership of schedules

Following are the steps to transfer ownership of schedules,

1. Navigate to the Workflow menu and Scheduler sub menu.
Click the Drop down Arrow next to Transfer schedule button.

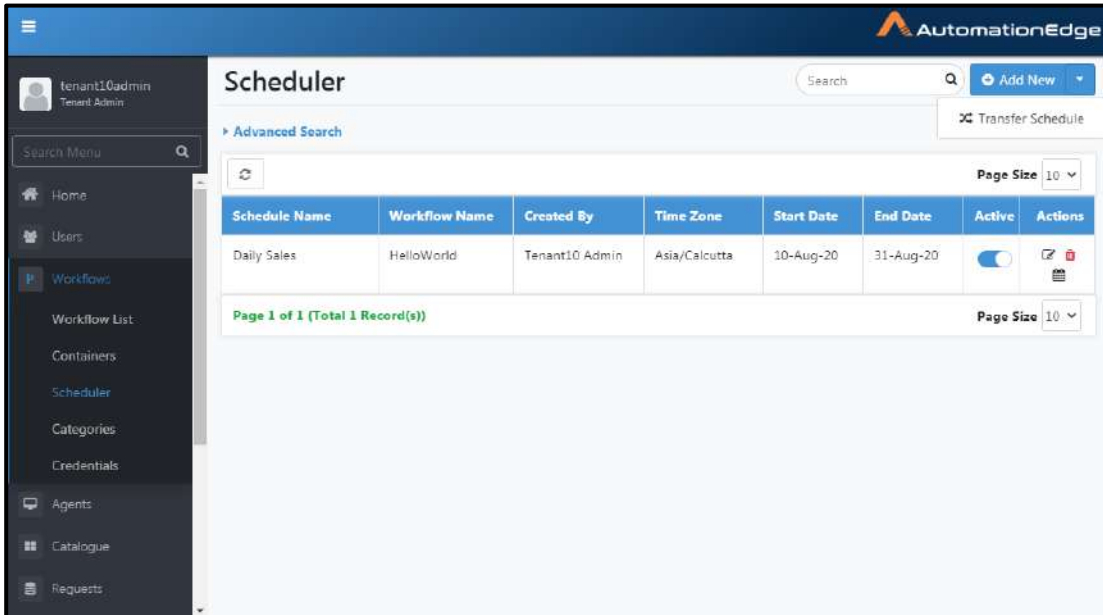


Figure 62a: Transfer Schedule

2. The Transfer Schedule Page appears where user can select owner's schedules for transfer. Select the Owner, whose schedules needs to be transferred.

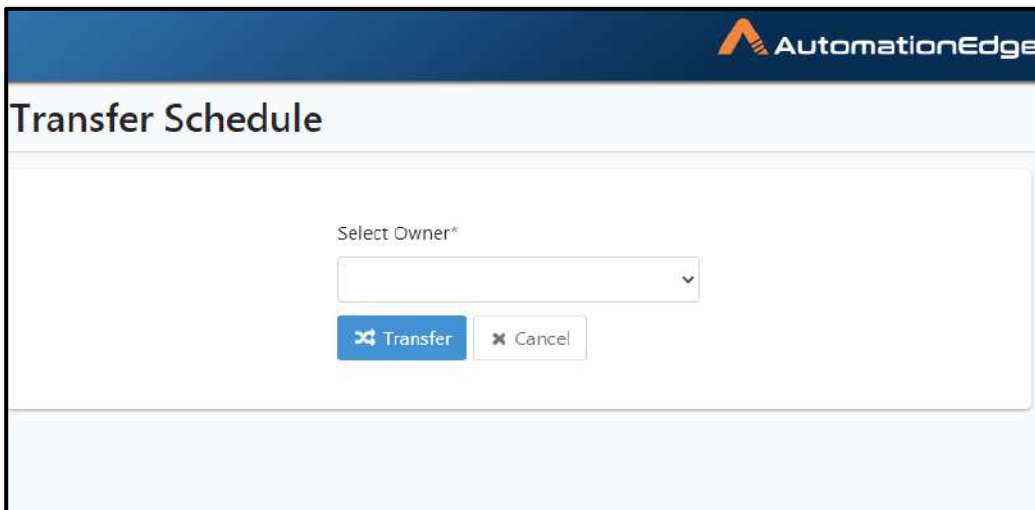
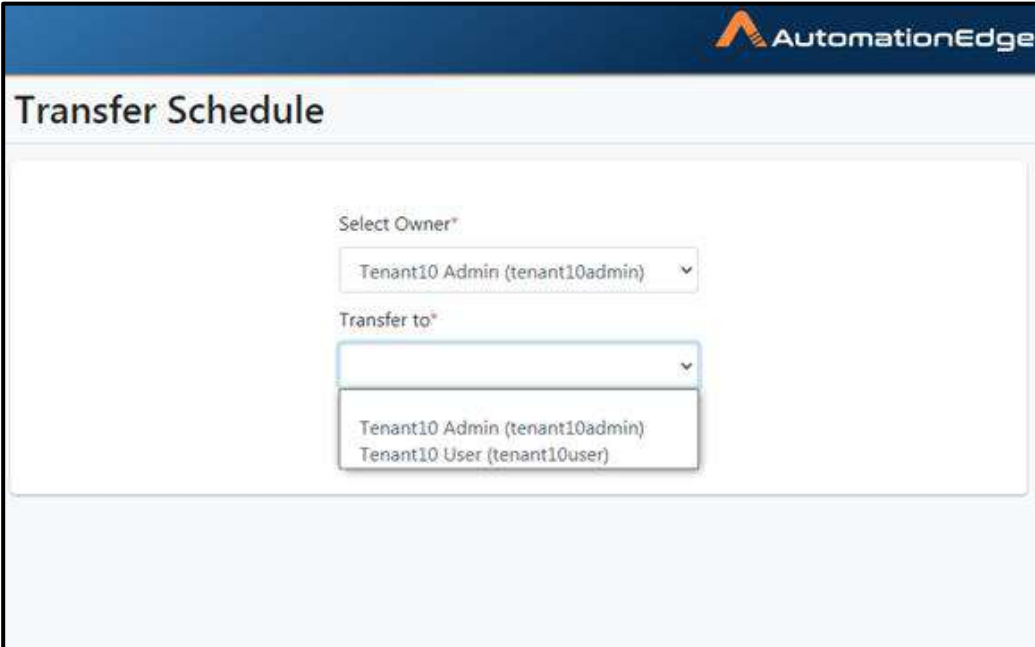


Figure 62b: Select Schedule Owner

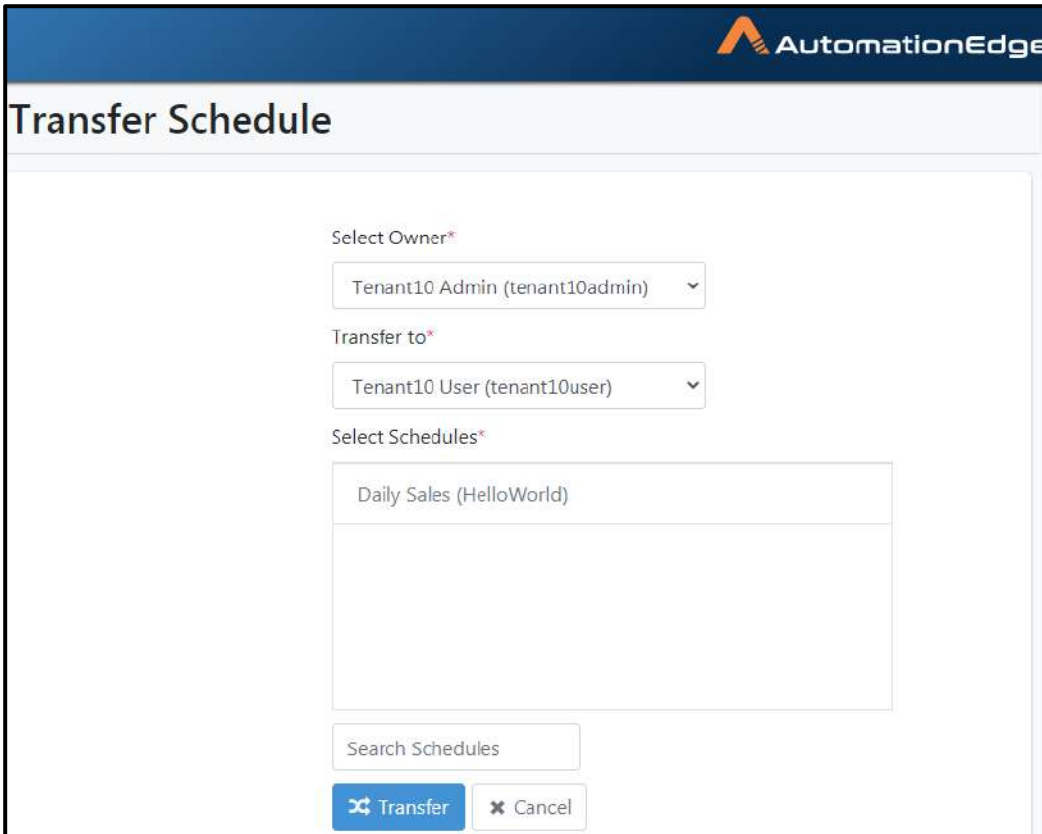
3. Select from Transfer to drop down list the the target user, who will be the new owner of the schedules.



The screenshot displays the 'Transfer Schedule' page in the AutomationEdge application. At the top right, the AutomationEdge logo is visible. The main heading is 'Transfer Schedule'. Below this, there are two dropdown menus. The first is labeled 'Select Owner*' and currently shows 'Tenant10 Admin (tenant10admin)'. The second is labeled 'Transfer to*' and is open, showing a list of options: 'Tenant10 Admin (tenant10admin)' and 'Tenant10 User (tenant10user)'.

Figure 62c: Select Target Owner

4. Select the Schedule to be transferred. Only those schedules can be selected for transfer for which the target user has WRITE access on the underlying workflow. In this case, tenant10user does not have access to the workflow for Daily Sales schedule, so this Schedule is not enabled for transfer.



AutomationEdge

Transfer Schedule

Select Owner*

Tenant10 Admin (tenant10admin) ▾

Transfer to*

Tenant10 User (tenant10user) ▾

Select Schedules*

Daily Sales (HelloWorld)

Search Schedules



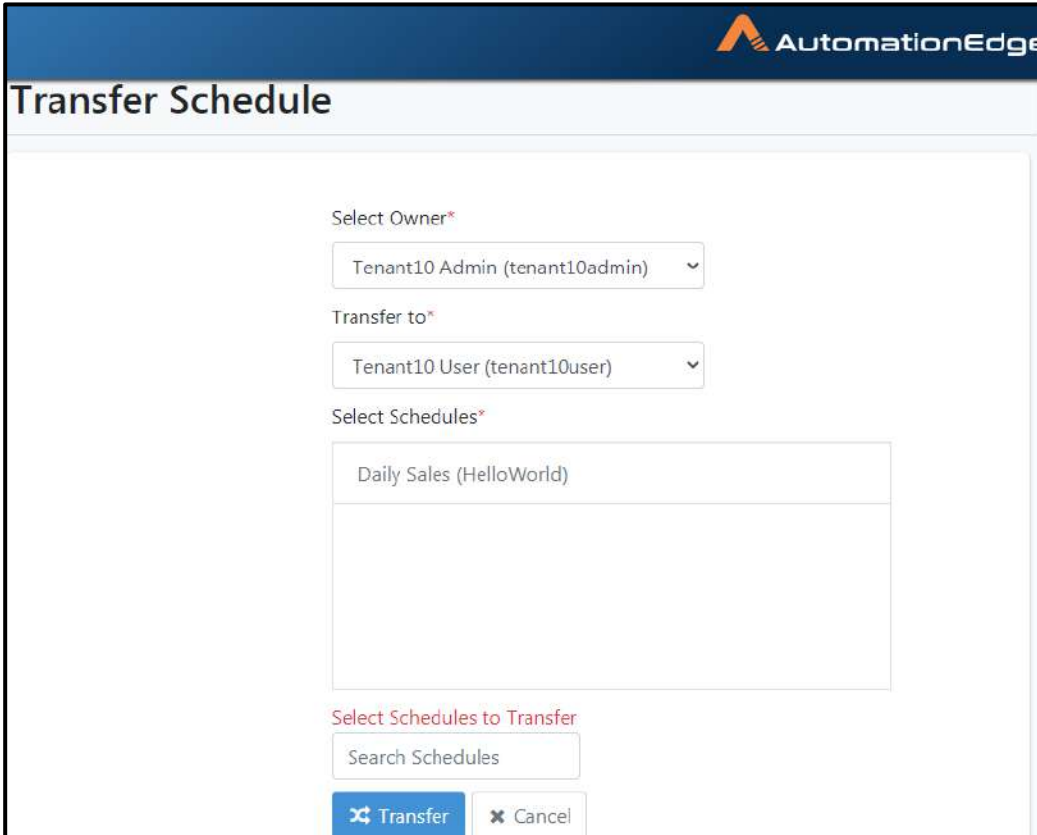
 Transfer  Cancel

Figure 62d: Schedule List

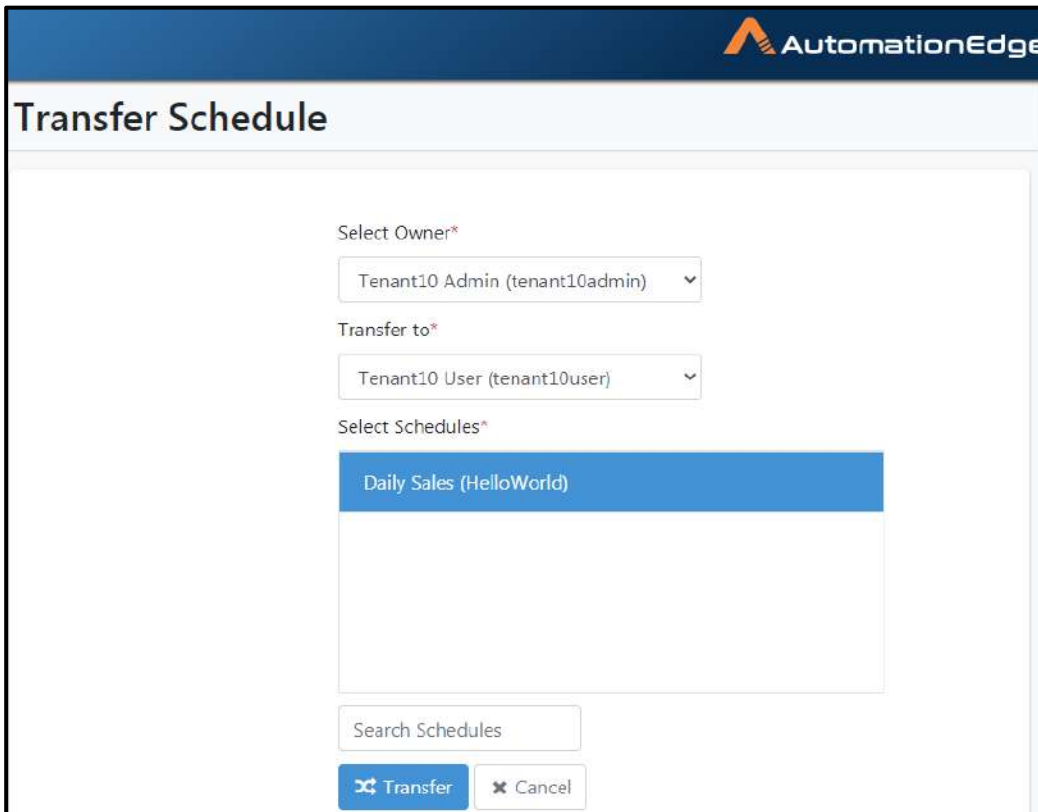
5. If user does not have permissions to the underlying workflow of the Schedule is not highlighted. If you Search Schedules box, you get a message in red still asking you to Select Schedules to Transfer.



The screenshot displays the 'Transfer Schedule' interface. It features three dropdown menus for selection: 'Select Owner*' (Tenant10 Admin (tenant10admin)), 'Transfer to*' (Tenant10 User (tenant10user)), and 'Select Schedules*' (Daily Sales (HelloWorld)). Below these is a red error message 'Select Schedules to Transfer' and a search box labeled 'Search Schedules'. At the bottom are two buttons: 'Transfer' and 'Cancel'.

Figure 62e: Target user does not have permission to underlying Workflow

6. Once the target user has write permissions the underlying workflow of the Schedule the Schedule is active in blue which can now be transferred. Click Transfer.



AutomationEdge

Transfer Schedule

Select Owner*

Tenant10 Admin (tenant10admin) ▾

Transfer to*

Tenant10 User (tenant10user) ▾

Select Schedules*

Daily Sales (HelloWorld)

Search Schedules

Transfer Cancel

Figure 62f: Select Schedule for which Target Owner has permissions

- On successful Transfer of the Schedules following message will be displayed.

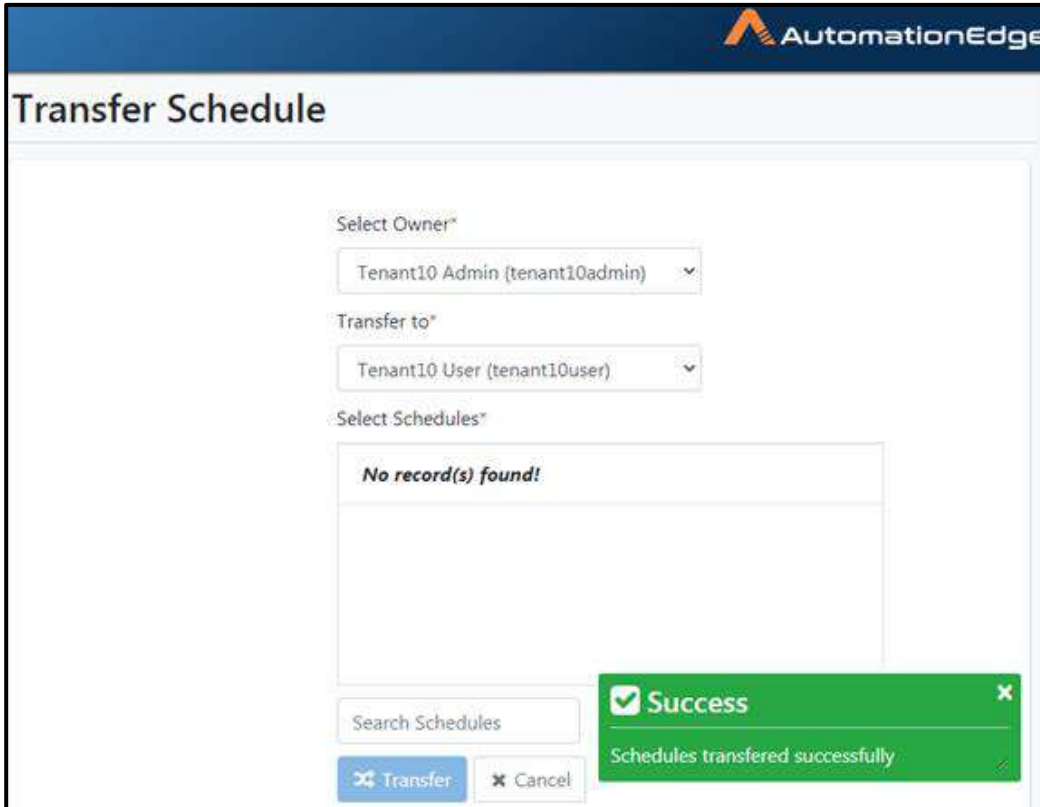


Figure 62g: Schedule Transferred Successfully

6.14 Scheduler: Features/Permissions for other users

Table 39: Scheduler Features

Feature/Role	Tenant Administrator	Workflow Administrator	User Administrator	Tenant User*	Activity Monitor
Scheduler: Add/Activate/Edit/Delete	✓	✓	-	✓	-

*Tenant users can use the AutomationEdge features depending on Read, Write or Execute permissions granted to them on workflows.

7 Agents

An Agent is a piece of software that works on behalf of AutomationEdge Engine, and executes workflows or acts as an Agent Controller. Agents provide scalability to AutomationEdge as Agents can be deployed on multiple machines and harness the processing power of multiple machines. However, each physical/virtual can have one Agent. In case of Windows Server OS, each user can have one Agent.

There are three categories of Agents:

Table 40: Categories of Agents

1. Agents
<p>Agents are further classified into three types as follows.</p> <ul style="list-style-type: none"> i. Standard Agents ii. Advanced Agents iii. Turbo Agents
2. Controller Agents
3. Assisted Agents

Agents and Assisted Agents are accessible on the Agents menu by default. Controller Agent is accessible only if one or more Controller Agents have been setup.

All the Agent categories and Agent types are described in the sections below.

7.1 Tab: Agents

On this Tab you can see three types of Agents:

7.1.1 Types of Agents

7.1.1.1 Standard Agents

A Standard Agent can execute one workflow at a time. It could be a sequential or a non-sequential workflow.

7.1.1.2 Advanced Agents

An Advanced Agent can execute two workflows concurrently. One can be a sequential workflow and the other a non-sequential workflow.

7.1.1.3 Turbo Agents

A Turbo Agent can execute four workflows concurrently. Out of the four one thread is reserved for sequential workflows and non-sequential workflows can utilize the remaining.

7.1.2 Maintain Agents

These following sections are applicable for Standard, Advanced and Turbo Agents.

7.1.2.1 View Agents

Under Agents menu go to Agents sub-menu. There are two buttons: 'Agents' and 'Assisted Agents' present. 'Agents' button is selected by default. A third 'Controller' button is only enabled if Controller is setup for the current Tenant, click this button to see and manage Controller Agents.

Use this page for Agent monitoring. It is also used to view and edit Agent details as seen in the snapshot below and described in the table below.

In this snapshot we can see one Agent in Stopped Status and one in Running status.

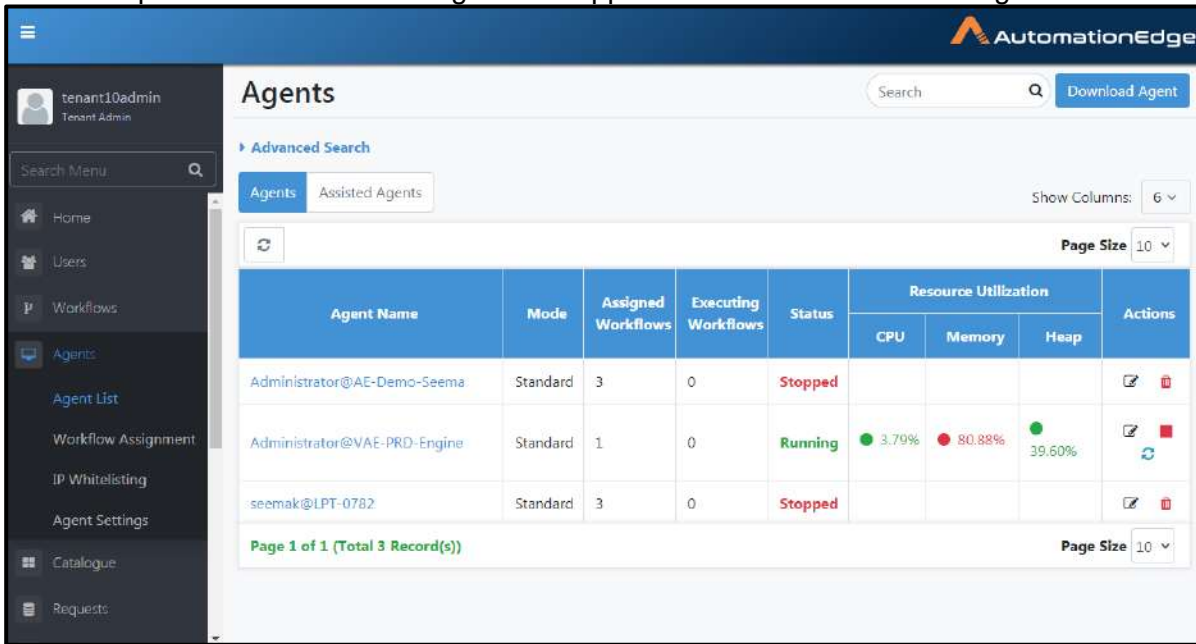


Figure 63a: View Agents

The Fields are explained in the table below.

Table 41: Agent Details Table

Field Name	Description
Agent Name	<p>Displays the name of the Agent.</p> <p>Hover over Agent Name to see the Agent details as highlighted in red below, including Agent Name, IP, hostname, Mac Address and JRE details - JRE version and whether agent is using bundled JRE.</p>
Mode	<p>Displays the Agent Type. Possible values are Standard, Advanced or Turbo.</p>

Field Name	Description
Assigned Workflows	Displays the number of Workflows assigned to the Agent. Assisted Workflows are not part of this number as Assisted Workflows cannot be assigned to Agents.
Executing Workflows	Displays the number of Requests in execution.
Status	<p>Displays the status of the Agent: Running, Unknown, Updating or Stopped.</p> <p>Unknown status is shown when server is not sure about the status of the agent due to factors such as, abrupt shutdown or network failure.</p> <p>The cases when an agent goes to UPDATING state are,</p> <ul style="list-style-type: none"> • When agent is actually upgrading itself from older version to a newer version. If an Agent needs to update and there are workflows already executing on Agent, then the Agent status changes to Updating, remains in state and waits for the workflow execution to complete. Once execution is completed the Agent updates. You can hover the Updating status to see the details such as workflow execution in progress. • When workflow assignments are changed • When plugin assignments are changed • When Workflows/plugins are updated • When agent mode is changed
Resource Utilization:	The following Resource Utilization parameters are captured and displayed on AutomationEdge UI: CPU, Memory, Disk Space and JVM Parameter (Heap size).
CPU	Displays CPU usage in percentage
Memory	Displays memory usage in percentage
Heap	Displays Heap usage in percentage
Actions:	
Edit (✎)	<p>Click pencil icon to edit the Agent Name, Domain name, IP address and windows password.</p> <p>Select Agent Mode such as Standard, Advanced or Turbo.</p> <p>Note: You may change Agent Mode depending on availability in license subscribed. However, Agent Mode cannot be changed when an Agent is in Unknown state.</p> <p>Optionally provide a configurable Remote Desktop Connection, Remote Port for connecting to agent VMs from Controller Agent machine.</p>

Field Name	Description
	<div data-bbox="532 226 1105 1031"> </div> <p data-bbox="532 1079 1317 1178">Expand restart Settings. By default the 'Use Tenant Level Settings' is selected for Agent Restart set in the menu option Agents->Agent Settings->Agent Restart Time.</p> <div data-bbox="532 1184 1105 1381"> </div> <p data-bbox="532 1434 1256 1499">Else, you may uncheck 'Use Tenant Level Settings' and 'Enable Agent Restart' checkbox is displayed.</p> <div data-bbox="532 1505 1105 1751"> </div> <p data-bbox="532 1797 1279 1864">Enable 'Enable Agent Restart' checkbox to see the Agent Restart Time option. Provide desired restart time.</p>

Field Name	Description
	<div data-bbox="537 226 1110 569" style="border: 1px solid black; padding: 5px;"> <p>▼ Restart Settings</p> <p><input type="checkbox"/> Use Tenant Level Settings</p> <p><input checked="" type="checkbox"/> Enable Agent Restart</p> <p>Agent Restart Time:*</p> <p>HH : MM</p> <p style="text-align: right;"><input type="button" value="Save"/> <input type="button" value="Cancel"/></p> </div> <p>Note: Agent restart features in not supported on Linux based OS</p>
Stop (■)	Stop icon is visible if the s agent status is running or unknown. Agent is gracefully stopped from running status. However, if agent is stopped from unknown status server simply marks it as stopped.
Delete (🗑)	When an agent is in stopped state delete icon is visible instead of stop icon. An agent can be deleted only when in 'Stopped' status. Deletion of Agent removes the agent's record from server's database. Once deleted agent cannot be started.
Restart(↻)	Agents can be manually restarted with this option. Note: Agent restart features in not supported on Linux based OS
Start(▶)	If an Agent is down, a Start option is visible. By default, the Start icon is disabled; assign Agent to one or one controllers to enable it. For details, please refer to the section: Agents: Controller Assignment. The Start option starts the Agent on the Controller Agent machine. The icon colour is grey when it is disabled and green when enabled.

7.1.2.2 Agent Monitoring

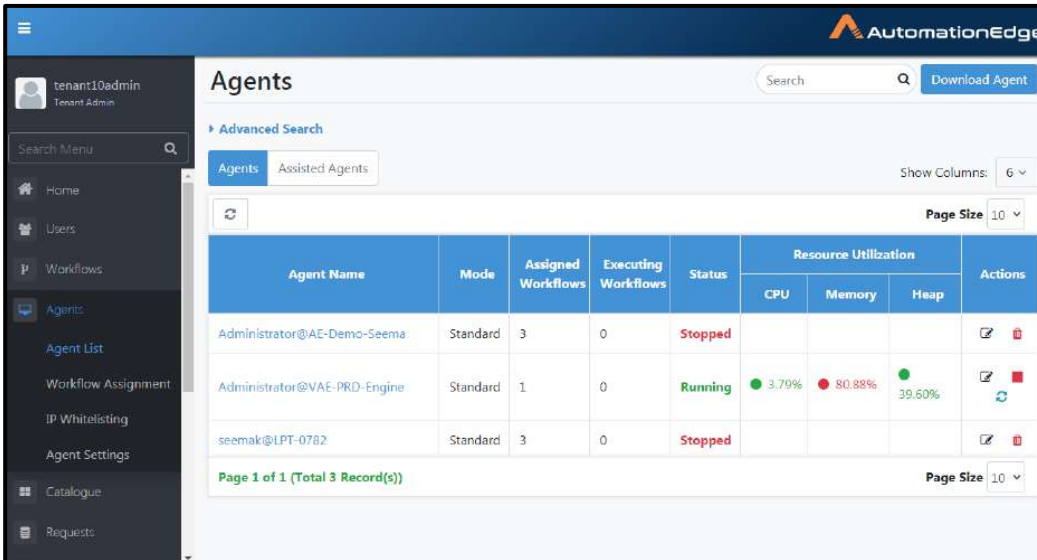
Agent Monitoring page displays Resource Utilization by the Agents graphically.

Following are the features of Agent Monitoring.

- Agent captures Resource Utilization information periodically (every minute), and sends to server every five minutes. It is retained for thirty days.
- The following Resource Utilization parameters are captured and displayed on AutomationEdge UI: CPU, Memory, Disk Space and JVM Parameter (Heap size).
- Resource Utilization is depicted as pie charts and line charts.
- The page has radio button options to display Agent Monitoring for different time period intervals.

Following are the steps to display Agent Monitoring page.

1. Navigate to the Agent menu. Click on an Agent Name link to navigate to the Agent Monitoring page for that Agent.



The screenshot shows the 'Agents' page in the AutomationEdge interface. The page includes a search bar, a 'Download Agent' button, and a table of agents. The table has columns for Agent Name, Mode, Assigned Workflows, Executing Workflows, Status, Resource Utilization (CPU, Memory, Heap), and Actions. The 'Agent Name' column is highlighted, indicating it is clickable.

Agent Name	Mode	Assigned Workflows	Executing Workflows	Status	Resource Utilization			Actions
					CPU	Memory	Heap	
Administrator@AE-Demo-Seema	Standard	3	0	Stopped				
Administrator@VAE-PRD-Engine	Standard	1	0	Running	3.79%	80.88%	39.60%	
seemak@LPT-0782	Standard	3	0	Stopped				

Figure 63b: Agent Name is clickable

2. The Agent Monitoring dashboard for Agent Name Administrator@VAE-PRD-Engine is seen below.
3. This dashboard below displays Agent Monitoring for a time period of 7 days by choosing the '7 Days' radio button.

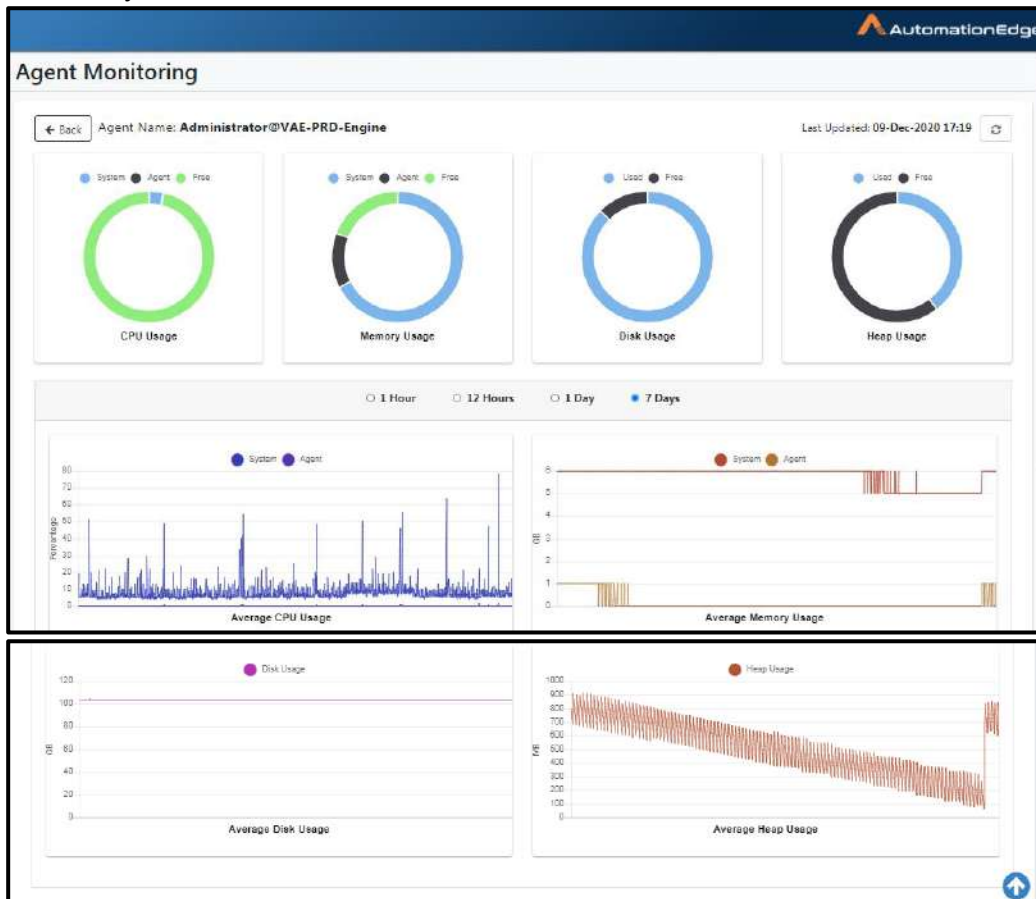


Figure 63c: Agent Monitoring

7.1.3 Agent: Download and Startup

An Agent can be downloaded from AE server and installed on available computers (either Windows or Linux OS). The agent connects to the server (using the same URL specified in URL setting under System Administrator) and is assigned workflows for running.

To download an agent:

1. Navigate to the Agents menu.
2. Click the Download Agent button on the top right corner.
(Note: Agent can be downloaded only if the 'Server URL' setting has been done by the System Administrator.)
3. A pop-up 'Do you need proxy for this agent?' appears.

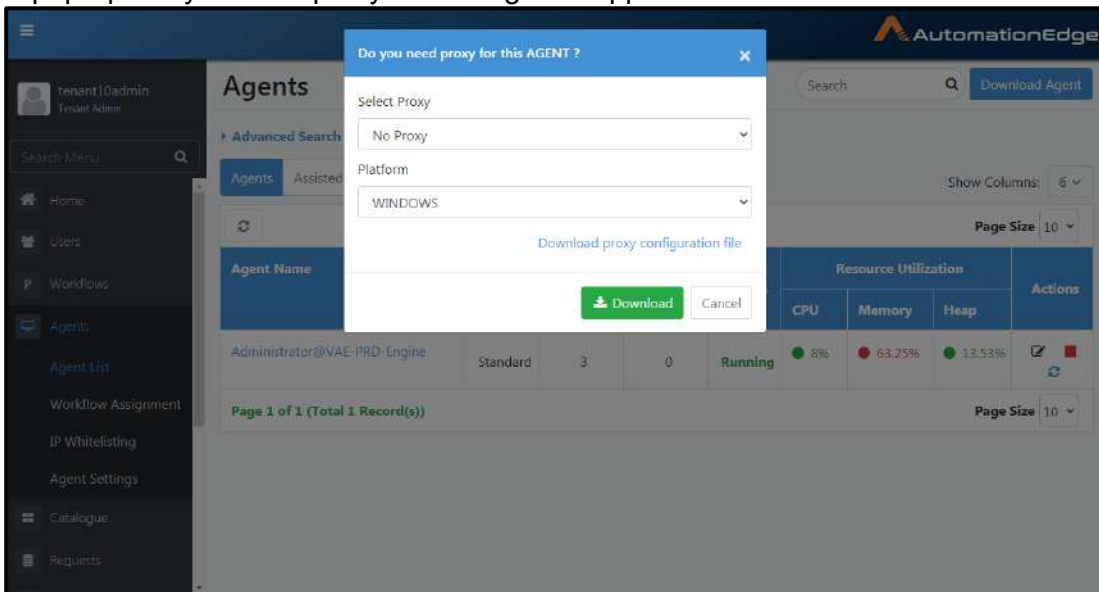


Figure 64a: Downloading Agent

4. Select Proxy and Authentication Type fields from the corresponding drop down lists. The list values are explained in the table below.

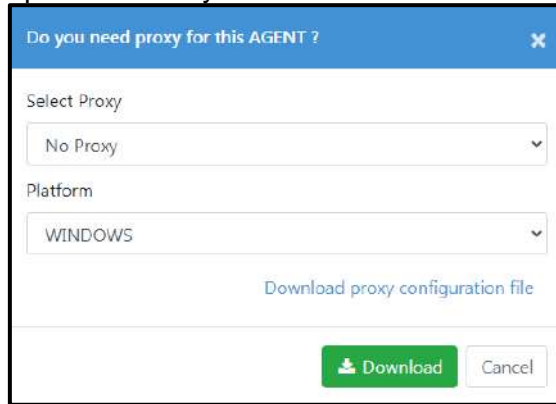
Table 42: Agent level Proxy configuration options

Field Name	Description
Select Proxy	<p>During Agent download you have the options to use Automatic Configuration or set Static Proxy by providing Proxy protocol (http/https), host, port or set Dynamic Proxy (base on PAC file from URL).</p> <p>If Proxy is already set at Tenant level it is automatically detected during Agent Download. You may overwrite it. The proxy set at Agent level will take precedence over that set at Tenant level.</p> <p>The following are the options in the drop down list for Select Proxy. You may overwrite Proxy set at</p>

Tenant level or set proxy afresh during Agent Download from the drop down list.

1. No Proxy

In case proxy is set at the system level and you do not want to use that, you may select the option No Proxy.



Do you need proxy for this AGENT ?

Select Proxy

No Proxy

Platform

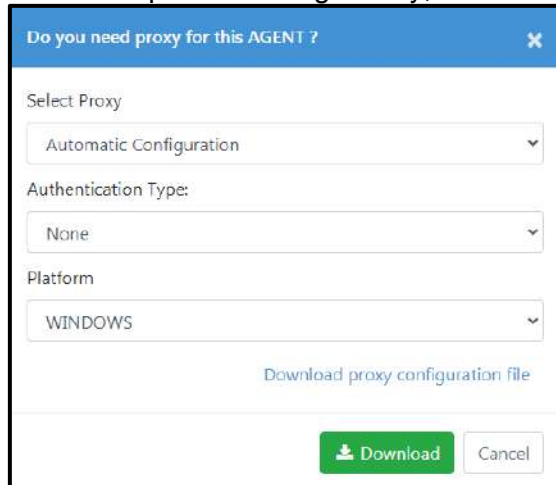
WINDOWS

Download proxy configuration file

Download Cancel

2. Automatic Configuration

Select Automatic Configuration if you wish to auto detect the proxy configuration from “Internet Options” settings if any, and use it.



Do you need proxy for this AGENT ?

Select Proxy

Automatic Configuration

Authentication Type:

None

Platform

WINDOWS

Download proxy configuration file

Download Cancel

3. Proxy Server

Select Proxy server to set a Static Proxy. You can now provide static Proxy details, Protocol (http, https), Host (e.g. 10.51.5.30) and Port (e.g. 3128).

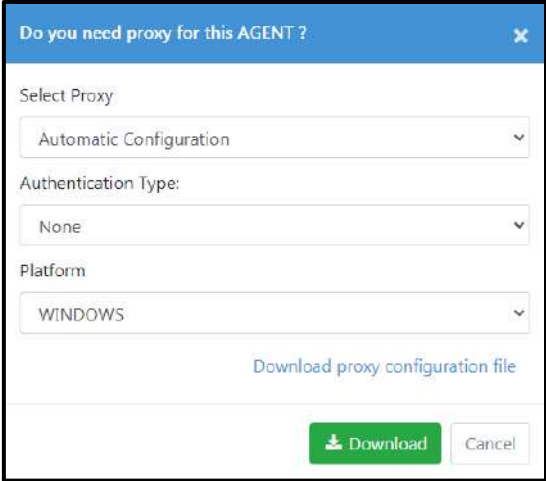
If you have set a static proxy at Tenant level Proxy details popup window appears with static proxy details pre-configured.

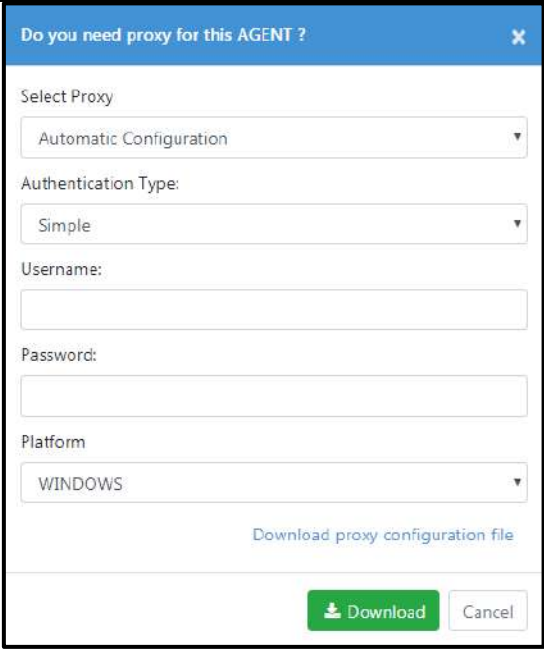
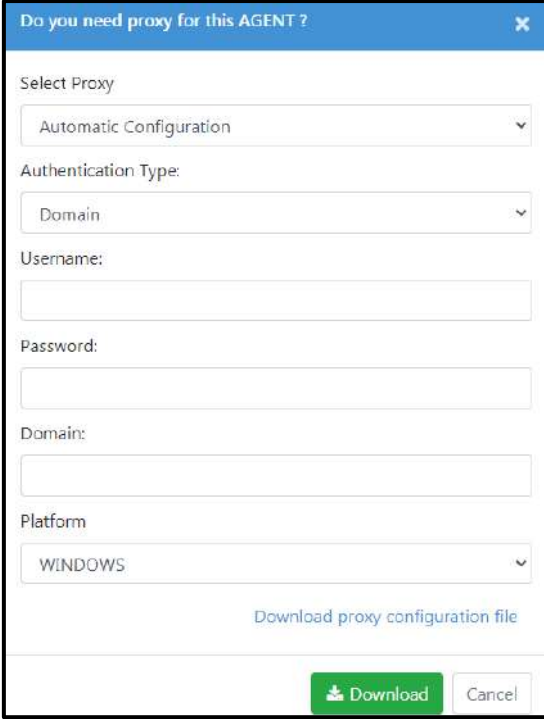
4. PAC

Choose this option to set a Dynamic Proxy and provide the PAC file URL (e.g. <https://10.51.5.30/proxy.pac>) to set the Dynamic Proxy.

If you have set a dynamic proxy at Tenant level the Proxy details popup window appears with dynamic proxy details PAC file from URL pre-configured.

5. For Automatic Configuration as well as both Static Proxy and Dynamic (PAC file URL), Proxy details are stamped into a file proxy-

	<p>config.properties and is packaged into agent zip on click of Download button.</p>
<p>Authentication Type</p>	<p>For Automatic Configuration, Proxy Server and PAC Proxy options the following three Authentication Types are available.</p> <ul style="list-style-type: none"> • None • Simple or • Domain <p>1. None Leave Authentication type to none when Proxy settings do not need authentication.</p>  <p>2. Simple In case Proxy settings in “Internet Options” needs authentication, select Authentication type- Simple from the dropdown list and provide a username and password. For Simple Authentication Type you need to provide Username (e.g. scott.tiger etc.) and password as shown below.</p>

	 <p>3. Domain If Authentication type is domain, you need to provide Domain (e.g.xxx.com) in addition to username and password.</p> 
Platform	The two platforms allowed in the drop down list are WINDOWS or LINUX
Download proxy configuration file	Once proxy is configured in the Agent Download UI these values will be stamped into a file proxy-

	<p>config.properties. You may download the file by clicking Download proxy configuration file link. Else if you click Download button, proxy-config.properties file will be packaged into agent zip and will be placed under <AGENT-HOME>/conf directory.</p> <p>This file may be downloaded and used for manually copying to Agent machine when there are changes in proxy details.</p> <p>In case a Server is upgraded and new Proxy details are configured there are two scenarios. If the agent is running Proxy details will not be updated and proxy-config.properties file needs to be manually copied but if the Agent is stopped then the new proxy details are updated in the Agent</p>
<p>Note: Agents Upgrades</p>	<p>During upgrades Agents acquires Tenant level Proxy settings if any. Following are the corrective actions for the two scenarios,</p> <ul style="list-style-type: none"> Agents may be without any Proxy Settings but during upgrade, Agent gets Tenant level proxy settings. User needs to delete the proxy configuration file from the Agent file system. <p>Agent may be using custom Proxy Settings(different from Tenant level settings) however, in case of upgrade, Agent gets Tenant level Proxy Settings, User's need to download custom proxy settings again and copy to the Agent file system.</p>

5. Provide Proxy Server details if required as explained in the table above and click Download.
6. Allow pop-ups for this site if required.
7. The following screen shows the Pop-up blocker that may appear in Chrome browser. Click the first radio button to allow pop-ups.

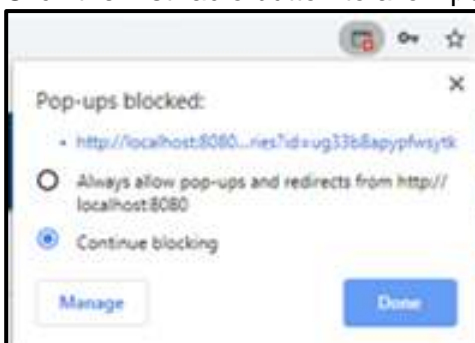


Figure 64b: Pop-up blocker in Chrome

- The following screen shows the Pop-up blocker that may appear in firefox browser. Click the first option to Allow pop-ups.



Figure 64c: Pop-up blocker in firefox

- Agent download in progress is seen below.

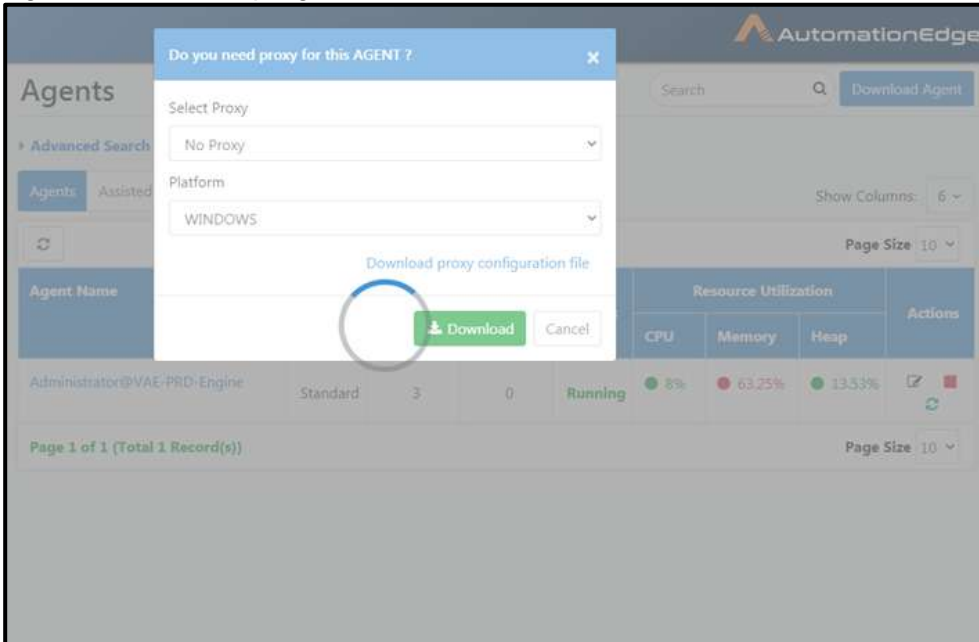


Figure 64d: Agent Downloading

- The Agent zip is downloaded as seen below.

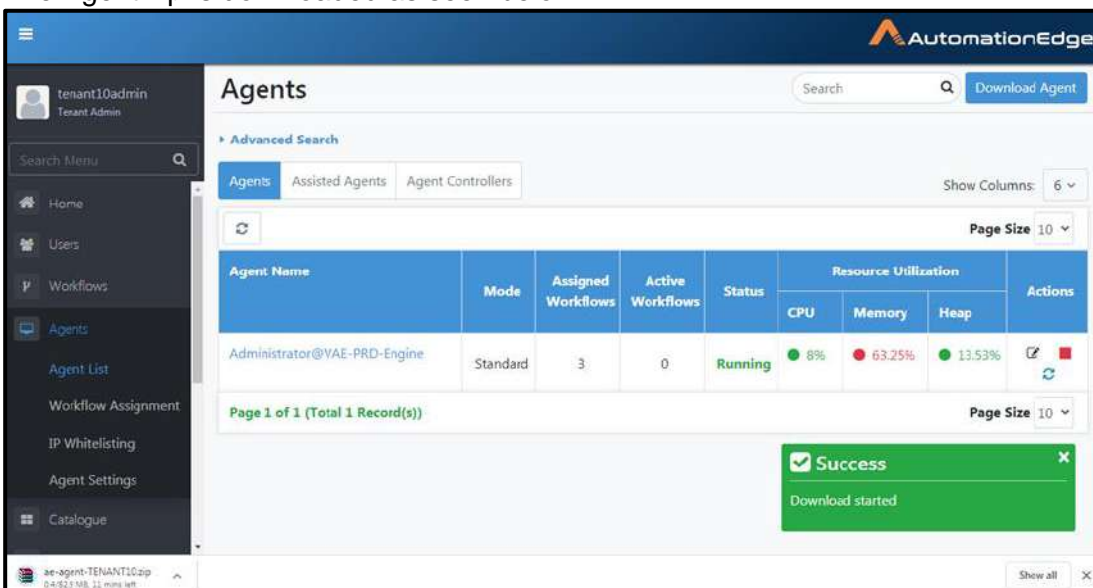


Figure 64e: Agent Downloaded

11. Unzip the downloaded file and extract an agent.
12. The downloaded zip file can be copied to one or more machines where we need to run the agent.
13. The agent's zip should be unzipped on the machine where it should run.
14. It creates ae-agent directory and unzips there.
15. Run ae-agent/bin/startup.bat or ae-agent/bin/startup.sh file (for Windows and Linux respectively) from command prompt as shown below. Agent will register itself with the server and will be available for assigning workflows as described in the next section.

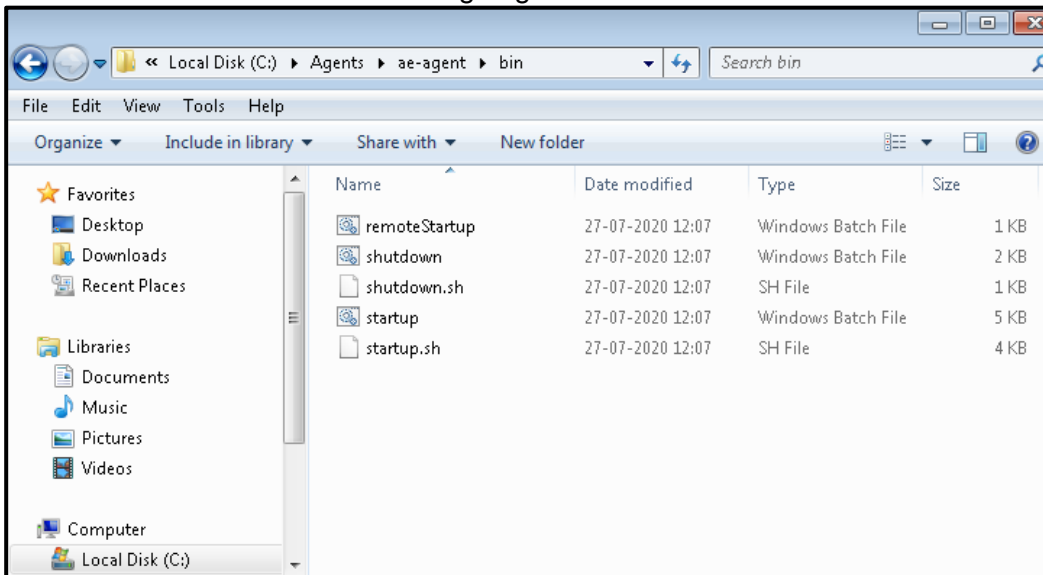


Figure 64f: Agent bin directory

16. Type cmd in the Windows explorer address bar and press keyboard enter.

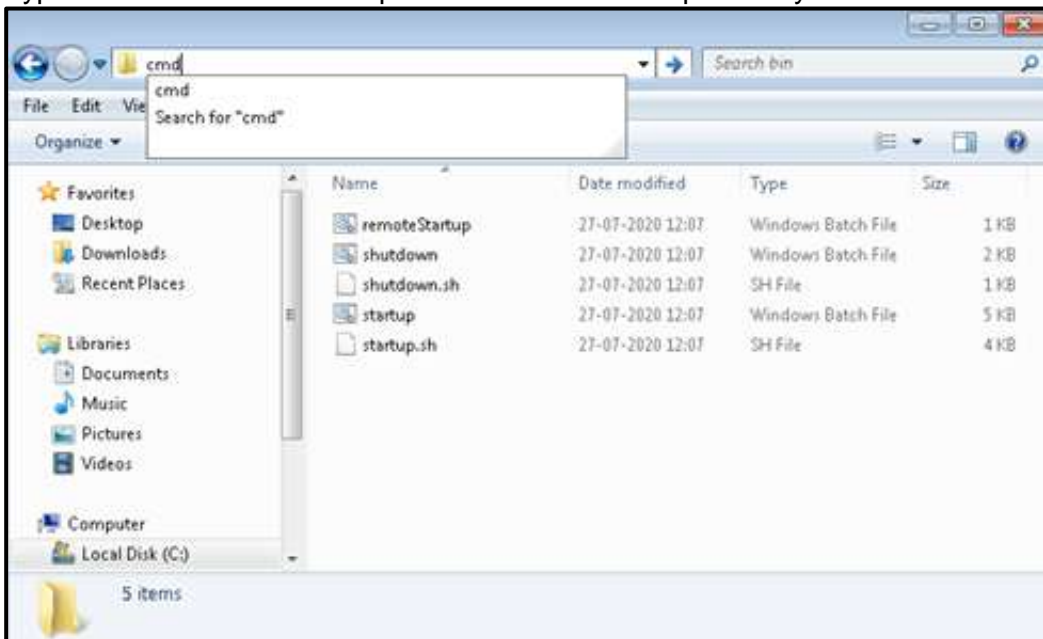
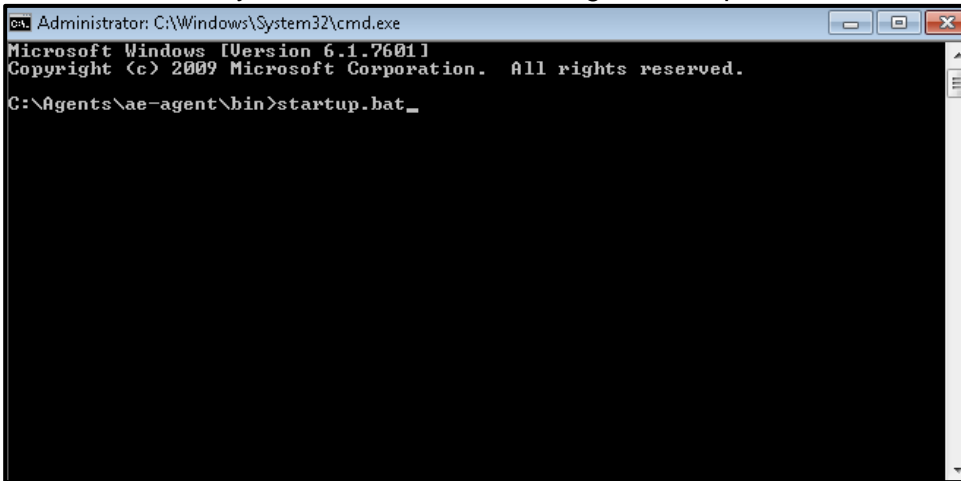


Figure 64g: Open command line at this location

17. Type startup.bat. Press Keyboard Enter. Starting Agent from command prompt is the recommended way rather than double clicking on startup.bat.



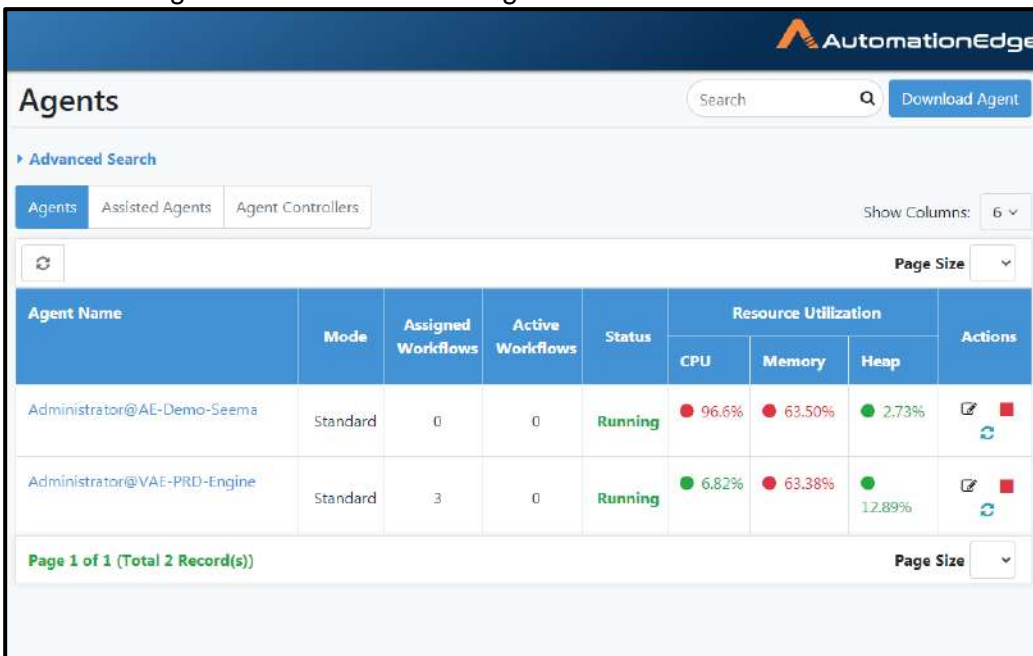
```

Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Agents\ae-agent\bin>startup.bat_
  
```

Figure 64h: Type startup.bat

18. Once Start-up is complete view Agents in UI. You can see the Agent status as Running for the first Agent in the list that was registered.







Agent Name	Mode	Assigned Workflows	Active Workflows	Status	Resource Utilization			Actions
					CPU	Memory	Heap	
Administrator@AE-Demo-Seema	Standard	0	0	Running	96.6%	63.50%	2.73%	 
Administrator@VAE-PRD-Engine	Standard	3	0	Running	6.82%	63.38%	12.89%	 

Figure 64i: View Agent Status

19. By default, and Agent is registered as type Standard Agent. Once registered Agent mode can be edited as type Advanced or Turbo; provided the license is provisioned for these types.
20. To stop an Agent Run ae-agent/bin/shutdown.bat or ae-agent/bin/shutdown.sh file (for Windows and Linux respectively) preferably from command prompt.

7.2 Agents: Memory Settings

7.2.1 Additional JVM Params in Agent Startup

Following are the java Memory settings for Agents in startup.bat by default.

Heap Settings	-Xms1024m -Xmx2048m
MaxMetaspace Setting	-XX:MaxMetaspaceSize=128m
Memory per thread	-Xss=1MB

In case workflows require more or less memory these settings may be changed in startup.bat or startup.sh. Once the Agent is restarted with the new Memory settings that suffice workflow requirements, the workflow should complete successfully.



Following is a rough formula for Total Memory calculations:

Note: Total Max memory = [-Xmx] + [-XX:MaxMetaspaceSize] + number of threads * [-Xss]

7.3 Agents vs. Assisted Agents

Agents can be downloaded and run by a Tenant Administrator or Agent Administrator. Agents can run any Workflows assigned to them. In case a workflow is assigned to multiple Agents, AutomationEdge randomly assigns the workflows to Agents for execution. Hence, it cannot be predicted on which Agent and hence which machine/VM the workflow runs. Many a times, Agents run on VMs that are not actively attended. Typically, the Workflows run without any manual intervention so it does not matter on which Agent/machine the workflow runs and hence Agents suffice the need.

For Workflows that need manual intervention such as 'captcha/OTP/Enter some run-time values' Workflows should run on the machine whose user can fulfill the intervention request. For this to happen, an Agent should also run on the said user machine, and the workflows should be assigned to that one Agent only that runs on that user machine.

Assisted Agents fulfill this requirement. Assisted Agents provide built-in support for running Workflows on user specific Agents. Assisted Agents are owned by users and run Assisted Workflows for which the owner has requisite (Read/Write/Execute) permissions. An Assisted Agent can run all Assisted Workflows for which the owner of the Assisted Agent has permission.

7.4 Tab: Assisted Agents

Tenant User, Workflow Administrator and Tenant Administrator will be able to download 'Assisted Agent' from AutomationEdge server. This Agent will be similar to the usual Agent except for the following:

- An Assisted Agent is owned by the User who downloads it.
- Only assisted workflows can be executed by Assisted agents.
- Any user can register only up to one Assisted Agent with the server.
- Assisted Agent can run only sequential Workflows.
- Assisted Agents will be configured to run between 6 and 23 hours of the day. This configuration is part of the provided license.
- In order to run an assisted Workflow, it is not required to assign such Workflow to any Agent as and they are assigned automatically by the server. User just needs to get execute permissions on the Workflow.
- Along with other Workflows, assisted Workflows will also appear on User's catalogue page, if User has execution permissions on them and User has at least one assisted Agent registered.
- Assisted Workflow can be run only if User's Agent is in running state otherwise the User will get an appropriate error message.
- Assisted Workflows cannot be run as a schedule.

7.4.1 Maintain Assisted Agents

7.4.1.1 Assisted Agents: View

Under Agents menu go to Agents sub-menu.

For Tenant Administrator and Agent Administrator, there will be three buttons on Agents menu page for Agent Monitoring. There are two buttons: 'Agents' and 'Assisted Agents' present. A third 'Controller' button is only enabled if a Controller is setup for the current Tenant, click this button to see and manage Controller Agents.

Select 'Assisted Agents' button. This page is for Assisted Agent monitoring. It is also used to view Assisted Agent details as seen in the figure and described in the table below.

The screenshot shows the 'Assisted Agents' page in the AutomationEdge interface. The page title is 'Assisted Agents' and it includes a search bar and a 'Download Assisted Agent' button. Below the title, there are tabs for 'Agents', 'Assisted Agents', and 'Agent Controllers', with 'Assisted Agents' selected. A table displays the following data:

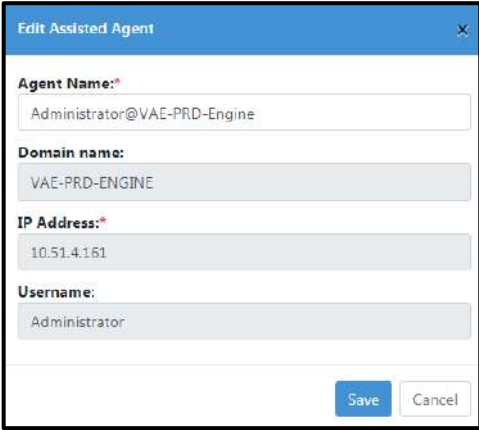
Agent Name	Username	Active Workflows	Status	Resource Utilization			Actions
				CPU	Memory	Heap	
Administrator@AE-Demo-Seema	tenant1Dadmin	0	Running				

Below the table, it indicates 'Page 1 of 0 (Total 0 Record(s))'. The page also features a sidebar with navigation options like Home, Users, Workflows, Agents, Agent List, Workflow Assignment, IP Whitelisting, Agent Settings, Catalogue, and Requests.

Figure 67a: Assisted Agent Monitoring

Agents View fields are explained in the table below.

Table 44: Agent Details Table

Field Name	Description
Agent Name	Displays the name of the Assisted Agent
Username	The Username of the owner of the Assisted Agent. Assisted Workflows are not explicitly assigned to Agents. All the Assisted Workflows for which user has permission can be run by assisted Agents.
Active Workflow	Displays the number of Requests in execution.
Status	Displays the status of the Assisted Agent: Running, Unknown, Updating or Stopped. Unknown status is shown when server is not sure about the status of the agent due to factors such as abrupt shutdown or network failure.
Actions:	
Edit (✎)	<p>Click pencil icon to edit the Assisted Agent Name. You may edit Agent Name.</p> 
Stop (■)	Stop icon is visible if the Assisted Agent status is running or unknown. Assisted Agent is gracefully stopped from running status. However, if agent is stopped from unknown status server simply marks it as stopped.
Delete (🗑)	<p>When an Assisted Agent is in stopped state delete icon is visible instead of stop icon. An Assisted Agent can be deleted only when in 'Stopped' status. Deletion of Assisted Agent removes the agent's record from server's database. Once deleted agent cannot be started.</p> <p>Assisted Agent, when in stopped sate, can be deleted only by the owner or Tenant Administrator.</p>

7.4.1.2 Assisted Agent: Download and Startup

Assisted Agents can be downloaded from AE server and installed on available computers (either Windows or Linux OS). The agent connects to the server (using the same URL specified in URL setting under System Administrator) and gets workflows for running. Tenant Administrator, Tenant user, Workflow Administrator can download and Run Assisted Agents.

7.4.1.3 Assisted Agent: Assign Users

To download an Assisted Agent:

1. Go to the Agents menu. Agent Menu is visible to Tenant Administrators and Agent Administrators. Login with Tenant Administrator or Agent Administrator users.
2. There are three buttons visible.
 - i. Agents: This button is enabled by default. Agents can be started/stopped/deleted.
 - ii. Assisted Agents: Click this button to see Assisted Agents of all the Users. Administrator Users will be able to view, stop or delete these Agents.
 - iii. Controller: This button is only enabled if Controller is setup for the current Tenant. Click this button to see and manage Controller Agents.
3. Click Assisted Agents tab.
4. Currently we can only see an 'Assign to Users' button. There is no 'Download Assisted Agent' button seen. This means that there is no user under the current Tenant that has been assigned permission for Assisted Agents.

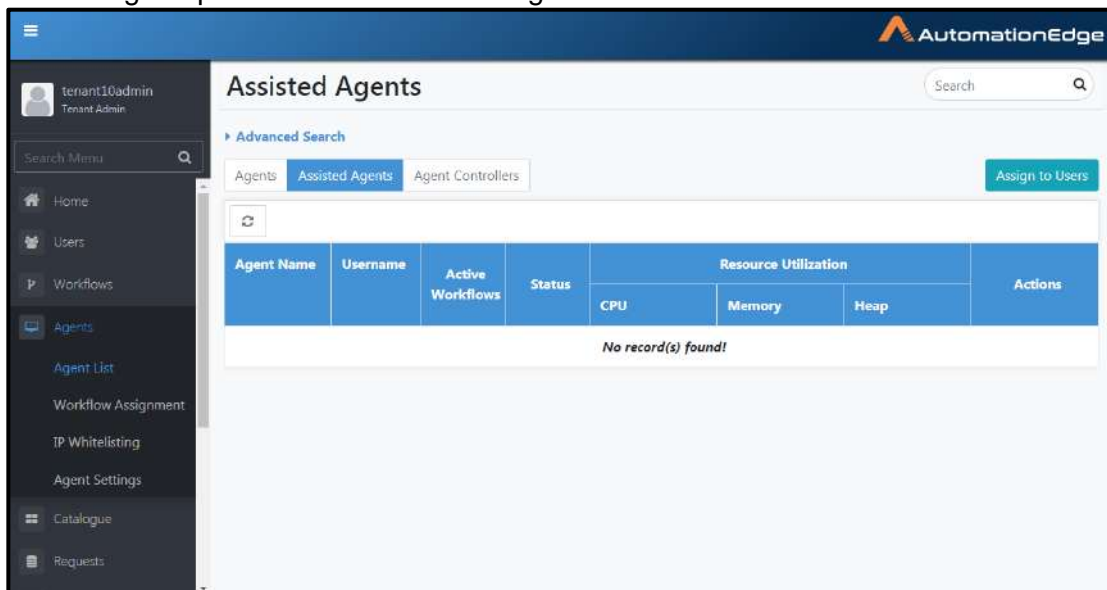


Figure 67b: Assisted Agents Tab

- Click Assign to Users button as shown in the screenshot below to give permissions to users for using Assisted Agents. Tenant Administrator can see the users available. The Administrator(Tenant3 Admin) is checked by default and the number of Assisted Agents. Hence, in the screenshot below we see one of five(1/5) Assisted Agents is used. Note: Five is the provision for number of Assisted Agents in the license.

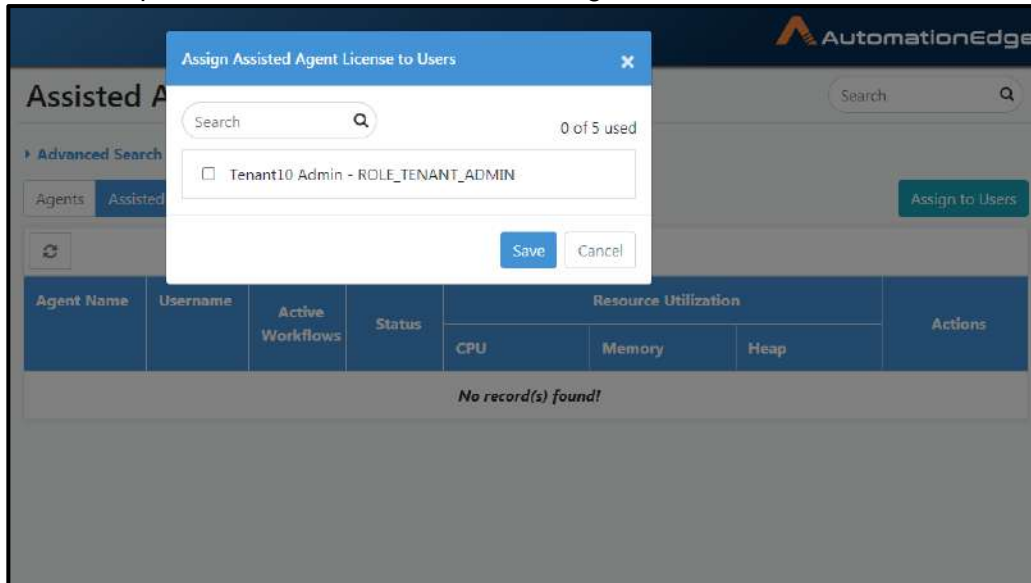


Figure 67c: Assisted Agents License to Users

- Enable checkbox for the users to whom permission is to be given. Click Save. Note: 3 of 5 used seen on the top right corner in the screenshot below shows that three Assisted Agents have been assigned to users out of a total of five Assisted Agents available or attached to the current Tenant. Click Save.

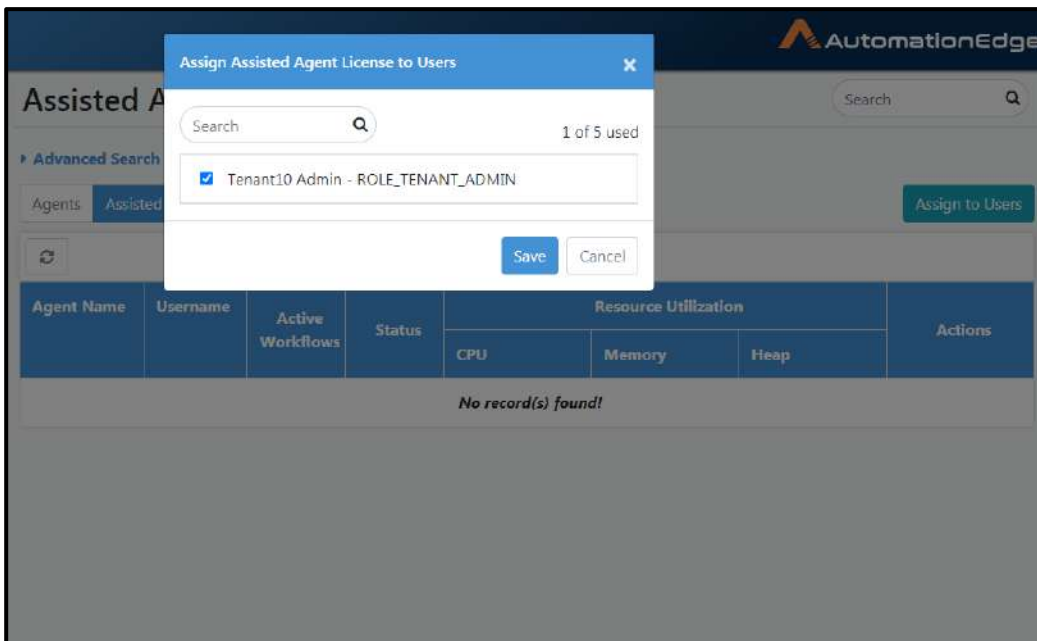


Figure 67d: Assign Assisted Agent License to Users

- We can see the Assisted Agent Assignment updated successfully message.

- Now Agent Menu and 'Download Assisted Agent' button will be visible to any Tenant Administrator and Agent Administrators and Tenant User Users that have been assigned permission to Assisted Agent. Click download.

Note: Assisted Agents can be downloaded only if the System setting - 'Server URL' has been set by the System Administrator.

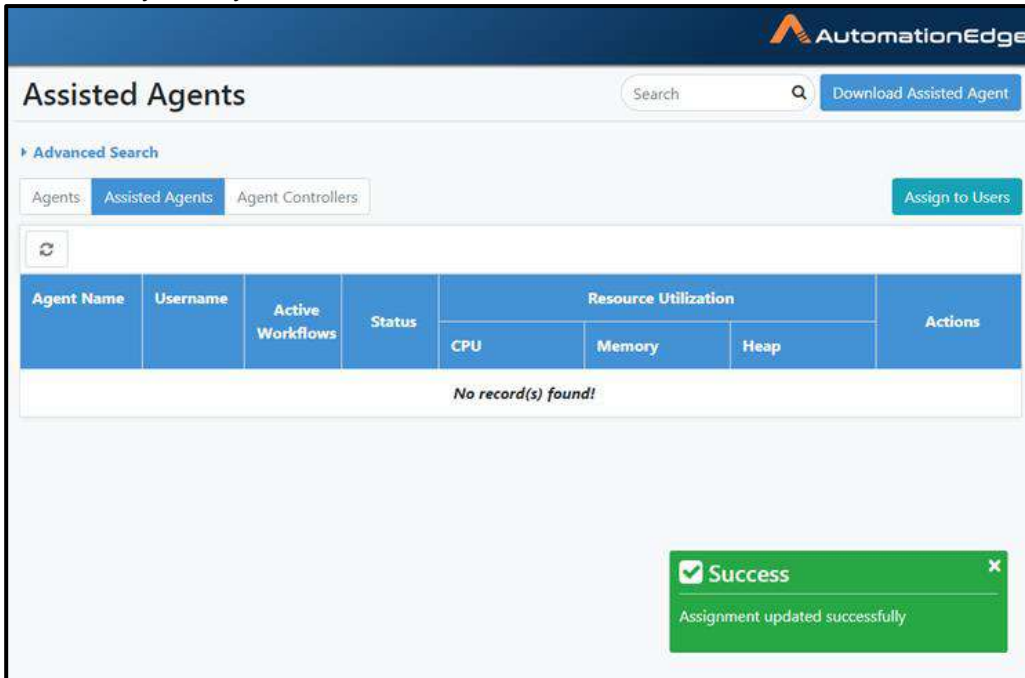


Figure 67e: License Assignment to Users Successful

7.4.1.4 Assisted Agent: Download

Following are the steps to download Agents,

- Once the assignment is done, you can now see the Download Assisted Agent button on the top right corner. Click on the button.

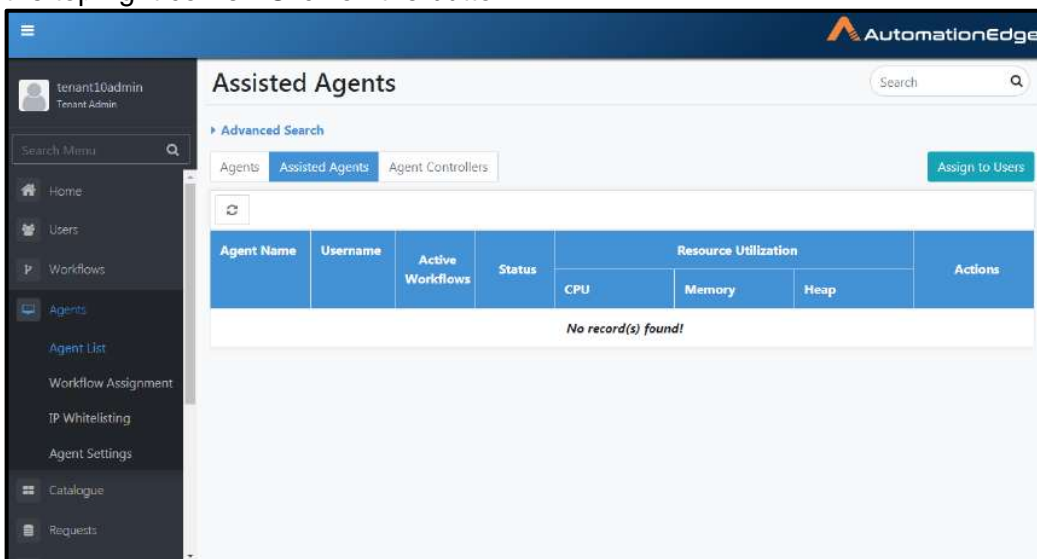


Figure 68a: Download Assisted Agent

2. The Proxy configuration window appears. Configure Proxy if required. Proxy configuration has been explained in the section. Click Download.

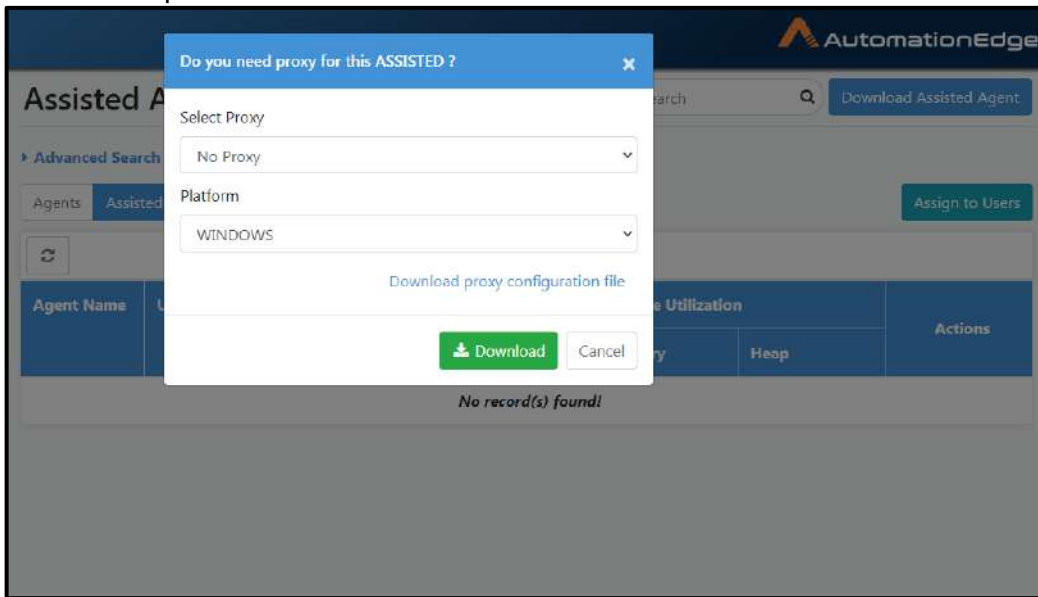


Figure 68b: Proxy window

3. We can see the Agent zip being downloaded and a Download started message appears.

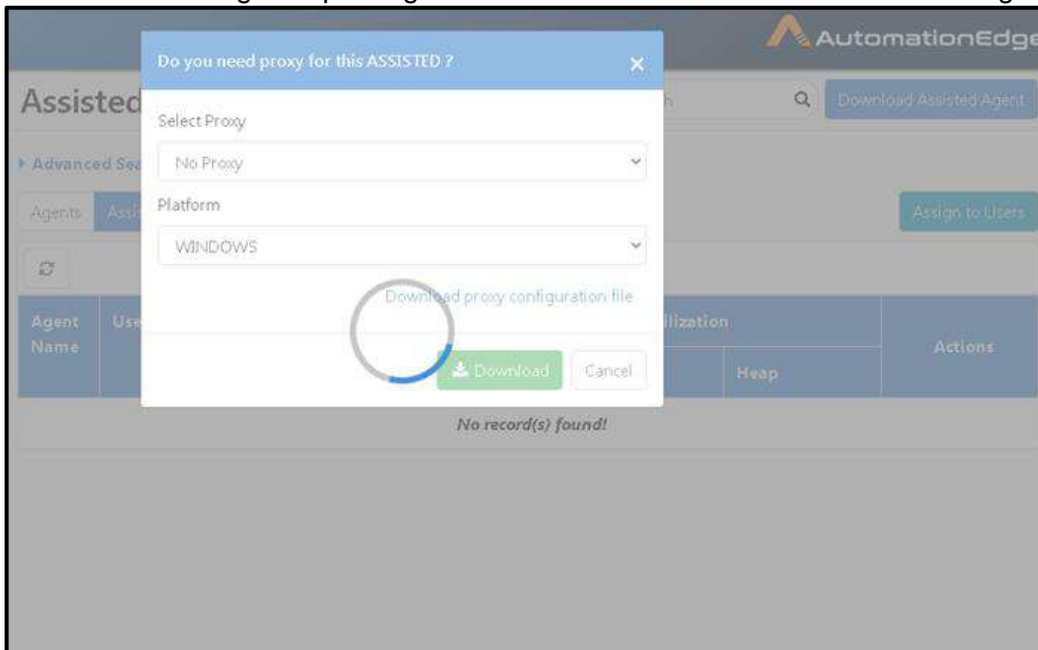


Figure 68c: Agent Download in progress

- A Download started message appears and Assisted Agent is downloaded as seen below.

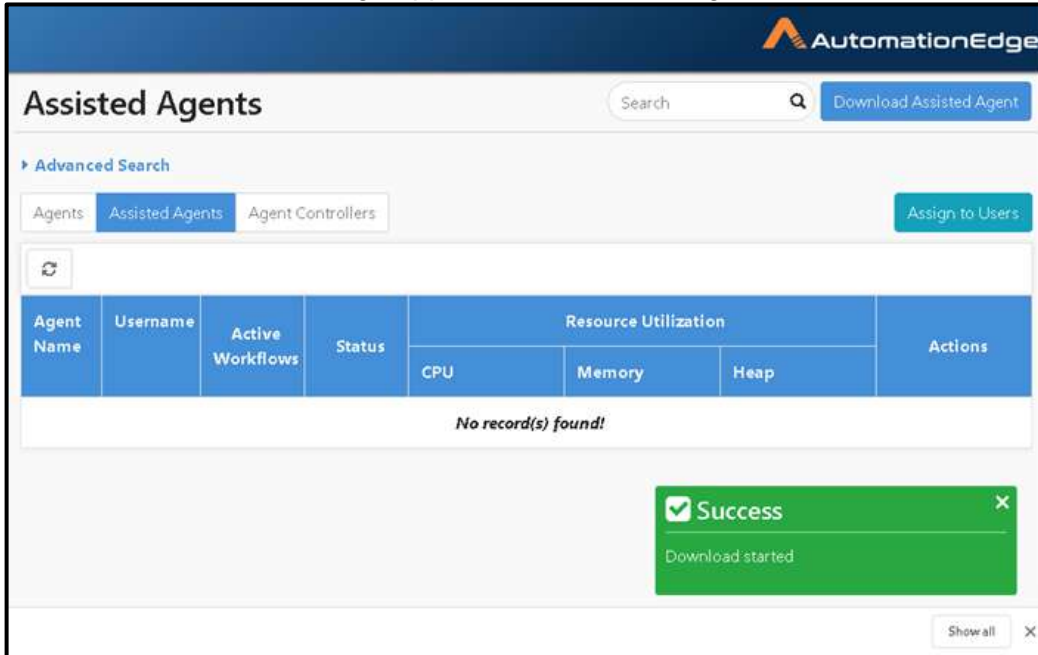


Figure 68d: Download with Automatic Configuration started

7.4.1.5 Assisted Agent: Startup

- Unzip the downloaded Agent zip file and extract an Assisted Agent.
- The agent's zip should be unzipped on the machine where it is to be run. It contains an ae-agent directory. The downloaded zip file can also be copied to one or more machines where we need to run an Assisted Agent.

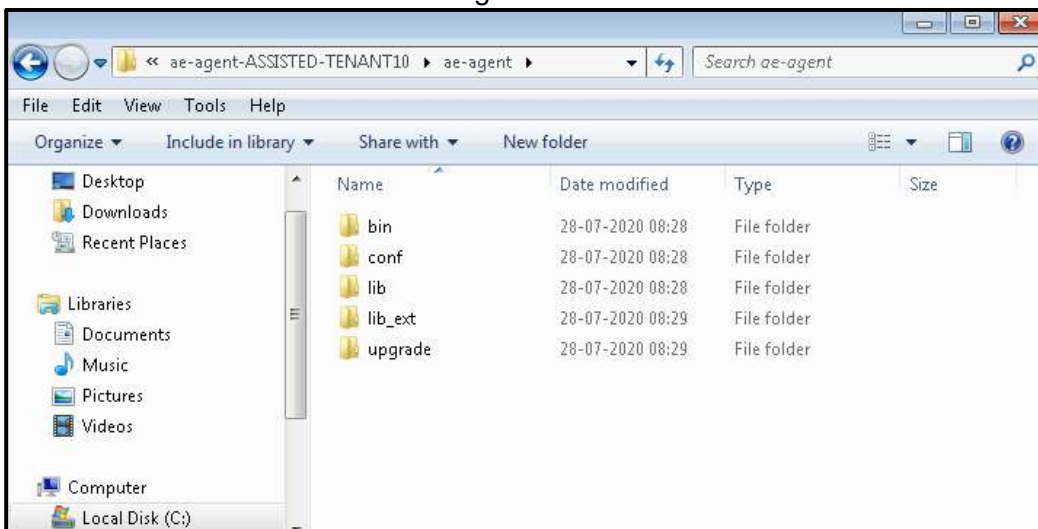


Figure 68e: Assisted Agent Directory

- Run `ae-agent/bin/startup.bat` or `ae-agent/bin/startup.sh` file (for Windows and Linux respectively) from command prompt. Assisted Agent will register itself with the server and

will be available to run any Assisted Workflows assigned to the user as described in the next section.

Please note if an Assisted Agent is already registered for the user a new Assisted Agent will not be registered and startup will fail.

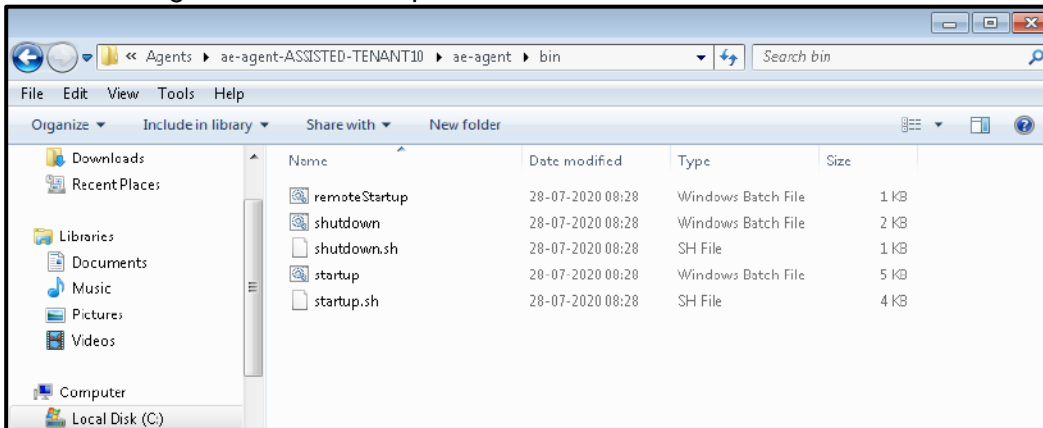


Figure 68f: Assisted Agent Startup Directory

8. Type `cmd` in the Windows explorer address bar and press keyboard enter.

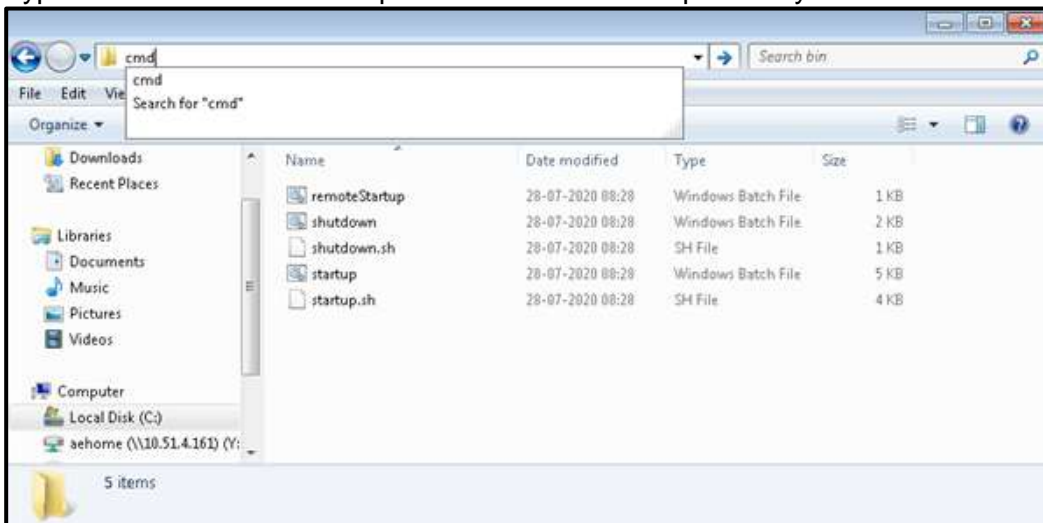
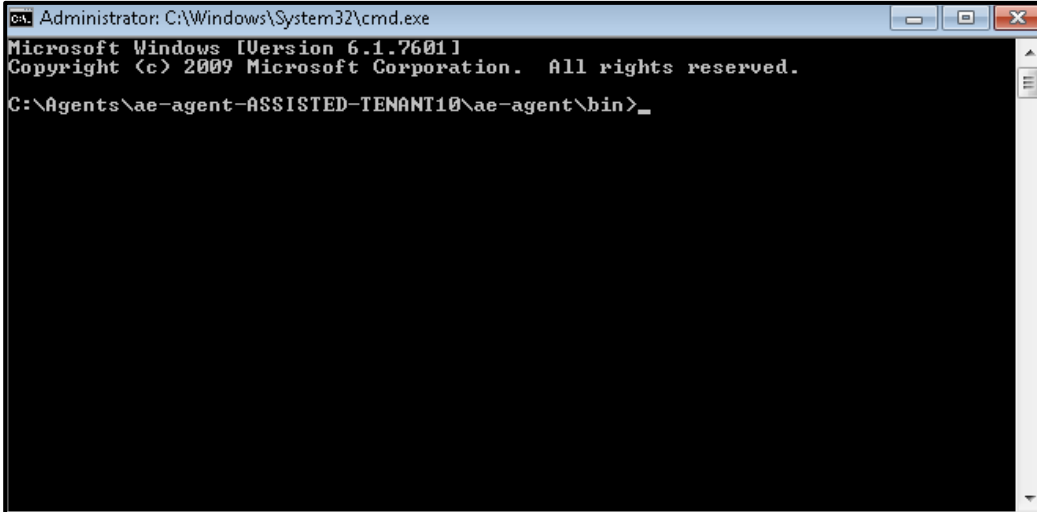


Figure 68g: Open Command Line at startup location

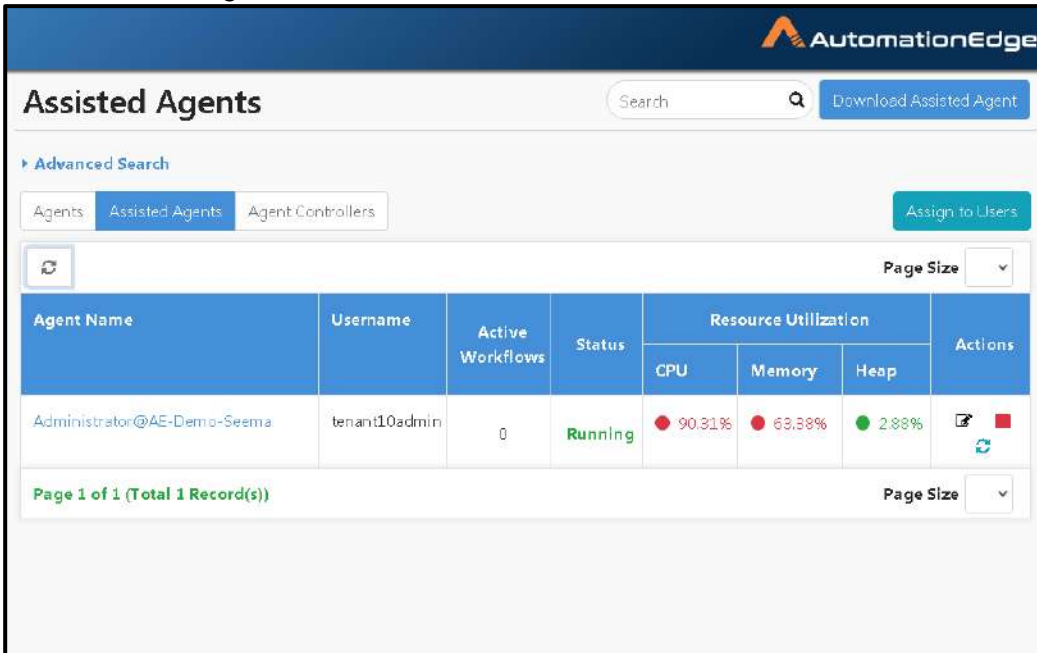
- Type startup.bat. Press Keyboard Enter. Starting Agent from command prompt is the recommended way rather than double clicking on startup.bat.






```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Agents\ae-agent-ASSISTED-TENANT10\ae-agent\bin>
```

Figure 68h: Execute startup.bat

- Once Startup is complete view Assisted Agents in UI. You can see the Assisted Agent status as Running.



Agent Name	Username	Active Workflows	Status	Resource Utilization			Actions
				CPU	Memory	Heap	
Administrator@AE-Demo-Seema	tenant10admin	0	Running	90.31%	68.38%	2.88%	  

Page 1 of 1 (Total 1 Record(s))

Figure 68i: View Agent Status: Running

Note: Assisted Agent license is configured with the number of hours (any number of hours between 6 and 23 hours) it can run. For long running Assisted Agent the Assisted Agent stops running after the time mentioned in the license. The Agent can be restarted on the next day.

- To stop an Agent Run ae-agent/bin/shutdown.bat or ae-agent/bin/shutdown.sh file (for Windows and Linux respectively).

7.4.2 Assigning Workflow to an Assisted Agent

Assisted Workflows cannot be assigned to an Assisted Agent. However, Assisted Agent can execute Assisted Workflows for which Assisted Agent Owner User has execution permissions. Please note that Assisted Workflows are always saved as sequential workflows.

7.5 Tab: Controller Agents

7.5.1 Introduction


Many of the AE workflows involving UI automation running on MS Windows machines encounter the following operational issues:

1. Agents cannot run as service: We need to start user's login session and start agent in that session. We cannot start it as windows service, as running UI from service is not possible.
2. Windows console cannot be locked: Some of the UI workflows do not run with locked windows console.
3. RDP should always be connected: If we login to windows using RDP, the RDP should always be connected while running the workflow. UI workflows do not work in case RDP is disconnected.
4. Agents should always be started manually after login to machine, and the login session should be kept unlocked.

This makes it cumbersome to manage Agents if they are large in numbers. Controller is a solution to control Agent's uptime from AE portal.

Agent Controller: At least one Agent machine should be designated as Agent Controller. This can be done by marking one or more agents as 'Controller' from AE Portal. The Agent Controller does not run any workflow. Agent controllers receive instructions from the server to start Agents on user demand. The Controller which takes the control first starts the Agent.

An Agent controller cannot be started automatically; it should always be started manually. To view controller from UI, need to set `enableController=True` in `TOMCAT_HOME\webapps\aeui\aeui-config.properties` property file.

 **Note:** Agent controller can run on Windows machines only and it can control Agents on Windows machines only.

Controlled Agents: Except controller agent, All Agents are controlled Agents. They can be started from AE Portal. As we need to start Windows session using RDP, Windows login password of the corresponding windows user needs to be supplied. Agent already captures other details like hostname, ip address, username where it is running. Password should be supplied using AE Portal.

The option to download controller and view controllers is available to Tenant Administrator and Agent Administrator.

Is RDP enabled workflows

Is RDP enabled is a configuration checkbox during workflow creation or update.

Controller could be a single point of risk with many RDP sessions to agent's machines open and unlocked. We have mitigated that risk by acquiring the RDP session only for the duration of workflow execution and for agent start-up. This is achieved by marking the workflows as **Is RDP enabled** true. For more details on **Is RDP enabled** refer section [Is RDP Enabled](#).

7.5.2 Manage Controller Agent

7.5.2.1 Agent Controller: Download

Following are the steps to start controller agent.

1. Go to the Agent menu and Controller sub-menu.
2. Click Download Controller button on top right corner.
3. A pop-up window appears for setting Proxy server details if required. Click Download.

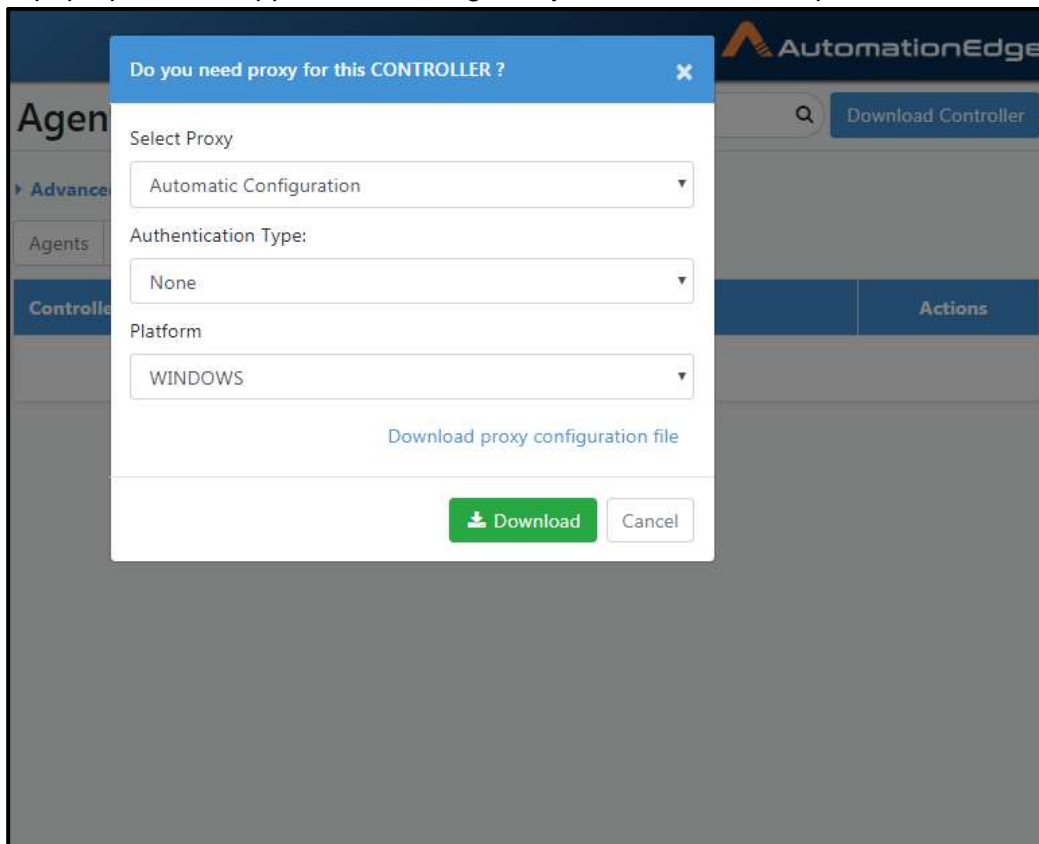


Figure 69a: Proxy Window

4. Agent Controller download in progress circle appears.

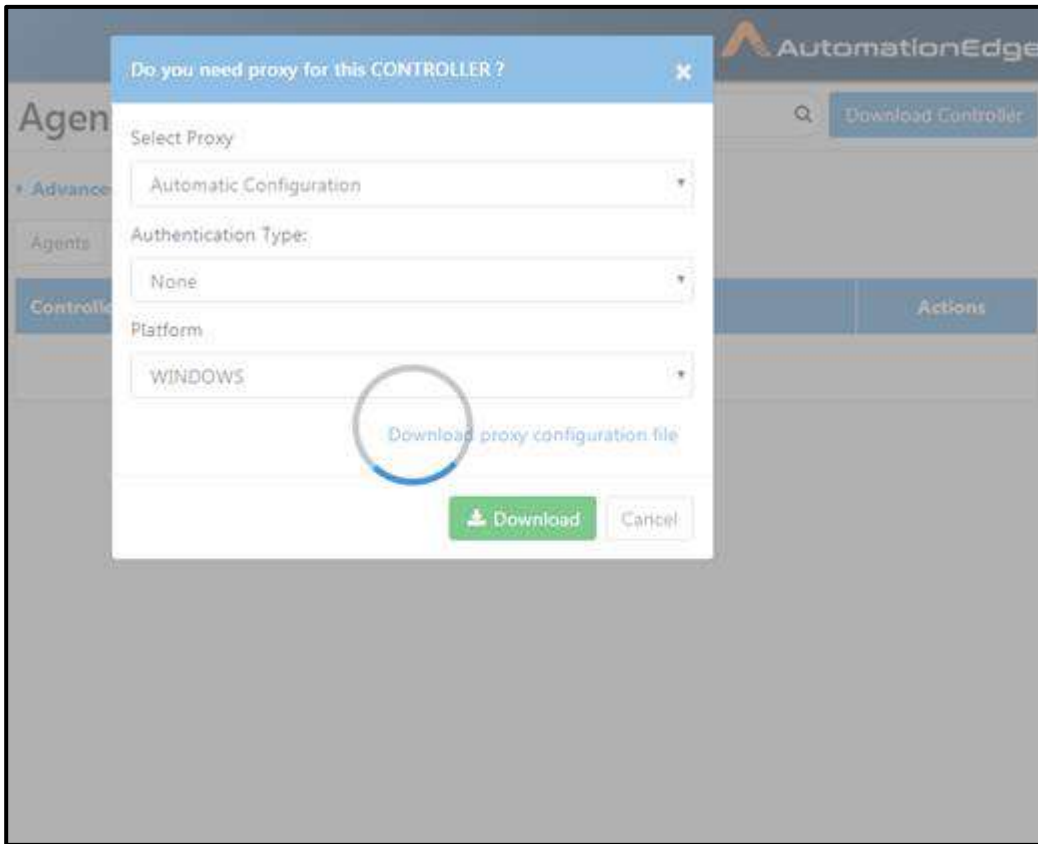


Figure 69b: Downloading Controller Agent

5. You get a message Download started. You can see the agent controller zip being downloaded.

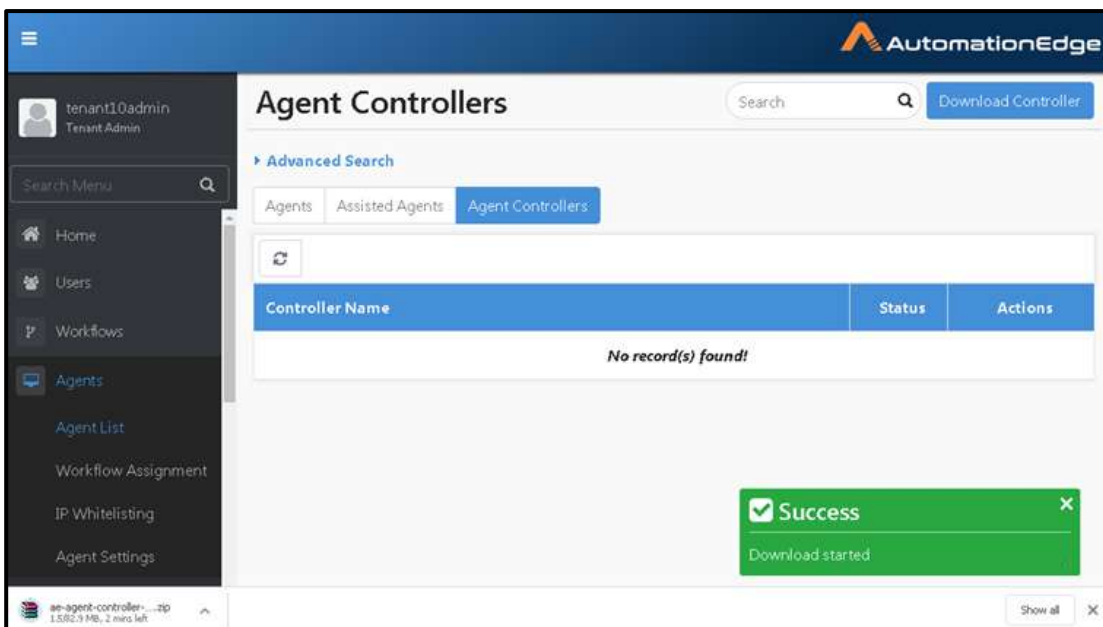


Figure 69c: Downloaded Controller Agent

7.5.2.2 Agent Controller: Start

1. Start Agent controller from ae_agent/bin directory by running startup.bat
2. You can now see the Agent Controller is running

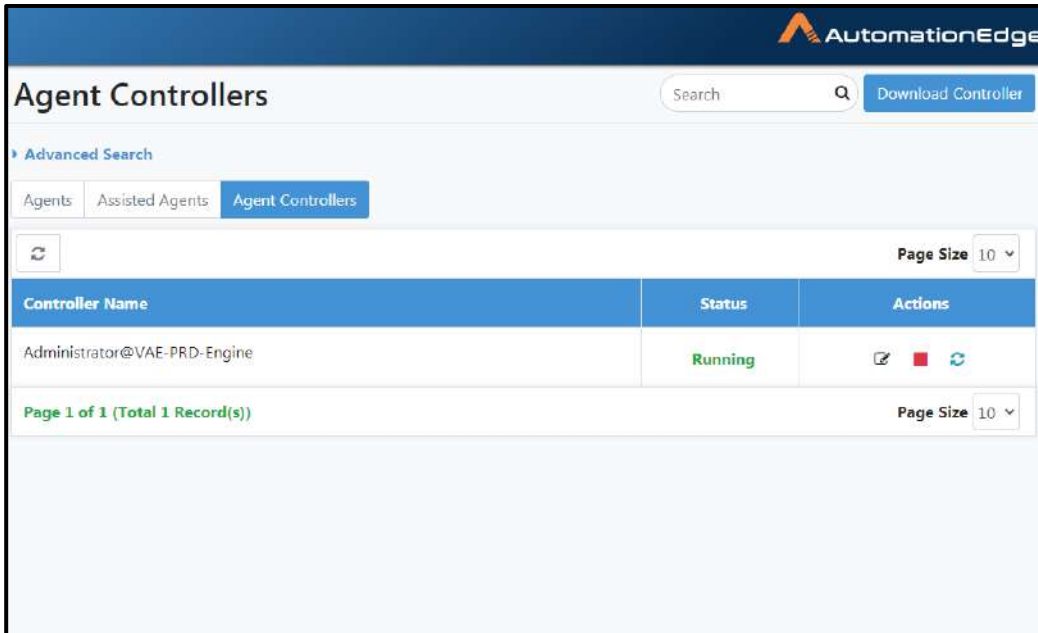


Figure 70a: Controller Agent Running

7.5.2.3 Agent Controller: Stop

1. You can now see Edit and Stop icons in the Actions column. You may click stop icon to see Stopping Agent message as below.

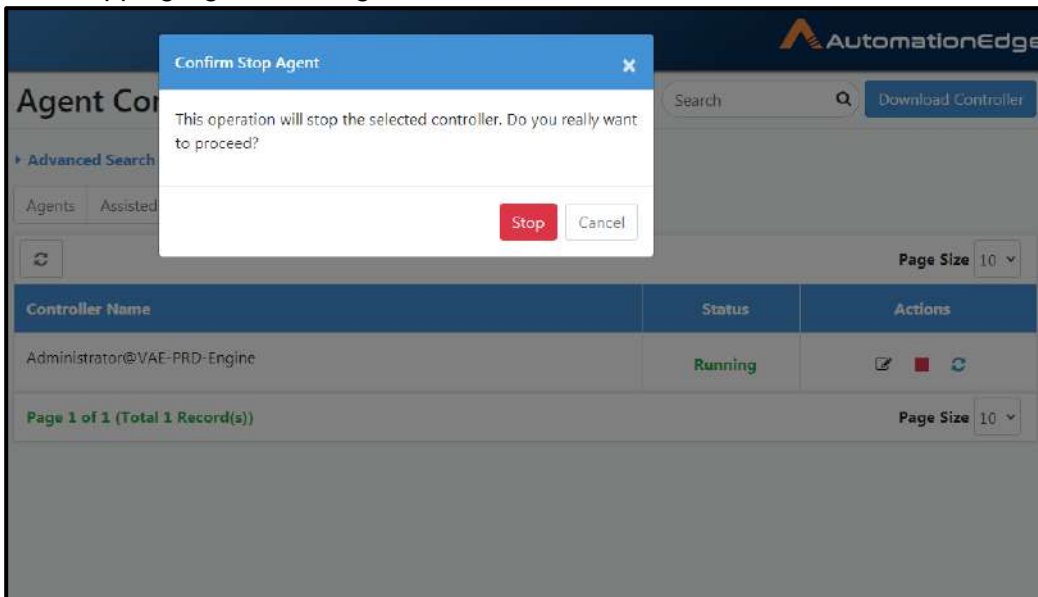
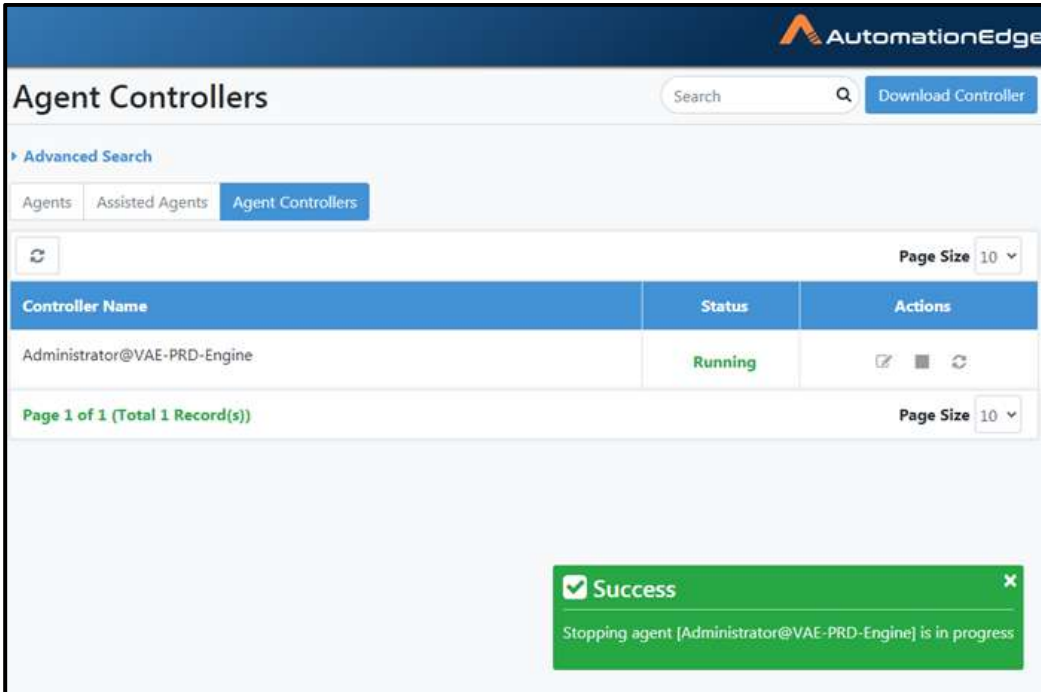


Figure 71a: Stopping Agent Controller

2. Note the message Stopping Agent is in progress.



The screenshot shows the AutomationEdge interface for Agent Controllers. The page title is "Agent Controllers" and it includes a search bar and a "Download Controller" button. Below the title, there are tabs for "Agents", "Assisted Agents", and "Agent Controllers". A "Page Size" dropdown is set to 10. The main table has columns for "Controller Name", "Status", and "Actions". The table contains one record: "Administrator@VAE-PRD-Engine" with a status of "Running". Below the table, a green success message box displays: "Success Stopping agent [Administrator@VAE-PRD-Engine] is in progress".




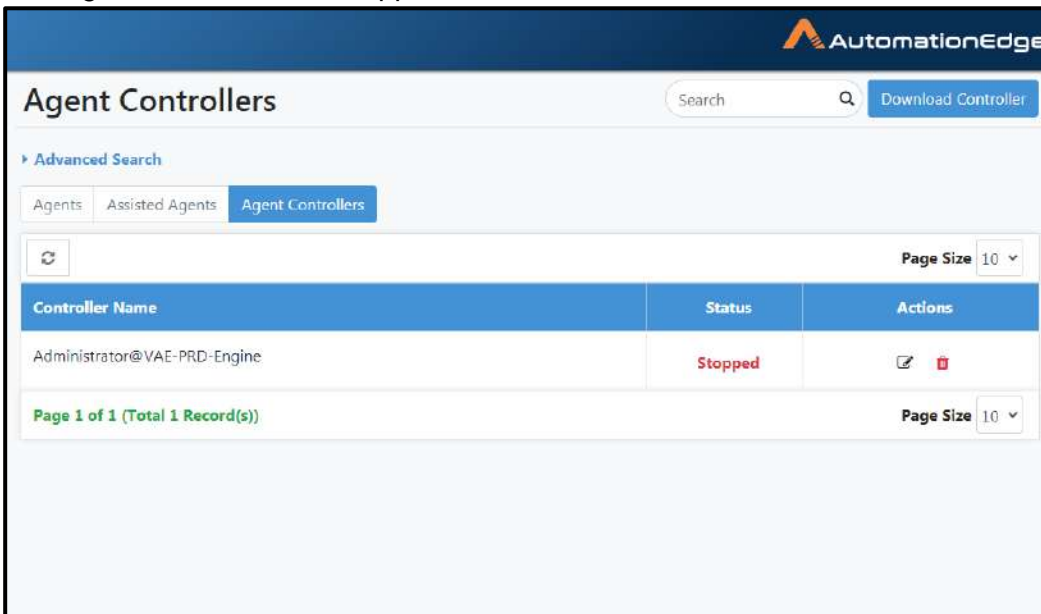
Controller Name	Status	Actions
Administrator@VAE-PRD-Engine	Running	  

Figure 71b: Stopping Controller Agent Success

3. The Agent now shows as stopped.



The screenshot shows the AutomationEdge interface for Agent Controllers. The page title is "Agent Controllers" and it includes a search bar and a "Download Controller" button. Below the title, there are tabs for "Agents", "Assisted Agents", and "Agent Controllers". A "Page Size" dropdown is set to 10. The main table has columns for "Controller Name", "Status", and "Actions". The table contains one record: "Administrator@VAE-PRD-Engine" with a status of "Stopped". Below the table, a green success message box displays: "Success Stopping agent [Administrator@VAE-PRD-Engine] is in progress".



Controller Name	Status	Actions
Administrator@VAE-PRD-Engine	Stopped	 

Figure 71c: View Agent Status is stopped

7.5.2.4 Agent Controller: Delete

1. Click the Delete icon. It gives a pop-up to configure delete.

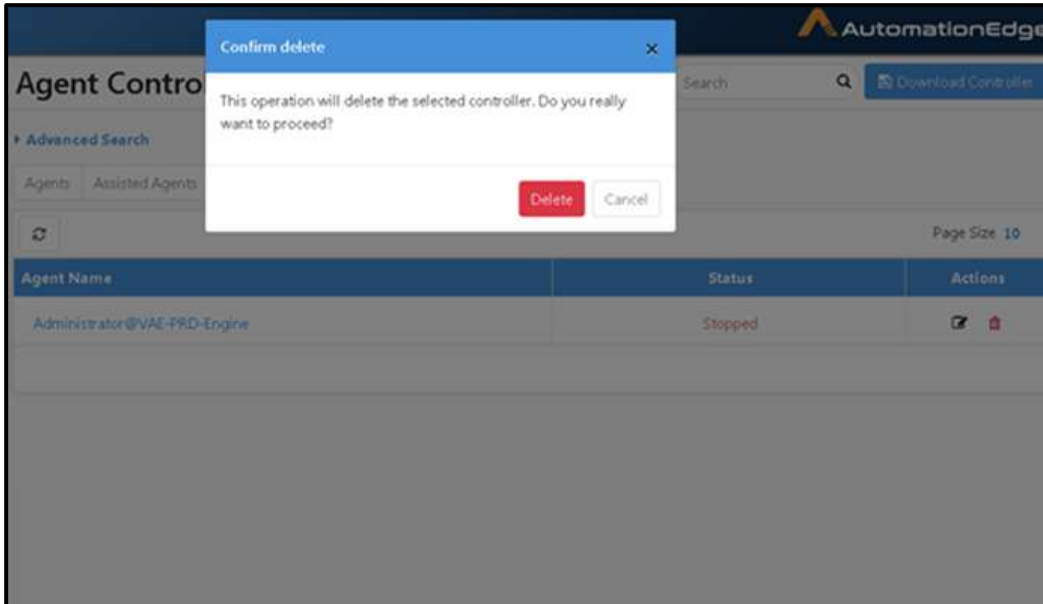


Figure 72a: Delete Controller Agent

2. Agent deleted successfully message is displayed.

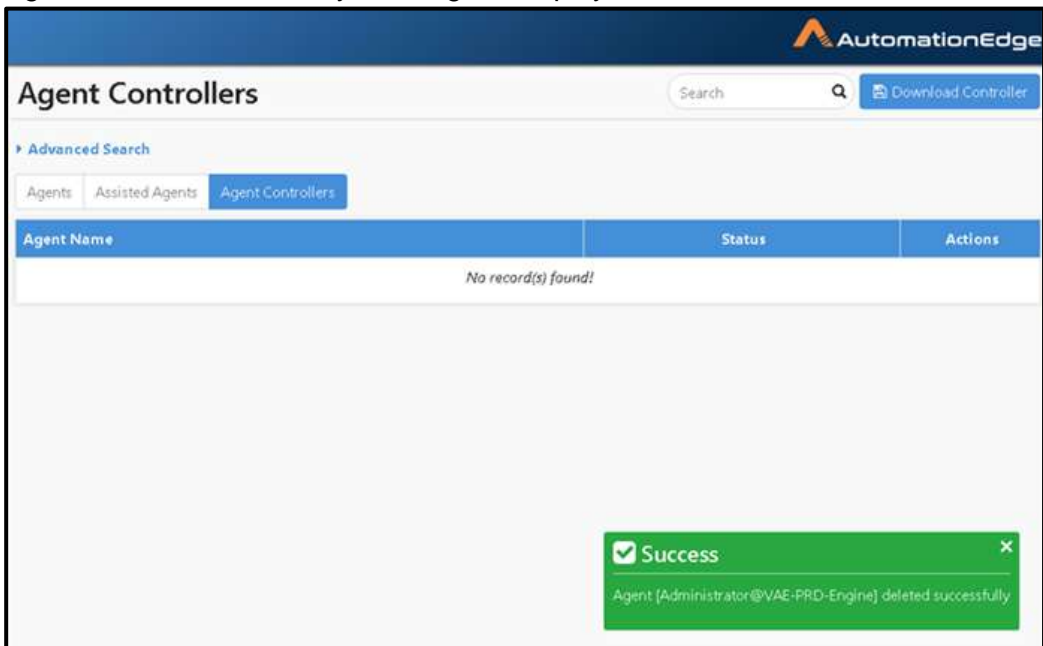


Figure 72b: Agent Controller Delete Success Message

7.5.2.5 Agent Controller: Edit

1. Click Edit button next to the Controller you wish to edit.

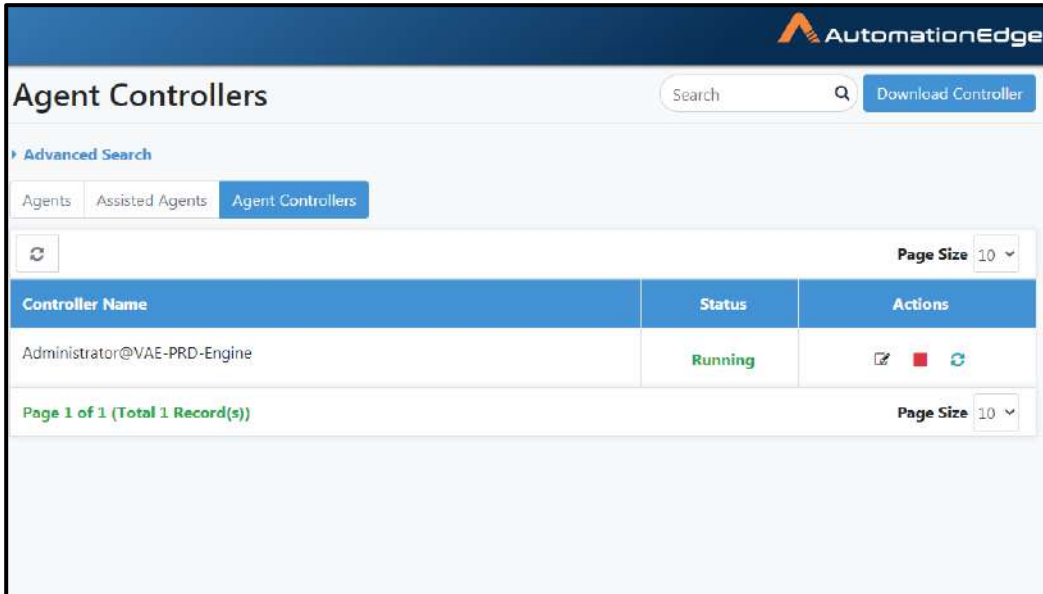


Figure 72c: Edit Controller


2. Edit the Agent Controller Agent Name, Domain name or IP Address.

Figure 72d: Agent Controller Edit

7.5.3 Agent Controller Setups

1. Agents are installed and registered on all agent VMs.
2. Click on Start→All Programs→Startup→Right Click open Startup. A shortcut of Agents bat file (remoteStartup.bat) should be copied to startup of each Agent machine.
3. At least one agent should be marked as Agent Controller.
4. For all the other Agents, windows password should be entered using Agent Edit dialog.
5. In case your Security policy does not allow the use of connection details for terminal services due to windows policy settings, you may need additional settings as discussed in the next section.
6. By default, windows show a Certificate confirmation dialog for every RDP session that is opened. We need to make sure that this dialog is suppressed on the controller machine.

Once this setup is done, clicking on 'Start' button against Agent (▶) will invoke RDP on the machine and start the Agent.

 **Note:** For Agent controllers, the time for which the password is stored to connect to the required Agent machine is configurable. The **<Agent_Controller_Home>/conf/application.properties** file has a property - "agent.rdp.password.cleanup.duration.seconds". The default value is 15 seconds. To save the password for a longer duration while establishing connectivity set the property to a higher value.

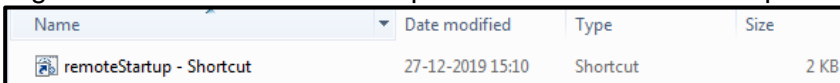
However, any previous RDP sessions should be logged off before Controller can attempt to start the Agent. Generally, Agent machines should be managed by the Agent Controller only. Otherwise any manual RDP session to the Agent's machine will also start the Agent.

On clicking on 'Stop' button against the running Agent, the Agent will stop and RDP session will be logged out.

7.5.3.1 Workflow Needs Administrator privileges

In case a workflow running on an Agent machine needs administrator access then the Agent must be Run as administrator. Follow the following two steps to Run Agent as administrator,

1. Right Click on the remoteStartup.bat shortcut and click Properties.




Name	Date modified	Type	Size
 remoteStartup - Shortcut	27-12-2019 15:10	Shortcut	2 KB

Figure 73a: remoteStartup executable on Agent machine

2. The remoteStartup - Shortcut Properties window appears as seen below.
3. Click Advanced button.

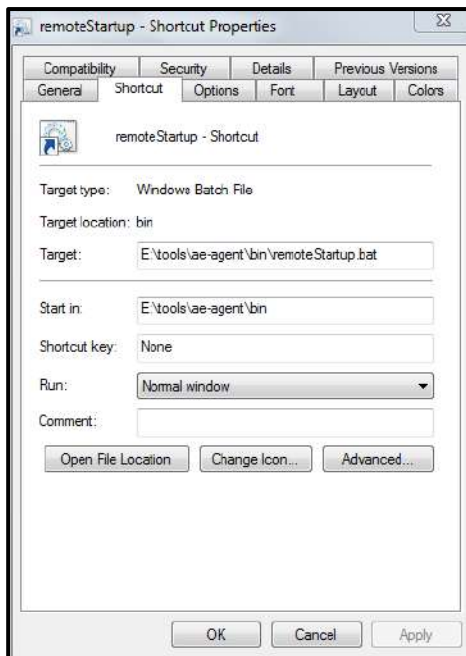


Figure 73b: Setup Advance properties

4. Enable Run as administrator check box.



Figure 73c: Enable Run as Administrator

7.5.4 Windows policies for Agent Controller

7.5.4.1 Windows Security policies for Agent Controller

In case your Security policy does not allow the use of connection details for terminal services due to windows policy settings, you may additionally need to configure following settings,

A. On Controller Machine:

1. On the Remote Desktop Connection Window, uncheck Always ask for credentials as seen below.

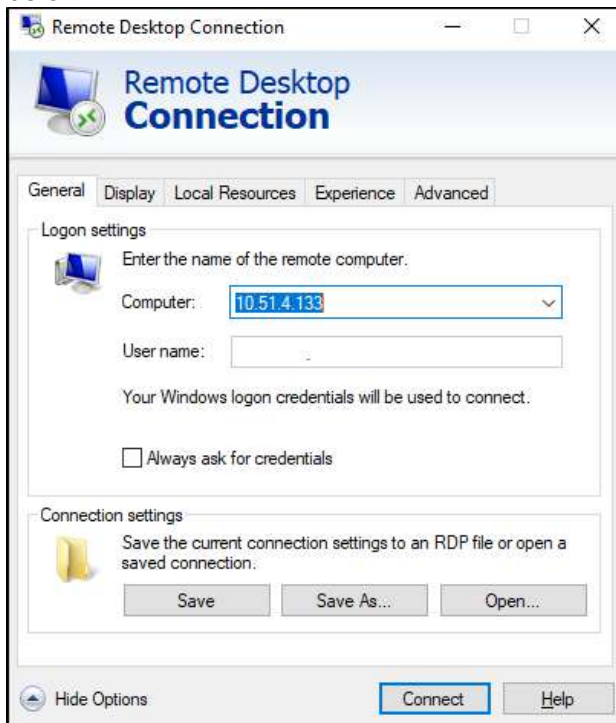


Figure 73d: On Controller machine uncheck 'Always ask for credentials'

2. We use a solution that uses Window Credential Manager to temporarily store credentials for automatic RDP connection. To use stored passwords on Controller VM navigate to the following path under group policy:

Computer Configuration (gpedit.msc) -> Administrative Templates -> System -> Credential Delegation

Enable the following policies on the Controller Machine

- i. Allow delegating default credentials with NTLM-Only server authentication
- ii. Allow Delegating Default credentials
- iii. Allow Delegating saved credentials
- iv. Allow Delegating saved credentials with NTLM-only server Authentication

3. Run the regedit.exe tool
4. Find the registry key: HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client.
Create a DWORD value with the name: RemoteDesktop_SuppressWhenMinimized and set its value to 2.

5. Find the registry key
HKEY_CURRENT_USER\Software\Wow6432Node\Microsoft\Terminal Server Client
Create a DWORD value with the name RemoteDesktop_SuppressWhenMinimized and set its value to 2.
6. Find the registry key: HKEY_LOCAL_MACHINE\Software\Microsoft\Terminal Server Client.
Create a DWORD value with the name: RemoteDesktop_SuppressWhenMinimized and set its value to 2.
7. Find the registry key
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Terminal Server Client
Create a DWORD value with the name: RemoteDesktop_SuppressWhenMinimized and set its value to 2.
8. Close the regedit.exe tool.

B. On Agent machine:

1. On the Agent Machine we need to disable following policies so that **Controller can automatically connect to agent Machine**.
Navigate to the following path under group policy,
Computer Configuration (gpedit.msc) -> Administrative Templates -> Windows Components -> Remote Desktop Services -> Remote Desktop Session Host -> Security
On the agent VMs disable the policy: **Always prompt for password upon connection**
2. If you are still unable to automatically create an RDP connection additionally
Set the following registry entry:
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services\DisablePasswordSaving = 0

7.5.4.2 Windows Remote Desktop policies for RDP enabled workflows

In case of Is RDP enabled workflows you may need to configure following settings,

C. On Agent machine

1. Idle timeout and Active Timeout.

If enabled, idle timeout value has to match the max workflow execution time. This is found under group policy at

Computer Configuration -> Administrative Templates -> Windows Components -< Remote Desktop Services -> Remote Desktop Session Host -> Session Time Limits

- i. Set Time Limit for Active but idle Remote Desktop Service sessions
- ii. Set Time Limit for Active Remote Desktop Service sessions

7.5.5 UI Configuration for Starting/Stopping Controlled Agents

AutomationEdge Agents can be started by their respective Controller Agents to which they are assigned. Please refer to section [7.7 Agents: Controller Assignment](#) for steps to assign Agents to Controllers. Following are the steps for AutomationEdge Agents Start/Stop,

1. Go to Agents menu and Agent List sub-menu. Currently there is one Agent registered on some other machine.

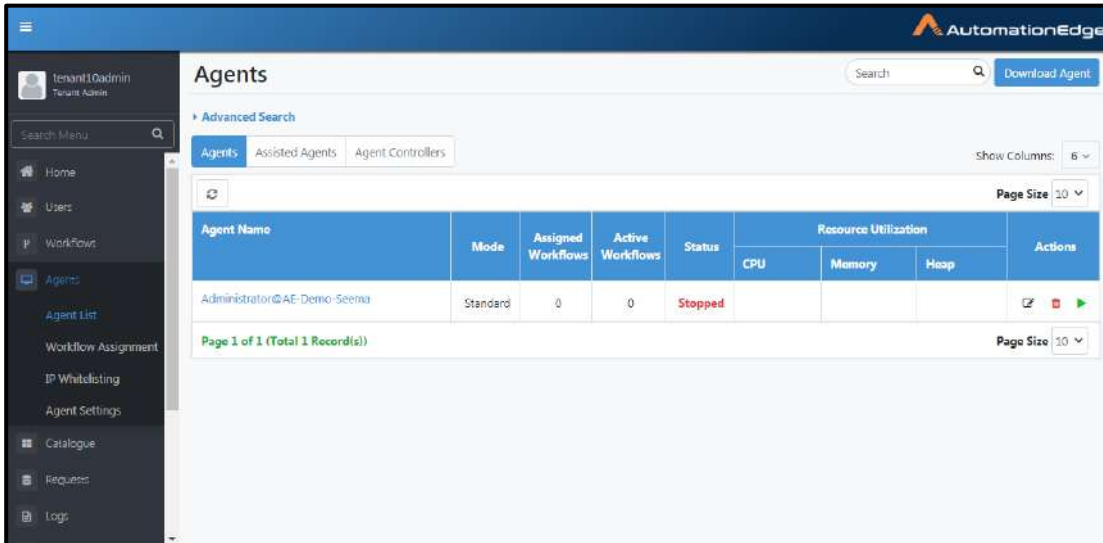


Figure 74a: Agents View

2. Click Download button on top right corner to download the Agent.
3. You may start the Agent on your machine/VM.
4. You can now see the Agent in the Agent List Column is in running state.

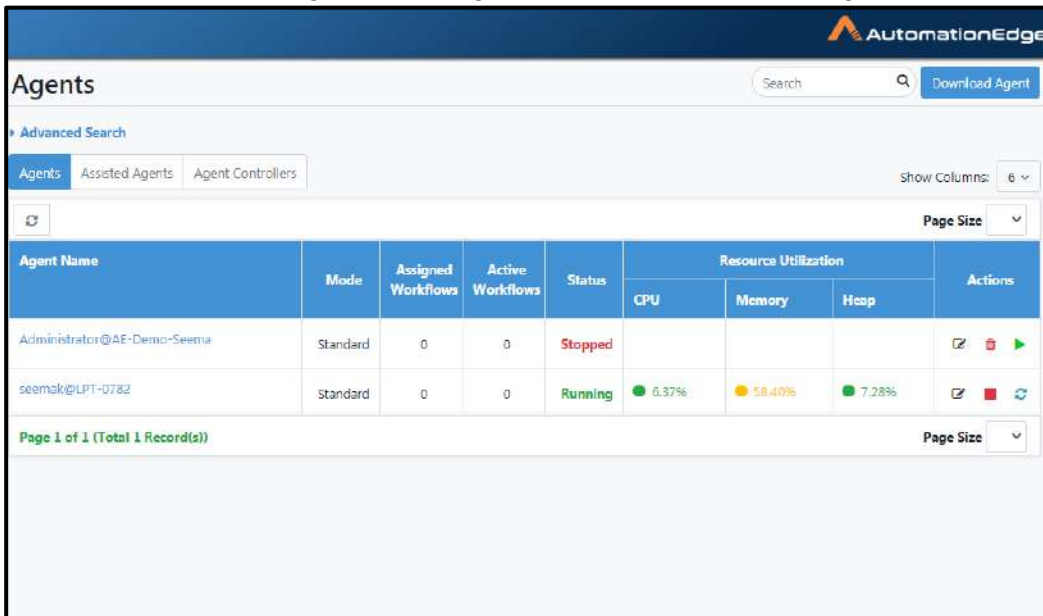


Figure 74b: Agent on remote machine registered

5. For taking RDP and starting the Agent on Controller machine you need to edit the Agent and provide Agent machine credentials. Click Edit in the Action column.

- Click Edit in the Action column. Provide Remote Machine Password for the User. Click Save.

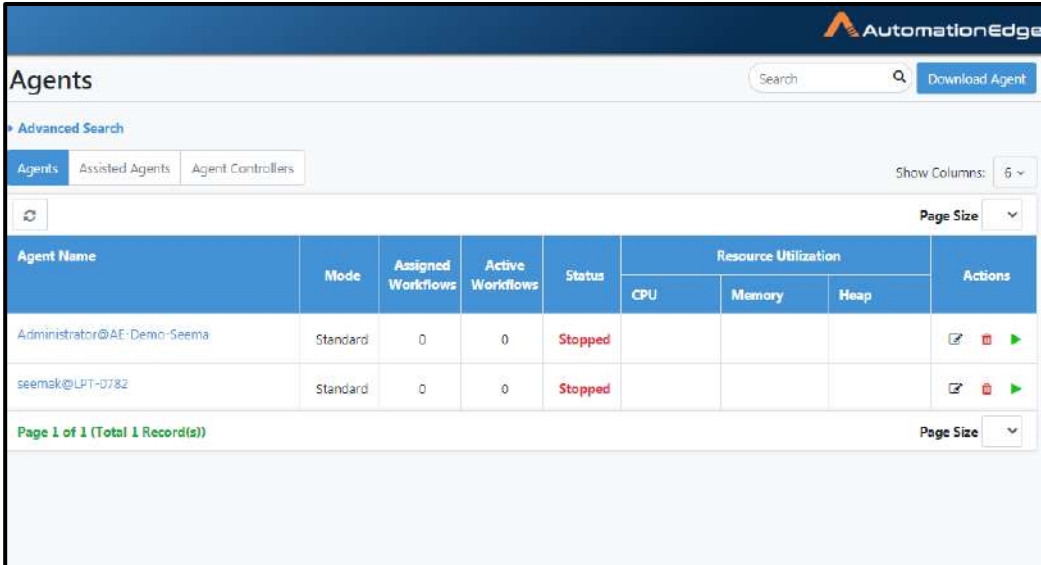
Figure 74c: Edit Agent to set Remote Desktop password

- Successful Changes saved to Agent message displays.

Agent Name	Mode	Assigned Workflows	Active Workflows	Status	Resource Utilization			Actions
					CPU	Memory	Heap	
Administrator@AE-Demo-Seema	Standard	0	0	Stopped				
seemak@LPT-0782	Standard	0	0	Running	6.37%	58.40%	7.26%	

Figure 74d: Agent Configured for IP and Password

- Once the Agent machine details have been saved, the start arrow in the Actions list is enabled whenever Agent is in stopped state. The options available in the Actions column are Edit, Start and Delete when Agent is in stopped state.
- You may click the Start arrow next to the Agent to take an RDP of the Agent machine/VM and start the Agent.









Agent Name	Mode	Assigned Workflows	Active Workflows	Status	Resource Utilization			Actions
					CPU	Memory	Heap	
Administrator@AE-Demo-Seema	Standard	0	0	Stopped				  
seemak@LPT-0782	Standard	0	0	Stopped				  

Figure 74e: Start Agent from Controller

- When you click on Start icon for the Agent a message box Initiated Start command for Agent is displayed.

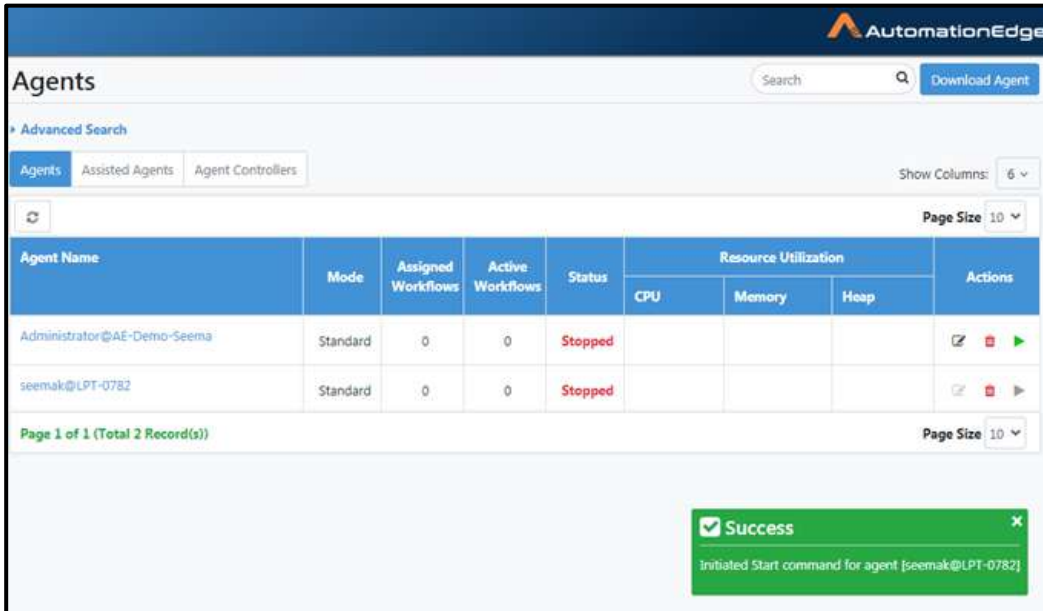


Figure 74f: Initiated Remote Start

- While the Agent is starting the start icon is disabled.

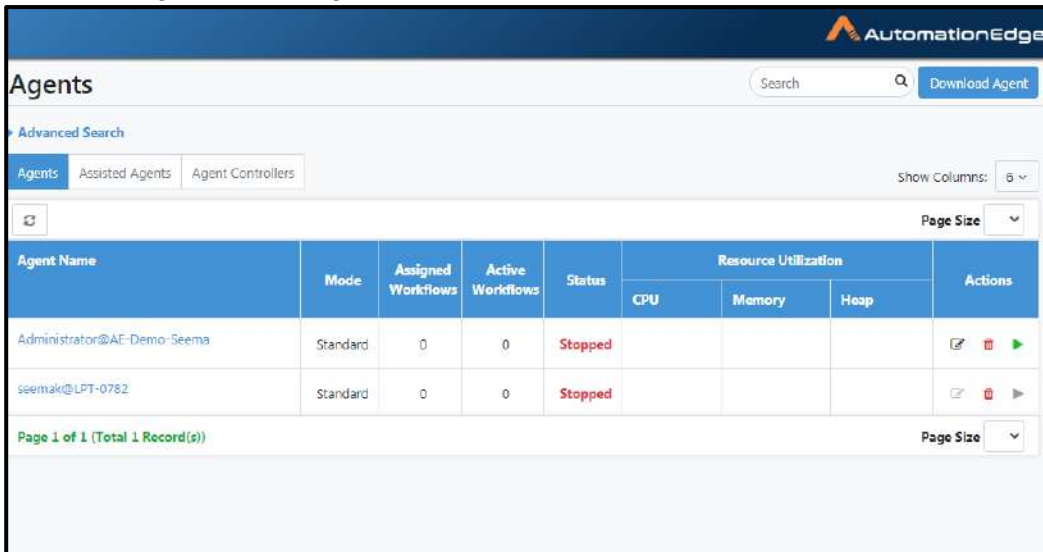


Figure 74g: Start icon disabled

12. Also, the first time you start an Agent you may see a pop-up to confirm authenticity of the remote machine. Enable checkbox (Don't ask me again for connection to the computer) and click Yes to connect to the remote machine.



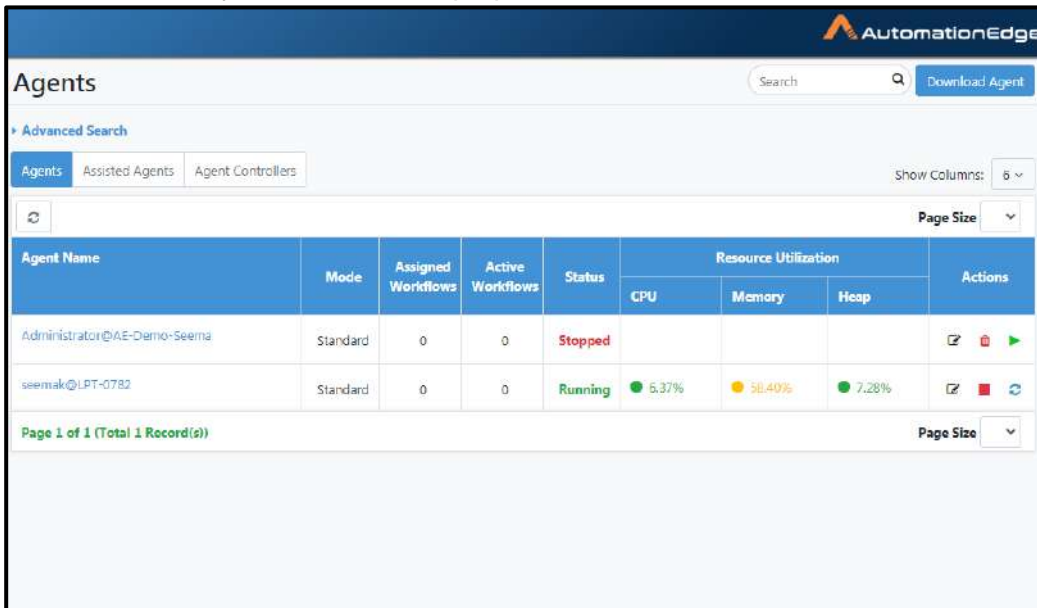
Figure 74h: Controller confirming the authenticity of remote machine

13. Controller Agent tries to establish Remote Desktop Connection.



Figure 74i: Controller starting remote machine and agent on remote machine

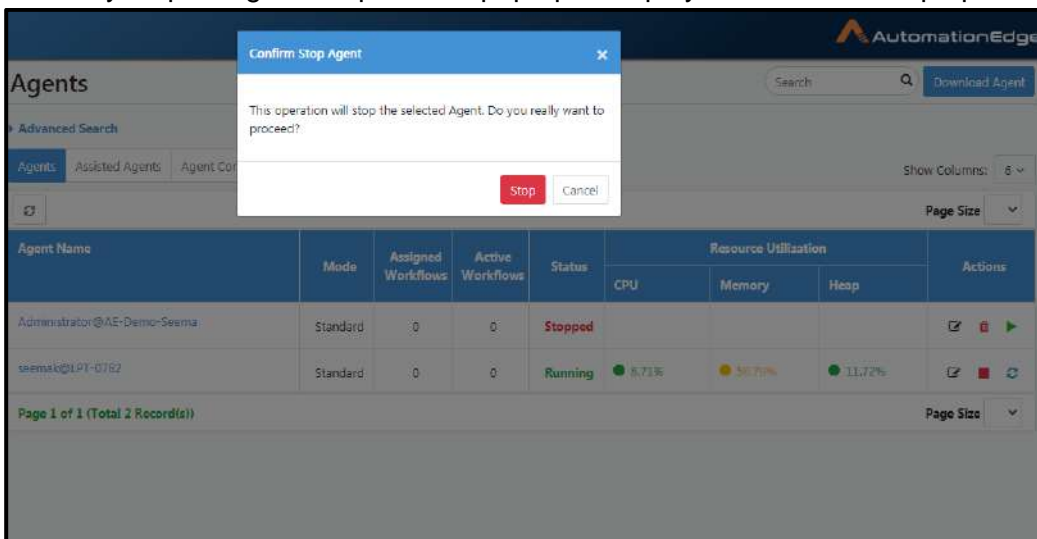
14. RDP starts the remote machine. Controlled Agent is also started on the machine.
15. The start icon is no longer visible next to the first Agent and Agent in the Running state.
16. You now see only the Edit and Stop options in the Action columns.



Agent Name	Mode	Assigned Workflows	Active Workflows	Status	Resource Utilization			Actions
					CPU	Memory	Heap	
Administrator@AE-Demo-Seema	Standard	0	0	Stopped				[Edit] [Stop] [Start]
seemak@LPT-0782	Standard	0	0	Running	5.37%	58.40%	7.28%	[Edit] [Stop] [Refresh]

Figure 74j: Controlled Agent is running

17. You may stop using the stop icon. A pop up is displayed to confirm Stop operation.



Agent Name	Mode	Assigned Workflows	Active Workflows	Status	Resource Utilization			Actions
					CPU	Memory	Heap	
Administrator@AE-Demo-Seema	Standard	0	0	Stopped				[Edit] [Stop] [Start]
seemak@LPT-0782	Standard	0	0	Running	5.73%	58.70%	11.72%	[Edit] [Stop] [Refresh]

Figure 74k: Stop Remote Agent

18. In this case it displays Stopping Agent is in Progress. When a running Agent is stopped the RDP session is also logged out.

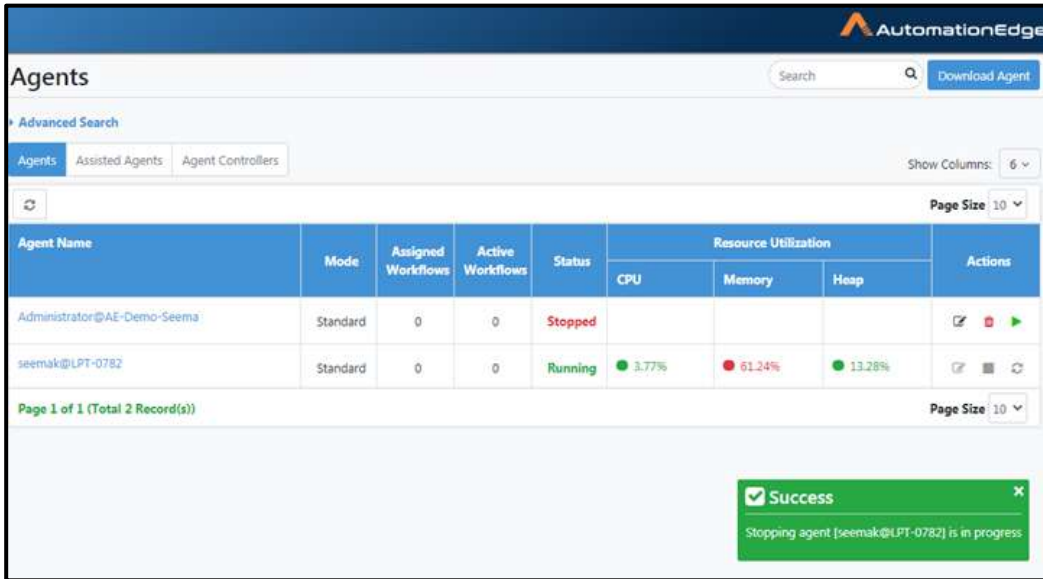


Figure 74l: Stopping Remote Agent Message

19. The snapshot below displays that the first agent in the list is stopped.

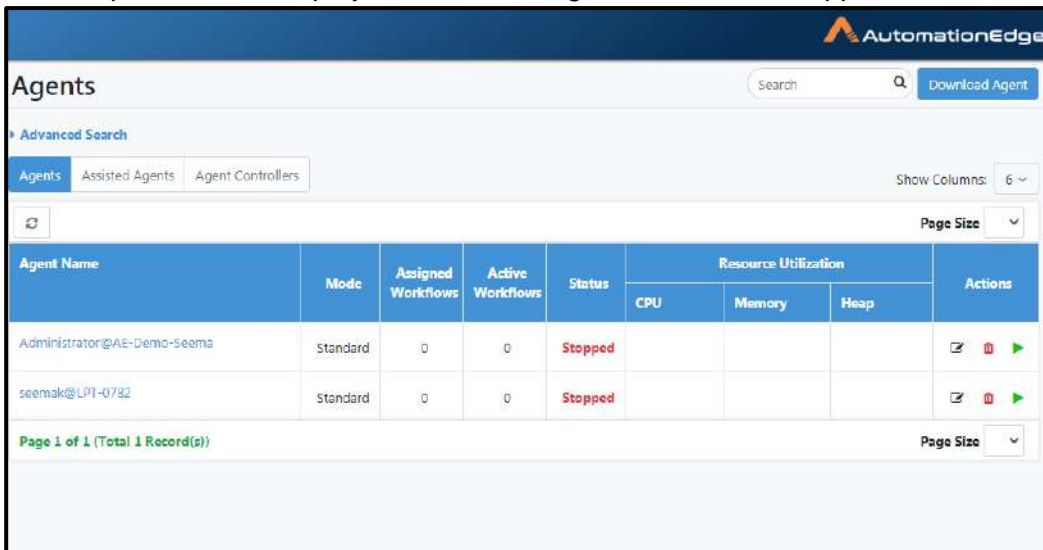


Figure 74m: First Agent is stopped and start icon is visible

7.6 Agents: Workflow Assignment

Using Workflow Assignment menu, you can assign and edit workflows assignment to agents.

To assign a workflow to an agent using Workflow Assignment:

1. Navigate to Agents → Workflow Assignment menu.
2. By default, the Agents tab is selected.

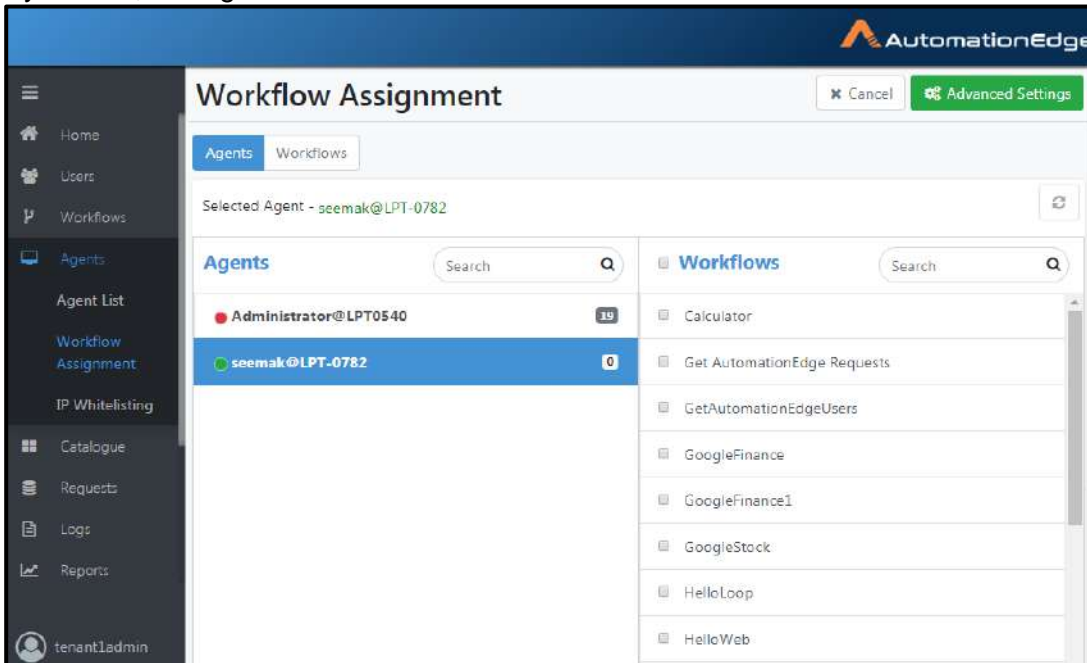


Figure 65a: Assigning Workflows to Agent

3. Scroll or Search for Workflows on the right-hand side column of the page. Enable or disable checkbox for workflows to be assigned to the Agent.
4. Enable checkbox next to two workflows – HelloWebGeneric2 and HelloWorld as seen below.

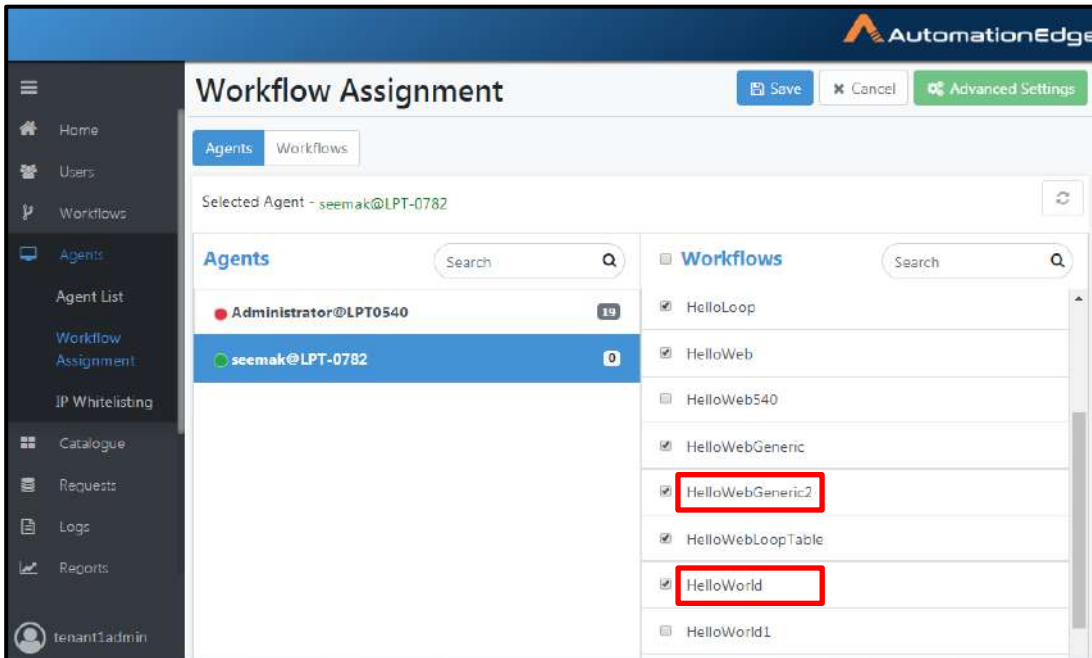


Figure 65b: Selecting Workflow to be assigned to an Agent

5. Click Save to save the assigned workflow to an agent.

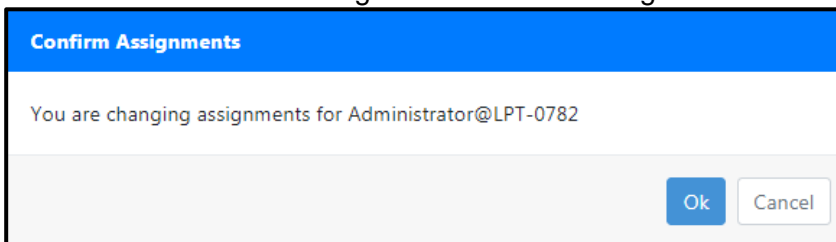


Figure 65c: Workflow Assignment Confirmation Box

- Assignment saved successfully message appears.

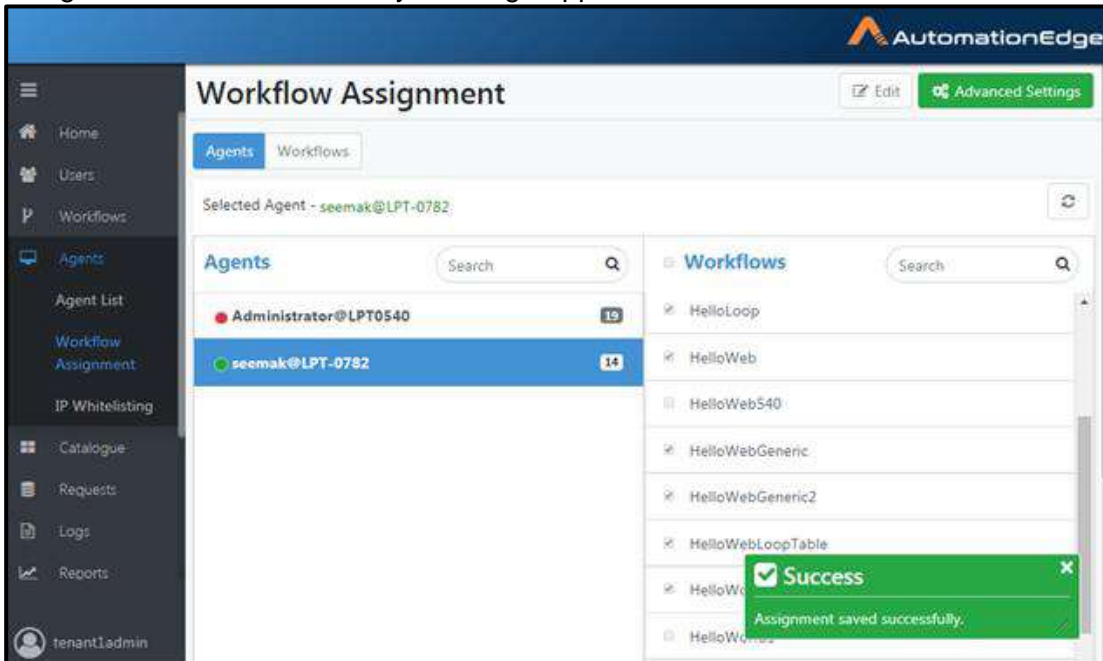


Figure 65d: Assigning Workflow to an Agent Using Workflow Assignment

- Similarly, you can go to the Workflows tab, next to the Agents tab. Select Agents on the right-hand column for the workflow selected on the left-hand column.

Note: In order to run an assisted Workflow, User just needs to get execute permissions on that Workflow. It is not required to assign such Workflow to any Agent.

- This completes the process of workflow assignment to Agent(/s).

7.6.1 Import Agent Assignments

This option is used for assigning all the workflows of one agent to another agent.

To assign a workflow to an agent:

1. Navigate to Agents→Workflow Assignment menu.
2. Click Advanced Settings Button on top right corner.

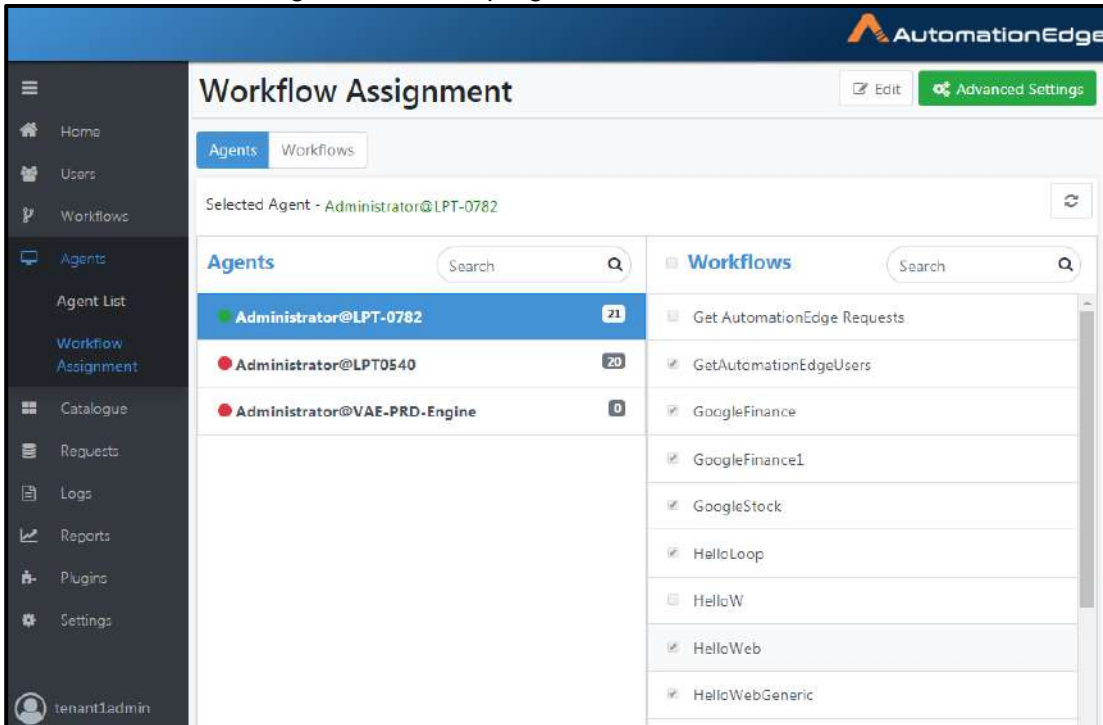


Figure 66a: Advanced Settings

3. An Import Assignment screen appears.

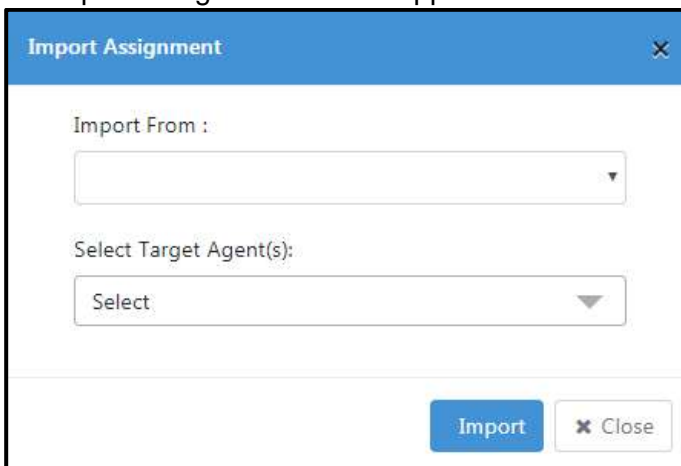


Figure 66b: Source and Target Agents

4. Click Import from drop down list and select an Agent to import from.
5. Select agent from the drop-down of Select Target Agent(s).

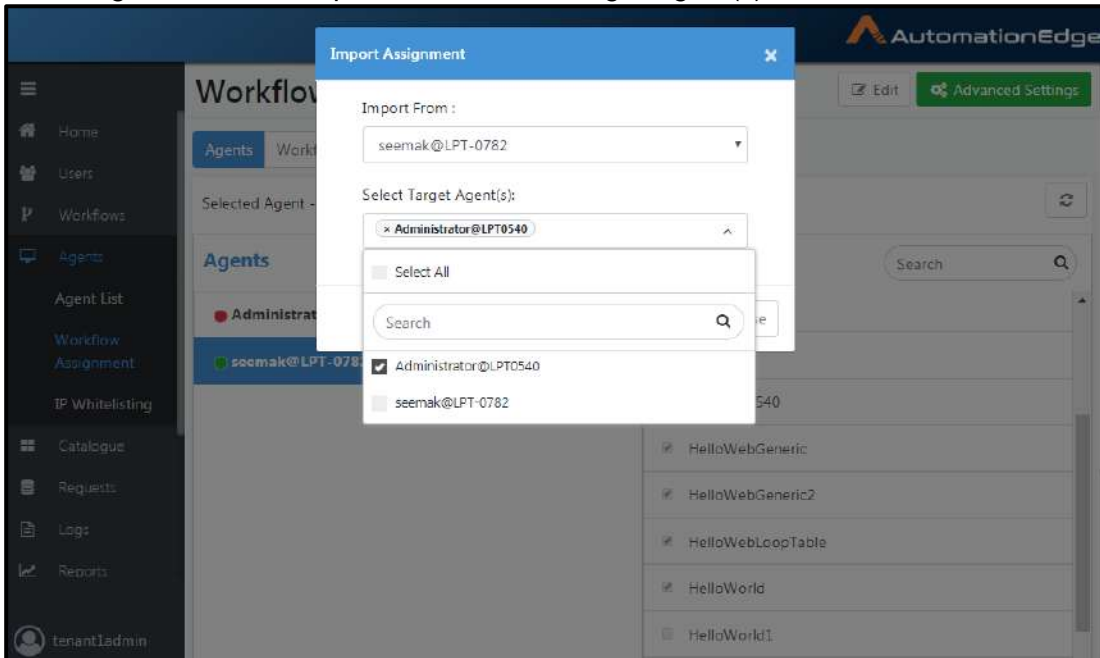


Figure 66b: Select Agent

6. The Import Assignment is seen below.

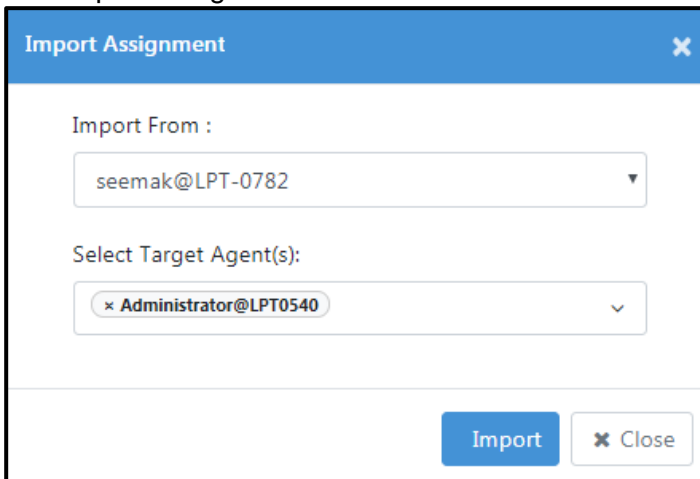


Figure 66c: Import Assignment

7. Click Import. Notice the Operation successfully completed message.

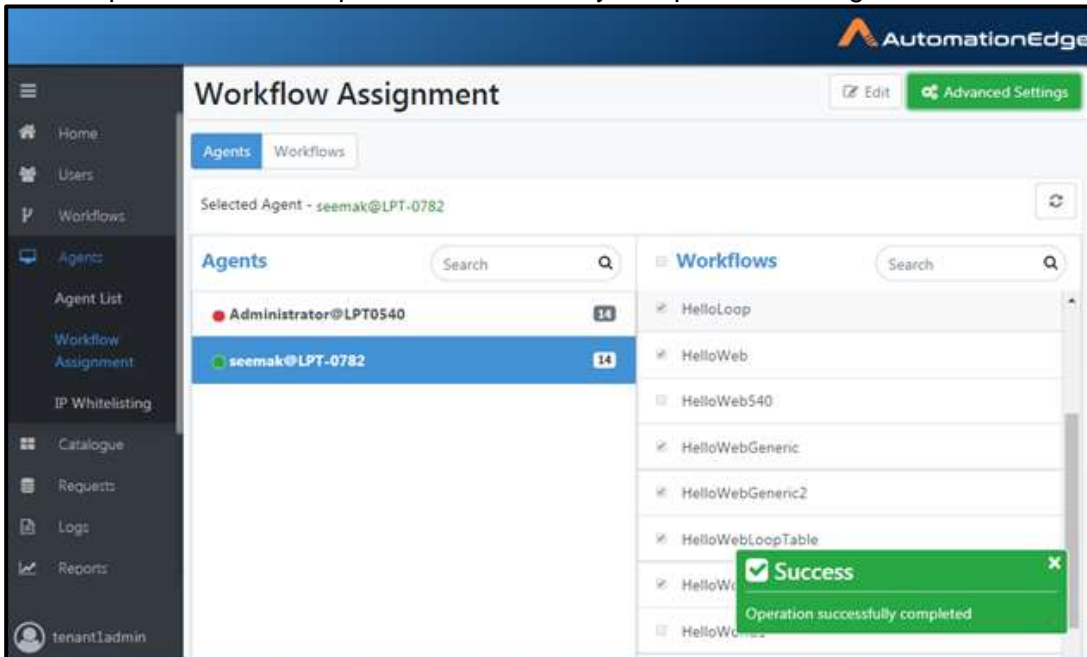


Figure 66d: Agent Import Successfully Completed

Following is a table to describe the fields for Select Target Agent(s).

Table 43: Agent Configuration Field Description

Field Name	Description
Select Agent(s)	To select an agent from the drop-down list.
Select all	To select all the agents in the drop-down list.
Deselect all	To deselect all the selected agents in the drop-down list.
Import From	To select location from the drop-down list for importing agents.
Save Button	To save agent configuration.
Reset Button	To clear the selected details of the agent.

7.7 Agents: Controller Assignment

Controllers can start Agents assigned to them. The Actions column on the Agents menu has an icon to Start Agents but is disabled by default. Assign Agents to one or more Controllers to enable the Start icon.

If an Agent is assigned to more than one Controller, then any idle Controller can start the Agent. Deleting an Agent Controller deletes all its Agent assignments.

A well planned Agent assignment to Controllers acts as a load balancer to balance the load on Controllers. It also serves security purposes by restricting Agent access to the designated Controllers.

From the Controller Assignment menu, assign and edit,

- Agents to a Controller or
- Controllers to an Agent

1. Navigate to Agents → Controller Assignment menu.
2. By default, the Agents tab is selected. Select an Agent from the list.
3. Click the Edit button on the top right corner.

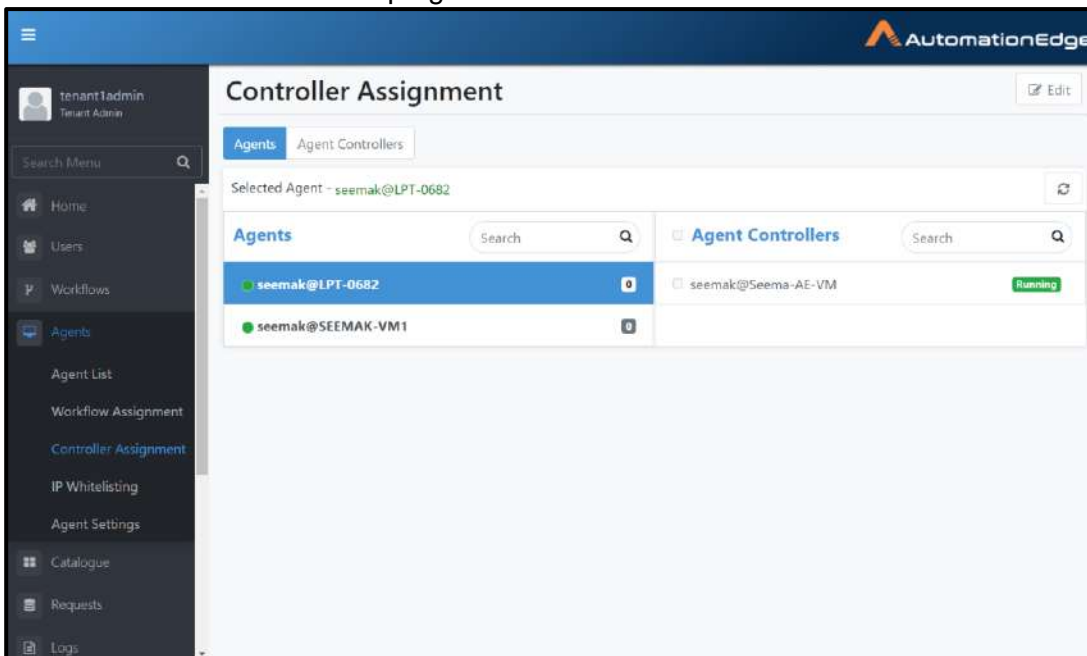


Figure 65a: Assigning Workflows to Agent

4. Select one or more Agent Controllers by enabling the checkboxes in the Agent Controllers column on the right.

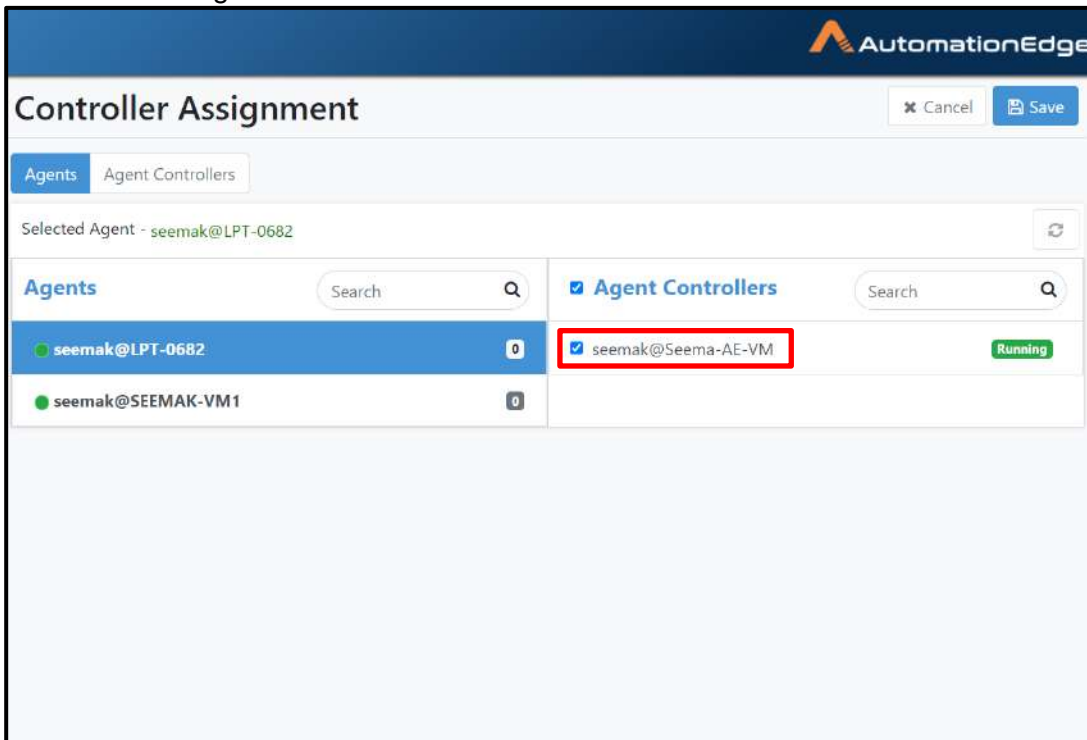


Figure 65b: Selecting Controllers to be assigned to an Agent

5. Click Save to save the assigned Controllers to an Agent.



Figure 65c: Workflow Assignment Confirmation Box

6. Assignment saved successfully message appears.

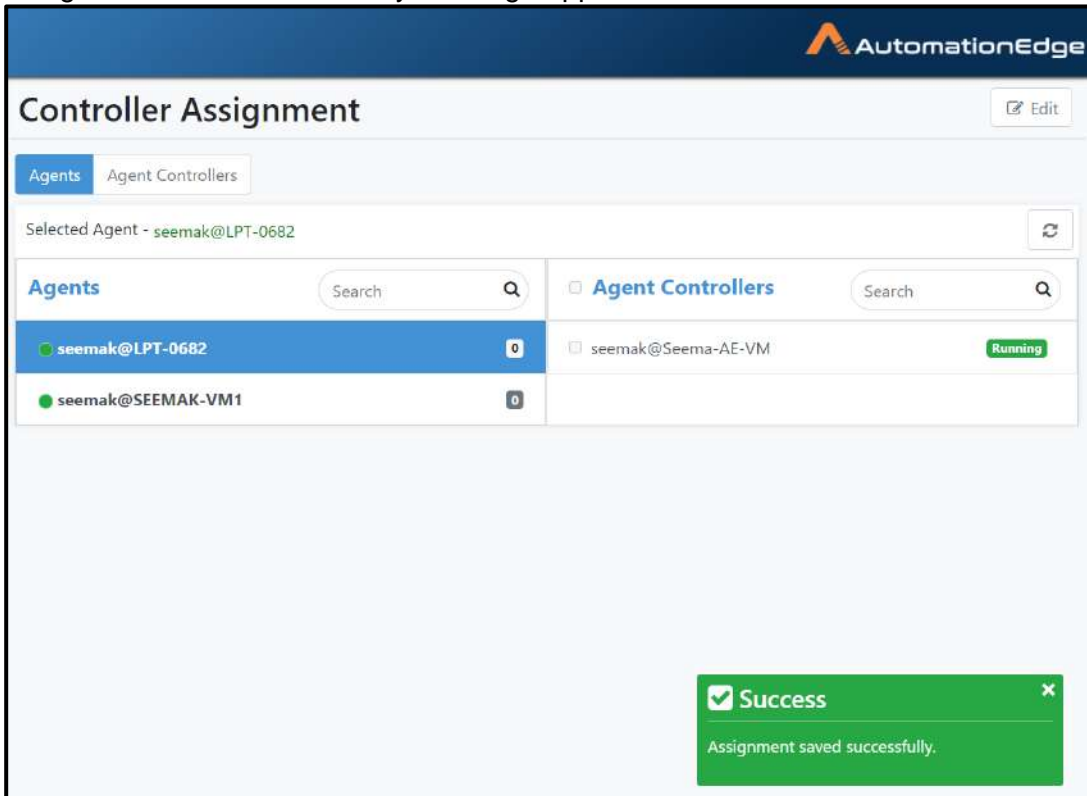


Figure 65d: Assigning Workflow to an Agent Using Workflow Assignment

7. Similarly, go to the Agent Controllers tab next to the Agents tab, select a Controller and assign Agents to it by selecting them from the right column.
8. The the process of Agent(/s) assignment to Controller(/s) is complete.

7.8 Agents: IP Whitelisting

Agents IP whitelisting allow Agents only from a certain set of IP Address to talk to AE Server. This feature is available at Tenant level (the default behavior allows Agents from any IP Address to talk to AE).

IP Whitelisting under Agents is used for Adding/Modifying/Listing/Deleting whitelisting's.

1. There are three options for whitelisting. By,
 1. IP
 2. IP Range 192.168.0.0 to 192.168.0.100
 3. CIDR Notation, e.g. 192.168.0.1/24 or 192.168.0.0/16
2. A Tenant Administrator can create multiple whitelisting.
3. Migration from Previous Versions:
 - ✓ During Server migration for each of the tenants (other than SYSADMIN Tenant) that are present for migration, white listings will be added as follows,
 - 0.0.0.0/0
4. Source IP Validations are done at the following level,
 - ✓ Agent Registration: The Source IP Address is verified on Agent registration. During agent registration, If IP whitelisting is specified for the Tenant, AE Server verifies the Source IP Addresses against this list. If the verification fails, Agent registration fails.
 - ✓ Agent Start up: The Source IP Address is verified on Agent Start up. If the Agent Source IP Address validation fails against the Agent IP Whitelisting list, then start-up fails.
 - ✓ Thirdly, the Source IP is also validated per day for the first call.
5. The following screenshot shows the default IP whitelisting.



Figure 74a: Default IP Whitelisting

7.9 Agent Settings

In Agent Settings you can enable a setting to Include JRE with Agent. Once Include JRE with Agent is enabled Agent is bundled with JRE when downloaded. There is no need to separately install JRE on Agent machine. You may also configure Agent machine remote port.

Following are the steps to configure Agent Settings,

1. Navigate to Settings→Agent Settings. Click Edit button.

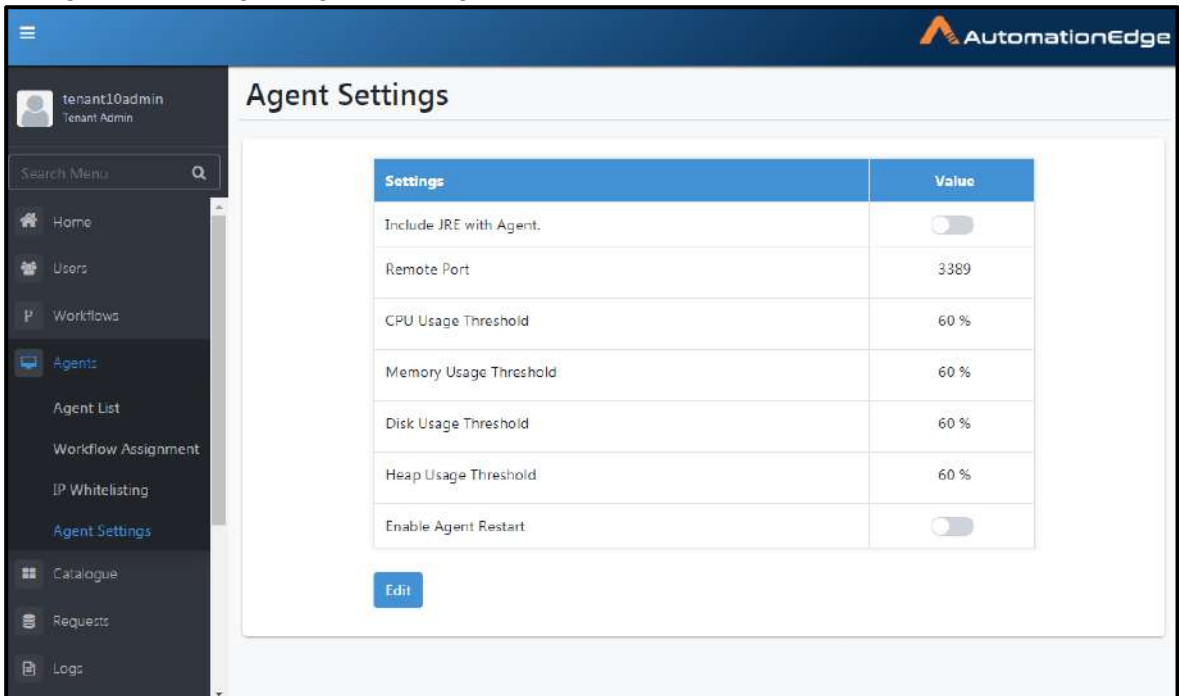


Figure 74b: Edit Agent Settings

2. Each of the Agent Settings is explained in the table below.

Setting	Explanation
Include JRE with Agent	This is set using a toggle switch. Click to include JRE with Agent during download.
Remote Port	RDP connects to Agent on this port. The default value is 3389.
CPU Usage Threshold	Configure the thresholds for CPU Usage after which notifications are sent. The default value is 60%.
Memory Usage Threshold	Configure the thresholds for Memory Usage after which notifications are sent. The default value is 60%.
Disk Usage Threshold	Configure the thresholds for Disk Usage after which notifications are sent. The default value is 60%.
Heap Usage Threshold	Configure the thresholds for Heap Usage after which notifications are sent. The default value is 60%.
Enable Agent Restart	This is set using a toggle switch. Click to enable Agent Restart. Note: Agent restart features in not supported on Linux based OS

Agent Restart Time	Schedule an Agent Restart Time if Agent Restart is enabled. The restart time can be configured at Tenant level in this menu, or individual agents by editing Agent in the Agent List menu.
--------------------	--

3. Edit the settings as desired. Click Save. When settings are changed, the settings come into effect next time the agent requests for workflows from the Server.
4. For any update in the setting here at the Tenant level or at the Agent level in Agent List menu Audit logs are maintained.

Settings	Value
Include JRE with Agent.	<input checked="" type="checkbox"/>
Remote Port	<input type="text" value="3389"/>
CPU Usage Threshold	<input type="text" value="60"/> %
Memory Usage Threshold	<input type="text" value="60"/> %
Disk Usage Threshold	<input type="text" value="60"/> %
Heap Usage Threshold	<input type="text" value="60"/> %
Enable Agent Restart	<input checked="" type="checkbox"/>
Agent Restart Time	<input type="text" value="00"/> : <input type="text" value="00"/>

Save Cancel

Figure 74c: Edit Agent Settings at Tenant Level

1. Agent Settings Updated Successfully message appears.

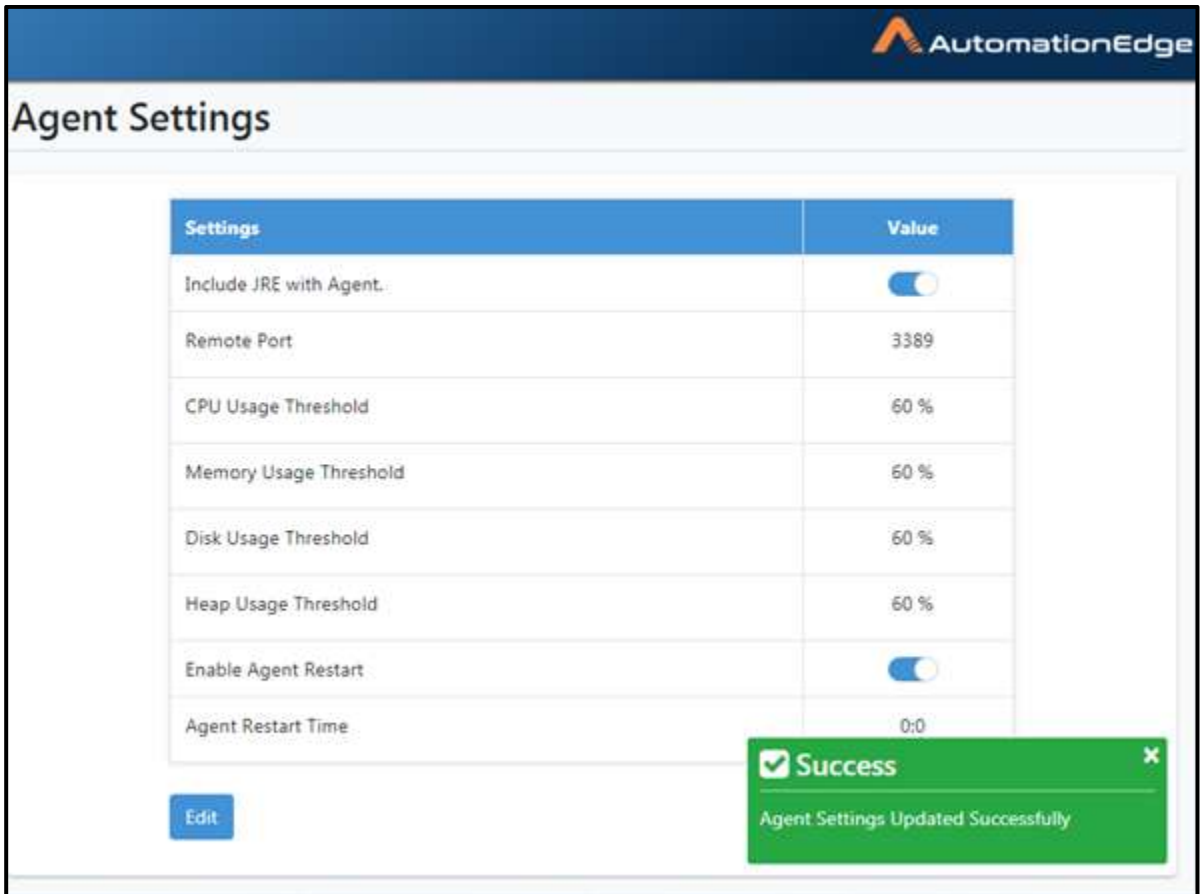


Figure 74d: Agent Settings updated successfully

7.10 Agents: Features/Permissions for other users

Table 45: Agents' features

Feature/Role	Tenant Administrator	Workflow Administrator	User Administrator	Agent Administrator	Tenant User	Activity Monitor
View Agent	✓	-	-	✓	-	✓
Download Agent	✓	-	-	✓	-	-
Workflow Assignment	✓	-	-	-	-	-
Agent Import	✓	-	-	-	-	-
Assisted Agent	✓	✓	✓	✓	✓	✓
Controller	✓	-	-	✓	-	-

8 Catalogue

Catalogue is used for submitting workflow requests.

Note that a user will see only those Workflows/Assisted Workflows on which they have Execute permissions.

8.1 Submit Request

To submit the request:

1. Click Catalogue. Select a category from which you want to submit a workflow. All the workflows in that category appear.
2. Click on a workflow tile to submit a request. It opens a parameters dialog, if there are any runtime parameters. Provide the parameter values and Click on the Submit button.

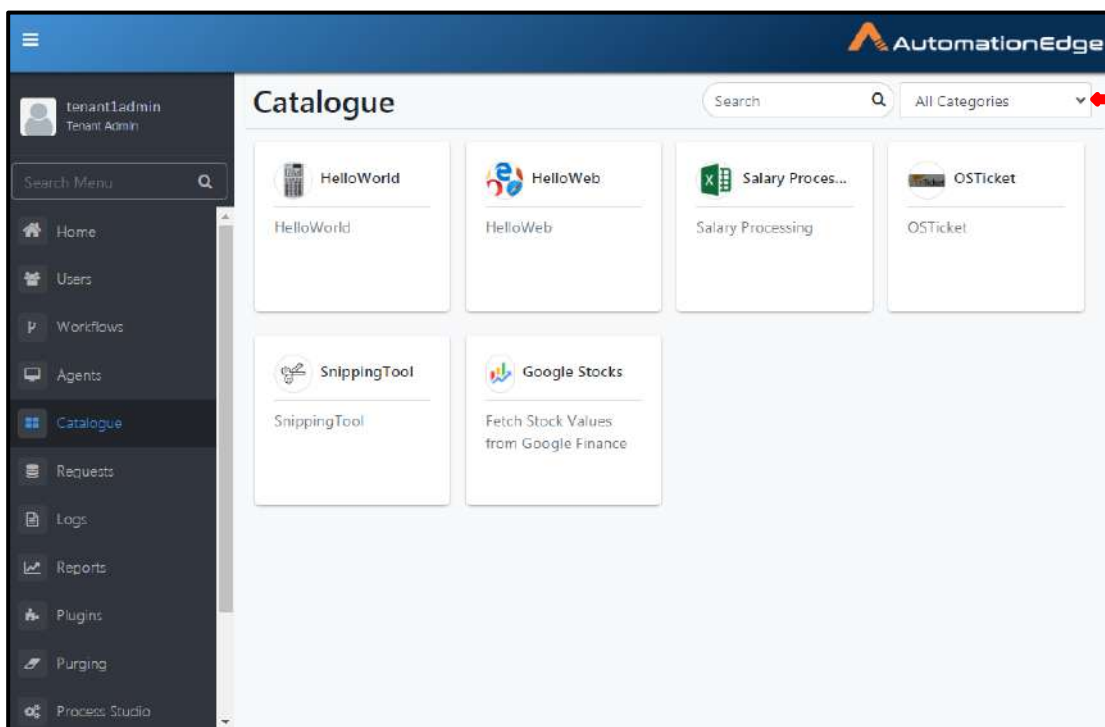


Figure 75a: Selecting a Request from Catalogue

A description of the fields is provided in the table below.

Table 46: Catalogue Field Description

Field Name	Description
Search	To search service requests.
Category List <ol style="list-style-type: none"> 1. Default 2. All Categories 	<p>Catalogue displays workflow tiles depending on the category selected.</p> <p>Displays all the Requests if All Categories is selected.</p>

8.2 Request details

Click a workflow tile on the Catalogue; if the workflow has runtime parameters it displays the Request Details dialog.

If there are considerable number of parameters on an AutomationEdge UI - Request Submission page can be cumbersome for users to handle while submitting the request. Simplify parameter handling by grouping parameters in Process Studio. Refer to section Parameter Configuration in AutomationEdge_R7.0.0_ProcessStudio_User_Guide for more details.

1. Parameter Groups in workflow/process in Process Studio, are also reflected on AutomationEdge UI Request details dialog.
2. Expand or collapse the groups as required, by clicking the + sign next to the group; provide values and submit the request.

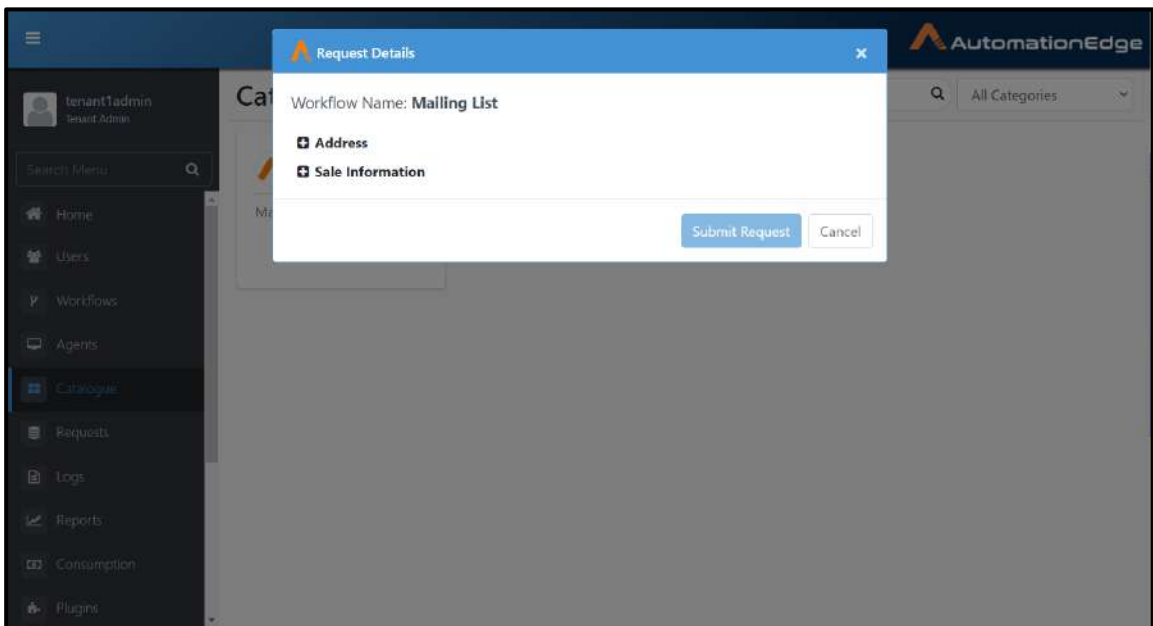


Figure 75b: Request details parameter form with groups

3. Expand the Address Group, it has two subgroups and a parameter.

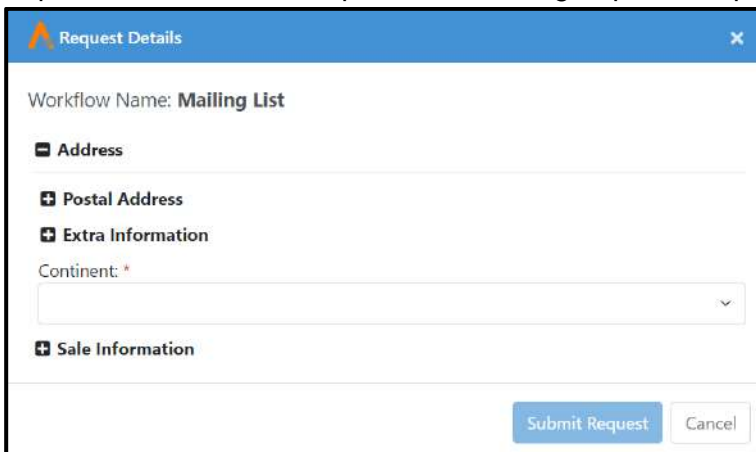
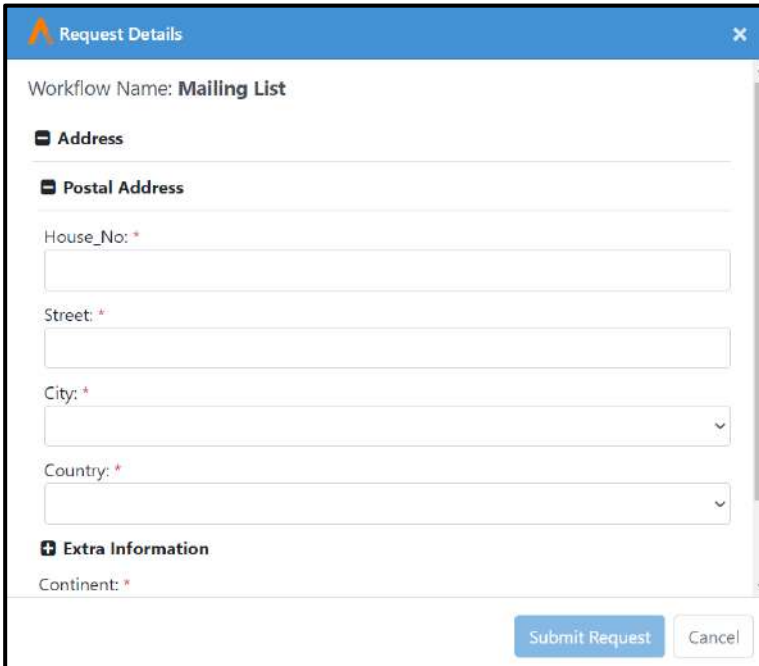


Figure 75c: Sub groups

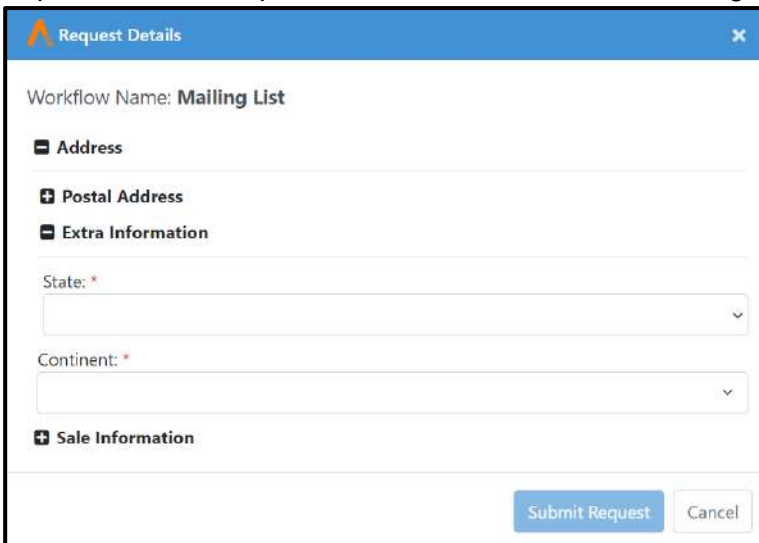
- Expand to view the parameters of the Postal Address group.



The screenshot shows a 'Request Details' window for a workflow named 'Mailing List'. The 'Address' group is expanded, revealing the 'Postal Address' sub-group. This sub-group contains five required fields: 'House_No', 'Street', 'City', and 'Country', each with a text input field, and 'Continent', which is a dropdown menu. At the bottom right, there are 'Submit Request' and 'Cancel' buttons.

Figure 75d: Parameters in a group

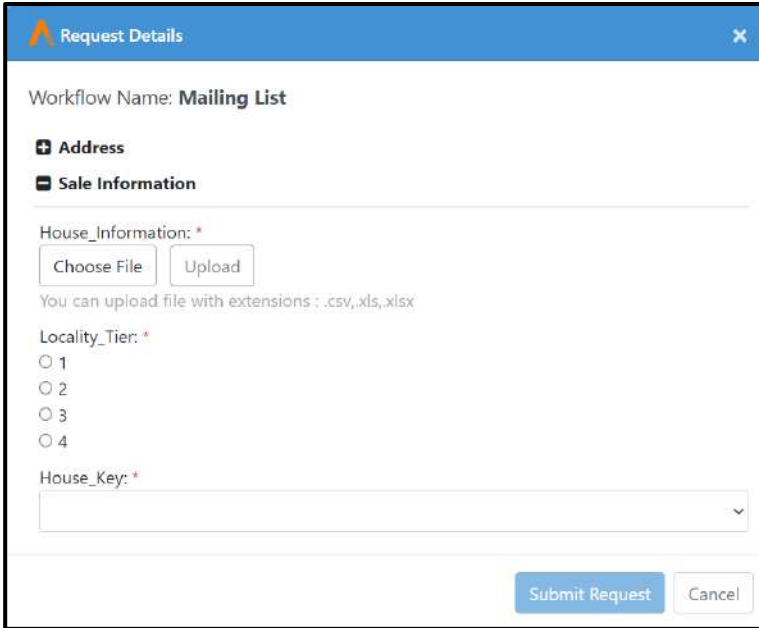
- Expand to view the parameters of the Extra Information group.



The screenshot shows the same 'Request Details' window. The 'Postal Address' group is collapsed, and the 'Extra Information' group is expanded. This group contains two required fields: 'State' and 'Continent', each with a dropdown menu. Below this, the 'Sale Information' group is visible but collapsed. The 'Submit Request' and 'Cancel' buttons remain at the bottom right.

Figure 75e: Parameters in a group

- The following screenshot shows an expanded view of the Sale Information group



Request Details

Workflow Name: **Mailing List**

+ Address

- Sale Information

House_Information: *

Choose File Upload

You can upload file with extensions : .csv, .xls, .xlsx

Locality_Tier: *

1

2

3

4

House_Key: *

Submit Request Cancel

Figure 75f: Parameters in a group

7. This section showcased the Request submission details with parameters and parameter groups.

8.3 Catalogue: Features/Permissions for other users

Table 47: Catalogue Features

Feature/Role	Tenant Administrator	Workflow Administrator	User Administrator	Tenant User	Activity Monitor
Catalogue to view and execute Requests	✓	✓	-	✓	-

*Tenant users can view and execute Requests depending Execute permissions granted to them on workflows.

8.4 Features to improve efficiency of Requests

A number of features are available that can be used to improve information on Requests and improve efficiency of requests.

8.4.1 Notification Options

Several Email Notifications Options depending on Request status can be configured. The configuration details are provided in section 13.4(Settings: Email Notifications).

8.4.2 Cleanup Old Request older than H number of hours

Mostly in case of scheduled requests when one cycle of requests is missed, the next request takes care of the work/tasks which earlier requests can/would do. It can make sense to clean up the requests which are older than 'H' numbers of hours. The 'H' can be 24 hours, 120 hours or anything based on the Use Case that the Workflow is handling. Requests remaining in New state older than 'H' number of hours will be cleaned up and marked as Expired. Expired Requests are also added to Audit logs.

There is a workflow specific setting for this, which can regulate time after which the workflow request will be cleaned. This is shown in the section Add/Update Workflow-Enter Basic Details.

A System level setting for clean-up hours is also available. The Sysadmin can set this which will be applicable for all workflows (Refer Settings section in System Administrator Guide). If workflow also has clean up hours specified, then preference is given to smaller value between the two.

9 Requests

This Requests menu shows a list of all the submitted workflow execution requests (latest on the top). You can also see details of these requests.

Note: A user can only see those requests to which the user has access.

9.1 Viewing Request Details

The status of submitted requests can be viewed from the requests menu.

1. From the Columns field on the extreme right you can choose the columns to see.
2. Three navigation options are available at the top and bottom of the Request Details section. Size field can be used to select the number of rows per page. There is a field for the page number and a total number of pages. You can directly provide the page number you wish to go to. Also there are scrolling options for First Page, Last Page, Previous Page and Next Page as shown in the figure below.
3. Request details (Id, Workflow Name, Status, Agent name, Source, Source ID, Submitted By, creation and completion times as well as six additional output attributes (Attribute1 to Attribute6) and six additional input attributes (Input Attribute1 to Input Attribute6)) can be viewed. Output Attributes can be mapped to workflow output parameters and Input Attributes can be mapped to workflow input parameters. Input Attribute 1 has been mapped to Remedyforce Service Request ID.

Id	Workflow Name	Status	Agent Name	Created	Completed
6	HelloWorld	Complete	Administrator@VAE-PR...	21-Jul-2020 20:36:28	21-Jul-2020 20:37:54
5	HelloWebGeneric	Complete	Administrator@VAE-PR...	21-Jul-2020 17:31:30	21-Jul-2020 17:31:54
3	StockValues - Notepad			21-Jul-2020 10:55:18	21-Jul-2020 10:55:37







```

Message: Execution Successful
StockValues.txt: Click here to download the file

File: Edit: Format: View: Help
Company Name: Stock Symbol: Stock Value
Alphabet Inc. : NASDAQ: GOOGL:1,563.84
Infosys Ltd. : NYSE:INFY :12.58
Samsung Electronics Co Ltd: KRX:005930 :55,300
  
```

Figure 76a: Viewing Request Details

Table 48: Viewing Request Details Field Description

Field Name	Description
ID	Displays request ID number.
Workflow Name	Displays workflow name.
Status	<p>Displays request status along with message description (Message description appears when  is clicked. Message description appears and remains expanded even if user navigates to another menu. It disappears only when  is clicked).</p> <p>AutomationEdge has a set of states of a workflow like “New”, “Execution Started”, “Complete”, “Diverted” and “Failure”. The status can also be “Expired” or “Terminated”.</p> <p>In addition, a user defined Intermediate message can also be set in case of long running workflows using ‘Intermediate Status Step’ as described below in the section Elaboration of Status below.</p> <p>If a workflow is in Failure Status, there is a restart icon () next to the () icon. This is elaborated in the section “Manual Restart of Request/Workflows” below.</p> <p>If a workflow is in Execution Started Status there is a Terminate icon () next to the () icon. This is elaborated in the section “Manual Termination of Request/Workflows” below.</p> <p>Note: Workflow is not marked as failure if output file upload fails from agent onto Server. It considers the result received from workflow execution.</p>
Agent Name	Displays name of the agent.
Source	<p>Displays request source from where the request is received.</p> <p>Note: If the Request is triggered by scheduler Source column displays ‘Scheduler: <schedule name>’</p>
Source ID	
Submitted By	Displays the name of a person who has submitted the request.
Created	Displays request creation date & time.
Completed	Displays request completion date & time.
Attribute1	<ul style="list-style-type: none"> Any extra workflow information can be retrieved in these six Attribute columns provided.
Attribute2	
Attribute3	
Attribute4	

Field Name	Description
Attribute5	<ul style="list-style-type: none"> These values can be set from the 'Set Workflow Result' step in the 'AutomationEdge Core' category in Process Studio workflows. The values of these attributes can be set from in-stream field, variable or as a constant.
Attribute6	
Input Attribute1	<ul style="list-style-type: none"> Input Attributes can be mapped to input parameters (e.g. ITSM systems: Remedyforce "task id" Remedy, "workorder id" or any other Source /Target System) Input Attribute 1 is mapped to Remedyforce Service Request ID
Input Attribute2	
Input Attribute3	
Input Attribute4	
Input Attribute5	
Input Attribute6	

9.1.1 Elaboration of Request (/Workflow) Status

9.1.1.1 New

If a Request is yet to be picked up by an Agent the Request status is set as New.

9.1.1.2 Execution Started

If the request has been picked up by an Agent the status is set as 'Execution Started'. The Current State of running Workflows can be further elaborated by setting one or more intermediate status in workflows.

9.1.1.3 Diverted

The Request status can be set as diverted using Set Workflow Result workflow step or process entry. This is for requests that have to be diverted outside AutomationEdge as the issue is beyond the purview of AutomationEdge.

9.1.1.4 Complete

If the workflow completes Request Status is set as Complete.

9.1.1.5 Failure

AE workflow may fail due to various reasons. Workflow Failure Reasons of failures can be broadly categorized into a few categories which may help the user with better understanding and reporting.

These failure categories are not visible on UI but can be seen in Failure description.

Following are a set of predefined failure reasons:

1. License Expired
2. Invalid Request parameters
3. Invalid Credentials (expired etc.)
4. Invalid Workflow Definition
5. Agent Stopped/Restarted

6. Failed to connect to an external system
7. Authentication to external system failed
8. Workflow failed due to internal reason
9. Error while uploading/downloading file with server
10. Unknown reason

Table 49: Common Workflow Failure Reasons and System Response

No.	Workflow Failed Due to:	Failure reason:
1	License/Subscription expired	Workflow can be marked with the reason (1).
2	Invalid workflow parameter values, values that are not allowed	Workflow can be marked with reason (2).
3	Credential/Credential Pool deleted which is in use	Workflow can be marked with the reason (2).
4	Credential has expired which is in use	Workflow can be marked with the reason (2).
5	Resources not found at the location as specified in "resourceFolderPath" attribute in manifest	Workflow can be marked with the reason (4).
6	Manifest parameters updated/removed	Workflow can be marked with the reason (4).
7	Manifest action removed	Workflow can be marked with the reason (4).
8	Execution/CheckStatus Script names modified or removed	Workflow can be marked with the reason (4).
9	Workflow marked as failure because of agent stopped/restarted while running workflow	Workflow can be marked with the reason (5).
10	Workflow could not connect to external system due to network or other error	Workflow can be marked with the reason (6).
11	Authentication to external systems failed	Workflow can be marked with the reason (7).
12	Process Studio Workflow failed	Workflow can be marked with the reason (8).
13	Could not download input file from AE server from Agent (URL in agent.properites is wrong)	Workflow can be marked with the reason (9).
14	Could not upload output file onto AE server from Agent (URL in agent.properites is wrong)	Workflow can be marked with the reason (9).
15	Workflow failed due to unknown/unexpected reasons	Workflow can be marked with the reason (10).

9.1.1.6 Expired

This status is applicable for requests that are not picked up by an Agent for execution and the status remains as New. Such requests are subject to 'cleanup requests' execution after elapse of a number of hours as set in the workflow configuration or in System Settings for sysadmin user. Such Requests are marked as 'Expired'.

9.1.1.7 Terminated

Requests manually terminated by Tenant Administrator or Workflow Administrator in case of long running requests are marked with status 'Terminated'. This is elaborated in the section "Manual Termination of Request/Workflows" below.

9.1.1.8 Intermediate Status

The following feature can also be used. If a workflow runs for a long duration, then there is no information on the server regarding the state of a running workflow. In this case Process Studio step "Intermediate Status" can be used to send the intermediate status of a workflow to AE Server. The step has a free textbox where user can set the status like % of completion or any other user defined status. This status is also displayed on the UI in addition to the six states mentioned in the table above.

9.1.2 Manual Restart of Requests/Workflows

For all the failure reasons, manual restart of a workflow is allowed. A workflow can be restarted only if it is in the failure state.

When running again, the workflow will take the same runtime parameters. If configuration parameters values are changed between failure and restart, it will take updated configuration parameters while restart. It will run with the same instance id as before.

Workflow can be restarted if,

- It has failed
- It's in enabled state
- It's not modified after the failure

9.1.3 Manual Termination of Requests/Workflow

Manual termination of Requests/Workflows is a mechanism to terminate long running or stuck workflows manually. Termination option will be available once the expected execution time has lapsed.

This option is to terminate the workflow once the workflow execution is started on the agent. On the "Requests" page, there will be a button to execute this feature. Once clicked, it will send a signal to the agent to terminate the corresponding workflow.

TENANT_ADMIN and WORKFLOW_ADMIN users have access to terminate all the workflows of their tenant. Request owner (TENANT_USER) has access to terminate its own workflows.

This feature is enabled only when a workflow is in 'ExecutionStarted' state.

Note: Some steps/entries might remain in "Halting" state even if the workflow's main process is terminated.

9.1.3.1 Manual Termination of Requests: Use Cases

Table 50: Use Cases for Manual Termination of Requests

User Action	Conditions	System Response
Workflow termination is invoked	Workflow is in state other than "ExecutionStarted"	API will return error message
Workflow termination is invoked	Workflow is in "ExecutionStarted" state	Workflow's main process will be terminated
Workflow termination is invoked	Workflow has Audit log steps used.	Audit logs are uploaded on server and workflow's main process is terminated

9.2 Searching Requests

To search request:

1. Click Requests.
2. Click Advanced Search
3. Select a column from the drop down list to setup filter criteria. Setup one or more filters.
4. You will see the filtered records in the view.

The screenshot shows the AutomationEdge 'Requests' page. At the top right, there is a 'Download Requests' button. Below it, the 'Advanced Search' section is active, with a dropdown menu open for selecting a column. The dropdown menu lists various columns: Id, Workflow Name, Priority, Status, Source, Source Id, Agent Name, Submitted By, Created, Input Attribute 1 through 6, and Attribute 1 through 4. The main table below has columns: Name, Status, Agent Name, Created, and Completed. The table contains three rows of data, all with a 'Complete' status. The first row shows a request for 'Administrator@VAE-PR...' created on 21-Jul-2020 at 20:36:28. The second row shows a request for 'Administrator@VAE-PR...' created on 21-Jul-2020 at 17:31:30. The third row shows a request for 'Administrator@VAE-PR...' created on 21-Jul-2020 at 10:55:18. The table also includes 'Show Columns: 6' and 'Page Size: 10' controls.

Figure 77a: Searching Requests

- For sake of convenience Advanced Filter with column selection on Requests page is saved along with filtered records as a view. If an Advanced search is done on Requests Page in AutomationEdge UI and the current window is closed or reloaded, Requests page still shows filtered data and the Advanced Search filters are saved and shown above Requests table as a view.

Note: Advanced search options for Requests are explained below.

Table 51: Advanced Search Options by ID

Search by ID:	
Dropdown list	Description
Equal To	To search entries matching the entered text.
Not Equal To	To search entries not matching the entered text.
Less Than	To search entries with ID less than the entered text.
Greater Than	To search entries with ID greater than the entered text.
In Range	To search entries with ID in the range (From-ID to To-ID)
Not In Range	To search entries with ID not in the range (From-ID to To-ID)

Table 52: Advanced Search Options by Workflow Name, Status, Submitted By, Source, Source ID, Agent Name and six attributes as well as six input attributes:

Field	Description
Equal To	To search entries by the exact entered text.
Not Equal To	To search entries not matching the entered text.
Like	To search entries containing the entered text
Begins With	To search entries that begins with the entered text.
Ends With	To search entries that ends with the entered text.

Table 53: Advanced Search Options by Date

Field	Description
Exact Date	To search entries by the exact entered date.
Before	To search entries before the entered date.
After	To search entries after the entered date.
In Between	To search entries in between the entered dates.
Not In Between	To search entries not in between the entered dates.

Table 53: Advanced Search Options by Priority:

Field	Description
Equal To	To search entries by the exact entered text.
Not Equal To	To search entries not matching the entered text.

9.3 Download Requests

Use Download Requests Button to download request pages in csv format.

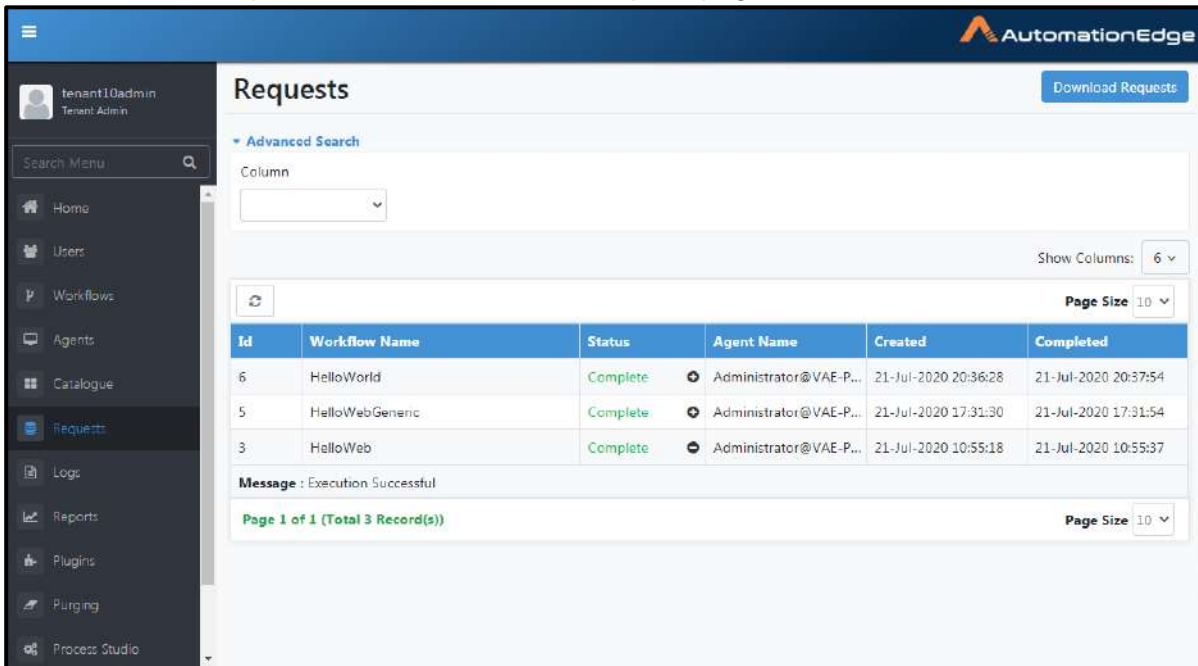


Figure 77b: Requests

On Clicking the Download Requests button a popup appears as below. Select the page number and click Download to download a csv file.

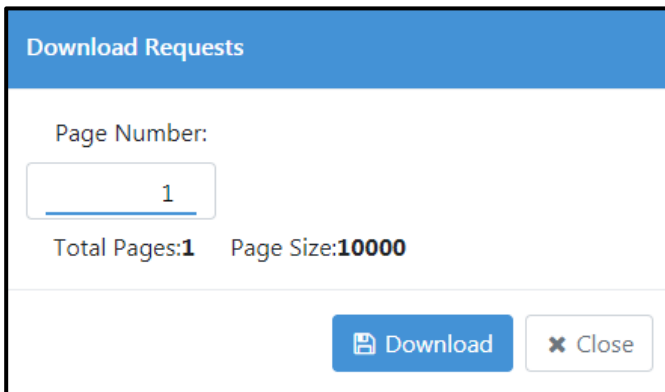


Figure 77c: Total Download Pages

9.4 Requests: Features/Permissions for other users

Table 54: Requests Features

Feature/Role	Tenant Administrator	Workflow Administrator	User Administrator	Agent Administrator	Tenant User	Activity Monitor
View Requests	✓	✓	-	-	✓	✓
Search Requests	✓	✓	-	-	✓	✓

10 Logs

In the logs menu we can see Agent Logs and Audit Logs

10.1 Agent Logs

Agent Logs is a menu option to download agent log files.

Agent logs can be downloaded by one or more agents along with dates or by Workflow request id.

10.1.1 Introduction

Agent log contains Agent or workflow execution logs as well as Process Studio step Debug Log's Debug Log messages. There is a workflow step in Process Studio called Debug Logs. When workflow request executes, it logs the Debug Log variables and fields and Debug Log messages. These debug messages are also present in agent logs.

Using, Agent Logs menu option users can download Agent log files which include debug logs from AE portal.

10.1.2 Working

AutomationEdge users can download agent logs by submitting one or more agent names with from and to dates. Users can also download logs for particular workflow instance. User can see all Agent log requests submitted on AE portal with their date criteria's and link to download the Agent log file.

Agent logs can be downloaded only for requests executed within the last 15 days. Logs for any request executed before that cannot be fetched. AE server keeps these requests for 24 hours after the link to download is active. User needs to download debug logs during that time.

10.1.3 Agent Logs: View

1. Go to the Logs menu and Agent Logs sub-menu.
2. You can view Agent Log files that may be downloaded .

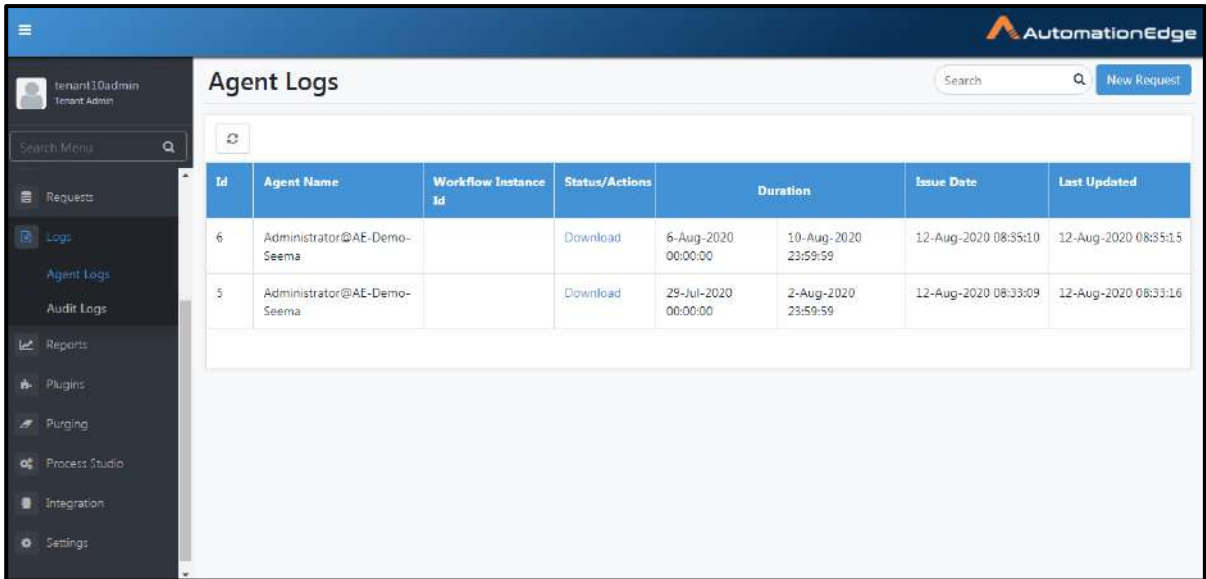


Figure 78a: Agent Logs

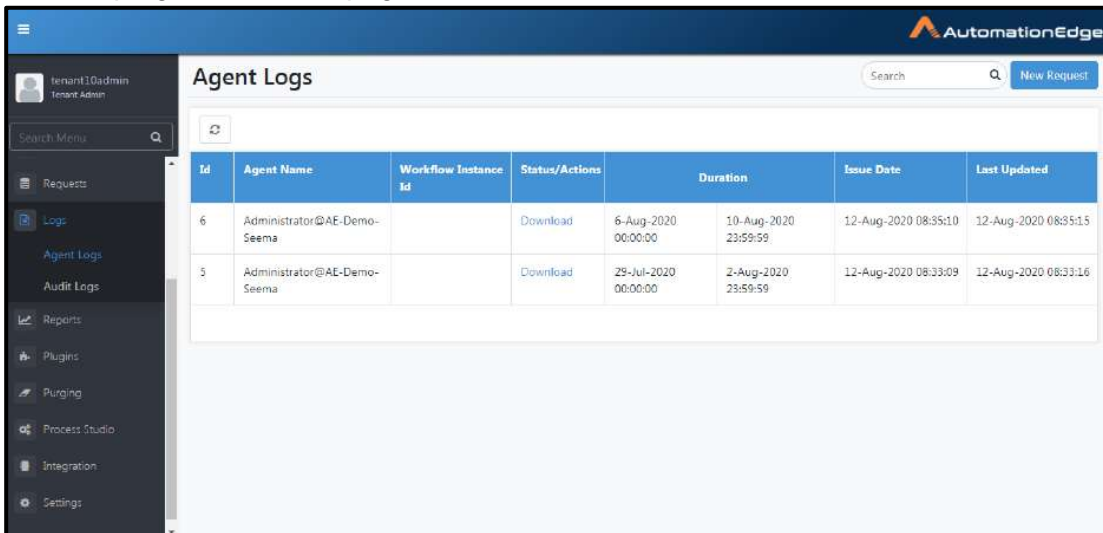
Table 55: Agent Logs Table

Component	Description
Id	A serial number is seen here.
Agent Name	The name of the Agent with which the Agent log file is associated.
Workflow Instance Id	This is id of workflow request submitted.
Status/Actions	The status of operation can be: New, In Progress, Complete, Failed. If Request is completes then a Download link is available to download the logs.
Duration:	The period for which the agent log file has been retrieved.
From Date	The start timestamp of the period.
To Date	The end timestamp of the period.
Issue Date	The timestamp of the request.
Last Updated	The timestamp when the request was last updated.

10.1.4 Agent Logs: Search

Provide a search string in the search box to filter Agent Logs by the search string.

1. At the top right side of the page there is a Search box.

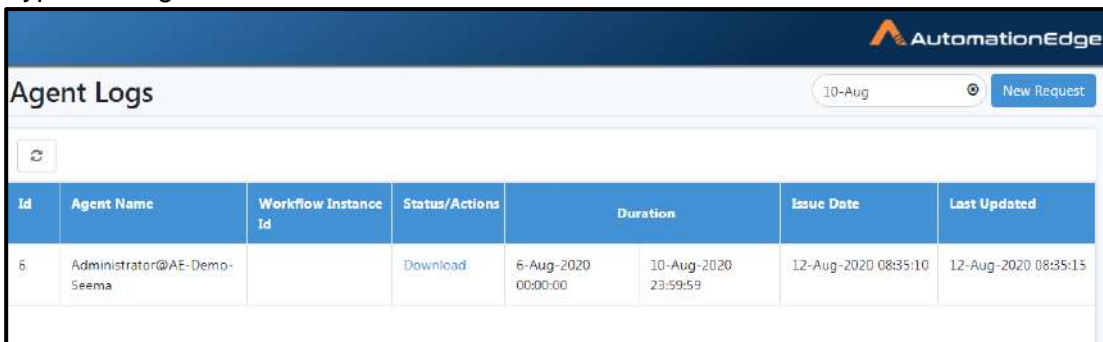


The screenshot shows the AutomationEdge interface. On the left is a navigation menu with options like Requests, Logs, Agent Logs, Audit Logs, Reports, Plugins, Purging, Process Studio, Integration, and Settings. The main area is titled 'Agent Logs' and contains a search box with a magnifying glass icon and a 'New Request' button. Below the search box is a table with the following data:

Id	Agent Name	Workflow Instance Id	Status/Actions	Duration	Issue Date	Last Updated
6	Administrator@AE-Demo-Seema		Download	6-Aug-2020 00:00:00	10-Aug-2020 23:59:59	12-Aug-2020 08:35:10
5	Administrator@AE-Demo-Seema		Download	29-Jul-2020 00:00:00	2-Aug-2020 23:59:59	12-Aug-2020 08:33:16

Figure 79a: Agent Logs Search

2. Type a string in the Search box. Notice that once record is now filtered out.



The screenshot shows the same AutomationEdge interface, but the search box now contains the text '10-Aug'. The table below it now only displays the record with ID 6, as the record with ID 5 has been filtered out.

Id	Agent Name	Workflow Instance Id	Status/Actions	Duration	Issue Date	Last Updated
6	Administrator@AE-Demo-Seema		Download	6-Aug-2020 00:00:00	10-Aug-2020 23:59:59	12-Aug-2020 08:35:10

Figure 79b: Filter Agent Logs

10.1.5 Agent Logs: Download

Agent Logs can be downloaded by,

- Agent or
- Request Id

Following are the steps to download Agent Logs,

10.1.5.1 Agent Logs: Download by Agent

1. Go to the Logs menu and Agent Logs sub menu.

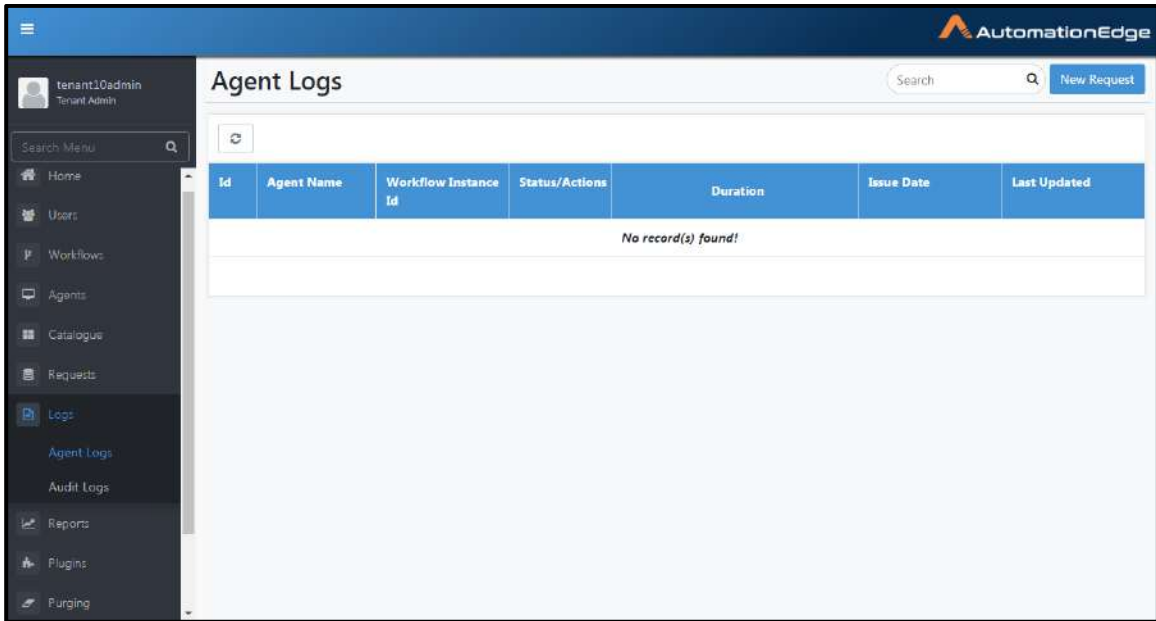


Figure 80a: Download Agent Logs

2. Click New Request on the top right corner. A pop-up box appears. You may submit a new request for Agent or Workflow Requests.

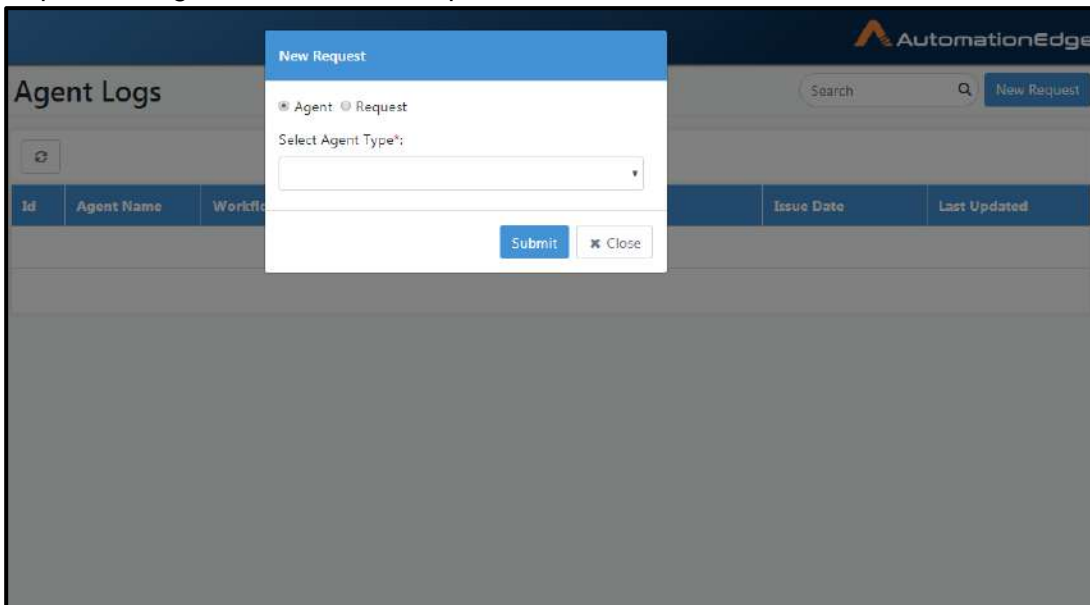


Figure 80b: Select Agent Log Entity

3. In this case Agent was chosen. Now select Agent Type.

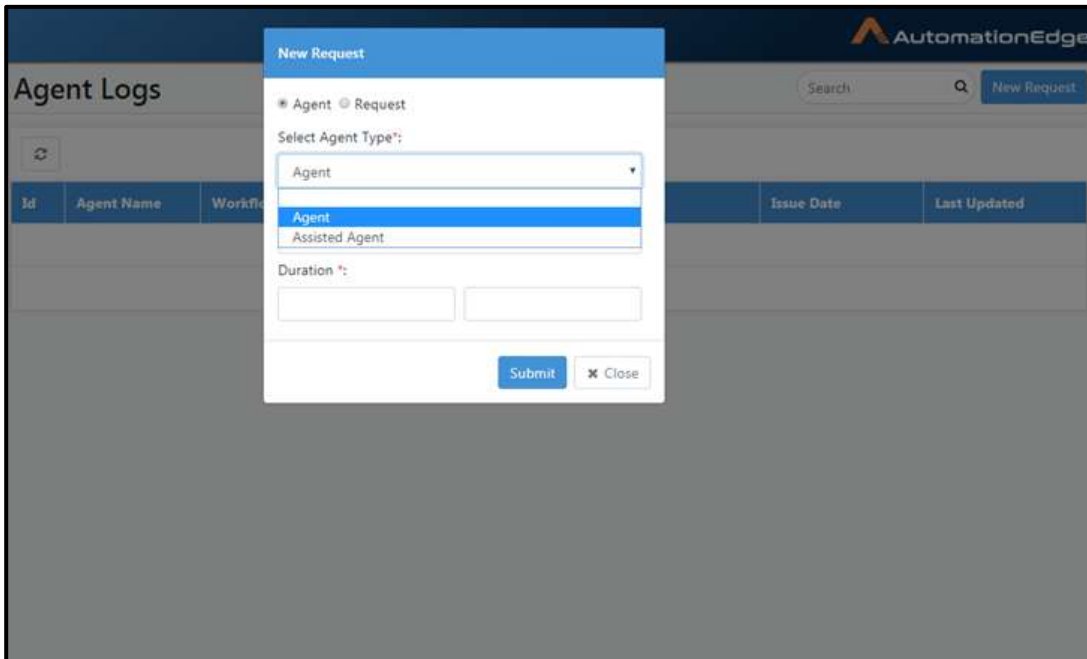


Figure 80c: Select Agent Type

4. Depending upon the Agent type a list Agents appears. Enable checkbox next to Agent or Agents for which you want to download the Agent logs.

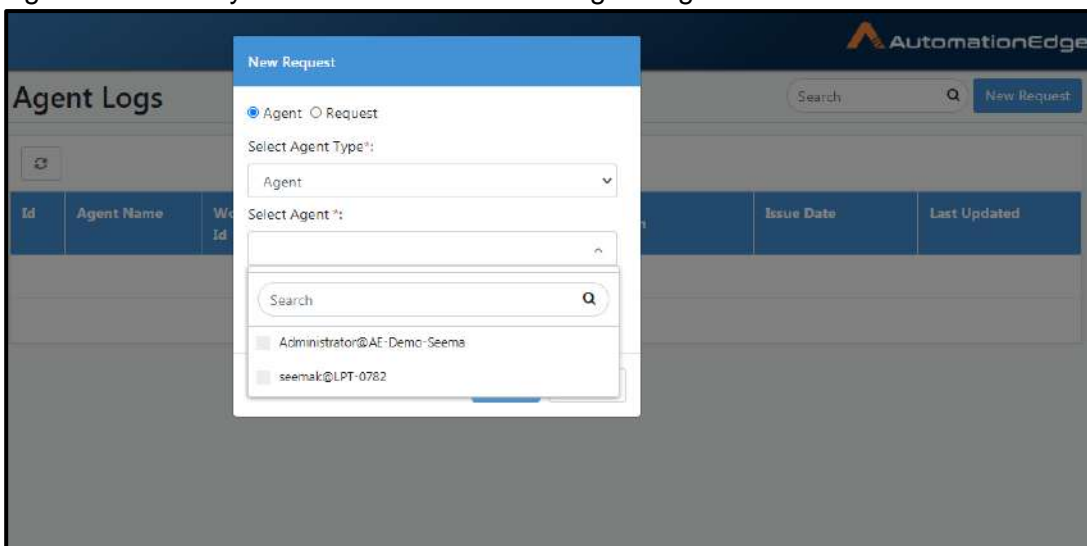


Figure 80d: Select Agent name as entity is Agent

5. Select the time period for which you want the logs.

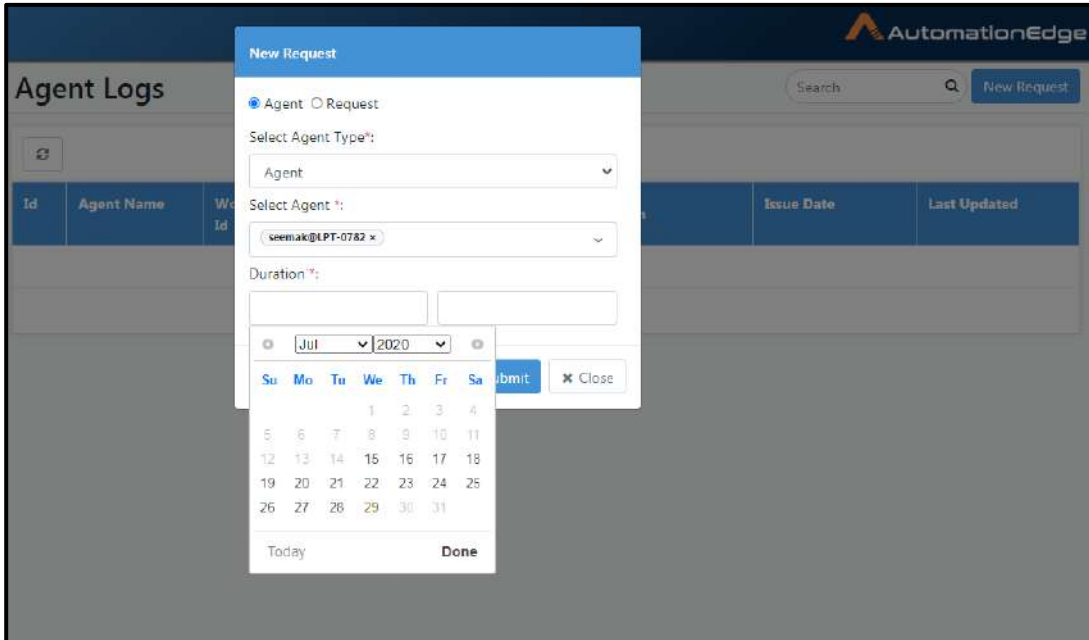


Figure 80e: Select From-To Dates

6. Click Submit.

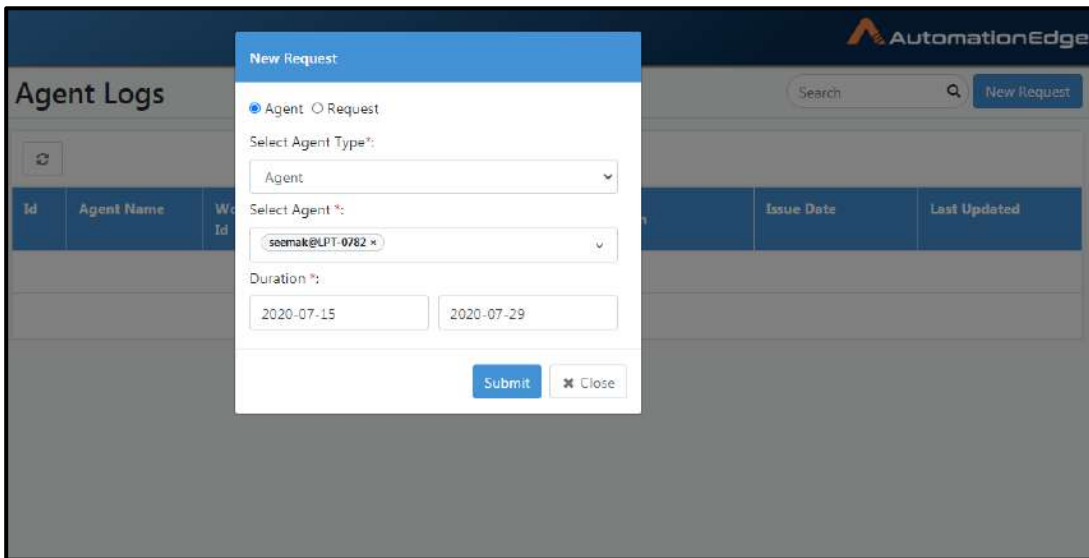


Figure 80f: Click Submit

- To download Agent level logs Agent must be up and running else it throws an error message as below.

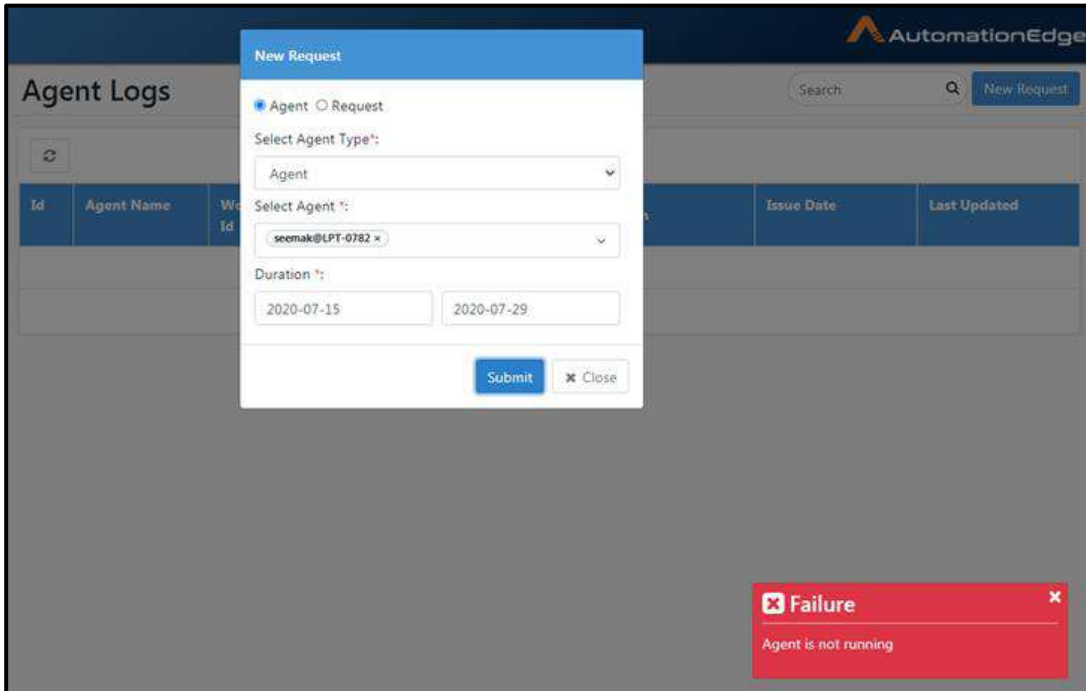


Figure 80g: Agent Log Download Error when Agent is not running

- The maximum duration for which log files that can be downloaded is 5 days. If the difference in days is more than 5 days an error message showing difference between dates cannot exceed 5 days is displayed.

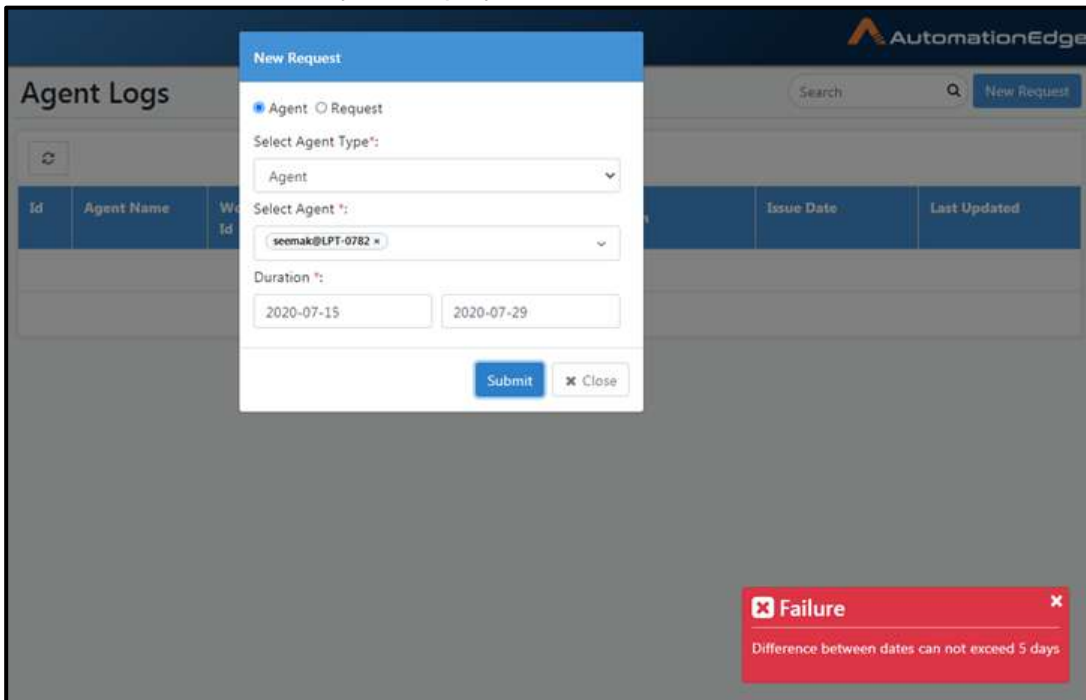


Figure 80h: Agent Logs can be downloaded only for 5 days

- Provide appropriate duration with difference in duration not more than 5 days. Click Submit.

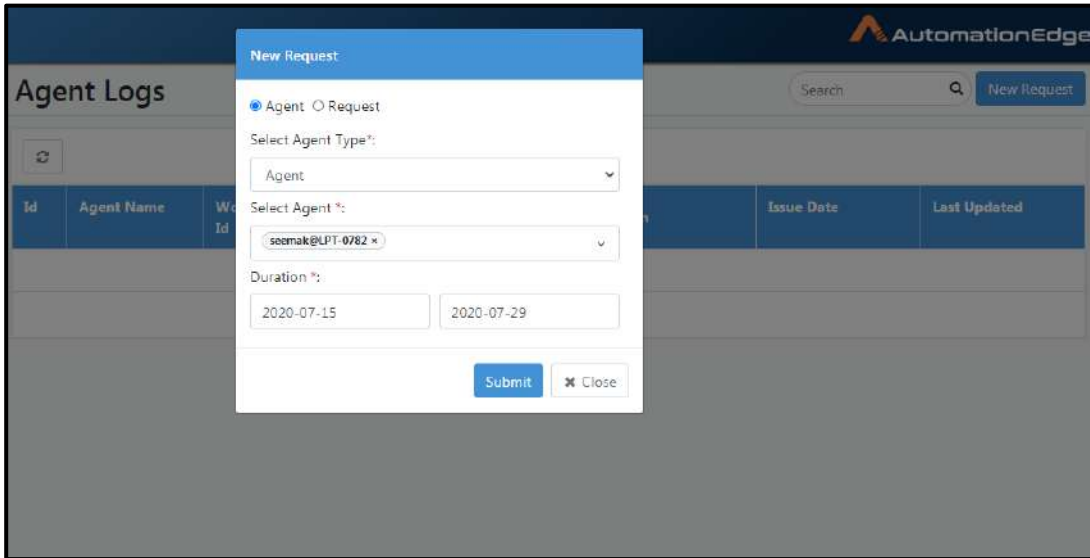


Figure 80i: Agent Logs request

- Request submitted successfully message is displayed.

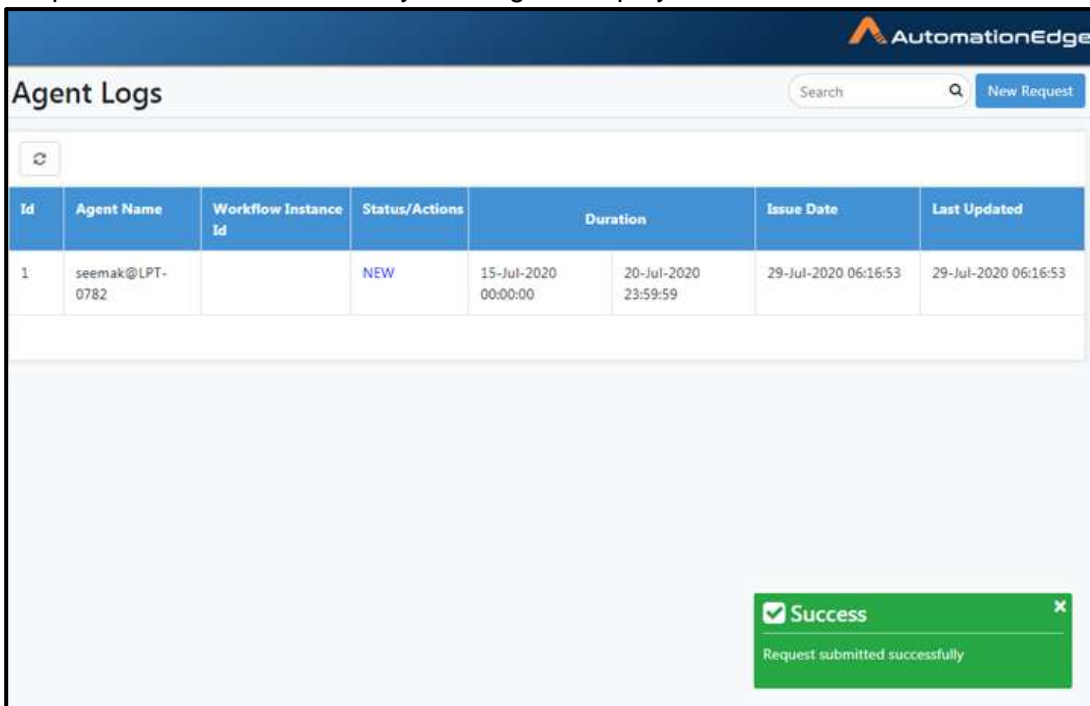
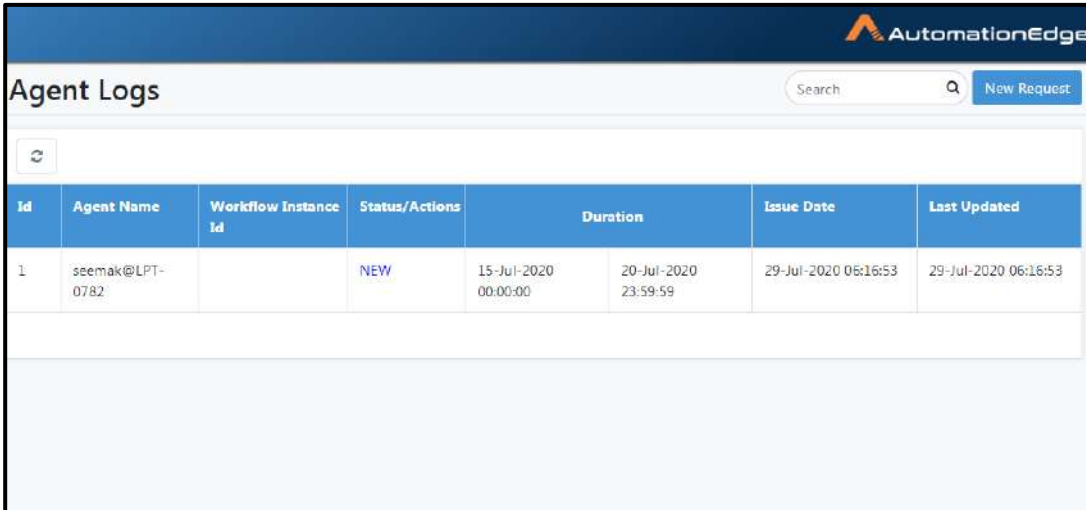


Figure 80j: Agent Log Request submitted successfully

11. A new entry in the Agent Logs with Status NEW appears.

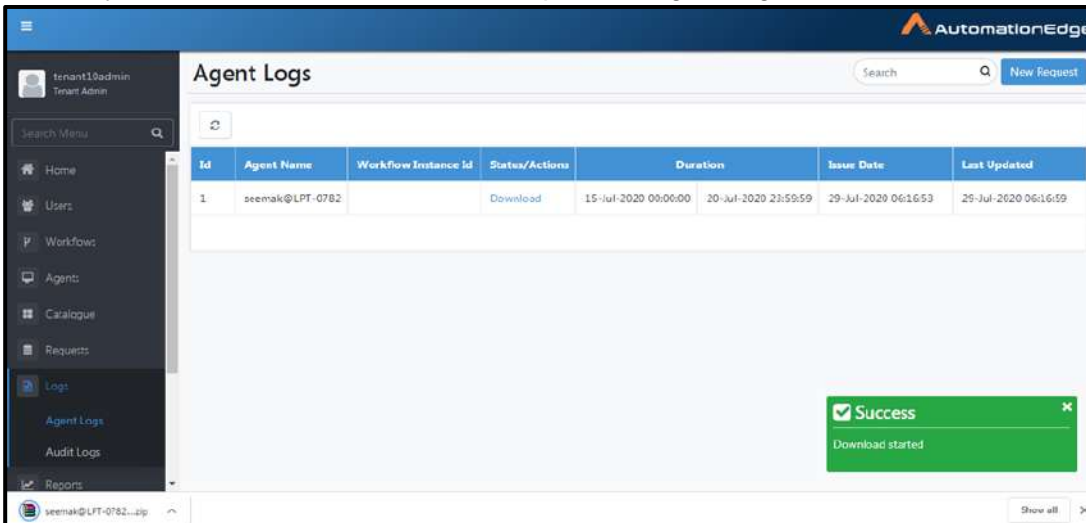


Id	Agent Name	Workflow Instance Id	Status/Actions	Duration	Issue Date	Last Updated
1	seemak@LPT-0782		NEW	15-Jul-2020 00:00:00	20-Jul-2020 23:59:59	29-Jul-2020 06:16:53

Figure 80k: Agent Log with status NEW

12. After some time, the status changes to Download.

13. You may click Download to download a zip of the Agent log files.



Id	Agent Name	Workflow Instance Id	Status/Actions	Duration	Issue Date	Last Updated
1	seemak@LPT-0782		Download	15-Jul-2020 00:00:00	20-Jul-2020 23:59:59	29-Jul-2020 06:16:59

Success
Download started

Figure 80l: Agent Logs Download with Download Link

14. Similarly, you can see more sets of Agent Logs for different time durations were requested and ready for download as seen below.

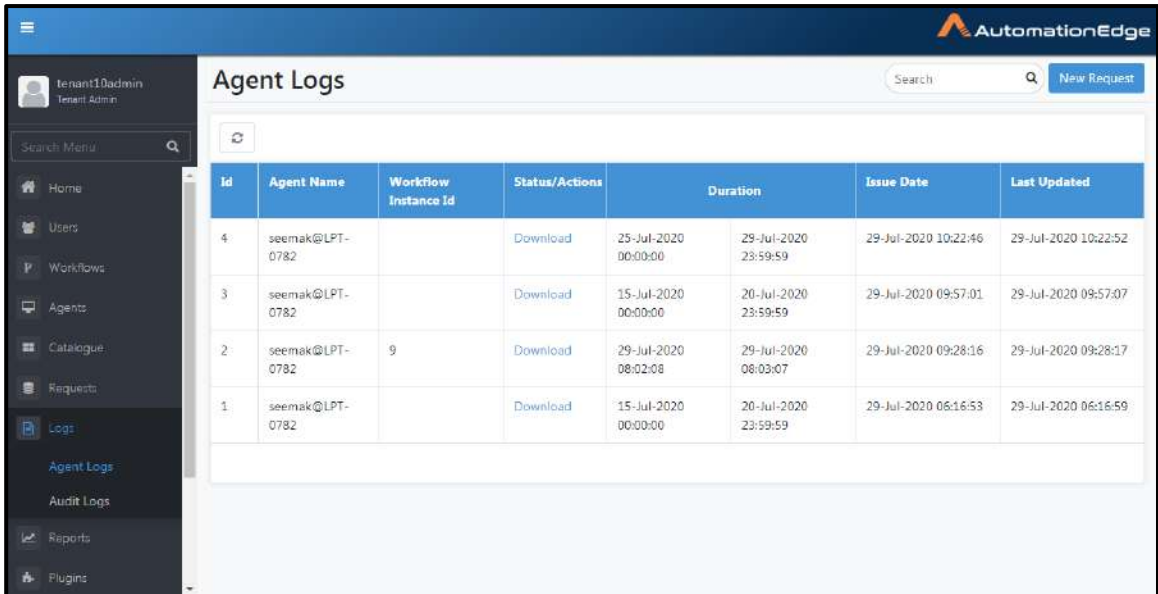


Figure 80m: Another Agent Log request with Id 7

15. The following snapshot shows Agent log downloaded for Id 4.

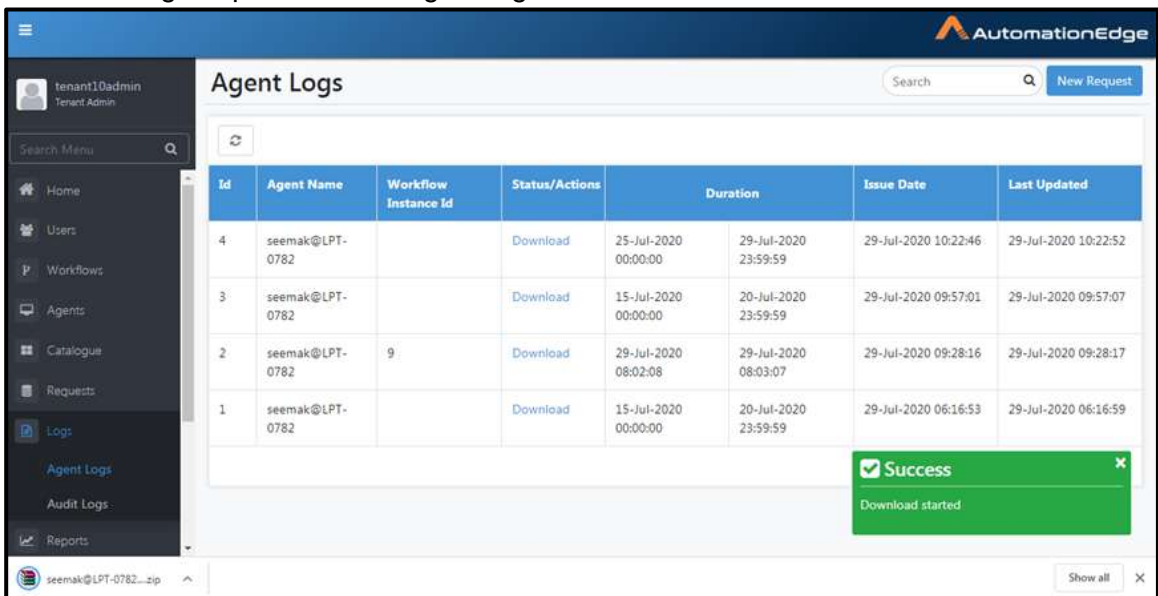


Figure 80n: Agent log download started

16. Unzip the downloaded file to get the following Agent log zip files are downloaded as seen below. Unzip the files.

Name	Date modified	Type	Size
aeagent_2020-07-29.log	29-07-2020 10:22	WinRAR ZIP archive	37 KB
aeagent_2020-07-28.log	29-07-2020 10:22	WinRAR ZIP archive	42 KB

Figure 80o: Downloaded Agent zip files

17. Below you can see unzipped agent log files.

Name	Date modified	Type	Size
aeagent	29-07-2020 10:22	Text Document	989 KB
aeagent_2020-07-28	29-07-2020 06:05	Text Document	1,038 KB

Figure 80p: Unzipped Agent log files

10.1.5.2 Agent Logs: Download by Request Id

1. The second option is to download Agent log by Request Id.

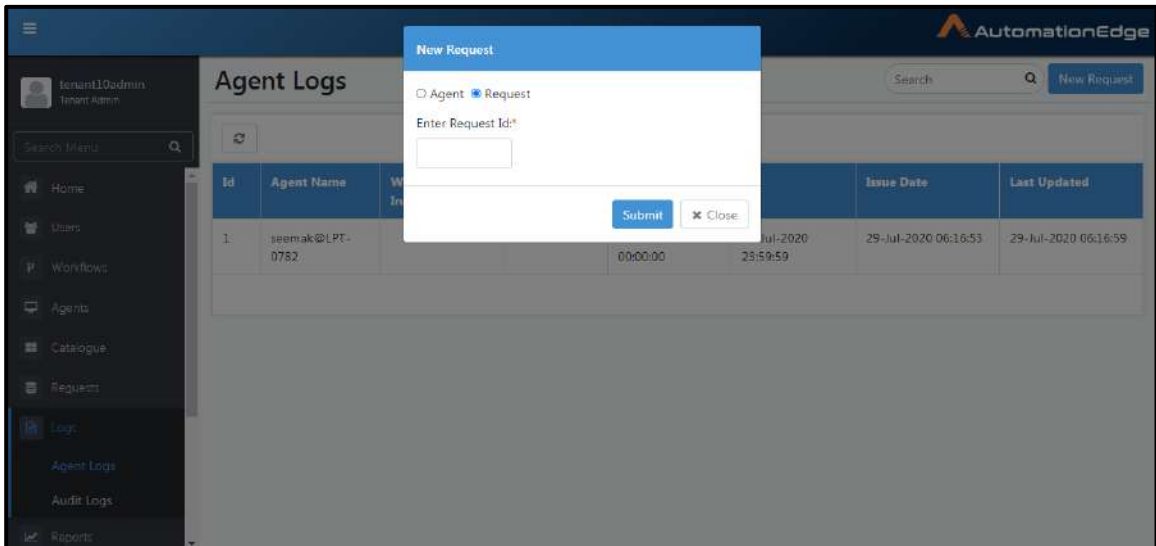


Figure 80q: Choose Entity Workflow

2. Type a Request id for which you need Agent Logs. Click Submit.

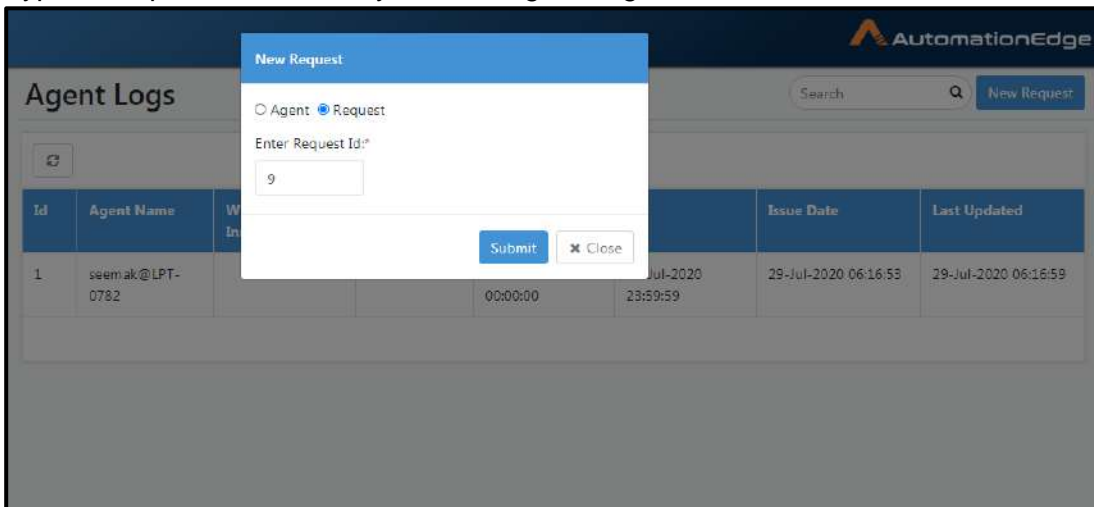


Figure 80r: Enter Request Id

3. Request submitted successfully message appears and an entry in the Agent log list appears with status NEW.

Id	Agent Name	Workflow Instance Id	Status/Actions	Duration		Issue Date	Last Updated
2	seemak@LPT-0782	9	NEW	29-Jul-2020 08:02:08	29-Jul-2020 08:03:07	29-Jul-2020 09:28:16	29-Jul-2020 09:28:16
1	seemak@LPT-0782		Download	15-Jul-2020 00:00:00	20-Jul-2020 23:59:59	29-Jul-2020 06:16:53	29-Jul-2020 06:16:59

Success
Request submitted successfully

Figure 80s: Agent Log Entry with Status NEW

- The status changes to Download. Click the Download link.

Id	Agent Name	Workflow Instance Id	Status/Actions	Duration		Issue Date	Last Updated
2	seemak@LPT-0782	9	Download	29-Jul-2020 08:02:08	29-Jul-2020 08:03:07	29-Jul-2020 09:28:16	29-Jul-2020 09:28:17
1	seemak@LPT-0782		Download	15-Jul-2020 00:00:00	20-Jul-2020 23:59:59	29-Jul-2020 06:16:53	29-Jul-2020 06:16:59

Figure 80t: Agent Log with Download Link

- It downloads a zip file as seen below.

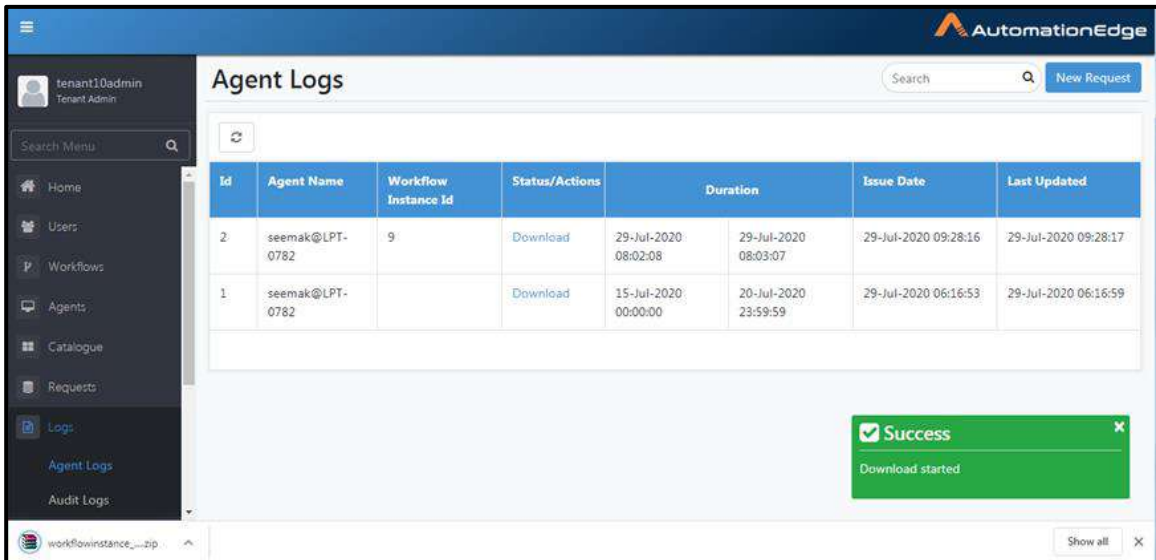


Figure 80u: Agent Log Zip by Request Id

- Unzip the downloaded workflowinstance_9_log.zip to get the aeagent_2020-07-29.log.zip file and unzip it to see agent.log containing the log for the requested workflow Id.

Name	Date modified	Type	Size
workflowinstance_9_log	29-07-2020 09:28	WinRAR ZIP archive	19 KB
aeagent	29-07-2020 09:27	Text Document	804 KB
aeagent_2020-07-29.log	29-07-2020 09:27	WinRAR ZIP archive	29 KB

Figure 80v: agent.log available in downloaded zip file

10.2 Audit Logs

The following Audit log information is maintained.

- Audit Logs are maintained for operations on entities and the source can be Server, Agent or Process. In Process Studio, there is an 'Audit Log' plugin step through which users can send Process Audit Logs if any; in this case, Audit Logs will be added with the source as "PROCESS". Agent Log generated by Server or Agent are marked with source Server and Agent respectively.
- In case of Update operation second level of information i.e. description is also captured. Fields updated are added in description of Audit log. Field values before the update as well as new field values are also added in Audit log description.
- More information in audit logs such as Source IP is also maintained in Audit logs.

Only Tenant Administrators have access to this menu. Tenant Administrators can search/download audit logs in the .csv format.

10.2.1 Audit Logs: View

Audit Logs can be viewed under Logs menu.

1. Click Logs menu and Audit Logs sub-menu. You can see a listing of Audit logs. Each of the columns is explained in the table below.

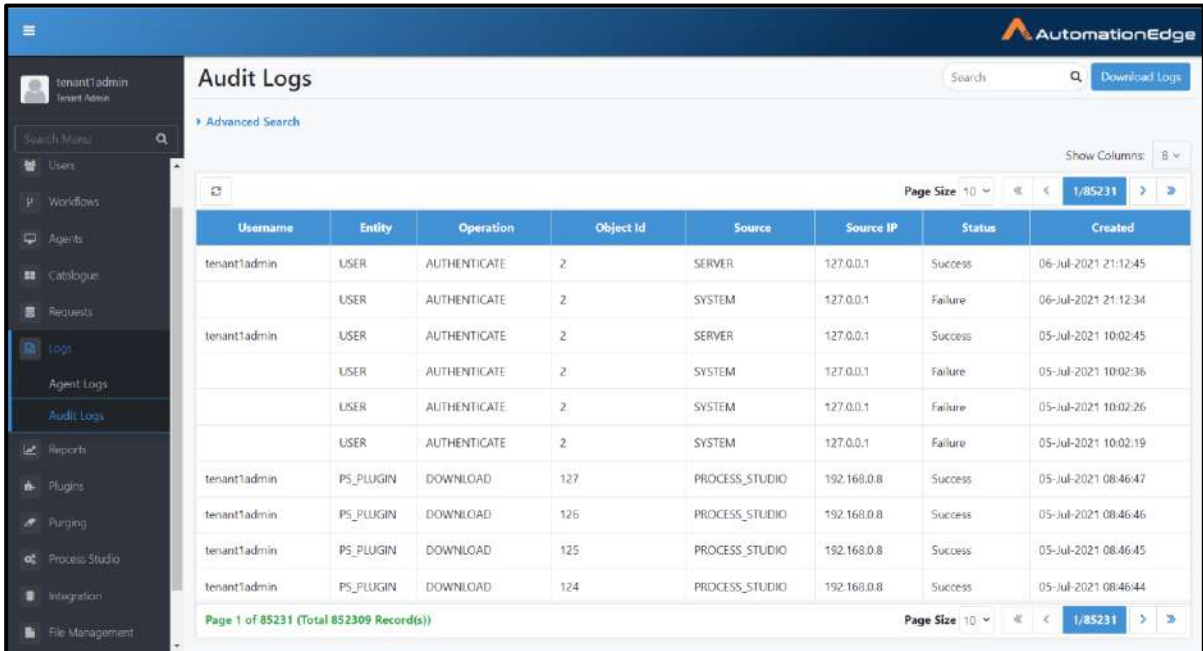


Figure 81a: Audit Logs

Table 56: Audit Logs Table

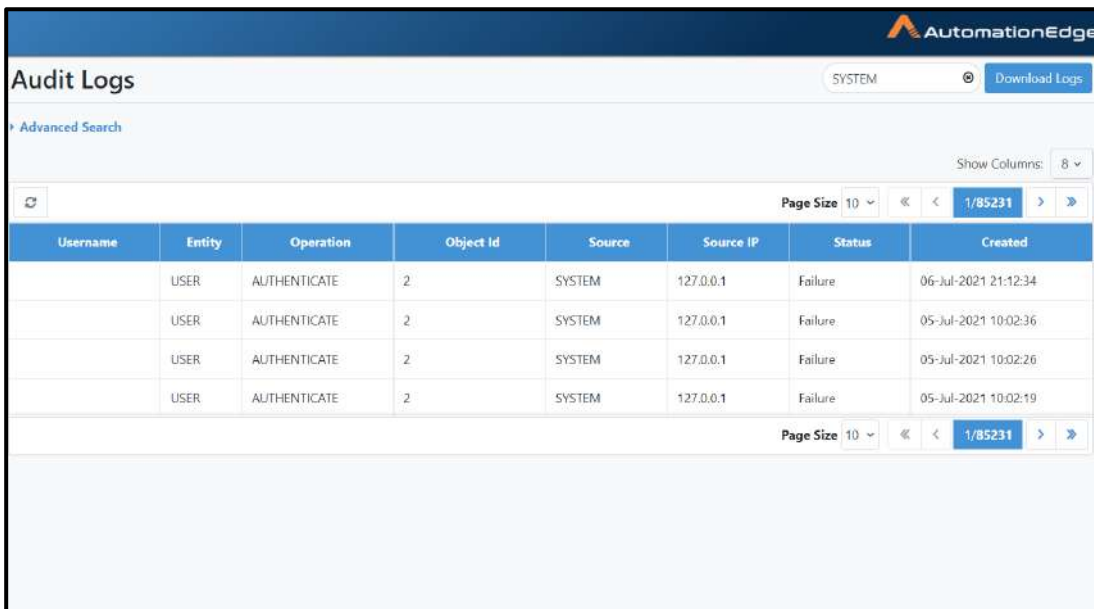
Username	Login Username
Entity	Entity name on which operation is performed. Following is the list of entities being accessed by users. AGENT, AGENT_CONSUMPTION, APPLICATION, ARTIFACT, ASSISTED_AGENT_LICENSE CATEGORY, CREDENTIAL, CREDENTIAL_POOL, DEBUG_LOG_REQUEST, FILE, LDAP_CONFIGURATION, LICENSE, NOTIFICATION_CONFIGURATION, PS_PLUGIN, PS_PLUGIN_PROPERTY, REMEDY_FORCE_CONFIGURATION, REPORT_DASHBOARD, REPORT_DATASOURCE,

Username	Login Username
	REPORT_INSTANCE, REPORT_TEMPLATE, ROLE, SCHEDULE, SERVER_URL, SMTP_CONFIGURATION, SYSTEM_SETTING, TENANT, USER, USER_GROUP, USER_GROUP_MAPPING, WORKFLOW, WORKFLOW_CONSUMPTION. WORKFLOW_INSTANCE, WORKFLOW_PARAMETER,
Operation	It is the operation performed. Following is the current list of operations being done on entities. ASSIGN, ASSIGN_PERMISSIONS AUTHENTICATE, CHANGE_PASSWORD, CREATE, DELETE, DOWNGRADE, DOWNLOAD, EXECUTE, EXPORT, IMPORT, LOGOUT, OWNERSHIP_TRANSFER, REGISTER, REQUEST, RESPONSE, RESTART, START, STOP, SYNC, UNASSIGN, UPDATE, UPGRADE, UPLOAD
object id	Id of the entity object on which operation was performed object.
Source	The source for Audit Log can be: SERVER, AGENT, WORKFLOW Notes: If audit logs are added as source "SERVER", username value is populated. If audit logs are added as

Username	Login Username
	source "AGENT/WORKFLOW", agent name value is populated
Status	This is the operation status. The status of operation can be: Success, Failure
Created Date	It is the audit log creation date. It is the Date of operation.
log level	Log level can be set to INFO or TRACE for source WORKFLOW in Process Studio Audit log step. For source Server and Agent Audit logs are system generated and we do not specify log level.
username	If source is SERVER, logged in username is populated.
agent name	If source is AGENT/WORKFLOW, agent name is populated.
Object name (OPTIONAL)	name of the entity object on which operation was performed
description (OPTIONAL)	A description of the Audit Log.

10.2.2 Audit Logs: Search

1. Type a string in the search box on the top right corner to filter records.
2. Type SYSTEM in the Search Box. Records with operation SYSTEM are filtered as seen below.



The screenshot shows the AutomationEdge Audit Logs interface. At the top right, there is a search box containing the text 'SYSTEM' and a 'Download Logs' button. Below the search box, there is an 'Advanced Search' link and a 'Show Columns: 8' dropdown. The main area displays a table of audit logs with the following columns: Username, Entity, Operation, Object Id, Source, Source IP, Status, and Created. The table contains four rows of data, all filtered by the search term 'SYSTEM'. The table also includes pagination controls at the bottom, showing 'Page Size 10' and '1/85231'.

Username	Entity	Operation	Object Id	Source	Source IP	Status	Created
	USER	AUTHENTICATE	2	SYSTEM	127.0.0.1	Failure	06-Jul-2021 21:12:34
	USER	AUTHENTICATE	2	SYSTEM	127.0.0.1	Failure	05-Jul-2021 10:02:36
	USER	AUTHENTICATE	2	SYSTEM	127.0.0.1	Failure	05-Jul-2021 10:02:26
	USER	AUTHENTICATE	2	SYSTEM	127.0.0.1	Failure	05-Jul-2021 10:02:19

Figure 82a: Filtered Search Results

10.2.3 Audit Logs: Advanced Search

Advanced Search can be done by selecting one or more of the search criteria: Entity, Source, Log Level, Operation, Created and Status.

1. Entity, Source, Log Level, Operation and Status can equal to a value in the list.

The screenshot shows the AutomationEdge Audit Logs interface. The 'Advanced Search' section is active, and a dropdown menu is open for selecting a column. The dropdown options are: Select Column, Entity, Source, Log Level, Username, Agent Name, Source IP, Operation, Created, and Status. The table below shows a list of audit logs with columns: Entity, Operation, Object Id, Source, Source IP, Status, and Created.

Entity	Operation	Object Id	Source	Source IP	Status	Created	
USER	AUTHENTICATE	2	SERVER	127.0.0.1	Success	06-Jul-2021 21:49:40	
USER	REQUEST	2	SYSTEM	10.81.25.10	Failure	06-Jul-2021 21:49:20	
USER	AUTHENTICATE	2	SERVER	127.0.0.1	Success	06-Jul-2021 21:12:45	
USER	AUTHENTICATE	2	SYSTEM	127.0.0.1	Failure	06-Jul-2021 21:12:34	
tenant1admin	USER	AUTHENTICATE	2	SERVER	127.0.0.1	Success	05-Jul-2021 10:02:45
USER	AUTHENTICATE	2	SYSTEM	127.0.0.1	Failure	05-Jul-2021 10:02:36	
USER	AUTHENTICATE	2	SYSTEM	127.0.0.1	Failure	05-Jul-2021 10:02:26	

Figure 83a: Advanced Search Filter Criteria

2. Agent Name and Username can be with values equal to, not equal to, like, begins with, ends with as seen below.

The screenshot shows the AutomationEdge Audit Logs interface. The 'Advanced Search' section is active, and a dropdown menu is open for selecting a comparator. The dropdown options are: Select Comparator, equal to, not equal to, like, begins with, and ends with. The table below shows a list of audit logs with columns: Username, Object Id, Source, Source IP, Status, and Created.

Username	Object Id	Source	Source IP	Status	Created
tenant1admin	2	SERVER	127.0.0.1	Success	06-Jul-2021 21:49:40
USER	2	SYSTEM	10.81.25.10	Failure	06-Jul-2021 21:49:20
tenant1admin	2	SERVER	127.0.0.1	Success	06-Jul-2021 21:12:45
USER	2	SYSTEM	127.0.0.1	Failure	06-Jul-2021 21:12:34
tenant1admin	2	SERVER	127.0.0.1	Success	05-Jul-2021 10:02:45
USER	2	SYSTEM	127.0.0.1	Failure	05-Jul-2021 10:02:36
USER	2	SYSTEM	127.0.0.1	Failure	05-Jul-2021 10:02:26

Figure 83b: Advanced Search Filter Criteria

- Created Date can be set using the options exact date, before, after, in between or not in between.

The screenshot displays the 'Audit Logs' interface. At the top, there is a search bar and a 'Download Logs' button. Below this is the 'Advanced Search' section, which includes a 'Column' dropdown set to 'Created' and a 'Comparator' dropdown. The 'Comparator' dropdown is open, showing the following options: 'exact date', 'before', 'after', 'in between', and 'not in between'. There are 'Add Filter' and 'Cancel' buttons next to the comparator dropdown. Below the search section is a table of audit log entries. The table has columns for 'Username', 'Object Id', 'Source', 'Source IP', 'Status', and 'Created'. The table contains several rows of data, including entries for 'tenant1admin' and 'USER' with various 'Status' values like 'Success' and 'Failure'.

Username	Object Id	Source	Source IP	Status	Created
tenant1admin	2	SERVER	127.0.0.1	Success	06-Jul-2021 21:49:40
USER	2	SYSTEM	10.81.25.10	Failure	06-Jul-2021 21:49:20
tenant1admin	2	SERVER	127.0.0.1	Success	06-Jul-2021 21:12:45
USER	2	SYSTEM	127.0.0.1	Failure	06-Jul-2021 21:12:34
tenant1admin	2	SERVER	127.0.0.1	Success	05-Jul-2021 10:02:45
USER	2	SYSTEM	127.0.0.1	Failure	05-Jul-2021 10:02:36
USER	2	SYSTEM	127.0.0.1	Failure	05-Jul-2021 10:02:26

Figure 83c: Advanced Search Filter Criteria

10.2.4 Audit Logs: Download

Following is the process to download Audit Logs.

1. On the Agent Logs menu click Download Logs Button at the top right corner.

The screenshot shows the AutomationEdge interface for 'Audit Logs'. The user is logged in as 'tenant1admin'. The left sidebar contains a menu with options: Users, Workflows, Agents, Catalogue, Requests, Logs (selected), Agent Logs, Audit Logs, Reports, Plugins, and Purging. The main content area displays a table of audit logs with columns: Username, Entity, Operation, Object Id, Source, Source IP, Status, and Created. The table contains four rows of data, all showing 'Failure' status. At the top right, there is a 'Download Logs' button. Below the table, there are pagination controls showing 'Page Size 10' and '1/85231'.

Figure 84a: Download Audit logs

2. Alternatively, you may put a filter text as shown below. You can now see the filtered records. Click Download logs.

The screenshot shows the AutomationEdge interface for 'Audit Logs' with a filter applied. The interface is identical to Figure 84a, but the 'Advanced Search' section is visible. The table of audit logs is the same as in Figure 84a, showing four rows of 'Failure' records. The 'Download Logs' button is still present at the top right. The pagination controls at the bottom show 'Page Size 10' and '1/85231'.

Figure 84b: Filter and Download Logs Audit

- Specify the Page Number to download.

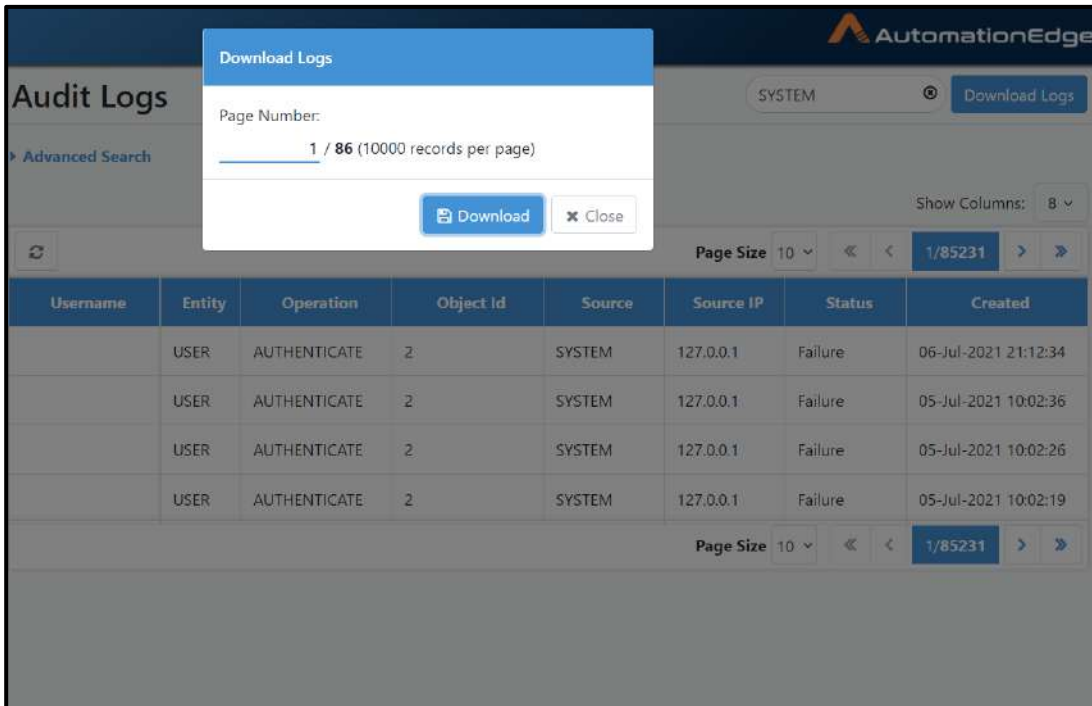


Figure 84c: Select Page Number

- A Success message appears showing Audit Logs download started and a .csv file opens.

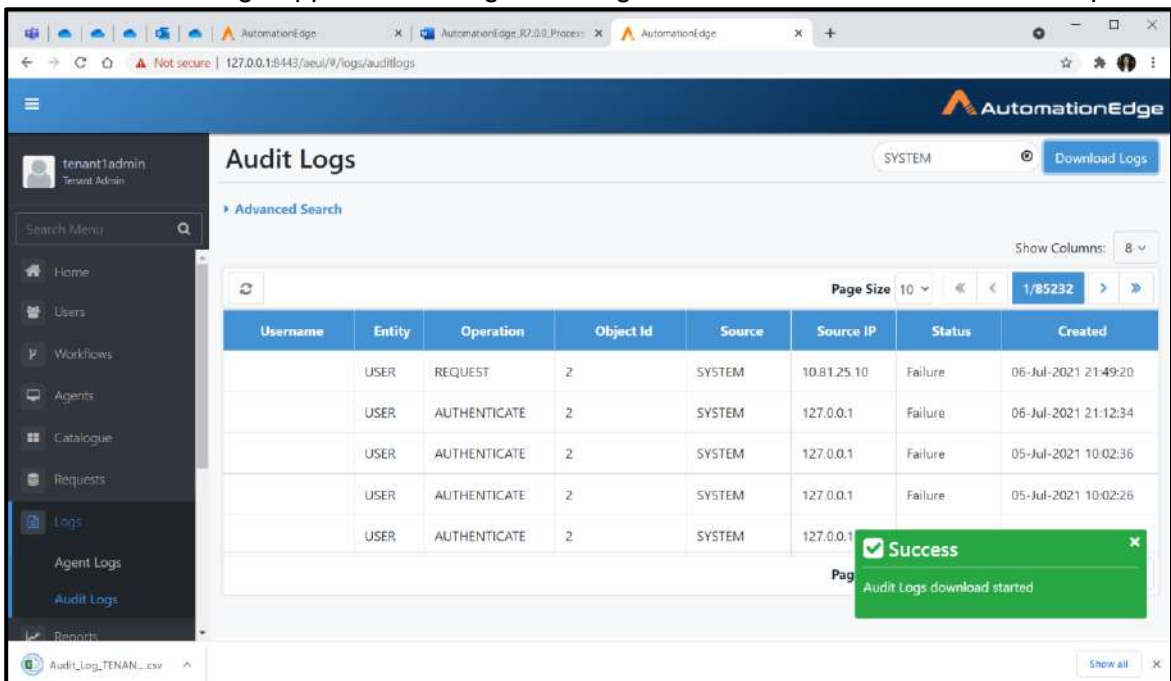


Figure 84d: Audit Logs Download Started

- The Audit log file is downloaded in the file system.

11 Reports

This menu allows you to create Dashboards to Add/View reports.

Click Reports menu the first time to see the screen below. You can see a button to add a New Dashboard.

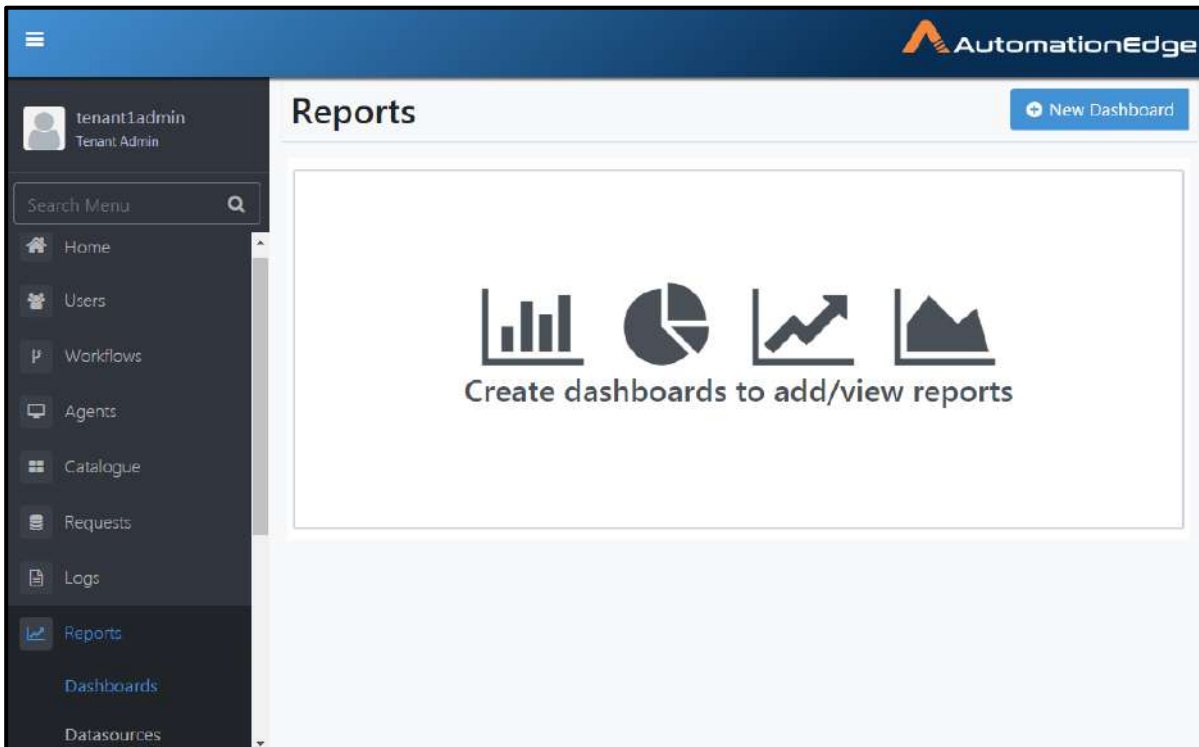


Figure 85a: Reports Home Page

11.1 Dashboards

11.1.1 New Dashboard

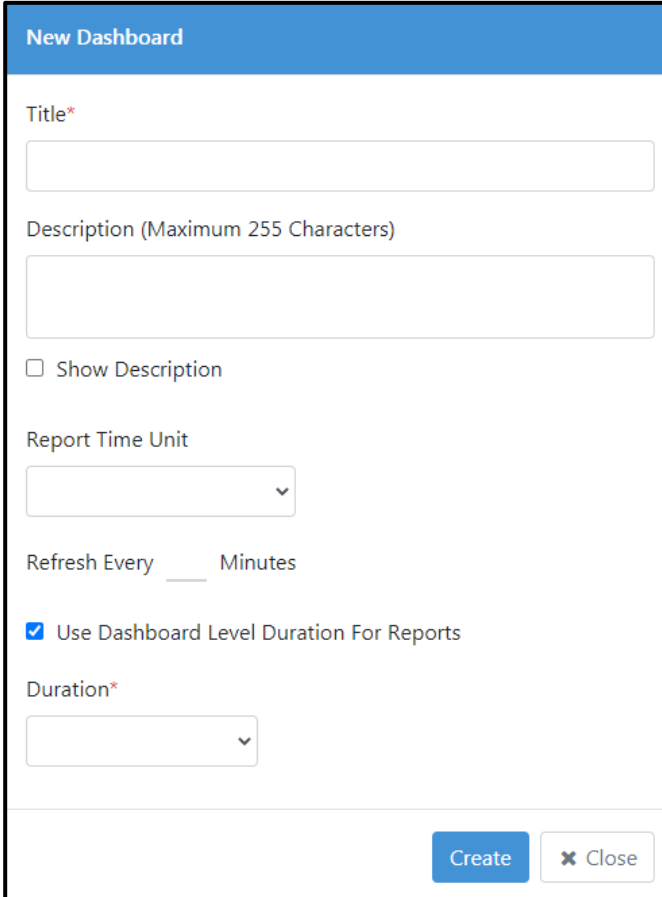
Dashboard is a container for multiple reports. All the related reports, that one wants to view together, can be kept on one dashboard. At least one dashboard is required to start creating reports.

To create a new Dashboard,

1. Click on 'New Dashboard' button.
2. Enter a dashboard title and an optional description.
3. Enable Show Description checkbox to see the Dashboard name along with the description.
4. Choose a Report Time Unit in seconds, minutes or hours.
5. Put a figure in minutes for the refresh interval. A refresh interval can be set between 1-15 minutes for the dashboard. The dashboard reports will refresh the reports after every

refresh cycle. The user session will not timeout if the refresh interval is set. After 15 minutes' user session times out.

6. Enable Use Dashboard Level Duration for reports to have a common duration for all reports on the dashboard. This is a global duration and if it is set, all the requests on the dashboard will show data for the specified duration. When Dashboard Level Duration for Reports is enabled, one can not specify durations for individual reports.



New Dashboard

Title*

Description (Maximum 255 Characters)

Show Description

Report Time Unit

Refresh Every ___ Minutes

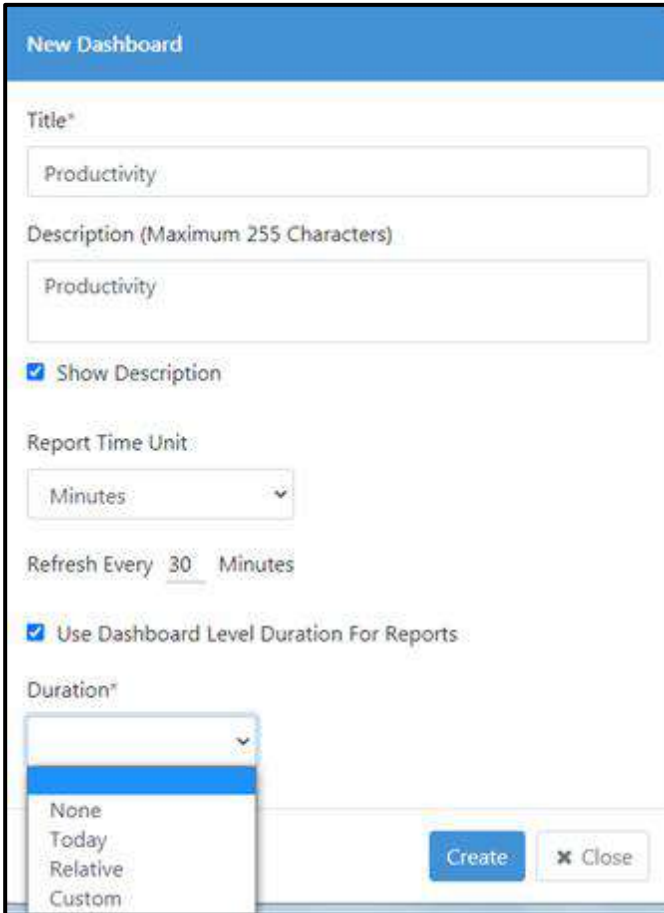
Use Dashboard Level Duration For Reports

Duration*

Create Close

Figure 86a: New Dashboard

7. Choose a value for Duration for Reports from the dropdown list as shown below.



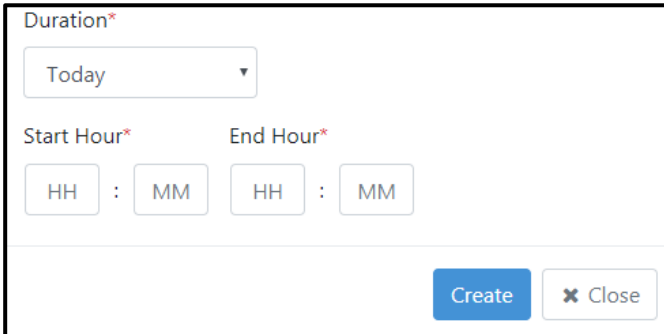
The screenshot shows a 'New Dashboard' form with the following fields and options:

- Title*: Productivity
- Description (Maximum 255 Characters): Productivity
- Show Description
- Report Time Unit: Minutes
- Refresh Every: 30 Minutes
- Use Dashboard Level Duration For Reports
- Duration*: A dropdown menu is open, showing options: None, Today, Relative, and Custom.

Buttons: Create, Close

Figure 86b: Report Duration

8. Following are the options when Duration selected is Today



The screenshot shows the 'Duration' form with the following fields and options:

- Duration*: Today
- Start Hour*: HH : MM
- End Hour*: HH : MM

Buttons: Create, Close

Figure 86c: Today in Duration

9. Following are the options when Duration selected is Relative. Select a relative period. Provide a numeric value in Last field. Select the relative period from the list as seen below.

Duration*

Relative

Last* :

Minutes
Hours
Days
Months
Years

Create Close

Figure 86d: Relative in Duration

10. Following are the options when Duration selected is Custom.

Duration*

Custom

Date Range:

Create Close

Figure 86e: Custom Duration

11. Click the two fields for Date Range to pop up a calendar. Choose the two dates.

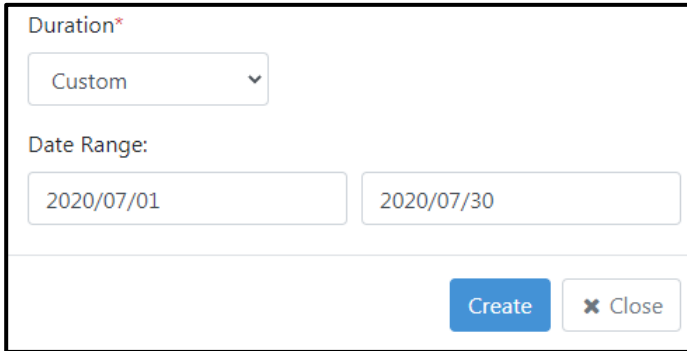
Jul 2020

Su	Mo	Tu	We	Th	Fr	Sa
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

Today Done

Figure 86f: Custom Duration: Date Range

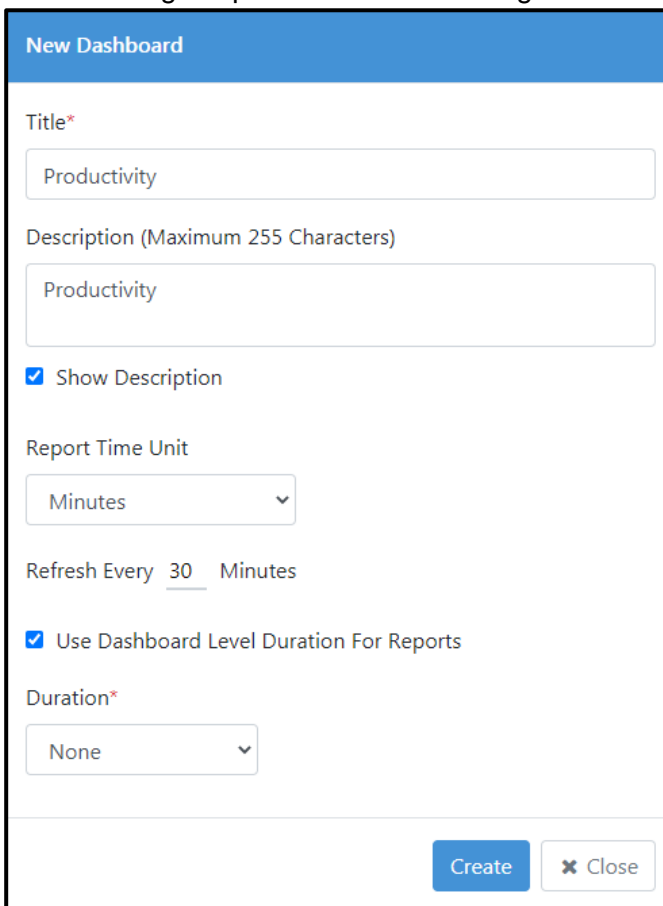
12. The following snapshot shows a chosen date range chosen for Custom Duration.



The screenshot shows a form titled "Duration*" with a dropdown menu set to "Custom". Below this, the "Date Range:" is specified with two input fields: "2020/07/01" and "2020/07/30". At the bottom right, there are two buttons: "Create" and "Close".

Figure 86g: Custom Duration: Dates Chosen

13. The following snapshot shows our configuration for a dashboard. Click Create.



The screenshot shows a form titled "New Dashboard" with the following fields and options:

- Title***: Productivity
- Description (Maximum 255 Characters)**: Productivity
- Show Description
- Report Time Unit**: Minutes
- Refresh Every 30 Minutes
- Use Dashboard Level Duration For Reports
- Duration***: None

At the bottom right, there are two buttons: "Create" and "Close".

Figure 86h: Duration None

14. Dashboard created successfully message appears.

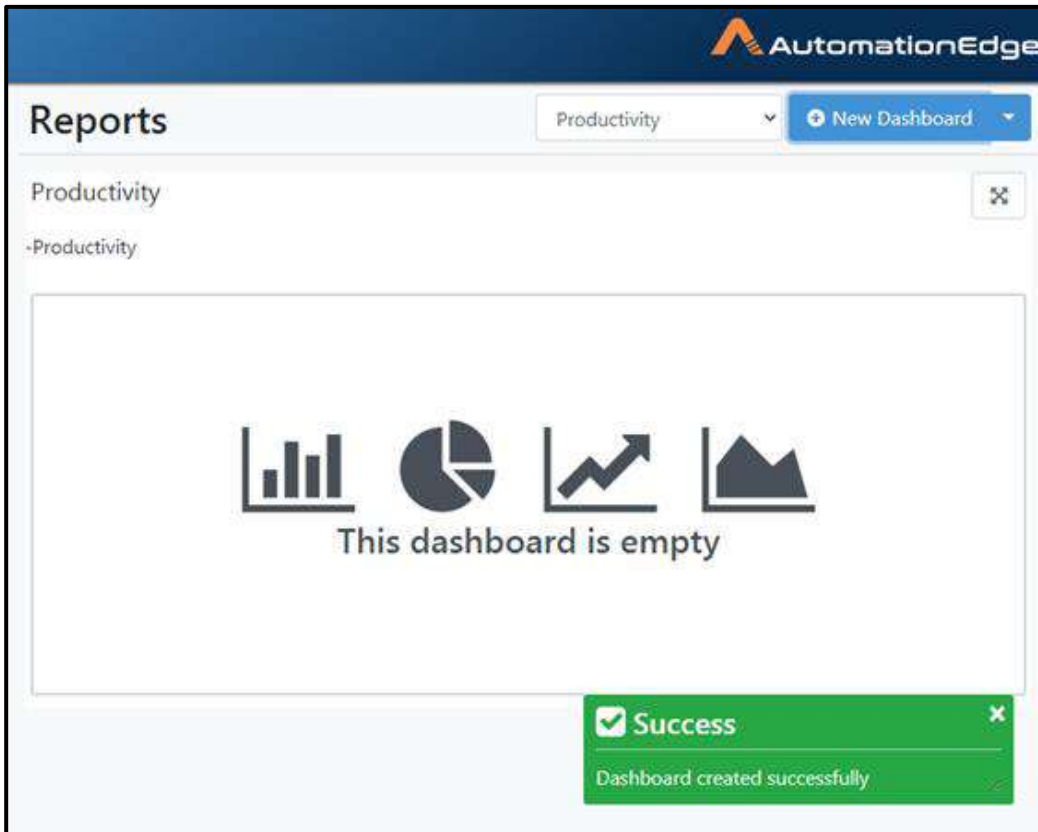


Figure 86i: Successful Dashboard creation message

15. The new Agents Dashboard is now visible. You can now see a Dashboard selection box and a dropdown arrow next to New Dashboard button.
16. Click on Toggle Full Screen Mode button on the right to display dashboard in full screen mode and click again to reverse back to normal mode display.

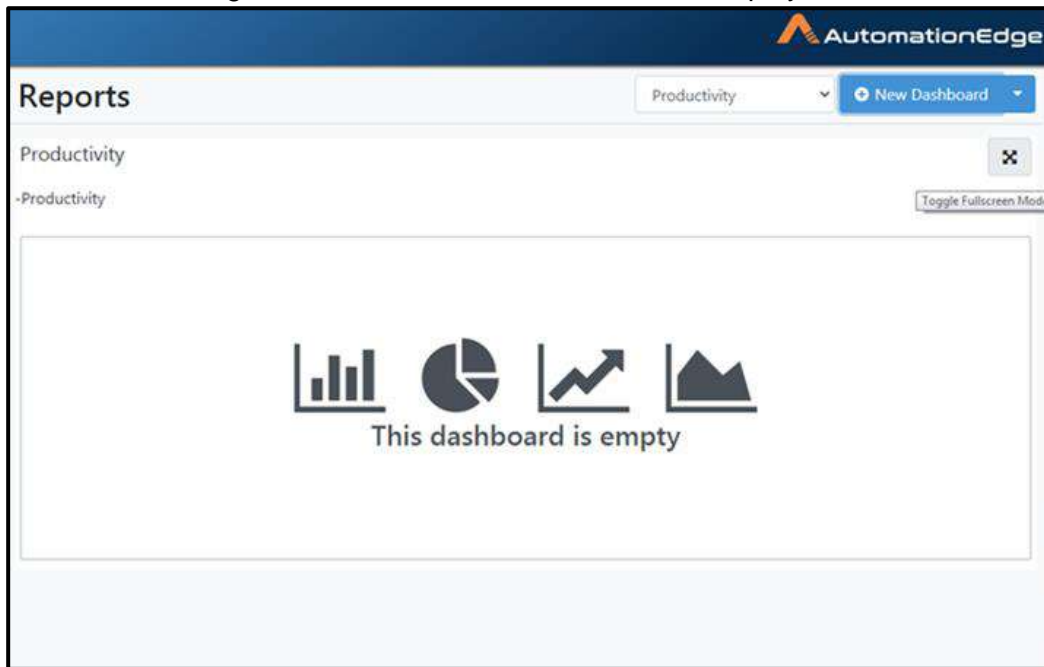


Figure 86j: Toggle to Full Screen Mode for Dashboard

11.1.2 Dashboard Selection

You can choose a dashboard to display from the available list of dashboards. This field is to the left of the 'New Dashboard' button.

11.1.3 Dashboard Options

Click the dropdown arrow next to New Dashboard. The options include, Edit Dashboard, Set As Default, Add Report and Delete Dashboard as seen in the figure below.

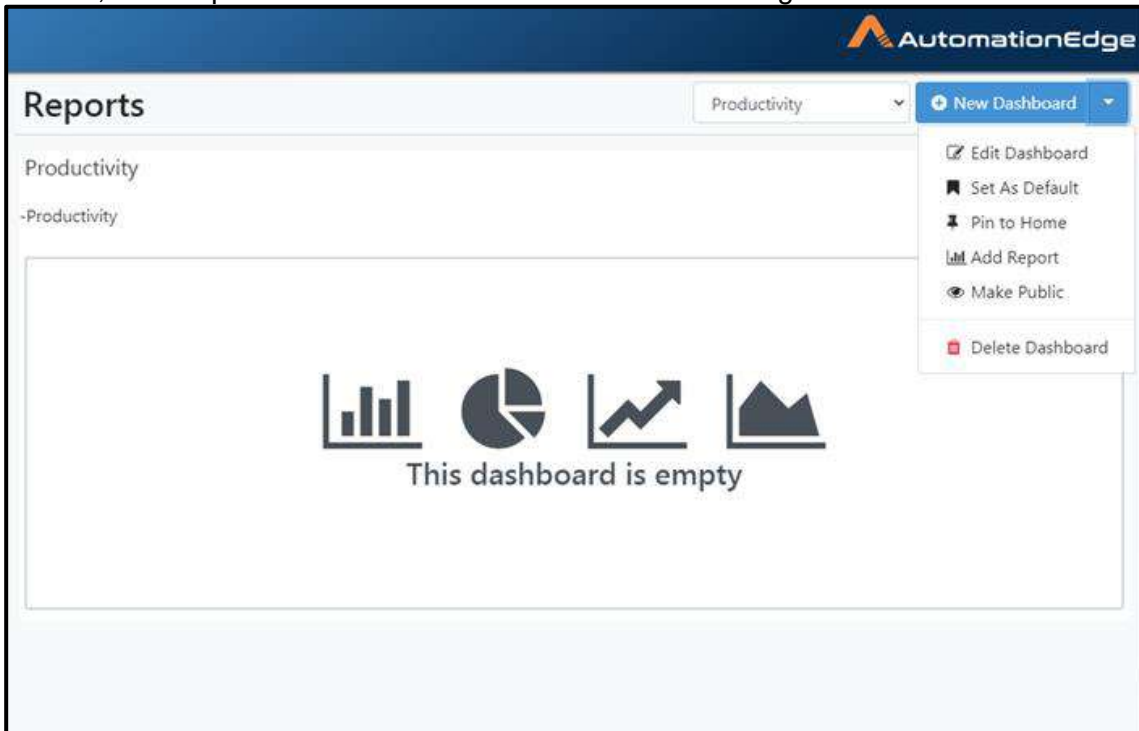


Figure 87a: Dashboard Options

Table 57: Dashboard options

Field	Description
Select Dashboard	Select a dashboard from the drop down list to display.
Options:	
Edit Button (✎)	Click to edit the dashboard properties.
Set as default (🚩)	Click to set the selected dashboard as default.
Pin to Home (📌)	Click to pin Dashboard to Home. However, please note that the bottom 'Agent Utilization' section is not visible on home page if Dashboard is pinned to home.
Add Report (📊)	Click to Add Report
Make Public (👁)	Click to publish the Dashboard to public.
Delete Button (🗑)	Click to delete the dashboard.

11.1.3.1 Edit Dashboard

Following are the steps to Edit Dashboard,

1. Click the dropdown arrow next to New Dashboard. Click Edit Dashboard as seen in the figure below.

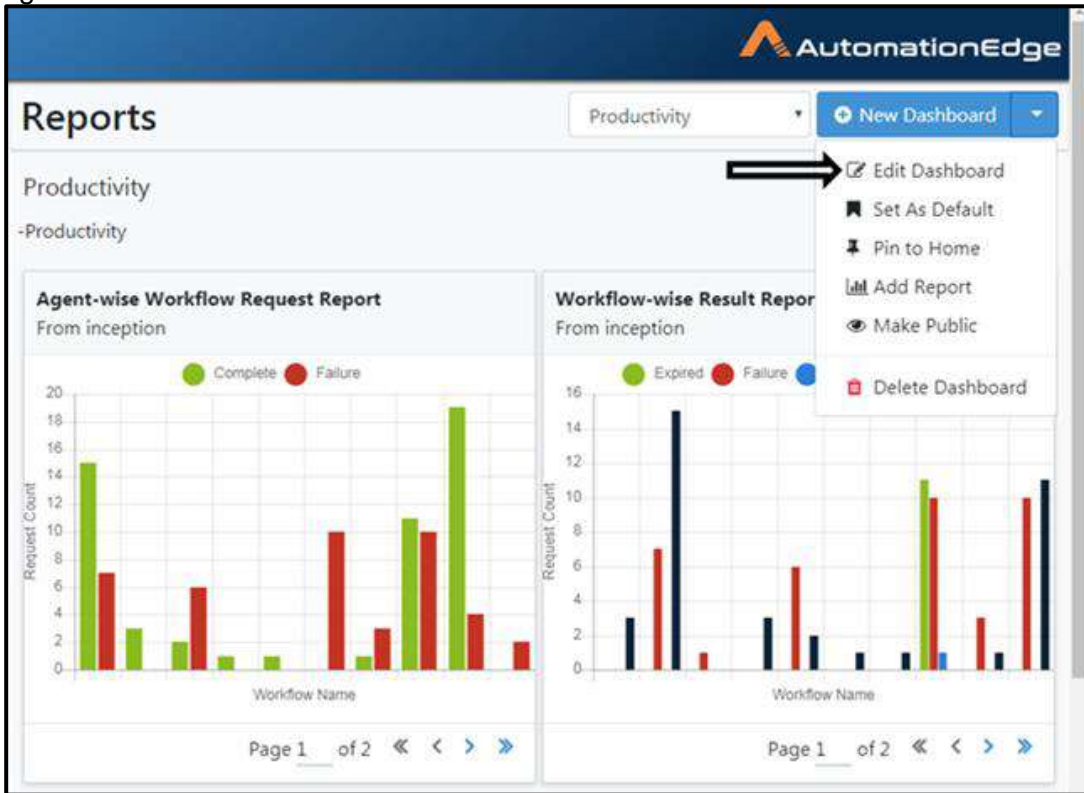
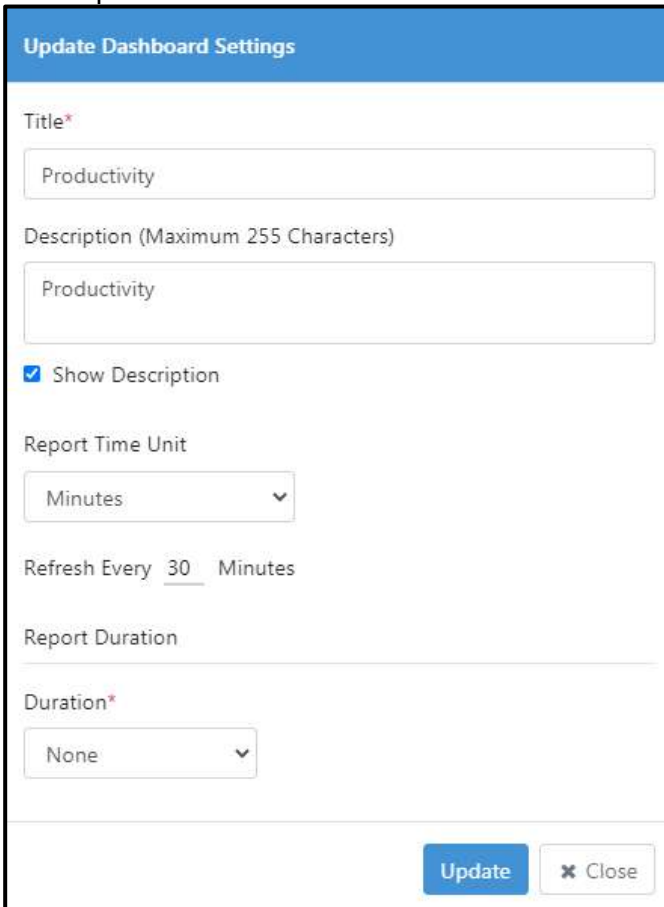


Figure 87b: Dashboard Options

2. An Update Dashboard Settings window appears. Edit Dashboard settings as desired. Click Update.



Update Dashboard Settings

Title*

Productivity

Description (Maximum 255 Characters)

Productivity

Show Description

Report Time Unit

Minutes

Refresh Every 30 Minutes

Report Duration

Duration*

None

Update Close

Figure 87c: Update Dashboard Settings

3. Dashboard save successfully message appears as seen below.

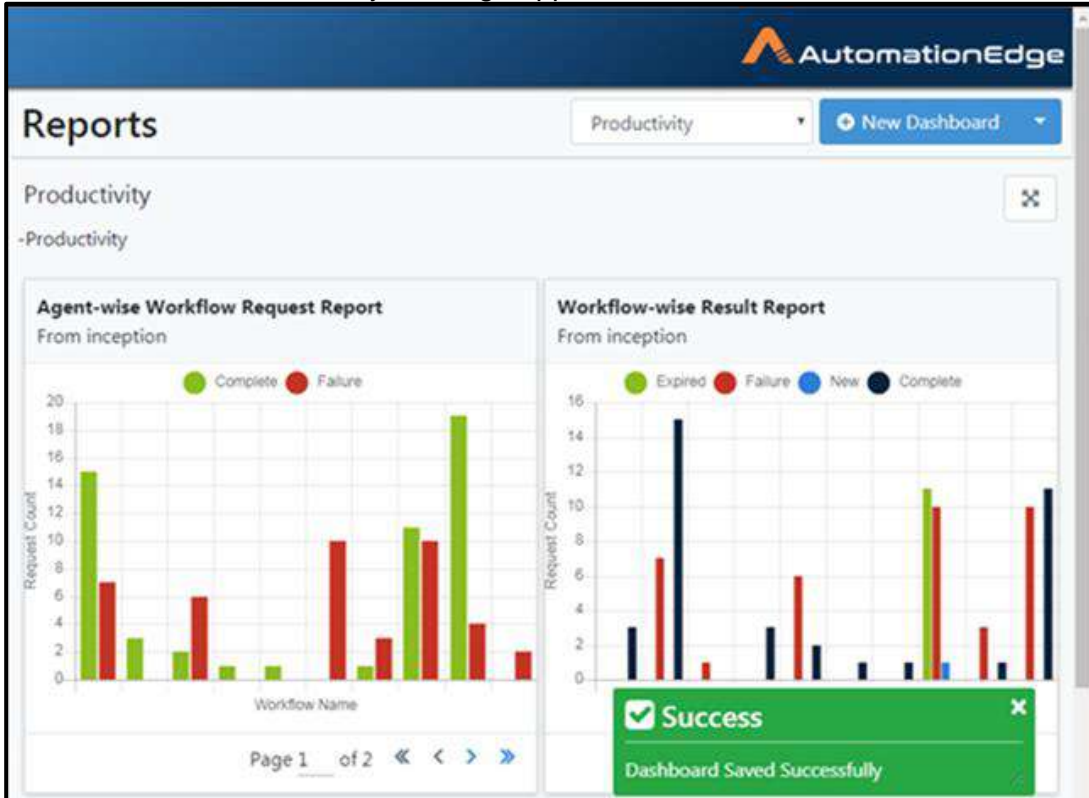


Figure 87d: Dashboard updated successfully

11.1.3.2 Set as Default

Following are the steps to set the Dashboard as the Default Dashboard.

1. Select the dashboard you wish to Set As Default. In the case below we have chosen Productivity dashboard.
2. Click the Arrow next to New Dashboard. Click the second option Set As Default.

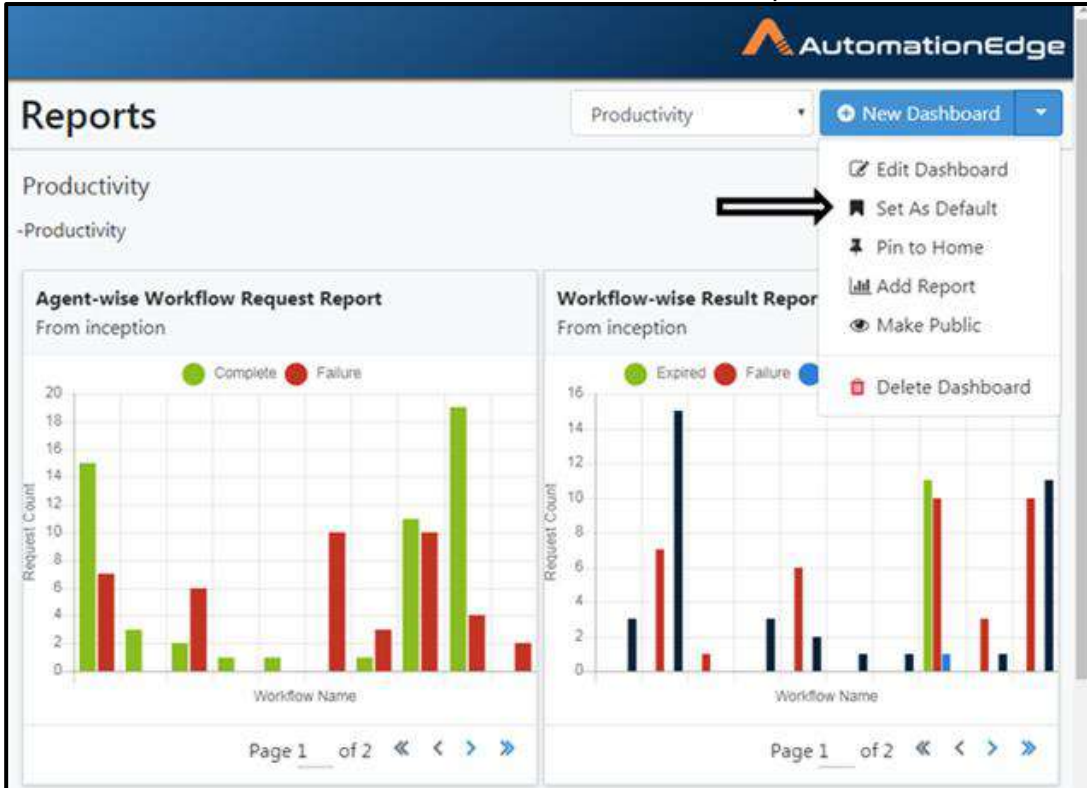


Figure 87e: Dashboard Set as Default

- 3. You get a message Operation Completed successfully. Productivity is now the default dashboard.

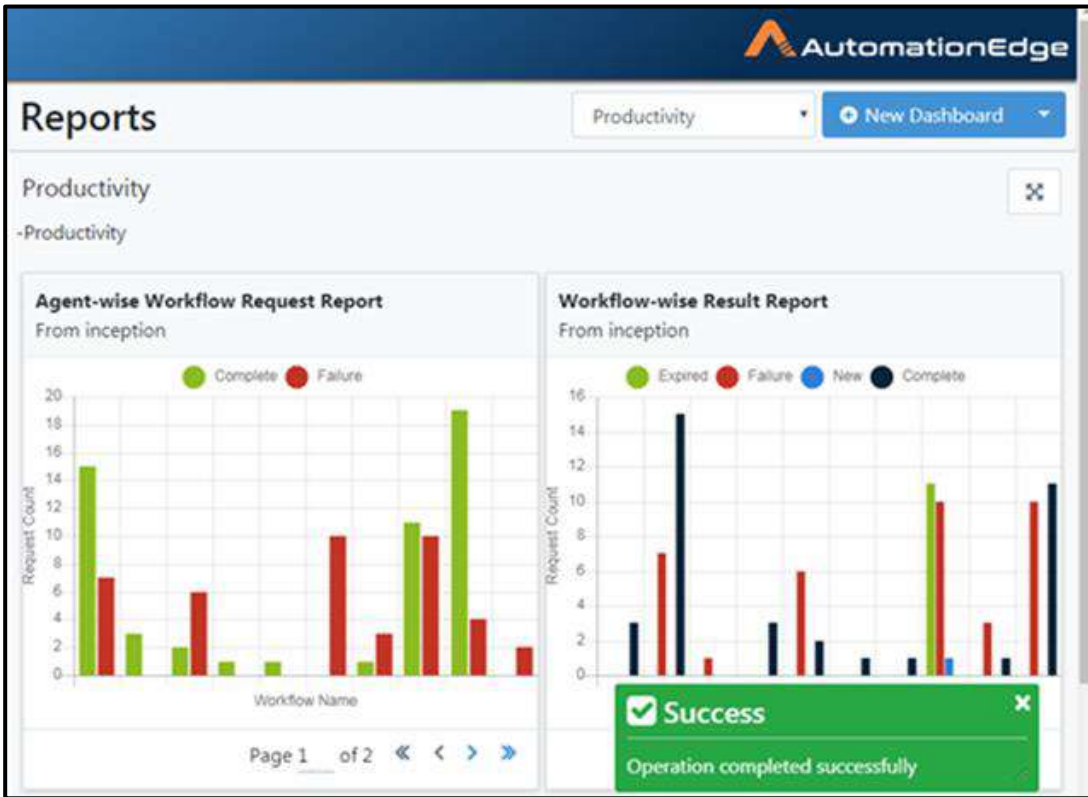


Figure 87f: Dashboard Set as Default

- Set as Default is no longer visible for Productivity dashboard as it is already the default dashboard as seen below.

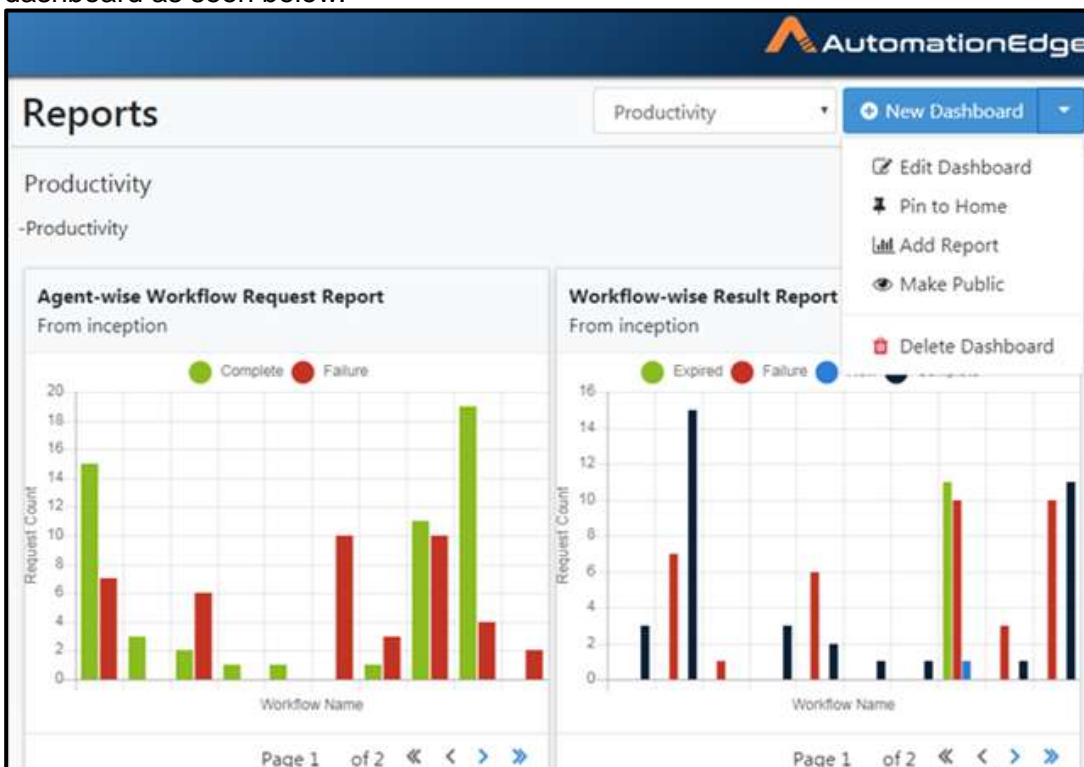


Figure 87g: Set as Default option not available

11.1.3.3 Pin to Home

1. Click the Arrow next to New Dashboard. Click the third option Pin to Home.
2. Note the message Dashboard [Productivity] set as home dashboard.

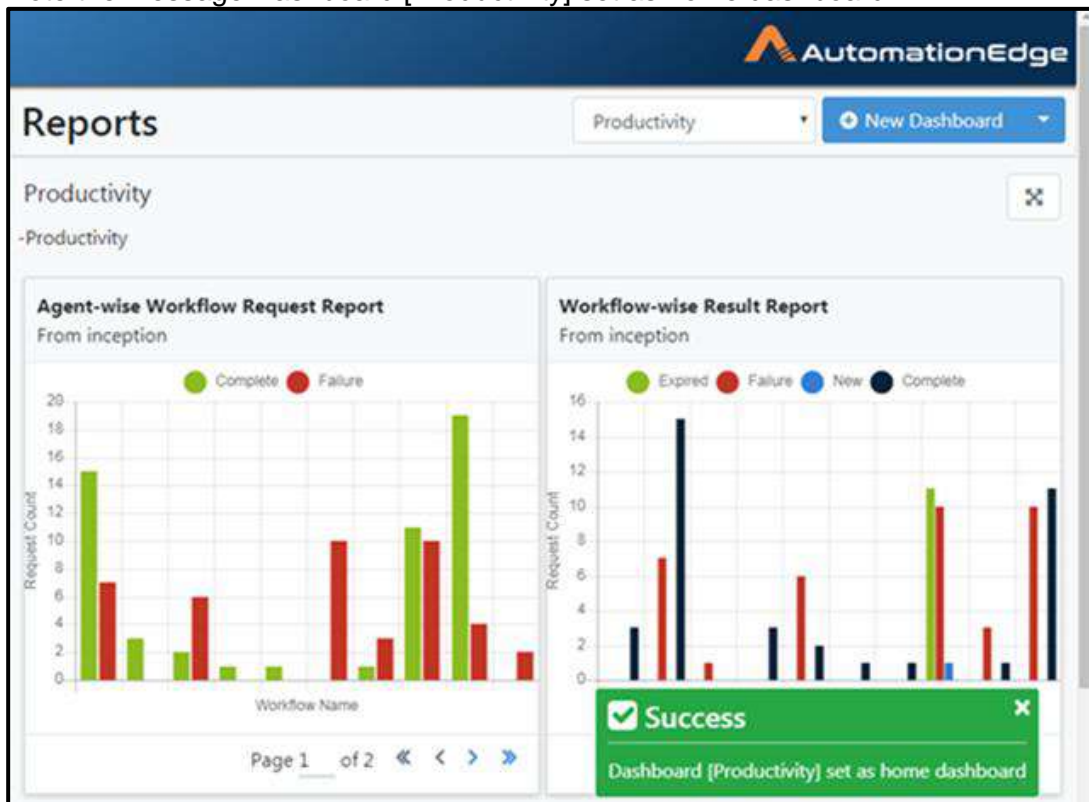


Figure 87h: Dashboard Set as Home Dashboard

3. Go to the Home page. You can see that the Productivity Dashboard is now set as home page.



Figure 87i: Review Home Dashboard

4. Click the arrow next to New Dashboard. You can see that for Productivity Dashboard Pin to Home is no longer visible. You have the option Unpin from Home.
5. Click Unpin from Home to reset the Home page to default.

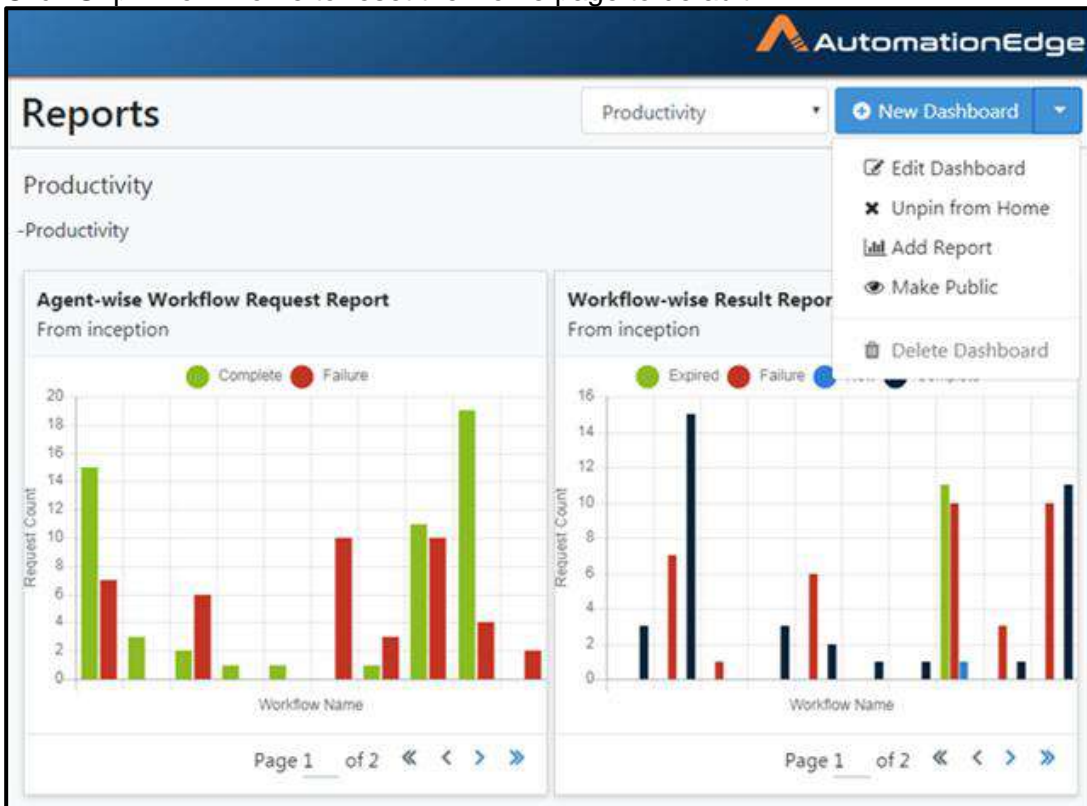


Figure 87c: View Unpin from Home

- Note the message Dashboard [Productivity] removed as home dashboard.

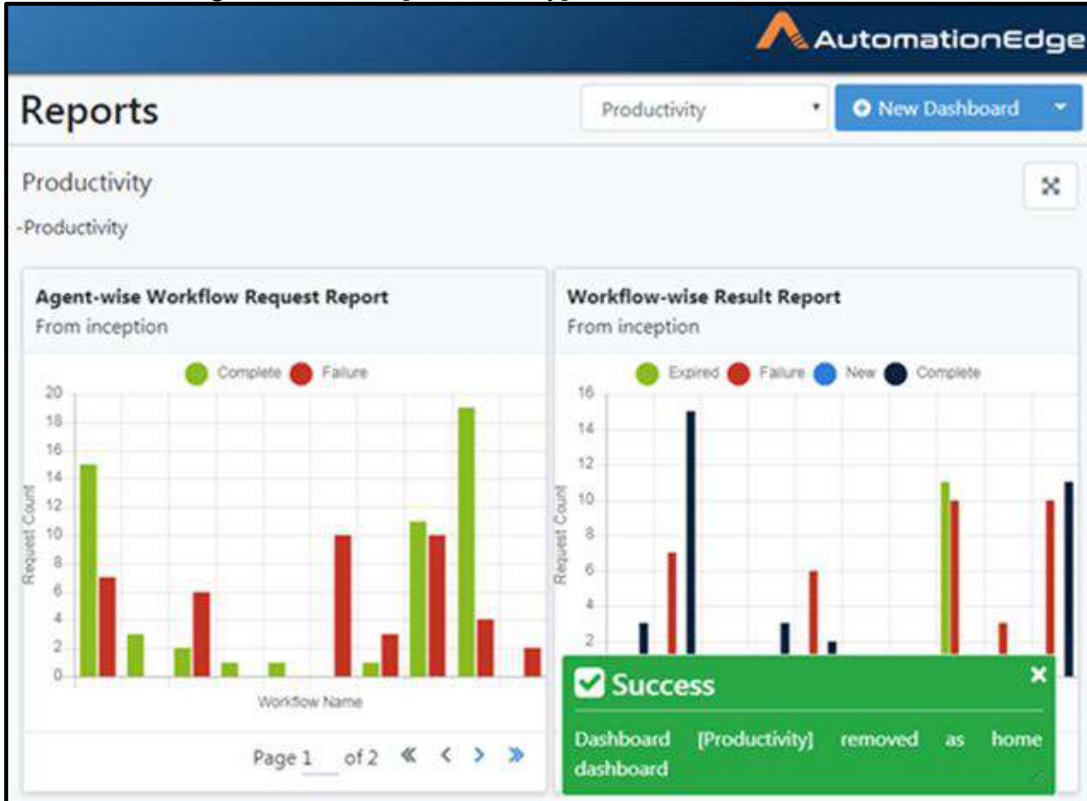


Figure 87c: Dashboard removed as Home Dashboard

11.1.3.4 Add Report

Add Report has been discussed in detail in the section Add Report.

11.1.3.5 Make Public

Following are the steps to make a Dashboard Public.

- Click the Arrow next to New Dashboard. Click the fourth option Make Public.
- Note the message Dashboard [Productivity] Access Level set to Public.
- Notice (Public) is suffixed next to the Dashboard name.

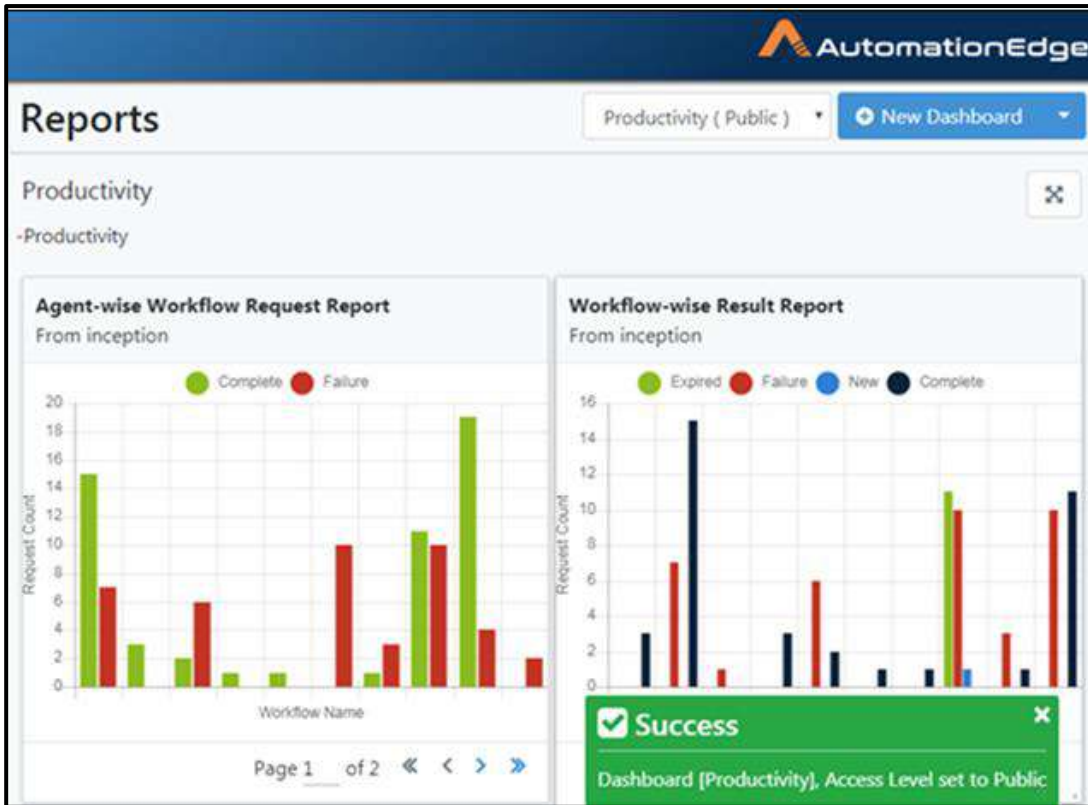


Figure 87c: Dashboard made public

4. Login with another user in the same Tenant. Notice that the user is able to see Productivity (Public) as seen below. All users in the Tenant will be able to see the public dashboard.

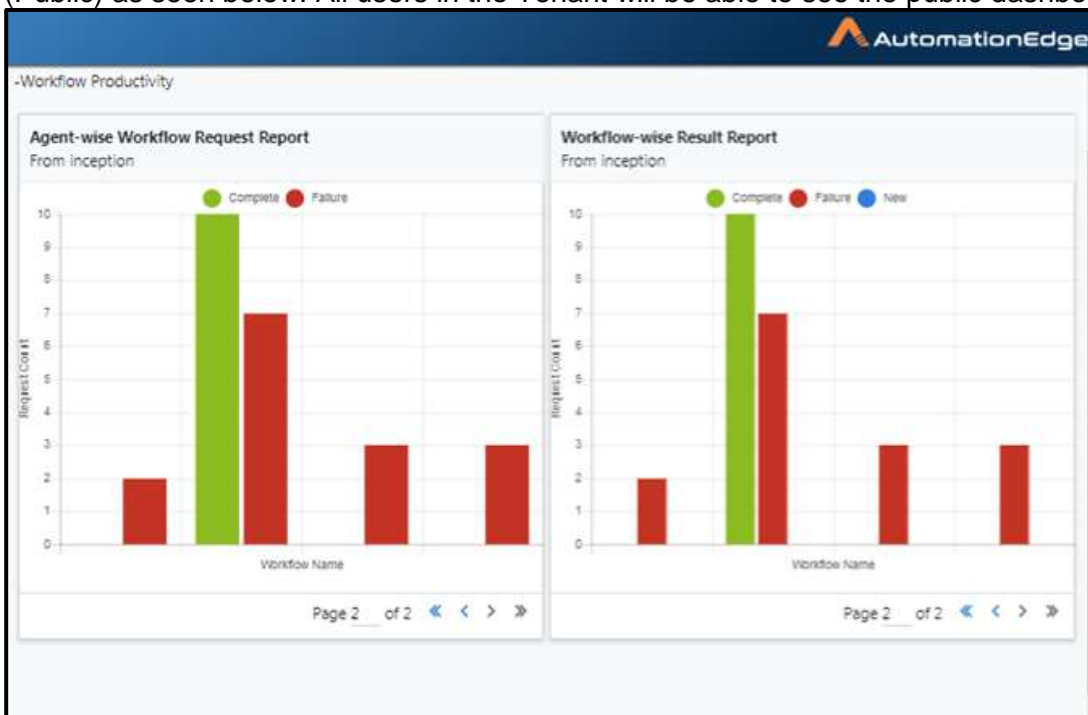


Figure 87c: Other users can see public Dashboard

- Click the arrow next to New Dashboard. Make Public is no longer visible. You can now see Make Private.

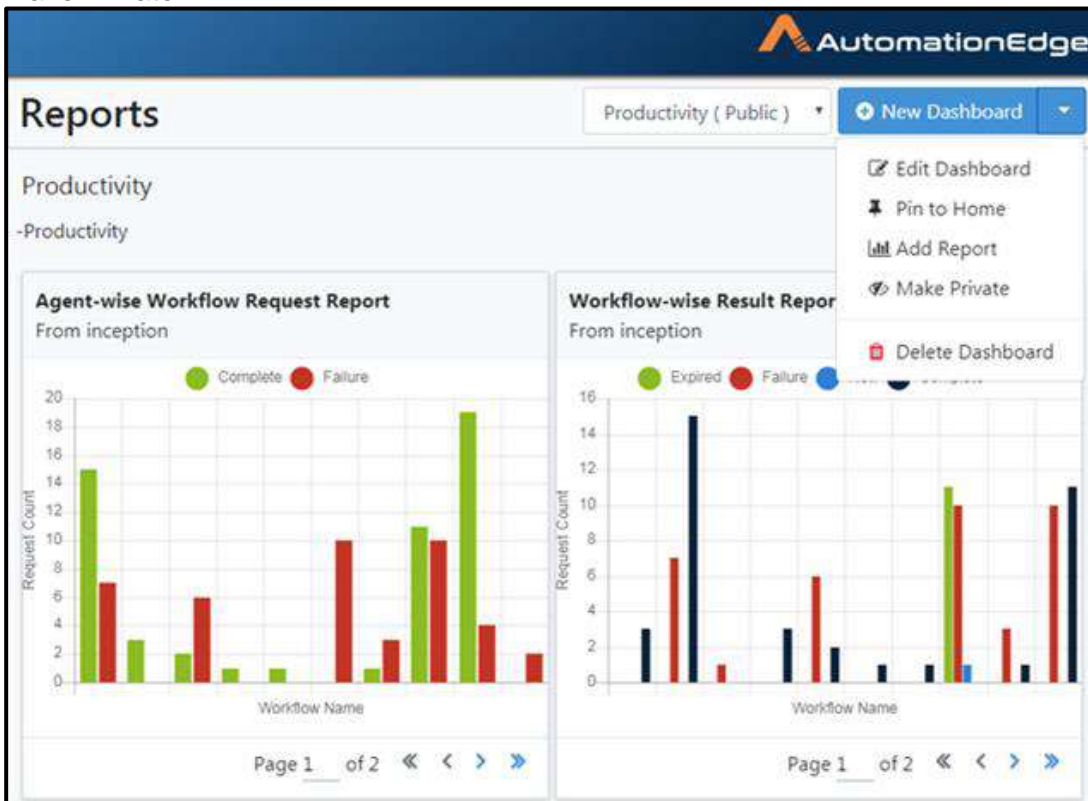


Figure 87c: Make Dashboard Private

- Click Make Private. Note the message Dashboard [Productivity] Access Level set to Private. You can no longer see the suffix (public) next to Productivity.

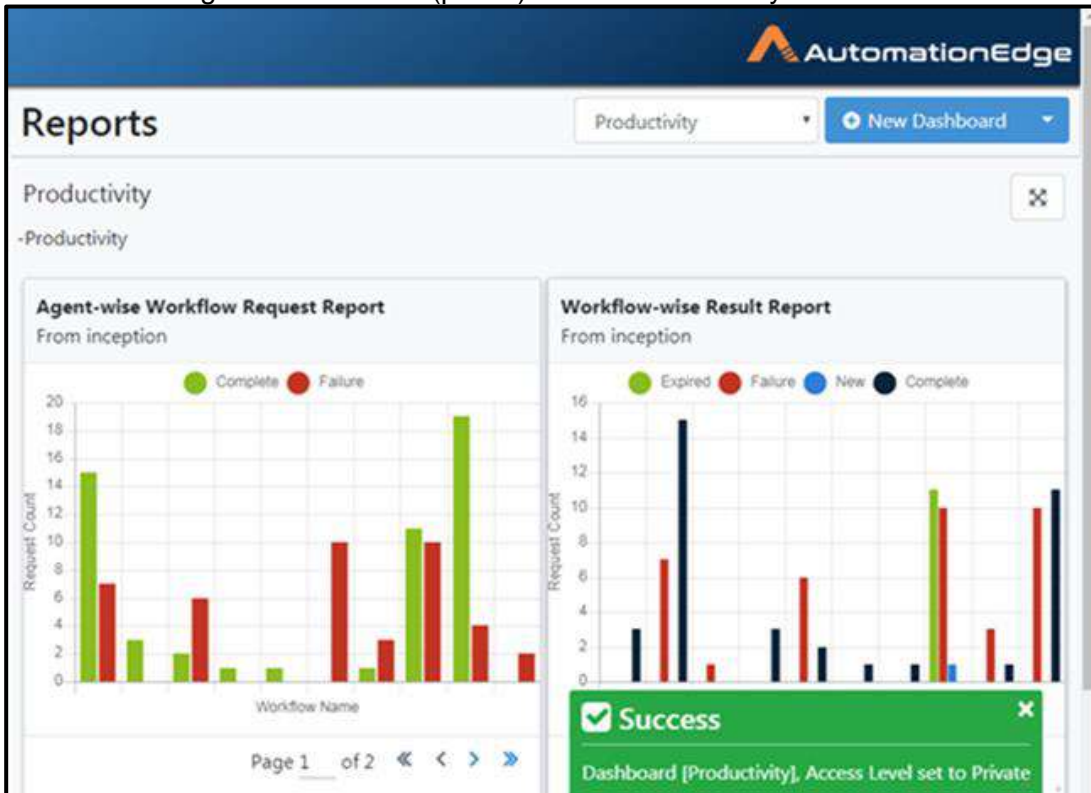


Figure 87c: Dashboard made Private

11.1.3.6 Delete Dashboard

Click the Arrow next to New Dashboard. Click the last option Delete Dashboard to delete the Dashboard.

11.2 Maintain Reports on Dashboard

11.2.1 Add Report

Reports can be created and viewed as Line graphs, Bar charts, Doughnut Chart, Line Chart, Pie chart, Polar Area and Radar. A tabular view is available for all reports. Reports can be generated by choosing periods based on dates or relative periods like hours, minutes, days, weeks or months. You can also edit dashboards to get the options to edit reports.

Following are the steps to create a New Report,

1. Go to the Requests menu.
2. Select a Dashboard from the field dropdown list.

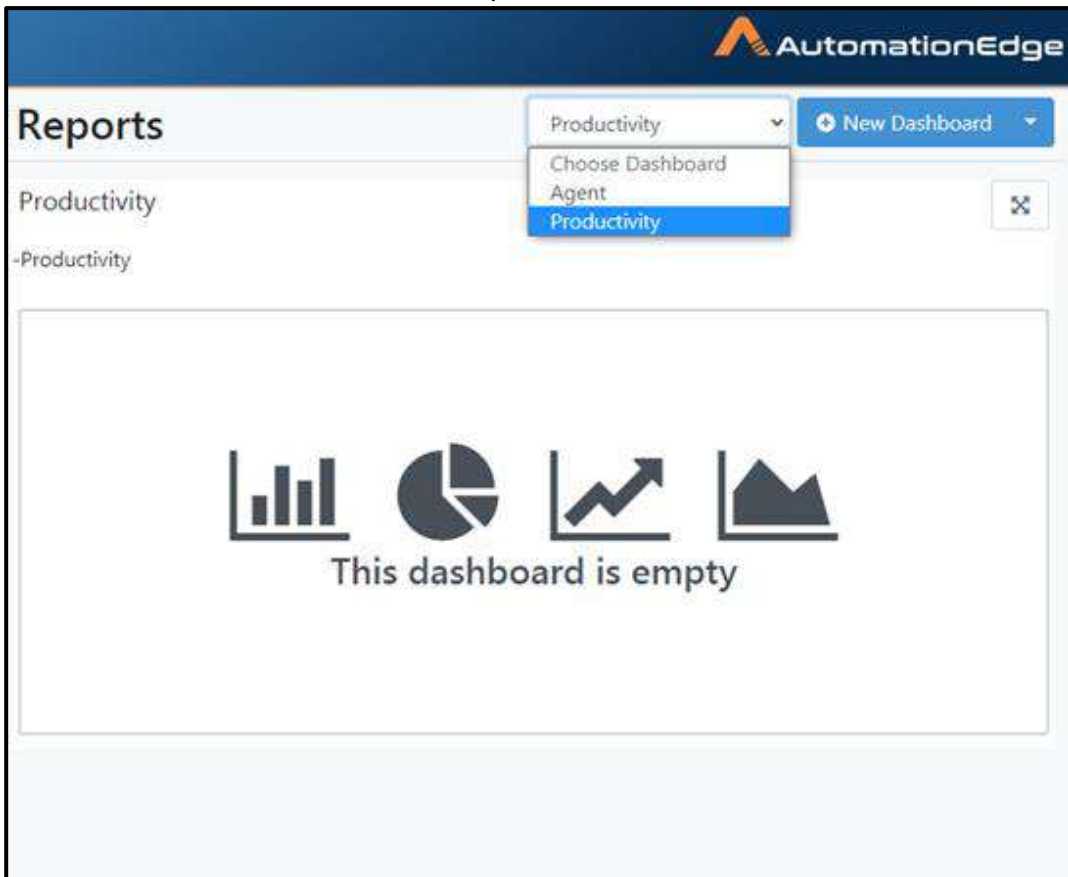


Figure 88a: Select Dashboard

3. The dashboard selected(Productivity) is now the current dashboard.

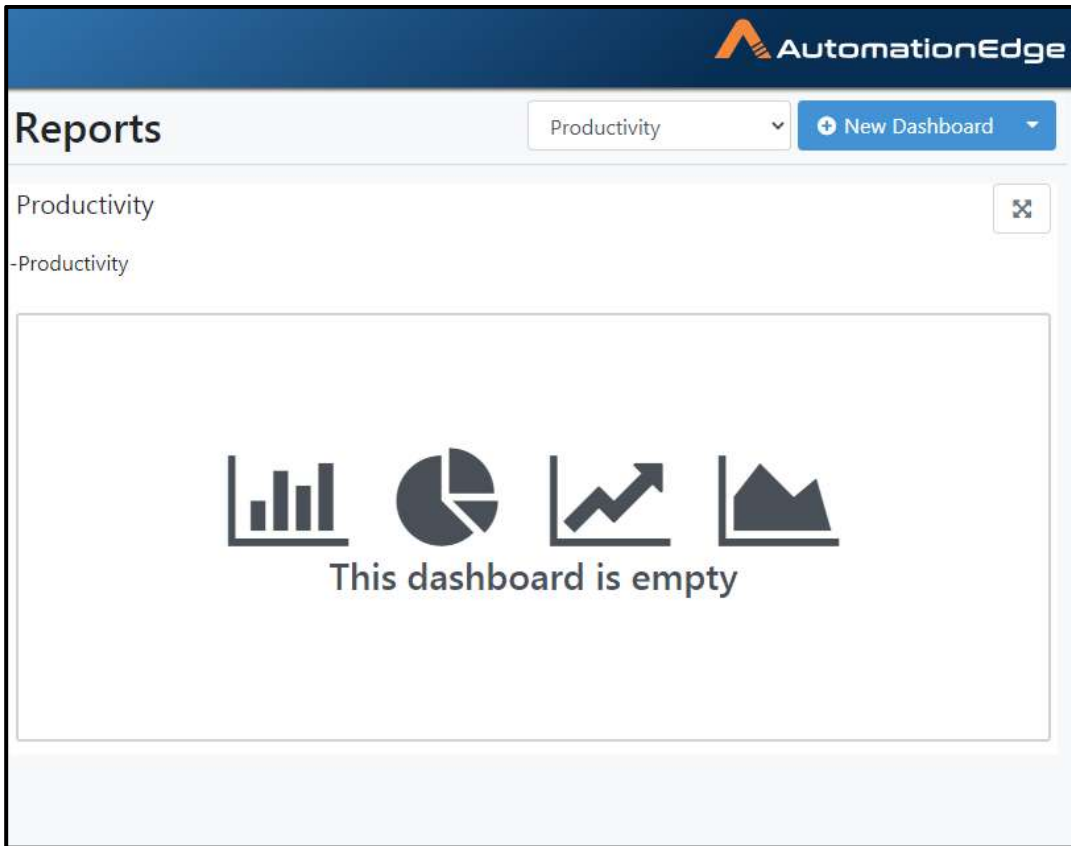


Figure 88b: Dashboard Productivity selected

4. Click the dropdown arrow next to New Dashboard. Click Add Report.

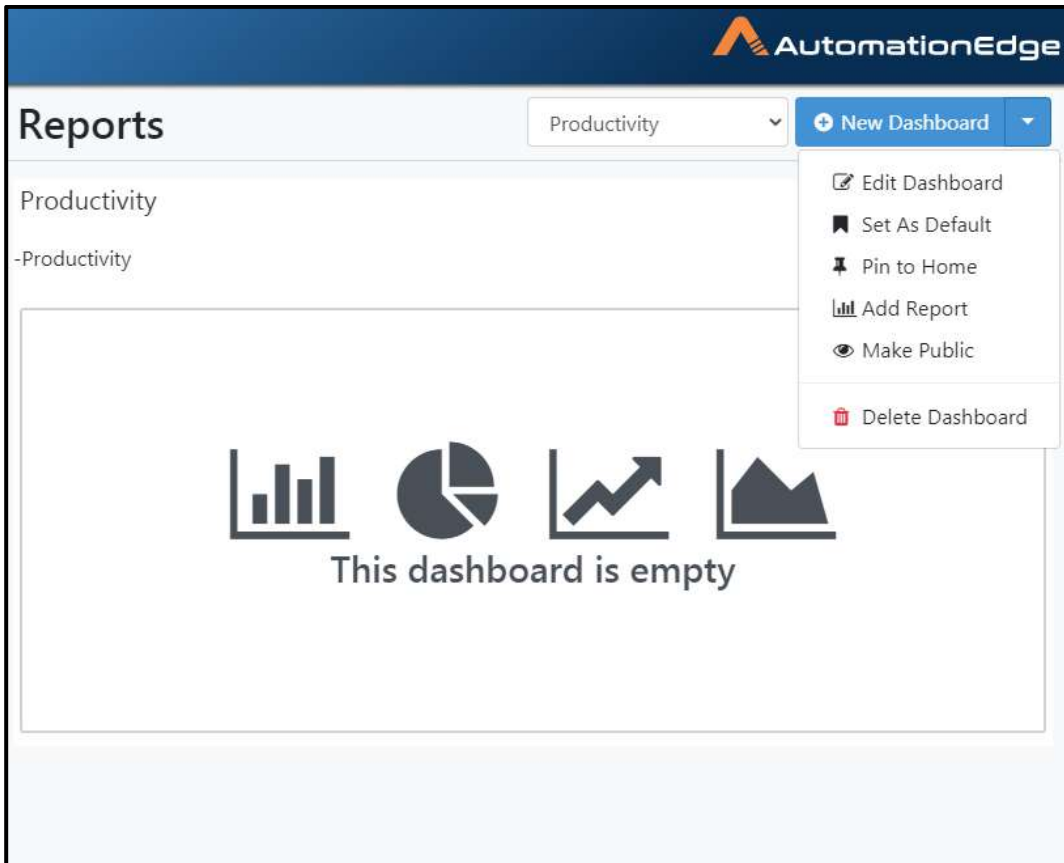


Figure 88c: Add Report

5. Provide the details, for the new report to be added to the Dashboard. The Add Report configuration options are described in the following table.

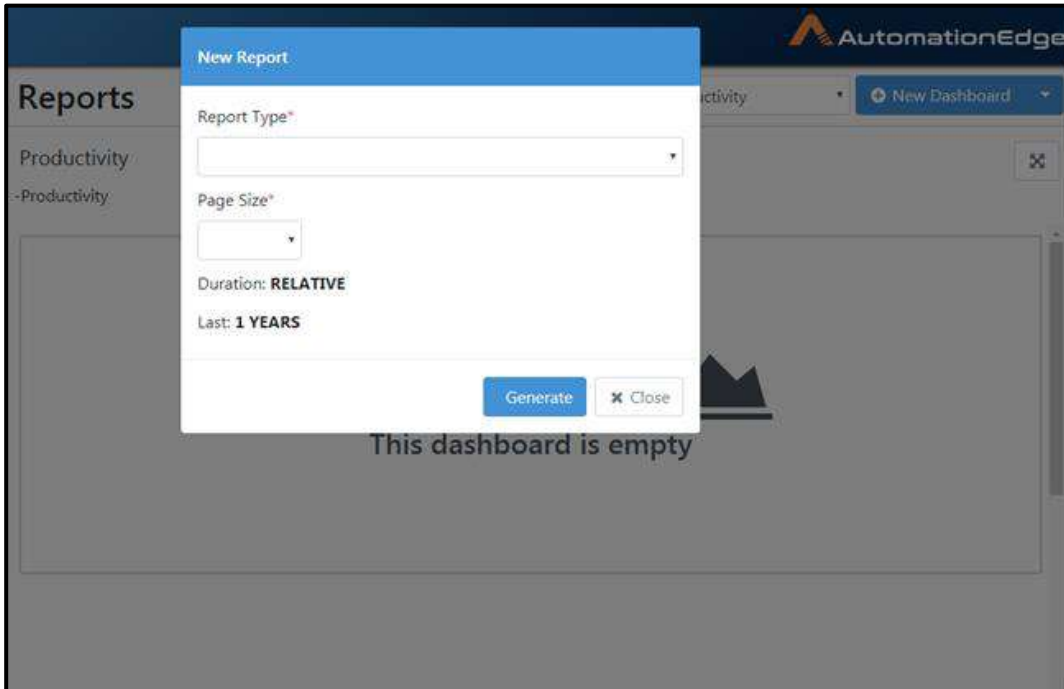


Figure 88d: Add New Report to 'Agent' Dashboard

The following table provides a description of the fields for report creation.

Table 58: Reports Features

Field	Description
Report Type	Select a Report Type from a list of pre-existing reports.
Page Size	Select a page size from the drop down list from 10,20,30,40 or 50.
Duration*	If the Use Dashboard Level Duration for reports is enabled on the dashboard, then Duration is inherited from Dashboard. Else choose from the Duration options: None, Today, Relative or Custom.
Duration – Custom:	If Custom is chosen the following fields display.
Start Date	Select a start date of the custom duration.
End Date	Select an end date of the custom duration.
Duration – Relative:	If Relative is chosen the following fields display.
Last	Put a number for minutes, hours, days, months or years.

*Description and of the Duration Types is same as provided in the section above on New Dashboard.

17. Select a Report Type from the Report Type drop down list. AutomationEdge comes with 16 predefined reports.

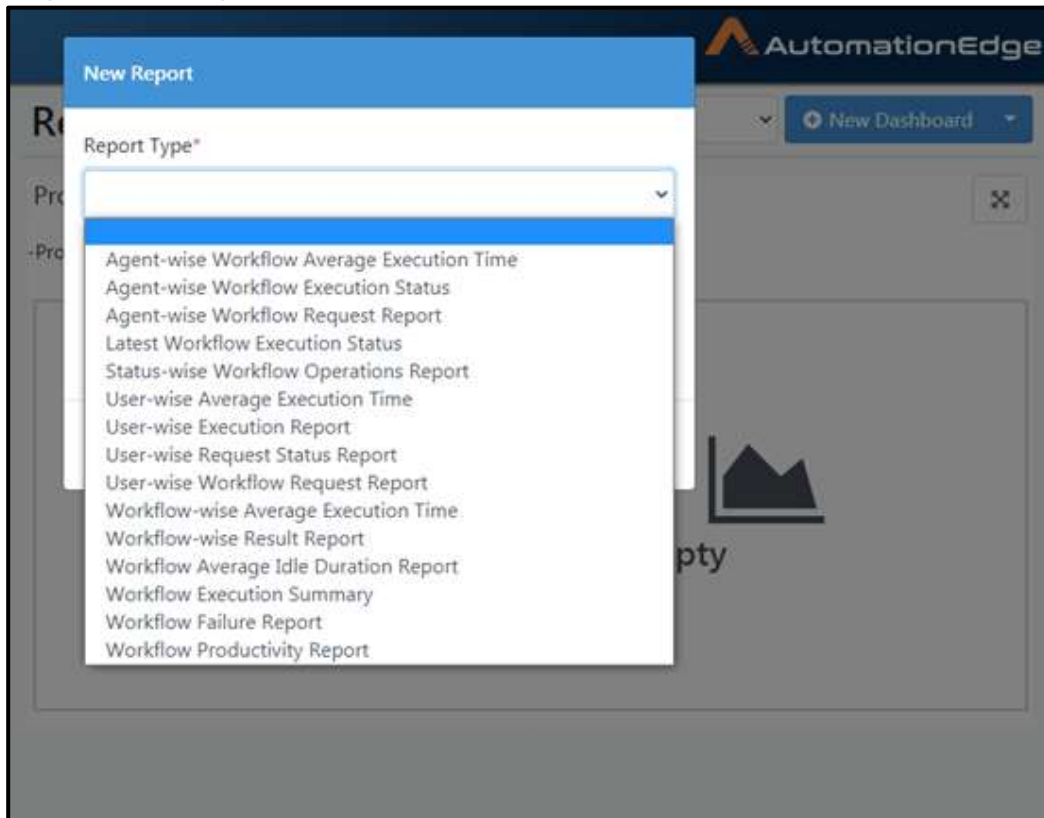


Figure 88e: New Report Creation: Selection of Report

These reports can help you monitor your automation performance in several aspects. Refer to [11.3 Out of the box Reports](#) for a description.

18. The Page size field has drop down as seen below.

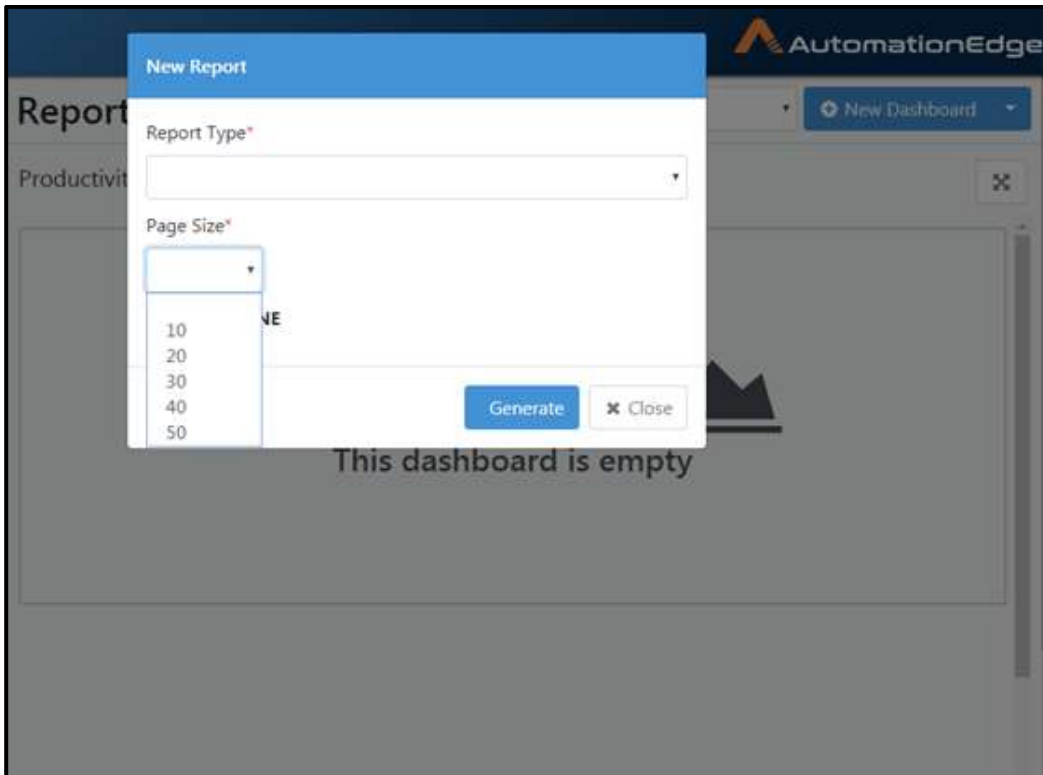


Figure 88g: New Report Creation: Selection of Page Size

19. Once Report Type is chosen additional fields are visible on the New Report window as seen below.
20. Click radio button for Generate on Workflows or Categories.
21. Choose from the list of workflows or categories.
22. Select a Page Size from the drop down list to determine the number of rows that are visible on the first page of the report on the dashboard. Possible page size values are 10,20,30,40 or 50. Page size is mandatory.

23. Duration type may be inherited from the Dashboard. In the screenshot below Duration is not inherited and duration option can be chosen from the drop down list.

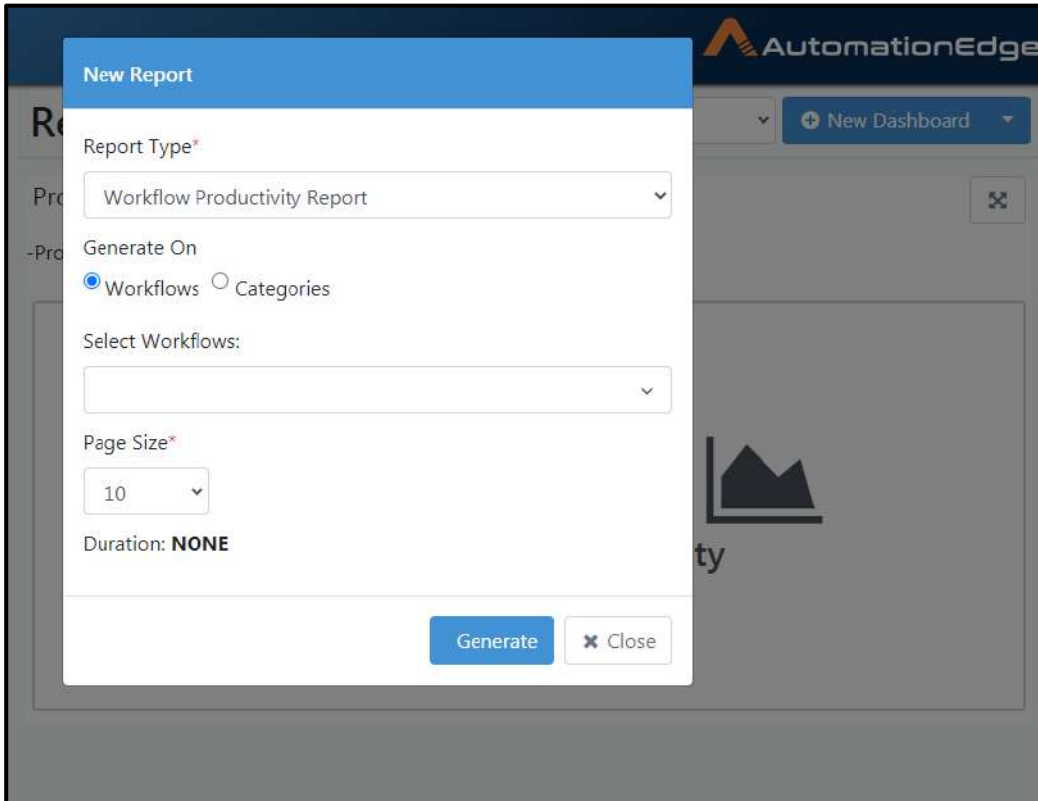


Figure 88h: Reports Duration Option

24. If the Duration inherited is NONE the Duration NONE is visible as shown below.

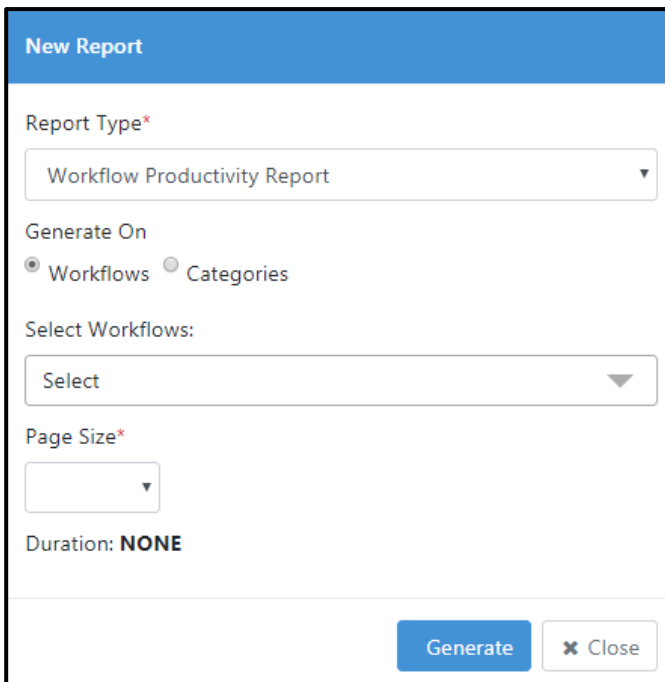
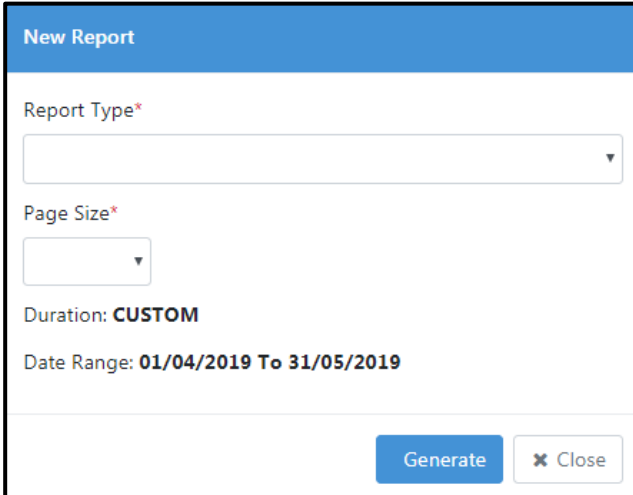


Figure 88i: New Report Creation: Duration NONE inherited from Dashboard

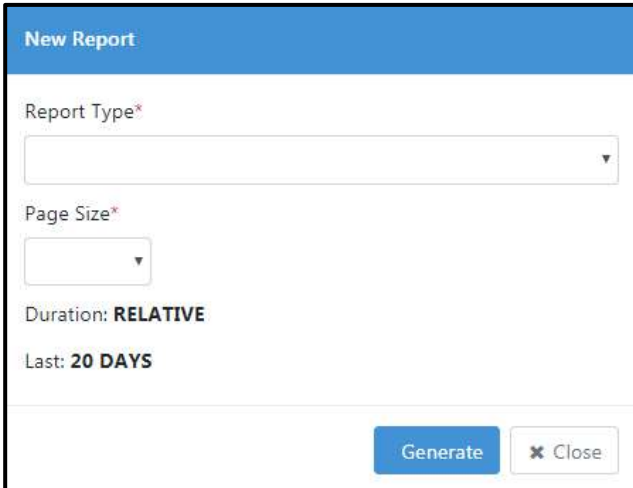
25. If the Duration inherited is Custom, then Custom Start Date and Custom End Date fields are visible.



The screenshot shows a 'New Report' dialog box with a blue header. Below the header, there are two dropdown menus: 'Report Type*' and 'Page Size*'. Below these, the text 'Duration: CUSTOM' is displayed, followed by 'Date Range: 01/04/2019 To 31/05/2019'. At the bottom right, there are two buttons: 'Generate' and 'Close'.

Figure 88j: New Report Creation: Select Duration Type

26. If duration inherited is Relative the Last number of days, minute, hours, days, months or years is visible.



The screenshot shows a 'New Report' dialog box with a blue header. Below the header, there are two dropdown menus: 'Report Type*' and 'Page Size*'. Below these, the text 'Duration: RELATIVE' is displayed, followed by 'Last: 20 DAYS'. At the bottom right, there are two buttons: 'Generate' and 'Close'.

Figure 88k: Choose relative period

27. The following snapshot shows that report will be created on fourteen filtered workflows since inception as duration selected is NONE. If no workflows are selected, then all workflows are included in the report. Click Generate.

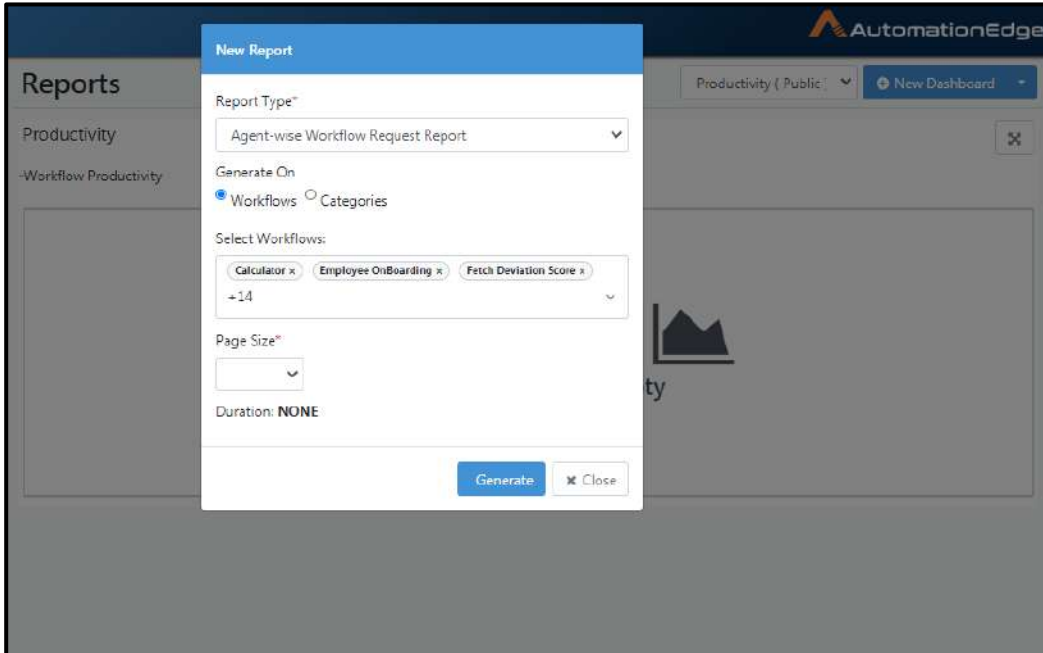


Figure 88l: Report Configurations

28. Upon generation the Report View is visible.

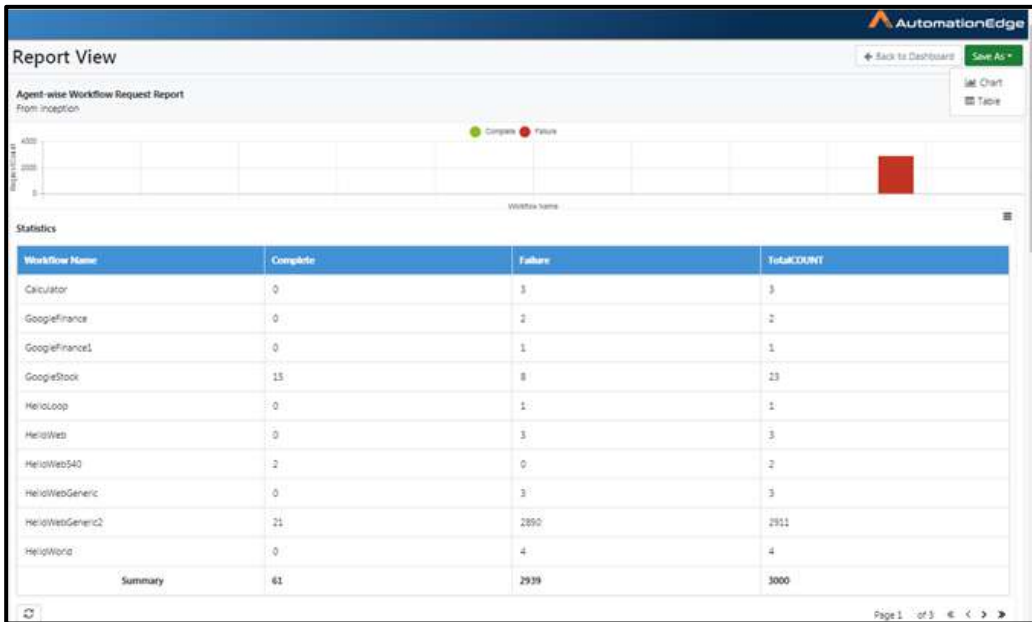


Figure 88m: Report View

29. Click 'Add As' button and choose Chart or Table to add the report to the current dashboard. Or Close the report clicking on button Back to Dashboard.
30. If you 'Add As' Chart a Save As pop-up is displayed asking to confirm the Title of the report. Click Save.

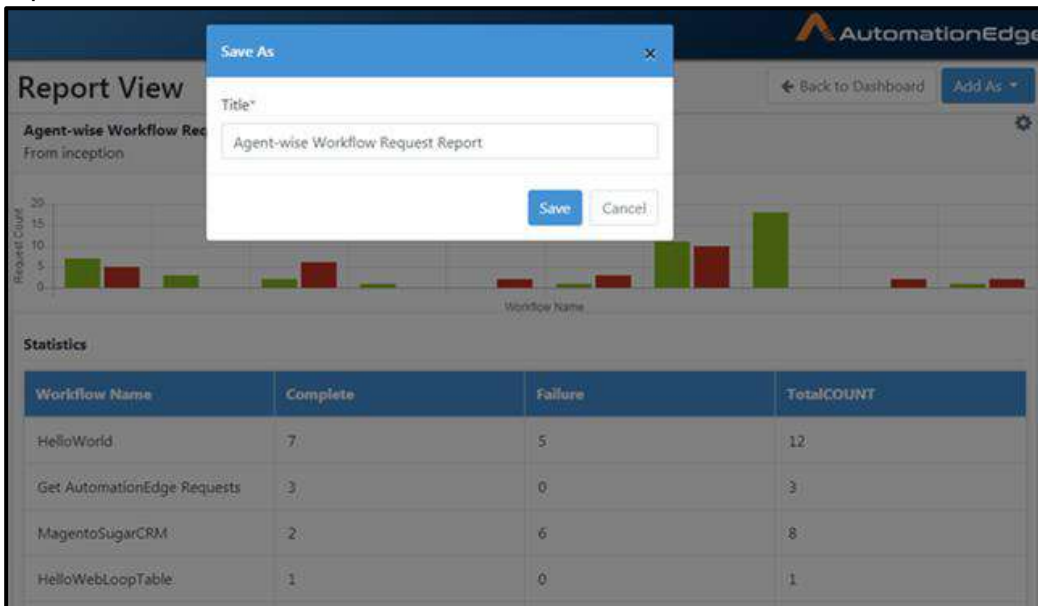


Figure 88n: Chart Report on Dashboard

31. The Chart report is visible on the dashboard as shown below and Report added successfully message is displayed.



Figure 88o: Chart Report on Dashboard Added Successfully

32. In case chart has more than one page the right scroll bar is enabled.

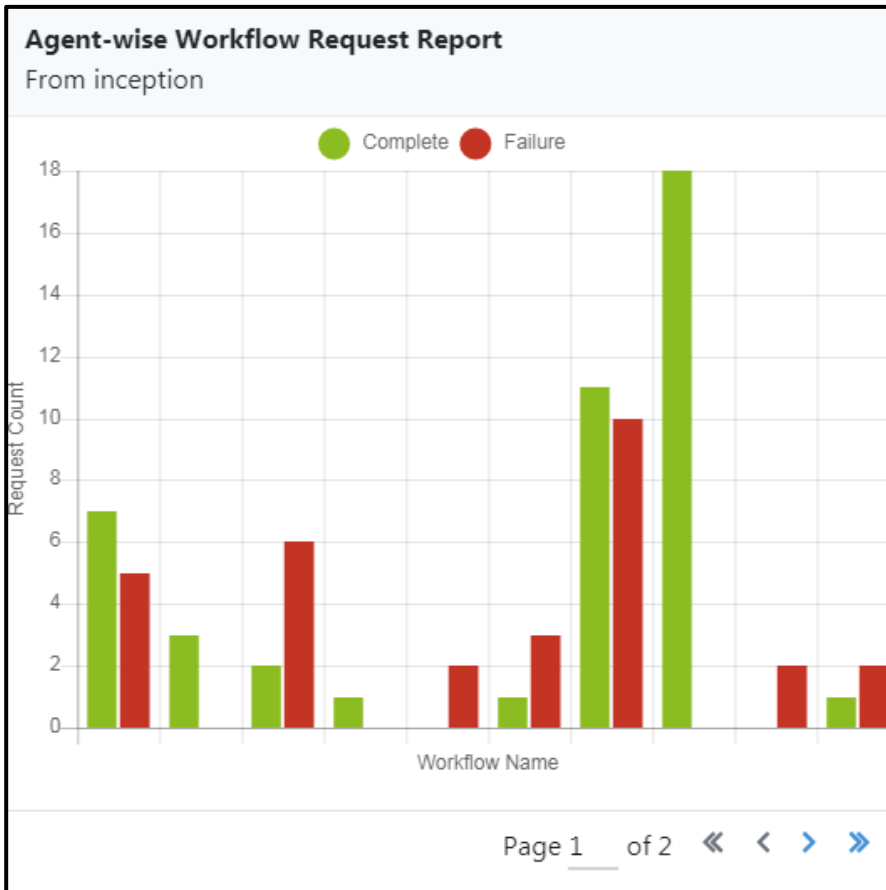


Figure 88p: Table Report on Dashboard saved successfully

33. You may maximise the report by clicking on the maximise icon at the bottom of the report.



Figure 88q: Maximise icon

34. Clicking on the Maximise icon opens the Report View as shown below. In the tabular section there is an icon on the top right corner. Click on this icon to see the columns as shown below.



Figure 88r: Column name toggle for tabular views in Report View

35. You may select or deselect any column to add or remove it from the table. In the snapshot below the Failure column is de-selected and is also removed from display.

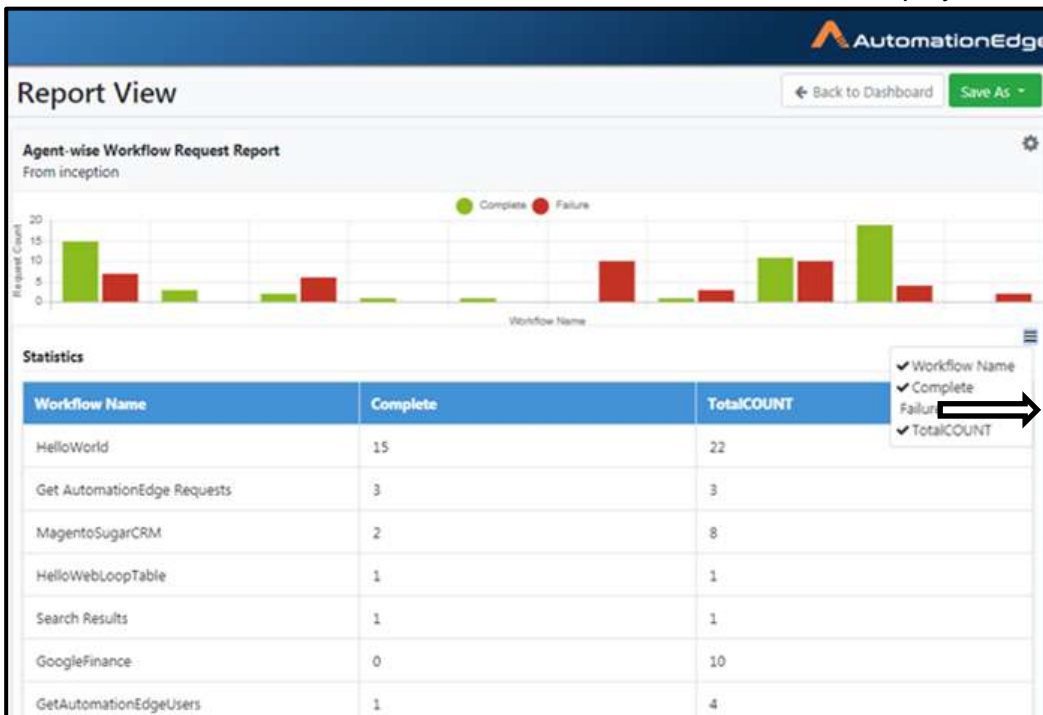


Figure 88s: Column name toggle

36. You may Save As, Table as shown below.

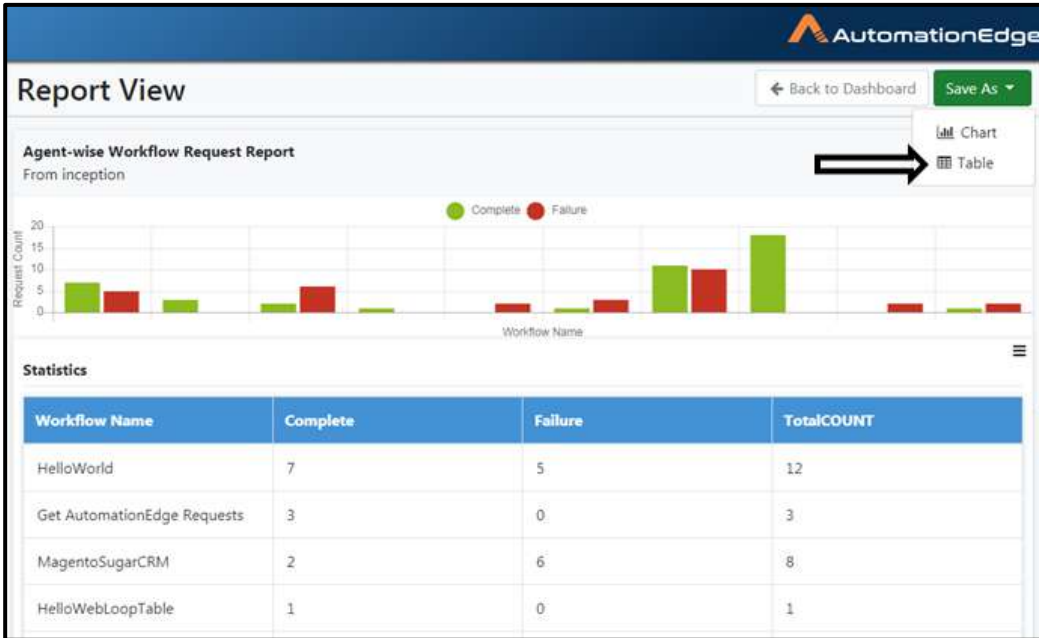


Figure 88t: Column name toggle

37. You may change the title suitably in the Title field shown below. Click Save.

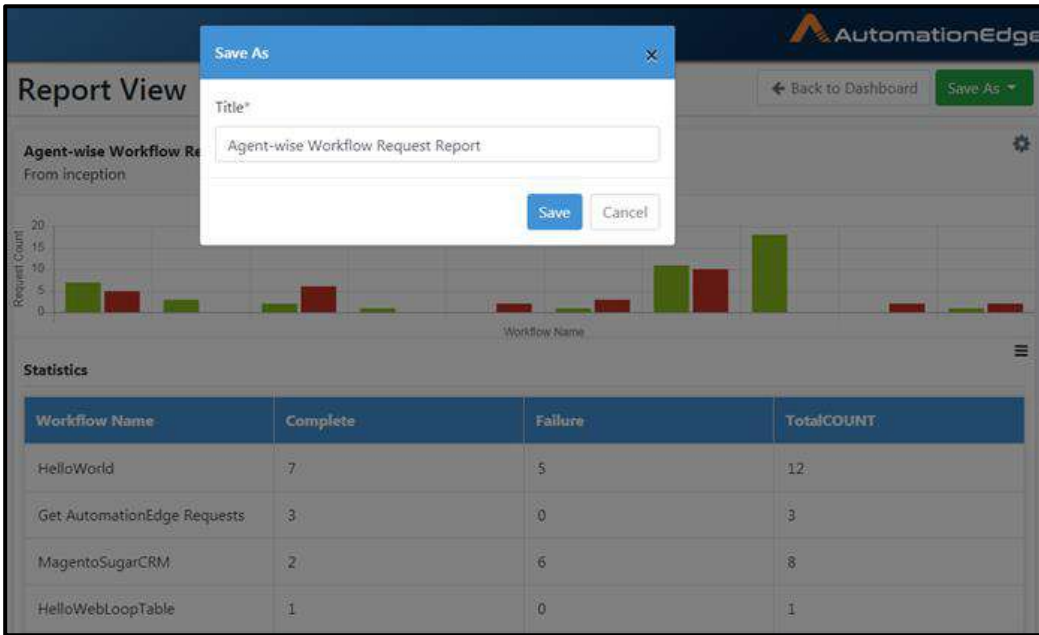


Figure 88u: Column name toggle

38. A tabular view of the table is saved on the dashboard as seen below. In addition to the Report View the toggle to see the column names is also visible on the table on the dashboard. You may select or deselect the columns. In the snapshot below Failure column is deselected and is not visible in the tabular report.

Workflow Name	Complete	TotalCOUNT
HelloWorld	7	12
Get AutomationEdge Requests	3	3
MagentoSugarCRM	2	8
HelloWebLoopTable	1	1
GoogleFinance	0	2
GetAutomationEdgeUsers	1	4
OSTicket	11	21

Figure 88v: Table Report on Dashboard saved successfully

39. In the snapshot below Failure column is selected and is visible in the table.

Workflow Name	Complete	Failure	TotalCOUNT
HelloWorld	7	5	12
Get AutomationEdge Requests	3	0	3
MagentoSugarCRM	2	6	8
HelloWebLoopTable	1	0	1
GoogleFinance	0	2	2
GetAutomationEdgeUsers	1	3	4
OSTicket	11	10	21

Figure 88w: Column name toggle

40. In case the tabular report has more than one page's right scroll bar is enabled.

Agent-wise Workflow Request Report			
From inception			
HelloWebLoopTable	1	0	1
GoogleFinance	0	2	2
GetAutomationEdgeUsers	1	3	4
OSTicket	11	10	21
HelloWebGeneric2	18	0	18
IT Categorization	0	2	2
RemoteDesktop	1	2	3
Summary	48	32	80

Page 1 of 2

Figure 88x: Table Report on Dashboard with scroll to right option enabled

41. This completes the process of adding reports to dashboard.

11.2.2 Managing Reports

11.2.2.1 Custom Positioning of Reports on Dashboard

Once added to dashboard reports can be rearranged by moving them within the dashboard.

1. Reports can be moved left and right as well as up and down on the dashboard.
2. Reports can be resized to a preferable width and height. Reports can be resized up to a maximum of page width and a custom height.

- The following snapshot shows a sample dashboard with reports of same size

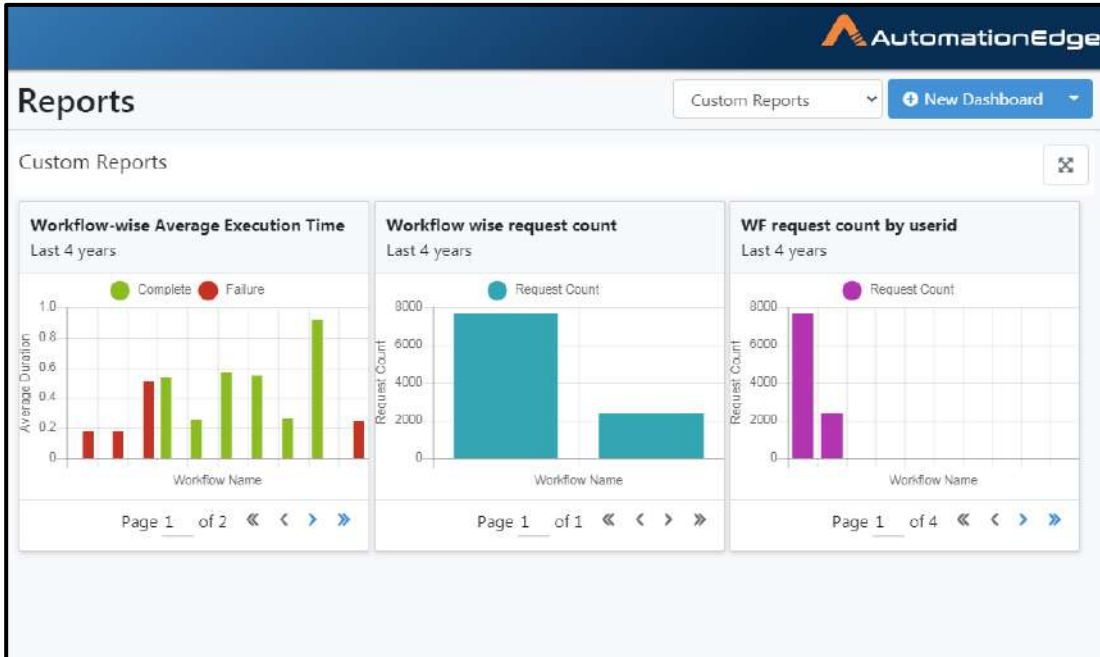


Figure 89a: Sample dashboard

- The following snapshot shows dashboard with custom sizing of reports on dashboard. The report on the left Request Count By User Id was stretched by pulling the right edge of the report.

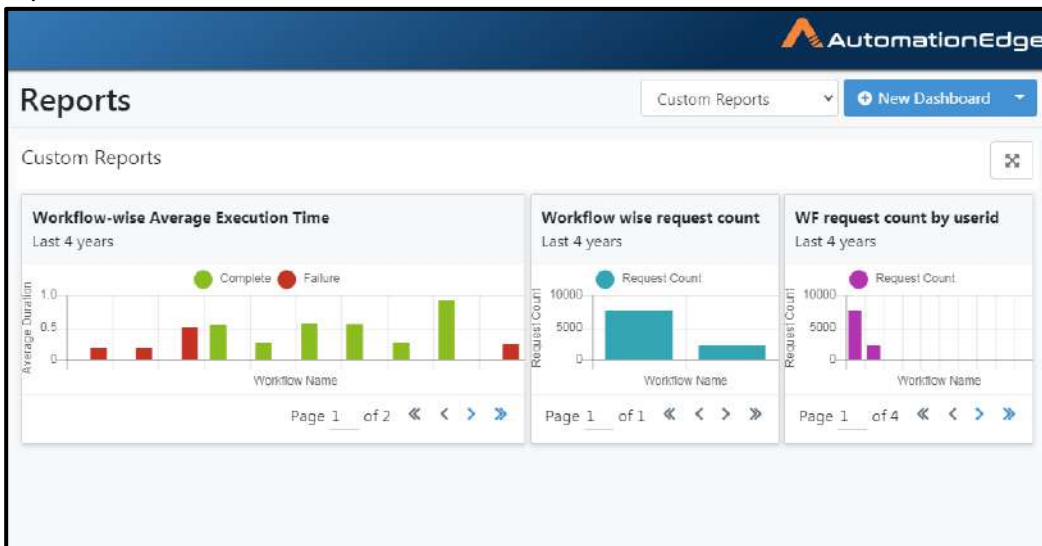


Figure 89b: Sample dashboard with custom sizing of reports

11.2.2.2 Report Options

There is a set of options at the bottom of each report. Hover anywhere on the report to see these options explained below.

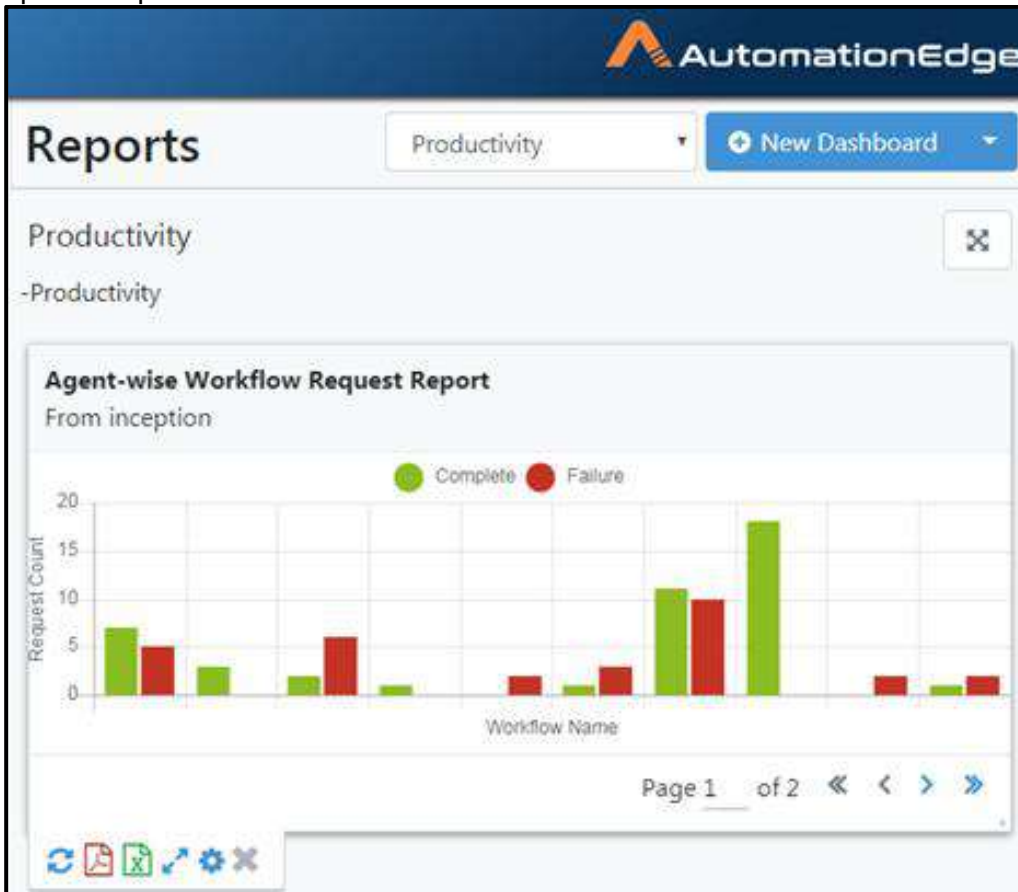


Figure 89c: Report Options bottom left corner of the chart report

The six options are described below.

- i. The first option is to refresh the report.
- ii. Download that report in PDF format, by clicking pdf icon.

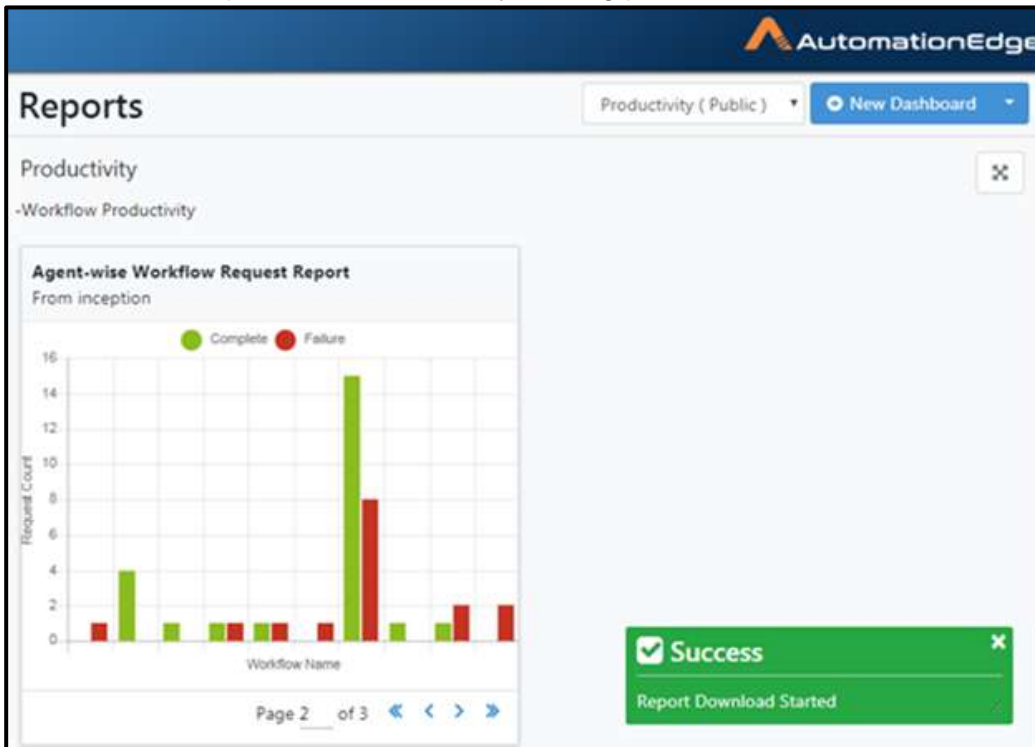




Figure 89d: Download pdf

- iii. Download that report in excel format, by clicking excel icon ().
- iv. You can edit the report by opening the report in Report View. Maximise the report by clicking () icon. It opens the Report View.

- v. You can change the report from chart to table or vice-versa. For Chart you can change the chart type by choosing a chart type as depicted in the screenshot below.

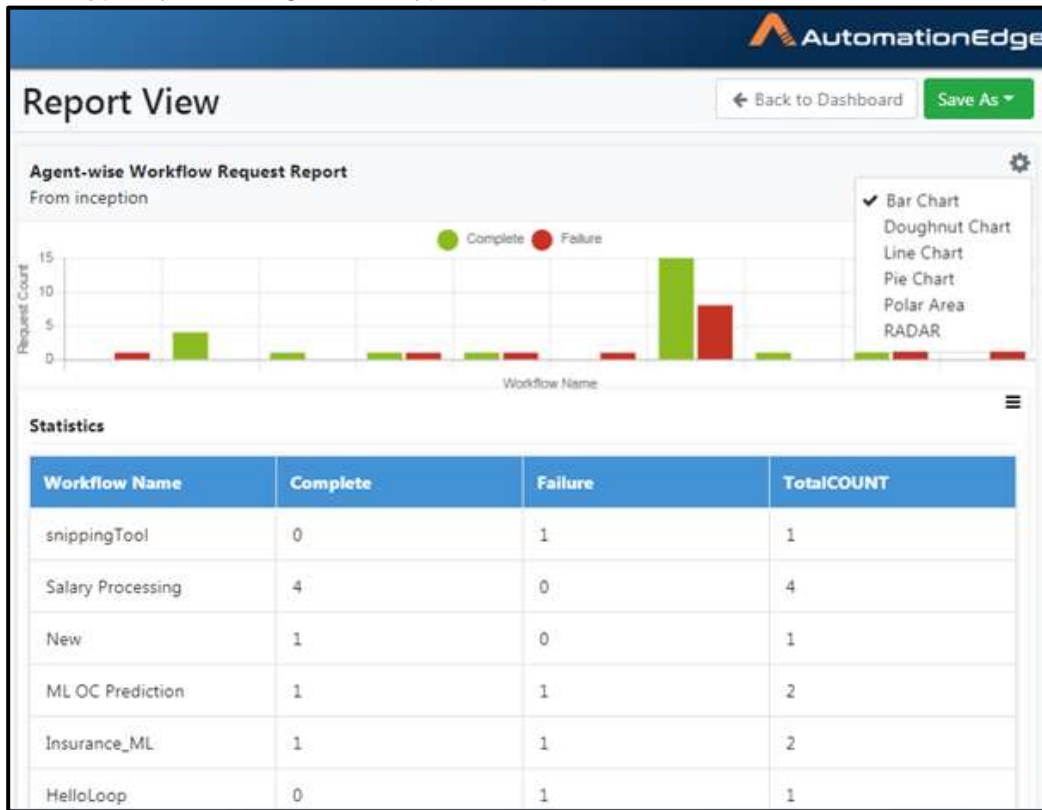


Figure 89e: Edit Report in Report View

- vi. You can also change labels for columns in report in the Report View. Just click on any column heading label as seen in the screenshot below and overwrite it. These new labels are persistent.

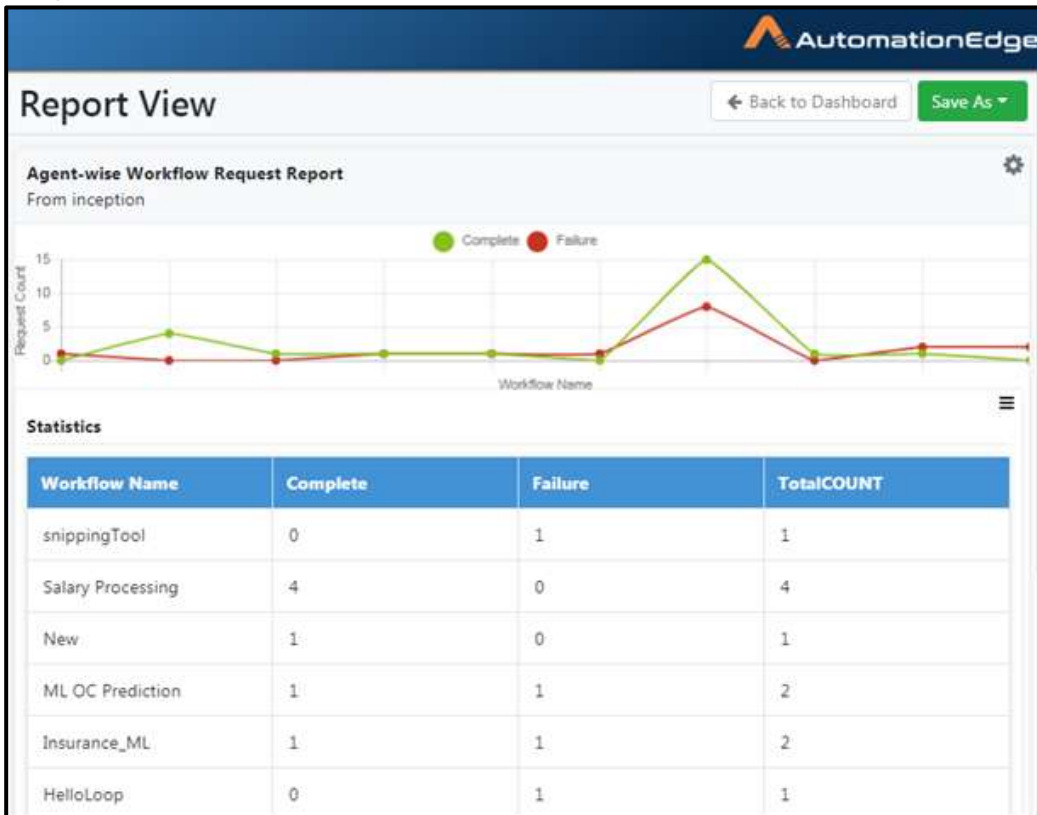


Figure 89f: Edit column label in Report

- vii. Click Report Settings (⚙️) to update the report configuration.

The 'Update Report' dialog box contains the following configuration options:

- Report Type*:** Agent-wise Workflow Request Report
- Generate On:** Workflows Categories
- Select Workflows:** Calculator x Employee OnBoarding x
- Page Size*:** 10
- Duration:** NONE

Buttons: Generate, Close

Figure 89g: Reports Settings

- viii. Click (✖) to delete the report from the dashboard. Upon clicking the delete icon, a pop-up message appears to confirm removal of the report.

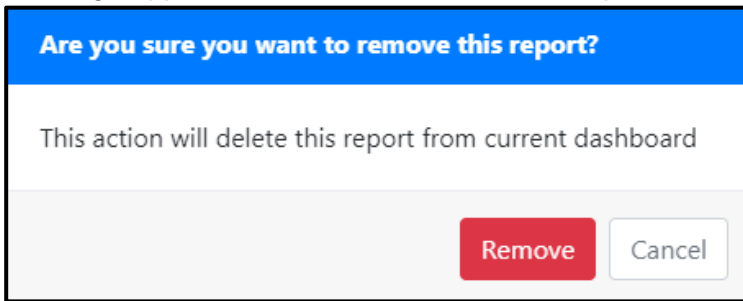


Figure 89h: New Report Creation: Deletion Confirmation

11.3 Out of the box Reports

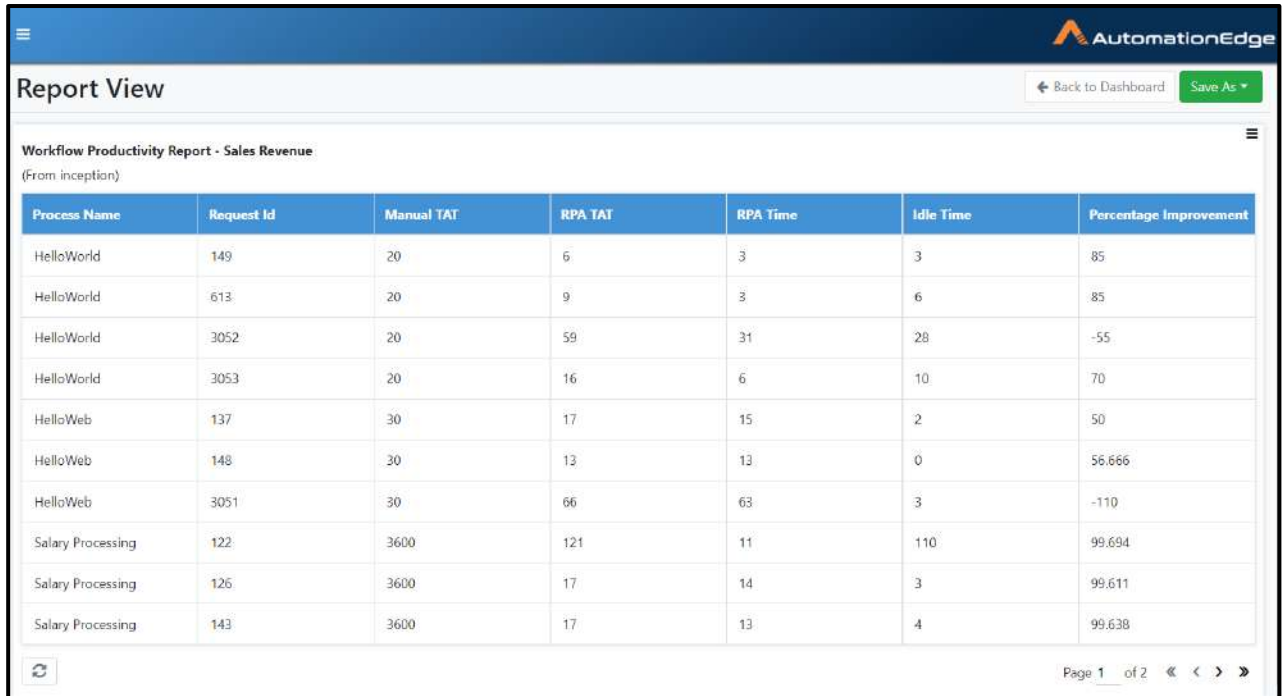
AutomationEdge comes with 16 predefined report types; reports based on these can help you monitor your automation performance in several aspects. Following is the list of available Reports,

- i. Agent-wise Workflow Average Execution Time - Shows average time of execution of requests by Agent.
- ii. Agent-wise Workflow Execution Status – Shows workflow execution status such as Execution Started, Complete, failure or unknown by Agent.
- iii. Agent-wise Workflow Request Report–It shows the number of completed and failed requests by Agent.
- iv. Latest Workflow Execution Status– It shows the request status for the chosen period.
- v. Status-wise Workflow Operations Report– It shows the requests ordered by status
- vi. User-wise Average Execution Time - shows average request execution time for the User.
- vii. User-wise Execution Report– It shows the number of completed and failed requests by user.
- viii. User-wise Request Status Report –It shows the number of requests by the user for request status like New, Execution Started, Complete, failure or unknown.
- ix. User-wise Workflow Request Report – Shows report of User requests.
- x. Workflow-wise Average Execution Time - Shows average time execution of requests by Workflow.
- xi. Workflow-wise Result Report–It shows the number of completed and failed requests by request.
- xii. Workflow Average Idle Duration Report– Shows average idle time for a workflow after it is triggered. This will help in understanding load on the system, and adding/removing agents based on the information.
- xiii. Workflow Execution Summary–It is a report of all execution details of the workflows.
- xiv. Workflow Failure Report - Shows failed workflow requests.
- xv. Workflow Productivity Report–It compares manual turnaround time (TAT) with RPA TAT for the workflows. It readily shows the percentage improvement with RPA.

The following section explains one of the reports in detail,

11.3.1 Workflow Productivity Report

It compares manual turnaround time (TAT) with RPA TAT for the workflows. It readily shows the percentage improvement with RPA. Following is a sample Workflow Productivity Report snapshot. The columns are explained in the table below.



Process Name	Request Id	Manual TAT	RPA TAT	RPA Time	Idle Time	Percentage Improvement
HelloWorld	149	20	6	3	3	85
HelloWorld	613	20	9	3	6	85
HelloWorld	3052	20	59	31	28	-55
HelloWorld	3053	20	16	6	10	70
HelloWeb	137	30	17	15	2	50
HelloWeb	148	30	13	13	0	56.666
HelloWeb	3051	30	66	63	3	-110
Salary Processing	122	3600	121	11	110	99.694
Salary Processing	126	3600	17	14	3	99.611
Salary Processing	143	3600	17	13	4	99.638

Figure 88f: Workflow Productivity Report

Table: Workflow Productivity Report Description

No.	Column	Description
1	Process	The name of the AutomationEdge workflow
2	Request Id	The workflow execution Request Id
3	Manual TAT*	Manual execution time (in Seconds) specified while configuring a workflow
4	RPA TAT*	Total time taken by a workflow to complete execution (RPA Time + Idle Time). This is the same time that can be seen on the Requests tab.
5	RPA Time	Actual time (in Seconds) taken for the request to complete once it has been picked up by the Agent
6	Idle Time	The time span (in Seconds) between submitting a request and the Agent picking it up for execution
7	Percentage Improvement	It is the Improvement in terms of TAT as compared to manual execution It is calculated as below,

*TAT => Turn Around Time

11.4 Custom Reports

Custom Reports are typically required when there is a need to assimilate, workflow related data generated in AutomationEdge with customers' business data. Preferably a separate schema should be maintained for custom report creation. The users need to create and maintain the schema. It can contain business data in tables as well as AutomationEdge data preferably exposed as views.

AutomationEdge provides two features, Datasources and Templates to create and manage custom reports. Datasource is the schema from which report data is fetched. Templates are used to define the layout of the report in terms of data to be fetched from the Datasource and the report format.

Template creation permission to create tenant specific and workflow specific templates is available to Tenant Administrators and Workflow Administrators respectively. Tenant users can use these templates for creating reports.

Datasources and Templates are described in the sections below.

11.5 Datasources (for custom reports)

AutomationEdge needs to connect to an external database to fetch data for Custom Reports. The Datasources sub-menu provides options to Add, Update or Delete Datasources.

11.5.1 New Datasource

To create a new data source,

1. Click Reports menu and the Datasources sub-menu.
2. Click New Datasource button

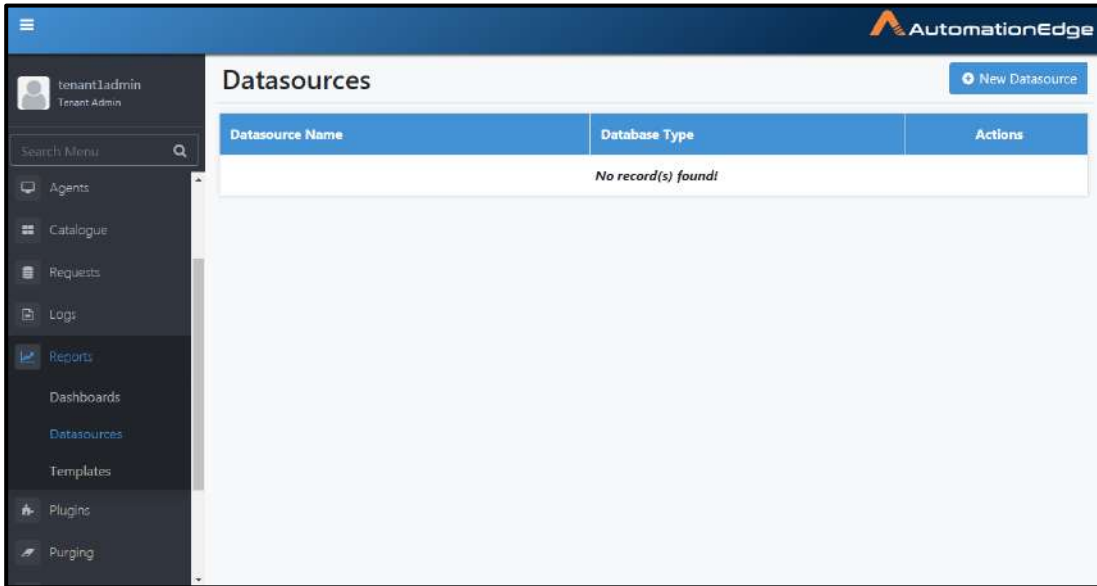


Figure 90a: Create New Datasource

3. Provide details as shown in the image below and described in the table underneath. Datasource Type. Click Create.

New Datasource

Database Type*

PostgreSQL ▾

Datasource Name*

customReports

Connection String*

jdbc:postgresql://localhost:5432/CustomReports

Username*

postgres

Password*

.....

Test Connection

✕ Cancel

Figure 90b: Create New Datasource

The following table provides a description of the fields for Datasource creation.

Table 59: Datasource fields

Field	Description
Name	Provide a name for the Datasource
Connection String	Provide a jdbc connection string to the database (e.g. jdbc:postgresql://localhost:5432/CustomReports, assuming you have database on same machine as AutomationEdge, else replace with ip address).
Username	Provide database username
Password	Provide password
Datasource Type	Select Datasource Type from the dropdown list.

4. Test Connection successful message is displayed.

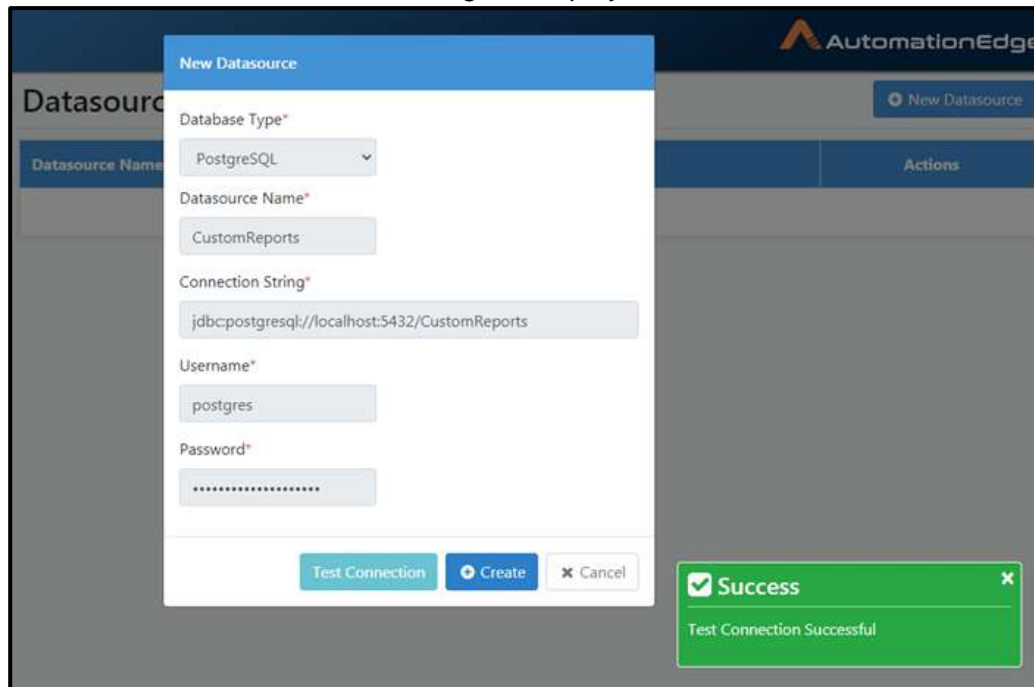


Figure 90c: Test Connection Successful

5. Dashboard created successfully message is displayed.

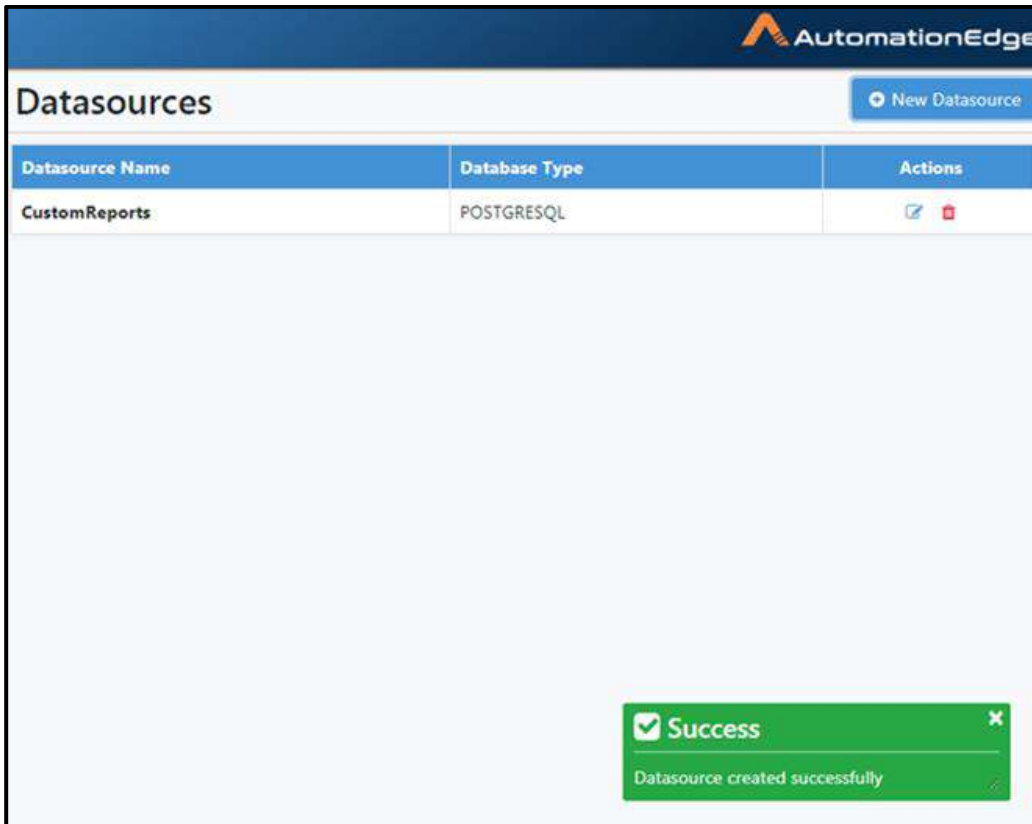


Figure 90c: Dashboard created successfully

11.5.2 Update Datasource

To update a new data source,

1. Click Reports menu and the Datasources sub-menu.
2. From the list of Datasources click edit in the Actions column for the Datasource to be updated.

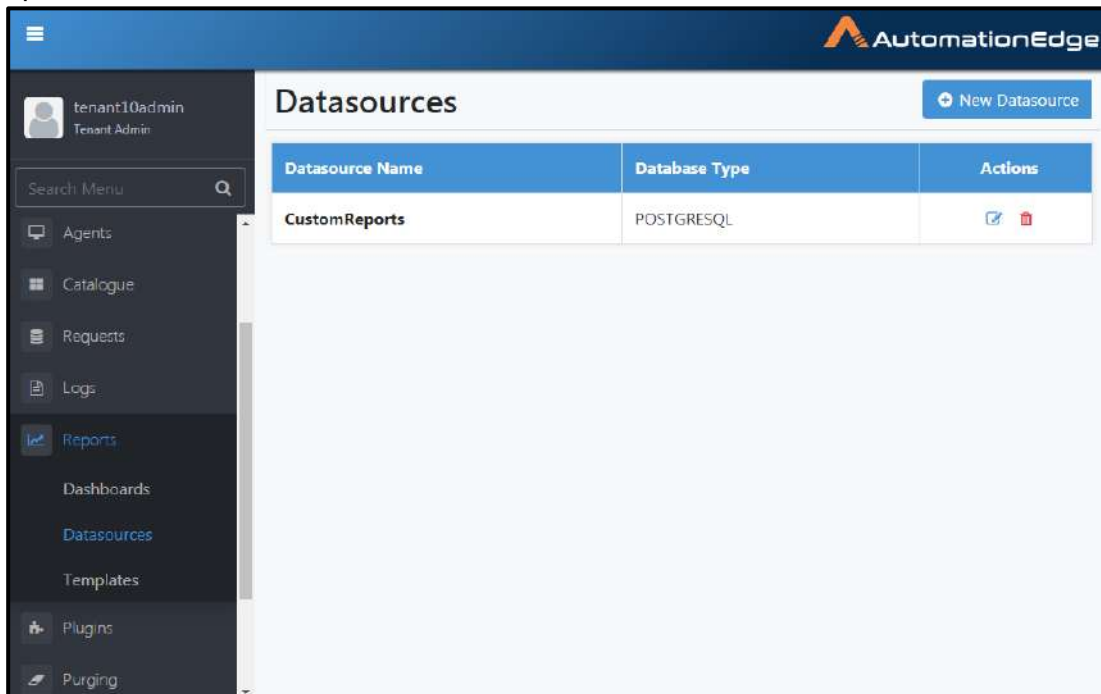
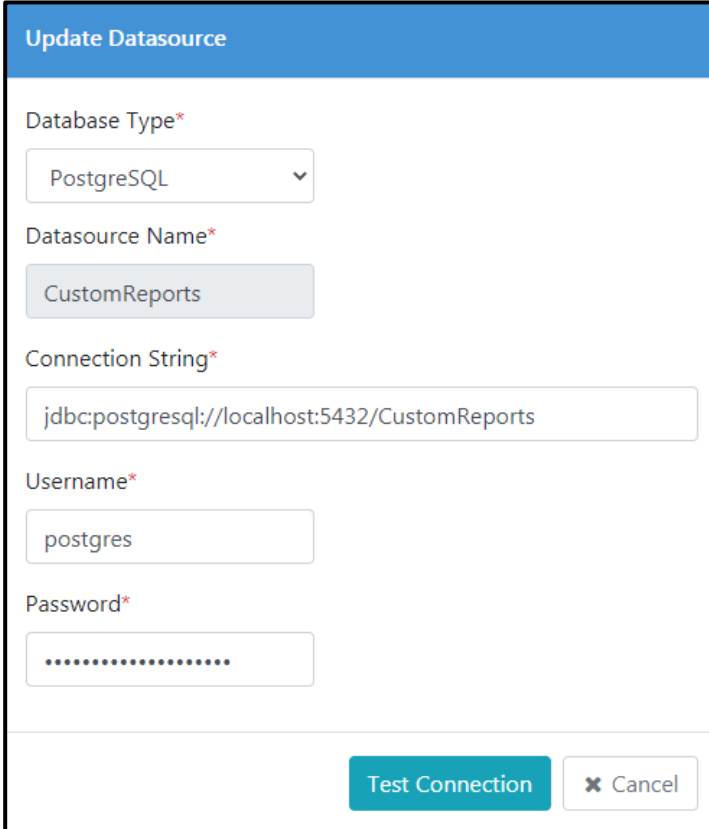


Figure 91a: Edit Datasource

- The Update Datasource window opens as shown below. The Datasource name cannot be modified. Make the required changes to any of the other attributes. Click Update. Click Test Connection.



Update Datasource

Database Type*
PostgreSQL

Datasource Name*
CustomReports

Connection String*
jdbc:postgresql://localhost:5432/CustomReports

Username*
postgres

Password*
.....

Test Connection ✕ Cancel

Figure 91b: Update Datasource

4. Test Connection Successful message appears. Click Update.

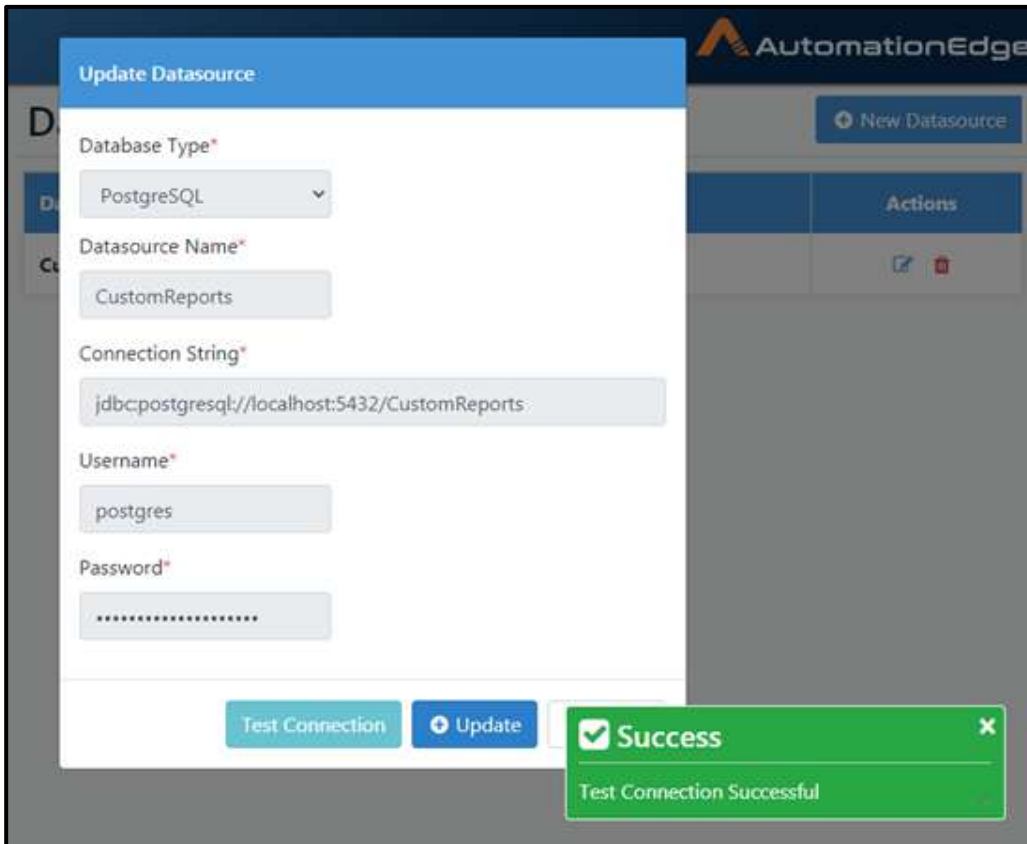
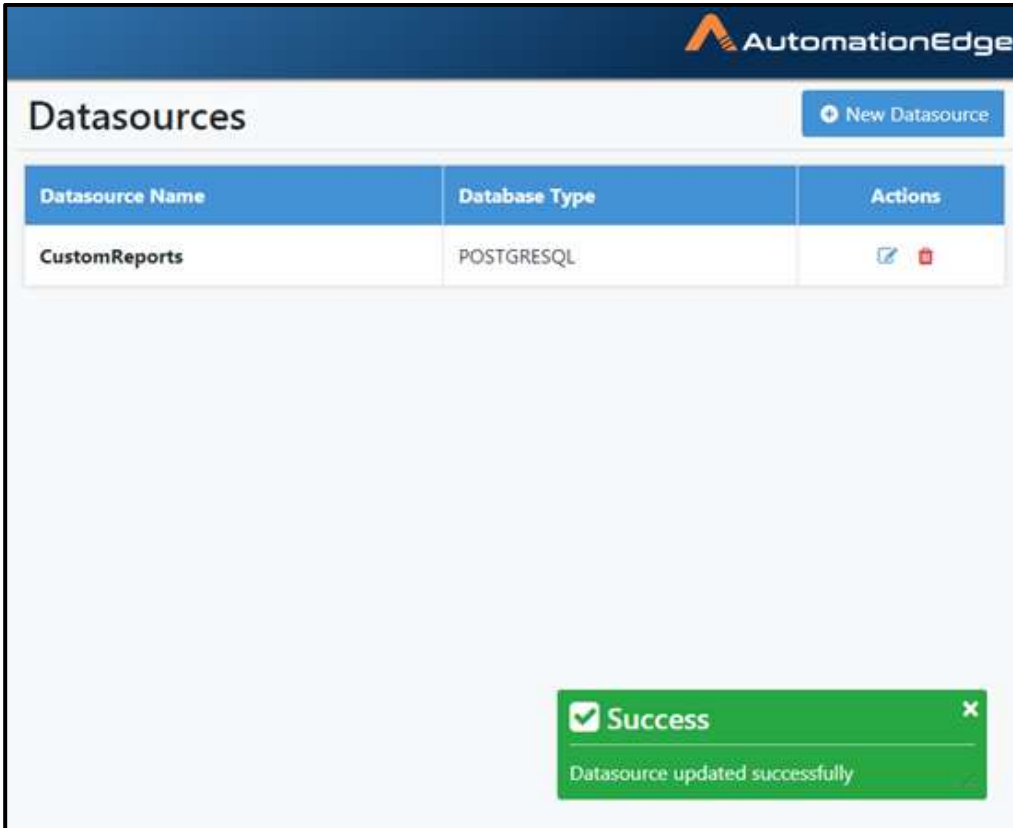




Figure 91c: Test Connection Successful

5. Datasource updated successfully message is displayed.



The screenshot displays the AutomationEdge interface for managing Datasources. At the top, the AutomationEdge logo is visible. Below it, the title "Datasources" is shown next to a "New Datasource" button. A table lists the existing Datasources:

Datasource Name	Database Type	Actions
CustomReports	POSTGRESQL	 

A green success message box is displayed at the bottom right of the interface, containing a checkmark icon, the word "Success", and the text "Datasource updated successfully".

Figure 91d: Datasource updated successfully.

11.6 Templates (for custom reports)

Templates are defined by specifying a database query, the desired attributes and the desired format for generating reports.

11.6.1 New Template

To create a new Template,

1. Click on Reports menu and Template sub-menu. Click New Template.

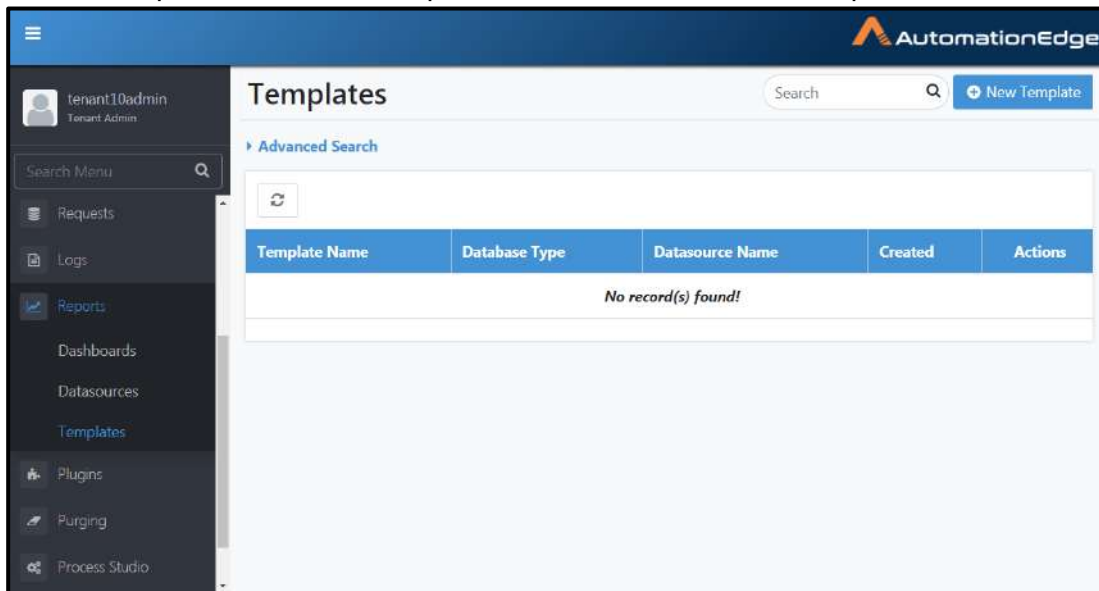
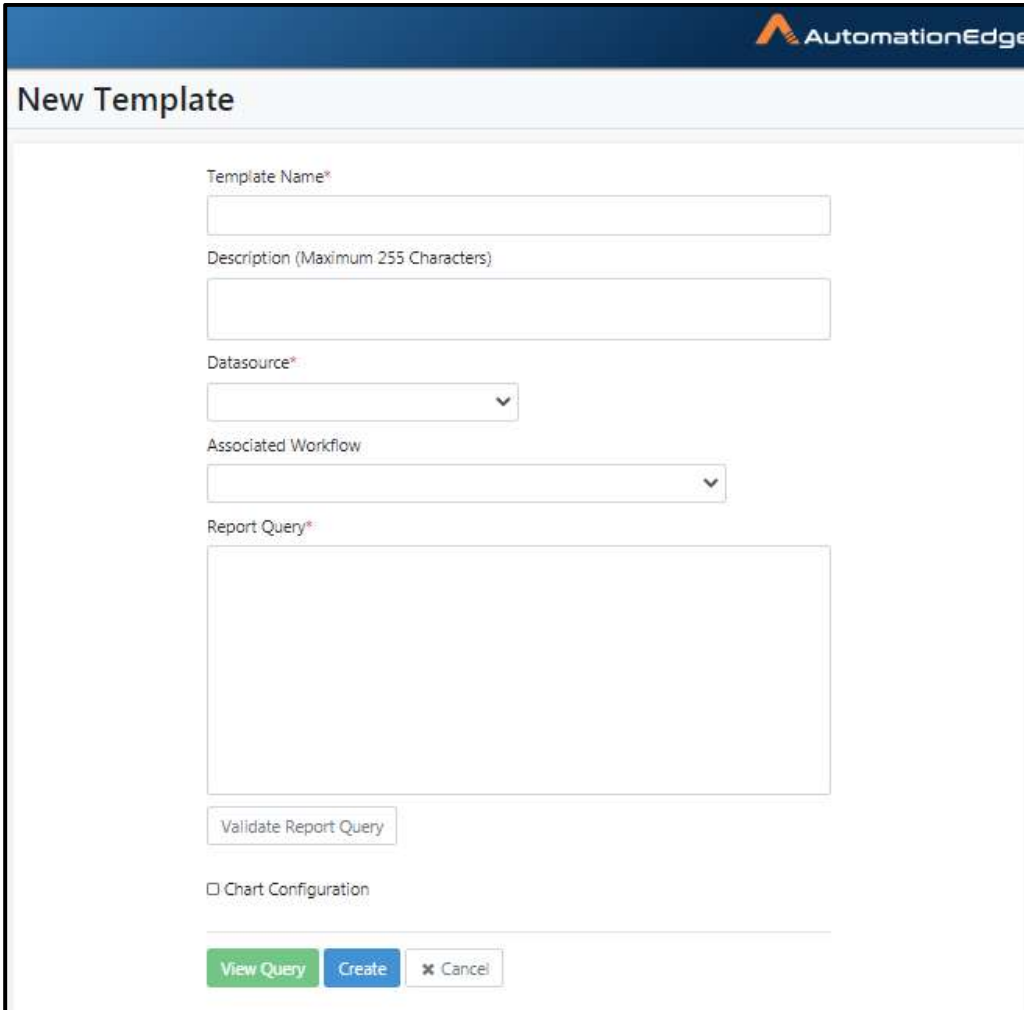


Figure 92a: Template Menu

2. New Template page opens as seen below.



The screenshot shows the 'New Template' page in the AutomationEdge interface. The page features a blue header with the AutomationEdge logo. The main content area is titled 'New Template' and contains the following elements:


- Template Name***: A text input field.
- Description (Maximum 255 Characters)**: A text input field.
- Datasource***: A dropdown menu.
- Associated Workflow**: A dropdown menu.
- Report Query***: A large text area for entering the report query.
- Validate Report Query**: A button located below the report query text area.
- Chart Configuration**: A checkbox.
- View Query**: A green button.
- Create**: A blue button.
- Cancel**: A grey button with an 'x' icon.

Figure 92a: New Template page

3. Fill in the details for the Template as shown below. Click Create.

New Template

Template Name*

Description
 

Datasource*

Associated Workflow

Report Query*

```
{
  "queryString": "SELECT wi.user_id, wf.name, COUNT(wi.id) FROM
vae_workflow_instance AS wi, vae_workflow_configuration AS wf WHERE wi.iscontainer
= false AND wi.tenant_id = :tenantId AND status IN ('Complete', 'Failure') AND wf.id =
wi.workflow_config_id GROUP BY wi.user_id, wf.name ORDER BY COUNT(wi.id) desc",
  "projections": [
    {
      "column": null,
      "label": "User Id",
      "type": null,

```

Chart Configuration

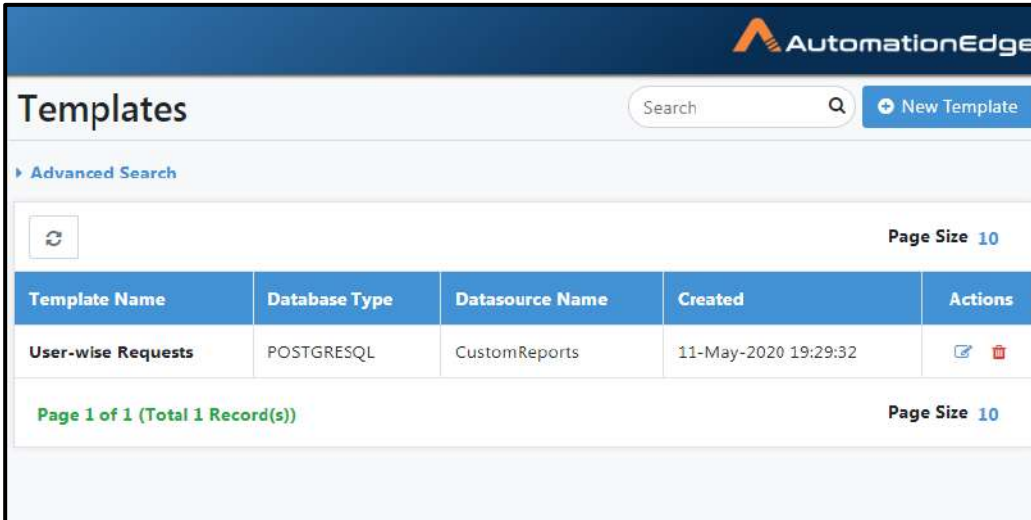
X-Axis Label*
 Non-numeric



Y-Axis Label*
 Non-numeric

Plot Against Label

Figure 92c: Create a custom report Template

4. A Template is created as seen below.



Template Name	Database Type	Datasource Name	Created	Actions
User-wise Requests	POSTGRESQL	CustomReports	11-May-2020 19:29:32	 

A description of the fields is provided in the table below.

Table 60: Template Creation

Field	Description
Template Name	Provide a Template name. This field is mandatory.
Description	Provide a Template description
Datasource	Select an existing Datasource from the list. This field is mandatory.
Associated Workflow	Select an associated workflow. If selected, only users with permission to the workflow will have access to the template. And this report will be specifically for data of that workflow.
Report Query*	Enter JSON text for report query.
Validate Report Query button	Click on this button to validate the JSON text for the report query.
Chart Configuration	Enable Check box to see the chart configuration fields – X-Axis Label, Y-Axis Label, Plot Against Label
X-Axis Label	X-axis label should match a label in projection
Y-Axis Label	Y-axis label should match a label in projection
Plot Against Label	Provide a label matching a label in projection to get a transposed display of value selected. Else leave it null to display a singular value.
Download Query button	Click on this button to download the report query.
Create button	Click to create the Template.
Cancel button	Click to Cancel creation.

* A detailed description of Report Query and Chart Configuration is provided below.

Table 61: Report Query

Report Query:		
<p>Provide a json script for the query. Report query can be a flat query or structured query. Users can give SQL string for a flat query or can give details about projection, selection etc. for a structured query.</p> <p>The main difference between flat query and structured query in terms of usability is flat query can be used when query is available. Structured query has additional features of summary and inner query.</p> <p>The various parts of the query are described below with a mention of need in flat or structured query. We shall demonstrate Custom Reports in the following sections.</p>		
1	queryString:	<p>(only for flat query) The user can give the SQL query as a string in this field. If this field is used, the query mentioned in the field will directly be run on the database. If user wants to filter data based on date, tenant and workflow ids or user ids; parameters for the same should be added in the query at appropriate places so that they are applied on the corresponding columns.</p> <p>E.g. SELECT col1, col2, col3 FROM table1 AS t1 INNER JOIN table2 AS t2 ON t1.fid=t2.id WHERE col1=xxx AND someDateCol <= :startDateParam AND someDateCol >= :endDateParam AND workfloodCol in (:wfldParam) AND ... GROUP BY xxx ...</p> <p>In this case words followed by ':' are place holders for parameters. These parameter names are to be mentioned as a field in the json (explained below).</p>
2	projections:	<p>(for both flat query and structured query) This field mentions all the projections/columns that are to be listed in the report. In case queryString is present (flat query), it should match all the columns/expressions that are selected. If queryString is absent, projections are used for generating SQL query. Projection is an array of the following elements:</p> <pre>{ "column": "columnExpression", "label": "Count", "type": "DURATION", "aggregateFunction": null }</pre> <p>column: should match to column expression that is to be used in query, null in case of flat query. label: Label for showing this field in the report type: Column type is optional. If not specified, the column type is taken from the data returned by the query. Available column types are STRING, NUMBER, DURATION, DATE and HYPERLINK.</p> <p>In case the column is showing duration (e.g. time taken for running workflow), the type should be set to DURATION. In case of duration, AEngine will assume that the data is specified in seconds, and will convert it to appropriate unit (minutes/hours) as per dashboard setting.</p>

		<p>aggregateFunction: AVG, COUNT, SUM etc. this function is applied over the column expression e.g. AVG(columnExpression).</p> <p>If the column type declared in report query is “HYPERLINK”, URL will be added in report with the text ‘Click Here’. On click the URL will navigate to the URL specified in the database column (for e.g. https://ondemand.automationedge.com) in a new browser tab. The HYPERLINK type column will appear with a “Click Here” link on the report.</p> <p>However, to get a custom link text, the value in the database column must be in the following json format with values for target and linkText. (for e.g. <code>{"target":"https://ondemand.automationedge.com","linkText":"Click to open AutomationEdge Cloud"}</code>) In this case the custom link displayed will be Click to open AutomationEdge Cloud</p>
3	fromClause:	(only for structured query) Specifies from clause of the resultant query.
4	whereClause	(only for structured query) Specifies where clause of the resultant query. The where clause should have place holder for parameters (for date, tenant id, workflow id and user id) if applicable.
5	groupBy:	(only for structured query) List of columns that will be in ‘group by’ clause of the query. (e.g. [“col1”, “col2”])
6	orderBy:	(only for structured query) list of ‘order by’ expressions in the query (e.g. [“col1 asc”, “col2 desc”])
7	needSummary:	(only for structured query) A boolean value specifying if summary row should be present for the report or not.
8	innerQueryColumnNames:	(only for structured query) If report needs to have a feature where clicking on a row drills down further, user has to populate this field with name of the column that should be used for further grouping. This name must be present in projections.
9	tenantIdParamNames:	(for both flat query and structured query) It specifies a list of parameter names for tenant ids (e.g. [“param1”, “param2”]). AE engine identifies these parameters in the query. These parameters should be present in the query as ‘:param1’ and ‘:param2’. It substitutes these query parameters by run time values of the tenant id of the user running the report. This parameter value in query table should be numeric.
10	workflowIdParamNames:	(only for flat query) It specifies a list of parameter names for workflow ids. AE engine identifies these parameters in the query. It substitutes these query parameters by run time values. This parameter value in query table should be numeric.
11	startDateParamNames:	(only for flat query) It specifies a list of parameter names for start date. AE engine identifies these parameters in the query. AE engine substitutes these query parameters by start date-time stamp of the report. This parameter value in query table should be of type date.

12	endDateParamNames:	(only for flat query) It specifies a list of parameter names for end date. AE engine identifies these parameters in the query. AE engine substitutes these query parameters by end date-time stamp of the report. This parameter value in query table should be of type date.
13	workflowIdColumnName:	(for structured query only) This parameter can be present only if workflowParamNames is not present. This parameter has the name of the workflow id column on which workflow id filter is added by the engine.
14	dateColumnName:	(only for structured query) This parameter can be present only if startDateParameterNames and endDateParamNames are not present. This parameter has the name of the column on which date filter is added by the engine. This parameter value in query table should be of type date.
15	userIdParamNames:	(for both flat query and structured query) It specifies a list of parameter names for user ids (e.g. ["param1", "param2"]). AE engine identifies these parameters in the query. These parameters should be present in the query as ':param1' and ':param2'. It substitutes these query parameters by run time values of the user id running the report. If a custom report with userIdParamNames option is executed by tenant users, the user can see rows which contain his user id. However, if a custom report with userIdParamNames option is executed by Tenant Administrators, the user can see all rows for first (i.e. oldest created) 1000 users. This parameter value in query table should be numeric.

Table 62: Chart Configuration

Chart Configuration: Provide the following values for the report format.		
1	X-Axis	X-axis label should match a label in projection
2	Y-Axis	Y-axis label should match a label in projection
3	Plot Against Label	Provide a label matching a label in projection to get a transposed display of all the types of the value selected. Else leave it null to display a singular value.

5. Once Template is created it is visible as Report Type in Add Report.

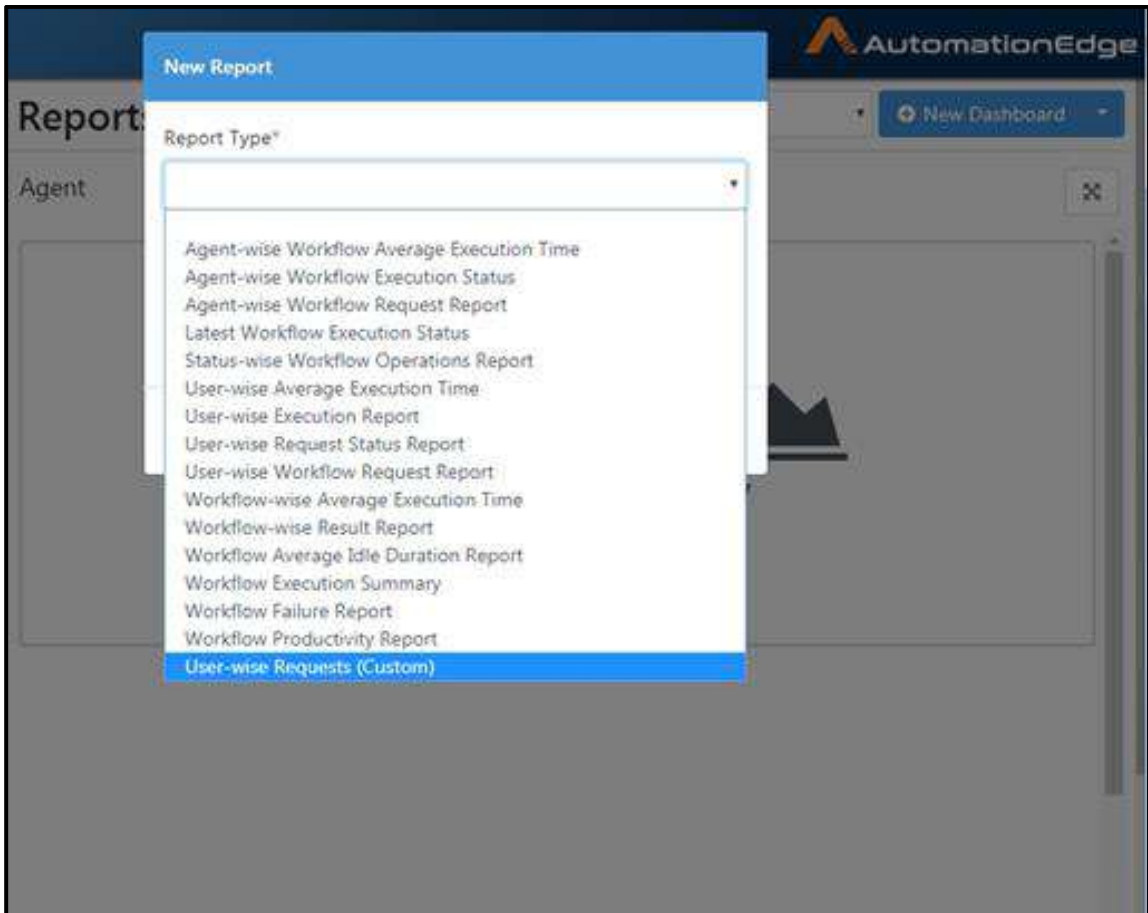


Figure 92d: Template visibility in Add New Report

11.6.2 Sample JSON for Flat Query

11.6.2.1 Sample JSON for Flat Query and Chart view

The following table shows the query script, Chart Options configuration and the custom report.

Table 63: Flat Query for Workflow Request Count by user id

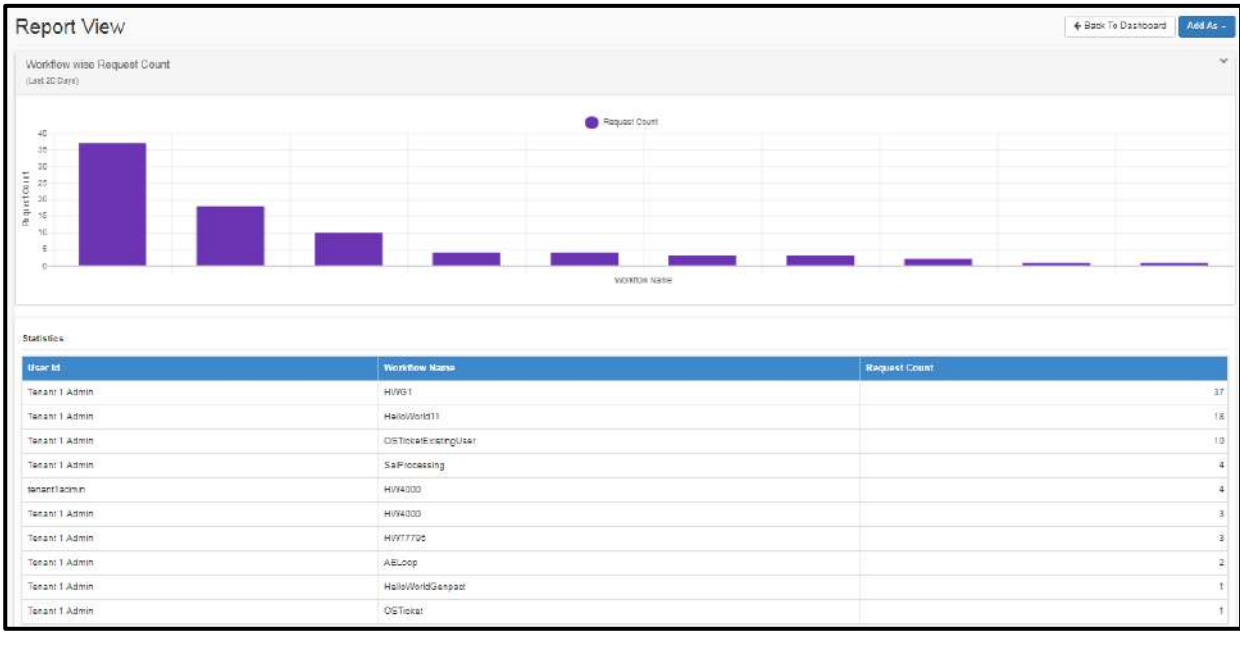
Sample JSON for Flat Query for: "Workflow Request Count by userid"
<pre>{ "queryString": "SELECT wi.user_id, wf.name, COUNT(wi.id) FROM vae_workflow_instance AS wi, vae_workflow_configuration AS wf WHERE wi.tenant_id = :tenantId AND status IN ('Complete', 'Failure') AND wf.id = wi.workflow_config_id GROUP BY wi.user_id, wf.name ORDER BY COUNT(wi.id) desc", "projections": [{ "column": "wi.user_id", "label": "User Id", "type": null, "aggregateFunction": null }, { "column": "wf.name",</pre>

```

        "label": "Workflow Name",
        "type": null,
        "aggregateFunction": null
    },
    {
        "column": "wi.id",
        "label": "Request Count",
        "type": null,
        "aggregateFunction": null
    }
},
"fromClause": null,
"whereClause": null,
"groupBy": [],
"orderBy": [],
"needSummary": false,
"innerQueryColumnName": null,
"dateColumnName": null,
"workflowIdColumnName": null,
"workflowIdParamNames": null,
"startDateParamNames": null,
"endDateParamNames": null,
"tenantIdParamNames": ["tenantId"],
"userIdParamNames": null
}
    
```

Sample Chart Configuration with Flat Query:

X-Axis Label	Workflow Name	<input type="checkbox"/> Non-numeric. Do not enable Non-numeric checkbox to specify that User ID is numeric.
Y-Axis Label	Request Count	<input type="checkbox"/> Non-numeric. Do not enable Non-numeric checkbox to specify that Request Count is numeric.
Plot Against Label	null	Leave it null to display a singular value.



11.6.2.2 Alter Flat Query with filter on Workflow ID

We will now create a New Template as a replica of the one in section above. However, we will additionally put a filter on workflow ID and date.

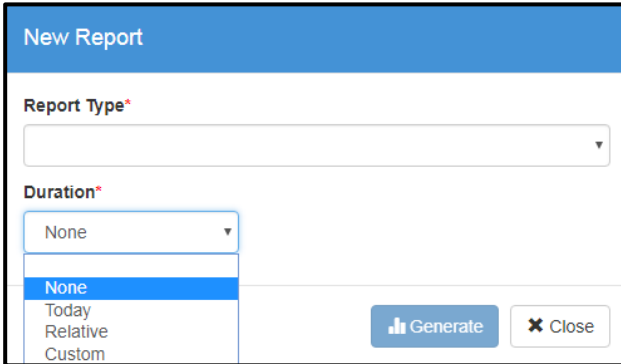
1. Create a new Template exactly as in section above.
2. In the configuration page Template additionally choose a value in the Associated Workflow.



The image shows a dropdown menu titled "Associated Workflow". The selected option is "HW1".

Figure93a: Choose Associated Workflow for dataset

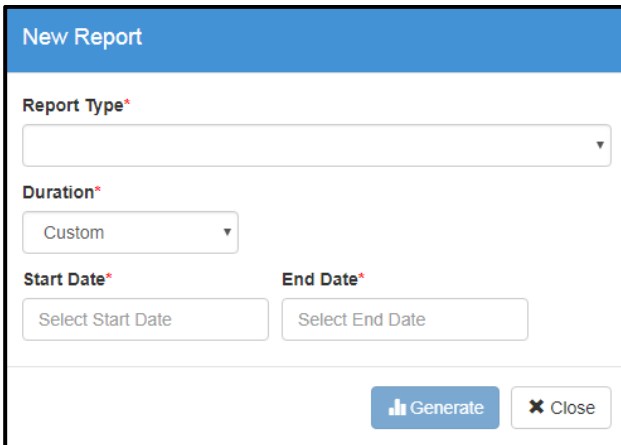
3. Select a custom duration. Available options are shown in the image below.



The image shows the "New Report" configuration page. The "Report Type" dropdown is empty. The "Duration" dropdown is open, showing options: None, Today, Relative, and Custom. The "Generate" button is highlighted.

Figure93b: Options for Duration

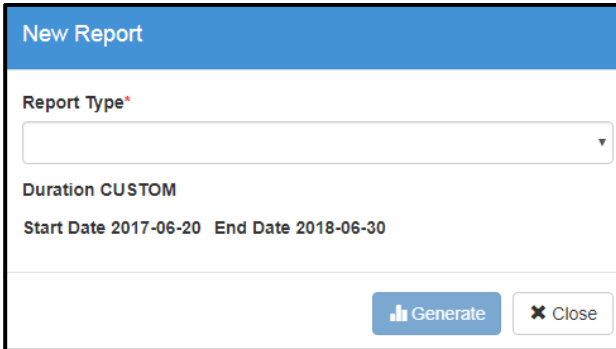
4. Select Custom as the Duration.



The image shows the "New Report" configuration page. The "Report Type" dropdown is empty. The "Duration" dropdown is set to "Custom". Below it, there are two date selection fields: "Start Date" and "End Date", both with "Select" buttons. The "Generate" button is highlighted.

Figure93c: Choose Start and End Date for Custom Duration

- Choose Dates as shown below.



New Report

Report Type*

Duration CUSTOM

Start Date 2017-06-20 End Date 2018-06-30

Generate Close

Figure93d: Start and End Date Chosen

- The following table shows the modified query script, Chart Options configuration and the custom report.

Table 64: Flat Query for Workflow Request Count by user id with filter on workflow id

Sample JSON for Flat Query with filter on workflow id for: "Workflow Request Count by userid"
<pre>{ "queryString": "SELECT wi.user_id, wf.name, COUNT(wi.id) FROM vae_workflow_instance AS wi, vae_workflow_configuration AS wf WHERE wi.tenant_id = 2 AND status IN ('Complete', 'Failure') AND wf.id = wi.workflow_config_id AND wf.id IN (:wfid) GROUP BY wi.user_id, wf.name ORDER BY COUNT(wi.id) desc", "projections": [{ "column": "wi.user_id", "label": "User Id", "type": null, "aggregateFunction": null }, { "column": "wf.name", "label": "Workflow Name", "type": null, "aggregateFunction": null }, { "column": "wi.id", "label": "Request Count", "type": null, "aggregateFunction": null }], "fromClause": null, "whereClause": null, "groupBy": [], "orderBy": [], "needSummary": false, "innerQueryColumnName": null, "dateColumnName": null, "workflowIdColumnName": null, "workflowIdParamNames": ["wfid"],</pre>

```

"startDateParamNames": null,
"endDateParamNames": null,
"tenantIdParamNames": null
}
    
```

Sample Chart Configuration with Flat Query:

X-Axis Label	Workflow Name	<input type="checkbox"/> Non-numeric. Do not enable Non-numeric checkbox to specify that User ID is numeric.
Y-Axis Label	Request Count	<input type="checkbox"/> Non-numeric. Do not enable Non-numeric checkbox to specify that Request Count is numeric.
Plot Against Label	null	Leave it null to display a singular value.

Report View ← Back To Dashboard [Add As](#)

Workflow wise Request Count
(Last 20 Days)

Statistics

User Id	Workflow Name	Request Count
Tenant1 Admin	H/W/1	37
Tenant1 Admin	HelloWorld11	18
Tenant1 Admin	OSTicketCreatingUser	10
Tenant1 Admin	SaPProcessing	4
tenant1admin	H/W/200	4
Tenant1 Admin	H/W/200	3
Tenant1 Admin	H/W/7770	3
Tenant1 Admin	ABLoop	2
Tenant1 Admin	HelloWorldGenpass	1
Tenant1 Admin	OSTicket	1

11.6.2.3 Alter flat query with filter on Workflow ID and Created Date.

The following table shows the modified query script, Chart Options configuration and the custom report.

1. The following table shows the modified query script, Chart Options configuration and the custom report.

Table 65: Flat Query for Workflow Request Count by user id with filter on workflow id & date

Sample JSON for Flat Query with filter on workflow id and created date for: "Workflow Request Count by userid"

```

{
  "queryString": "SELECT wi.user_id, wf.name, COUNT(wi.id) FROM vae_workflow_instance AS wi, vae_workflow_configuration AS wf WHERE wi.tenant_id = 2 AND status IN('Complete', 'Failure') AND wf.id = wi.workflow_config_id AND wf.id in (:wfid) and wi.created_date >= (:startDate) and wi.created_date <= (:endDate) GROUP BY wi.user_id, wf.name ORDER BY COUNT(wi.id) desc ",
  "projections": [
    ]
}
    
```

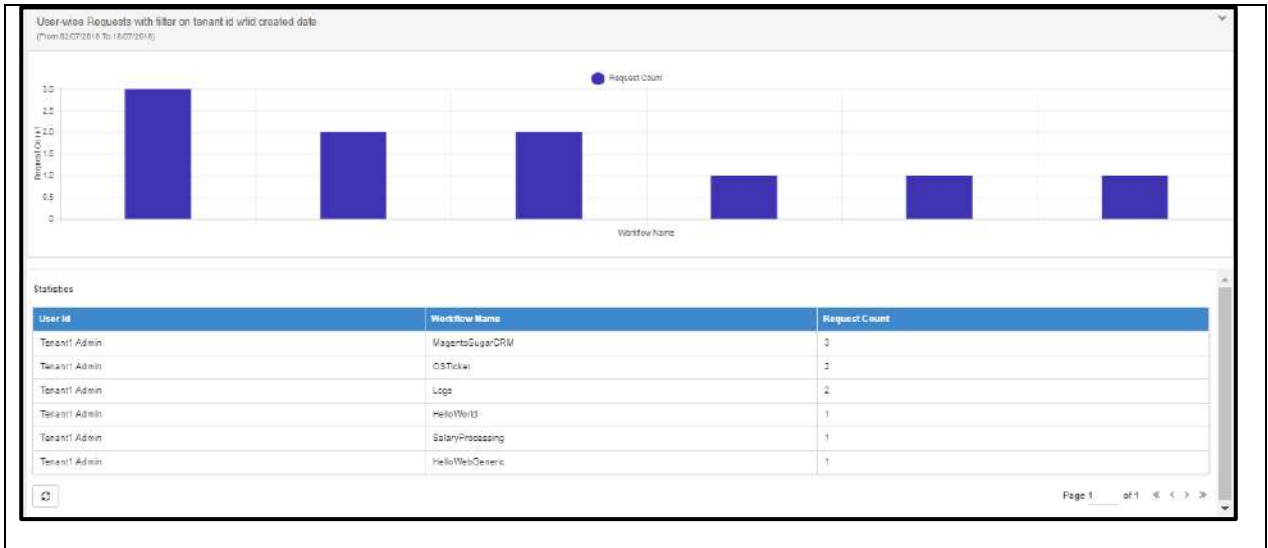
```

    {
      "column": "wi.user_id",
      "label": "User Id",
      "type": null,
      "aggregateFunction": null,
      "colorCodes": null,
      "width": 0,
      "iconOnly": false,
      "h_alignment": null,
      "v_alignment": null
    },
    {
      "column": "wf.name",
      "label": "Workflow Name",
      "type": null,
      "aggregateFunction": null,
      "colorCodes": null,
      "width": 0,
      "iconOnly": false,
      "h_alignment": null,
      "v_alignment": null
    },
    {
      "column": "wi.id",
      "label": "Request Count",
      "type": null,
      "aggregateFunction": null,
      "colorCodes": null,
      "width": 0,
      "iconOnly": false,
      "h_alignment": null,
      "v_alignment": null
    }
  ],
  "fromClause": null,
  "whereClause": null,
  "groupBy": [],
  "orderBy": [],
  "needSummary": false,
  "innerQueryColumnName": null,
  "dateColumnName": null,
  "workflowIdColumnName": null,
  "workflowIdParamNames": ["wfid"],
  "startDateParamNames": ["startDate"],
  "endDateParamNames": ["endDate"],
  "tenantIdParamNames": null
}

```

Sample Chart Configuration with Flat Query:

X-Axis Label	Workflow Name	<input type="checkbox"/> Non-numeric. Do not enable Non-numeric checkbox to specify that User ID is numeric.
Y-Axis Label	Request Count	<input type="checkbox"/> Non-numeric. Do not enable Non-numeric checkbox to specify that Request Count is numeric.
Plot Against Label	null	Leave it null to display a singular value.



11.6.2.4 Flat query with a column of type: HYPERLINK.

The following table shows a flat query JSON, and the custom tabular report.

Table 66: Flat Query for 'Automation Efficiency Report'

wfid bigint	tenantid character(1)	rftaskid text	rfstatus text	aestatus text	aelink text
2	4	10	TOAE	COMPLETE	https://ondemand.automationedge.com
2	4	11	Invalid		https://ondemand.automationedge.com
5	4	12	TOAE	COMPLETE	{target:"https://ondemand.automationedge.com","linkText":"Click to open AutomationEdge Cloud"}
5	4	13	Invalid		{target:"https://ondemand.automationedge.com","linkText":"Click to open AutomationEdge Cloud"}
5	4	14	TOAE	COMPLETE	{target:"https://ondemand.automationedge.com","linkText":"Click to open AutomationEdge Cloud"}
5	4	15	TOAE	FAILURE	{target:"https://ondemand.automationedge.com","linkText":"Click to open AutomationEdge Cloud"}
8	1		TOAE	COMPLETE	https://ondemand.automationedge.com
9	4	16	TOAE	FAILURE	https://ondemand.automationedge.com
10	4	17	TOAE	COMPLETE	https://ondemand.automationedge.com
10	1	18	TOAE	DIVERTED	https://ondemand.automationedge.com
10	1	19	Invalid		https://ondemand.automationedge.com

This flat query is based on custom business data.
(A snapshot of the business data is shown below.)

Sample JSON for Flat Query with a column of type HEPERLINK
"Automation Efficiency Report"
to check AE (AutomationEdge) status against RF(RemedyForce) status

```
{
  "queryString": "SELECT wfid, rfstatus, aestatus, aelink FROM custnew WHERE
tenantid = '4' ORDER BY rfstatus desc, aestatus desc",
  "projections": [
    {
      "column": null,
      "label": "WF Id",
      "type": null,
      "aggregateFunction": null,
      "colorCodes": null,
      "width": 0,
      "iconOnly": false,
    }
  ]
}
```



```

        "h_alignment": null,
        "v_alignment": null
    },
    {
        "column": null,
        "label": "RF Status",
        "type": null,
        "aggregateFunction": null,
        "colorCodes": null,
        "width": 0,
        "iconOnly": false,
        "h_alignment": null,
        "v_alignment": null
    },
    {
        "column": null,
        "label": "AE Status",
        "type": null,
        "aggregateFunction": null,
        "colorCodes": null,
        "width": 0,
        "iconOnly": false,
        "h_alignment": null,
        "v_alignment": null
    },
    {
        "column": null,
        "label": "AE Link",
        "type": "HYPERLINK",
        "aggregateFunction": null,
        "colorCodes": null,
        "width": 0,
        "iconOnly": false,
        "h_alignment": null,
        "v_alignment": null
    }
},
"fromClause": null,
"whereClause": null,
"groupBy": [],
"orderBy": [],
"needSummary": false,
"innerQueryColumnName": null,
"dateColumnName": null,
"workflowIdColumnName": null,
"workflowIdParamNames": null,
"startDateParamNames": null,
"endDateParamNames": null,
"tenantIdParamNames": null,
"userIdParamNames": null
}

```

Sample Tabular Report: with hyperlink default ([Click Here](#)) and specific link ([Click to open AutomationEdge Cloud](#)) text.

Report with Hyperlink
From inception

WF Id	RF Status	AE Status	AE Link
5	TOAE	FAILURE	Click to open AutomationEdge Cloud
9	TOAE	FAILURE	Click Here
2	TOAE	COMPLETE	Click Here
5	TOAE	COMPLETE	Click to open AutomationEdge Cloud
10	TOAE	COMPLETE	Click Here
5	TOAE	COMPLETE	Click to open AutomationEdge Cloud

Page 1 of 1 << >>

AutomationEdge Efficiency - with Hyperlink
(From inception)

WF Id	RF Status	AE Status	AE Link
5	TOAE	FAILURE	Click to open AutomationEdge Cloud
9	TOAE	FAILURE	Click Here
2	TOAE	COMPLETE	Click Here
5	TOAE	COMPLETE	Click to open AutomationEdge Cloud
10	TOAE	COMPLETE	Click Here
5	TOAE	COMPLETE	Click to open AutomationEdge Cloud
2	Invalid		Click Here
5	Invalid		Click to open AutomationEdge Cloud

Page 1 of 1 << >>

11.6.3 Sample JSON for Structured Query

11.6.3.1 Sample JSON for Structured Query and Chart view

The following table shows a sample JSON for a structured query and chart view.

Table 67: Structured Query for Workflow Request Count by user id and status.

Sample JSON for a Structured Query for:
“Workflow Request count by User ID and Status”

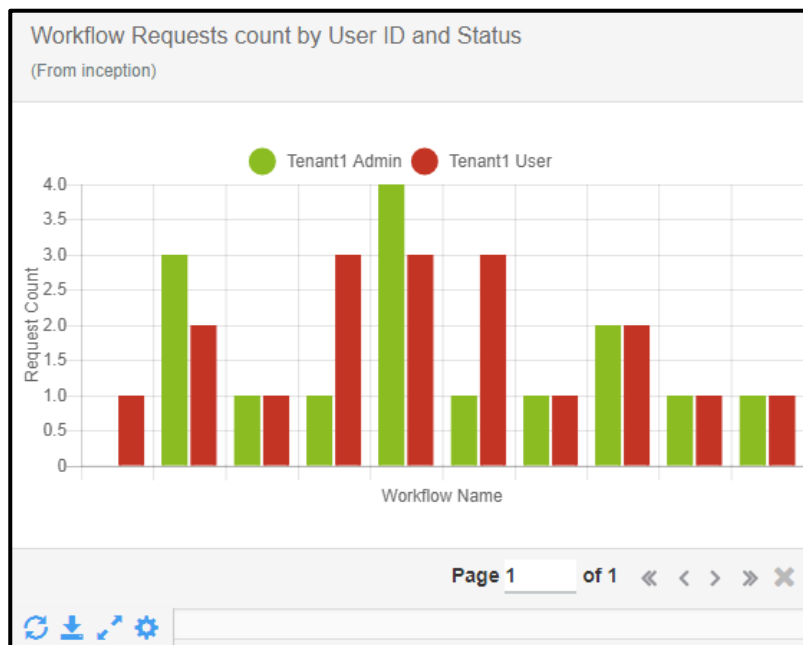
```

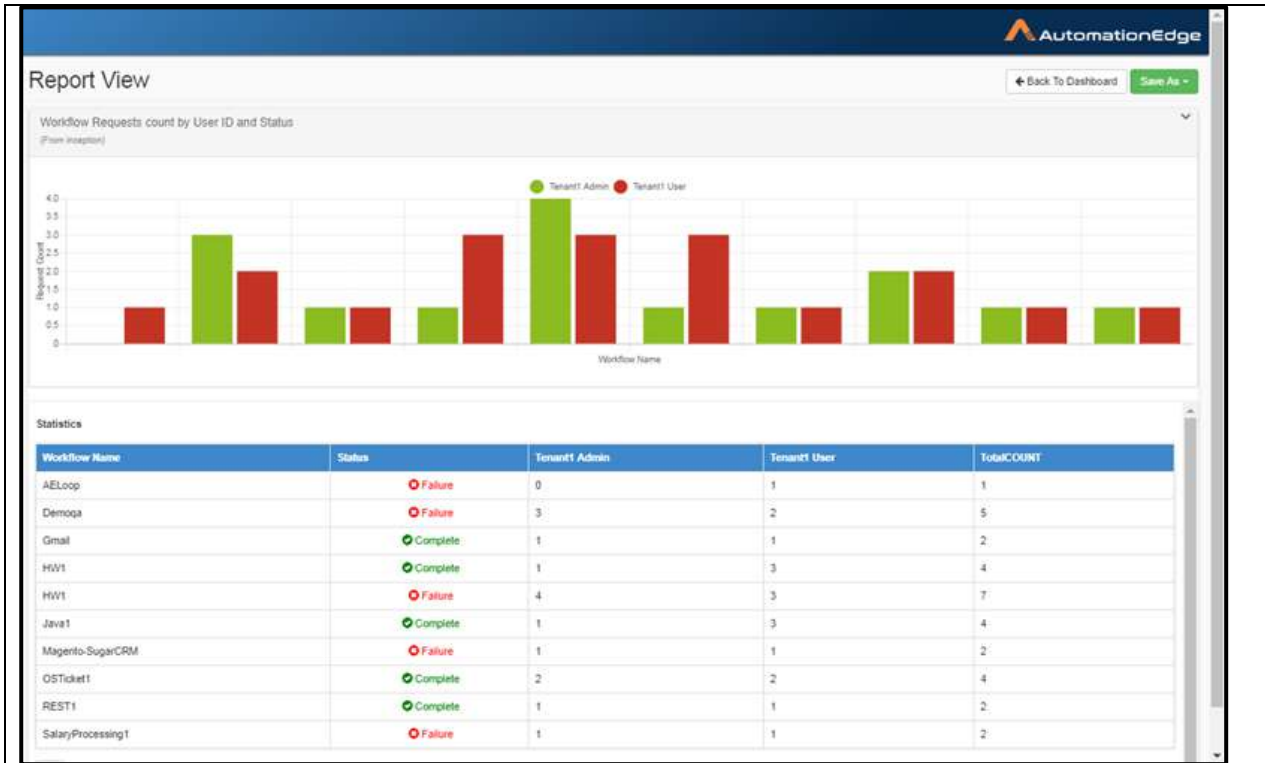
{
  "queryString": null,
  "projections": [
    {
      "column": "wi.user_id",
      "label": "User Id",
      "type": null,
      "aggregateFunction": null
    },
    {
      "column": "wf.name",
      "label": "Workflow Name",
      "type": null,
      "aggregateFunction": null
    },
    {
      "column": "wi.status",
      "label": "Status",
      "type": null,
      "aggregateFunction": null
    },
    {
      "column": "wi.id",
      "label": "Request Count",
      "type": null,
      "aggregateFunction": "COUNT"
    }
  ],
  "fromClause": "vae_workflow_instance AS wi, vae_workflow_configuration AS wf",
  "whereClause": "wi.tenant_id = :tenantId AND status IN ('Complete', 'Failure') AND
wf.id = wi.workflow_config_id",
  "groupBy": [
    "wi.user_id",
    "wf.name",
    "wi.status"
  ],
  "orderBy": [
    "wi.user_id",
    "wf.name",
    "wi.status"
  ],
  "needSummary": false,
  "innerQueryColumnName": null,
  "dateColumnName": null,
  "workflowIdColumnName": null,
  "workflowIdParamNames": null,
  "startDateParamNames": null,
  "endDateParamNames": null,
  "tenantIdParamNames": [
    "tenantId"
  ]
}

```

Sample Chart Configuration with Structured Query:

X-Axis Label	Workflow Name	<input type="checkbox"/> Non-numeric. Enable checkbox to specify that Workflow Name is Non-numeric.
Y-Axis Label	Request Count	<input type="checkbox"/> Non-numeric. Do not enable checkbox to specify that Request Count is Non-Numeric.
Plot Against Label	User Id	Get a transposed display of User Id.





11.6.3.2 Alter Structured Query with filter on Workflow ID and Created Date.

Table 68: Structured Query for Workflow Request Count by user id and status with filters.

Sample JSON for a Structured Query for: "Workflow Request count by User ID & Status" with filter on Workflow ID & Created Date
<pre>{ "queryString": null, "projections": [{ "column": "wi.user_id", "label": "User Id", "type": null, "aggregateFunction": null, "colorCodes": null, "width": 0, "iconOnly": false, "h_alignment": null, "v_alignment": null }, { "column": "wf.name", "label": "Workflow Name", "type": null, "aggregateFunction": null, "colorCodes": null, "width": 0, "iconOnly": false, "h_alignment": null, "v_alignment": null }, { "column": "wi.status", "label": "Status", "type": null, "aggregateFunction": null, "colorCodes": null, "width": 0, "iconOnly": false, "h_alignment": null, "v_alignment": null }, { "column": "wi.id", "label": "Request Count", "type": null, "aggregateFunction": "COUNT", "colorCodes": null, "width": 0, "iconOnly": false, </pre>

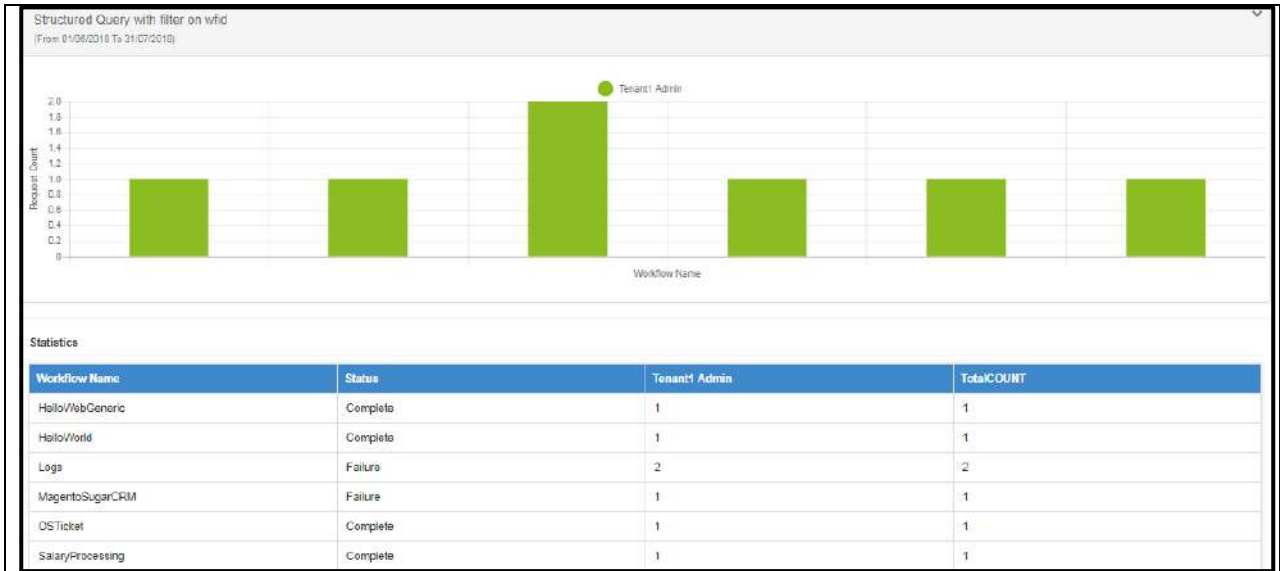
```

        "h_alignment": null,
        "v_alignment": null
    }
  ],
  "fromClause": "vae_workflow_instance AS wi, vae_workflow_configuration AS wf",
  "whereClause": "wi.tenant_id = :tenantId AND status IN ('Complete', 'Failure') AND wf.id
= wi.workflow_config_id",
  "groupBy": [
    "wi.user_id",
    "wf.name",
    "wi.status"
  ],
  "orderBy": [
    "wi.user_id",
    "wf.name",
    "wi.status"
  ],
  "needSummary": false,
  "innerQueryColumnName": null,
  "dateColumnName": "wi.created_date",
  "workflowIdColumnName": "wi.id",
  "workflowIdParamNames": null,
  "startDateParamNames": null,
  "endDateParamNames": null,
  "tenantIdParamNames": [
    "tenantId"
  ]
}

```

Sample Chart Configuration with Structured Query:

X-Axis Label	Workflow Name	<input type="checkbox"/> Non-numeric. Enable checkbox to specify that Workflow Name is Non-numeric.
Y-Axis Label	Request Count	<input type="checkbox"/> Non-numeric. Do not enable checkbox to specify that Request Count is Non-Numeric.
Plot Against Label	User Id	Get a transposed display of User Id.



11.6.3.3 Alter Structured Query with inner query

Table 69: Structured Query for Workflow Request Count by userid & status with inner query on status.

**Sample JSON for a above Structured Query altered for inner query on status:
"Workflow Request count with inner query on Status"**

Note: The changes compared to json query above are marked in yellow below.

```
{
  "queryString": null,
  "projections": [
    {
      "column": "wi.user_id",
      "label": "User Id",
      "type": null,
      "aggregateFunction": null
    },
    {
      "column": "wf.name",
      "label": "Workflow Name",
      "type": null,
      "aggregateFunction": null
    },
    {
      "column": "wi.status",
      "label": "Status",
      "type": null,
      "aggregateFunction": null
    }
  ]
}
```



```
        {
            "column": "wi.id",
            "label": "Request Count",
            "type": null,
            "aggregateFunction": "COUNT"
        }
    ],
    "fromClause": "vae_workflow_instance AS wi, vae_workflow_configuration AS wf",
    "whereClause": "wi.tenant_id = :tenantId AND status IN ('Complete', 'Failure') AND
wf.id=wi.workflow_config_id",
    "groupBy": ["wf.name"],

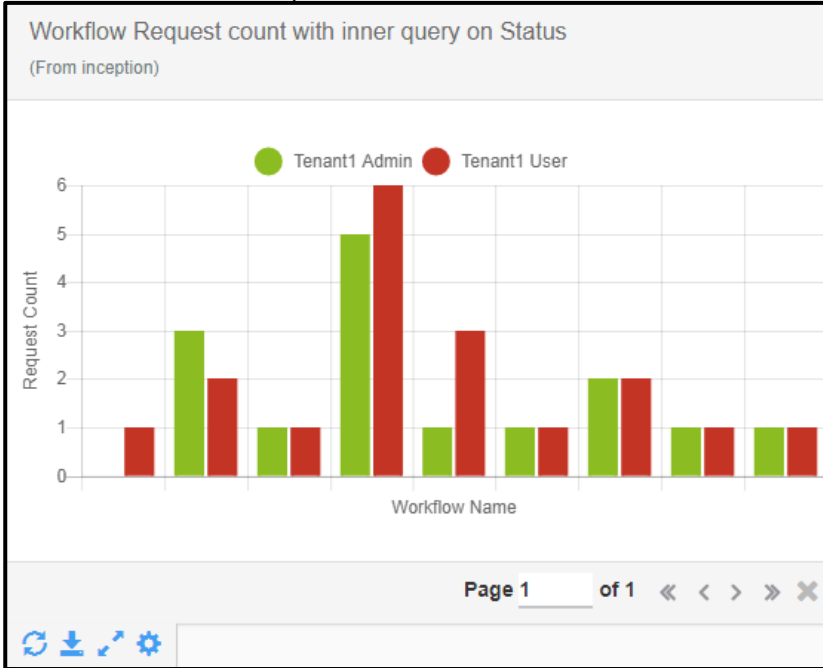
    "orderBy": ["wf.name"],

    "needSummary": true,
    "innerQueryColumnName": "wi.status",
    "dateColumnName": null,
    "workflowIdColumnName": null,
    "workflowIdParamNames": null,
    "startDateParamNames": null,
    "endDateParamNames": null,
    "tenantIdParamNames": ["tenantId"],
    "userIdParamNames": null
}
```

Sample Chart Configuration with Structured Query:

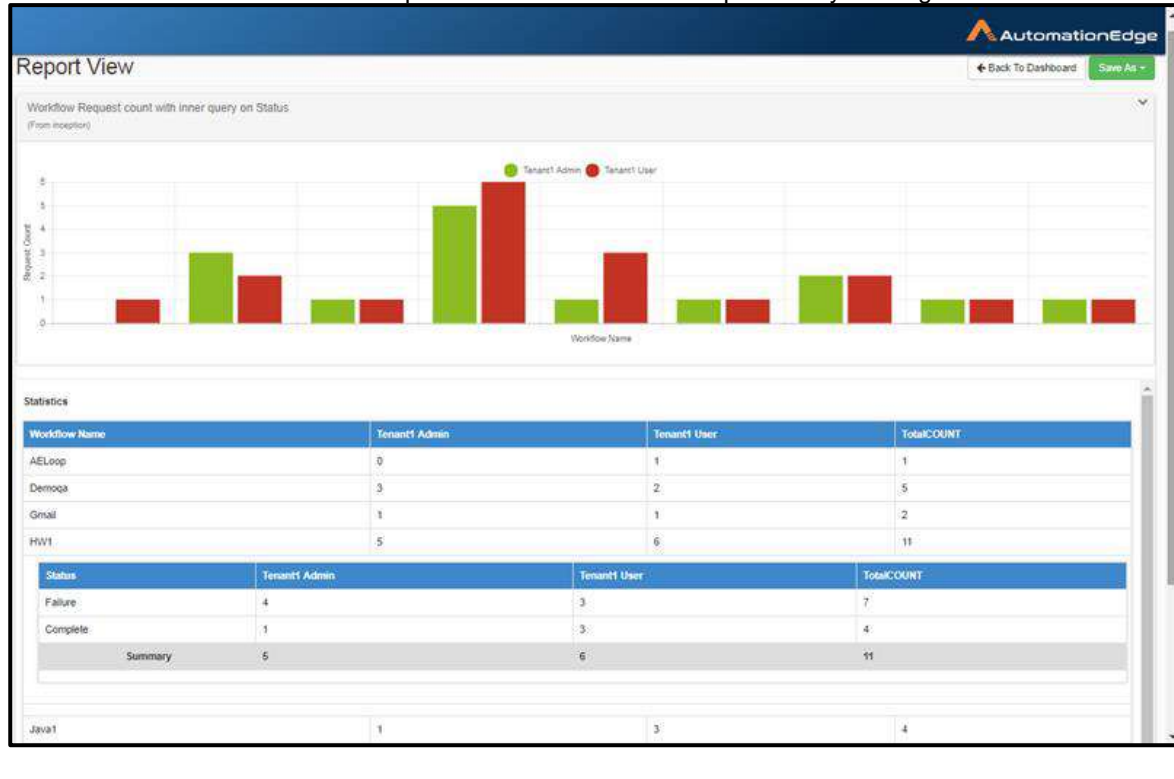
X-Axis Label	Workflow Name	<input type="checkbox"/> Non-numeric. Enable checkbox to specify that Workflow Name is Non-numeric.
Y-Axis Label	Request Count	<input type="checkbox"/> Non-numeric. Do not enable checkbox to specify that Request Count is Non-Numeric.
Plot Against Label	User Id	Get a transposed display of count of wf.id.

The chart below shows report on dashboard:



The chart and table below show Report View:

The chart and table below show Report View and some rows expanded by clicking on the row:



Following is report as downloaded as pdf:

Workflow Request count with inner query on Status			
From Inception To 13-06-2018 15:44:35 IST			
Workflow Name	Tenant1 Admin	Tenant1 User	TotalCOUNT
AELoop	0	1	1
Failure	0	1	1
Demoqa	3	2	5
Failure	3	2	5
Gmail	1	1	2
Complete	1	1	2
HW1	5	6	11
Failure	4	3	7
Complete	1	3	4
Java1	1	3	4
Complete	1	3	4
Magento-SugarCRM	1	1	2
Failure	1	1	2
OSTicket1	2	2	4
Complete	2	2	4
REST1	1	1	2
Complete	1	1	2
SalaryProcessing1	1	1	2
Failure	1	1	2
Summary	15	18	33

11.6.3.4 Alter Structured Query with filter on Workflow ID, Date

Table 70: Structured Query for Workflow Request Count by userid and status with inner query on status and filters on Workflow ID and Date.

**Sample JSON for a above Structured Query altered for inner query on status:
"Workflow Request count with inner query on Status"**

Note: The changes compared to json query above are marked in yellow below.

```
{
  "queryString": null,
  "projections": [
    {
      "column": "wi.user_id",
```

```

        "label": "User Id",
        "type": null,
        "aggregateFunction": null,
        "colorCodes": null,
        "width": 0,
        "iconOnly": false,
        "h_alignment": null,
        "v_alignment": null
    },
    {
        "column": "wf.name",
        "label": "Workflow Name",
        "type": null,
        "aggregateFunction": null,
        "colorCodes": null,
        "width": 0,
        "iconOnly": false,
        "h_alignment": null,
        "v_alignment": null
    },
    {
        "column": "wi.status",
        "label": "Status",
        "type": null,
        "aggregateFunction": null,
        "colorCodes": null,
        "width": 0,
        "iconOnly": false,
        "h_alignment": null,
        "v_alignment": null
    },
    {
        "column": "wi.id",
        "label": "Request Count",
        "type": null,
        "aggregateFunction": "COUNT",
        "colorCodes": null,
        "width": 0,
        "iconOnly": false,
        "h_alignment": null,
        "v_alignment": null
    }
],
"fromClause": "vae_workflow_instance AS wi, vae_workflow_configuration AS wf",
"whereClause": "wi.tenant_id = :tenantId AND status IN ('Complete', 'Failure') AND
wi.id=wf.workflow_config_id",
"groupBy": [
    "wf.name"
],
"orderBy": [
    "wf.name"
],

```

```

"needSummary": true,
"innerQueryColumnName": "wi.status",
"dateColumnName": "wi.created_date",
"workflowIdColumnName": "wi.id",
"workflowIdParamNames": null,
"startDateParamNames": null,
"endDateParamNames": null,
"tenantIdParamNames": [
    "tenantId"
],
"userIdParamNames": null
}

```

11.6.3.5 Structured Query with filter on Tenant ID, User ID

Table 71: Structured Query for Workflow Request Count with inner query on status.

**Sample JSON for above Structured Query altered for inner query on status:
“Workflow Request count with inner query on Status”**

```

{
  "queryString": null,
  "projections": [
    {
      "column": "wi.created_by",
      "label": "UserId",
      "type": null,
      "aggregateFunction": null,
      "colorCodes": null,
      "width": 0,
      "iconOnly": false,
      "h_alignment": null,
      "v_alignment": null
    },
    {
      "column": "wf.name",
      "label": "Workflow Name",
      "type": null,
      "aggregateFunction": null,
      "colorCodes": null,
      "width": 0,
      "iconOnly": false,
      "h_alignment": null,
      "v_alignment": null
    },
    {
      "column": "wi.status",

```

```

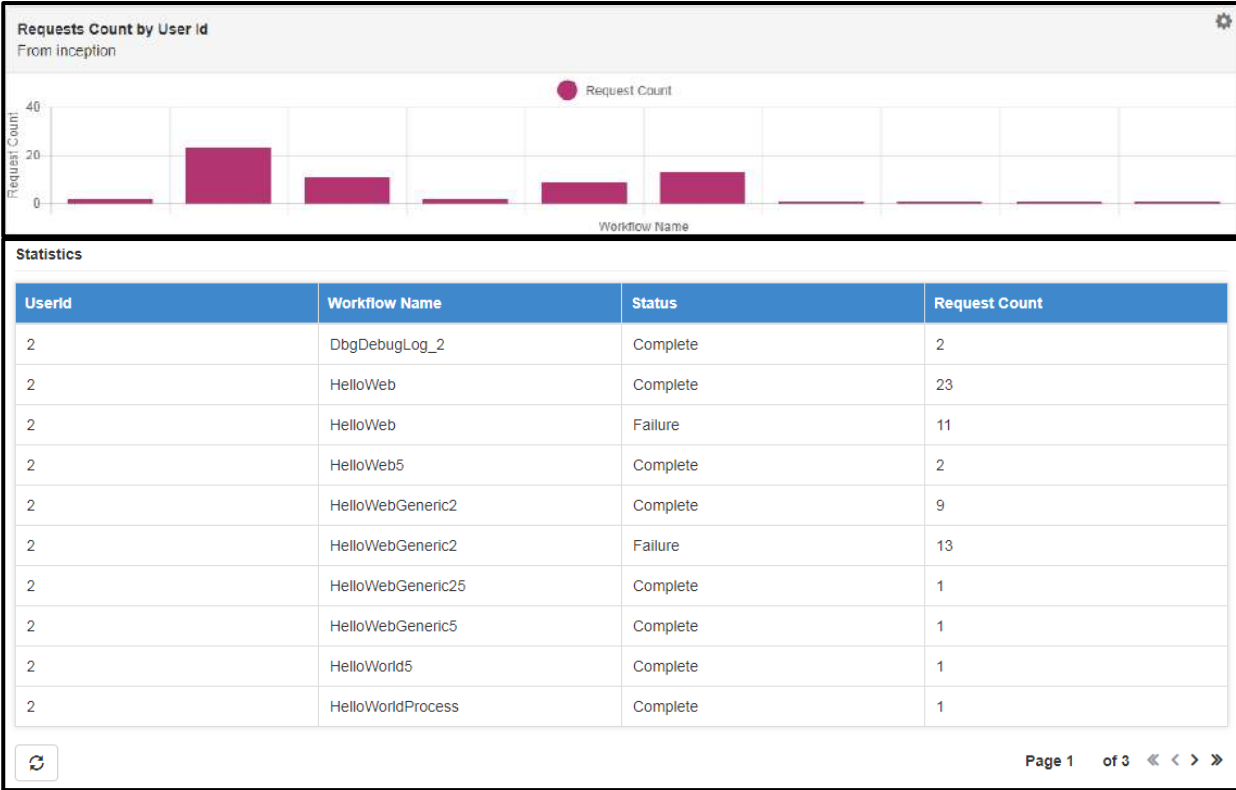
        "label": "Status",
        "type": null,
        "aggregateFunction": null,
        "colorCodes": null,
        "width": 0,
        "iconOnly": false,
        "h_alignment": null,
        "v_alignment": null
    },
    {
        "column": "wi.id",
        "label": "Request Count",
        "type": null,
        "aggregateFunction": "COUNT",
        "colorCodes": null,
        "width": 0,
        "iconOnly": false,
        "h_alignment": null,
        "v_alignment": null
    }
],
"fromClause": "vae_workflow_instance AS wi, vae_workflow_configuration AS wf",
"whereClause": "wi.tenant_id = :tenantId AND status IN ('Complete', 'Failure') AND
wf.id = wi.workflow_config_id AND wi.created_by IN (:UserId)",
"groupBy": [
    "wi.created_by",
    "wf.name",
    "wi.status"
],
"orderBy": [
    "wi.created_by",
    "wf.name",
    "wi.status"
],
"needSummary": false,
"innerQueryColumnName": null,
"dateColumnName": null,
"workflowIdColumnName": null,
"workflowIdParamNames": null,
"startDateParamNames": null,
"endDateParamNames": null,
"tenantIdParamNames": [
    "tenantId"
],
"userIdParamNames": [
    "UserId"
]
}

```

Sample Chart Configuration with Structured Query:

X-Axis Label	Workflow Name	<input type="checkbox"/> Non-numeric. Enable checkbox to specify that Workflow Name is Non-numeric.
Y-Axis Label	Request Count	<input type="checkbox"/> Non-numeric. Do not enable checkbox to specify that Request Count is Non-Numeric.
Plot Against Label		Get a transposed display of count of wf.id.

The chart below shows report on dashboard:



11.6.4 Custom Reports: Formatting Options

11.6.4.1 Introduction

We use color coding in reports to differentiate two rows if report is in tabular form. With help of this feature we can easily distinguish rows according to different process/workflow status, count of operations etc.

11.6.4.2 Changes in report query

Custom Report query object we submit through UI will have following changes in **Projections** list

Table 72: Formatting options in Custom Reports

```

"projections": [
  {
    "column": "workflowId",
    "aggregateFunction": null,
    "label": "Workflow Id",
    "type": "NUMBER",

    "iconOnly": false,
    "h_alignment": "align-center",
    "v_alignment": "align-middle",
    "width": 50,
    "colorCodes": null
  },

  {
    "column": "status",
    "aggregateFunction": null,
    "label": "Status",
    "type": null,

    "iconOnly": true,
    "h_alignment": "align-left",
    "v_alignment": "align-top",

    "width": 100,
    "colorCodes": {
      "Failure": {
        "color": "red",
        "icon": "glyphicon glyphicon-remove-sign"
      },
      "Complete": {
        "color": "green",
        "icon": "glyphicon glyphicon-ok-sign"
      },
      "default": {
        "color": "yellow",
        "icon": null
      }
    }
  }
]

```

```

    },
    {
      "column": id,
      "aggregateFunction": "SUM",
      "label": "Request Count",
      "type": null,

      "iconOnly": false,
      "h_alignment": "align-right ",
      "v_alignment": "align-bottom",
      "width": 50,
      "colorCodes": {
        "1_50": {
          "color": "red",
          "icon": "glyphicon glyphicon-remove-sign"
        },
        "52_100": {
          "color": "green",
          "icon": "glyphicon glyphicon-ok-sign"
        },
        "default": {
          "color": "yellow",
          "icon": null
        }
      }
    }
  ]

```

11.6.4.3 iconOnly

This json key can have three values viz. false, true or null (null will be considered as false and default value is false). If iconOnly is true, then the UI displays icons only instead of text/label. Icon image and color will be selected from colorCodes. colorCodes is discussed in a section below. If iconOnly is false, then the UI displays labels and icons (If a valid icon available in color code and color code of matching criteria exists)

11.6.4.4 h_alignment

This defines horizontal alignment of data or icon in a table cell. The possible values are – align-start, align-left, align-center, align-right and align-end. The meanings are straight forward.

Note: align-end does not work for Internet Explorer. So we have to use align-right if browser is Internet Explorer (IE11).

11.6.4.5 v_alignment

This defines vertical alignment of data or icon in a table cell. The possible values are: align-top, align-middle and align-bottom. The meanings are straight forward.

11.6.4.6 width

Each column can have customized width which can be defined by width key. The value is integer numbers without units.

11.6.4.7 colorCodes

colorCodes can be used in cases where a user knows possible values a column can have and he wants different colors for each possible value or range of values.

colorCode object contains colorCodes and icons. If column datatype is NUMBER, then all colorCode object keys are either a number or range (two numbers are separated by underscore '_'). In the above sample object 9 is single number and if data in cell is exactly equal to 9, then the color and icon will be applied. In case of 10_67, it is range and if the cell value x such that $10 < x \leq 67$ then the colorCode will be applied on UI.

If datatype of column is STRING, then cell value matches with colorCode object key. If they are same then colorCode will be applied.

Note: colorCoding for column with column dataType as 'Duration' is not supported yet. Please note that If you add colorCode to such column, then data will not be displayed

11.6.4.8 Color and Icons

Color can have any valid color format i.e. it supports RGB, RGBA, HSL, HEX or string representation

Icons are bundled with aeui and can have all valid Fontawesome icons found at <https://fontawesome.com/v4.7.0/icons/>

11.6.4.9 default

If cell value does not match with any colorCode, then default colorCode will be applied (If exists).

11.6.4.10 Sample Screens for Custom Reports with formatting options

The following are some sample screenshots with different custom Report configurations as shown below.

1. icon: null or icon value doesn't exist

Workflow Name	Status	Request Count	Successful Operations	Failed Operations	Total Operations
wf1	Failure	2	0	0	0
wf2	Complete	96	0	0	0
wf3	Complete	96	0	0	0
wf4	Failure	96	0	0	0
wf5	Complete	183	0	0	0

Figure 94a: icon not applied

- Icons value and colorCodes value provided as described in the sections above.

The screenshot shows the 'Reports' section of the AutomationEdge Monitoring Dashboard. It features a 'Monitoring Dashboard' dropdown and a 'New Dashboard' button. Below is a 'Status-wise Workflow Operations Report (From inception)' table with the following data:

Workflow Name	Status	Request Count	Successful Operations	Failed Operations	Total Operations
wf1	Failure	2	0	0	0
wf2	Complete	96	0	0	0
wf3	Complete	96	0	0	0
wf4	Failure	96	0	0	0
wf5	Complete	183	0	0	0

Page 1 of 1

Figure 94b: icon and colorCodes applied

- iconOnly: true and h_alignment: "align-center"

This screenshot shows the same 'Status-wise Workflow Operations Report' table as in Figure 94b, but with the 'iconOnly' option set to true and 'h_alignment' set to 'align-center'. The status column now only contains icons: a red asterisk for 'Failure' and a green checkmark for 'Complete'.

Workflow Name	Status	Request Count	Successful Operations	Failed Operations	Total Operations
wf1	✳	2	0	0	0
wf2	✔	96	0	0	0
wf3	✔	96	0	0	0
wf4	✳	96	0	0	0
wf5	✔	183	0	0	0

Page 1 of 1

Figure 94c: iconOnly with align-center option

11.7 Email Reports

Reports can be viewed in dashboards and can be downloaded as PDF/CSV.

Email Reports menu is used to configure schedules for reports in PDF/CSV format to be emailed as a zip file, to specified email addresses, as per the timezone specified. This feature is available only if SMTP configuration has been done for the tenant.

Note: This option generates and emails reports with the first 10000 records.

Following are the steps to configure Email Reports,

1. Navigate to the Reports→Email Reports sub menu.
2. Click Add New button on the top right corner.

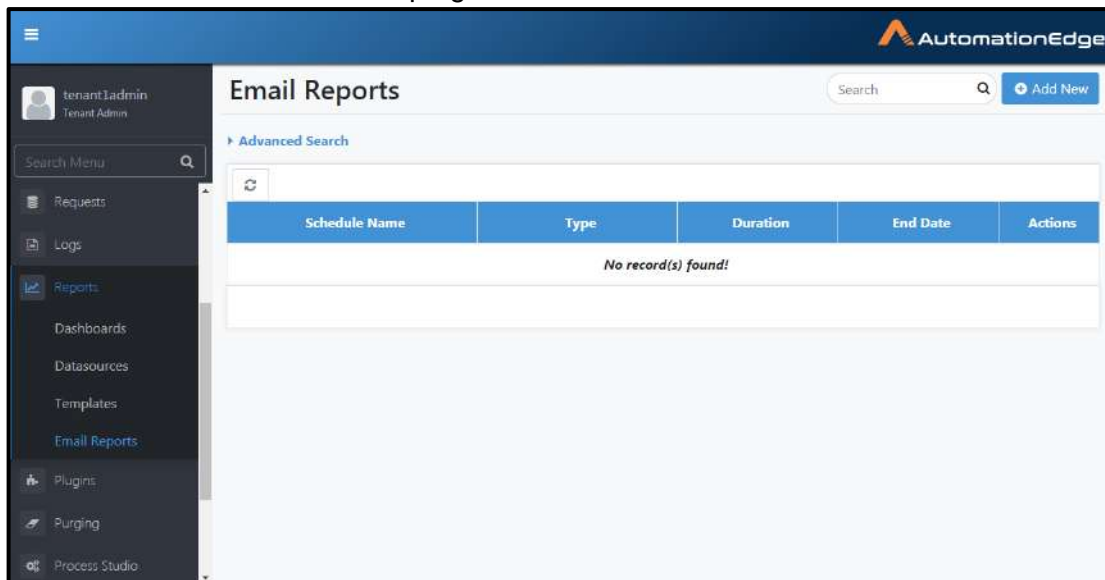
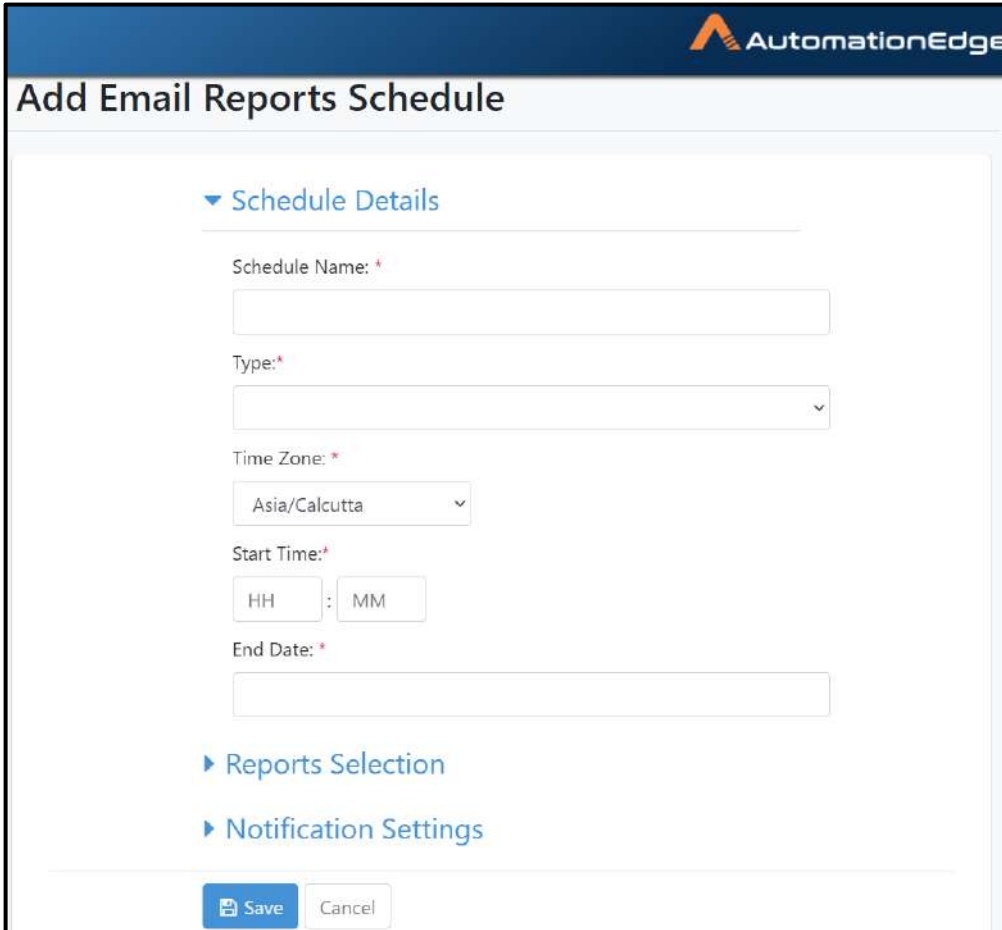


Figure 94d: Email Report Schedules

3. The Add Email Reports Schedule page appears as seen below.



Add Email Reports Schedule

AutomationEdge

▼ Schedule Details

Schedule Name: *

Type: *

Time Zone: *
Asia/Calcutta

Start Time: *
HH : MM

End Date: *

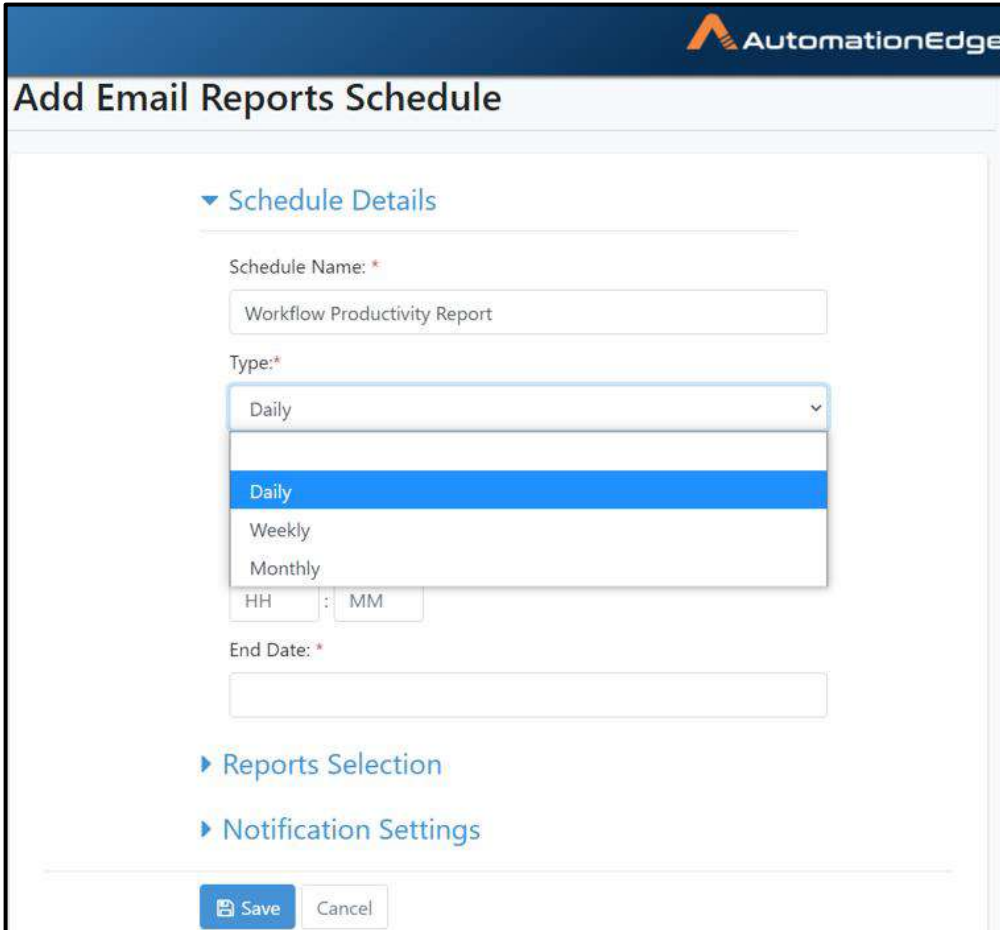
▶ Reports Selection

▶ Notification Settings

Save Cancel

Figure 94e: Add New Email Report Schedule

4. Provide a Schedule name and choose a Schedule Type from the drop down list.



Add Email Reports Schedule

AutomationEdge

▼ Schedule Details

Schedule Name: *

Workflow Productivity Report

Type:*

Daily

Daily

Weekly

Monthly

HH : MM

End Date: *

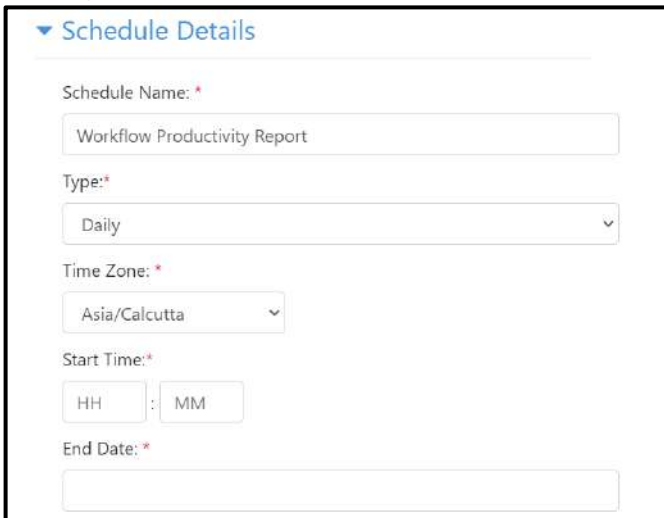
▶ Reports Selection

▶ Notification Settings

Save Cancel

Figure 94f: Schedule Type

5. If Type chosen is Daily for sending the reports by email, specify a Start time (HH:MM format) and an End Date.



▼ Schedule Details

Schedule Name: *

Workflow Productivity Report

Type:*

Daily

Time Zone: *

Asia/Calcutta

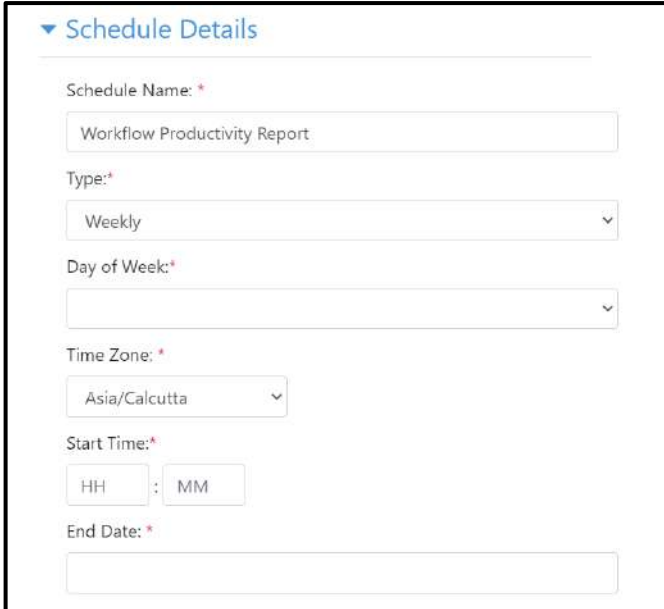
Start Time:*

HH : MM

End Date: *

Figure 94g: Daily Schedule Configuration

- If Type chosen is Weekly for sending the reports by email, specify the Day of Week, a Start time (HH:MM format) and an End Date.

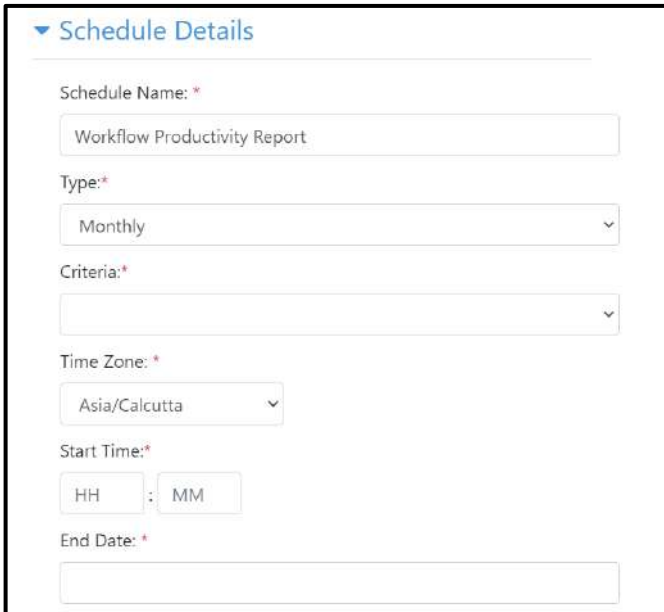


The screenshot shows a form titled "Schedule Details" with the following fields:

- Schedule Name:** * (Text input: Workflow Productivity Report)
- Type:** * (Dropdown menu: Weekly)
- Day of Week:** * (Dropdown menu: empty)
- Time Zone:** * (Dropdown menu: Asia/Calcutta)
- Start Time:** * (Time input: HH : MM)
- End Date:** * (Text input: empty)

Figure 94h: Weekly Schedule Configuration

- If Type chosen is Monthly for sending the reports by email, specify the Criteria, a Start time (HH:MM format) and an End Date.

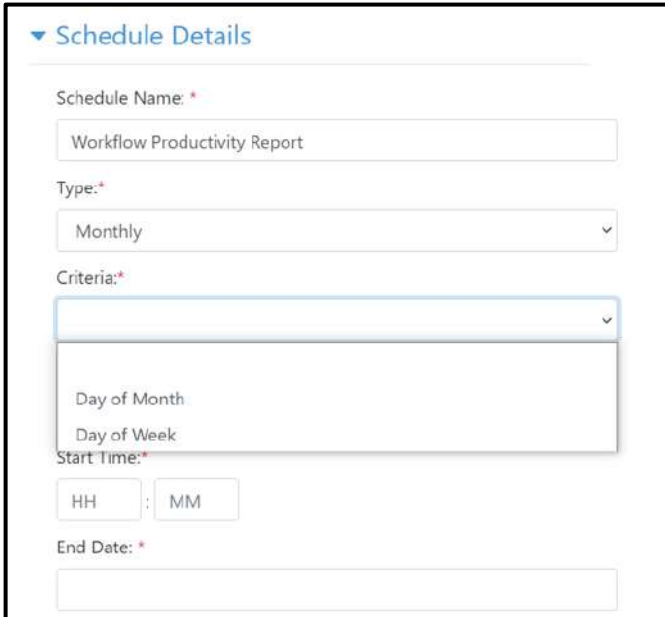


The screenshot shows a form titled "Schedule Details" with the following fields:

- Schedule Name:** * (Text input: Workflow Productivity Report)
- Type:** * (Dropdown menu: Monthly)
- Criteria:** * (Dropdown menu: empty)
- Time Zone:** * (Dropdown menu: Asia/Calcutta)
- Start Time:** * (Time input: HH : MM)
- End Date:** * (Text input: empty)

Figure 94i: Monthly Schedule Configuration

8. Choose a Criteria from the below – Day of Month or Day of Week.

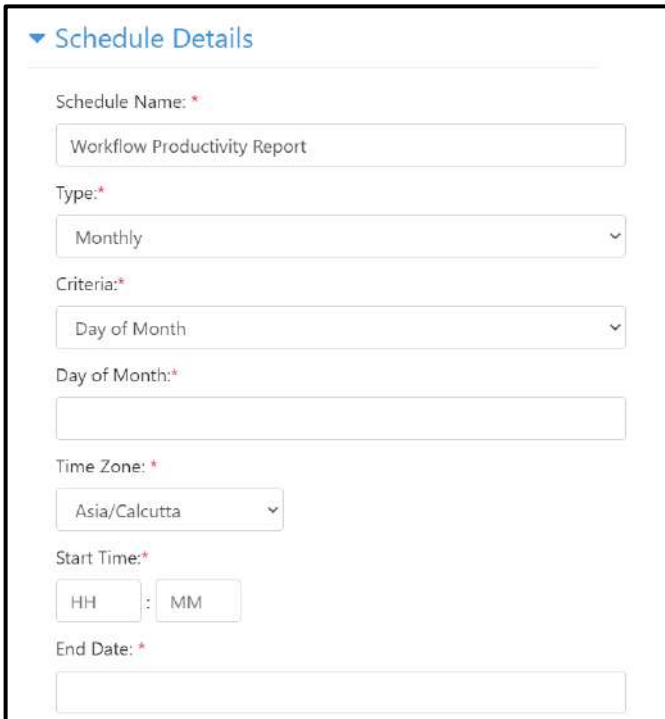


The screenshot shows the 'Schedule Details' form with the following fields:

- Schedule Name:** * Workflow Productivity Report
- Type:** * Monthly
- Criteria:** * (Dropdown menu is open, showing 'Day of Month' and 'Day of Week' options)
- Start Time:** * (HH : MM)
- End Date:** *

Figure 94j: Select Monthly Schedule Criteria

9. If Day of Month is chosen provide a Day of Month by scrolling the scroll bar in the field to increment or decrement the values.



The screenshot shows the 'Schedule Details' form with the following fields:

- Schedule Name:** * Workflow Productivity Report
- Type:** * Monthly
- Criteria:** * Day of Month
- Day of Month:** * (Input field with a scroll bar)
- Time Zone:** * Asia/Calcutta
- Start Time:** * (HH : MM)
- End Date:** *

Figure 94k: Select Day of the Month

10. If Day of Week is chosen in criteria, provide Day of Week and Weekday of Month. Day of the week can be Sunday-Saturday and Weekday of Month can be First, Second, Third, Fourth or Last. (e.g. Every last Friday of the Month at 7PM, or every First Monday at 8AM, or on every 4th day of the Month at 7AM or last day of the Month at 9PM)

▼ Schedule Details

Schedule Name: *

Type: *

Criteria: *

Day of Week: *

Weekday of Month: *

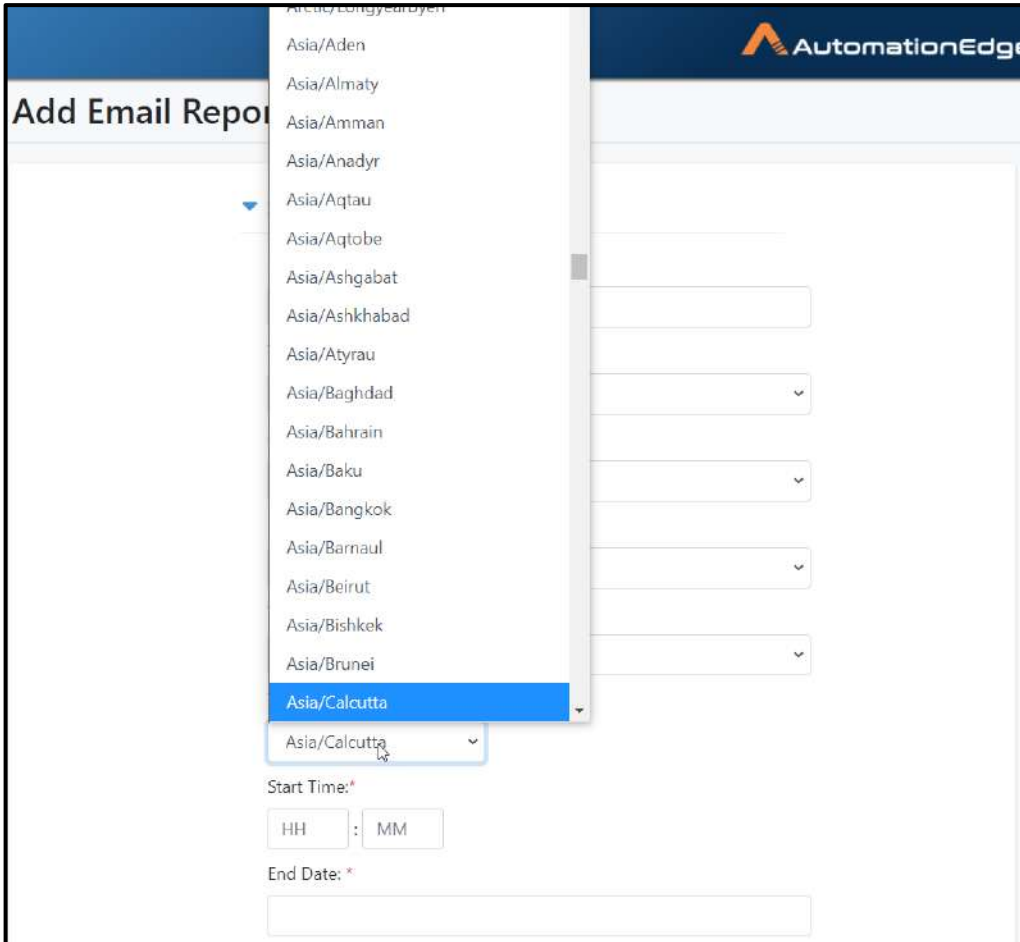
Time Zone: *

Start Time: *
 :

End Date: *

Figure 94I: Select Day of the Week

11. The user's (browser) time zone is populated by default. User can change the time zone if needed.
12. Select a Time Zone from the list. AutomationEdge server will generate and email the report, at the local time according to the time zone specified.



The screenshot shows the 'Add Email Report' form in the AutomationEdge interface. A dropdown menu is open, displaying a list of time zones. The 'Asia/Calcutta' option is highlighted in blue. Below the dropdown, there are input fields for 'Start Time: *' (with 'HH' and 'MM' sub-fields) and 'End Date: *'.

AutomationEdge

Add Email Report

- Asia/Aden
- Asia/Almaty
- Asia/Amman
- Asia/Anadyr
- Asia/Aqtau
- Asia/Aqtobe
- Asia/Ashgabat
- Asia/Ashkhabad
- Asia/Atyrau
- Asia/Baghdad
- Asia/Bahrain
- Asia/Baku
- Asia/Bangkok
- Asia/Barnaul
- Asia/Beirut
- Asia/Bishkek
- Asia/Brunei
- Asia/Calcutta**
- Asia/Calcutta

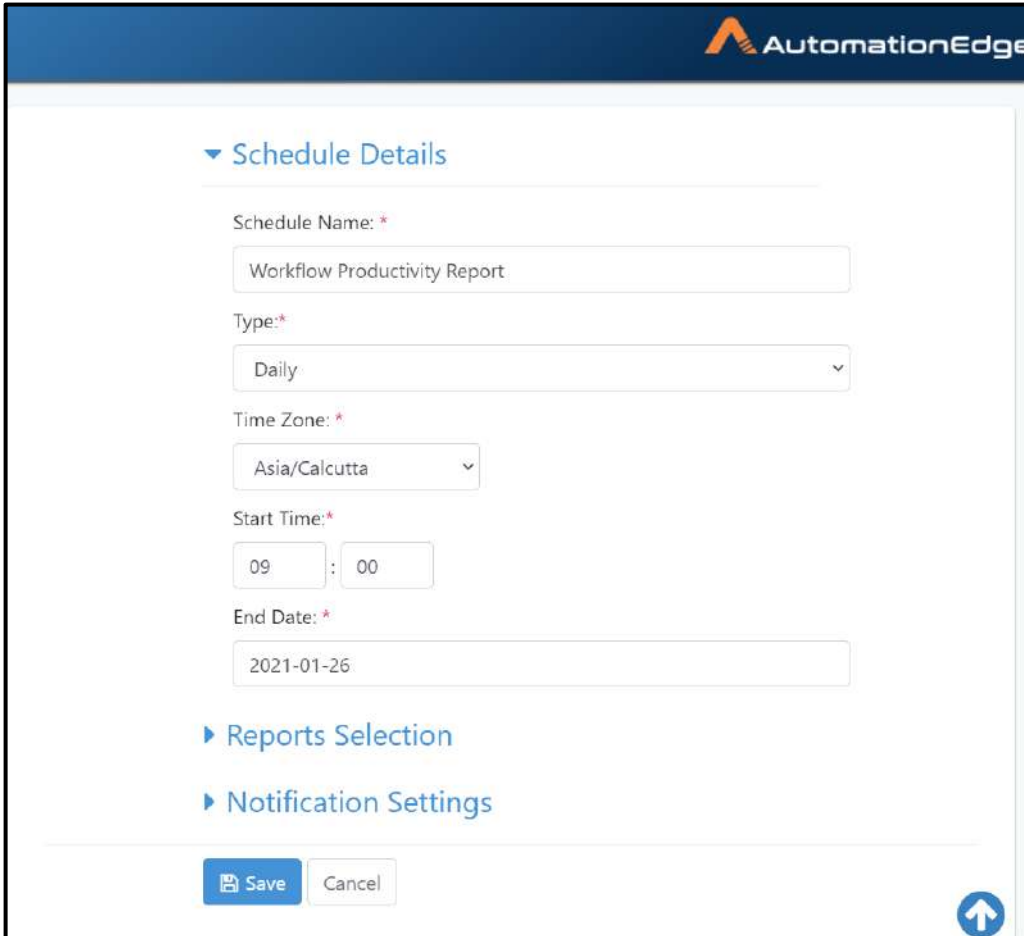
Start Time: *

HH : MM

End Date: *

Figure 94m: Select Time Zone

13. Let us create a Daily Email Reports Schedule with Schedule details as below.



AutomationEdge

▼ **Schedule Details**

Schedule Name: *
Workflow Productivity Report

Type: *
Daily

Time Zone: *
Asia/Calcutta

Start Time: *
09 : 00

End Date: *
2021-01-26

▶ **Reports Selection**

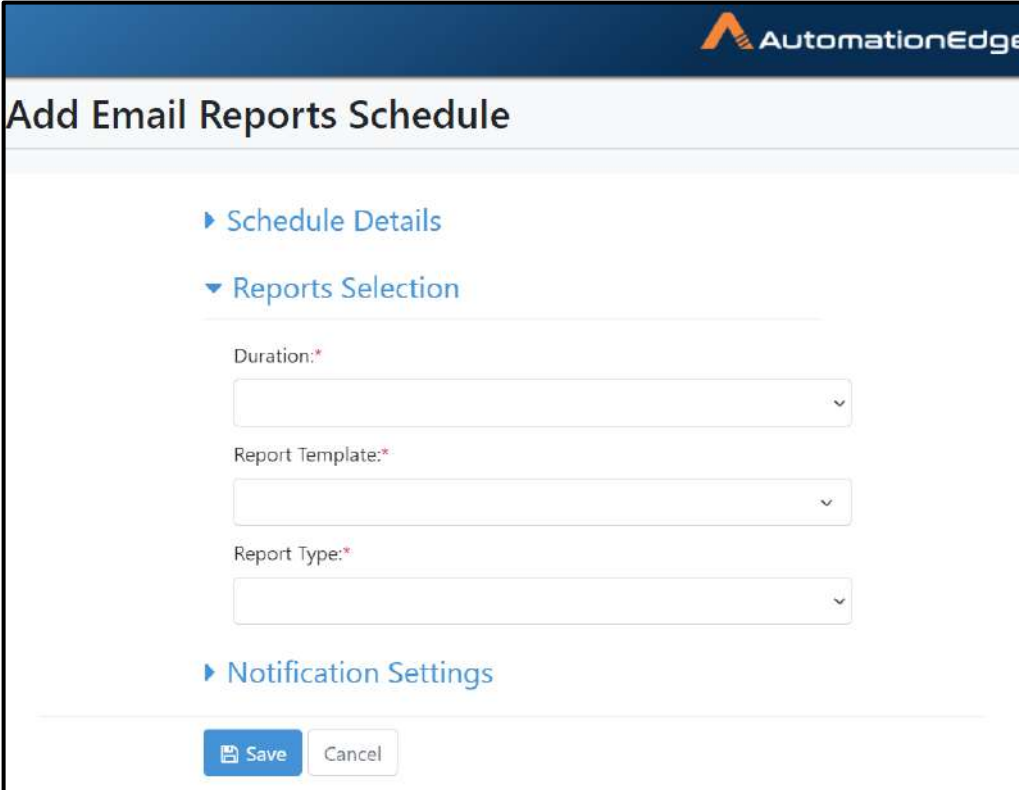
▶ **Notification Settings**

Save **Cancel**

↑

Figure 94n: A Daily Schedule

14. Next, let's go to the Reports Selection section.



Add Email Reports Schedule

▶ Schedule Details

▼ Reports Selection

Duration:*

Report Template:*

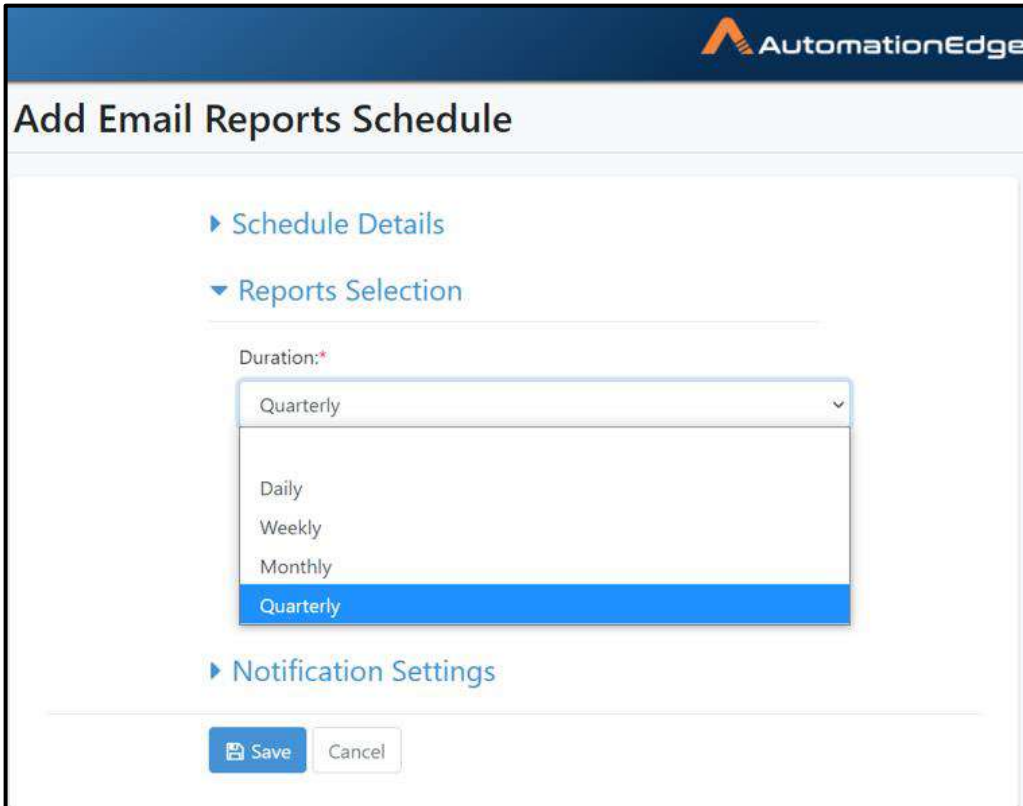
Report Type:*

▶ Notification Settings

Save Cancel

Figure 94o: Reports Selection

15. In the Duration field select the cumulative period of data to be included in the report. It has the following options – Daily, Weekly, Monthly or Quarterly.



The screenshot shows the 'Add Email Reports Schedule' interface. The 'Reports Selection' section is expanded, revealing a 'Duration' dropdown menu. The dropdown menu is open, showing the following options: Quarterly, Daily, Weekly, Monthly, and Quarterly. The 'Quarterly' option at the bottom of the list is highlighted in blue. Below the dropdown menu, there are 'Save' and 'Cancel' buttons.

Figure 94p: Report Data Duration

16. Choose one or multiple Report Templates by enabling checkbox next to the reports.

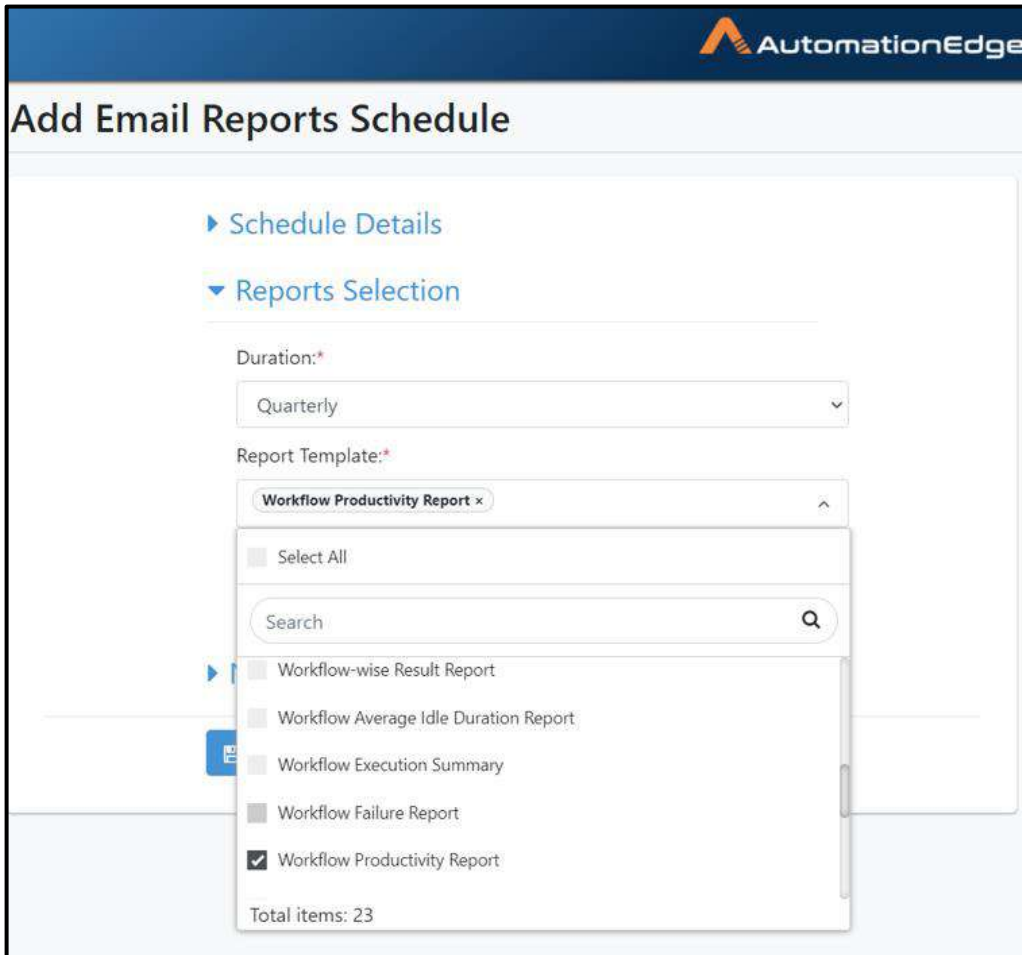
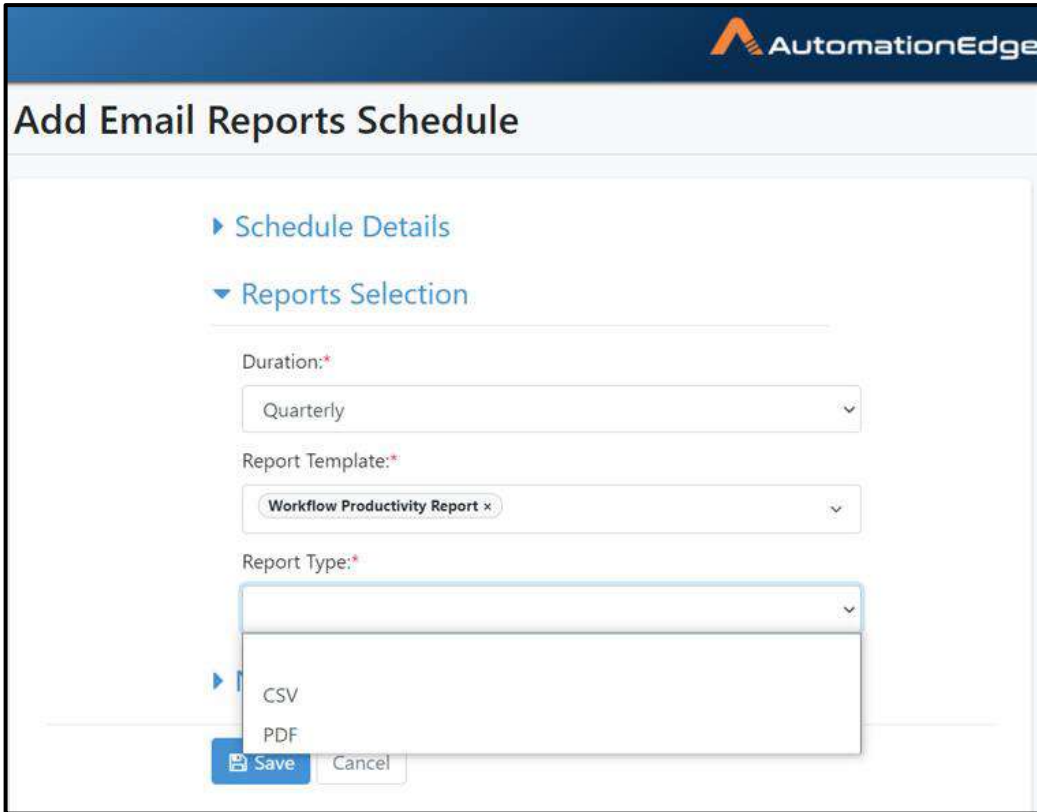


Figure 94q: Select Report Template

17. The Report Templates are now added in the Report Selection.
18. Select a Report Type from the list. Choose from CSV/PDF.



Add Email Reports Schedule

▶ Schedule Details

▼ Reports Selection

Duration:*
Quarterly

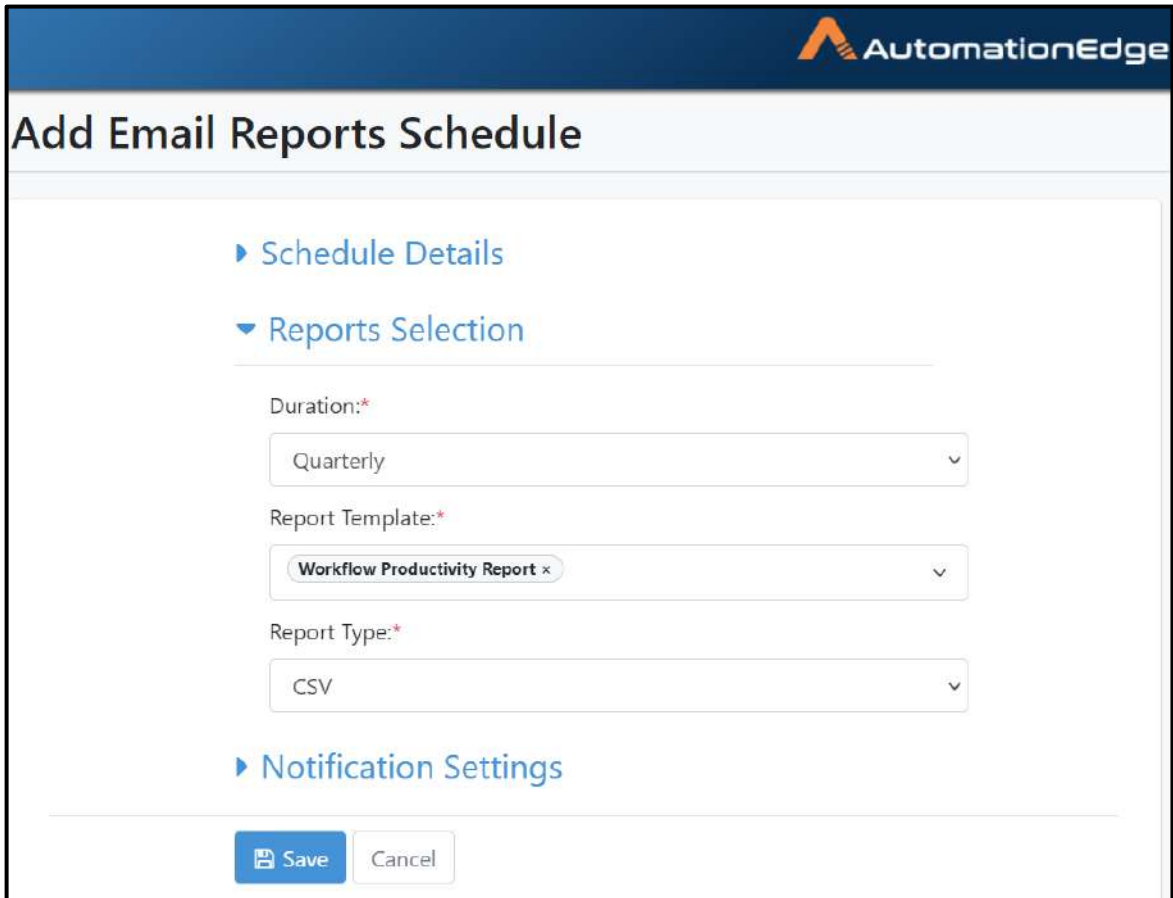
Report Template:*
Workflow Productivity Report x

Report Type:*
CSV
PDF

Save Cancel

Figure 94r: Selected Report Template

19. In this case CSV is selected.



AutomationEdge

Add Email Reports Schedule

▶ Schedule Details

▼ Reports Selection

Duration:*
Quarterly

Report Template:*
Workflow Productivity Report

Report Type:*
CSV

▶ Notification Settings

Save Cancel

Figure 94s: Selected Report Type

20. Next let us expand the Notification section.

21. Similar to Notification feature the following options to select the senders is provided

- By Roles (select the list of roles like tenant admin/WF admin)
- By Users (selecting the list of users)
- Providing the email addresses

22. Provide Email list entries and Press <Enter> or <Comma> key to add the entries to the Email List. Click Save.

Figure 94t: Notification Settings

23. The 'Email Reports Schedule' is now visible in the list.

Schedule Name	Type	Duration	End Date	Actions
Workflow Productivity Report	Daily	Quarterly	26-Jan-2021	

Figure 94u: Email Reports Schedule Added

24. This completes the process of configuring 'Email Reports Schedule'. Report is sent in zip format to the email addresses configured.

11.8 Reports: Features/Permissions for other users

Table 73: Reports Features

Feature/Role	Tenant Administrator	Workflow Administrator	User Administrator	Agent Administrator	Tenant User	Activity Monitor
New Report	✓	✓	-	-	✓	✓
New Dashboard	✓	✓	-	-	✓	✓
Dashboard Selection	✓	✓	-	-	✓	✓
Reports Datasources and Template	✓	-	-	-	-	-
New Report (using Custom Report Template)	✓	✓	-	-	✓	✓
Email Report	-	✓	-	-	-	-

*Tenant users can use the AutomationEdge features depending on Read, Write or Execute permissions granted to them on workflows.

12 Plugins

Plugins are managed by System Administrator (For details refer to the AutomationEdge_R7.0.0_System_Administrator_Guide). Tenant Administrator has a view only access to plugins except the option to set plugin properties.

The following screenshot shows the list of plugins current available in the system.

Plugin Name	Version			Created	Last Modified	Actions
	Release	Framework	Plugin			
PS_NATIVE	-	3	3.0	25-Jan-2019 15:29:23	24-Jun-2021 08:21:27	⋮ ⓘ
MSSQL-Server	3.0	3	3.0	5-Jul-2021 07:20:30	5-Jul-2021 07:20:30	⋮ ⓘ
active-directory	3.0	3	7.0	5-Jul-2021 08:11:27	5-Jul-2021 08:11:27	⋮ ⓘ
AirWatch	3.0	3	3.0	5-Jul-2021 08:11:27	5-Jul-2021 08:11:27	⋮ ⓘ
AmazonEC2	3.0	3	3.0	5-Jul-2021 08:11:29	5-Jul-2021 08:11:29	⋮ ⓘ
CAPTCHA	3.0	3	4.0	5-Jul-2021 08:11:29	5-Jul-2021 08:11:29	⋮ ⓘ
GoogleSheets	3.0	3	3.0	5-Jul-2021 08:11:29	5-Jul-2021 08:11:29	⋮ ⓘ
Intune	3.0	3	3.0	5-Jul-2021 08:11:30	5-Jul-2021 08:11:30	⋮ ⓘ
Jira	3.0	3	6.0	5-Jul-2021 08:11:31	5-Jul-2021 08:11:31	⋮ ⓘ
Jira-ServiceDesk	3.0	3	3.0	5-Jul-2021 08:11:31	5-Jul-2021 08:11:31	⋮ ⓘ

Figure 95a: Plugins View

A description of the columns is provided below.

Table 74: Plugin Details

Field Name	Description
Plugin Name	Displays the name of the plugin
Version:	
Release	Displays the AutomationEdge Plugin Release version.
Framework	Displays the Process Studio Framework version on which the plugin was created.
Plugin	Displays the plugin version.
Created	Displays the date the plugin was created.
Last Modified	Displays the date the plugin was last modified.
Actions:	
Plugin Steps (⋮)	Click to display the list of steps in the Plugin.
Plugin Utilization (ⓘ)	Click to display the list of workflows in which the plugin has been utilized.
Configure Properties (⚙)	Click to display the list of plugin properties that can be configured. These properties can be configured at Tenant level or Agent level.

Field Name	Description
	<p>A Tenant Administrator can configure properties at both Tenant level and Agent level.</p> <p>An Agent Administrator can configure properties only at Agent level.</p> <p>Note: Configure Properties icon is only on some Plugins that require configurations.</p>

12.1 Plugin Steps

Click on any Plugin Steps icon (☰) in the Actions column to see its steps.

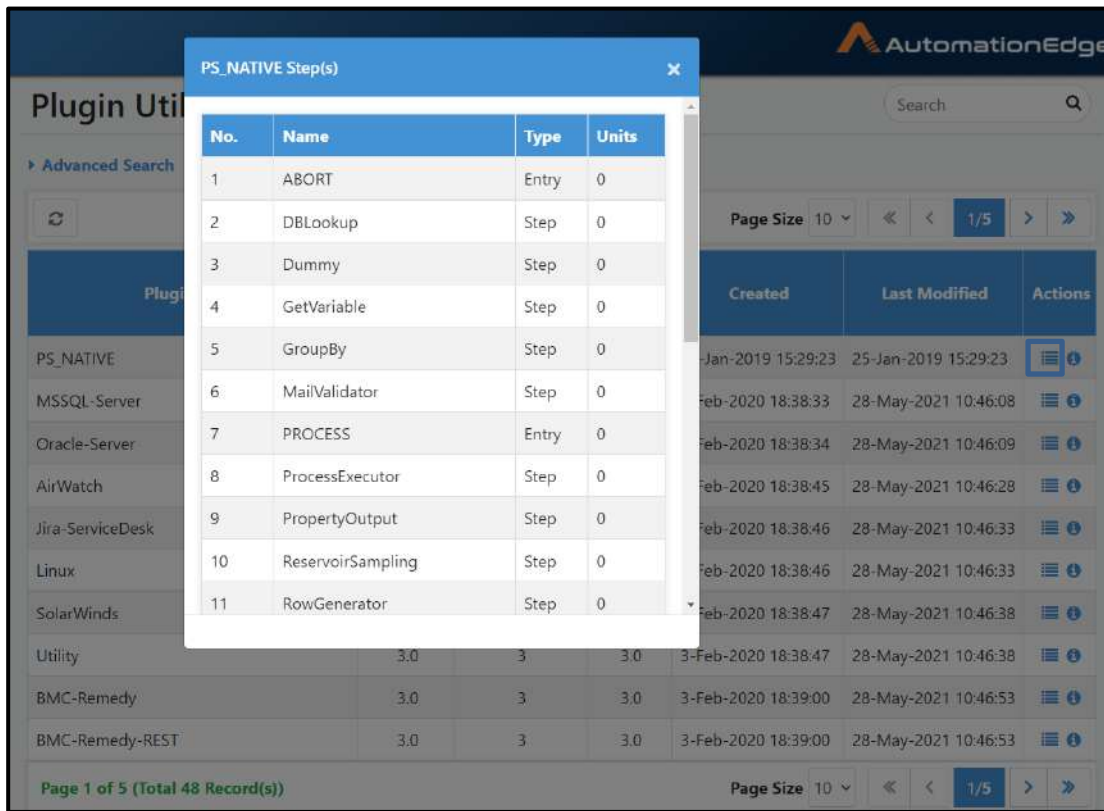


Figure 95b: Plugins Steps

12.2 Plugin Utilization

Click the Plugin Utilization icon (📊) in the Actions column, next to the OOTB-plugin. It shows the OOTB Plugin Step Units utilization in workflows. In the screenshot below plugin Utilization is seen in two workflows as marked below.

Note: These step units add up as consumption of License Step Units.

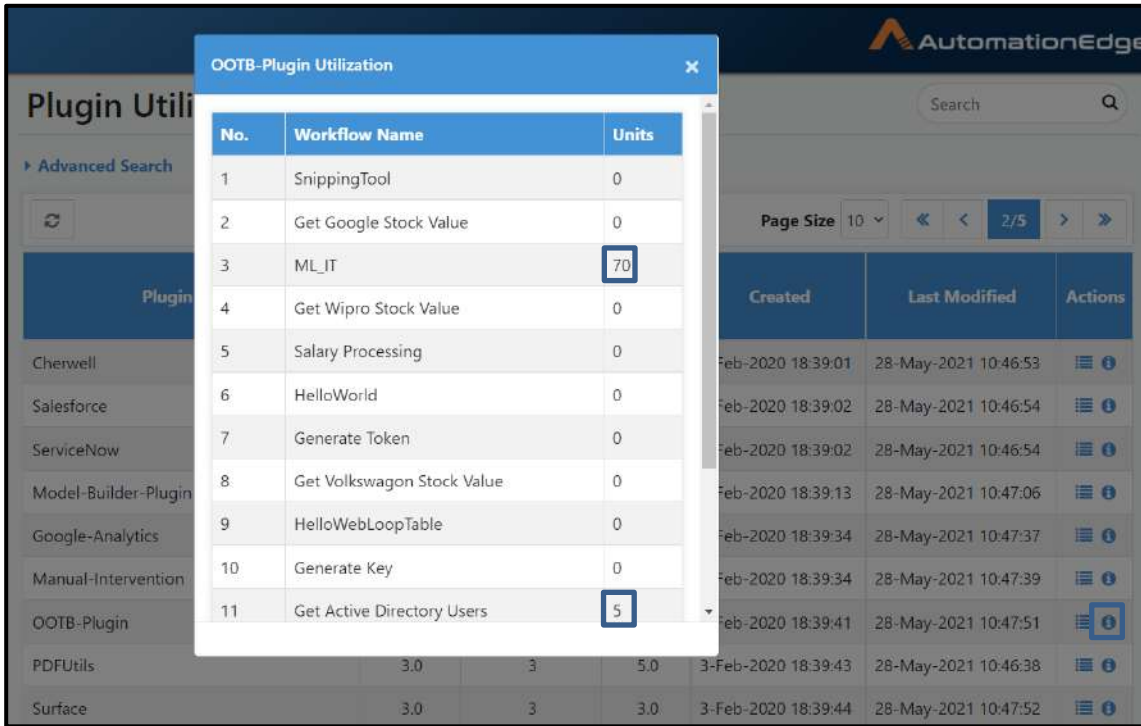
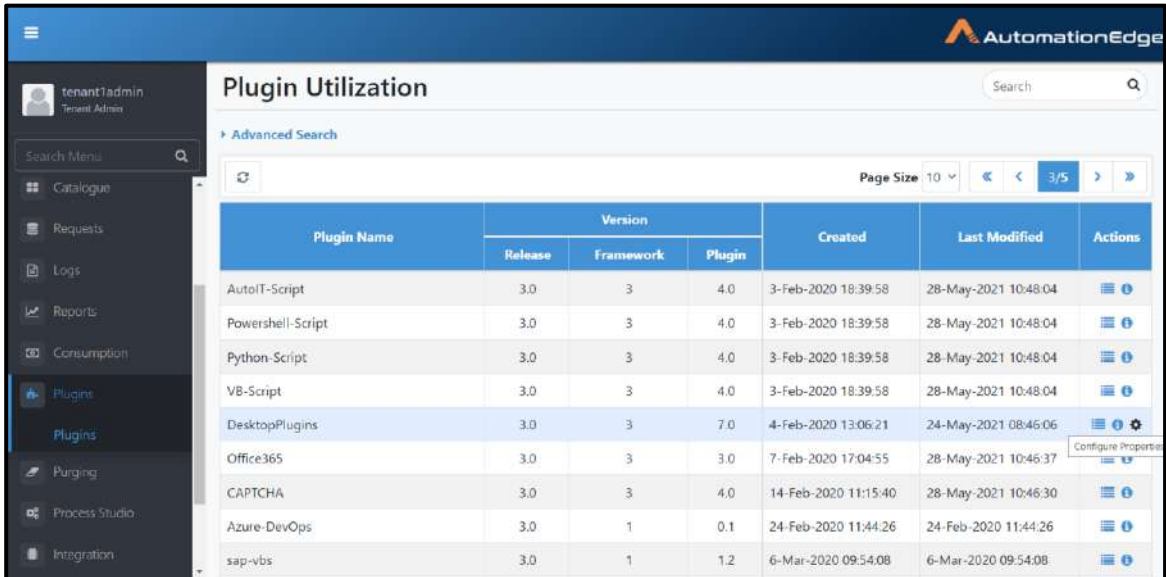


Figure 95c: OOTB-plugin utilization in workflows

12.3 Plugin Properties Configuration

Some plugins have the Configure Properties option (⚙️). Following are the steps to configure plugin properties.

1. Notice the plugin DesktopPlugins in the following snapshot. Next to Actions icon there is a gear icon to Configure properties.



Plugin Name	Version			Created	Last Modified	Actions
	Release	Framework	Plugin			
AutoIT-Script	3.0	3	4.0	3-Feb-2020 18:39:58	28-May-2021 10:48:04	⋮ ⓘ
Powershell-Script	3.0	3	4.0	3-Feb-2020 18:39:58	28-May-2021 10:48:04	⋮ ⓘ
Python-Script	3.0	3	4.0	3-Feb-2020 18:39:58	28-May-2021 10:48:04	⋮ ⓘ
VB-Script	3.0	3	4.0	3-Feb-2020 18:39:58	28-May-2021 10:48:04	⋮ ⓘ
DesktopPlugins	3.0	3	7.0	4-Feb-2020 13:06:21	24-May-2021 08:46:06	⋮ ⓘ ⚙️
Office365	3.0	3	3.0	7-Feb-2020 17:04:55	28-May-2021 10:46:37	⋮ ⓘ
CAPTCHA	3.0	3	4.0	14-Feb-2020 11:15:40	28-May-2021 10:46:30	⋮ ⓘ
Azure-DevOps	3.0	1	0.1	24-Feb-2020 11:44:26	24-Feb-2020 11:44:26	⋮ ⓘ
sap-vbs	3.0	1	1.2	6-Mar-2020 09:54:08	6-Mar-2020 09:54:08	⋮ ⓘ

Figure 95d: Configure plugin properties gear icon

2. Click the gear icon to configure properties. The DesktopPlugins Properties Configuration pop-up appears. As you can see there is one property Desktop Runtime Port that can be configured at Tenant Level. This property configuration will be applicable for all Agents of that Tenant.

- Click Edit to set a Property Value at Tenant Level. Set Desktop Runtime Port value at Tenant level as shown below. Confirm the value by clicking the tick mark under Actions.

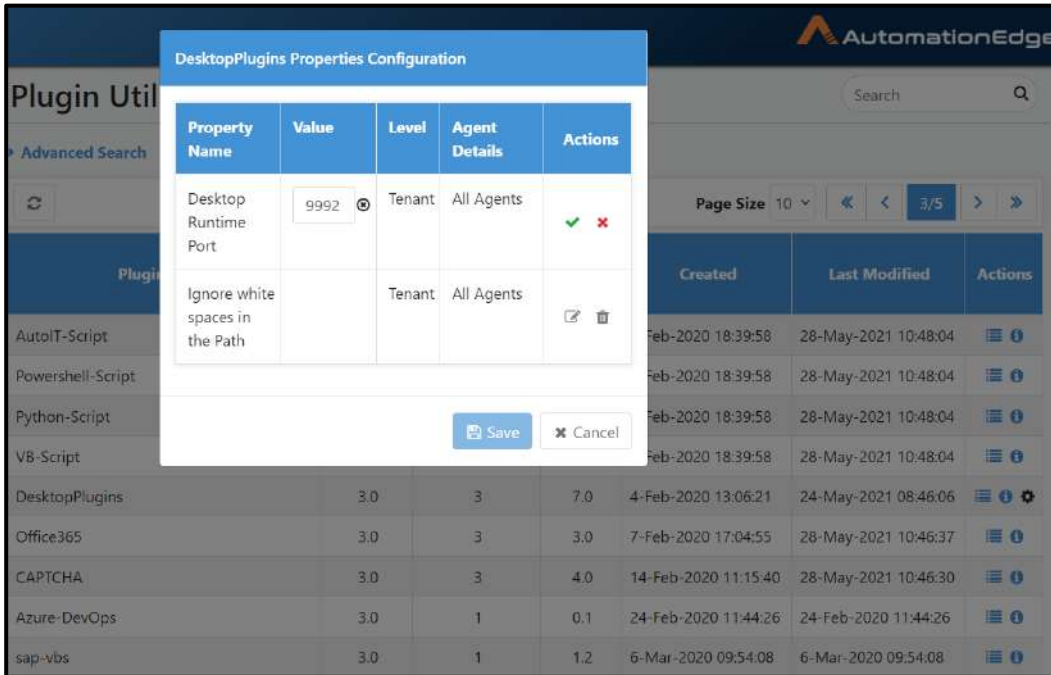


Figure 95e: Configure plugin properties with gear icon

- Set Ignore White Spaces in the Path value at Tenant level as shown below. The possible values are true/false. Confirm the value by clicking the tick mark under Actions.

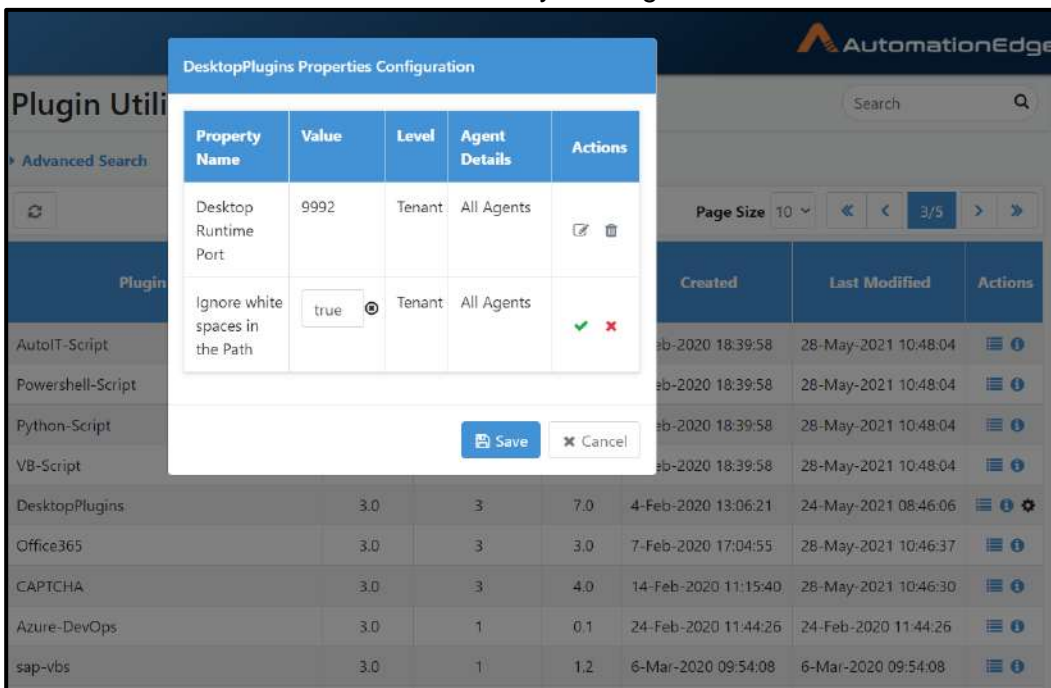


Figure 95f: Desktop Runtime port at Tenant Level

- Click Save to make the Desktop Runtime Port and Ignore White Spaces in Path at Tenant Level Permanent. Property Values updated for selected Plugin success message appears.
- Click Add Property Value to Add the Desktop Runtime Port/Ignore White Spaces in Path at Agent level.

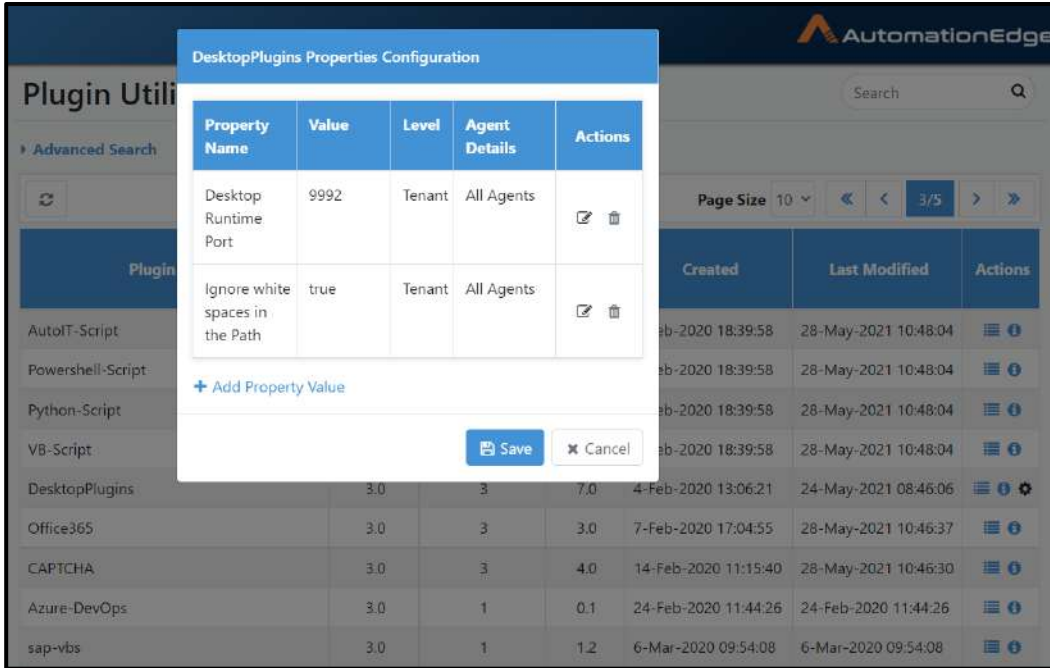


Figure 95g: Add Plugin Property

- If different values are set at Tenant level and Agent level the value at Agent level takes effect. In this case Desktop Runtime Port is added. Select an Agent from the drop down list. Confirm Desktop Runtime Property by clicking the tick mark.

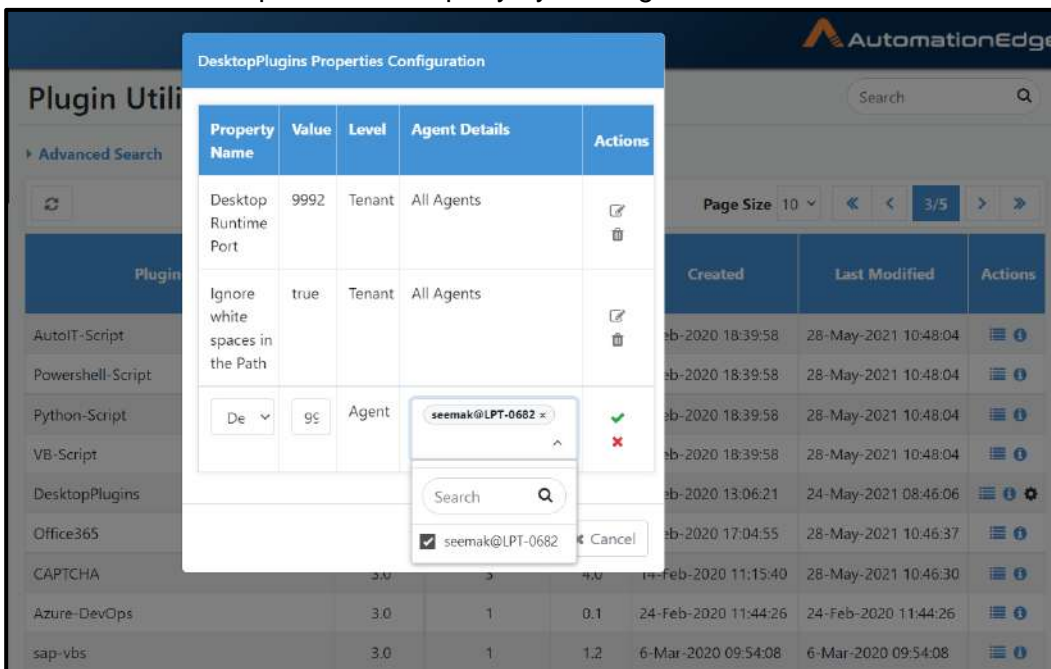


Figure 95h: Select Agent to configure property at Agent level

- Click Save to save the properties else Cancel to discard them.

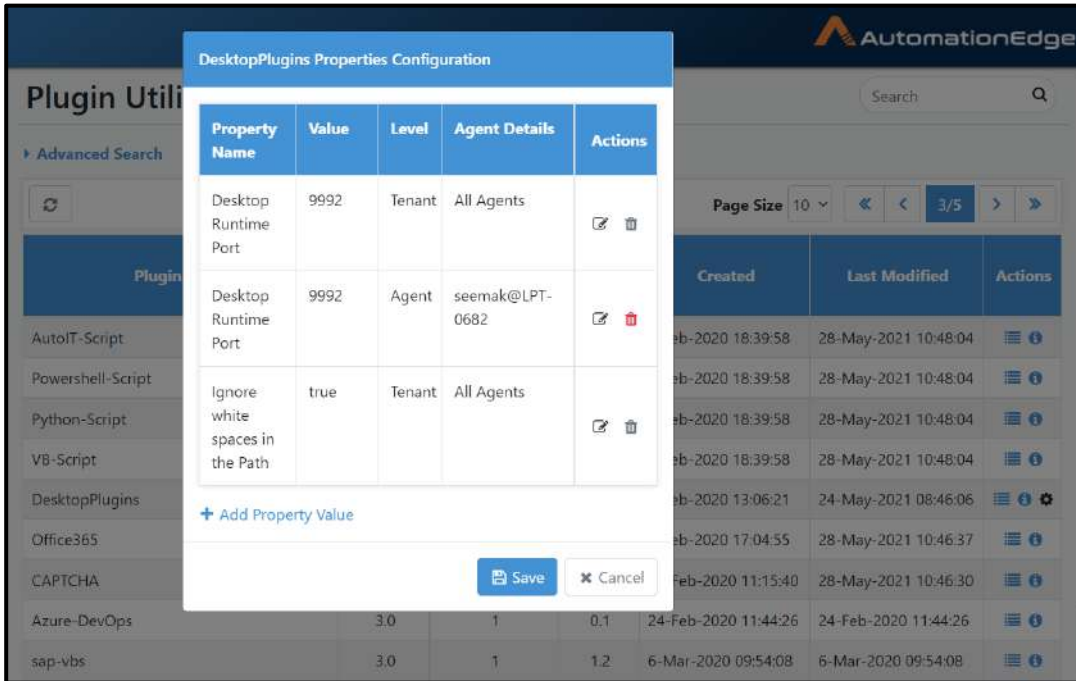


Figure 95i: Save plugin property

- Upon Save, Property Values updated for selected Plugin message appears.

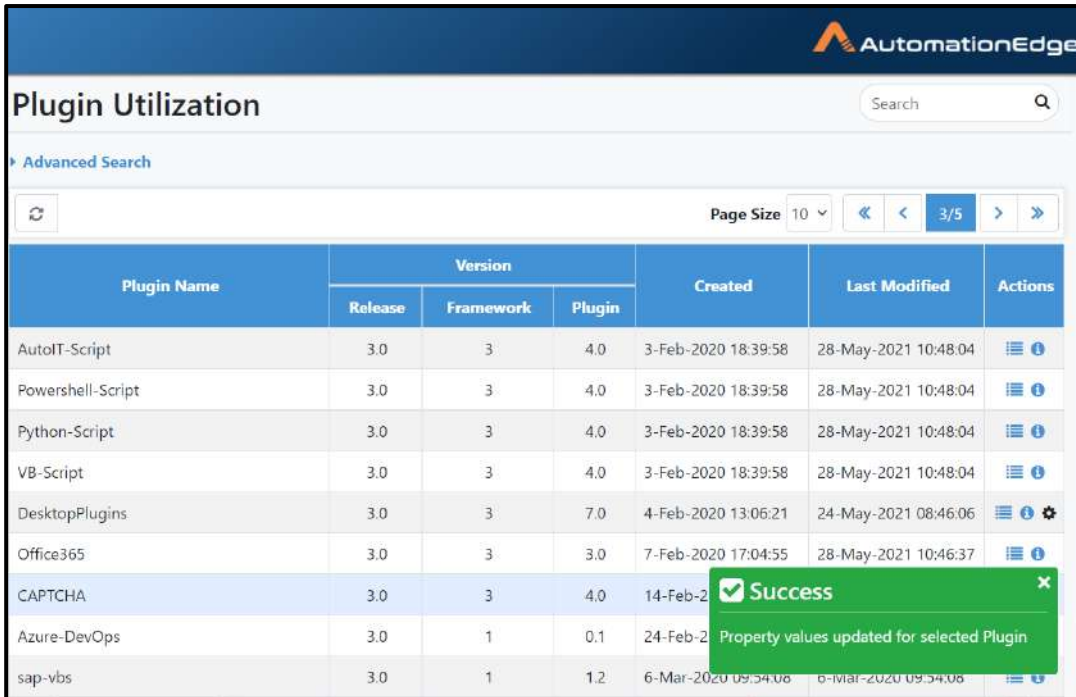


Figure 95j: Plugin property values updated success message

13 Purging

Few tables in the AutomationEdge(AE) system get populated with a large amount of data. Over a period of time the records in these tables grow and need to be purged so that the system can run with optimal performance.

Purging allows setup a Purge Policy and Purge Schedule to purge these database tables as needed. This results in, reduction of database and disk space usage and in turn increases AutomationEdge system performance.

Purging option is available for the following data tables,

- ❖ Audit Logs
- ❖ Workflow Requests
- ❖ Notification History

AE UI has a Purging menu under Settings for purging this data. Purging has three menu options: Purge Policy, Purge Schedule and Archives. A System Administrator has permissions to setup Purge Policy and Purge Schedule. A Tenant Administrator can only edit the Purge Policy at the Tenant level and view Purge Schedule. Thirdly, Archived menu is also visible to Tenant Administrator to view and download Archives.

These three menu options are discussed below,

13.1 Purge Policy

A Purging Policy includes a Purge Duration and Notification details. Purge Policy determines Purge Duration (in months) for each of the table data for Audit Logs, Workflow Requests and Notification History. The Purged data is then available as Archives.

13.1.1 Purge Duration

Set a Purge Duration for the following for the database tables in months. Minimum duration is one month. It is mandatory to set the duration for all the four tables (a value greater than zero).

13.1.2 Notification Details

Notifications may be sent by System Administrators or Tenant Administrators. Following are the use cases,

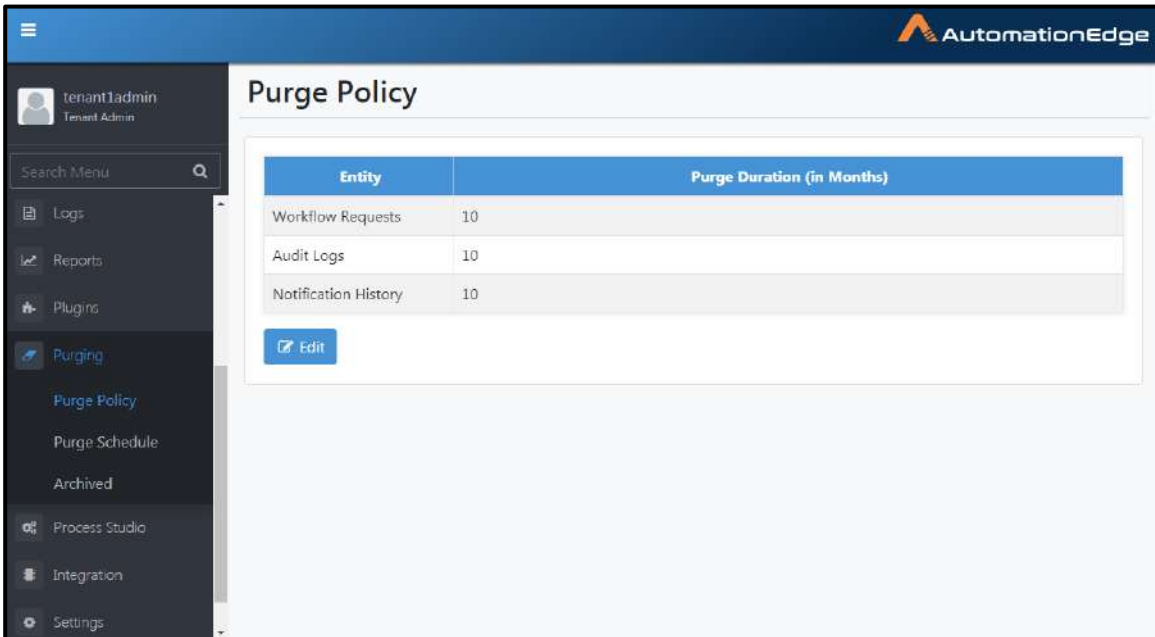
- If SMTP is configured for the Sysadmin, an email would be sent to all Tenant Administrators in following cases.
- But if Tenant overwrites the purging policy then mail is sent by Tenant Administrator from the SMTP configured for the Tenant; to all Tenant Administrators in the Tenant organization and the emails listed for notifying.

Notification is sent on the following events,

- Sysadmin creates/updates Purge Policy
- Sysadmin creates/updates/deletes Purge Schedule
- Tenant Admin updates Purge Policy. This specific to the Tenant. Email is sent to Tenant Admins in the Tenant or Users emails listed for notifying.
- 3 days before purging schedule, a notification is sent every day (The number of days is configurable such as 7 days etc. The number of days is configurable in AutomationEdge properties file. Set `ae.purge.notification.period=<number of days e.g.7>` to all Tenants Administrators and user emails listed for notifying.
- Notification after purging is completed is for all Tenants.

Following are the steps to create a Purge policy including Purge Duration and Notification Details,

1. Navigate to Purging→Purge Policy menu
2. The Purge Policy is visibly here as set by the System Administrator. A Tenant Administrator can edit the policy.
3. Click Edit.

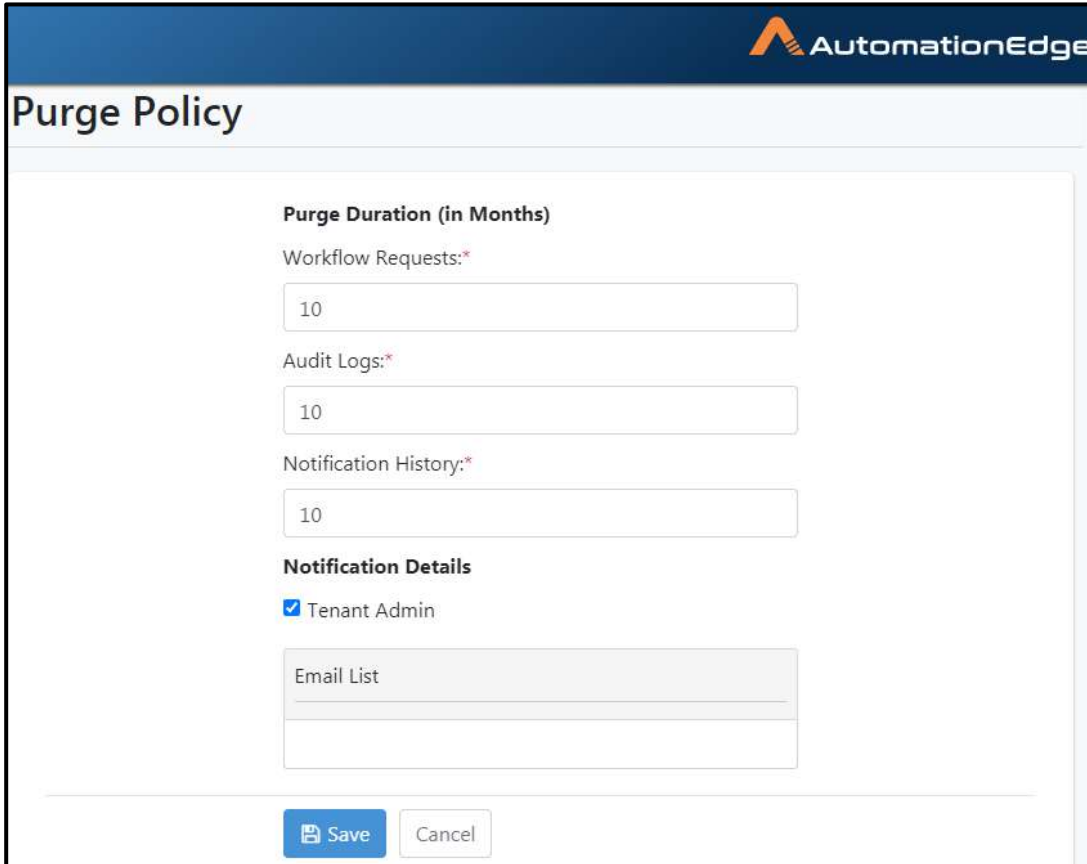


Entity	Purge Duration (in Months)
Workflow Requests	10
Audit Logs	10
Notification History	10

[Edit](#)

Figure 96a: Edit Purge Policy

4. Change Purge Duration by providing new Configuration details. Also, provide Notification Details.
5. Click Save.



Purge Policy

Purge Duration (in Months)

Workflow Requests:*
10

Audit Logs:*
10

Notification History:*
10

Notification Details

Tenant Admin

Email List

Save Cancel

Figure 96b: Update Policy Configuration

6. Policy saves successfully message is displayed as seen below.

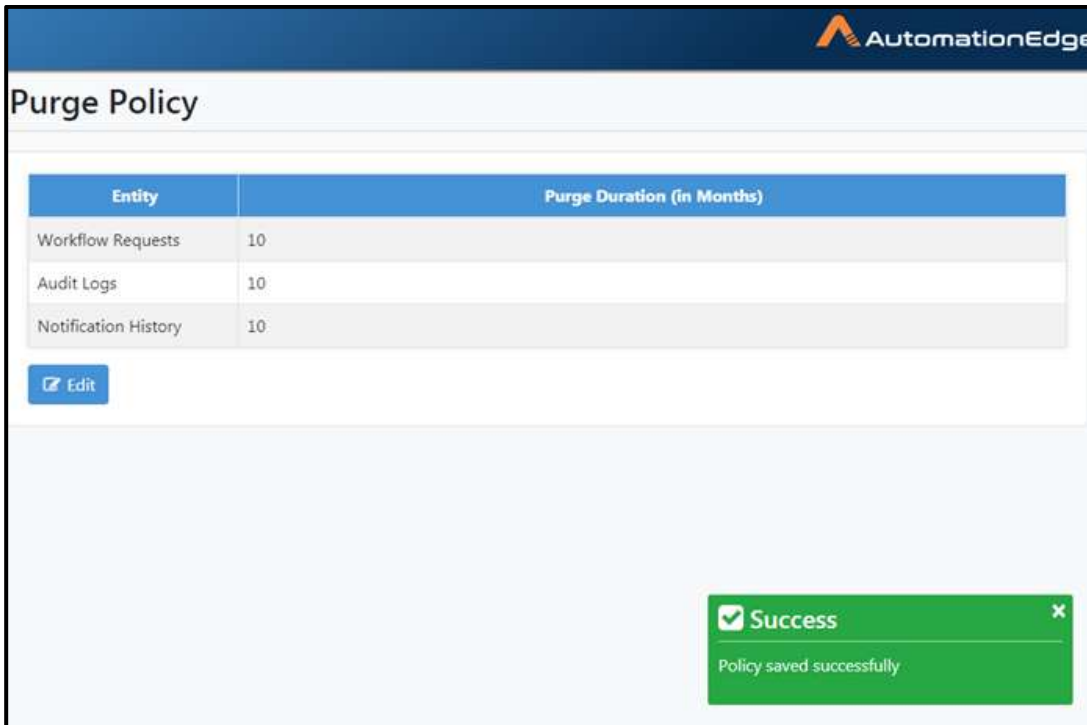


Figure 96c: Purge Policy Saved Successfully

13.2 Purge Schedule

Several options and flexibility in setting up Purge Schedule have been provided based on,

- Day of a month
- Day of a week (First, Second, Third, Fourth or Last)

Note:

- Purge schedule is executed a minimum after 7 days from current date.
- First execution of the Schedule will happen from the next month, if the days between now and next trigger is less than or equal to Seven days for the current month.
- In case if server is down on the day the schedule is to be triggered then schedule will execute the next day at the same time.

Following are the steps to view a Purge Schedule,

1. Navigate to Purging→Purge Schedule menu.

2. Purge Schedule set by the System Administrator. Tenant Administrator can only view the Purge Schedule as seen below.

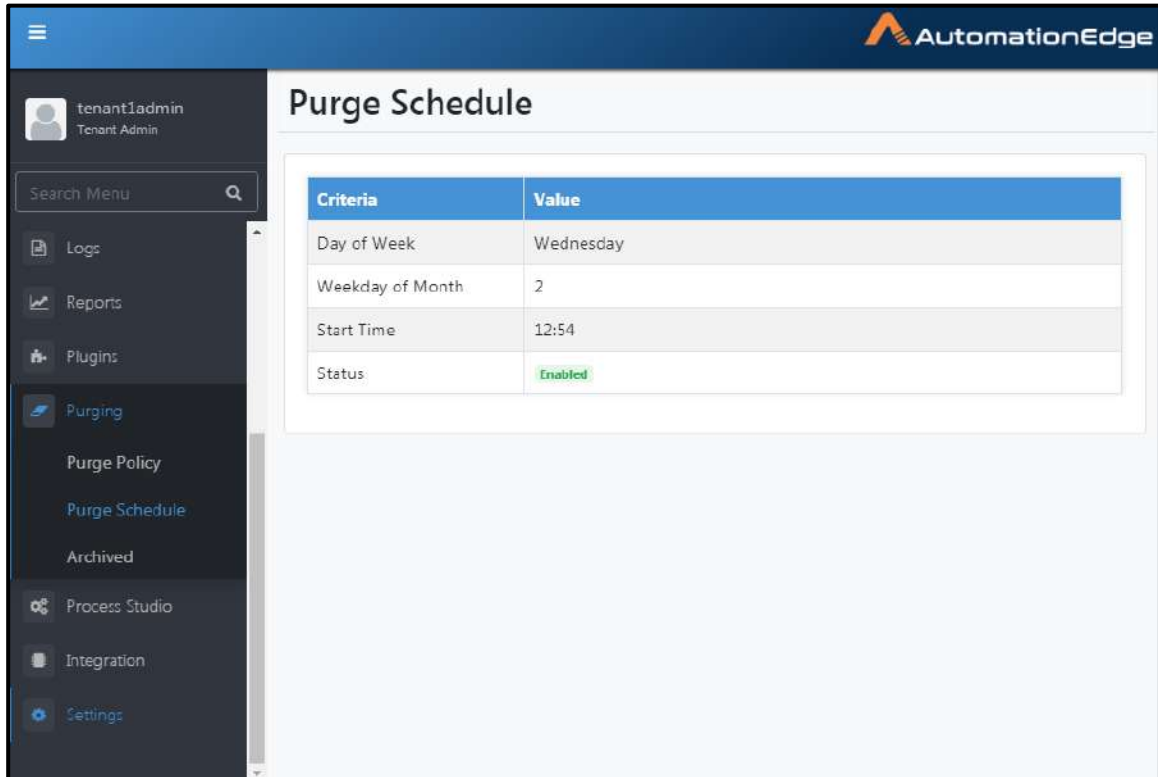


Figure 96d: View Purge Schedule

13.3 Archived

All the purged records are archived and exported to CSV files. Purged data is stored in csv files in batches of 10000 records.

Options are provided to download the archived files from AEUI or from purging target directory. Archives menu lists Archives and are also available for download. Archives are visible and available for download only once a Purge Schedule has executed. If multiple files are created for a purge job, those many entries are shown for downloading, for a purge job. This also applies to the Purging Target to fetch Archived records.

Both these options are discussed in the following sections.

13.3.1 Archives from AE UI

Following are the steps to view and download Archives from AE UI,

1. Navigate to Purging→Archives menu.

2. Archives are available once at least one Purge Schedule has been executed. To begin with there are no Archives.

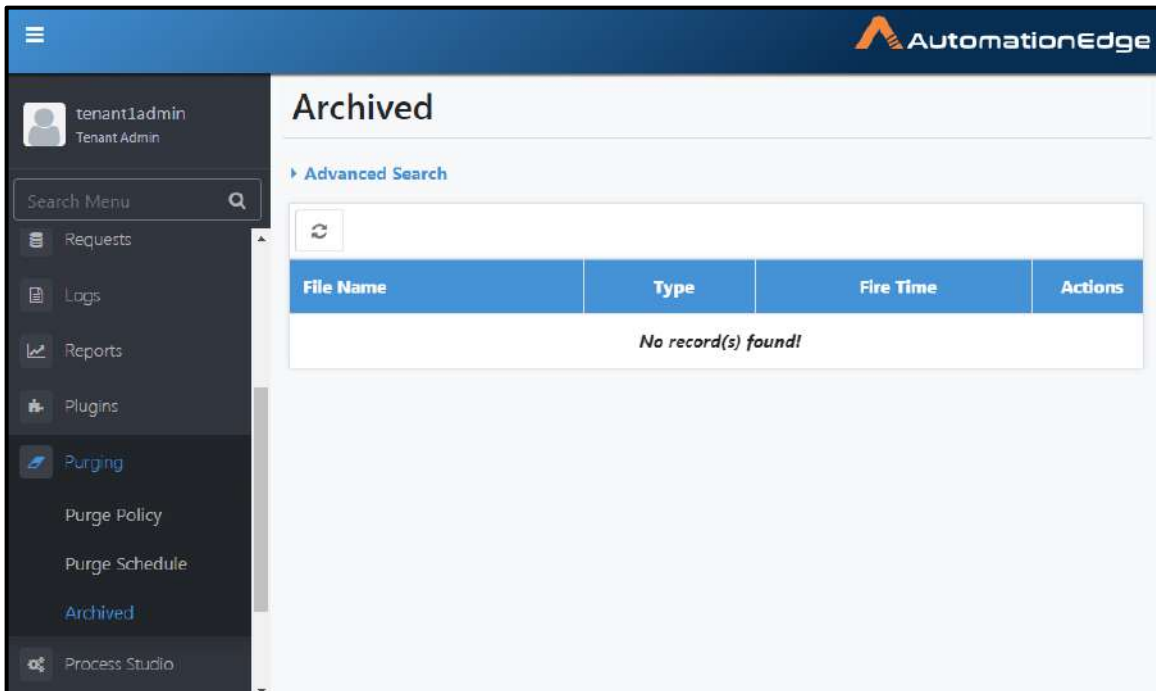


Figure 96e: View Archives

3. The following screen shows available Archives filtered by setting Advanced Search criteria. Purge Schedules is seen in the Fire Time column below.
4. Archives can be downloaded by clicking on any link of the File Name as seen below.
5. Archives can be deleted by clicking the delete icon (🗑️) in the Actions column.

The screenshot shows the AutomationEdge 'Archived' page. At the top, there is a search bar with 'Type = WORKFLOW_INSTANCE' selected. Below the search bar is a table with the following columns: File Name, Type, Fire Time, and Actions. The table contains six rows of workflow request archives, each with a delete icon in the Actions column. The footer of the table indicates 'Page 1 of 1 (Total 6 Record(s))' and a 'Page Size' dropdown set to 10.

File Name	Type	Fire Time	Actions
Workflow_Request_2020-7-08_1.csv.zip	WORKFLOW_INSTANCE	8-Jul-2020	🗑️
Workflow_Request_2020-6-10_1.csv.zip	WORKFLOW_INSTANCE	10-Jun-2020	🗑️
Workflow_Request_2020-5-13_1.csv.zip	WORKFLOW_INSTANCE	13-May-2020	🗑️
Workflow_Request_2020-3-11_1.csv.zip	WORKFLOW_INSTANCE	11-Mar-2020	🗑️
Workflow_Request_2020-2-12_1.csv.zip	WORKFLOW_INSTANCE	12-Feb-2020	🗑️
Workflow_Request_2020-1-08_1.csv.zip	WORKFLOW_INSTANCE	8-Jan-2020	🗑️

Figure 96f: Filter Archives

6. This completes the description of Purging menu option.

13.3.2 Archives from Purging Target

- In addition, archived CSV files are stored as zipped csv files in the default location, AE Home\Archives.
- However, the default purging destination is configurable. It can be set in AE_Home/conf/ae.properties by setting the following configuration parameter, `ae.archive.location = <Desired filepath(e.g D:/testPurge/Archives)>`
- Tenant folders are created in the purging destination.
- The Zips files include purging data of all the three entities (Workflow Requests, Audit Logs Notification History)

14 Process Studio

14.1 Process Studio: Download

Download button(/dropdown) on Process Studio menu, is used for downloading Process Studio for: i) Windows or ii) Linux.

Prerequisites:

- Process Studio zip is available for download only if the System Administrator has uploaded it on AutomationEdge server, through Artifacts menu (Refer, Artifacts in AutomationEdge_R7.0.0_System_Administrator_Guide),
- Process Studio license is assigned to the user. (Refer, Process Studio: Assign Licence in AutomationEdge_R7.0.0_User_Guide).

Following are the steps to download Process Studio,

1. Navigate to the Process Studio menu.
2. Click Download button or the option in the dropdown next to the Download button to download Process Studio for the required OS.
 - Click on the Download button to download Process Studio for the Browsers' machine OS
 - Click the dropdown next to the button to download Process Studio for the other OS
3. The screen shot below is for AutomationEdge UI opened in a browser on a Windows machine.

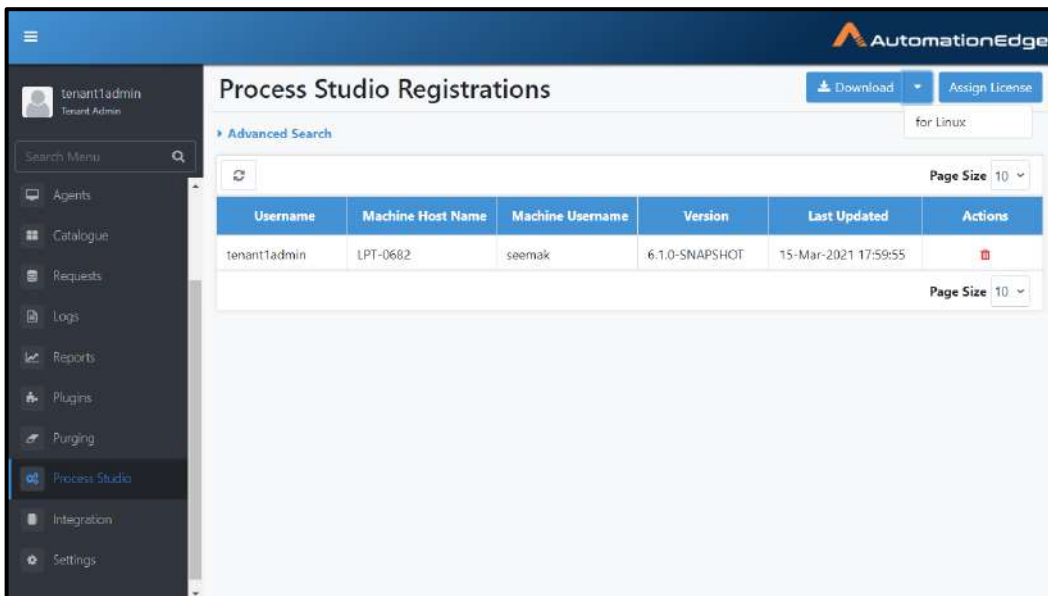


Figure 97a: Download Process Studio

4. The Process Studio folder downloaded, is suffixed with Tenant Organization Code (org code) of the user who downloaded it (e.g. Process-Studio-Tenant1.zip when org code is TENANT1).



The downloaded Process Studio is bundled with Java for the corresponding OS. It is recommended to use the bundled Java as it is automatically updated when Process Studio is auto-updated the next time.

14.2 Process Studio: Assign License

Before an AutomationEdge user can register a process studio instance, Tenant Administrator must assign Process Studio license to the user. The total number of AE users that can be assigned license is determined by the number of Process Studios allowed in the license.

Following are the steps to assign a Process Studio licence to an AutomationEdge user,

1. Navigate to Process Studio menu.
2. Click Assign License button on the top right corner.

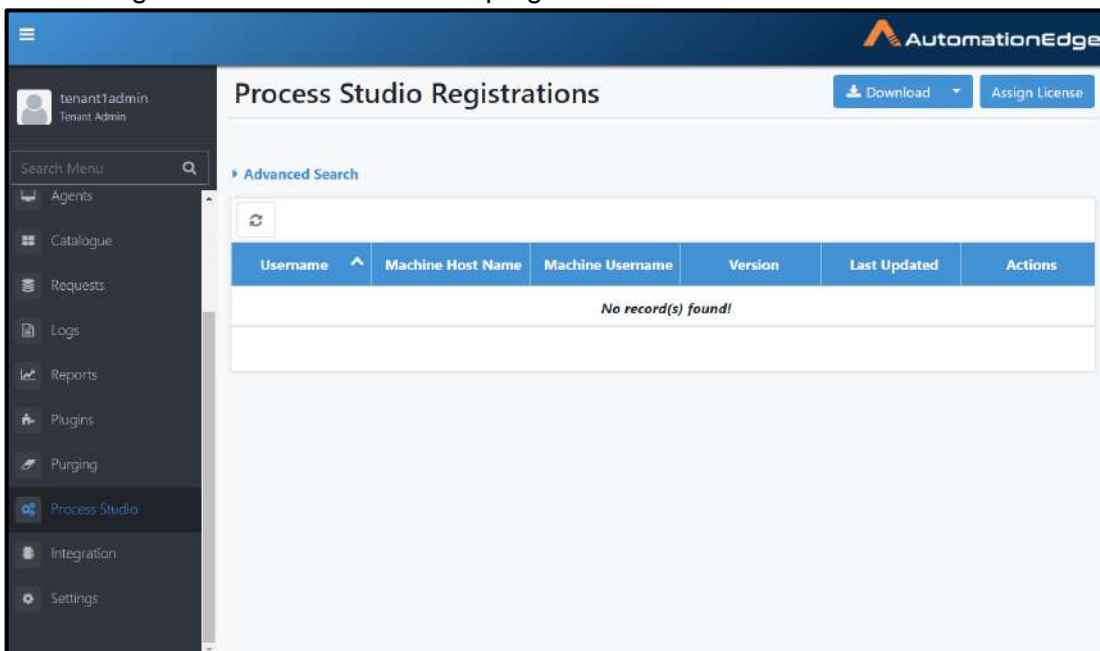


Figure 97b: Assign Process Studio License

3. Assign one or more licences to Tennat Users by enabling checkbox next to the username. Click save.

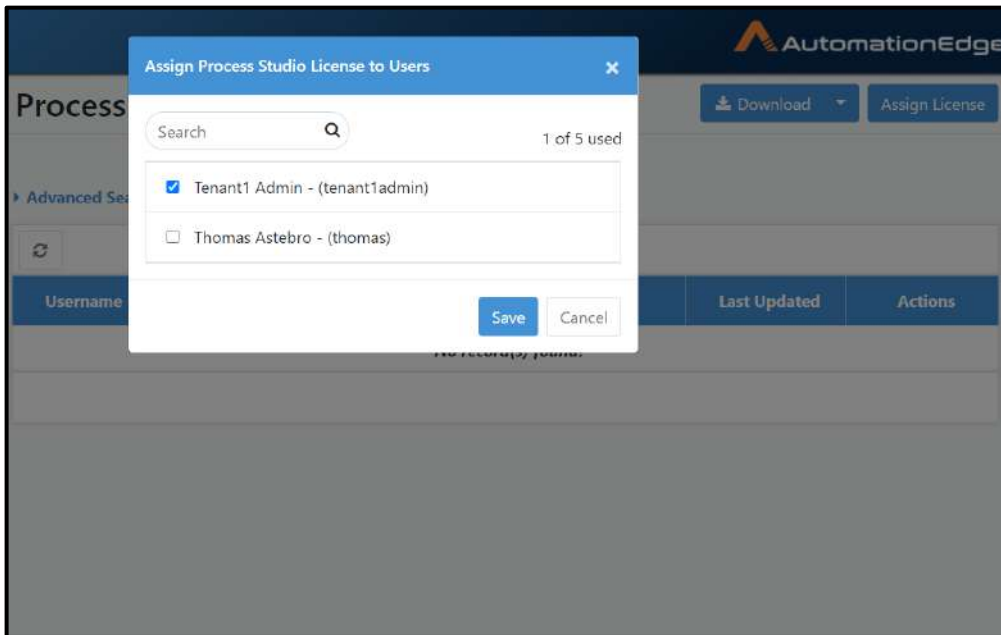


Figure 97c: Assign Process Studio License

4. License is now assigned user tenant1admin.

14.3 Process Studio Registration

Following are the steps for Process Studio registration.

1. Users can register an instance of process studio by connecting to AutomationEdge. An instance of Process Studio is registered to AutomationEdge with AE username, Machine hostname and Machine username. The details of the registered instance are then visible in this list. For now there are still no entries in the list as seen below.

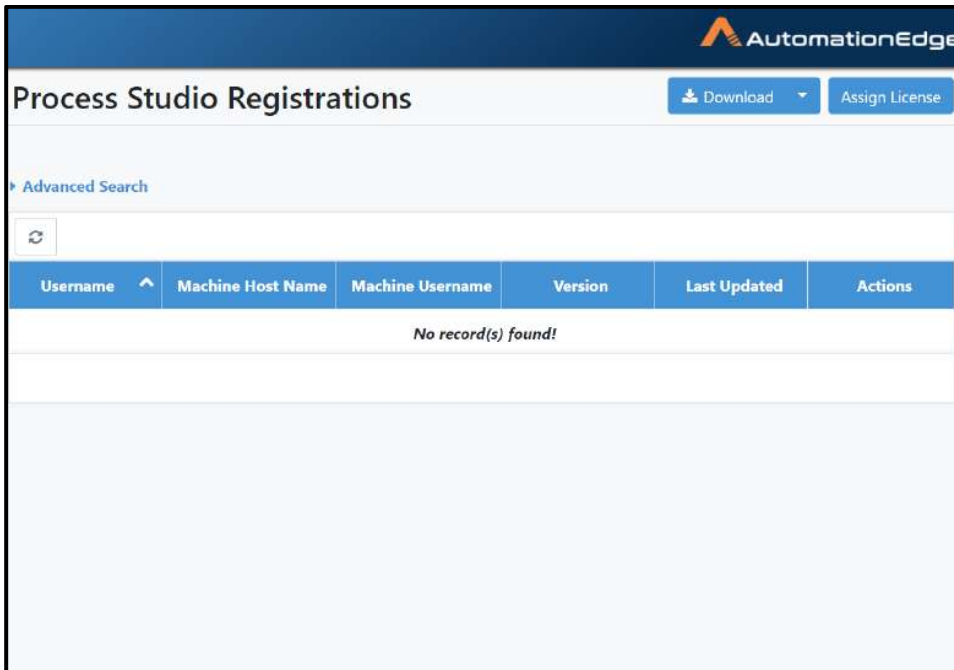


Figure 97d: Process Studio Registrations visible after user connects with PS

2. Start Process Studio application and connect to AutomationEdge. Provide connection details. Click Connect.
3. When a fresh instance of Process Studio connects to AutomationEdge it registers the Process Studio instance with AutomationEdge. There is a validation to check if the user has been already granted Process Studio license. The registration is made with AE username, Machine hostname and Machine username.

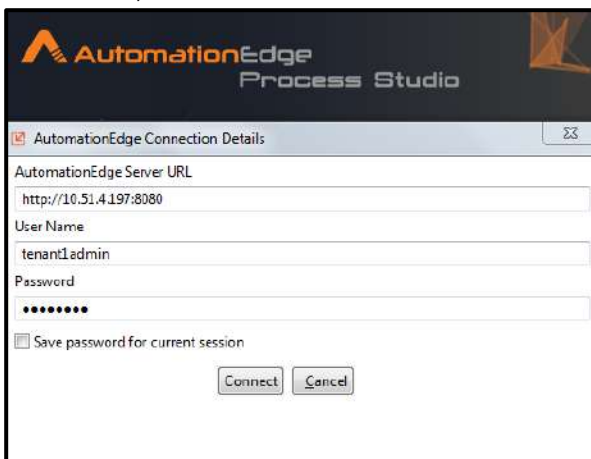
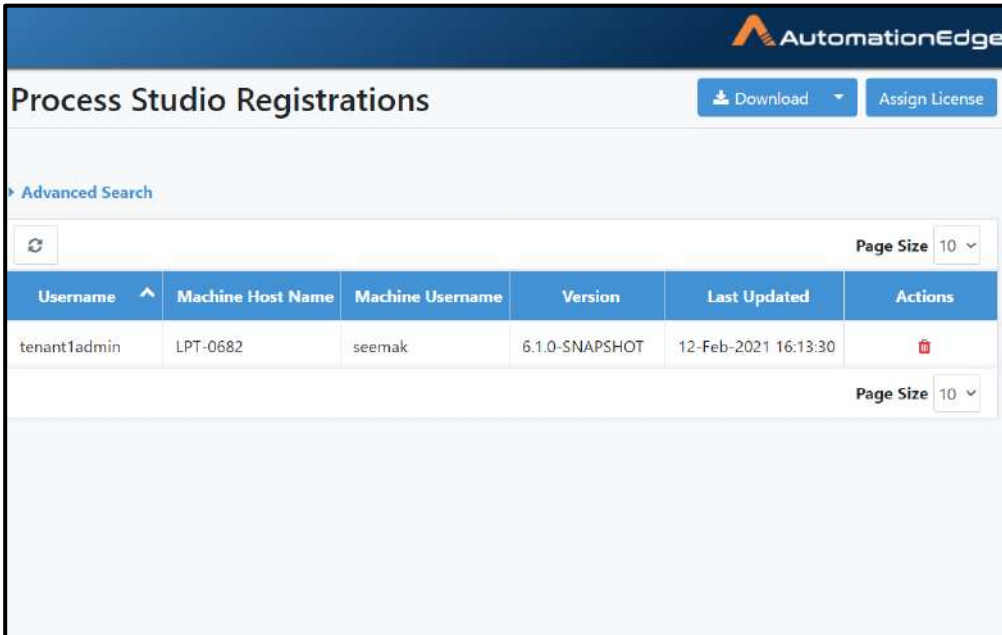


Figure 97e: Connect Process Studio

4. The Process Studio Registered appears in the list as seen below.




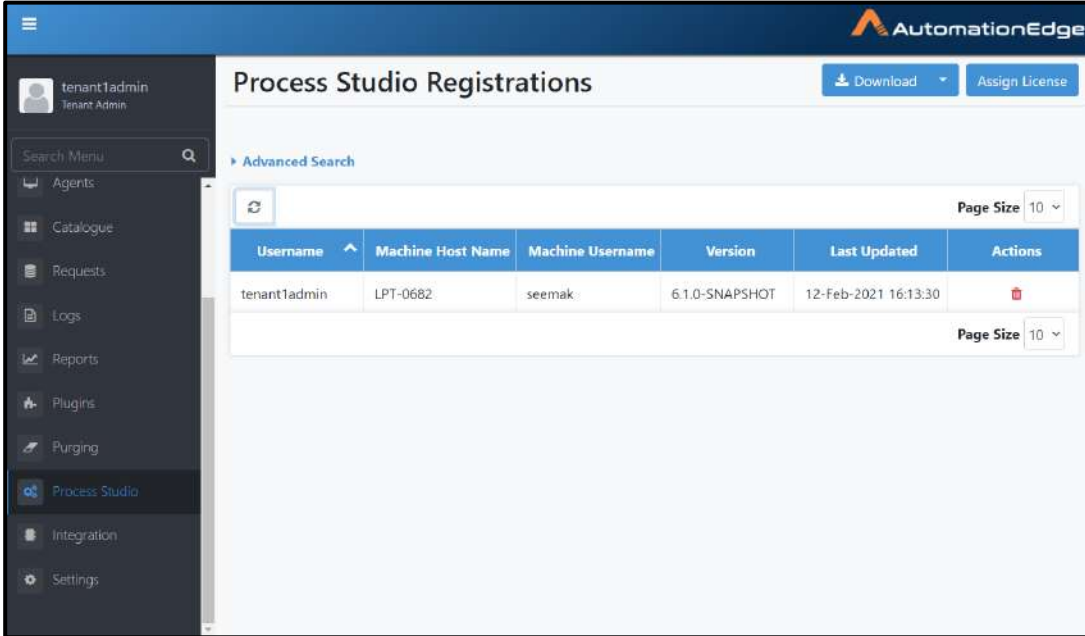
Username	Machine Host Name	Machine Username	Version	Last Updated	Actions
tenant1admin	LPT-0682	seemak	6.1.0-SNAPSHOT	12-Feb-2021 16:13:30	

Figure 97f: Process Studio registration for tenant1admin

14.4 Process Studio Registrations: View

When a connection is made from Process Studio to AutomationEdge for the first time, that instance of Process Studio is registered with AutomationEdge. This registration and all other registrations are visible as a list on this page.

1. Navigate to Process Studio menu.
2. You can see the Process Studio Registrations by AE username, machine hostname and machine username.




Username	Machine Host Name	Machine Username	Version	Last Updated	Actions
tenant1admin	LPT-0682	seemak	6.1.0-SNAPSHOT	12-Feb-2021 16:13:30	

Figure 97g: Process Studio assigned licenses

14.5 Process Studio Registration: Delete

You can delete Process Studio registration in the following two ways,

1. Deregister from Process Studio
 - ✓ Deregister during login or
 - ✓ Deregister from Process Studio Toolbar
 To deregister from Process Studio, refer
AutomationEdge_R7.0.0_ProcessStudio_User_Guide
2. Delete Registration from AutomationEdge UI followed by
 - ✓ Login from the Process Studio instance that was de-registered to release the license immediately.
 - ✓ Else, all the licenses, for PS registrations marked for deletion are automatically released the next day.

14.5.1 Deregister from AutomationEdge UI

Process Studio registration can be deleted by clicking the delete icon (🗑️) in the Actions column. However, once the registration is marked for deletion from server, user has to make a login call again from the deleted Process Studio to actually release the license. Else, all the licenses for PS registrations which were marked for deletion will be released in the daily nightly job by Server.

Following, are the steps to delete a Process Studio registration,

1. Click delete icon (🗑️) in the Actions column.
2. Acknowledge the pop up to delete the registration.

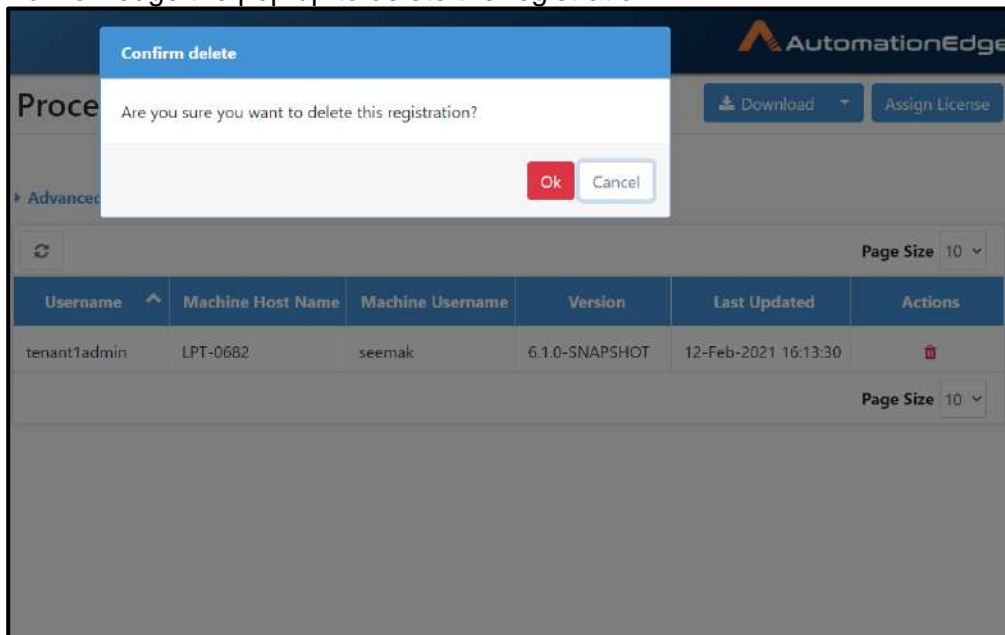


Figure 97h: Delete Process Studio License Assignment

- The Process Studio registration with AutomationEdge is deleted and removed from this list

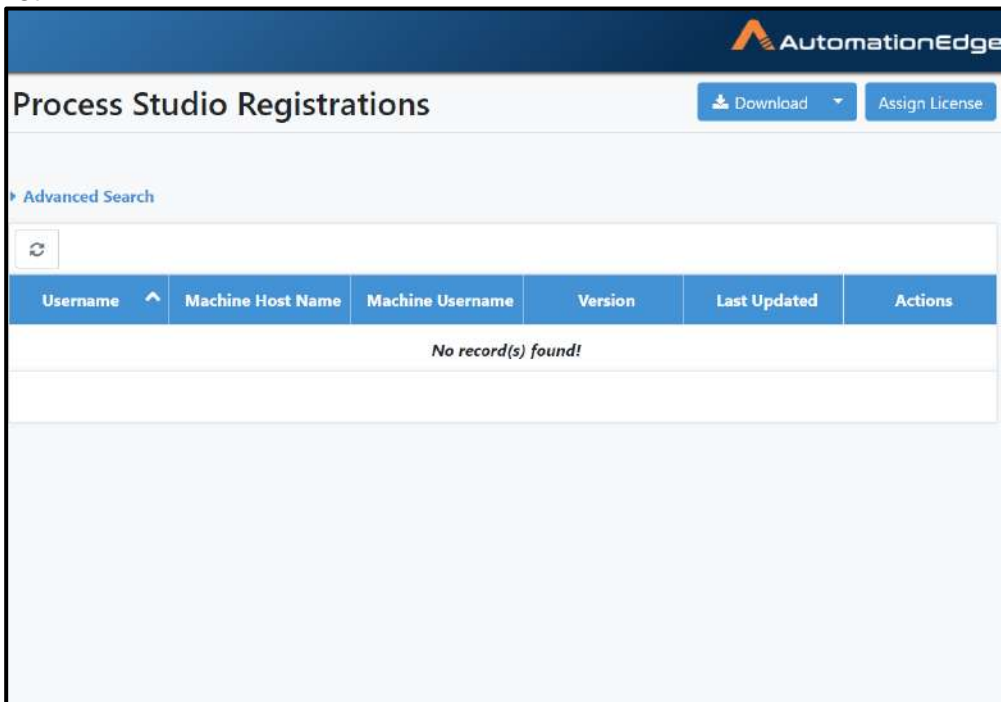


Figure 97i: Process Studio registration deleted

15 Integration

Integration menu and its sub-menus are visible if Integration Service is enabled for the logged in Tenant Administrator's Tenant.

1. Locate and navigate to the Integration menu.
2. The integration menu expands as seen below.
3. The Services and Types menu are same as those of System Administrator. Type Configuration menu is only available to Tenant Administrators.
4. Each of the Integration sub menus are discussed below.

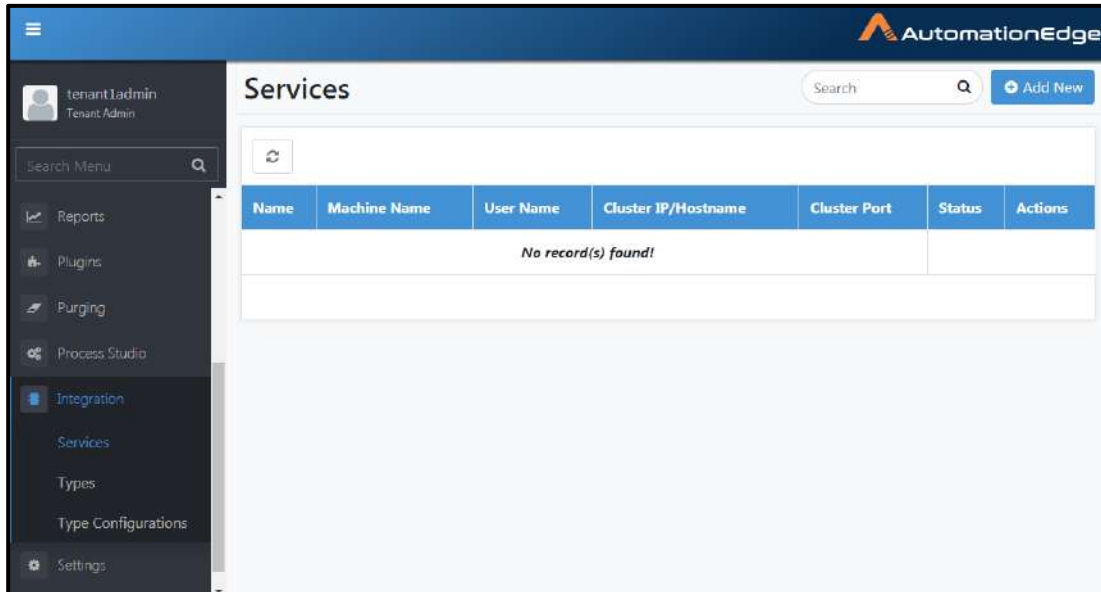


Figure 98a: Integration menu

15.1 Integration: Services

The steps to Add Integration Service, Download Integration Configuration file, edit and delete Integration Service are the same as System Administrator. A Tenant Administrator can use Integration Services added by a System Administrator. However, it can also create only one Integration Service.

Refer to AutomationEdge_R7.0.0_System_Administrator_Guide for details on how to use this menu option to configure an Integration Service.

15.2 Integration: Types

Integration type is a component (JAR file) used to connect to a third-party system and poll for Automation Requests.

The steps to Add, Edit and Delete Integration Types are the same as System Administrator. A Tenant Administrator can also use the Types configured by a System Administrator. Refer AutomationEdge_R7.0.0_System_Administrator_Guide for details on how to use this menu option to configure Integration Types.

Integration type Remedyforce (remedyforce-rest.jar) is released with R7.0.0.

Refer [Appendix 1: Integration with Type Remedyforce-](#) for steps to use Integration Services to integrate with Remedyforce.

15.3 Integration: Type Configuration

Integration Type configuration is an instance of integration type that is configured for a tenant to communicate with one third-party service. Integration Type menu option is only available to Tenant Administrators.

The following sections discuss the operations for Integration Type configuration.

15.3.1 Integration Type Configuration: Add

1. Navigate to Integration→Type Configuration

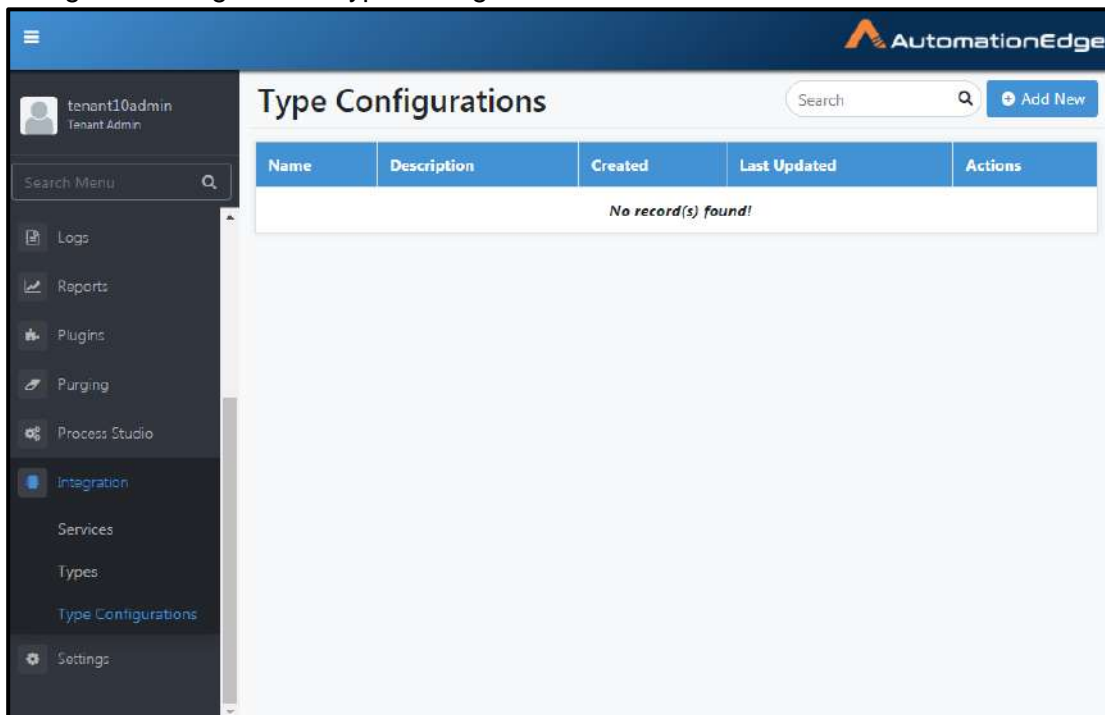


Figure 98b: Add New Integration Type Configuration

2. Provide desired configuration details.

3. Expand Polling Schedule.

New Configuration

Name:*
Remedyforce Service Requests

Description:*
AutomationEdge Integration Instance for Remedyforce Service Requests

Types:*
Remedyforce

Services:*
AutomationEdge Integration Services

Update Response via Service

▶ Polling Schedule

▶ Configuration Parameters

Test Submit Cancel

Figure 98c: Configuration Details

4. The Polling Schedule configuration section is visible as below.

▼ Polling Schedule

Time Zone: *
Asia/Calcutta

Run Schedule Infinitely

Start Date: * End Date: *
[] []

Repeat Every *
[] Hours []

Start Hour * End Hour *
HH : MM HH : MM

▶ Configuration Parameters

Test Submit Cancel

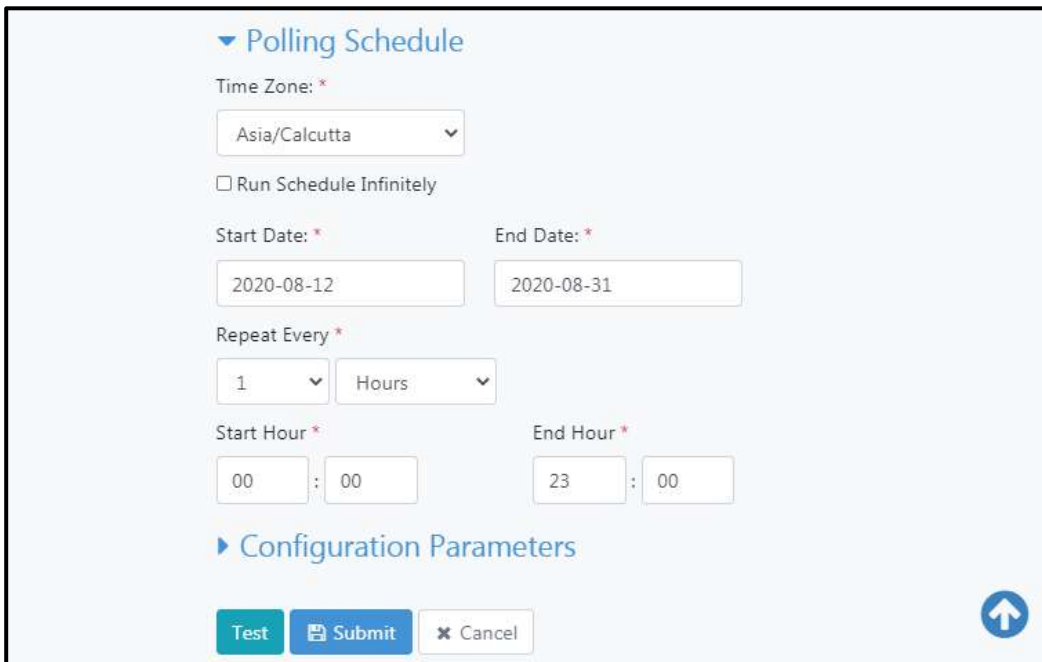
Figure 98d: Polling Schedule form

5. Provide desired Polling Schedule as seen below.

Note: Polling schedule is saved and runs in the default time zone of the machine on which Integration service is deployed and running. Other Time Zones support will be added in future.

Repeat interval values can be from the following,

- Hours: 1 to 23
- Minutes: 1, 2, 3, 4, 5, 10, 15, 20, 30, 45
- Seconds: 30

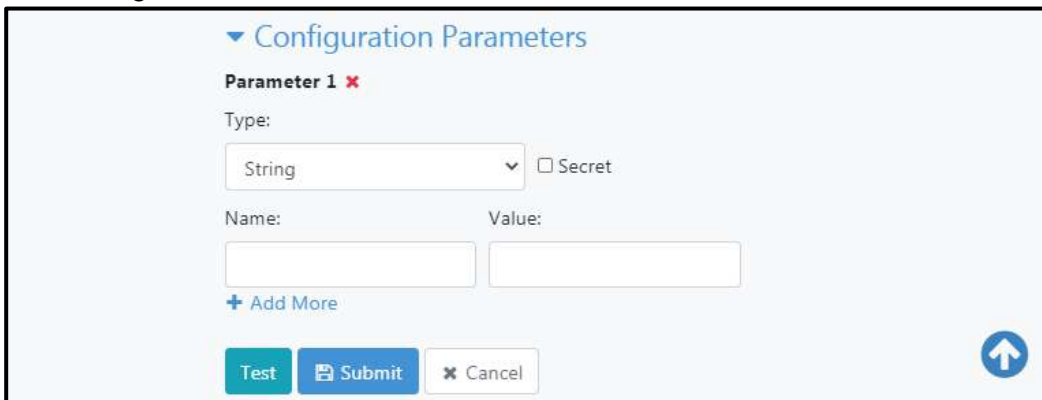


The screenshot shows the 'Polling Schedule' configuration form. It includes a dropdown for 'Time Zone' set to 'Asia/Calcutta', a checkbox for 'Run Schedule Infinitely', 'Start Date' (2020-08-12) and 'End Date' (2020-08-31) fields, 'Repeat Every' set to '1' 'Hours', 'Start Hour' (00) and 'End Hour' (23) fields, and a 'Configuration Parameters' section. At the bottom are 'Test', 'Submit', and 'Cancel' buttons, and an upward arrow icon.

Figure 98e: Polling Schedule details

6. Expand Configuration Parameters section.

7. The Configuration Parameters section is visible as below.



The screenshot shows the 'Configuration Parameters' form. It features a 'Parameter 1' section with a 'Type' dropdown set to 'String' and a 'Secret' checkbox. Below are 'Name' and 'Value' input fields, an '+ Add More' link, and 'Test', 'Submit', and 'Cancel' buttons. An upward arrow icon is in the bottom right corner.

Figure 98f: Configuration parameters form

8. Provide desired Configuration Parameters values.
9. Refer [Appendix 1: Integration with Type Remedyforce](#) for Configuration Parameters required by Remedyforce.

Configuration Parameters

Parameter 1 ✖

Type:

String Secret

Name: Value:

Result Success

[+ Add More](#)

Test Submit Cancel

Figure 98g: Configuration Parameters

10. If you have provided the correct parameters for connectivity to the Integration Type chosen here, you may click Test Connection button to test connectivity. Click Submit button.
11. Integration Type Configuration created successfully message appears.

AutomationEdge

Type Configurations

Search [Add New](#)

Name	Description	Created	Last Updated	Actions
Remedyforce Service Requests	Automationedge Integration Instance for Remedyforce Service Requests	12-Aug-2020 17:20:26	12-Aug-2020 17:20:26	Edit Delete

Success ✖

Integration configuration [Remedyforce Service Requests] created

Figure 98h: Integration Type saved successfully

12. In case of a duplicate Service name an error message is displayed as below.



Figure 98i: Duplicate Integration Type error message

15.3.2 Integration Type Configuration: Edit

1. Navigate to Integration→Type Configuration
2. Click Edit icon in the Actions column for the Type Configuration.

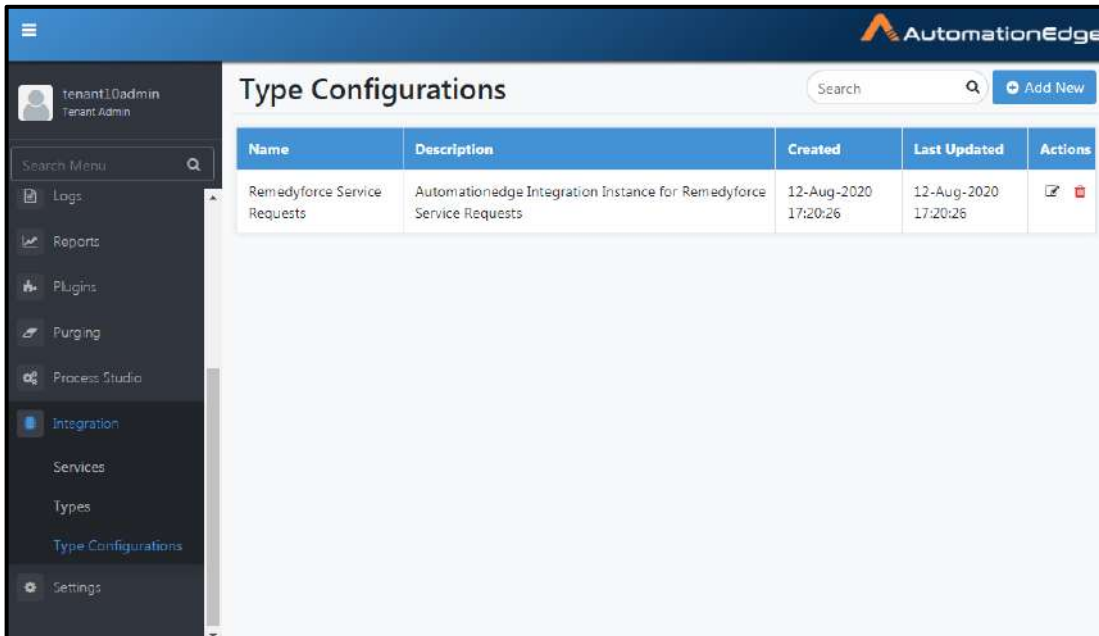
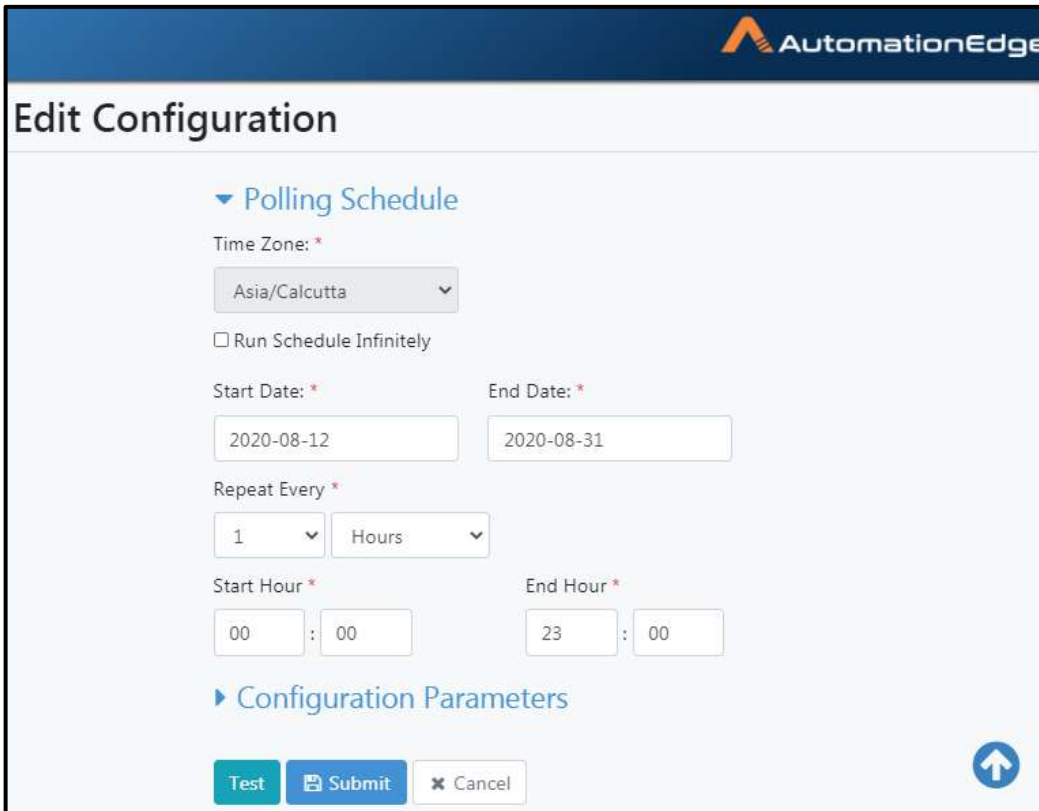


Figure 98j: Edit Integration Type

3. You can make changes in the Poling Schedule or Configuration parameters.



Edit Configuration

AutomationEdge

▼ Polling Schedule

Time Zone: *
Asia/Calcutta ▼

Run Schedule Infinitely

Start Date: * 2020-08-12 End Date: * 2020-08-31

Repeat Every *
1 ▼ Hours ▼

Start Hour * 00 : 00 End Hour * 23 : 00

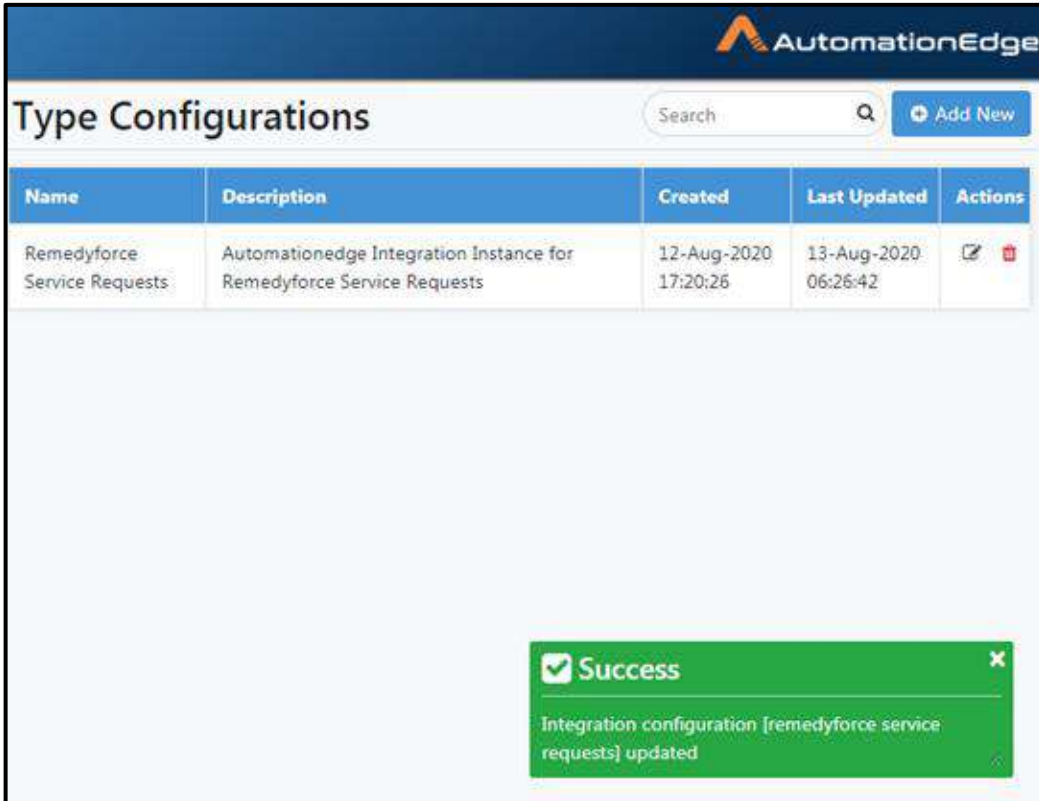
► Configuration Parameters

Test Submit Cancel



↑

Figure 98k: Update parameters

4. Integration Type Configuration updated successfully message appears.



The screenshot displays the 'Type Configurations' interface in the AutomationEdge application. At the top, there is a search bar and an 'Add New' button. Below this is a table with the following data:

Name	Description	Created	Last Updated	Actions
Remedyforce Service Requests	Automationedge Integration Instance for Remedyforce Service Requests	12-Aug-2020 17:20:26	13-Aug-2020 06:26:42	 

A green success message box is overlaid on the bottom right of the table, containing the text: 'Success' with a checkmark icon, and 'Integration configuration [remedyforce service requests] updated' with a close button (X) in the top right corner.

Figure 98I: Integration Type Updated successfully

15.3.3 Integration Type Configuration: Delete

1. Navigate to Integration→Type Configuration
2. Click Delete icon in the Actions column for the Type Configuration.

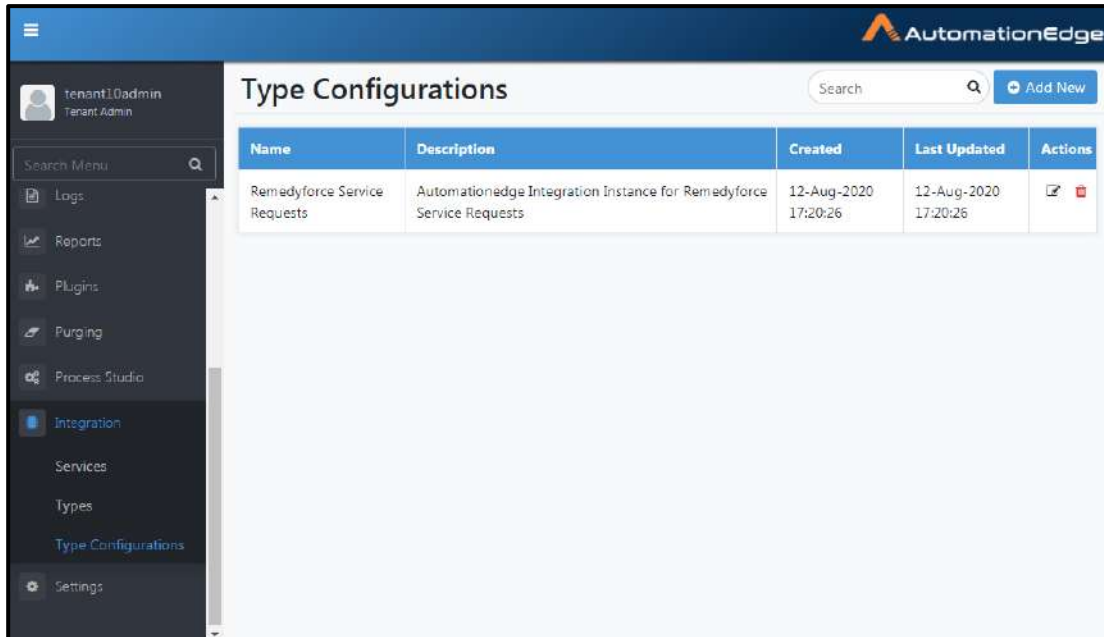


Figure 98m: Delete Integration Type

3. A warning pop up to confirm deletion appears. Click Delete button.

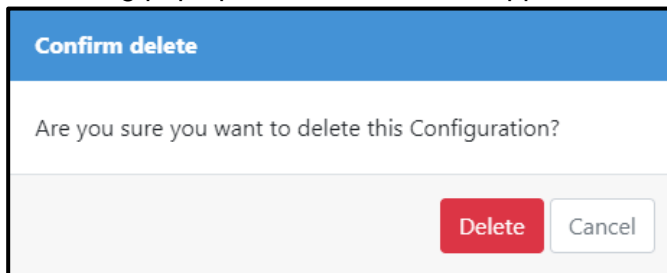


Figure 98n: Confirm Type Configuration deletion

4. Integration Type configuration deleted message appears.

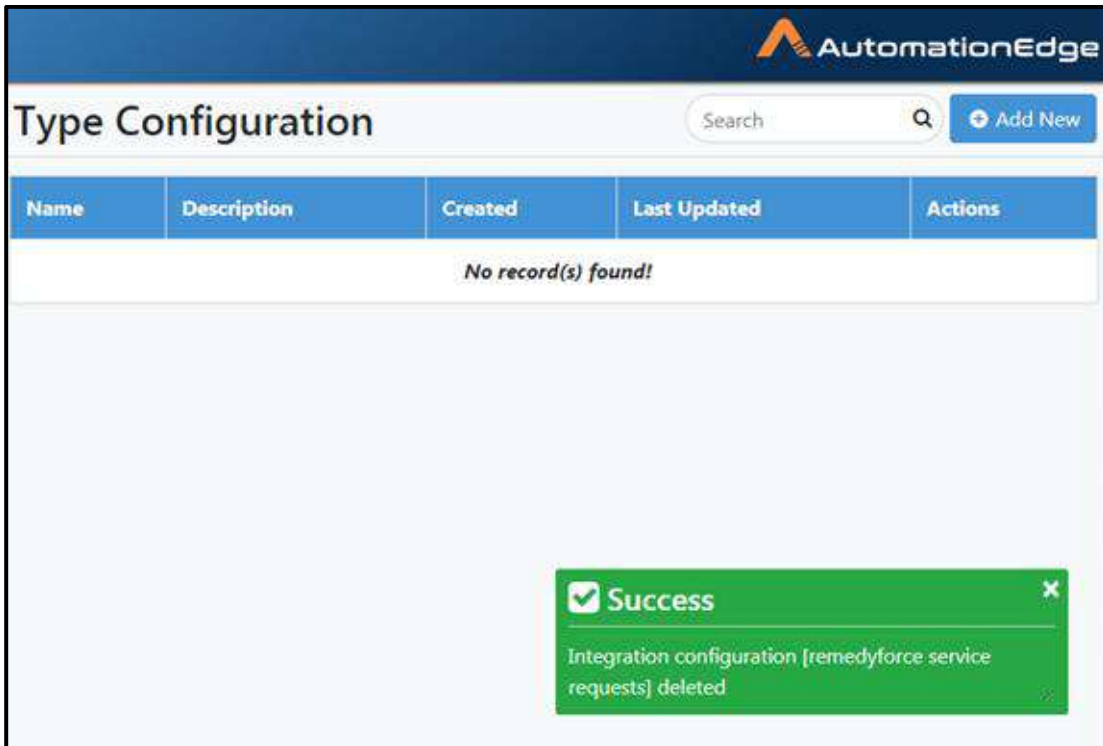


Figure 98o: Integration Type Configuration Type successfully deleted

15.4 Integration Services: Features/Permissions for other users

Table 75: Integration Services Permissions

Feature/Role	Tenant Administrator	Workflow Administrator	User Administrator	Agent Administrator	Tenant User	Activity Monitor
Services Enable/ Add/Edit/ Download/Delete	*✓	-	-	-	-	-
Types	✓	-	-	-	-	-
Type Configurations	✓	-	-	-	-	-

*Tenant Administrators do not have Enable permission. They can use Integration options once enabled by System Administrator

16 File Management

File Management feature and menu option is for ease of uploading and centrally managing related files for AutomationEdge artifacts viz., Plugin, Agent and Process studio. Especially, the main use of this feature is to upload the supporting files that are configurable or constantly changing, from the AutomationEdge UI and provide the files to its components in a seamless way.

File Management artifacts and menu permissions are listed in the table below,

Table: File Management Permissions

Artifact	File Management menu option available to -
i. Agent / Process Studio	Tenant Administrator
ii. Workflows	Tenant Administrator
iii. Plugins	System Administrator

Plugins are uploaded and managed by sysadmin; hence File Management menu for Plugins is accessible to System Administrator. File Management for Plugins is discussed in AutomationEdge_R7.0.0_System_Administrator_Guide. The following section discusses File Management for Workflows and Agents/Process Studio.

16.1 Workflows

File Management menu for Workflow Files manages supporting files for workflows centrally. When a file is uploaded or updated,

- The file automatically downloads onto an Agent.
- The file does not automatically download onto Process Studio.
- Additionally, workflow files can also be downloaded in a preferred target location during workflow execution by an Agent, using the Get Files from Server step.

To upload supporting files for a workflow,

1. On the File Management menu on the Workflows tab, click the Upload button.

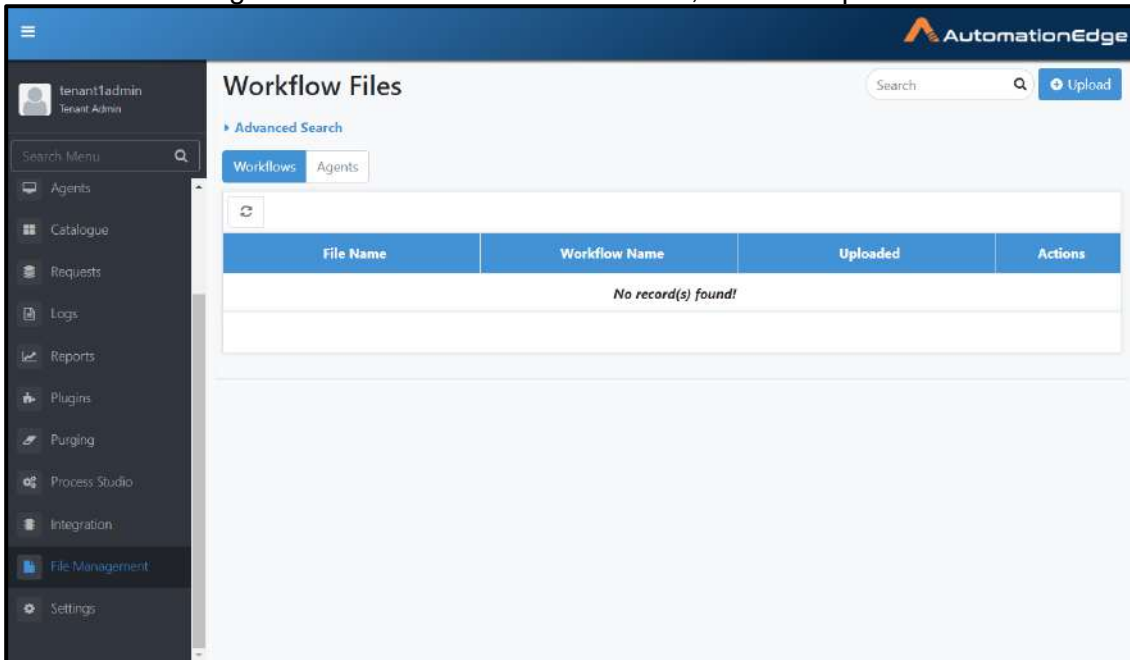
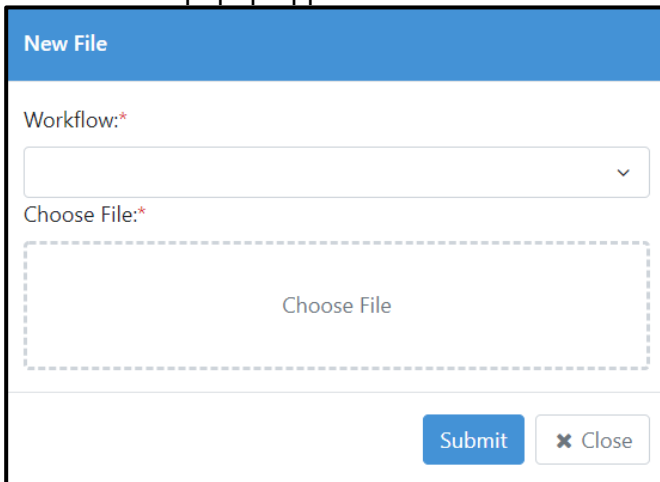


Figure 99a: File Management

2. The New File popup appears. Click the arrow next to the Workflow field.



The 'New File' popup form contains the following fields and controls:

- Workflow:** A dropdown menu with a downward arrow.
- Choose File:** A dashed rectangular box containing the text 'Choose File'.
- Submit:** A blue button.
- Close:** A button with an 'X' icon.

Figure 99b: Upload file for a Workflow

3. A list of workflows appears. Select the workflow for which a file is to be uploaded by enabling the check box next to the workflow, or type a search string to filter workflow names and then enable the checkbox.

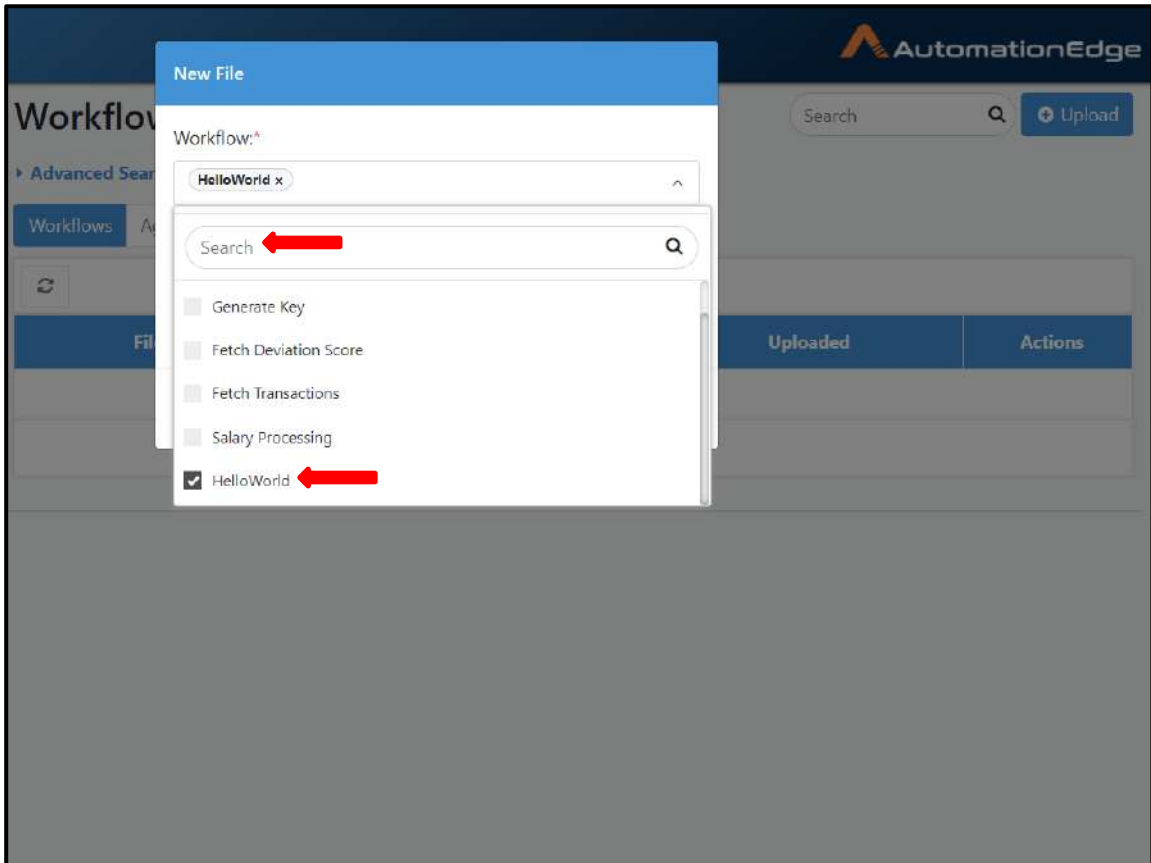


Figure 99c: Select Workflow

4. Click on Choose File box and browse for a file as seen below. Click Submit.

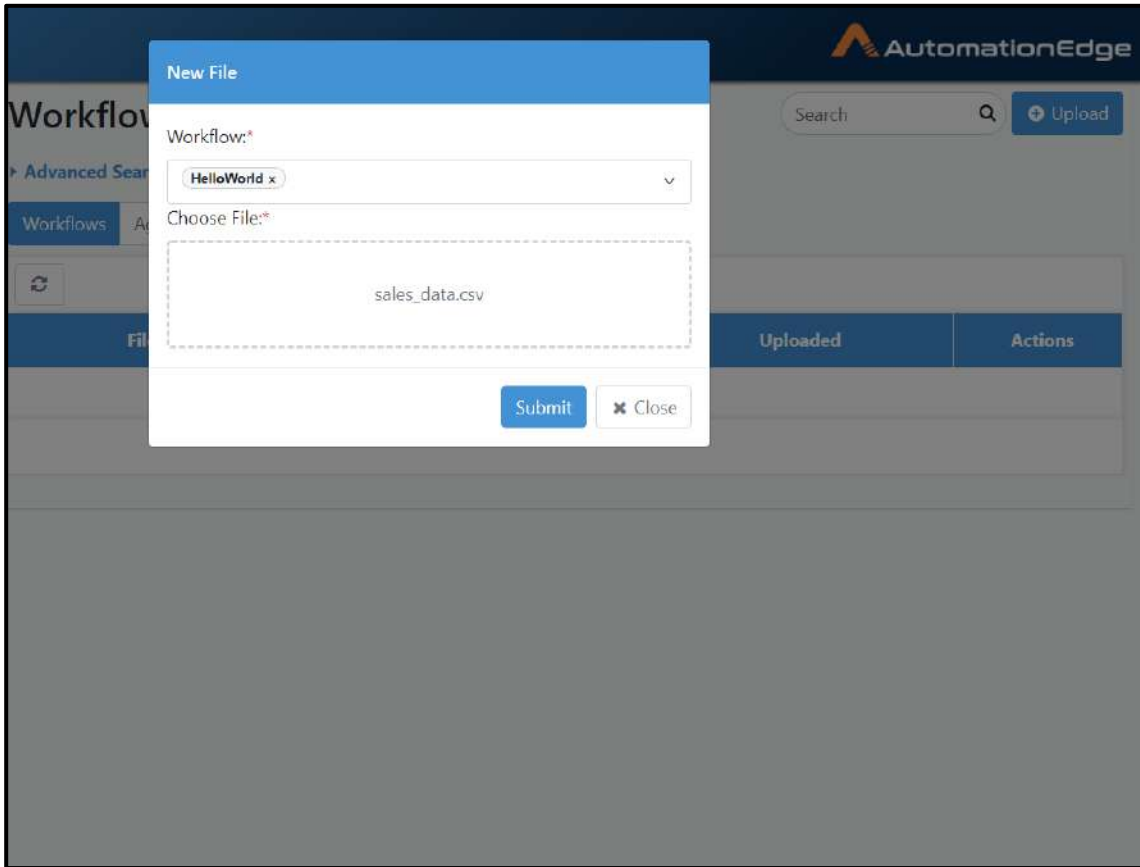


Figure 99d: Choose File to upload

5. A File Uploaded Successfully message appears, and the uploaded file is visible in the Workflow Files list.

16.1.1 View and Actions on supporting Files for a workflow

The File Management menu lists all the supporting files uploaded for workflows.

1. The File Management menu on the Workflows tab shows the list of supporting files uploaded for workflows.
2. The page components are described in the table below.

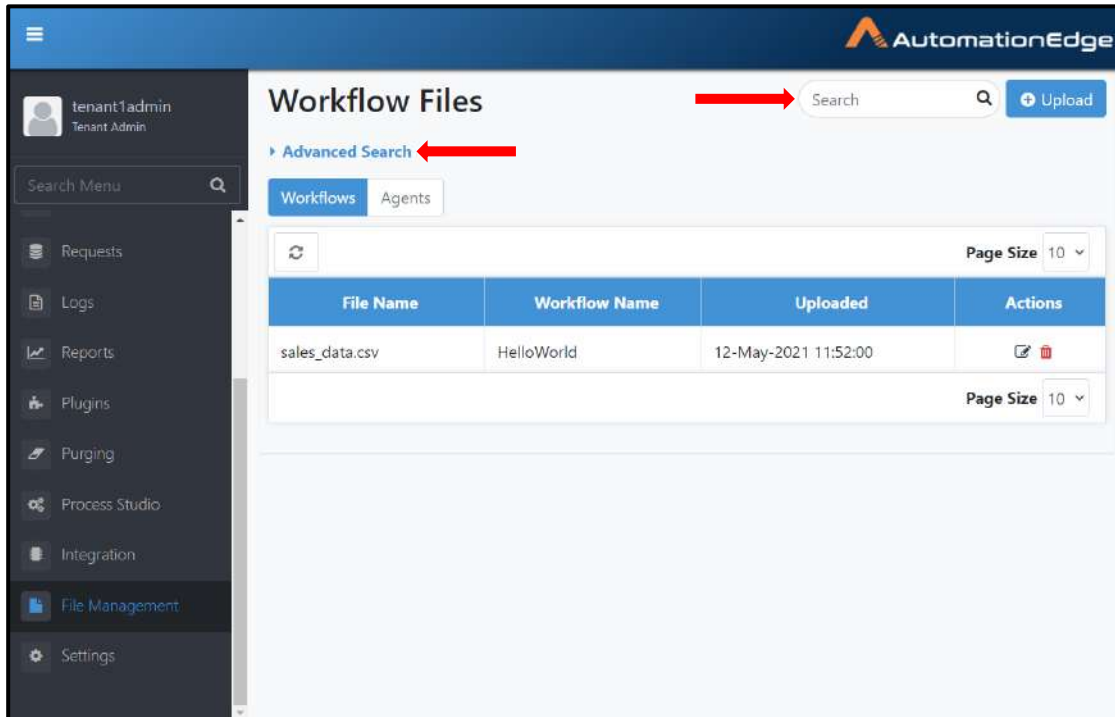


Figure 99e: Search and Advanced Search Options

The table below describes the page components.

Table: Workflow Files View

Column	Description
Search	Enter the Search string to filter the list.
Advanced Search	Expand to enter the advanced search criteria.
File Name	The name of the file uploaded
Workflow Name	The name of the workflow for which the file uploaded
Uploaded	The timestamp of the file was upload
Actions	<ol style="list-style-type: none"> Click the Edit icon (✎) to edit the file uploaded. Click on the Choose File box to browse for an updated version of the same filename. The Workflow field is not editable and cannot be changed. Click the Delete icon (🗑) to delete the file from the AutomationEdge server.

16.2 Agents

File Management menu for Agent Files manages supporting files for Agents centrally. When a file is uploaded or updated,

- The Agent restarts automatically, and the files download onto the Agent.
- The file downloads onto Process Studio upon the synchronization.
- Additionally, Agent files can also be downloaded in a preferred target location during workflow execution by an Agent, using the Get Files from Server step.

16.2.1 Upload supporting File for an Agent

To upload supporting files for an Agent,

1. On the File Management menu on the Agents tab, click the Upload button.

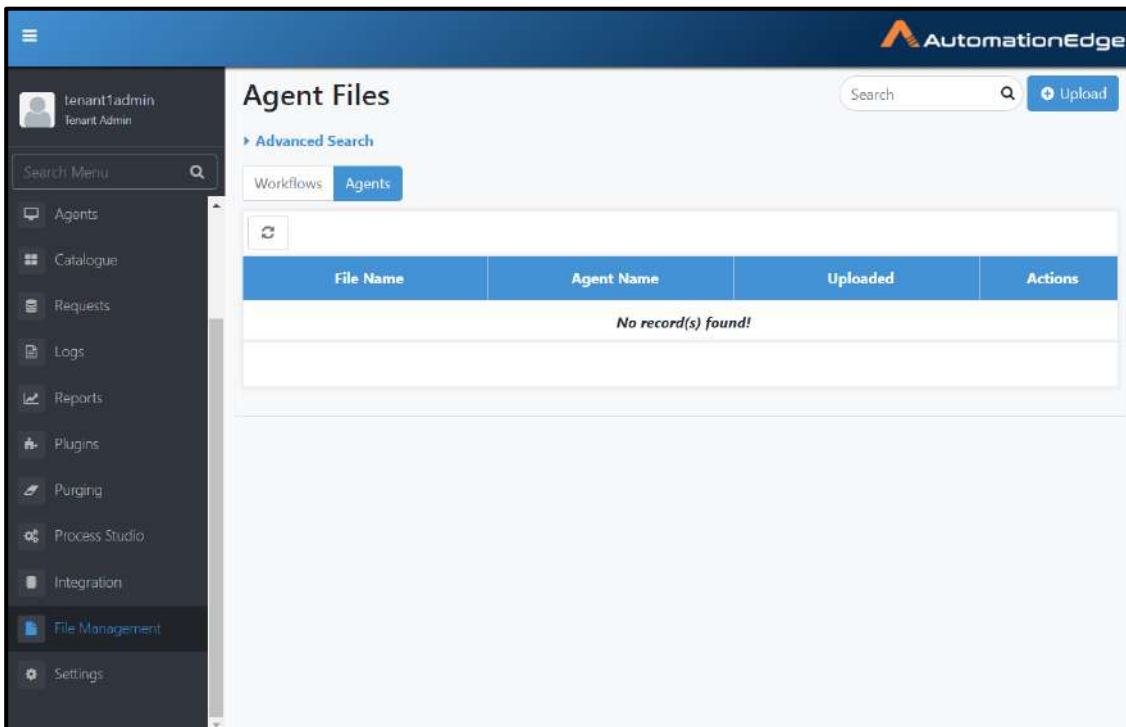
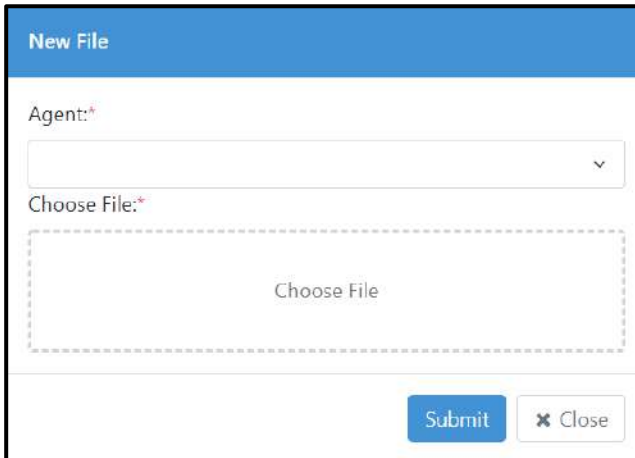


Figure 99f: File Management for Agents

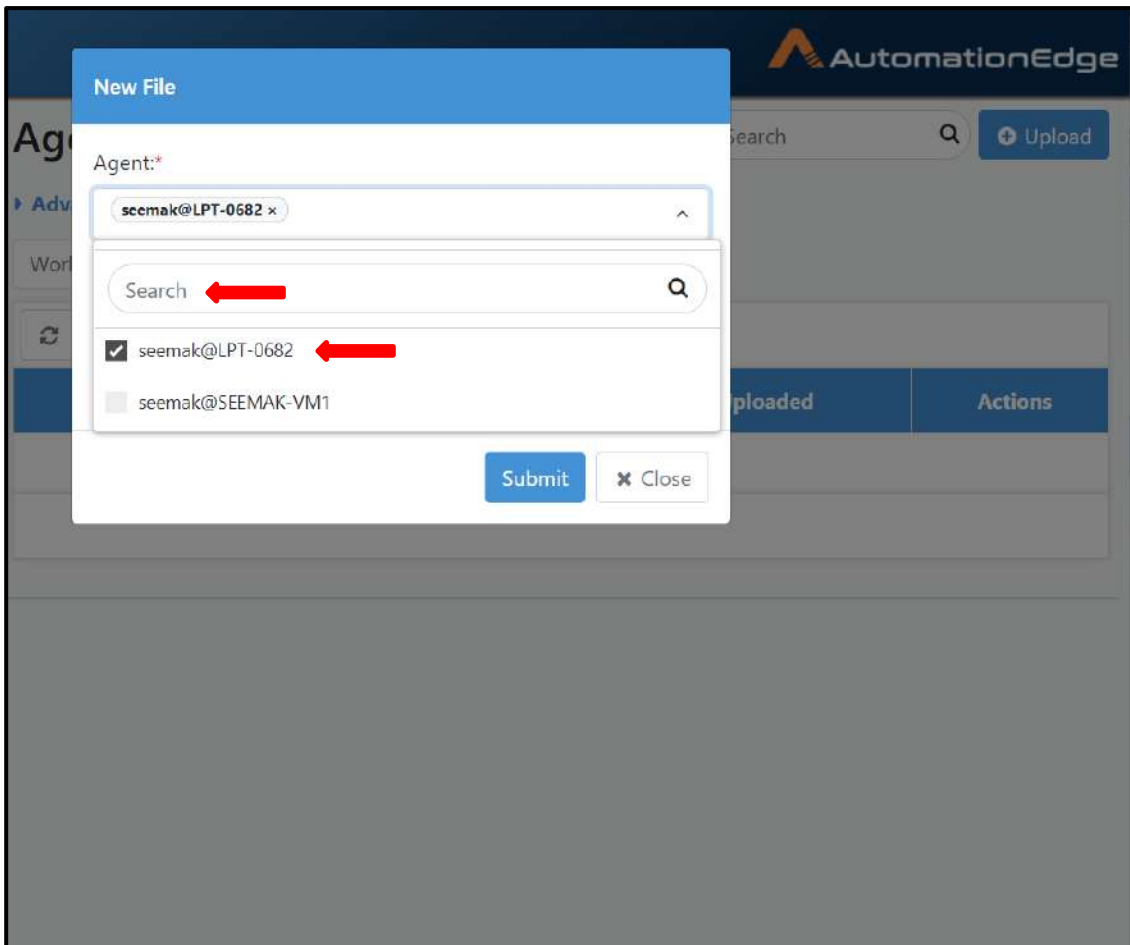
2. The New File popup appears. Click the drop-down arrow on the Agent field to see the list of Agents.



The image shows a 'New File' popup window. At the top, there is a blue header with the text 'New File'. Below the header, there is a label 'Agent:*' followed by a white dropdown menu with a downward arrow. Underneath the dropdown is a label 'Choose File:*' and a dashed rectangular box containing the text 'Choose File'. At the bottom right of the popup, there are two buttons: a blue 'Submit' button and a white 'Close' button with a small 'x' icon.

Figure 99g: Upload Files for Agents

3. Select an Agent to upload supporting files by enabling the check box next to the Agent, or type a search string to filter Agent names and enable the checkbox.



The image shows the 'New File' popup window overlaid on a blurred background of the AutomationEdge interface. The popup has a blue header with 'New File'. Below it, the 'Agent:*' label is followed by a dropdown menu showing 'seemak@LPT-0682 x'. Below the dropdown is a search bar with the text 'Search' and a magnifying glass icon. Underneath the search bar is a list of agents: 'seemak@LPT-0682' with a checked checkbox and a red arrow pointing to it, and 'seemak@SEEMAK-VM1' with an unchecked checkbox. At the bottom right, there are 'Submit' and 'Close' buttons. The background interface shows a search bar, an 'Upload' button, and a table with columns 'uploaded' and 'Actions'.

Figure 99h: Select Agent

4. Click on Choose File box and browse for the file upload. Click Submit.

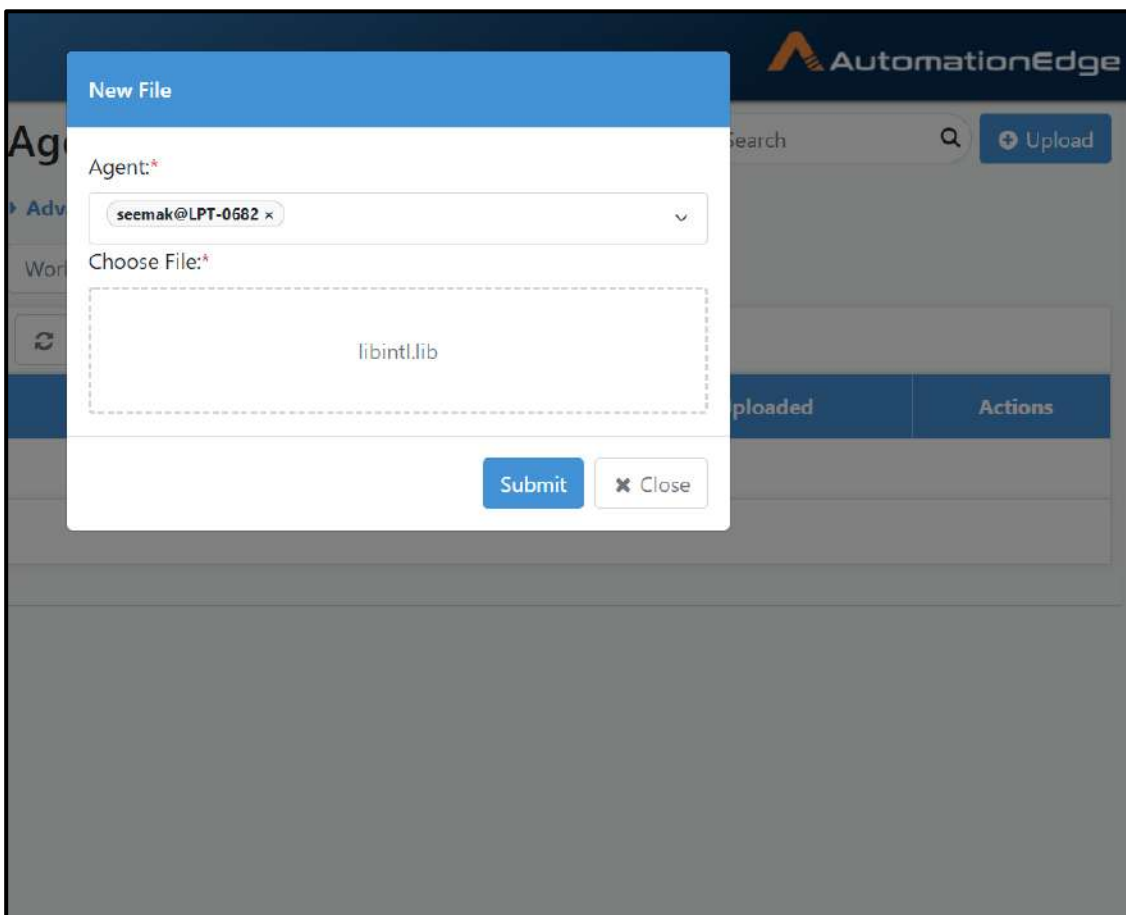


Figure 99i: Choose File

5. A File Uploaded Successfully message appears, and the uploaded file is visible in the Agent Files list.

16.2.2 View and Actions on supporting Files for an Agent

The File Management menu lists all the supporting files that were uploaded for Agents.

1. The File Management menu on the Agents tab shows the list of supporting files uploaded for Agents.
2. The page components are described in the table below.

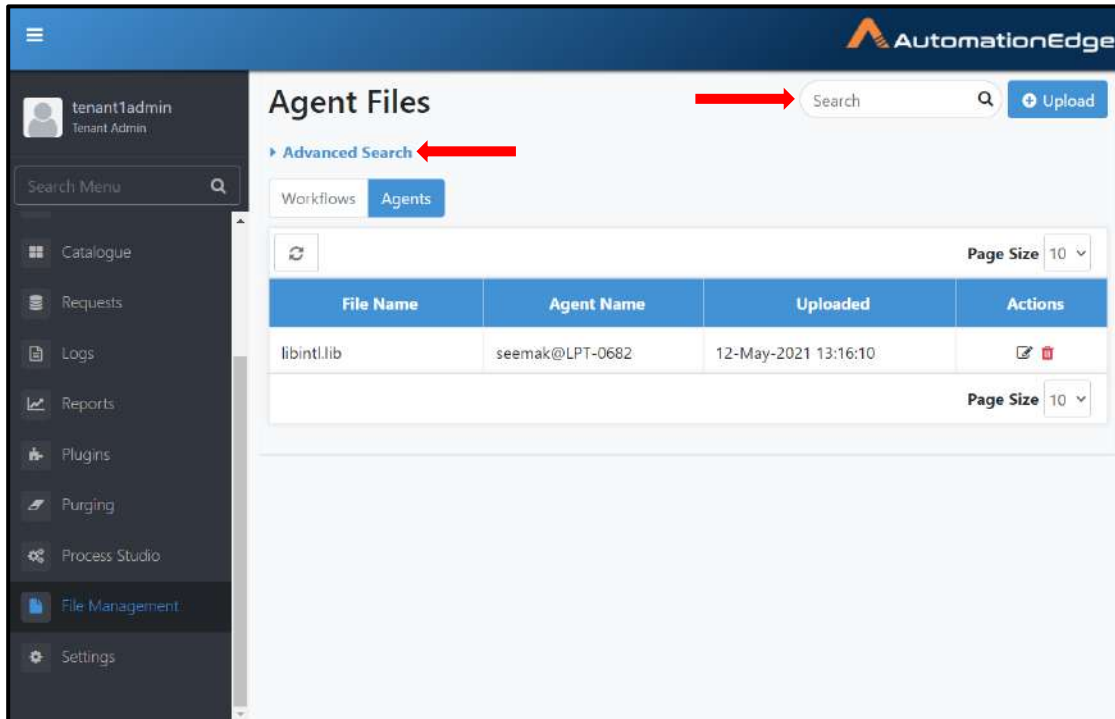


Figure 99j: Search and Advance Search for Agents File Management

The page components are described in the table below.

Table: Agent Files View

Column	Description
Search	Enter the Search string to filter the list.
Advanced Search	Expand to enter the advanced search criteria
File Name	The name of the file uploaded
Agent Name	The Agent name for which the file is uploaded
Uploaded	The timestamp for the file upload
Actions	<ol style="list-style-type: none"> iii. Click the Edit icon (✎) to edit the file uploaded. Click on the Choose File box to browse for an updated version of the same filename. The Agent field is not editable and cannot be changed. iv. Click the Delete icon (🗑) to delete the file from the AutomationEdge server.

17 Settings

17.1 SMTP

SMTP server is specific to the tenant for which it is configured. AEEEngine will use this SMTP server to send emails.

17.1.1 Add SMTP

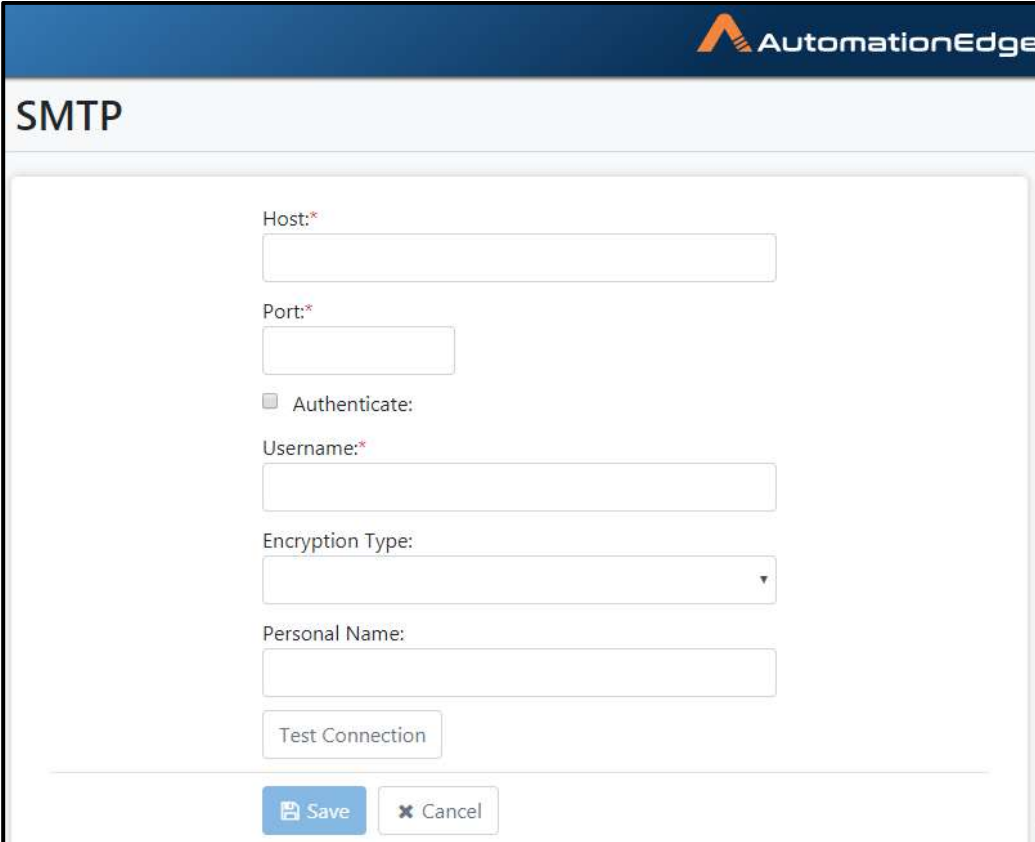
Following are the steps to configure SMTP.

1. Go to Settings menu and SMTP sub-menu.
2. Click Add SMTP button.



Figure 100a: Add SMTP

3. Configure SMTP in the form below.



Host:*

Port:*

Authenticate:

Username:*

Encryption Type:

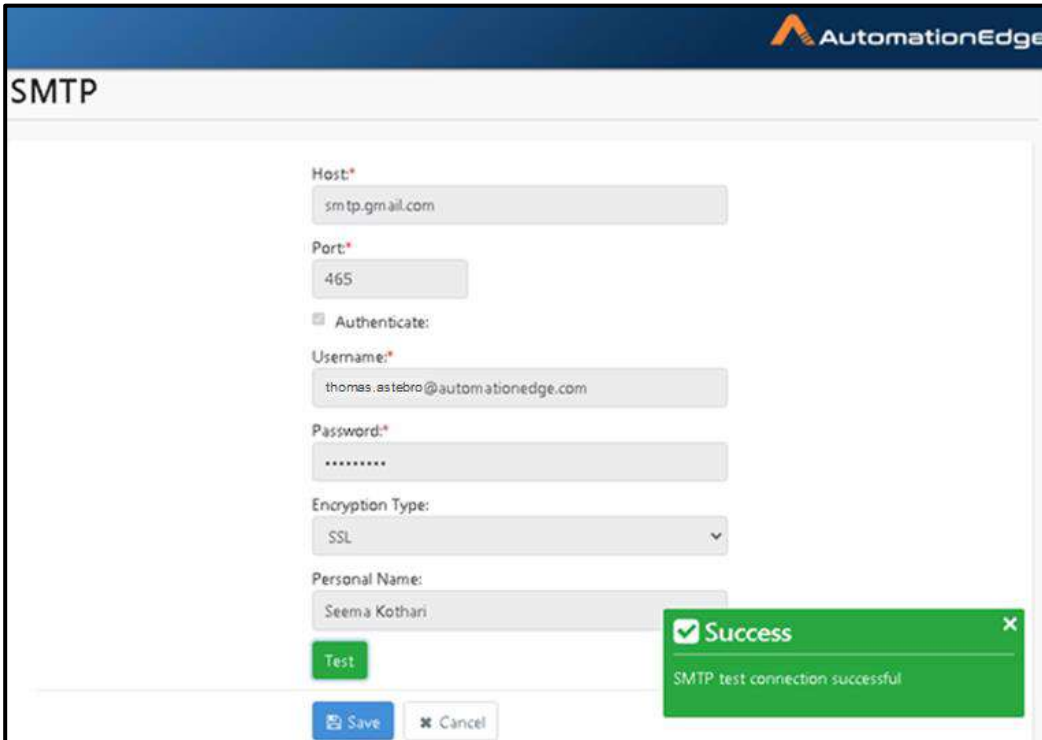
Personal Name:

Test Connection

Save Cancel

Figure 100b: SMTP configuration page

4. Enter SMTP configurations as shown below. Authenticate is checked. Click Test Connection. Test Connection Successful Message appears.



The screenshot shows the SMTP configuration interface in AutomationEdge. The form includes the following fields and controls:

- Host:** smtp.gmail.com
- Port:** 465
- Authenticate:**
- Username:** thomas.astebro@automationedge.com
- Password:** masked with dots
- Encryption Type:** SSL
- Personal Name:** Seema Kothari
- Test** button
- Save** and **Cancel** buttons
- Success** message box: SMTP test connection successful

Figure 100c: SMTP Test connection successful

5. The user also receives an SMTP test connection successful message.

6. Click Save. SMTP Settings Saved Successfully message appears.

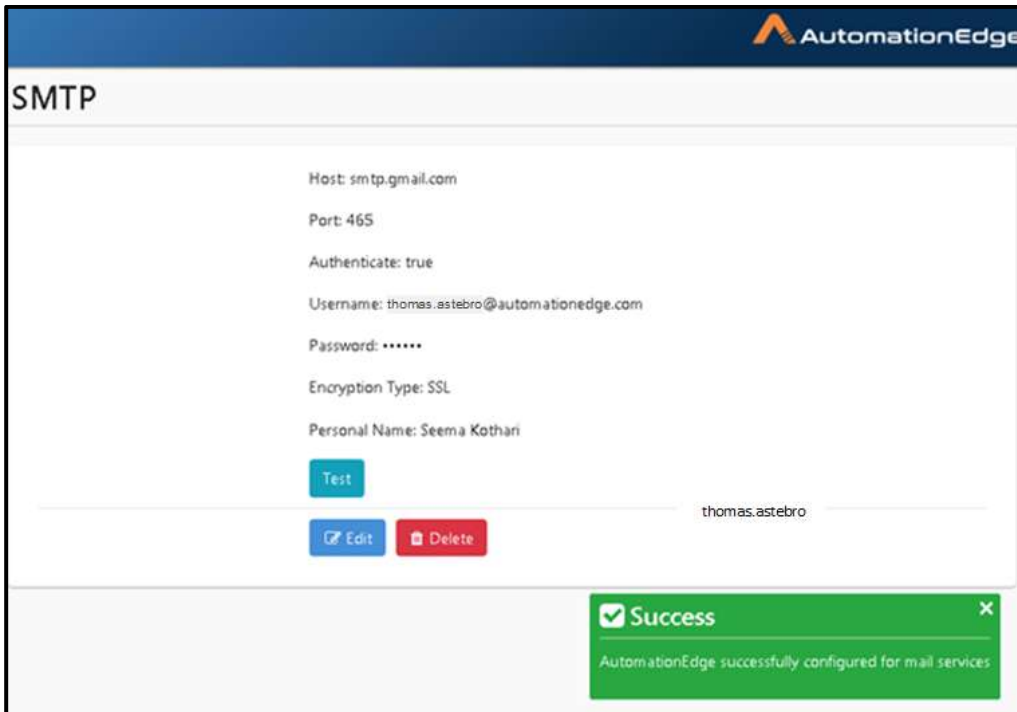


Figure 100d: SMTP configuration Success Message

Table 76: SMTP Server Configuration Details

Field	Description
SMTP host	Provide the fully qualified hostname or IP address of the LDAP server.
Port	Provide the port number for LDAP connectivity(e.g. for Gmail SMTP server SSL 465 TLS 582)
Is authentication required	Enable checkbox to use authentication to connect to the SMTP server.
Username	Provide a username for authentication
Password	Provide password for authentication
Encryption type	Choose from list: None, SSL or TLS
Sender name	This is personal name which will appear as from name in email. This is an optional field.
Button:	
Test Connection Button	Test Connection functionality is to validate SMTP details. Click Test Connection Button to validate/test SMTP connectivity with details provided.
Save Button	Click to save SMTP configurations.
Cancel Button	Click to Cancel.

17.1.2 SMTP: Delete

Following are the steps to delete SMTP configuration.

1. Go to Settings menu and SMTP sub-menu.
2. Click on the Delete button.

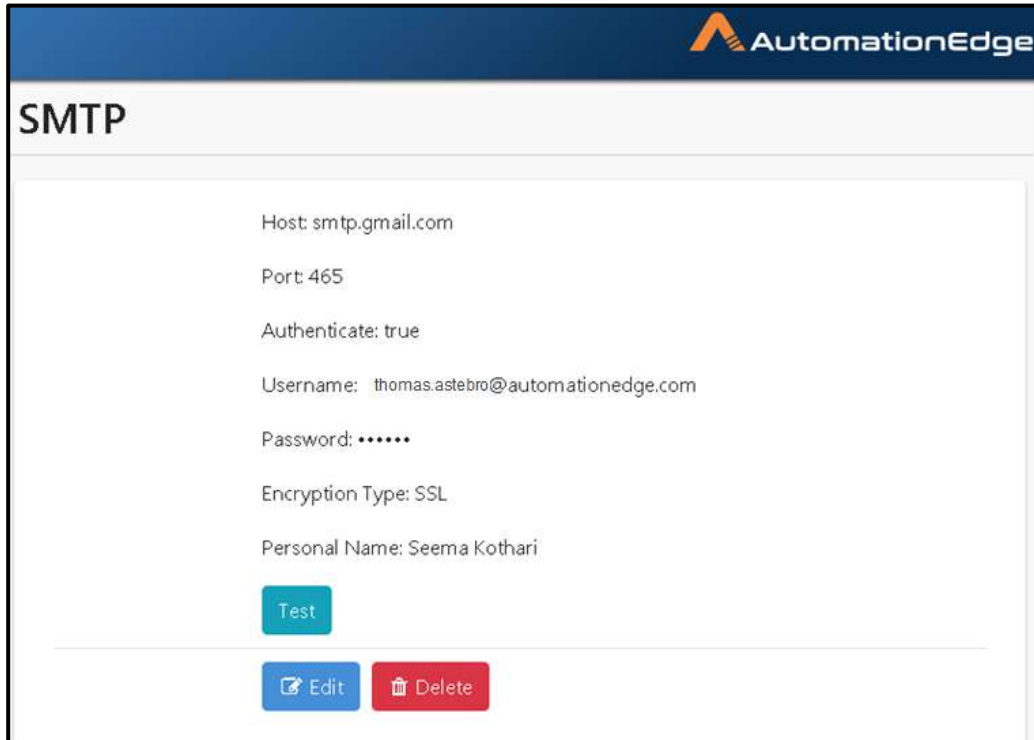


Figure 100f: Delete SMTP configuration

3. Confirm SMTP Configuration Deletion pop up appears. Click Delete button.

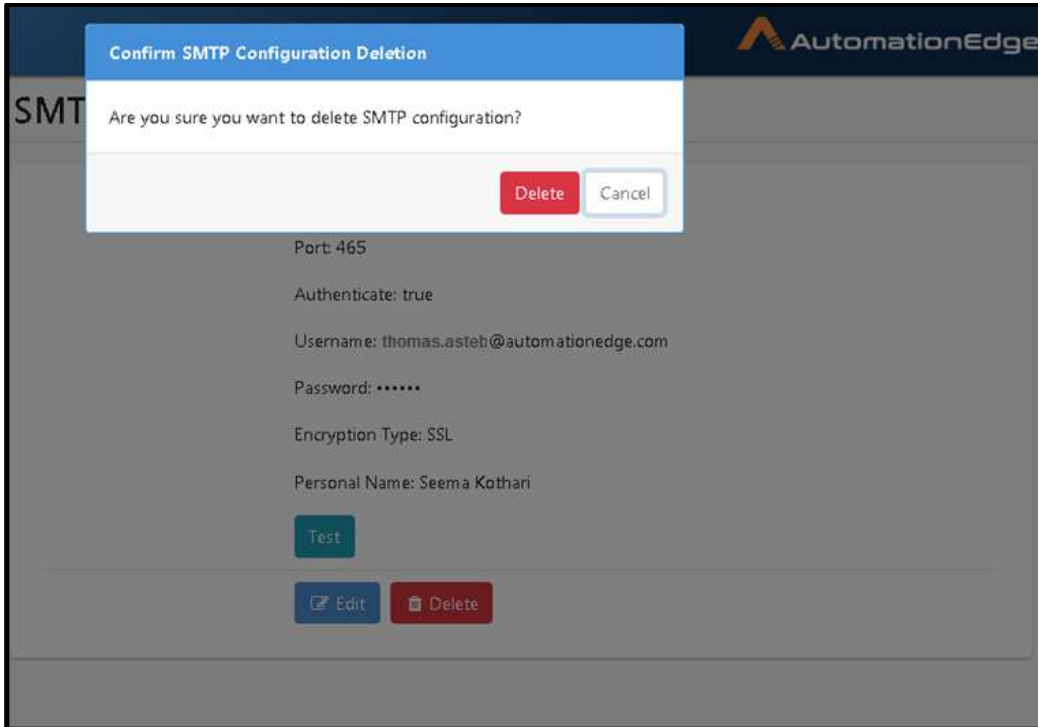


Figure 100g: Confirm SMTP deletion

4. SMTP configuration deleted successfully message appears.

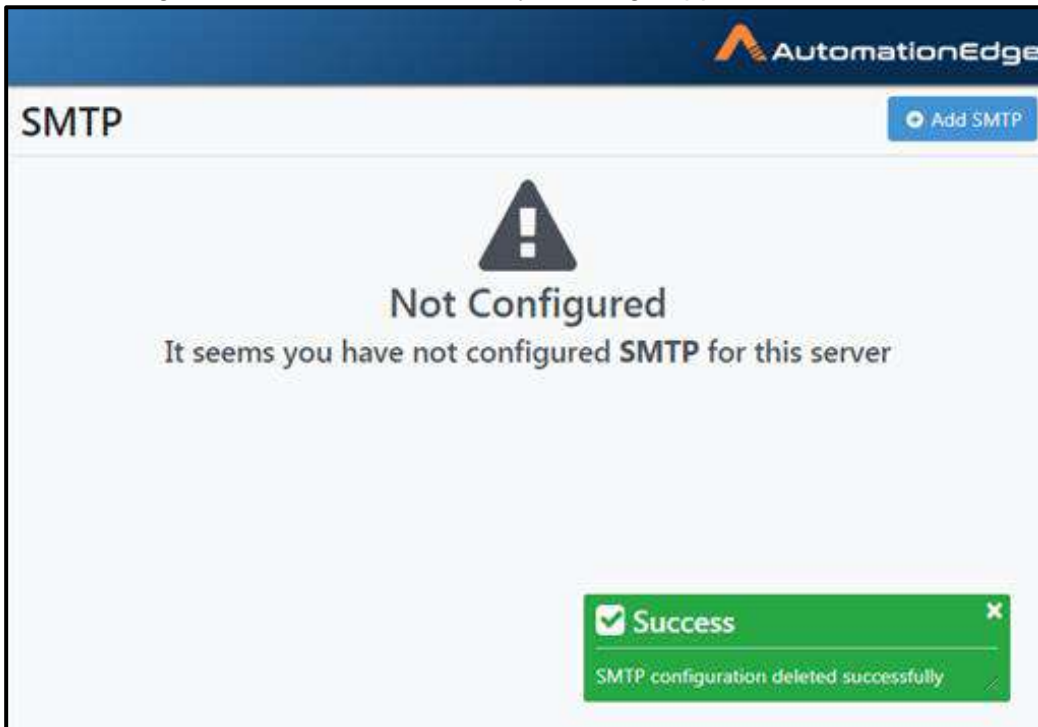


Figure 100h: SMTP deleted successfully message

17.1.3 Settings: Features/Permissions for other users

Table 77: Settings Features

Feature/Role	Tenant Administrator	Workflow Administrator	User Administrator	Agent Administrator	Tenant User	Activity Monitor
Configure SMTP	✓	-	-	-	-	-
Edit SMTP	✓	-	-	-	-	-

17.2 LDAP

In AutomationEdge there are three user types: Native, LDAP and SSO. Native users are authenticated locally, LDAP users are authenticated on LDAP servers, whereas SSO users are authenticated on an IDP server.

LDAP can be configured in the settings menu of a Tenant Administrator. Once LDAP is configured users of the type LDAP can be created.

17.2.1 Add LDAP Configuration

The configure LDAP settings,

1. Click Settings Tab and LDAP sub-menu.
2. The LDAP configuration page appears as shown in the following figure.

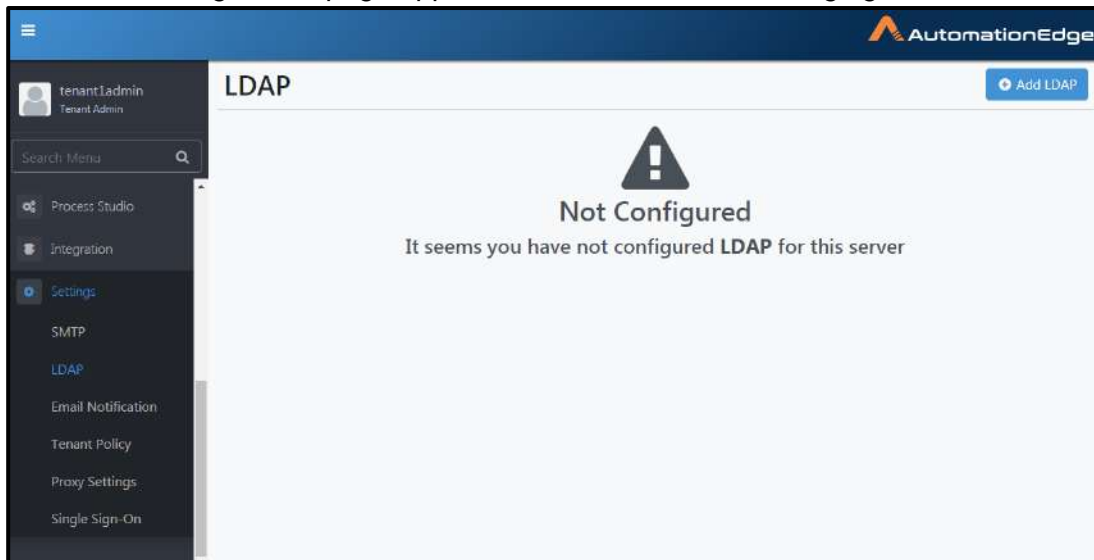


Figure 100i: Configure LDAP

3. Click Add LDAP

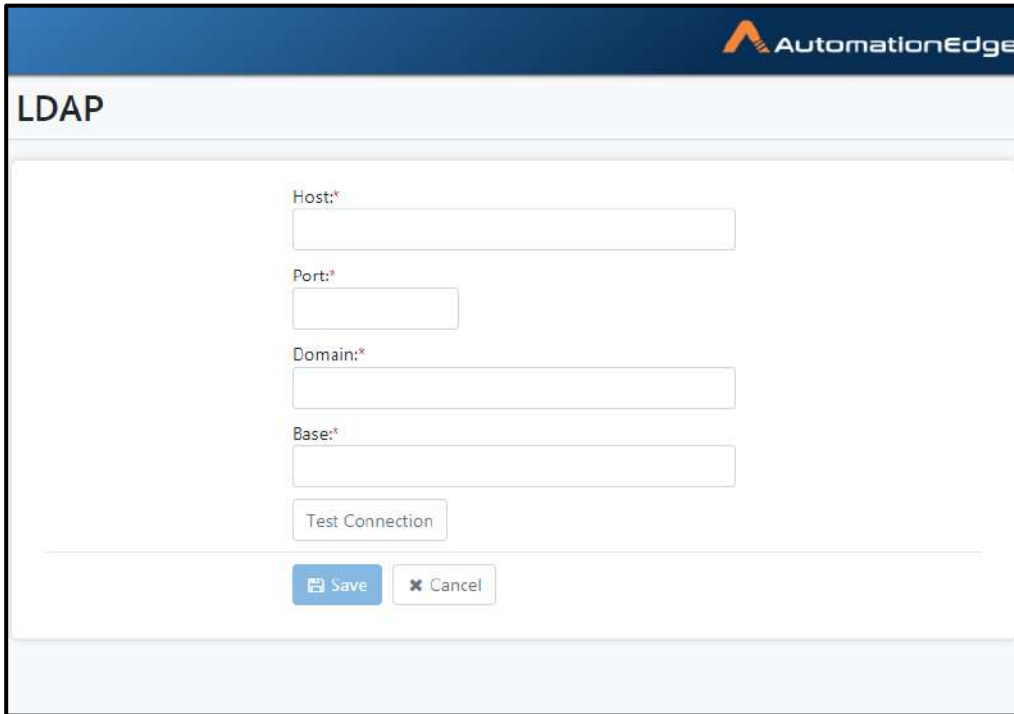


Figure 101j: LDAP Configuration page

4. Provide the LDAP configuration Settings and Test Connection.
5. Click Save button to save LDAP settings.

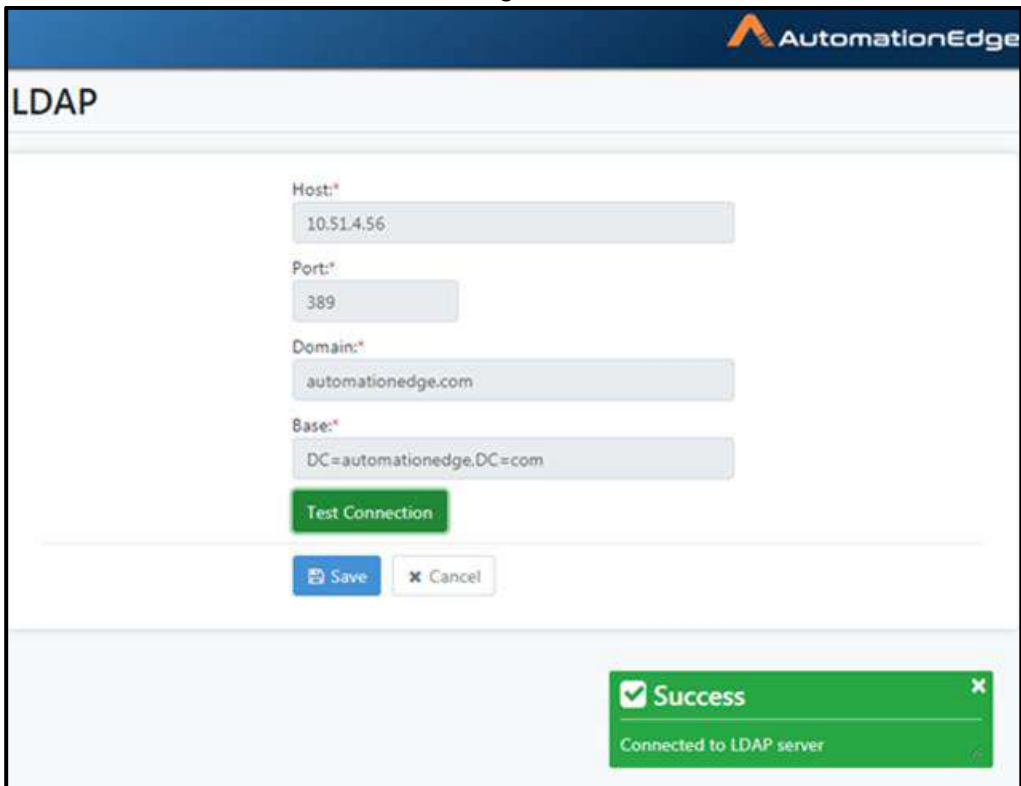


Figure 100k: LDAP Configurations and Test Connection

6. Save LDAP settings

AutomationEdge

LDAP

Host:*
10.51.4.56

Port:*
389

Domain:*
automationedge.com

Base:*
DC=automationedge,DC=com

Test Connection

Save Cancel

Figure 100l: Save LDAP Configurations

7. View LDAP settings saved Success Message.

AutomationEdge

LDAP

Host: 10.51.4.56

Port: 389

Domain: automationedge.com

Base: DC=automationedge,DC=com

Test Connection

Edit

Success
LDAP settings saved successfully

Figure 100m: LDAP Configurations Saved Success Message

The following table describes the fields for LDAP configuration.

Table 78: LDAP Configuration

Field	Description
Protocol	The protocol is LDAP by default.
Host	Provide the fully qualified hostname or IP address of the LDAP server.
Port	Provide the port number for LDAP connectivity.
Domain	Provide the fully qualified domain name of LDAP server.
Base	A base dn is the point from where a server will search for users. An ldap search for a user will be done by the server starting at the base dn (dc=example, dc=com).
Buttons:	
Test Connection Button	Click to test LDAP connectivity.
Save Button	Click to save LDAP configurations.
Cancel Button	Click to Cancel.

17.2.2 Settings: Features/Permissions for other users

Table 79: Settings Features

Feature/Role	Tenant Administrator	Workflow Administrator	User Administrator	Tenant User
Create LDAP User	✓	-	✓	-
Edit LDAP User	✓	-	-	-

Note: User Administrator can create LDAP users with role Tenant User only.

17.3 Tenant Policy

Password Policy for AutomationEdge login is discussed in this section. Password policy can be set and modified by a Tenant Administrator at the Tenant level.

17.3.1 View Tenant Policy

Following, are the details of Tenant Policy page.

1. Navigate to the Settings menu and Tenant Policy sub-menu. You can now see the Tenant Policy screen as shown below.
2. In the screenshot below Miscellaneous section is expanded.

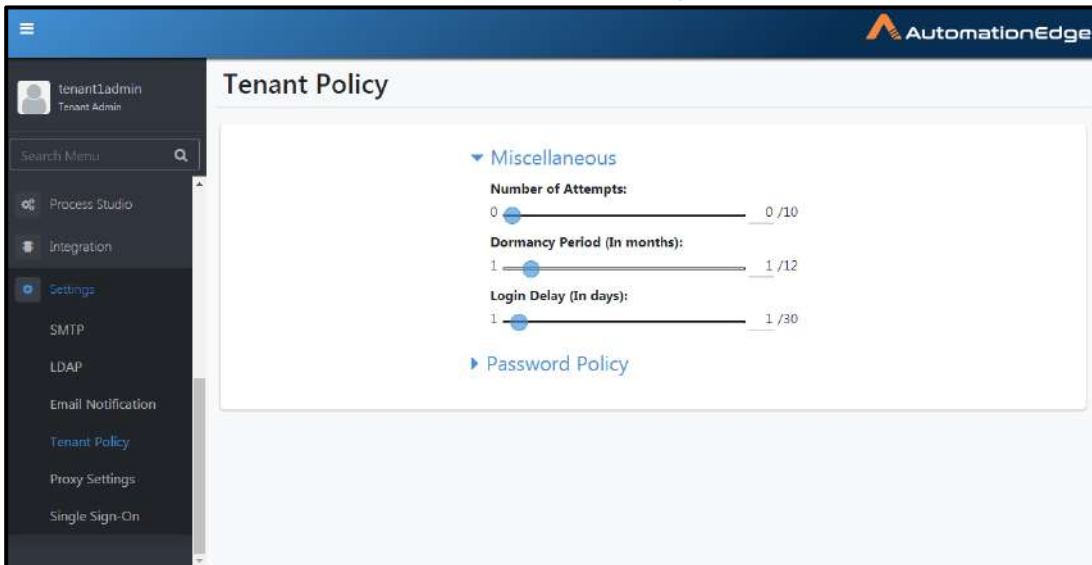


Figure 105a: View Miscellaneous section in Tenant Policy

3. In the screenshot below Password Policy section is expanded

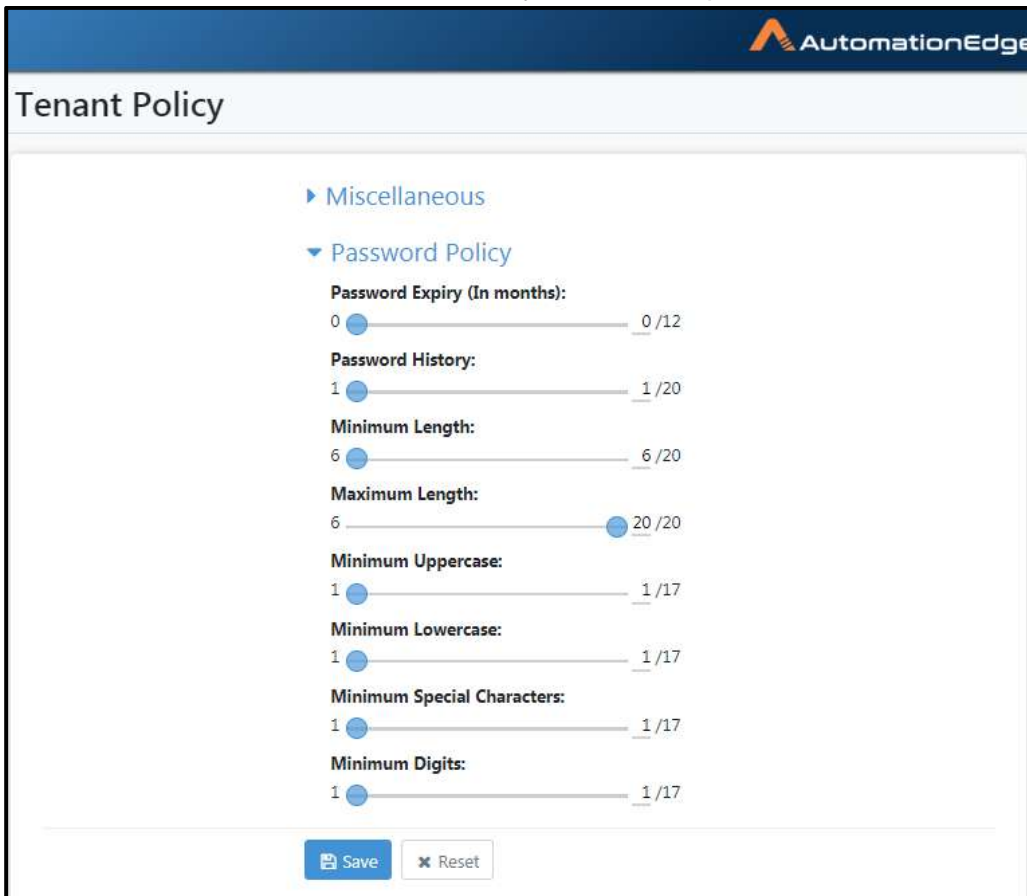


Figure 105b: View Password Policy under Tenant Policy

- The default values for the different password policy options are shown on the left hand end of the bar. The current value of the password policy and maximum values are shown on the right hand end.
- You may scroll the blue circles left or right to change these values. Below is a sample partial screenshot of Tenant Policy menu with modified settings.

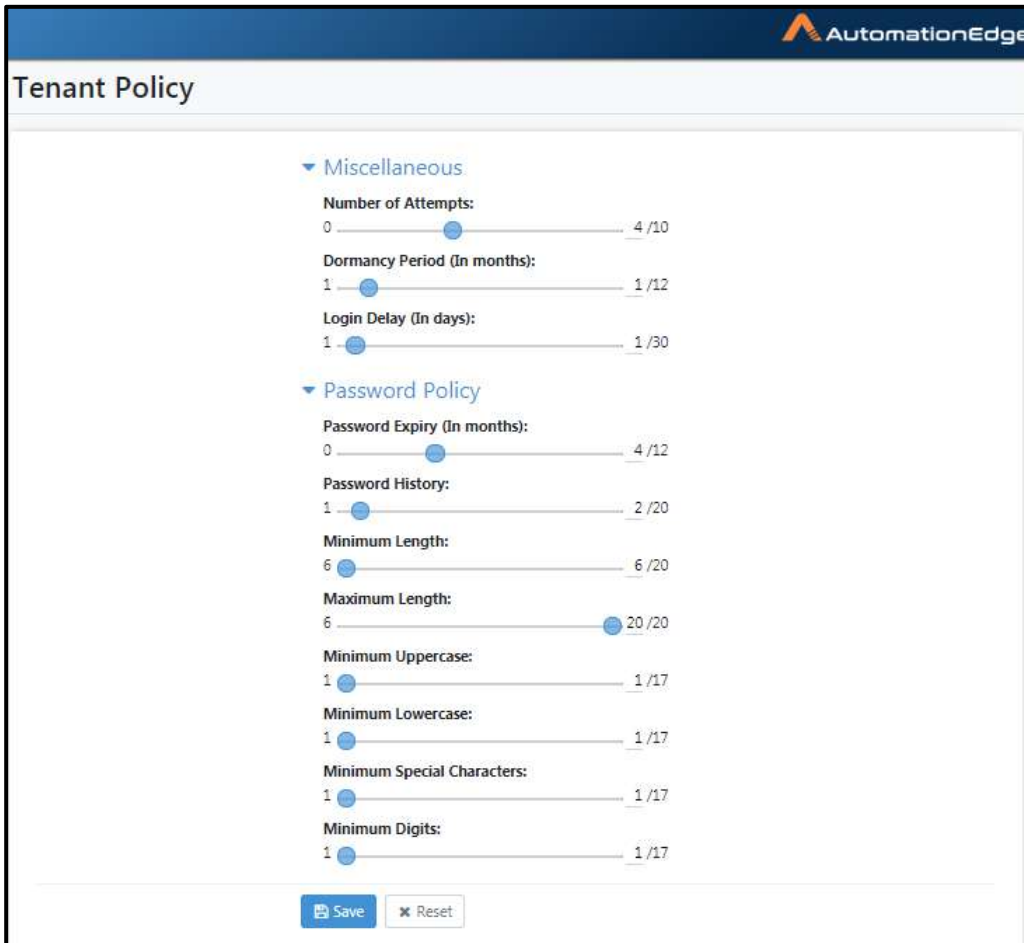


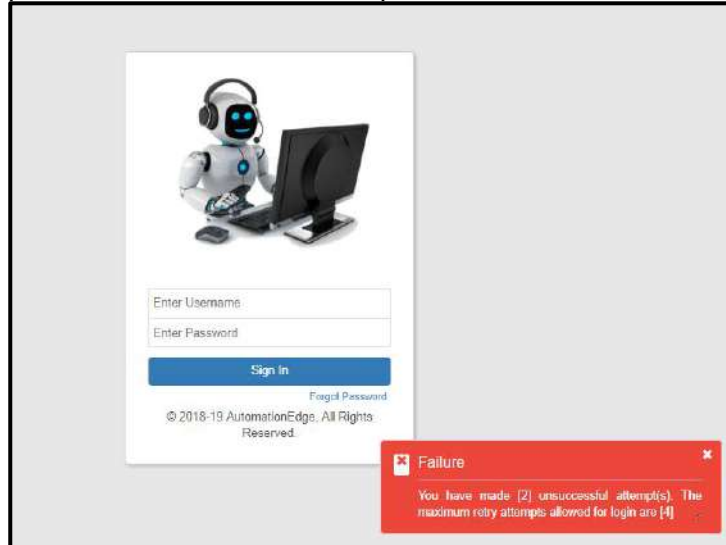
Figure 105c: Scroll Circle to change Policy configurations

All the policies are explained in the table below. The default policy rules/values are also provided in the table.

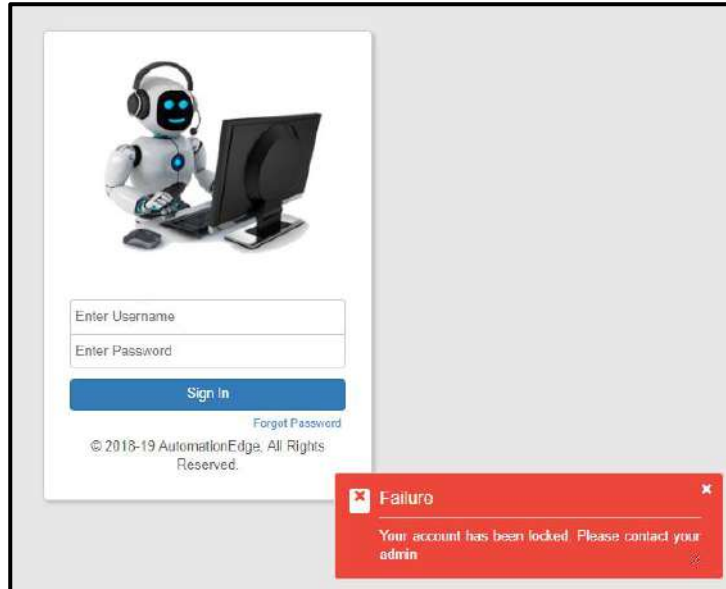
Table 80: Miscellaneous and Password Policy section attributes

Policy Complexity attribute	Default Rules
Miscellaneous	
Number of Attempts	As seen in the figure set the value for Number of Attempts between zero and ten (0-10). The default attempt limit is 0, i.e. there is no limit on the number of wrong password attempts.

The number of login attempts can be set by the Tenant Administrator. User is notified with remaining number of attempts every time when he/she tries to login with wrong password as seen in the snapshot below.

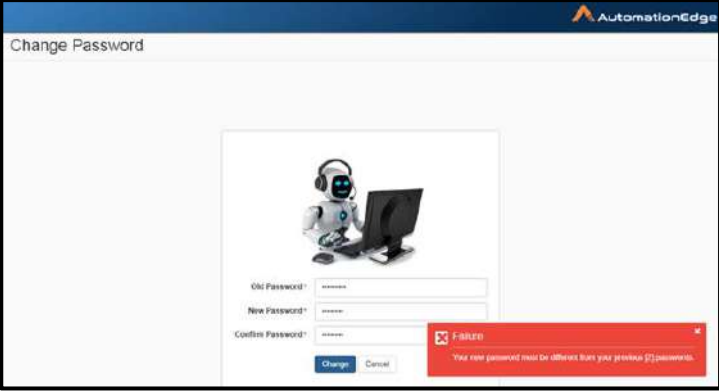


Once the user reaches the unsuccessful login attempt limit set by the Tenant Administrator the user account is locked as seen below.



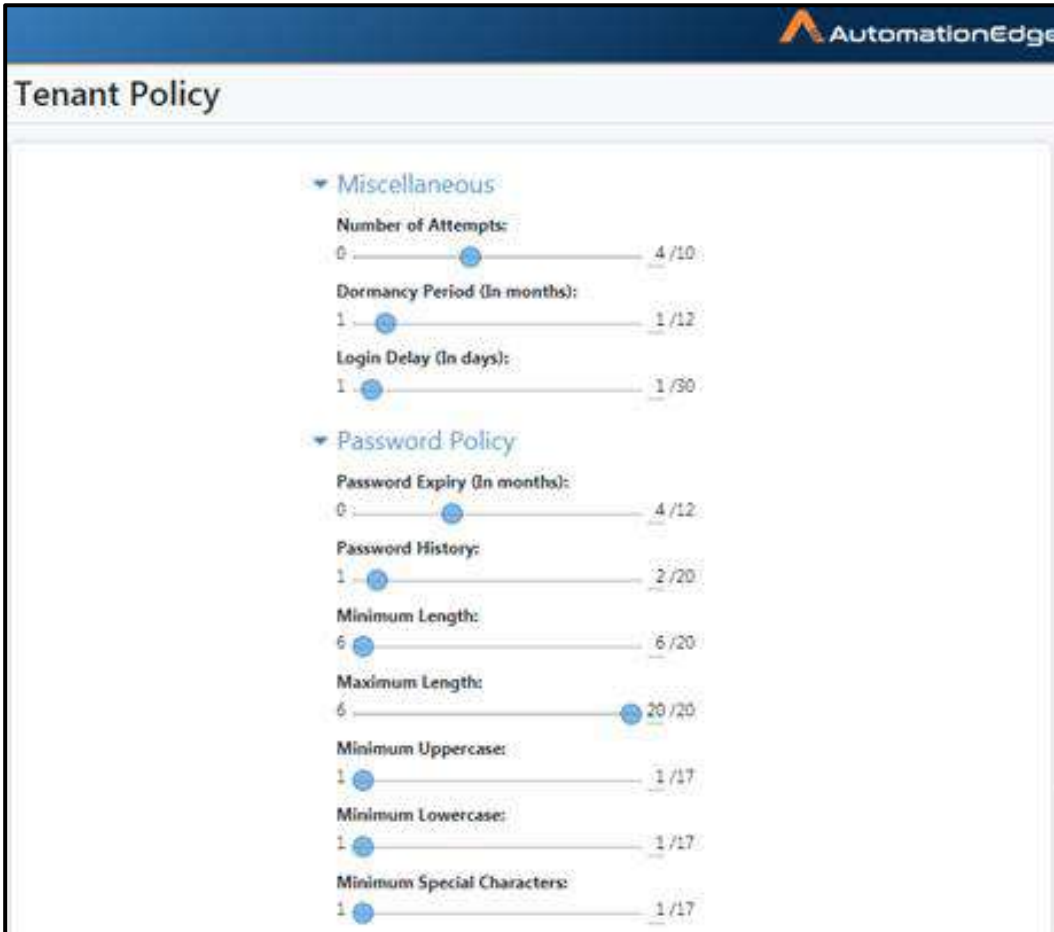
The locked user account can be unlocked only by the Tenant Administrator by setting the new password. The new password is sent to user via email if he/she is registered with email Id and SMTP is configured for the tenant and Email Notification is enabled for Password change. Else user has to contact the Tenant Administrator. When user logs in the first time after unlocking the account he/she will be forced to change password.

	<p>This is also applicable to LDAP users. For unlocking NATIVE users Tenant Administrator has to provide a new password, however there no requirement for password resetting in case of LDAP users</p>
Dormancy Period (In months)	<p>If an account has had no activity for a long period of time, then the account is marked as Dormant. The minimum setting for Dormancy is 1 month. You may increase the dormancy period up to 12 months.</p> <p>This state can be changed by a Tenant Administrator by enabling it. This state is the same as disabled state in every sense. Dormant Account status results in automatic disabling of account. Accounts are marked dormant during nightly job.</p>
Login delay (In days)	<p>When Tenant Administrator or User Administrator enables a locked/disabled/dormant user account, a user remains in enabled state until it logs in. On login an enabled user is marked as Active and logs in.</p> <p>By default, user should login to the account on the same day else account is automatically disabled again. The default setting is 1 day. This setting is configurable, the setting can be increased to a maximum of 10 days. However, if a user fails to login during this period the user is disabled.</p>
Password Policy	
Password Expiry/ Maximum password age (In months)	<p>As seen in the figure set the value for Password Expiry (In months) between zero and twelve (0-12). The default is Password Expiry Months is 0, i.e. there is no password expiry. The Password Expiry (In months) can be set by the Tenant Administrator.</p> <p>This policy forces the user to change their passwords within duration set by the Tenant Administrator. The duration is set in months. User must change their password within that duration otherwise he/she will be forced to change password. User will be notified before 15 days, 7 days, 1 day and on the day of password expiry, at the time of login.</p>
Password History	<p>Default and minimum value of password history is one (1), i.e. the new password changed by user is checked with at least one previous password.</p> <p>When Tenant Administrator changes the default value of password history to greater than 1, then after that whenever user changes password, system starts to store the user's passwords in a password history table. Any new password changed by user is checked with all previous passwords present in history table</p> <p>This feature will force user to use new passwords when he changes the password. Depending on the setting, users will not be able to use the last 'N' passwords while changing it as</p>

	<p>seen below.</p>  <p>User will notified with an error message if new password is same as one of the old passwords.</p>
<p>Password Complexity</p>	<p>Password Complexity comprises the following five attributes also seen in the screenshot below.</p> <div style="border: 1px solid black; padding: 5px;"> <p>Password length must be between 6-20</p> <ul style="list-style-type: none"> • At least 1 uppercase letter(s) • At least 1 lowercase letter(s) • At least 1 digit(s) • At least 1 special characters(s) out of @#\$!& </div>
<ul style="list-style-type: none"> • Maximum Length/Length of Password 	<p>As seen in the figure set the value for Maximum Length in between six and twenty (6-20). The default value is 20, i.e. the maximum length can be up to 20 characters.</p>
<ul style="list-style-type: none"> • Minimum Uppercase 	<p>As seen in the figure set the value for Minimum Uppercase in between zero and seventeen (0-17). The default value is 1, i.e. there must be at least one uppercase letter.</p>
<ul style="list-style-type: none"> • Minimum Lowercase 	<p>As seen in the figure set the value for Minimum Uppercase in between zero and seventeen (0-17). The default value is 1, i.e. there must be at least one Lowercase letter.</p>
<ul style="list-style-type: none"> • Minimum Special Characters 	<p>As seen in the figure set the value for Minimum Uppercase in between zero and seventeen (0-17). The default value is 1, i.e. there must be at least one Special Character [<u>@, #, \$, &, _</u>].</p>
<ul style="list-style-type: none"> • Minimum Digits 	<p>As seen in the figure set the value for Minimum Digits in between zero and seventeen (0-17). The default value is 1, i.e. there must be at least one Digit.</p>

17.3.2 Change Password Policy

1. Tenant Administrators can change password policies by scrolling the blue circles left or right to change these values.
2. Let us scroll the blue circle on Password history to the right. It is now place at 2 as can be seen on the right hand end. The user will not be allowed to use the previous two passwords.
3. Click Save.



The screenshot displays the 'Tenant Policy' configuration interface. It features two main sections: 'Miscellaneous' and 'Password Policy'. Each section contains several settings with sliders and numerical values. The 'Password Policy' section is expanded, showing the following settings:

Setting	Current Value	Range
Number of Attempts	4	0 / 10
Dormancy Period (In months)	1	1 / 12
Login Delay (In days)	1	1 / 30
Password Expiry (In months)	4	0 / 12
Password History	2	1 / 20
Minimum Length	6	6 / 20
Maximum Length	20	6 / 20
Minimum Uppercase	1	1 / 17
Minimum Lowercase	1	1 / 17
Minimum Special Characters	1	1 / 17

Figure 105d: Modify Password History

4. A confirm policy pop-up window appears. As you can see it shows number of last password(s) to be checked is 2. The other policies remain the same.

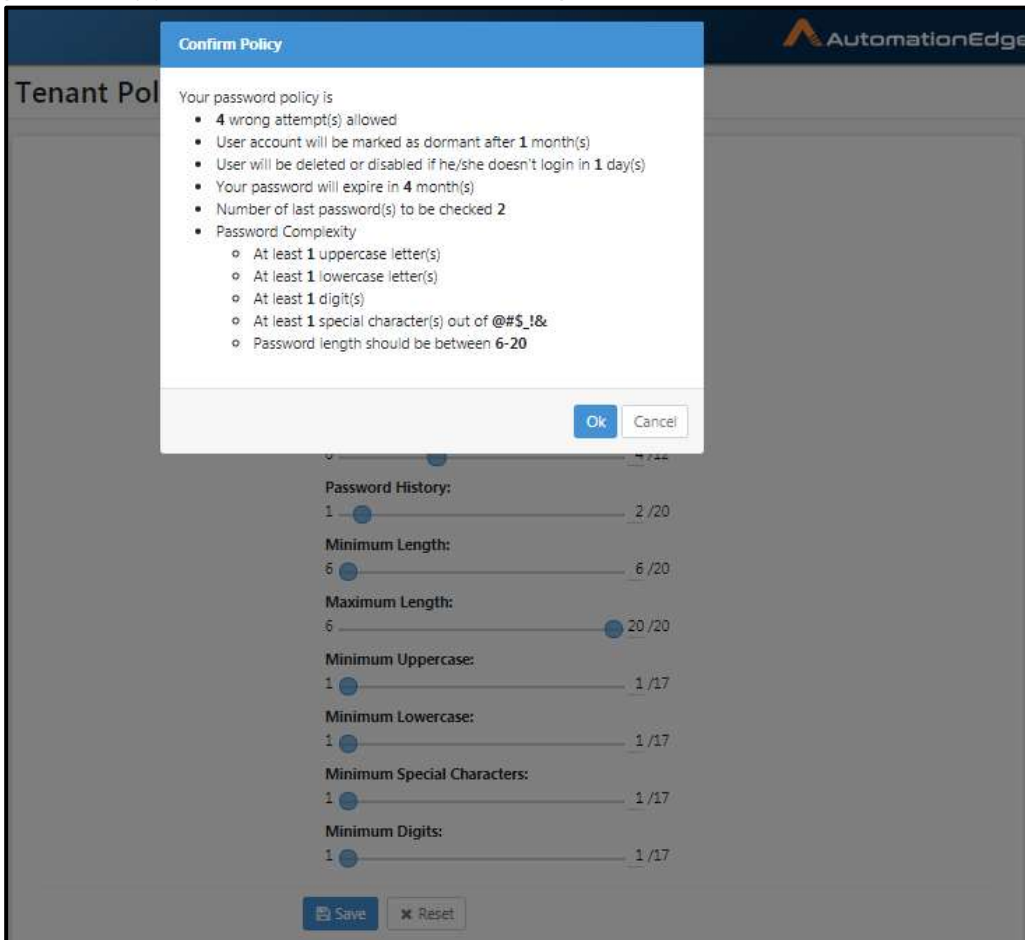


Figure 105e: Confirm new password policy

5. Password policy updated successfully message appears.

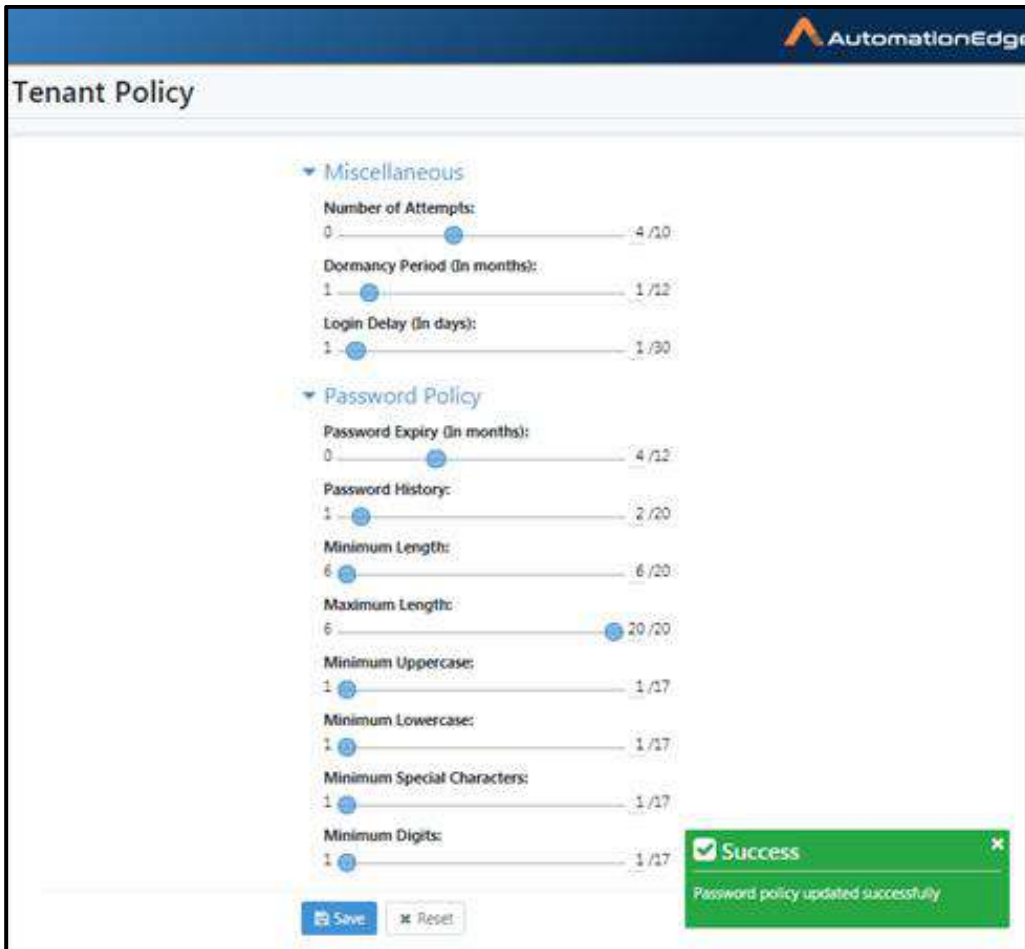


Figure 105f: Password Policy updated successfully message

6. This completes the process of setting password policies.

17.4 Email Notification

17.4.1 Introduction

AutomationEdge supports sending notifications via email to different stakeholders such as Tenant Administrator, Tenant Users. One of the scenarios for sending notifications is to send email to users in case a workflow request fails.

The SMTP server is configured at Tenant level. All Agent configured under this tenant have access and can use this SMTP server to send emails.

17.4.2 Notification Scenarios

AutomationEdge will support sending notifications in scenarios as discussed in the following sections.

17.4.2.1 Pending Requests

Higher and lower thresholds for pending requests are set in AutomationEdge. When the number of pending requests reaches the higher threshold; AutomationEdge stops accepting new requests. Scheduled requests also fail. In such a scenario a notification is sent to all System Administrators and Tenant Administrators by default.

However, one can enable notification for pending requests; which triggers notification once number of pending requests reaches the lower threshold and notification can be sent to System Administrators, Tenant Administrators and email ids as configured.

Following are the steps to configure pending requests:

1. Go to the Settings menu and Email Notification sub-menu.
2. In case you have not yet configured SMTP the Email Notification page appears as below.

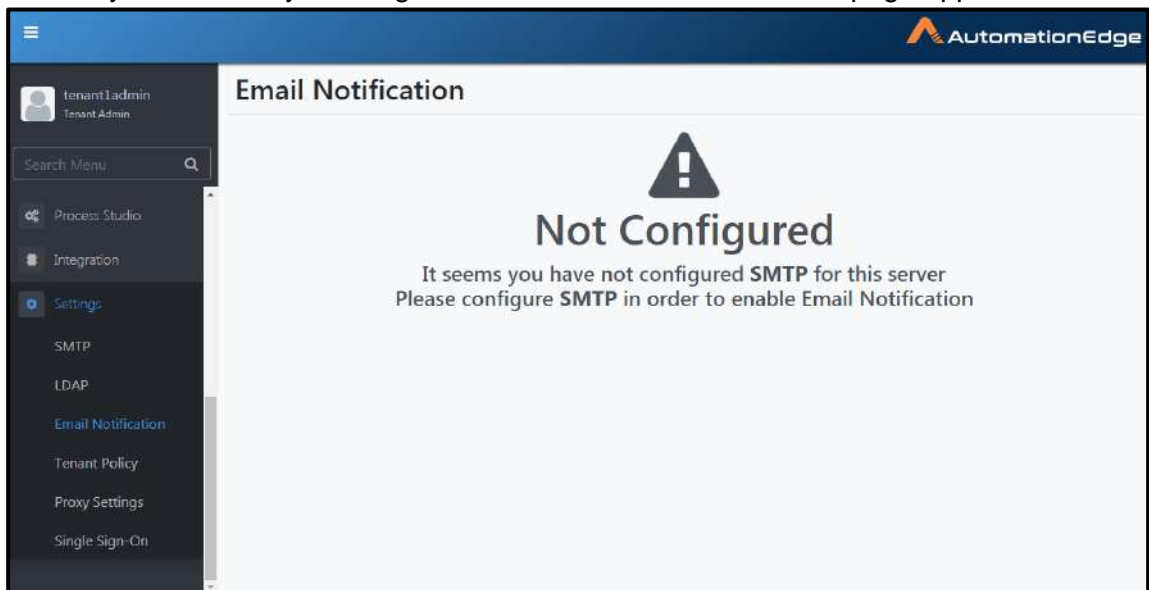
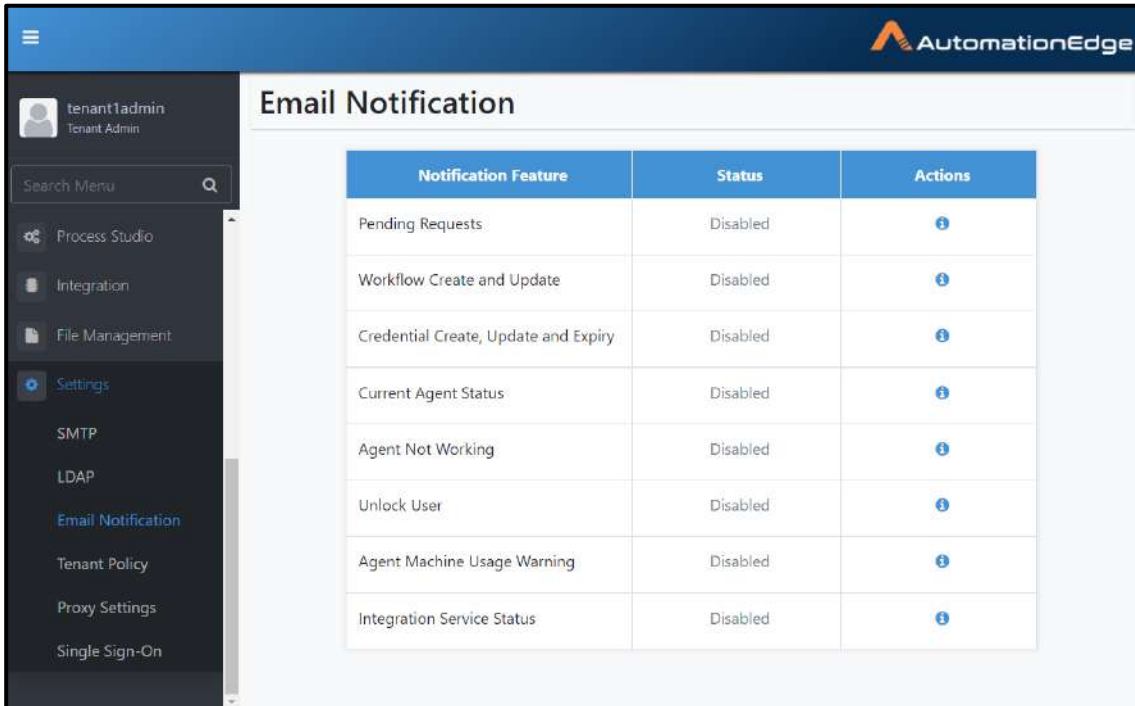


Figure 106a: Email Notification

3. Once SMTP is configured the following Email Notification page appears. Click Add next to Notification feature you wish to setup.
4. First click the Details icon (i) next to Pending Requests.



The screenshot displays the 'Email Notification' configuration page. On the left is a navigation menu with options: Process Studio, Integration, File Management, Settings (highlighted), SMTP, LDAP, Email Notification (highlighted), Tenant Policy, Proxy Settings, and Single Sign-On. The main content area shows a table with the following data:

Notification Feature	Status	Actions
Pending Requests	Disabled	(i)
Workflow Create and Update	Disabled	(i)
Credential Create, Update and Expiry	Disabled	(i)
Current Agent Status	Disabled	(i)
Agent Not Working	Disabled	(i)
Unlock User	Disabled	(i)
Agent Machine Usage Warning	Disabled	(i)
Integration Service Status	Disabled	(i)

Figure 106b: Email Notifications Menu

5. Pending Requests configuration page appears. Click the toggle to enable the feature and Click Save.

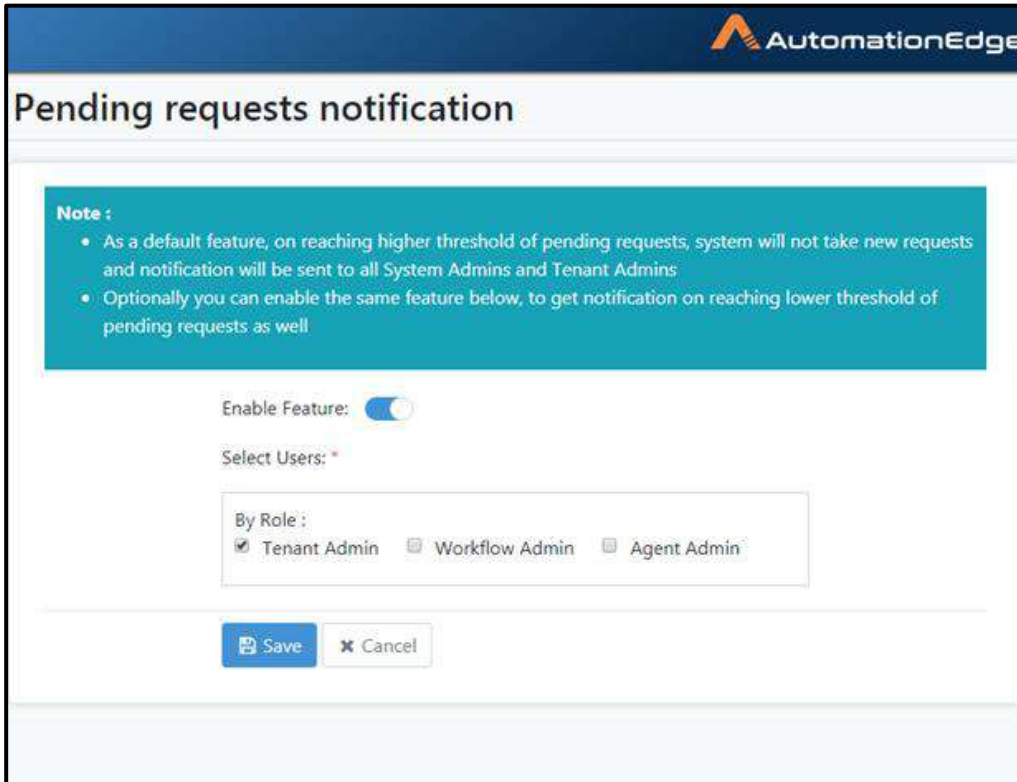


Figure 106c: Configurations for Email Notification for Pending Requests

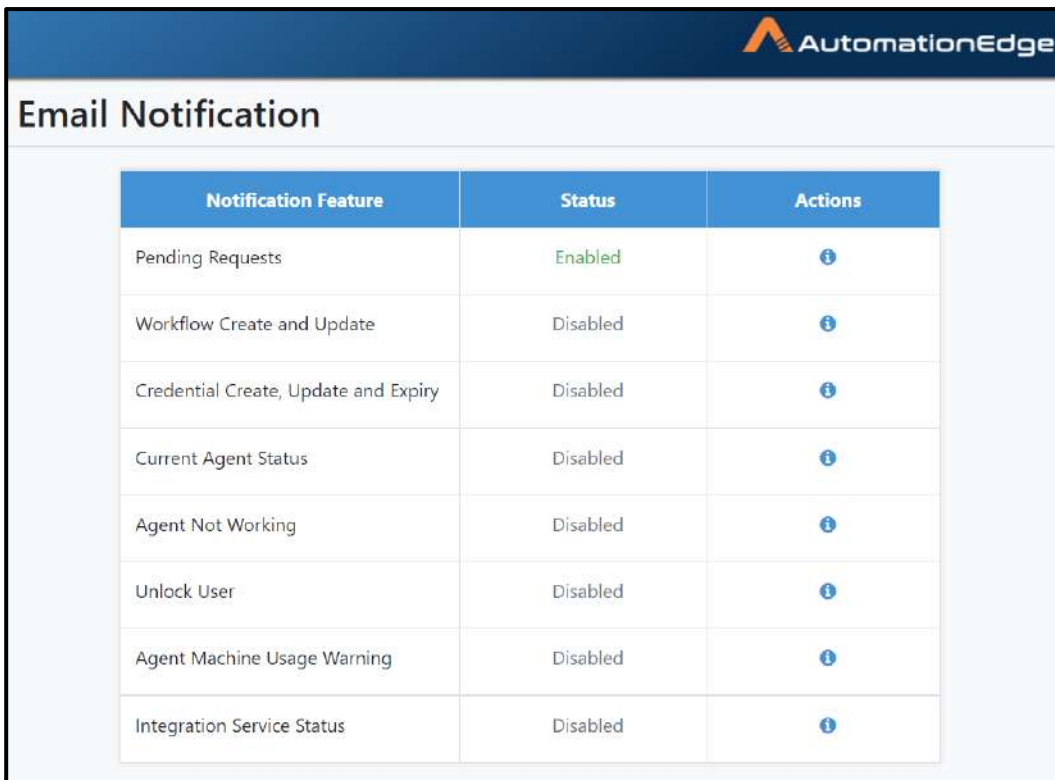
6. A message displays showing Notification Configuration saved successfully.

17.4.2.2 Workflow Configuration Changes

When workflow configuration parameters are changed while editing a workflow; email notification can be sent to all Tenant Administrators, Workflow Administrators and configured email ids.

Following are the steps to configure Email notification for workflow configuration changes,

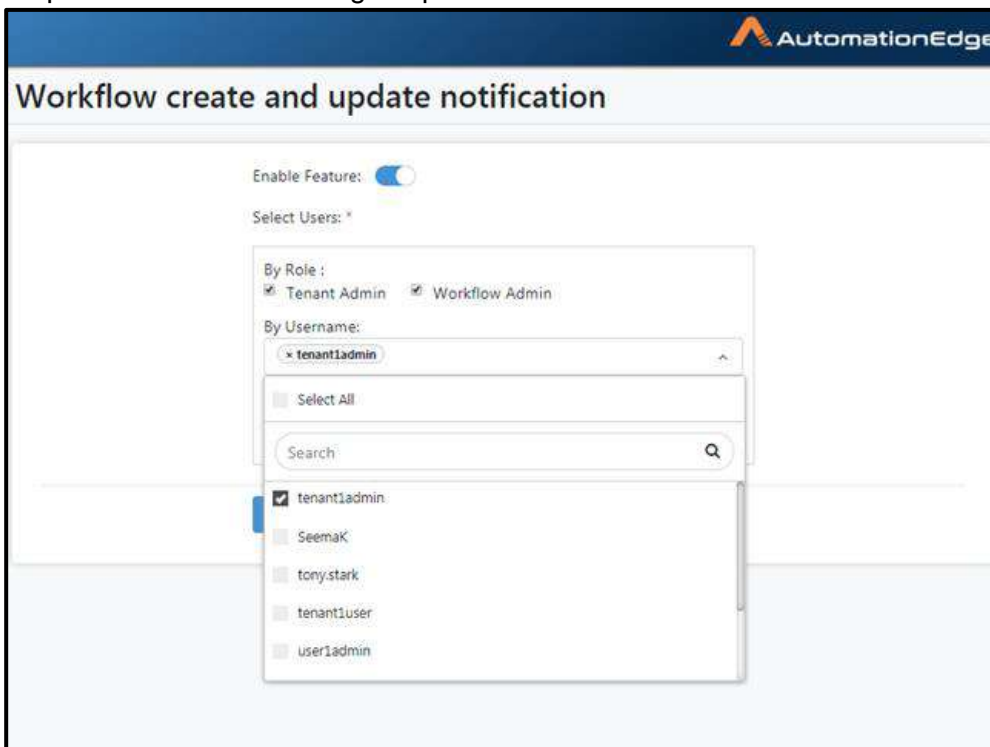
1. Go to the Settings menu and Email Notification sub-menu.
2. Click the Details icon (i) next to Workflow Configuration Changes.



Notification Feature	Status	Actions
Pending Requests	Enabled	i
Workflow Create and Update	Disabled	i
Credential Create, Update and Expiry	Disabled	i
Current Agent Status	Disabled	i
Agent Not Working	Disabled	i
Unlock User	Disabled	i
Agent Machine Usage Warning	Disabled	i
Integration Service Status	Disabled	i

Figure 107a: Add Email Notification for Workflow Configuration Changes

3. Click the toggle to enable the Workflow configuration changes notification feature.
4. Select users by role by enabling checkboxes or select usernames to be notified from the dropdown list. The following snapshot shows user tenant1admin is selected. Click save.



AutomationEdge

Workflow create and update notification

Enable Feature:

Select Users: *

By Role :

Tenant Admin Workflow Admin

By Username:

tenant1admin

Select All

Search

- tenant1admin
- SeemaK
- tony.stark
- tenant1user
- user1admin

Figure 107b: Select Users

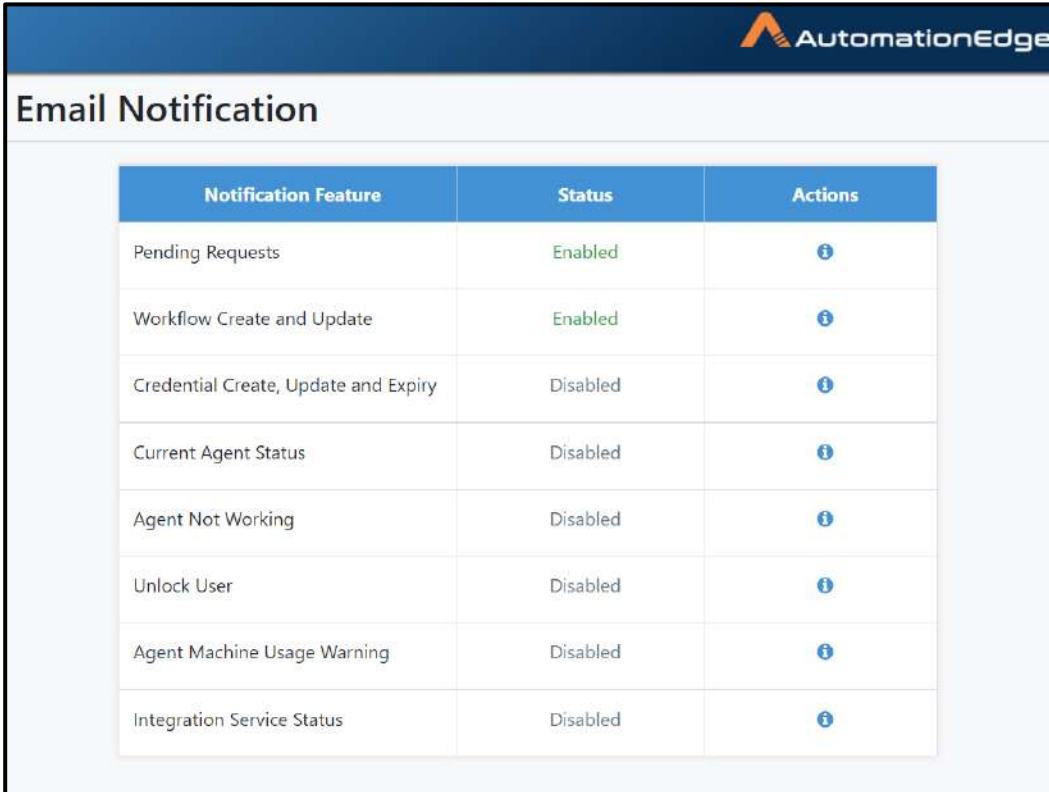
5. A message displays showing Notification Configuration saved successfully.

17.4.2.3 Credential Modification/Expiry

When credential is about to expire or is modified email notification will be sent. Notification can be sent to all Tenant Administrators, Workflow Administrators and configured email ids.

Following are the steps to configure Credential Create, Update and Expiry,

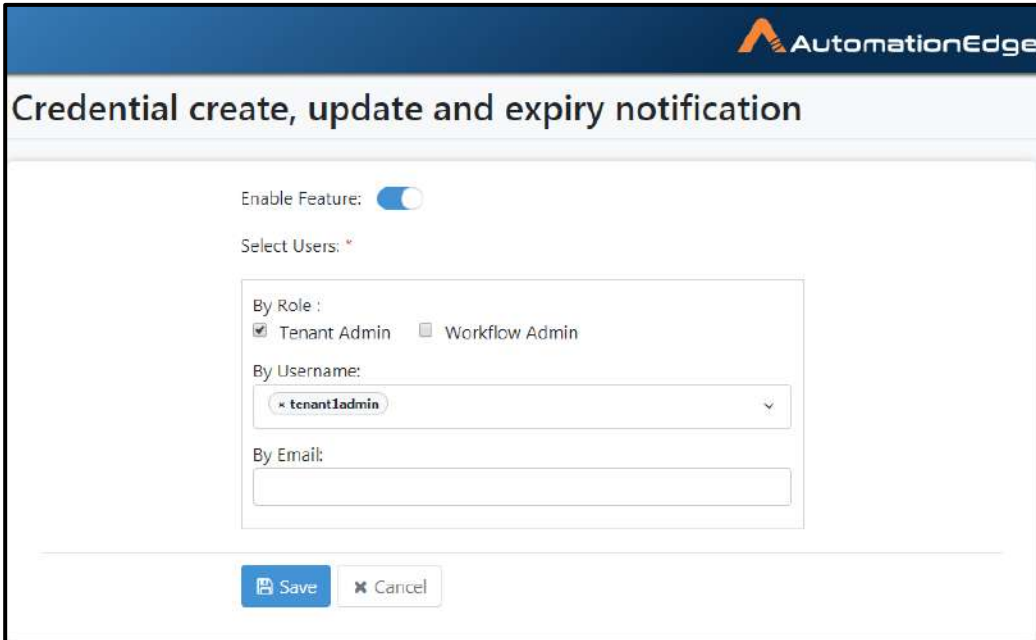
1. Go to the Settings menu and Email Notification sub-menu.
2. Click Details icon (i) next to Credential Create, Update and Expiry.



Notification Feature	Status	Actions
Pending Requests	Enabled	i
Workflow Create and Update	Enabled	i
Credential Create, Update and Expiry	Disabled	i
Current Agent Status	Disabled	i
Agent Not Working	Disabled	i
Unlock User	Disabled	i
Agent Machine Usage Warning	Disabled	i
Integration Service Status	Disabled	i

Figure 108a: Email Notification Setting

3. Click the toggle to enable the feature.



The screenshot shows the AutomationEdge interface for configuring email notifications. The page title is "Credential create, update and expiry notification". The "Enable Feature" toggle is turned on. The "Select Users" dropdown is open, showing options for "By Role" (Tenant Admin, Workflow Admin) and "By Username" (tenantAdmin). The "By Email" field is empty. "Save" and "Cancel" buttons are at the bottom.


Figure 108b: Email Notification for Credential Modification and Expiry

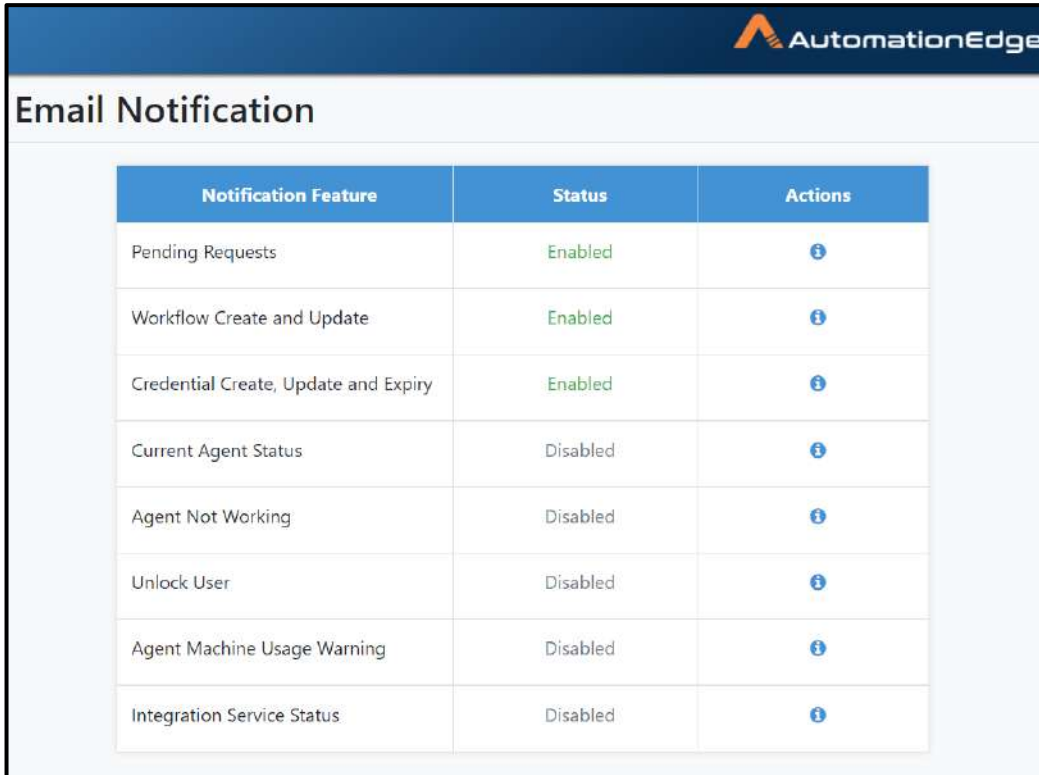
4. A message displays showing Notification Configuration saved successfully.

17.4.2.4 Current Agent Status

A notification regarding the number of running requests, number of Running agents and their status etc. can be periodically sent to all Tenant Administrators, Workflow Administrators and configured email ids. The period can be set in hours.

Following are the configuration steps:

1. Go to the Settings menu and Email Notification sub-menu.
2. Click Details icon () next to Current Agent Status.











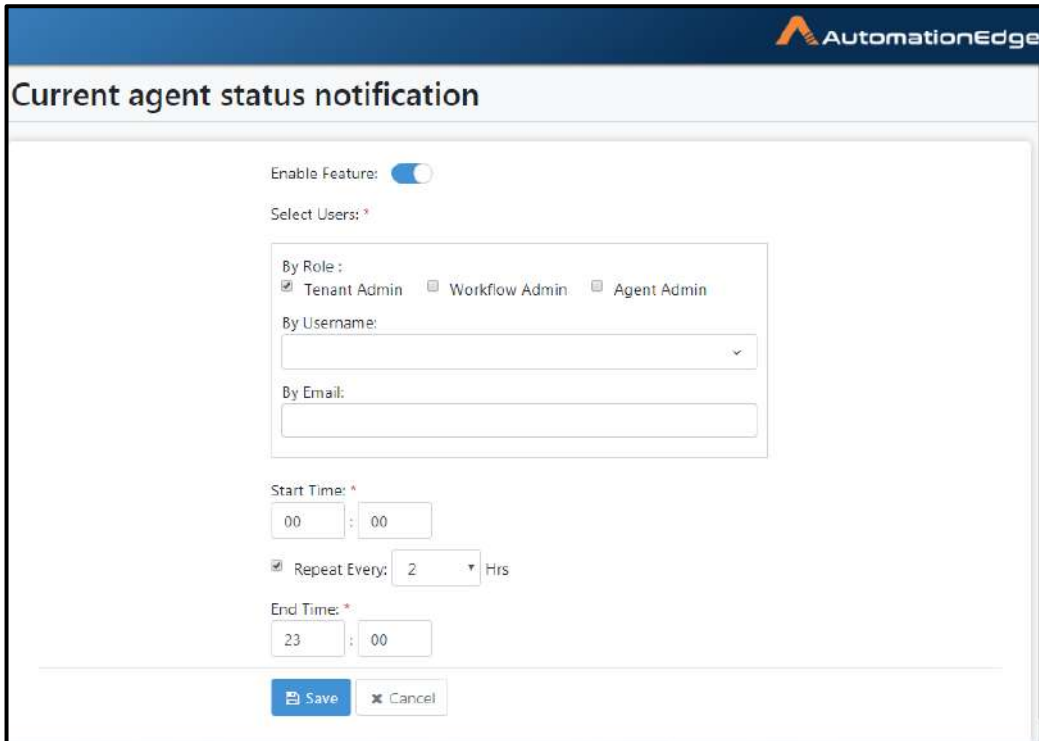
Notification Feature	Status	Actions
Pending Requests	Enabled	
Workflow Create and Update	Enabled	
Credential Create, Update and Expiry	Enabled	
Current Agent Status	Disabled	
Agent Not Working	Disabled	
Unlock User	Disabled	
Agent Machine Usage Warning	Disabled	
Integration Service Status	Disabled	

Figure 109a: Add Email Notification for Current Agent Status

3. Click the toggle to enable the feature.
4. Choose a time in Start time. Please provide end time if interval is non zero.
5. Select roles, specify AutomationEdge usernames or emails to receive notifications.
6. Click Save.



The screenshot shows the 'Current agent status notification' configuration interface. At the top, there is a blue header with the AutomationEdge logo. Below the header, the title 'Current agent status notification' is displayed. The main content area contains the following elements:

- Enable Feature:** A toggle switch that is currently turned on (blue).
- Select Users:** A dropdown menu with a downward arrow.
- By Role:** Three checkboxes: Tenant Admin, Workflow Admin, and Agent Admin.
- By Username:** A text input field with a dropdown arrow.
- By Email:** A text input field.
- Start Time:** Two input fields showing '00' and '00'.
- Repeat Every:** A checked checkbox, a text input field showing '2', and a dropdown menu showing 'Hrs'.
- End Time:** Two input fields showing '23' and '00'.
- Buttons:** A blue 'Save' button and a grey 'Cancel' button.


Figure 109b: Configurations for enabling Current Agent Status

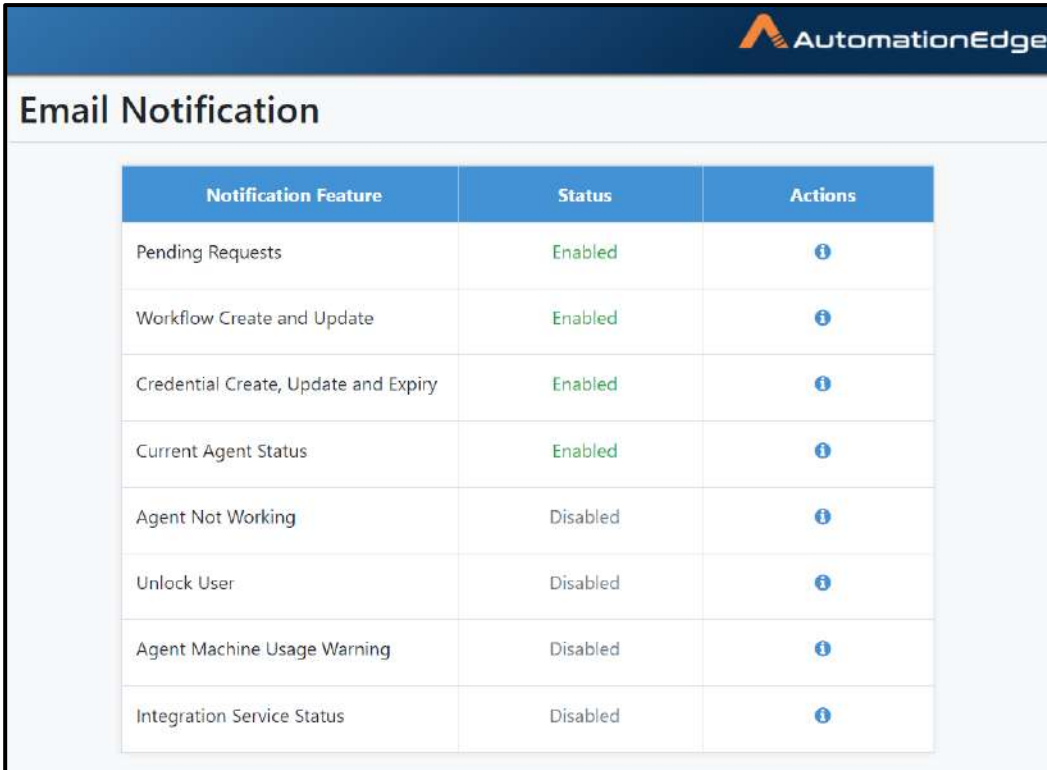
7. A message displays showing Notification Configuration saved successfully.
8. An email about Current Agent Status is sent to the configured users in the Notification settings.

17.4.2.5 Agent Not Working (Unknown/Dead)

If agent goes to unknown state or is stopped by Administrator, configure Agent Not Working to send email notification. The Notification can be sent to all Tenant Administrators, Workflow Administrators and configured email ids.

Following are the steps to configure Agent not working,

1. Go to the Settings menu and Email Notification sub-menu.
2. Click the Details icon () next to Agent Not Working.











Notification Feature	Status	Actions
Pending Requests	Enabled	
Workflow Create and Update	Enabled	
Credential Create, Update and Expiry	Enabled	
Current Agent Status	Enabled	
Agent Not Working	Disabled	
Unlock User	Disabled	
Agent Machine Usage Warning	Disabled	
Integration Service Status	Disabled	

Figure 110a: Email Notification for Current

3. The Agent not working notification page appears as seen below.
4. Click the toggle to enable the feature, select one or more roles, users and specify emails. Click Save.

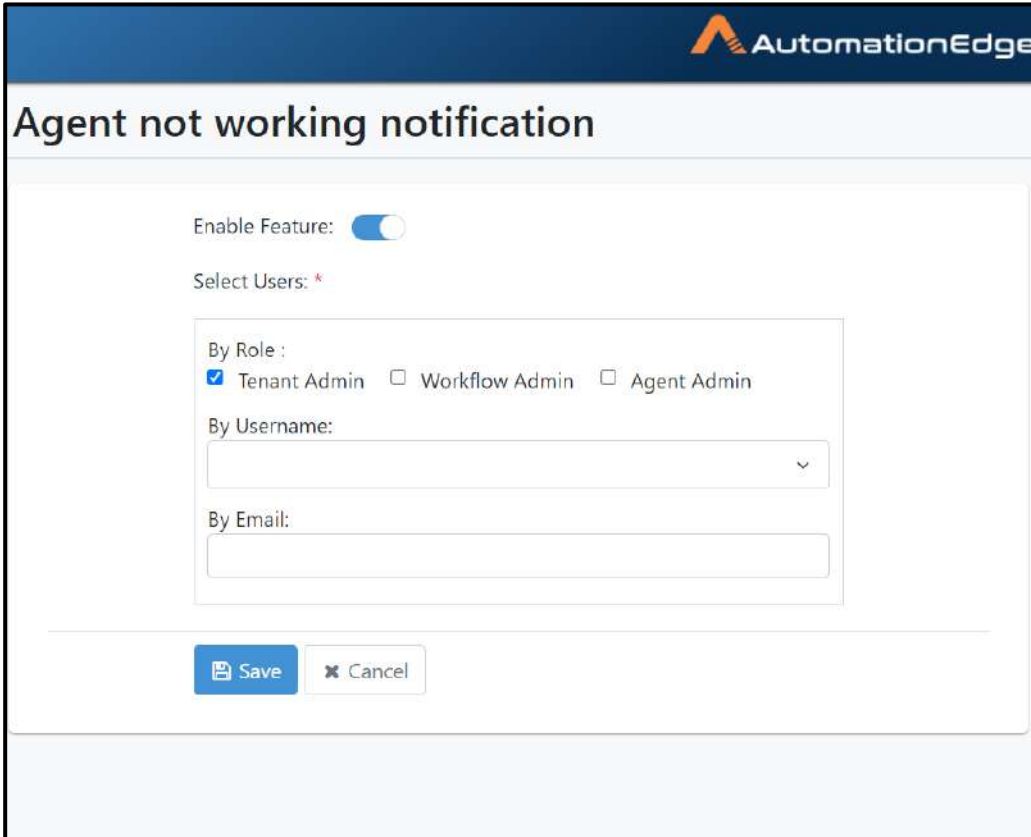


Figure 110b: Agent Not Working Notification Configuration

5. A message displays showing Notification Configuration saved successfully.
6. An email about Current Agent status such as Agent Stopped, Agent gone to Unknown Status is sent to all the users configured in the Notification settings.

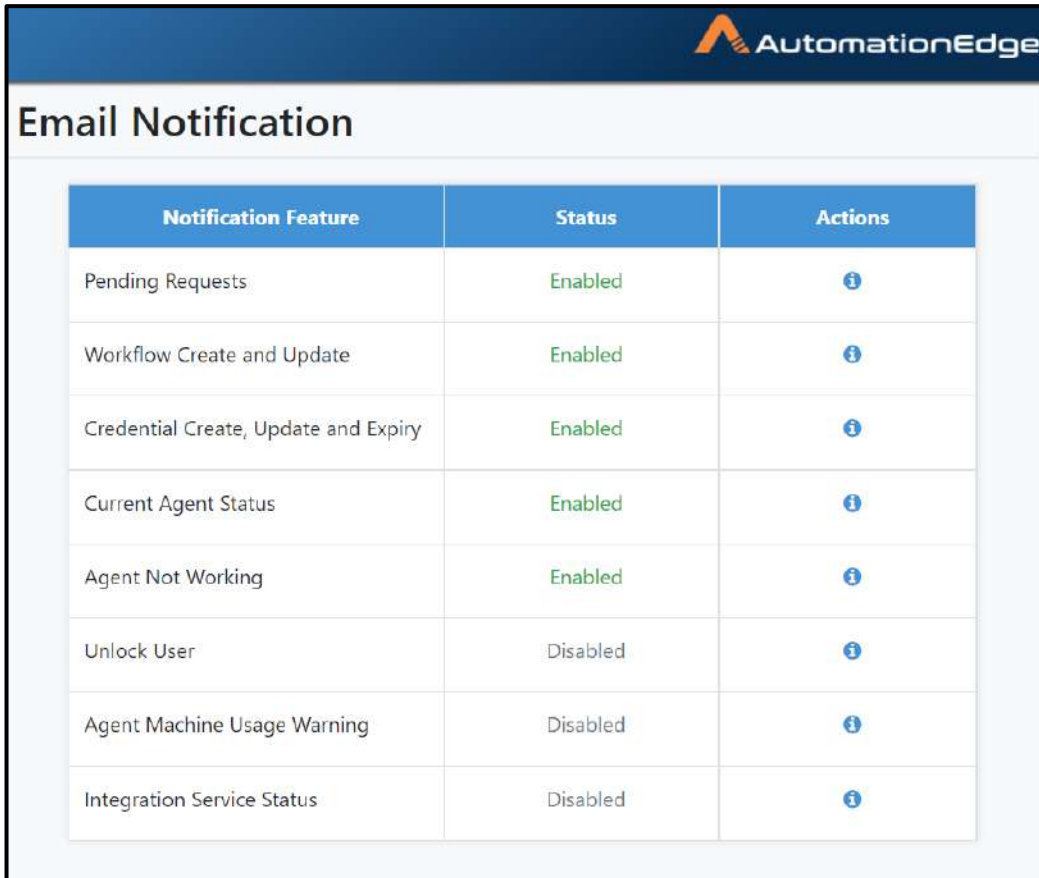
17.4.2.6 Unlock User

When a user account is unlocked an email is sent to the user with the new password. SMTP should be configured for this.

Following are the steps to configure:

1. Go to the Settings menu and Email Notification sub-menu.

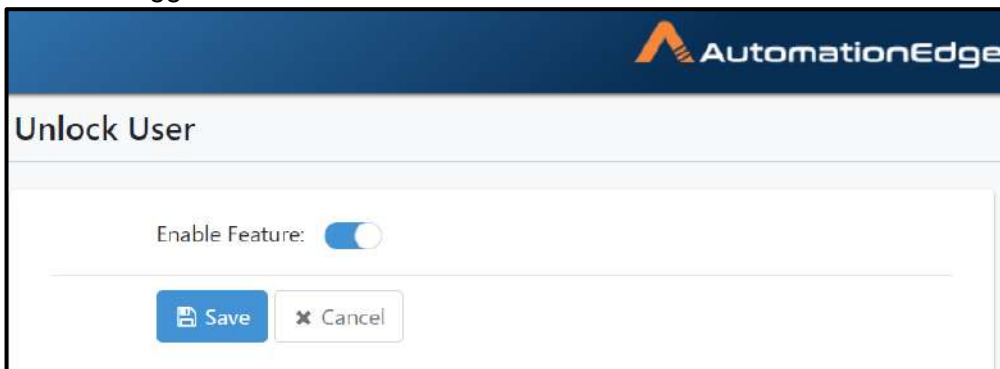
- Click the Details icon (i) next to Unlock User.



Notification Feature	Status	Actions
Pending Requests	Enabled	i
Workflow Create and Update	Enabled	i
Credential Create, Update and Expiry	Enabled	i
Current Agent Status	Enabled	i
Agent Not Working	Enabled	i
Unlock User	Disabled	i
Agent Machine Usage Warning	Disabled	i
Integration Service Status	Disabled	i

Figure 111a: Configure Email Notification for Reset Password

- The Unlock User notification configuration page appears.
- Click the toggle to enable the feature. Click Save.



AutomationEdge

Unlock User

Enable Feature:

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


Figure 111b: Enable Email Notification for Reset Password

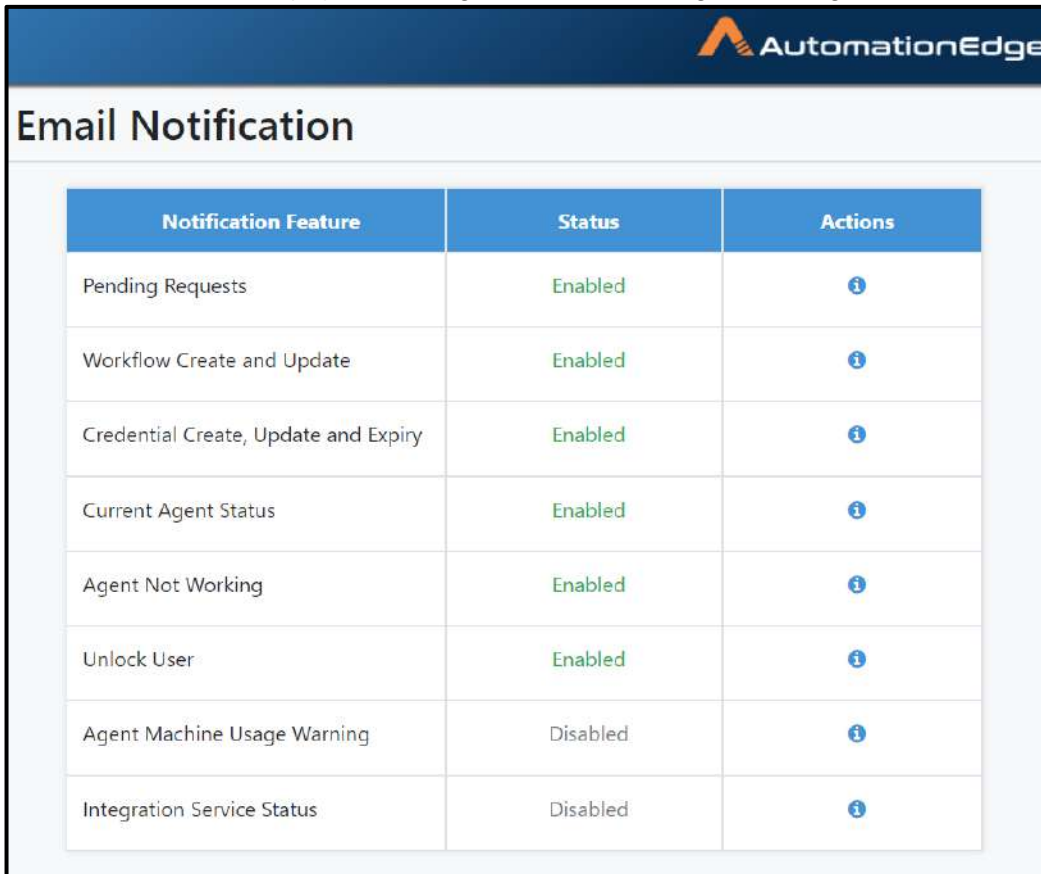
- A message displays showing Notification Configuration saved successfully.
- With this notification setting an email will be to sent to any users unlocked, with the new password.

17.4.2.7 Agent Machine Usage warning

You can configure 'Agent Not Working' to send email notification, if machine usage in terms of CPU, disk usage, memory usage and Heap usage exceeds the threshold set under Agent->Agent Settings. The Notification can be sent to all Tenant Administrators, Workflow Administrators and configured email ids.

Following are the steps to configure Agent not working,

1. Go to the Settings menu and Email Notification sub-menu.
2. Click the Details icon () next to Agent Machine Usage Warning.











Notification Feature	Status	Actions
Pending Requests	Enabled	
Workflow Create and Update	Enabled	
Credential Create, Update and Expiry	Enabled	
Current Agent Status	Enabled	
Agent Not Working	Enabled	
Unlock User	Enabled	
Agent Machine Usage Warning	Disabled	
Integration Service Status	Disabled	

Figure 110a: Email Notification for Current Agent Status

3. The Agent Machine Usage Warning page appears as seen below.
4. Click the toggle to enable the feature.
5. Select users for notification by role, username or email. Click Save.

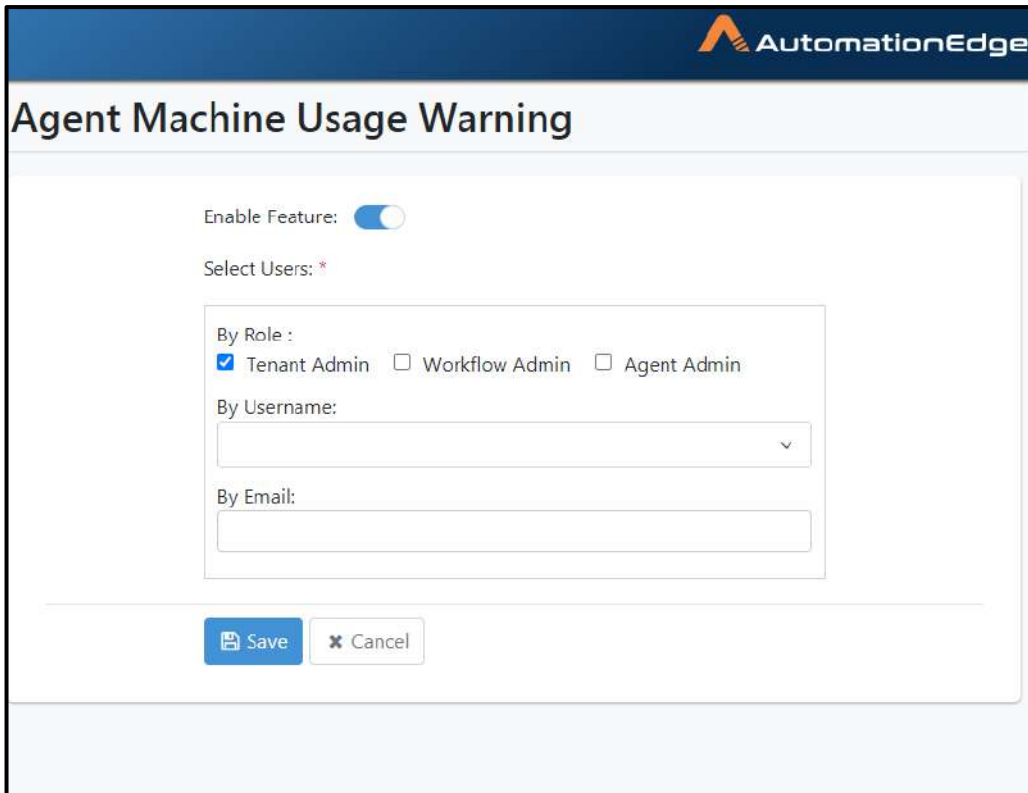


Figure 110b: Agent Not Working Notification Configuration

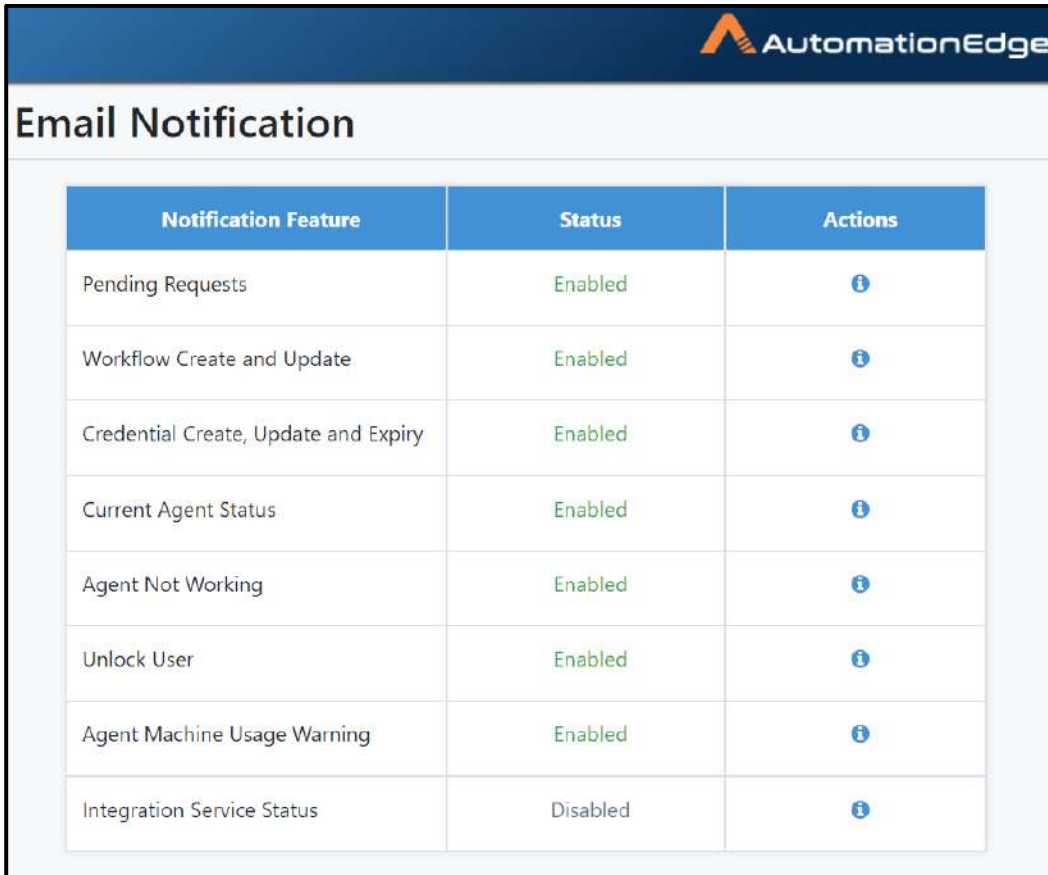
6. A message displays showing Notification Configuration saved successfully.

17.4.2.8 Integration Status

Configure 'Integration Status' to send email notification, if an Integration Service is added, updated or deleted. The Notification can be sent to all Tenant Administrators, Workflow Administrators and configured email ids.

Following are the steps to configure Agent not working,

1. Go to the Settings menu and Email Notification sub-menu.
2. Click Add (+) next to Integration Service Status.



Notification Feature	Status	Actions
Pending Requests	Enabled	i
Workflow Create and Update	Enabled	i
Credential Create, Update and Expiry	Enabled	i
Current Agent Status	Enabled	i
Agent Not Working	Enabled	i
Unlock User	Enabled	i
Agent Machine Usage Warning	Enabled	i
Integration Service Status	Disabled	i

Figure 111a: Email Notification for Integration Service status

3. The Integration status notification page appears as seen below.
4. Click the toggle to enable the feature.
5. Select users for notification by role, username or email. Click Save.

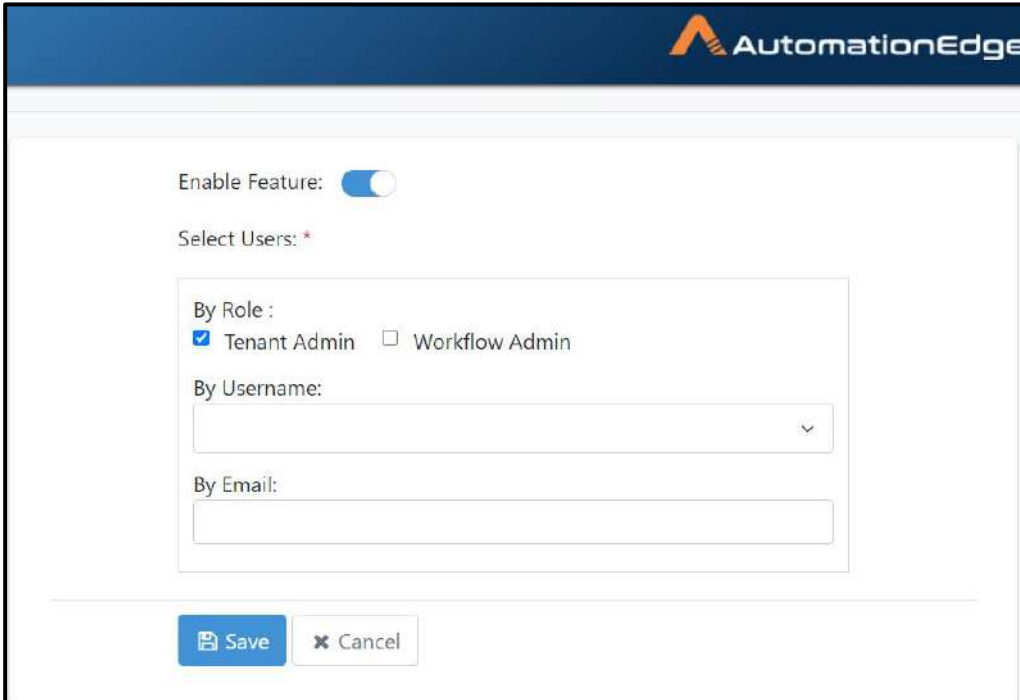


Figure 111b Integration Services Setup Notification Configuration

6. A message displays showing Notification Configuration saved successfully.

Note: In addition, the following notification settings can be configured at workflow level

1. Workflow request fails

Enable and configure this setting to receive email notification when workflow execution (request) fails. Email is sent to the recipients included in the workflow configuration.

2. Workflow request taking longer time to run

Enable and configure this setting to receive email notification when the workflow execution time exceeds the 'Maximum completion time', specified in the workflow configuration. Email is sent to the recipients included in the workflow configuration.

17.5 Proxy Settings

Proxy settings can be done at

- Tenant Level
- Individual Agent Level
- Process Studio Level manually

Proxy setting at Tenant level

Proxy Settings can be done on Proxy Settings menu on AutomationEdge UI.

Proxy setting at Agent level

Agent uses Proxy settings done at Tenant level, or Proxy Settings need to be done while downloading Agent in AutomationEdge UI or manually by copying <Tenant Name>-proxy-config.properties file to Agent\conf folder. Proxy settings are stored in the database or in a file <Tenant Name>-proxy-config.properties.

- If Proxy Settings are set at the Tenant level, by default these settings are displayed in AE UI during Agents download. You may accept or overwrite these settings.
- Proxy can also be set during Agent download. If Proxy is specified during Agent download it takes precedence over the options above.
- Proxy can also be set at agent level manually by copying <Tenant Name>-proxy-config.properties in the Agent/conf directory.
- If AutomationEdge server is upgraded from versions below 5.3.0 to 5.3.0 and above there are two scenarios for Agent upgrade.
 - Running Agents: If Agent is running during AutomationEdge upgrade it goes for auto upgrade. Since there is no Proxy configuration yet the Agent does not pick up any Proxy settings and Proxy settings need to be done manually.
 - Stopped Agents: If Agent is stopped during AutomationEdge upgrade and Proxy settings are done on server and Agent is started it picks up the Proxy settings.
- If at any later point of time, there are changes in proxy server configuration then users have to update the existing configuration at server side and download the new configuration file and replace it into already downloaded agents manually. Once the modified configuration file is replaced, agent needs to be restarted. Newly downloaded agents will have the updated proxy configuration if opt for.

Proxy setting at Process Studio level

Proxy settings at Process Studio level are done manually. Proxy settings need to be downloaded from Proxy Settings UI or Agent Download UI.

- Proxy in Process Studio is set manually, by copying <Tenant Name>-proxy-config.properties in the Process Studio Distribution/conf directory.
- If at any later point of time, there are changes in proxy server configuration then users have to update the existing configuration at server side and download the new configuration file and replace it into Process Studio distributions manually.

Proxy Settings provides two main options for Proxy settings, as listed in the table below.

Table 82: Proxy Settings options:

Add Proxy Button	<p>Click Add Proxy button for Automatic Configuration (dynamic) or Proxy Server configuration (static) at the Tenant level. Add Proxy is used to configure proxy and saves in the database. It also gives the option to download <Tenant Name>-proxy-config.properties for both dynamic and static configurations.</p> <p>It provides the following options,</p> <ul style="list-style-type: none"> ○ Automatic Configuration (Dynamic from Internet Options if available) ○ Proxy Server <ul style="list-style-type: none"> ✓ Use Proxy File from URL is checked (Dynamic) ✓ Use Proxy File from URL is unchecked (Static) ○ Download: For both Dynamic and Static Proxy, values are stamped into a file proxy-config.properties and downloaded on click of Download button. <p>For both static and dynamic and Proxy Server the following two Authentication Types are available: None or Simple.</p>
Download Button	<p>Click Download button for the following options,</p> <ol style="list-style-type: none"> 1. Automatic configuration to detect Internet Options proxy settings with none or simple authentication and download <Tenant Name>-proxy-config.properties. 2. Proxy Server to configure static or dynamic proxy at the Tenant level and download <Tenant Name>-proxy-config.properties <p>These options do not store proxy in database.</p>

The steps to configure Proxy Settings for each of the above options is described in the next three sections.

17.5.1 Add Proxy

You may add Proxy Settings for AutomationEdge server. In this section the steps to Add Proxy for the following Proxy options are discussed,

- No Proxy
- Automatic Configuration
- Proxy Server
- PAC (Proxy Auto-Configuration)

Following are the steps to add proxy settings,

1. Navigate to the Settings menu and Proxy Settings submenu.
2. Click Add Proxy button.

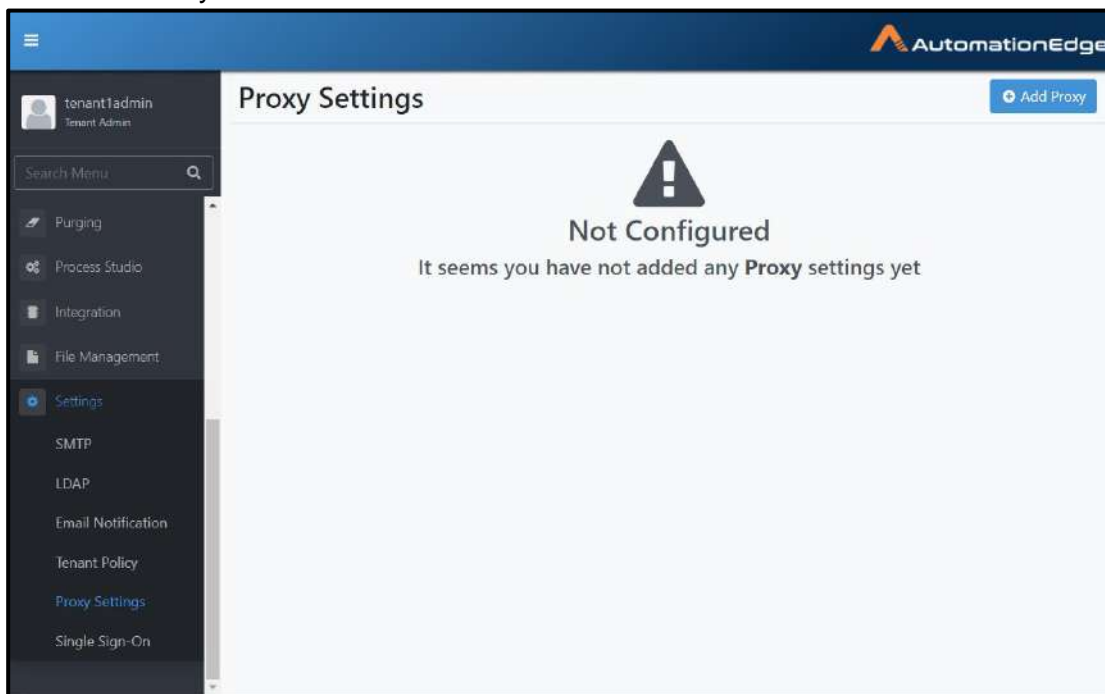


Figure 112a: Add Proxy Button

3. The default setting is No Proxy. Leave the default settings or modify as detailed in the next sections.

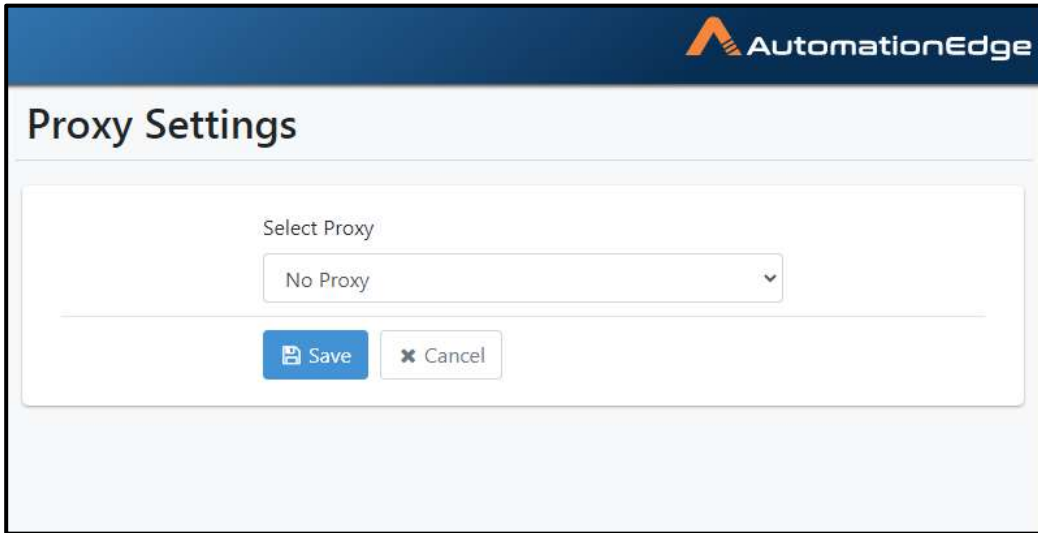


Figure 112b: Default is No Proxy

17.5.1.1 Add Proxy: No Proxy

In case the proxy is set at the system level and you do not want to use it, then use the option No Proxy. Following are the steps for the No Proxy option.

1. Navigate to the Settings menu and Proxy Settings submenu.
2. Click Add Proxy button.
3. The Proxy Settings page appears as seen below. The default Proxy is No Proxy.

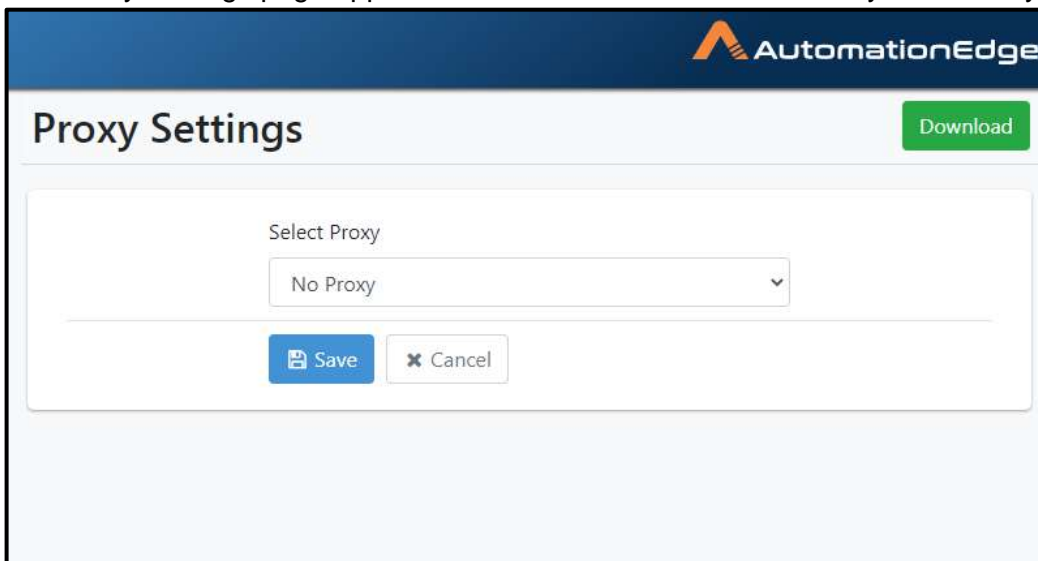


Figure 112c: Add No Proxy

4. In the Select Proxy drop down list select No Proxy. Click Save.

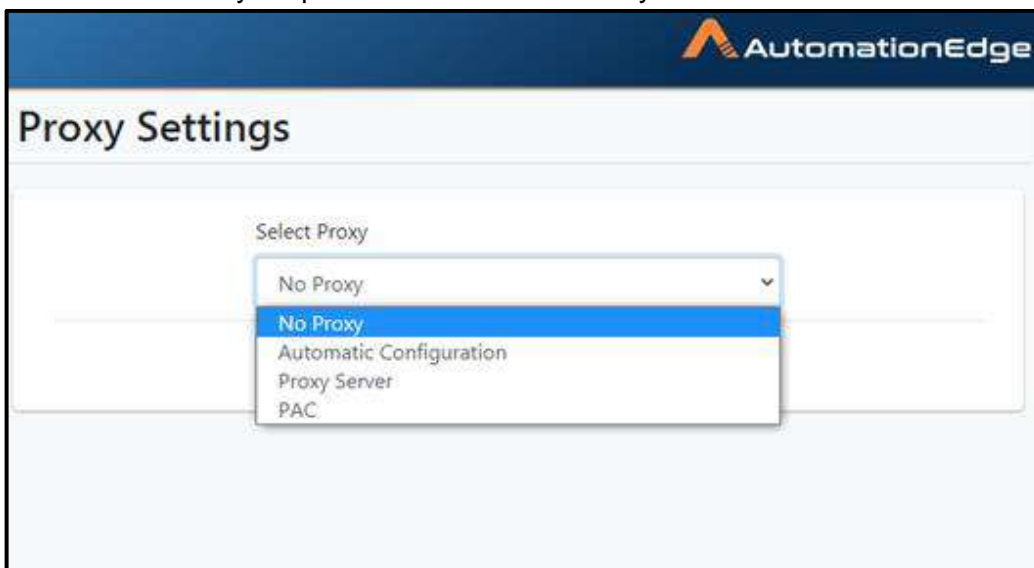


Figure 112d: Select No Proxy

5. Proxy Configuration saved successfully message appears.

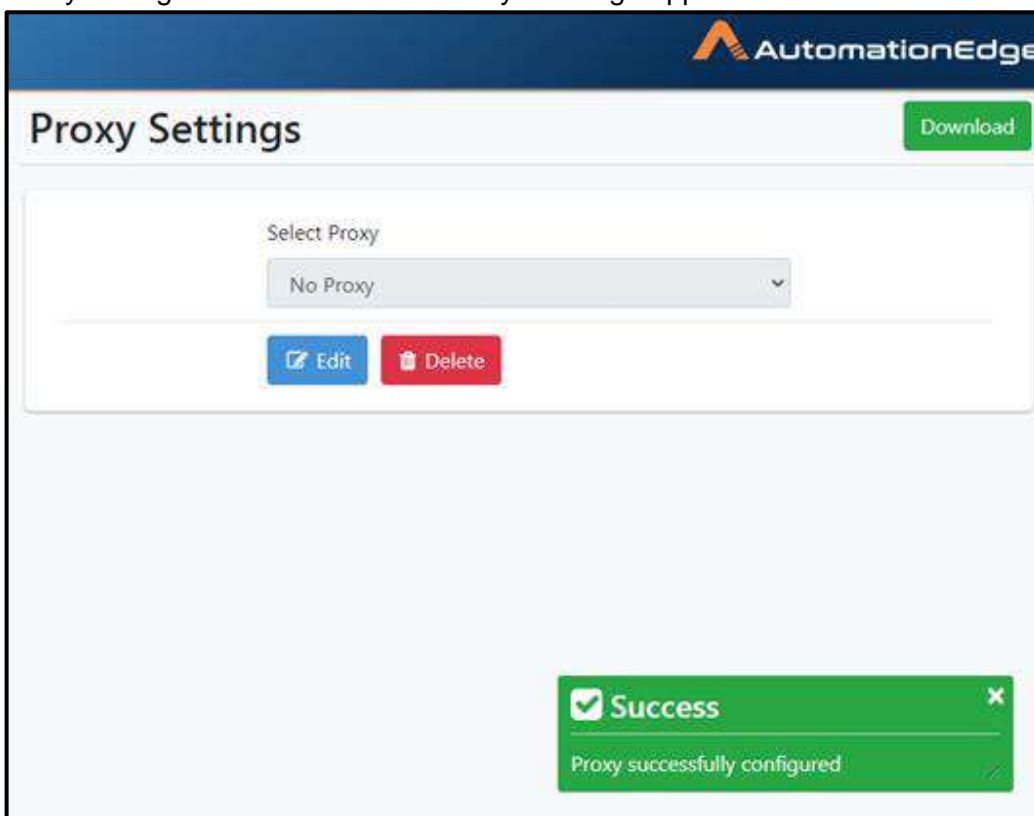


Figure 112e: No Proxy Saved successfully.

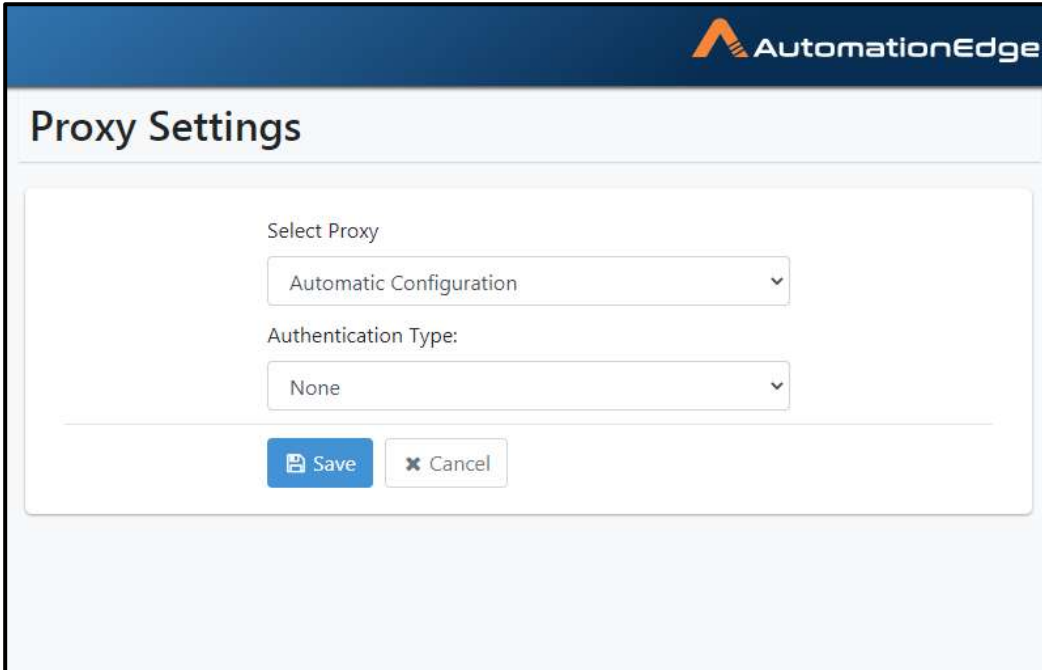
6. This completes the process of adding No Proxy.

17.5.1.2 Add Proxy: Automatic Configuration

Automatic Configuration detects proxy from Windows Internet options. In case of Linux environment Automatic configuration is not a valid option.

Following are the steps for Automatic Configuration.

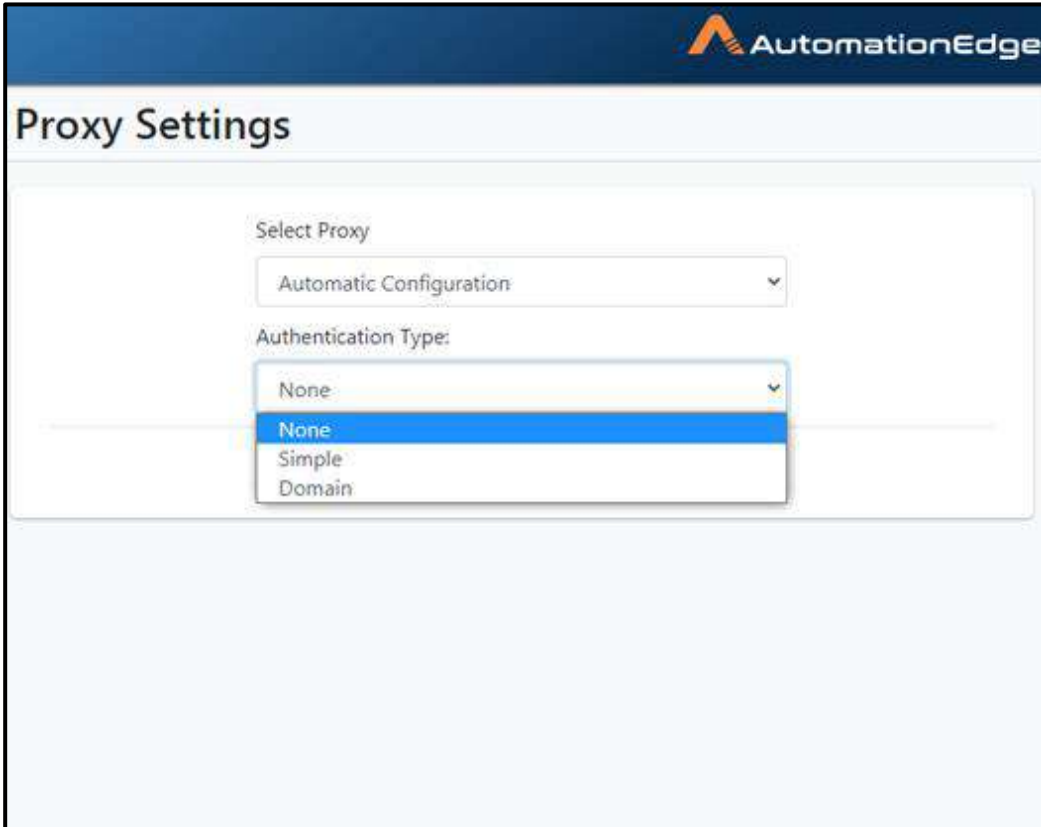
1. Navigate to the Settings menu and Proxy Settings submenu.
2. Click Add Proxy button.
3. In Proxy Settings page the default is No Proxy. Select Automatic configuration as seen below. You may leave Authentication type as None.



The screenshot shows the 'Proxy Settings' dialog box. The title bar is dark blue with the AutomationEdge logo. The main content area is white and contains two dropdown menus. The first dropdown is labeled 'Select Proxy' and has 'Automatic Configuration' selected. The second dropdown is labeled 'Authentication Type:' and has 'None' selected. Below the dropdowns are two buttons: a blue 'Save' button and a grey 'Cancel' button.

Figure 112f: Automatic Proxy with no Authentication

4. You may choose desired Authentication type from the dropdown list.
5. In case your Automatic Internet options proxy needs authentication you may select Simple or Domain Authentication from the dropdown list as shown below.

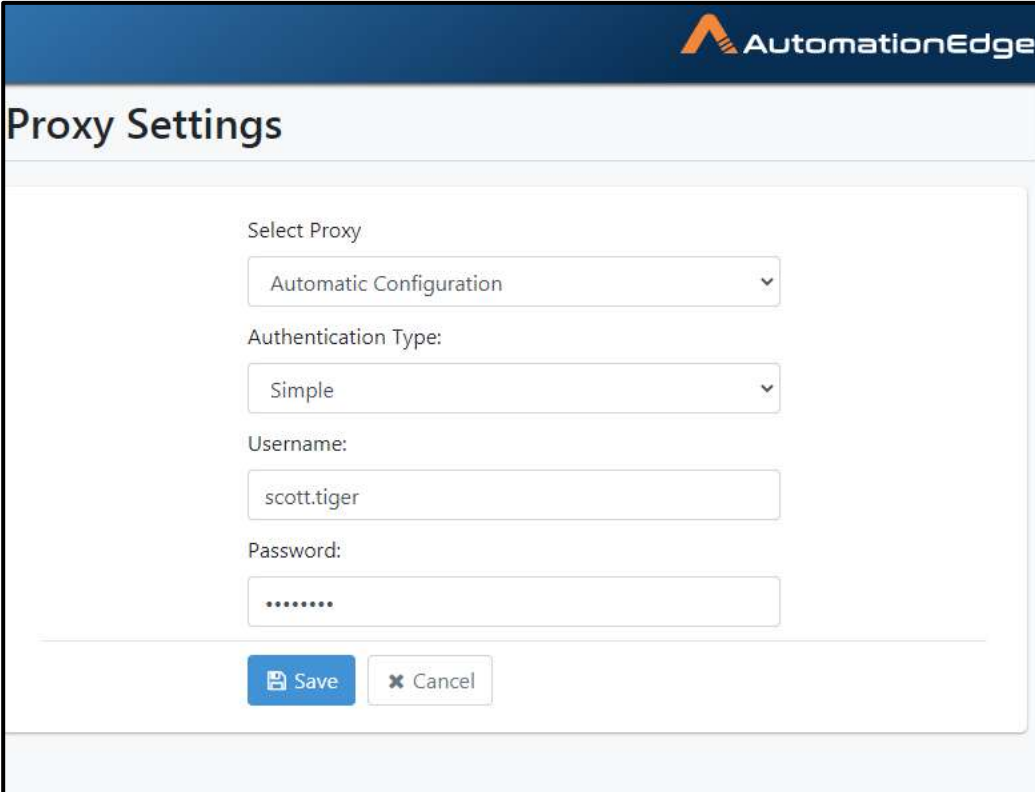


The screenshot shows the 'Proxy Settings' page in the AutomationEdge interface. At the top, there is a dark blue header with the AutomationEdge logo. Below the header, the title 'Proxy Settings' is displayed. The main content area contains two dropdown menus. The first is labeled 'Select Proxy' and has 'Automatic Configuration' selected. The second is labeled 'Authentication Type:' and is open, showing three options: 'None' (which is highlighted in blue), 'Simple', and 'Domain'.

Figure 112g: Authentication Options

6. If Simple is chosen provide Username and Password.

7. Provide Simple Authentication details as shown below. Click Save.



AutomationEdge

Proxy Settings

Select Proxy

Automatic Configuration

Authentication Type:

Simple

Username:

scott.tiger

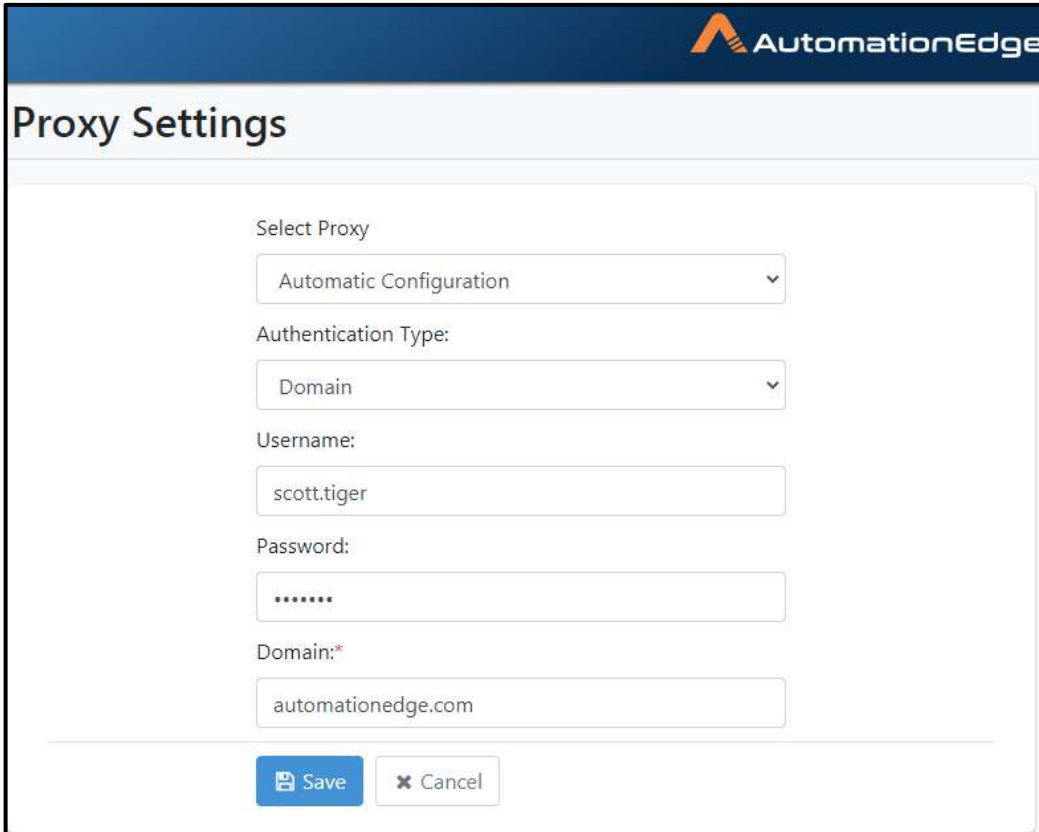
Password:

.....

Save Cancel

Figure 112h: Automatic Configuration with Simple Authentication

8. If Domain is chosen additionally provide the Proxy Server Domain.



AutomationEdge

Proxy Settings

Select Proxy

Automatic Configuration

Authentication Type:

Domain

Username:

scott.tiger

Password:

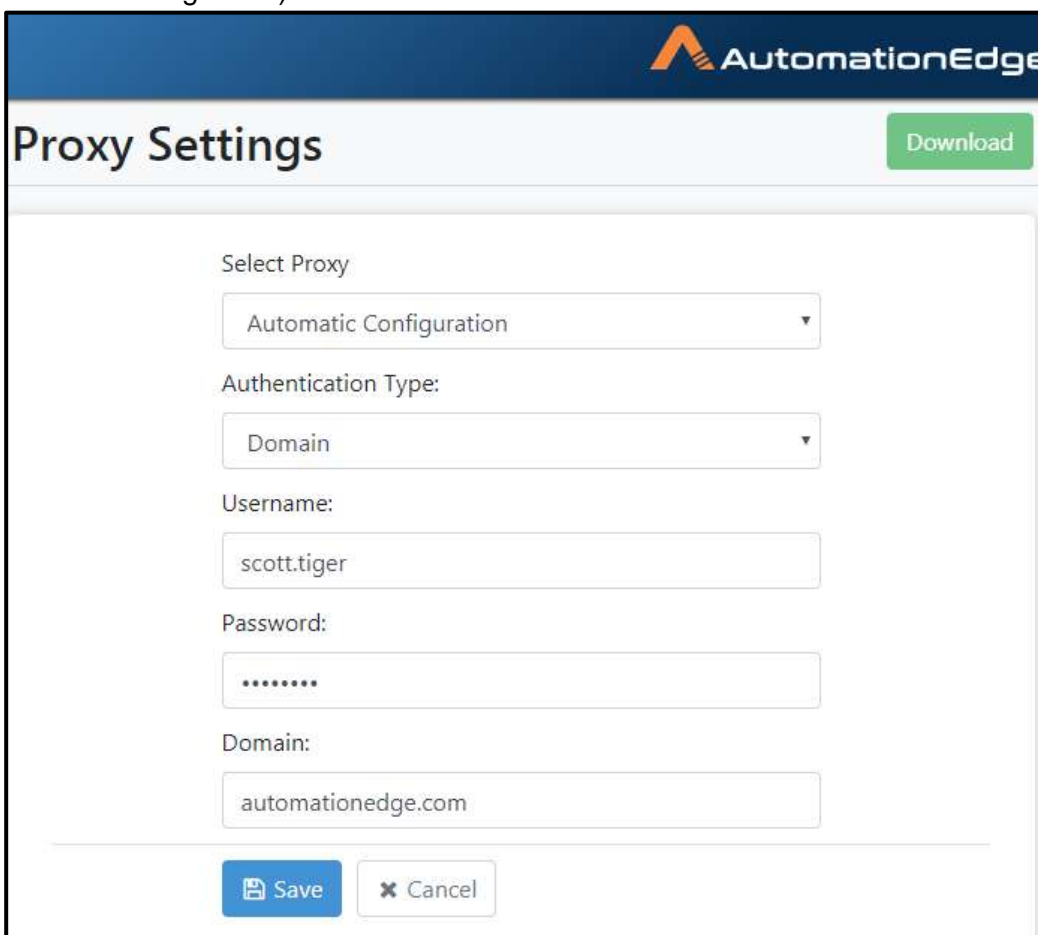
Domain:*

automationedge.com

Save Cancel

Figure 112i: Automatic Configuration with Domain

9. In case of Domain Authentication additionally provide the domain(e.g. automationedge.com). Click Save



AutomationEdge

Proxy Settings

Download

Select Proxy

Automatic Configuration

Authentication Type:

Domain

Username:

scott.tiger

Password:

.....

Domain:

automationedge.com

Save Cancel

Figure 112j: Automatic Configuration with Domain Authentication

10. The following screenshot shows a Simple configuration saved. Proxy successfully configured message appears as seen below.

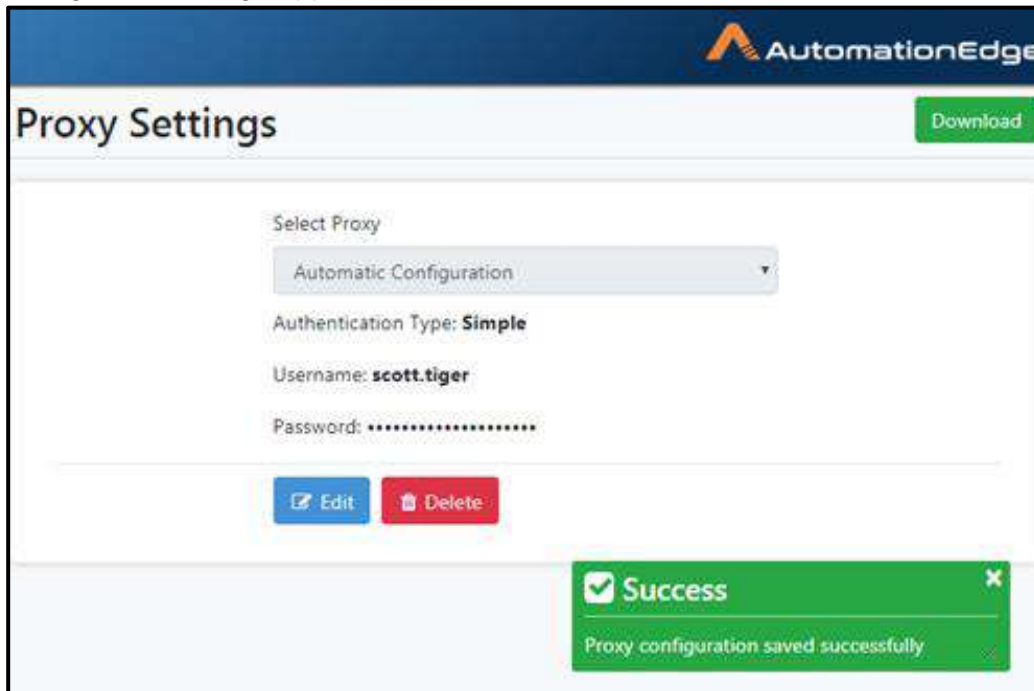


Figure 112k: Automatic Proxy Successfully Configured

11. This completes the process of Automatic configuration.

17.5.1.3 Add Proxy: Proxy Server

Following are the steps to configure proxy Proxy using static proxy details.

1. Navigate to Settings→Proxy Settings menu.
2. Click Add Proxy button.
3. The screen appears as shown below. Select Proxy Server from the Select Proxy dropdown.

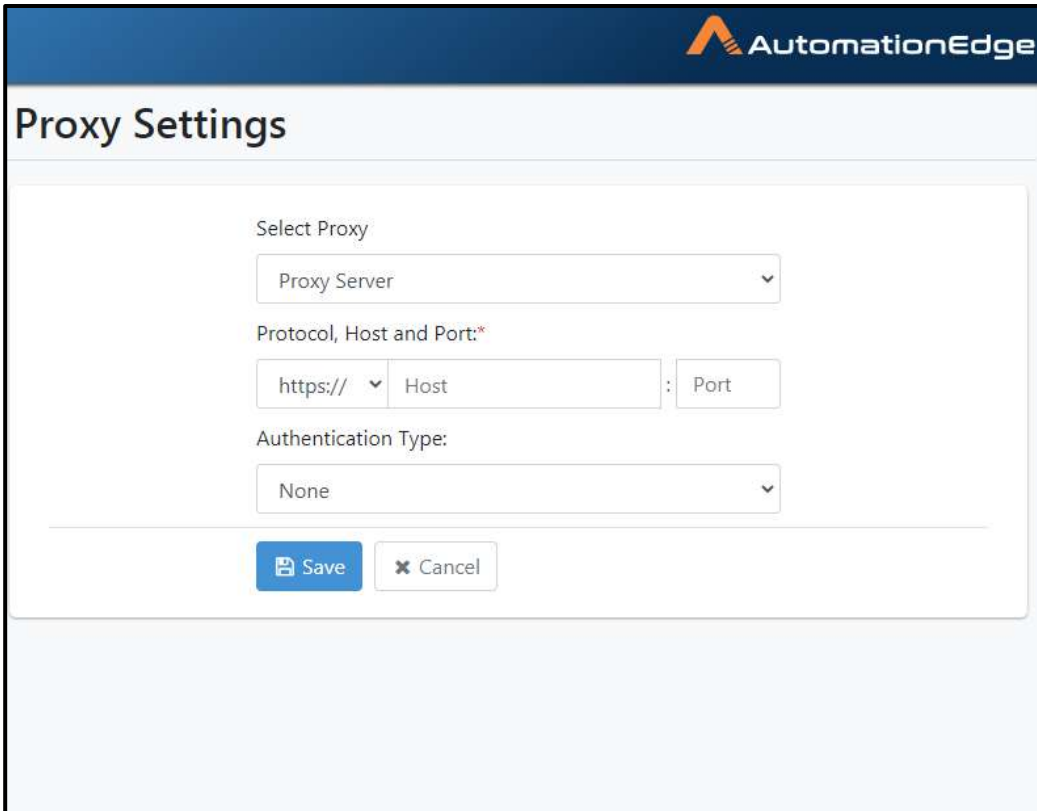
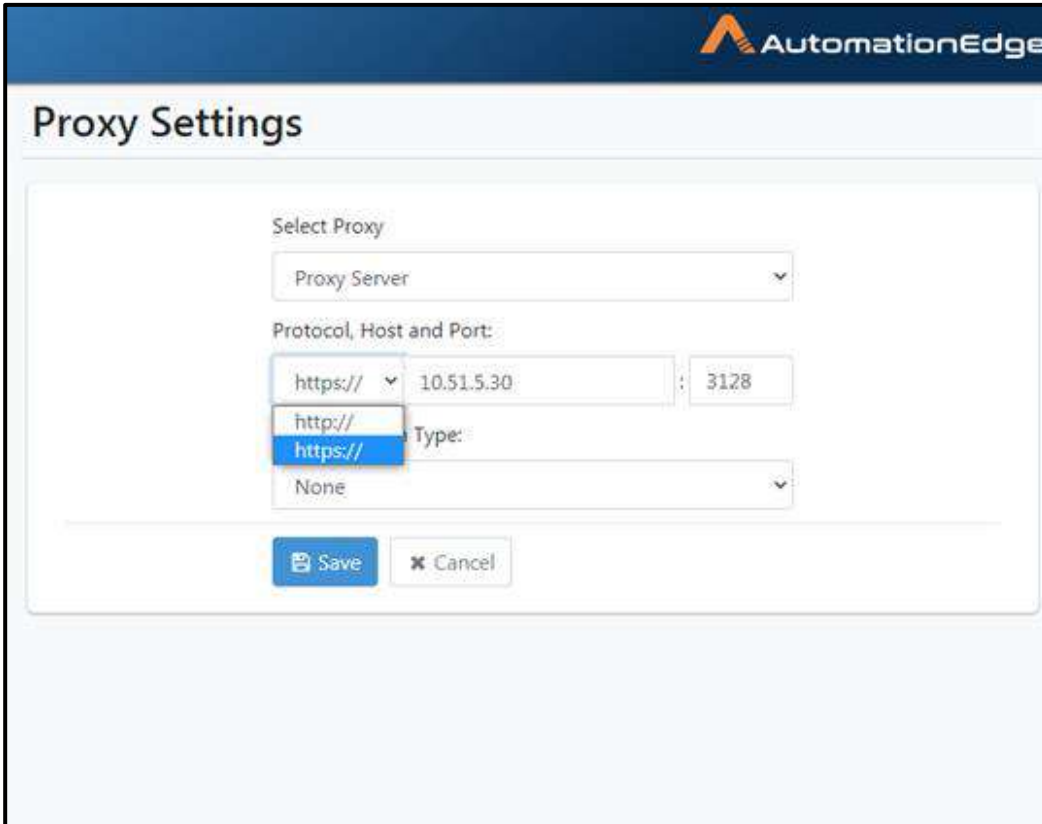


Figure 113a: Default Screen for Automatic Configuration

4. Choose the correct protocol, Host and Port as seen below for a static Proxy configuration.



AutomationEdge

Proxy Settings

Select Proxy

Proxy Server

Protocol, Host and Port:

https:// 10.51.5.30 : 3128

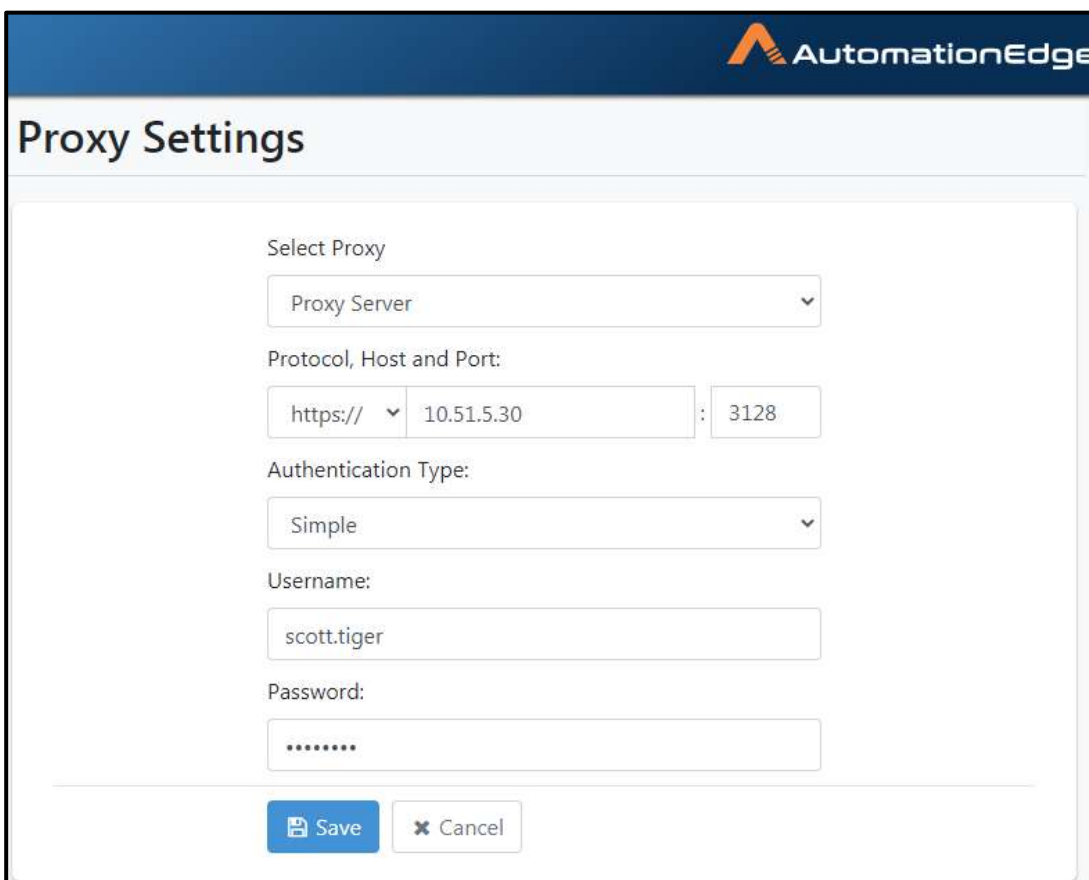
http://
https:// Type:

None

Save Cancel

Figure 113b: Select Protocol

5. You may choose Authentication type Simple as seen below. Provide Username and Password.



AutomationEdge

Proxy Settings

Select Proxy

Proxy Server

Protocol, Host and Port:

https:// 10.51.5.30 : 3128

Authentication Type:

Simple

Username:

scott.tiger

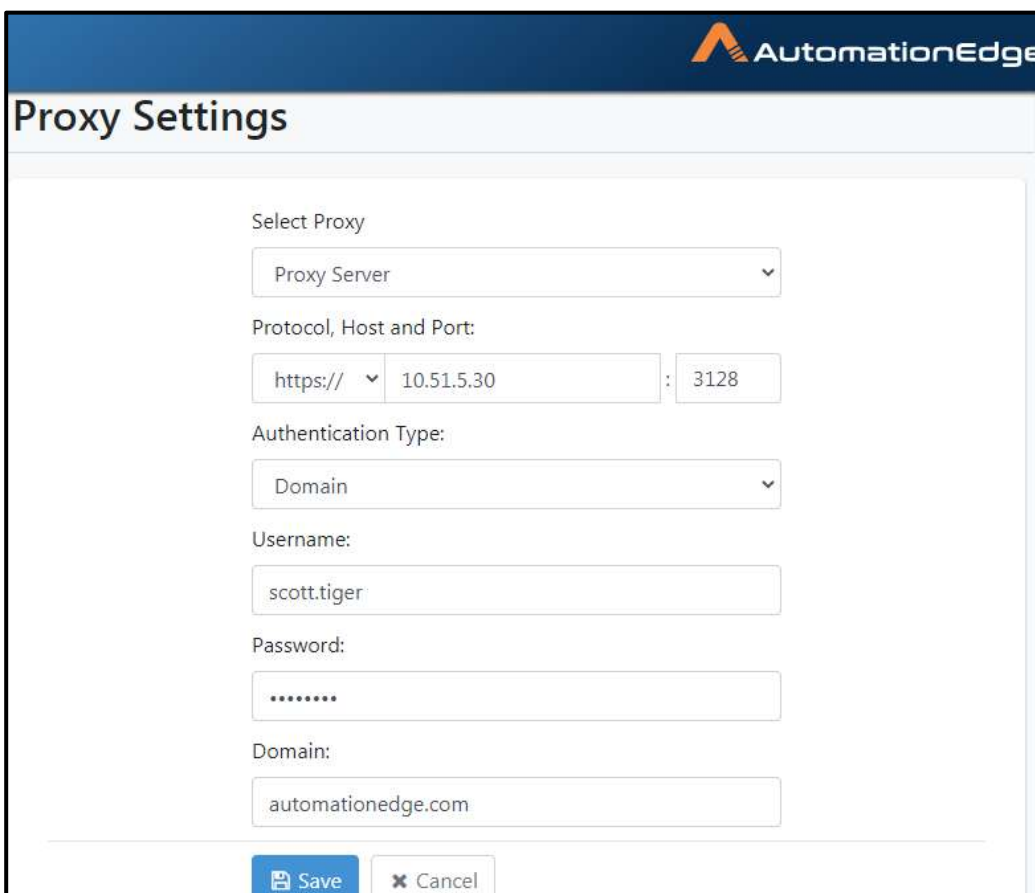
Password:

.....

Save Cancel

Figure 113c: Configure Simple Authentication

6. In case you select Authentication Type as Domain additionally provide Domain name. Click Save.



AutomationEdge

Proxy Settings

Select Proxy

Proxy Server

Protocol, Host and Port:

https:// 10.51.5.30 : 3128

Authentication Type:

Domain

Username:

scott.tiger

Password:

.....

Domain:

automationedge.com

Save Cancel

Figure 113d: Domain Authentication

7. Proxy successfully configured message appears.

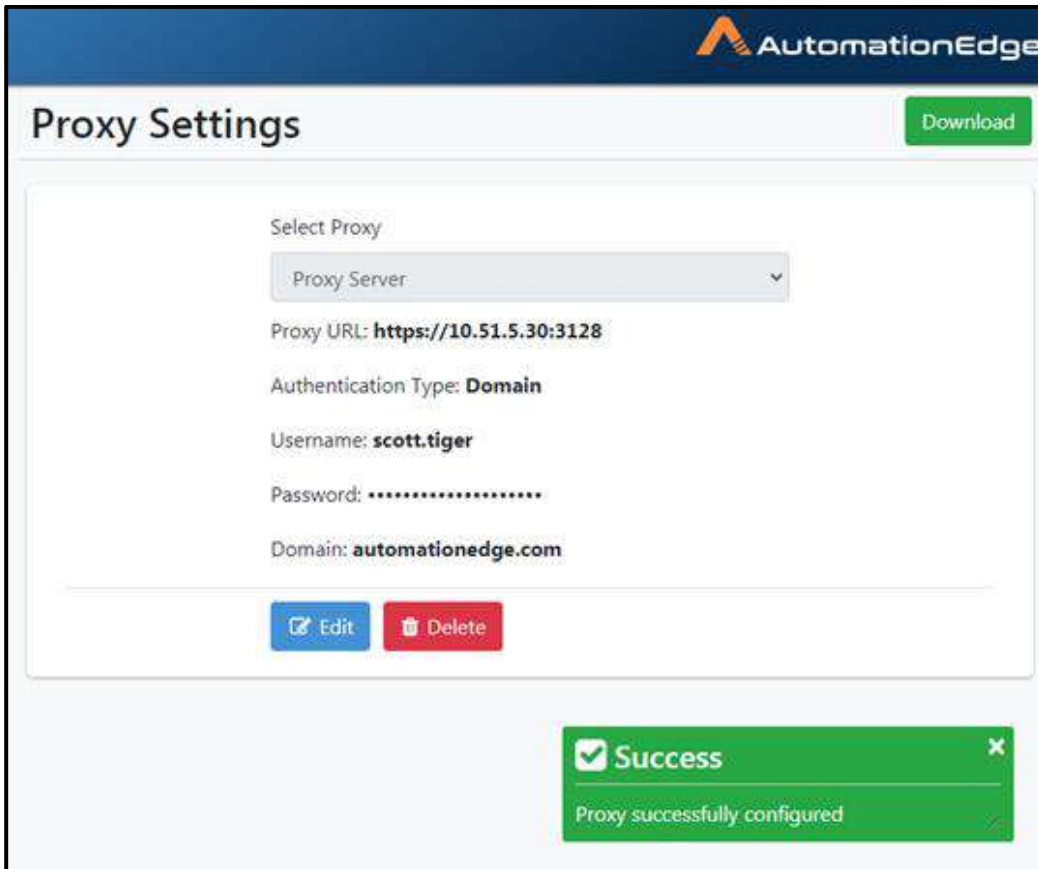


Figure 113e: Proxy Server successfully configured

8. This completes the process of setting a static Proxy Server.

17.5.1.4 Add Proxy: PAC

This option sets a Dynamic Proxy and you provide the PAC (proxy auto-config) file URL to set a Dynamic Proxy.

Following are the steps to configure Proxy settings using PAC file URL.

1. Navigate to Settings→Proxy Settings menu.
2. Click Add Proxy button.
3. Select Proxy as PAC.

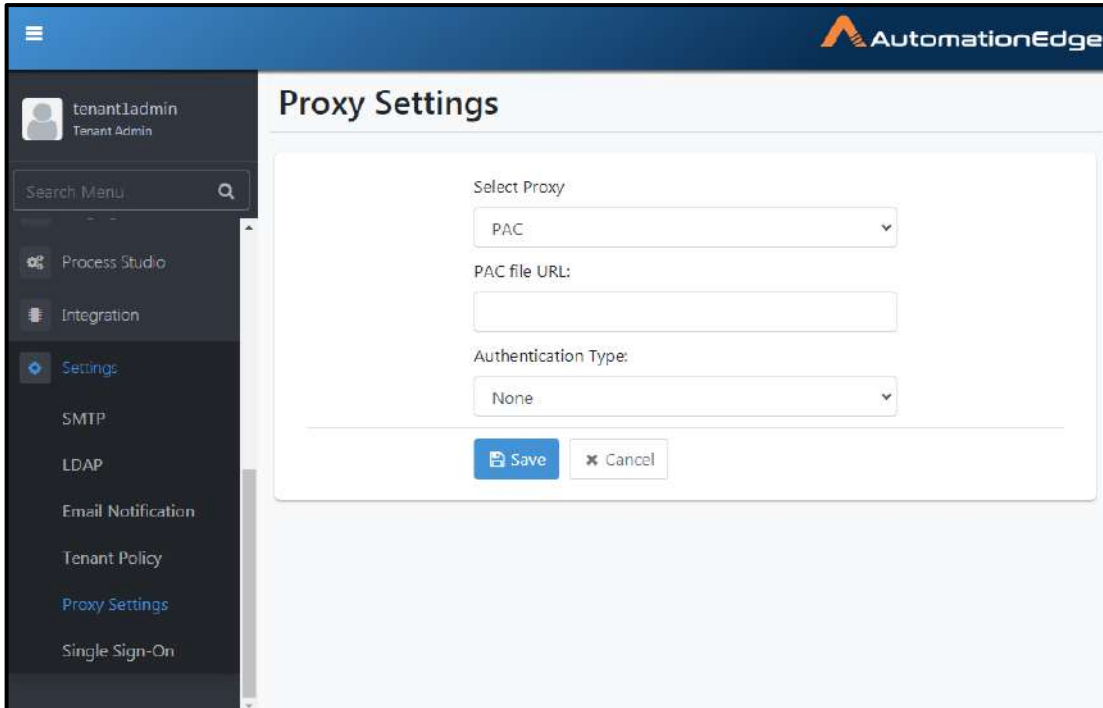
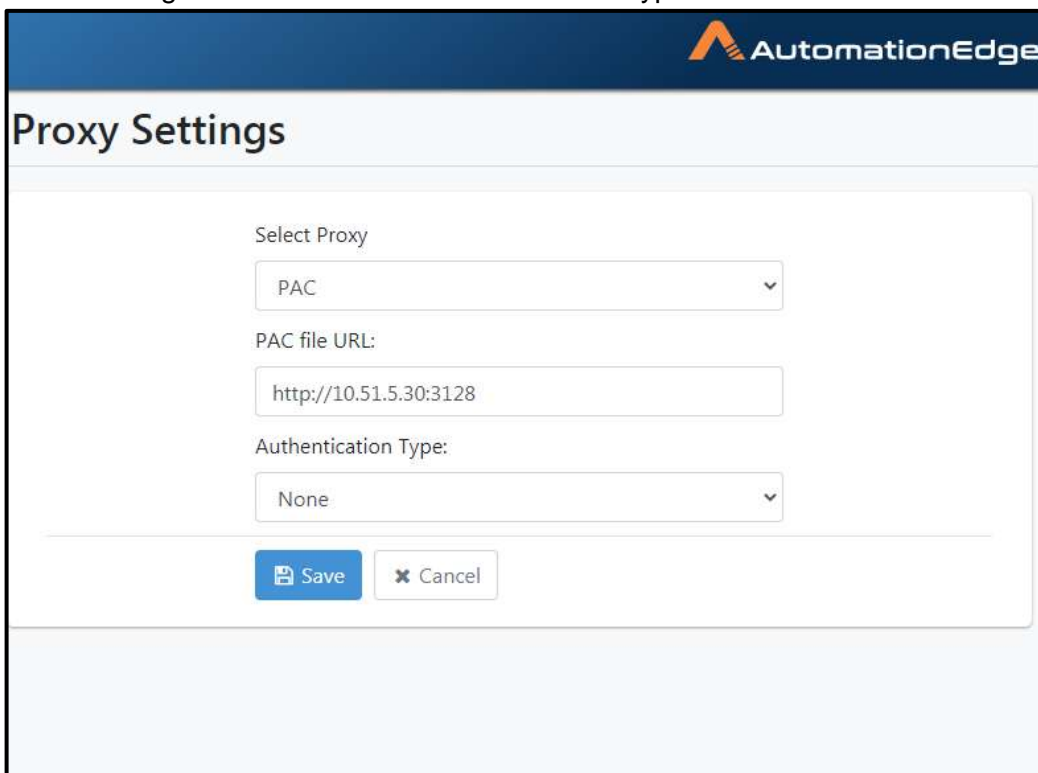


Figure 114a: Proxy auto-cofig(PAC)

4. Provide the URL for the proxy auto-config(PAC) file. Choose Authentication Type from None and Simple or Domain. Click Save.

5. The following screenshot shows Authentication Type None.



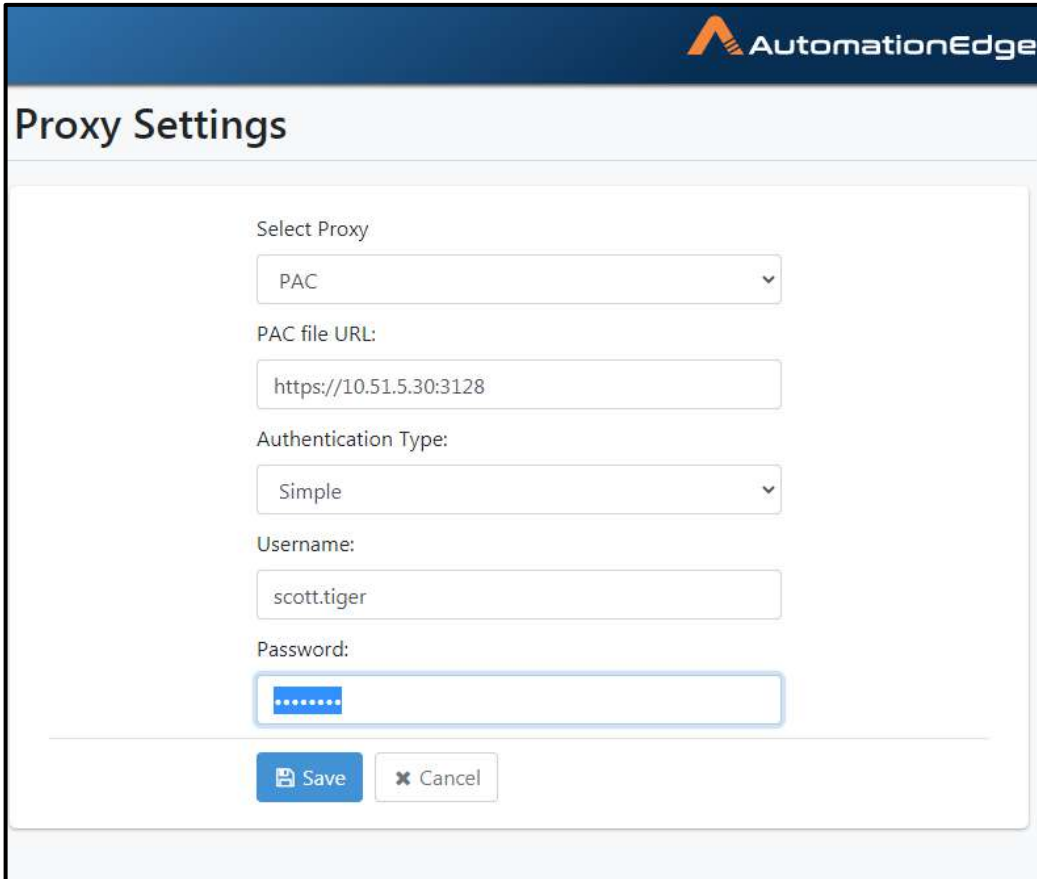
The screenshot shows a dialog box titled "Proxy Settings" with the AutomationEdge logo in the top right corner. The dialog contains the following fields:

- Select Proxy:** A dropdown menu with "PAC" selected.
- PAC file URL:** A text input field containing "http://10.51.5.30:3128".
- Authentication Type:** A dropdown menu with "None" selected.

At the bottom of the dialog, there are two buttons: "Save" (with a floppy disk icon) and "Cancel" (with an 'x' icon).

Figure 114b: PAC URL

6. The following screenshot shows details of Authentication Type Simple.



The screenshot displays the 'Proxy Settings' configuration page. At the top, the AutomationEdge logo is visible. The main heading is 'Proxy Settings'. Below this, there are several input fields and a dropdown menu:

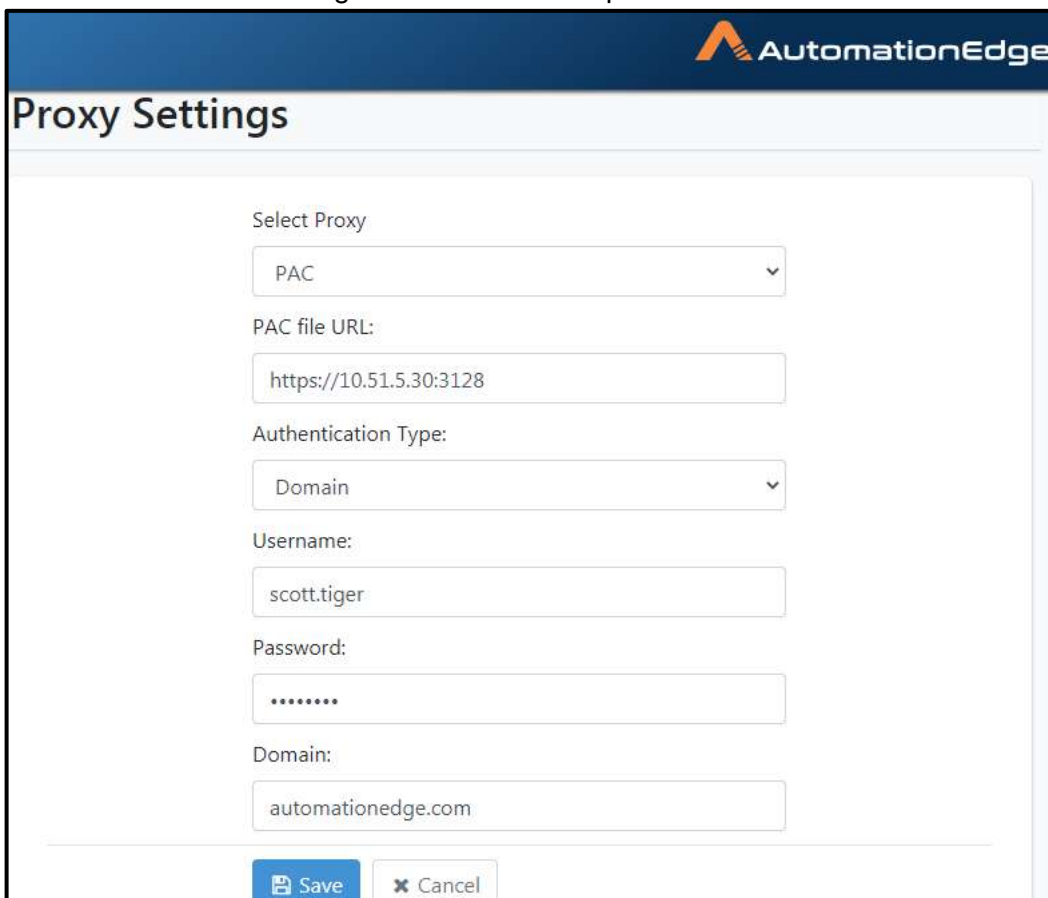
- Select Proxy:** A dropdown menu with 'PAC' selected.
- PAC file URL:** A text input field containing 'https://10.51.5.30:3128'.
- Authentication Type:** A dropdown menu with 'Simple' selected.
- Username:** A text input field containing 'scott.tiger'.
- Password:** A password input field with masked characters (dots).

At the bottom of the form, there are two buttons: a blue 'Save' button and a grey 'Cancel' button.

Figure 114c: Proxy Settings with PAC File from URL with Simple Authentication

7. The following screenshot shows details of Authentication Type Domain.

8. Click Save once the configurations details are provided.



AutomationEdge

Proxy Settings

Select Proxy

PAC

PAC file URL:

https://10.51.5.30:3128

Authentication Type:

Domain

Username:

scott.tiger

Password:

.....

Domain:

automationedge.com

Save Cancel

Figure 114d: Proxy Settings with PAC File from URL with Domain Authentication

9. Proxy successfully configured message appears as seen below.

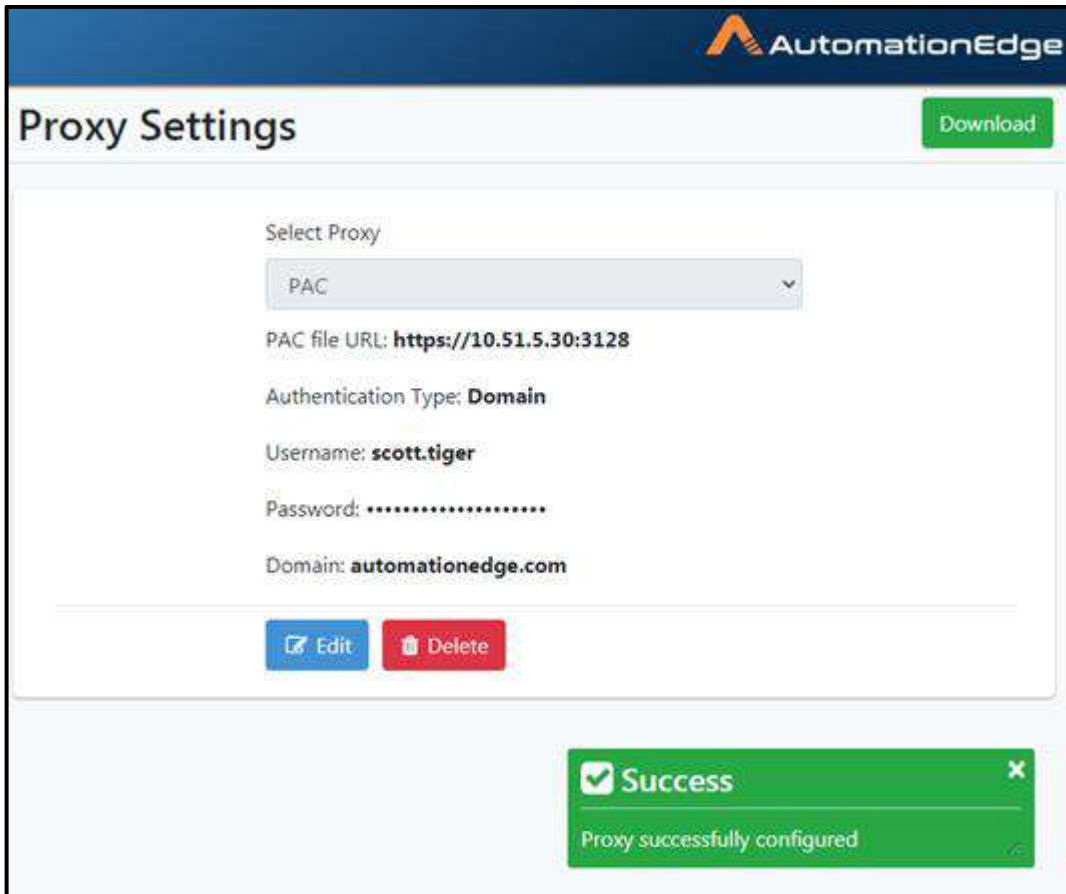


Figure 114e: Proxy Configuration with PAC File from URL Successful

10. This completes the process configuring proxy from PAC File URL.

17.5.2 Download Proxy Configuration file

1. Navigate to Settings→Proxy Settings
2. Once Proxy Configuration with any of the Proxy options (No Proxy, Automatic Configuration, Proxy Server or PAC) has been set up a Download button appears on the top right corner.
3. In the snapshot below we can see Automatic Proxy Configuration with Authentication Type Domain has been setup.
4. Click the download button on the top right corner.

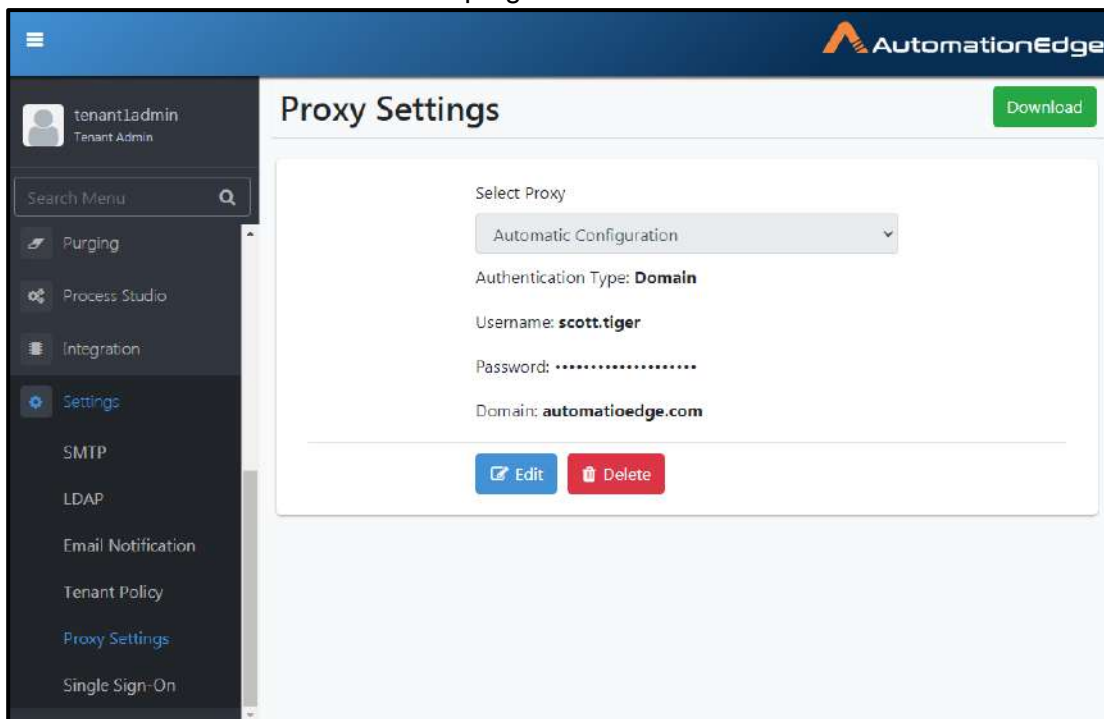


Figure 116a: Downloaded Proxy Configuration File

5. By default, you will see the file configuration same as the one already set on the screen.
6. You may use the already configured settings or change the configurations for the Configuration file to be downloaded.

7. To change configurations click on the Edit button. Note that all the fields are editable.

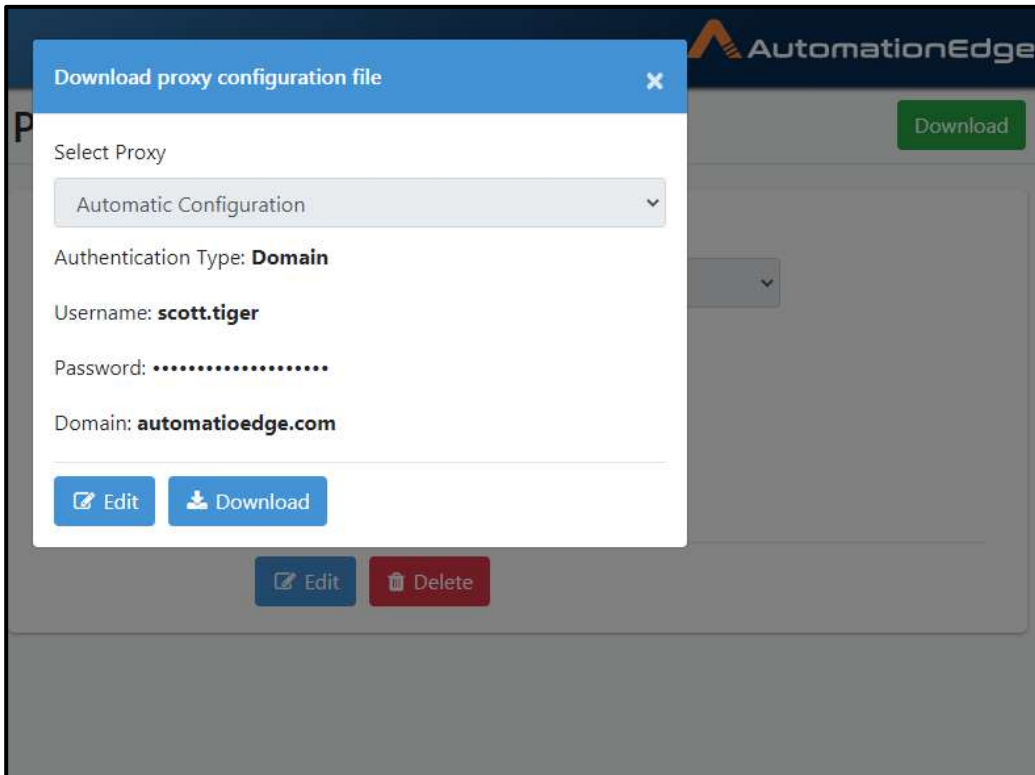


Figure 116b: Edit Proxy Configuration File

8. Make changes as desired. Click Download.

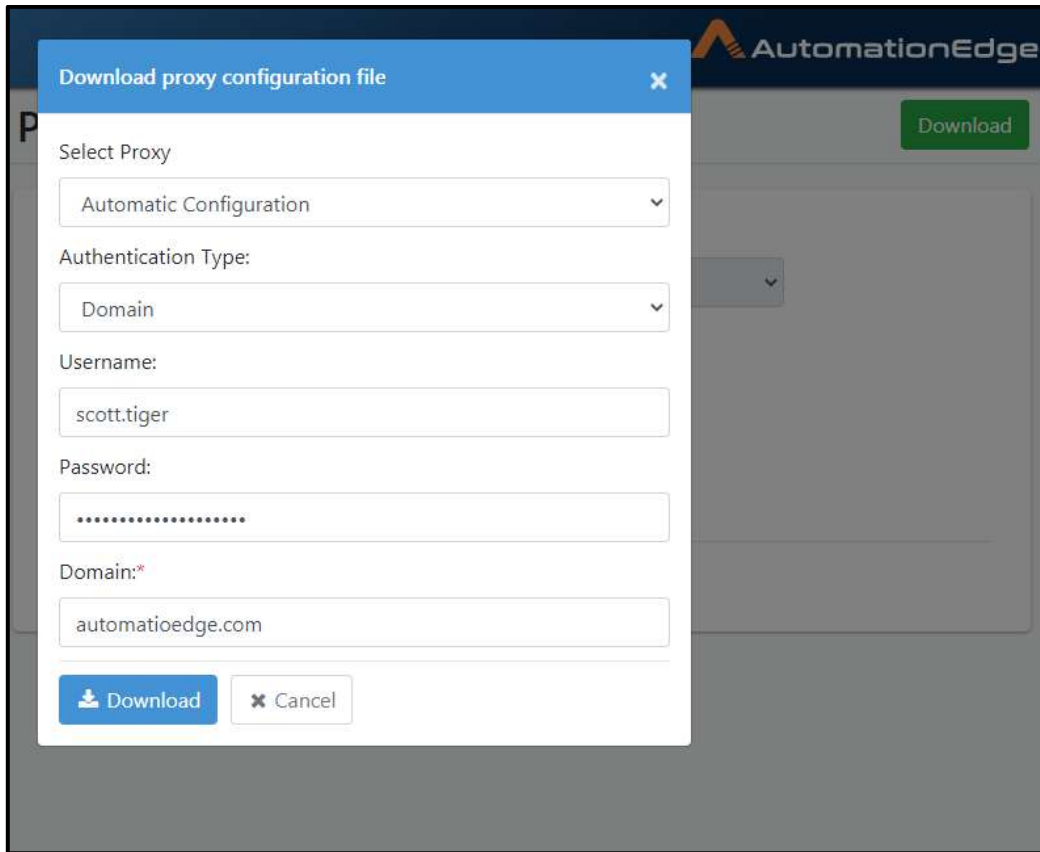


Figure 116c: Edit and Download Proxy Configuration file

9. Proxy configuration file <Tenant Name>-proxy-config.properties file is downloaded as seen below.
10. You may use the file to copy to <Agent>\conf or <Process Studio Distribution>\conf folders if desired.

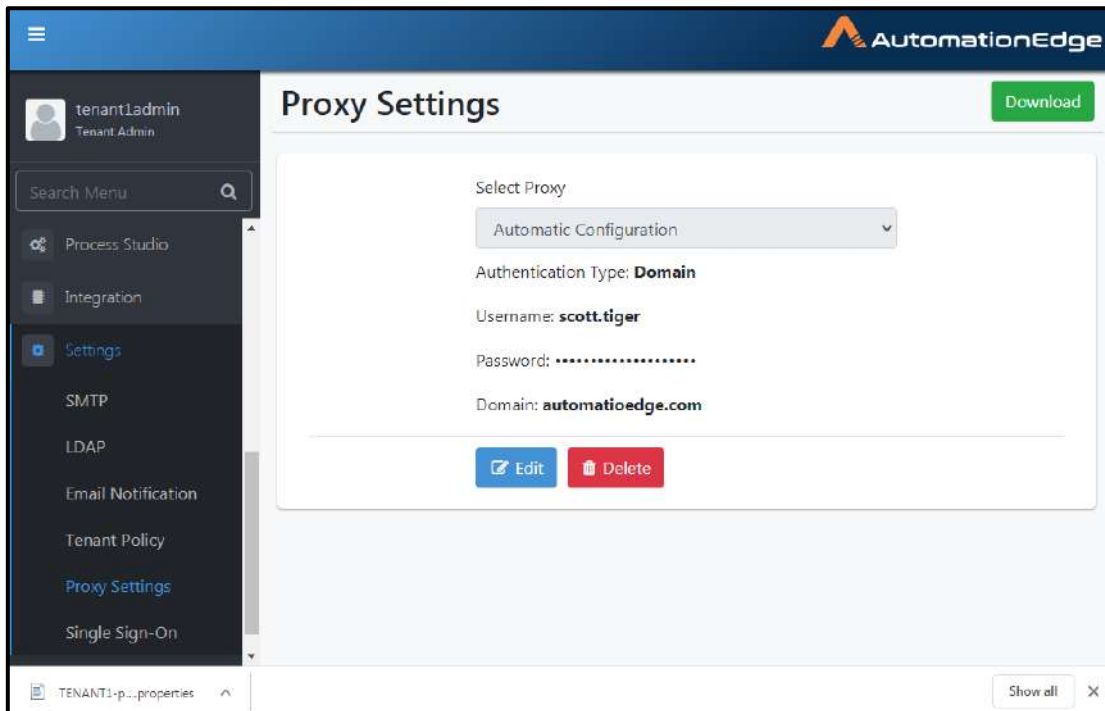


Figure 116d: Downloaded Proxy Configuration file

11. This completes the process of downloading Proxy Configuration file.

17.5.3 Edit Proxy Settings

1. Navigate to Settings→Proxy Settings. Click Edit.

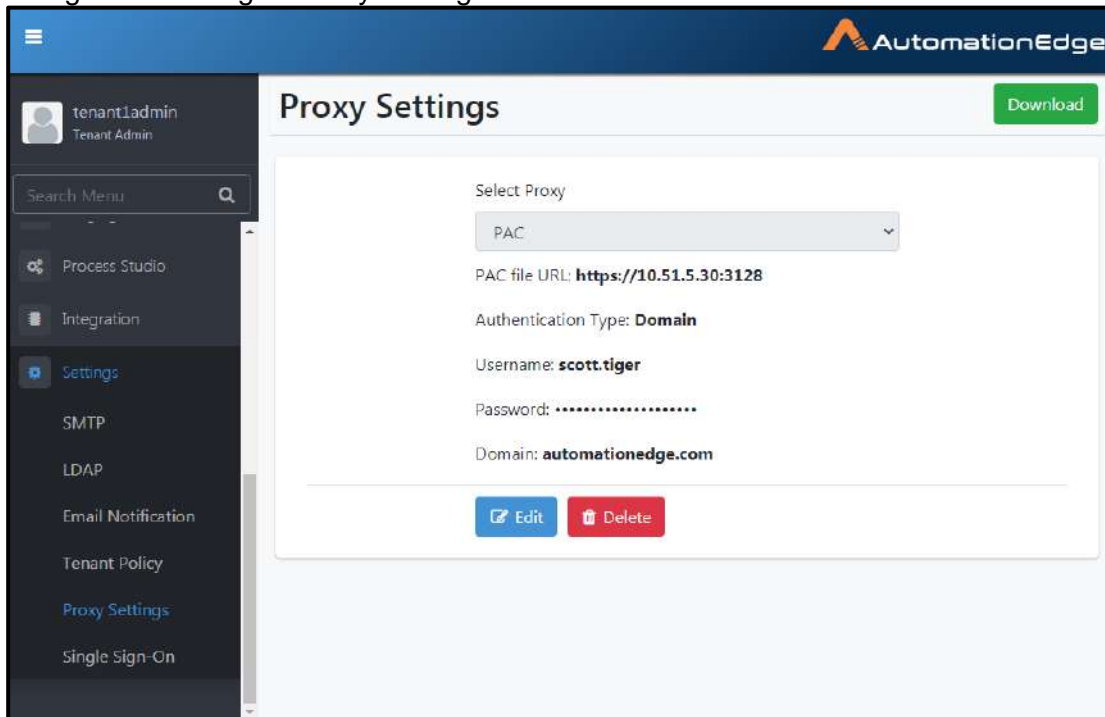
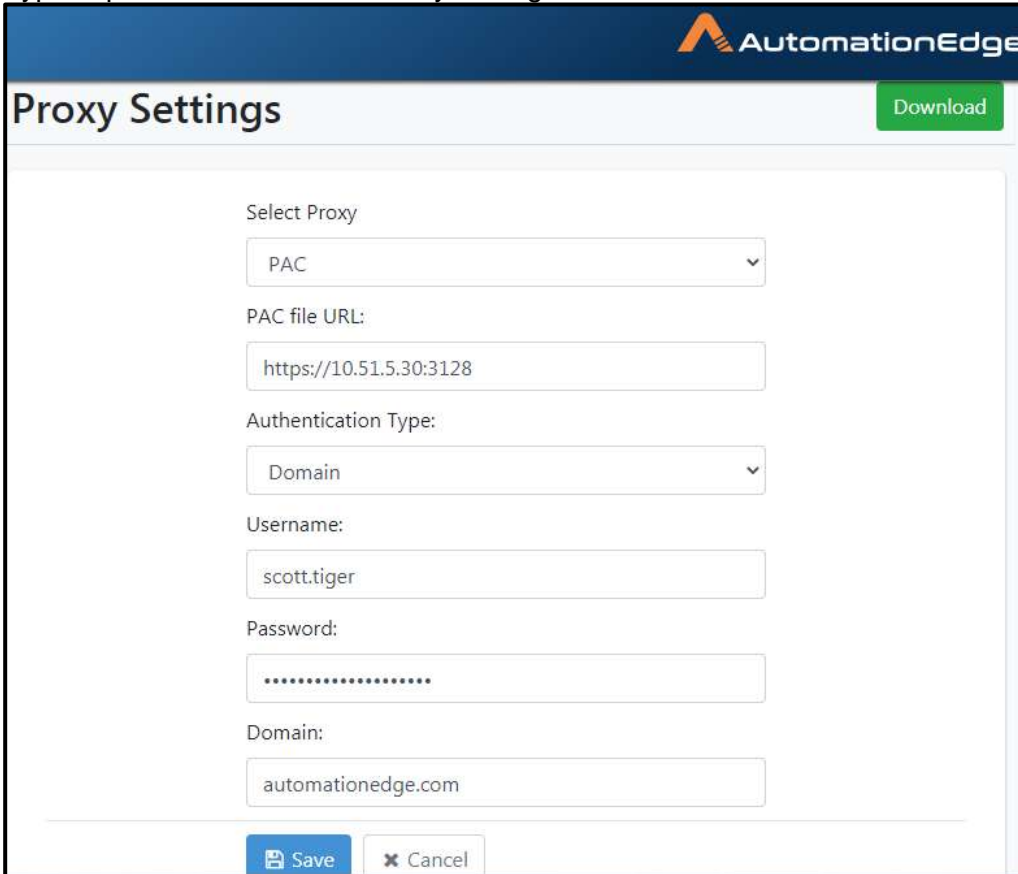


Figure 117a: Edit Proxy Settings

2. Notice that all fields are editable. You may change the Proxy as well as Authentication Type. Update to the desired Proxy settings. Click Save.



AutomationEdge

Proxy Settings

Download

Select Proxy

PAC

PAC file URL:

https://10.51.5.30:3128

Authentication Type:

Domain

Username:

scott.tiger

Password:

.....

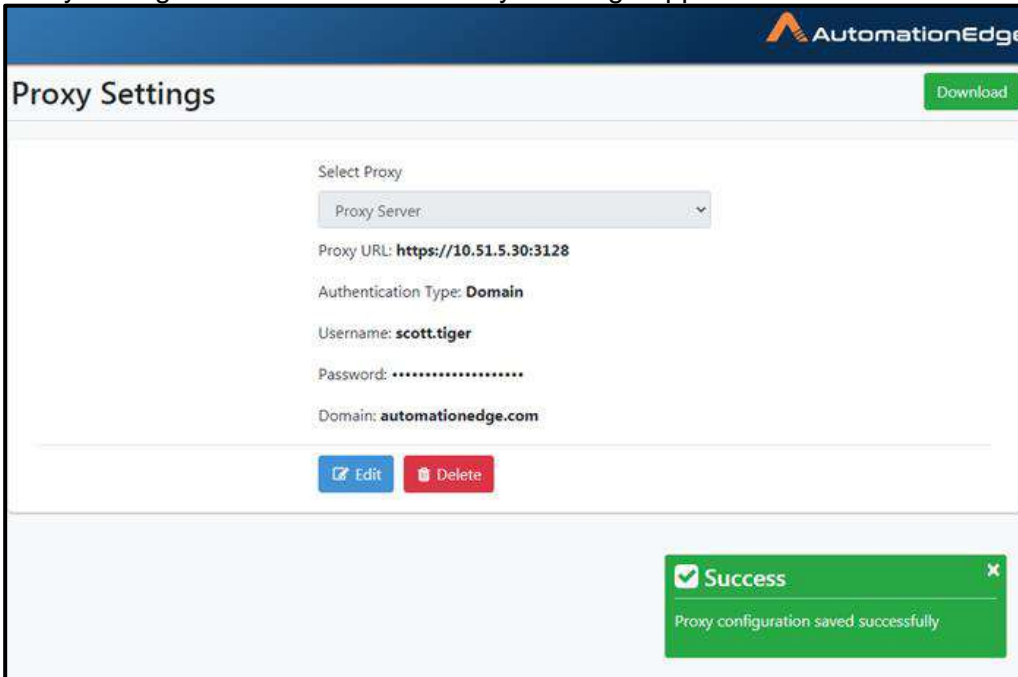
Domain:

automationedge.com

Save Cancel

Figure 117b: Enter updated Proxy Details

3. Proxy Configuration saved successfully message appears.



AutomationEdge

Proxy Settings

Download

Select Proxy

Proxy Server

Proxy URL: **https://10.51.5.30:3128**

Authentication Type: **Domain**

Username: **scott.tiger**

Password:

Domain: **automationedge.com**

Edit Delete

Success X
Proxy configuration saved successfully

Figure 117c: Proxy configuration saved successfully

17.5.4 Delete Proxy Settings

Following are the steps to delete Proxy Settings. The procedure is same for all types of Proxy configurations.

1. Navigate to Settings→Proxy Settings. Click Delete.

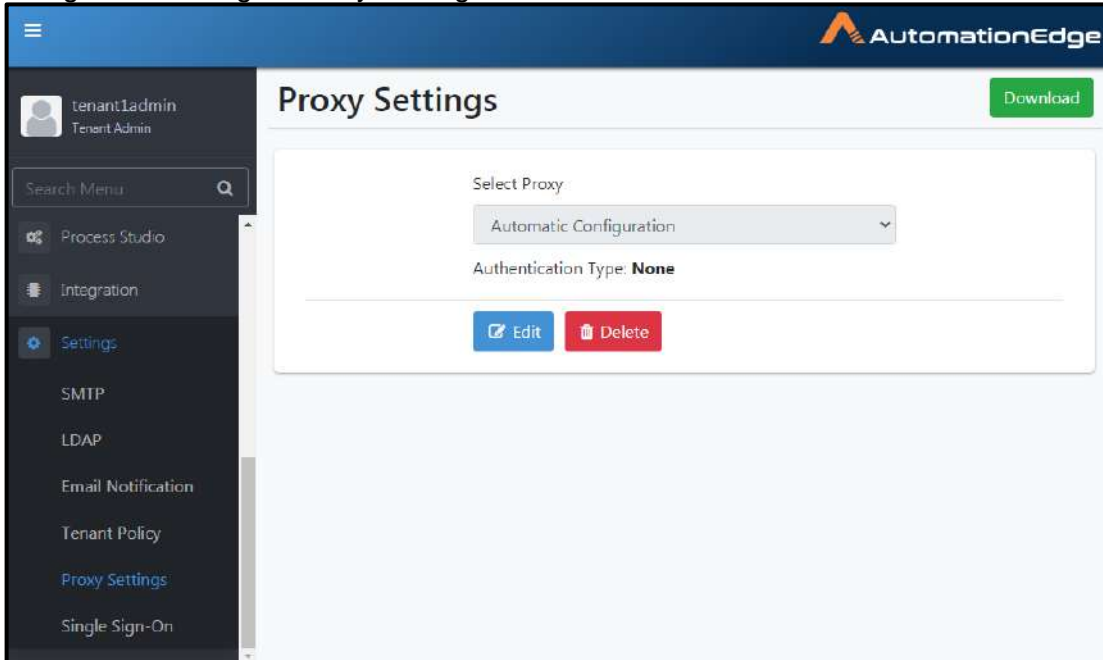


Figure 118a: Delete Proxy Configuration

2. You may Click Delete to delete the proxy configuration.

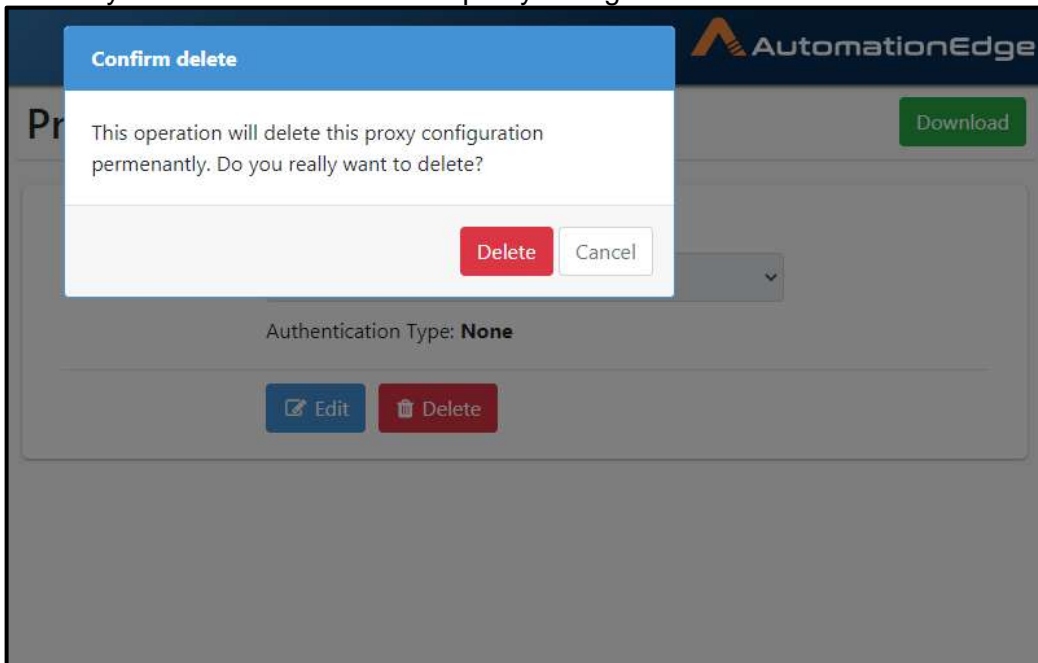


Figure 118b: Confirm Proxy Configuration Deletion

3. Proxy configuration deleted successfully message appears.
4. This completes Proxy deletion at Tenant level from database. Database record will be soft deleted.
5. Proxy configuration has to be removed manually from existing agents or PS distributions.

17.6 Single Sign-On

AutomationEdge supports Single Sign-On using an Identity Provider. The following protocols are supported,

- OAuth 2.0 / OpenID Connect
- SAML

In this section we will discuss the steps to configure Single Sign-On. In particular, the following configuration is for Okta SPA (Single Page Application) with OpenID. We shall also discuss configuration aspects of Identity Providers Keycloak and ADFS with OpenID; as well as with SAML for Okta, Keycloak and ADFS.

1. Navigate to the Settings menu and Single Sign-On submenu. Click Configure button.

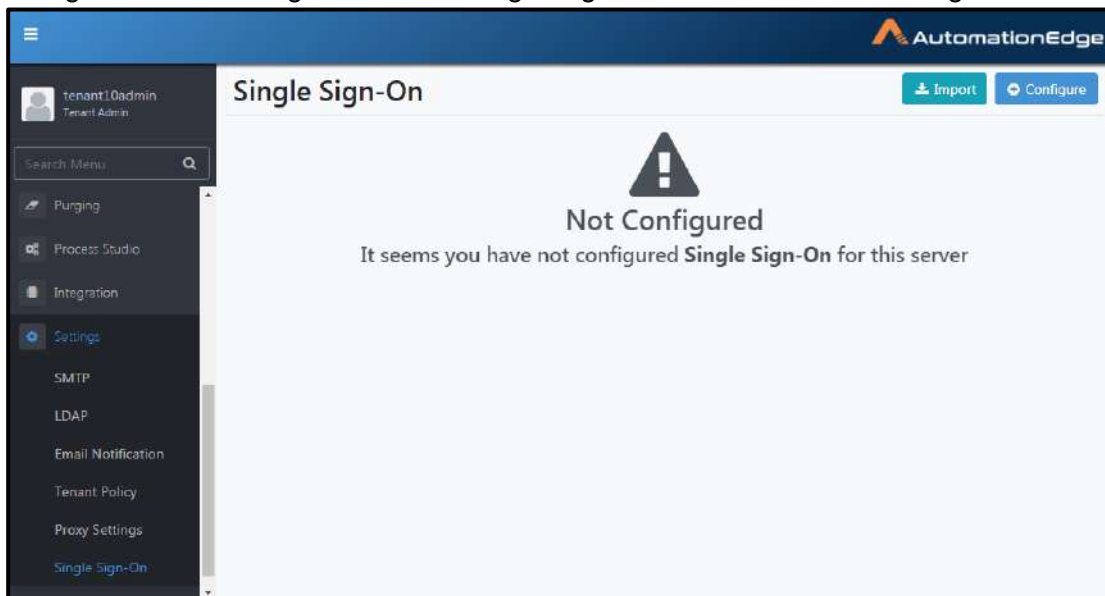


Figure 119a: Single Sign-On

17.6.1 Configure AE Single Sign-On for OAuth2.0/OpenID

17.6.1.1 Configure SSO with Import Button for OAuth/OpenID

In this section we will configure Single Sign-On by importing Endpoint Configurations. This section applies to Okta/Keycloak/ADFS for OAuth/OpenID protocols.

1. Click Import button on the Single Sign-On page.

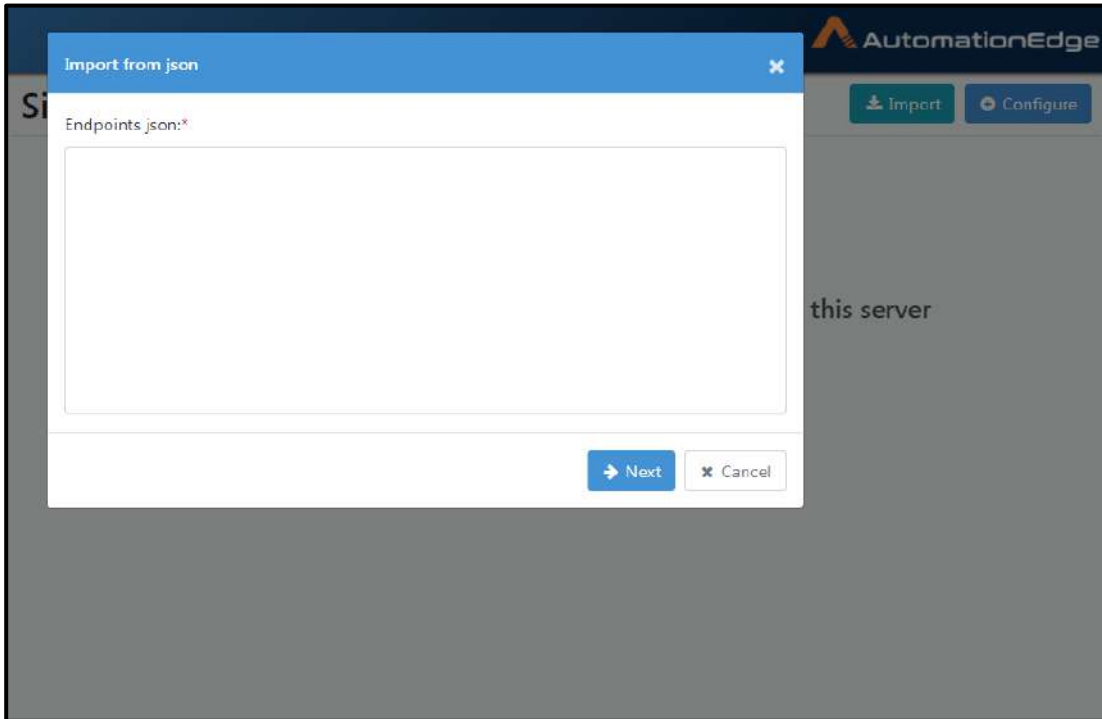


Figure 119b: Endpoints JSON input window

Provide all the Endpoints in JSON format. Sample Endpoints JSON for Okta Identity Service Management provided is provided in Table: Single Sign-On Import –Sample Endpoints JSON

2. Refer [Appendix 2.1 AE initiated SSO with Okta using OAuth/OpenID](#) to fetch Endpoints JSON in Okta; refer [2.5 AE initiated SSO with Keycloak using OAuth/OpenID](#) to fetch Endpoints JSON in Keycloak; and refer [2.7 AE initiated SSO with ADFS using OAuth/OpenID](#) to fetch Identity Provider Metadata.

3. Click Next.

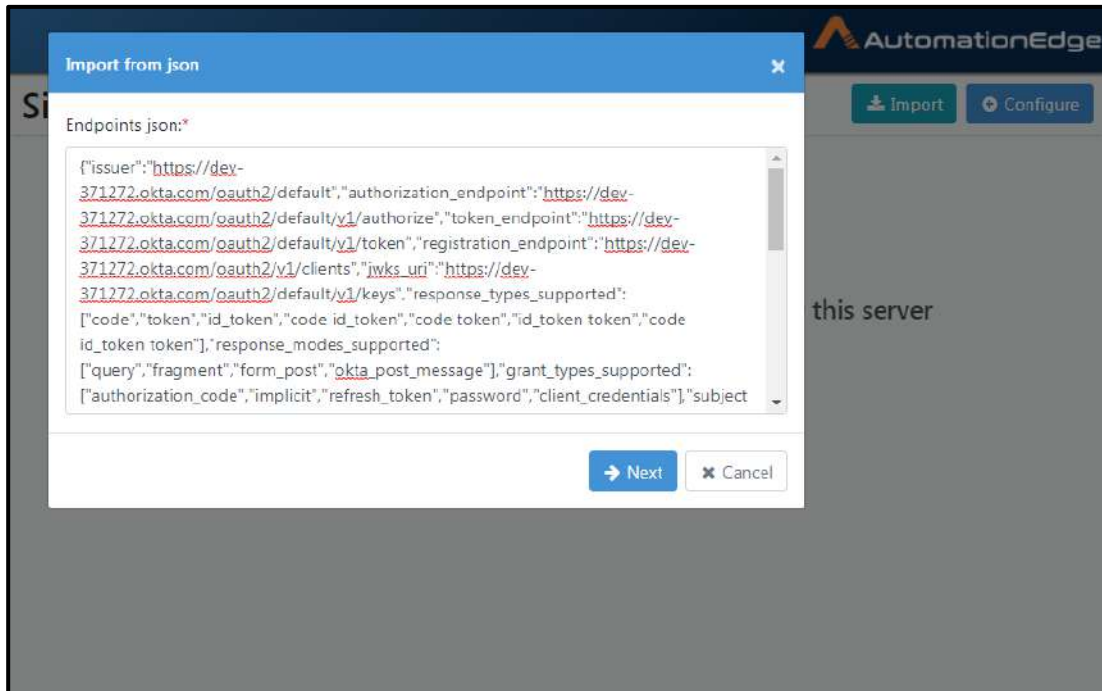


Figure 119c: Provide Endpoints JSON

4. The Single Sign-On page appears. The fields from the Endpoints JSON are populated in the Single Sign-On Configuration page as seen below.

Single Sign-On

Identity Provider:*

Protocol:*

Issuer:*

Redirect URL:*

Client ID:*

Client Secret:

Authorization Endpoint:*

Token Endpoint:*

End Session Endpoint:*


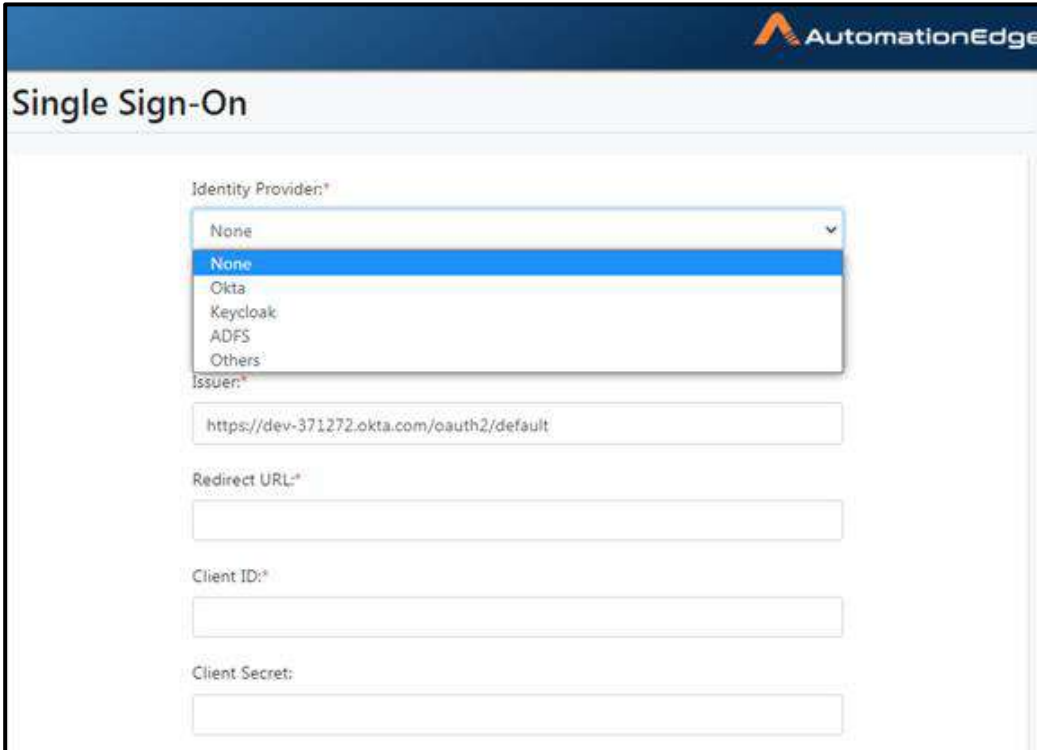


Figure 119d: Imported Single Sign-On configurations

5. Fill in the remaining fields. All the fields are explained in the table : Single Sign-On Configuration below.
6. Choose the Identity Provider and Protocol from the drop down list.



AutomationEdge

Single Sign-On

Identity Provider:^{*}

- None
- None
- Okta
- Keycloak
- ADFS
- Others

Issuer:^{*}

https://dev-371272.okta.com/oauth2/default

Redirect URL:^{*}

Client ID:^{*}

Client Secret:

Figure 119e: Select Identity Provider

7. In the snapshot below all the required fields have been filled up.
8. Redirect URL and Client ID from the configurations in the Identity Provider portal.
9. In this example the identity provider is Okta for SPA(Single Page Application). In case of Okta for Web Application Client Secret is additionally required. Keycloak supports OpenID Connect, OAuth 2.0 and SAML protocol. Refer [Appendix 2: SSO](#) to see how we can fetch configuration values in Okta and Keycloak and ADFS.
10. Click Save.

Single Sign-On

Identity Provider:*
Okta

Protocol:*
OpenID Connect

Issuer:*
https://dev-371272.okta.com/oauth2/default

Redirect URL:*
https://10.51.4.161:8443/aeui

Client ID:*
0oakoh32sjrxlMy314x6

Client Secret:

Authorization Endpoint:*
https://dev-371272.okta.com/oauth2/default/v1/authorize

Token Endpoint:*
https://dev-371272.okta.com/oauth2/default/v1/token

End Session Endpoint:*
https://dev-371272.okta.com/oauth2/default/v1/logout




Figure 119f: Complete Single Sign-On configurations

Table: Single Sign-On Import –Sample Endpoints JSON

Import Sample Endpoints JSON
<pre>{ "issuer": "https://dev-371272.okta.com/oauth2/default", "authorization_endpoint": "https://dev-371272.okta.com/oauth2/default/v1/authorize", "token_endpoint": "https://dev-371272.okta.com/oauth2/default/v1/token", "registration_endpoint": "https://dev-371272.okta.com/oauth2/v1/clients", "jwks_uri": "https://dev-371272.okta.com/oauth2/default/v1/keys", "response_types_supported": ["code", "token", "id_token", "code id_token", "code token", "id_token token", "code id token token"], "response_modes_supported": ["query", "fragment", "form_post", "okta_post_message"], "grant_types_supported": ["authorization_code", "implicit", "refresh_token", "password", "client_credentials"], "subject_types_supported": ["public"], "scopes_supported": ["openid", "profile", "email", "address", "phone", "offline_access"], "token_endpoint_auth_methods_supported": ["client_secret_basic", "client_secret_post", "client_secret_jwt", "private_key_jwt", "none"], "claims_supported": ["ver", "jti", "iss", "aud", "iat", "exp", "cid", "uid", "scp", "sub"], "code_challenge_methods_supported": ["S256"], "introspection_endpoint": "https://dev-371272.okta.com/oauth2/default/v1/introspect", "introspection_endpoint_auth_methods_supported": ["client_secret_basic", "client_secret_post", "client_secret_jwt", "private_key_jwt", "none"], "revocation_endpoint": "https://dev-371272.okta.com/oauth2/default/v1/ revoke", "revocation_endpoint_auth_methods_supported": ["client_secret_basic", "client_secret_post", "client_secret_jwt", "private_key_jwt", "none"], "end_session_endpoint": "https://dev-371272.okta.com/oauth2/default/v1/logout", "request_parameter_supported": true, "request_object_signing_alg_values_supported": ["HS256", "HS384", "HS512", "RS256", "RS384", "RS512", "ES256", "ES384", "ES512"]} }</pre>

Table: Single Sign-On Configuration with OAuth 2.0/OpenID

Fieldname	Description
Identity Provider	<p>Select an Identity Provider from the drop down list. It contains the following values,</p> <ul style="list-style-type: none"> • None (SSO configuration cannot be saved with None option) • Okta • Keycloak • ADFS • Others
Protocol	<p>The Single Sign-On protocols supported are</p> <ul style="list-style-type: none"> • None (SSO configuration cannot be saved with None Protocol)

	<ul style="list-style-type: none"> • OpenID Connect • OAuth 2.0 • SAML 2.0 <p>Select OpenID Connect/OAuth2.0.</p>
Issuer	Identity Provider Base URL (e.g. <code>https://dev-371272.okta.com/oauth2/default</code> in case of Okta). It can be obtained from the Endpoints URL or from Identity Provider Portal.
Redirect URL	<p>Your web application must host a route that Identity Provider sends information to when a user signs in. Redirect URL must be an absolute URI i.e. <code>https://host:port/aeui/</code>. Redirect URL in aeui portal SSO configuration page must be the same as <code>redirect_uri</code> in Identity Provider portal.</p> <p>Note: SSO authentication is supported only for secure sites (https), either with a domain name or IP address. (e.g. <code>https://mydomain:8443/aeui</code> or <code>https://10.51.4.161:8443/aeui</code>).</p> <p>SSO functionality is supported in an HTTPS environment for IE11, Chrome browser and Firefox.</p>
Client ID	The public identifier for apps.
Client Secret	It is the secret known only to the application and the authorization server
Authorization Endpoint	<p>It is the Identity Provider Authorization Endpoint (in the form of a URL, e.g. in Okta - <code>https://dev-371272.okta.com/oauth2/default/v1/authorize</code>). Here Authorized Code is generated by IDP and sent to AutomationEdge Server.</p> <p>Refer Appendix 2: SSO to fetch Authorization Endpoints.</p>
Token Endpoint	<p>Token Endpoint is an IDP URL containing the Token parameter which can be used by AE.</p> <p>Following are the steps,</p> <ul style="list-style-type: none"> • AE server uses the Authorized Code from Authorization Endpoint to request Token from IDP. • Token Endpoint (e.g. <code>https://dev-371272.okta.com/oauth2/default/v1/token</code>) uses the Authorized Code sent back from AE server, generates Token and sends the Token to AutomationEdge Server.
End Session Endpoint	<p>This Endpoint is used for logout from IDP. (e.g. <code>https://dev-371272.okta.com/oauth2/default/v1/logout</code>)</p>

Note: [Refer Appendix 2: SSO](#) to fetch Identity Provider Issuer, Redirect URIs, Client ID, Client Secret, Authorization Endpoint, Token Endpoint and End Session Endpoint.

11. SSO Configuration created successfully message appears.

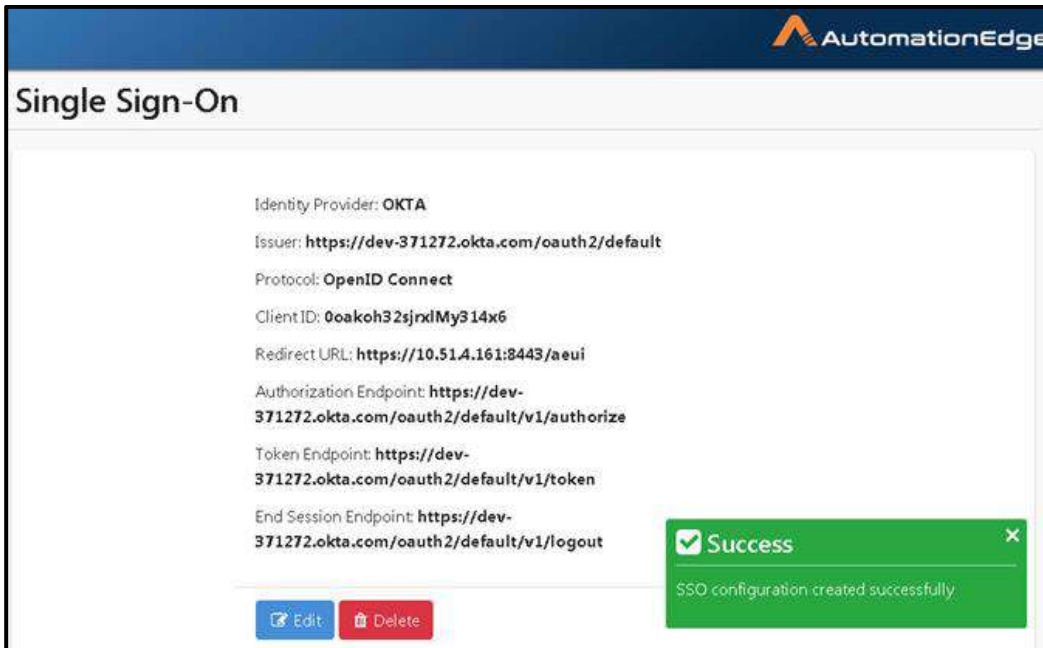


Figure 119g: SSO configuration created successfully

12. This completes the process of Single Sign-On configuration by importing the Endpoints json.
13. You may now create AutomationEdge SSO users by linking users to an Identity Provider user.

17.6.1.2 Configure SSO with Configure Button for OAuth/OpenID

In this section we will Configure SSO using the configure button.

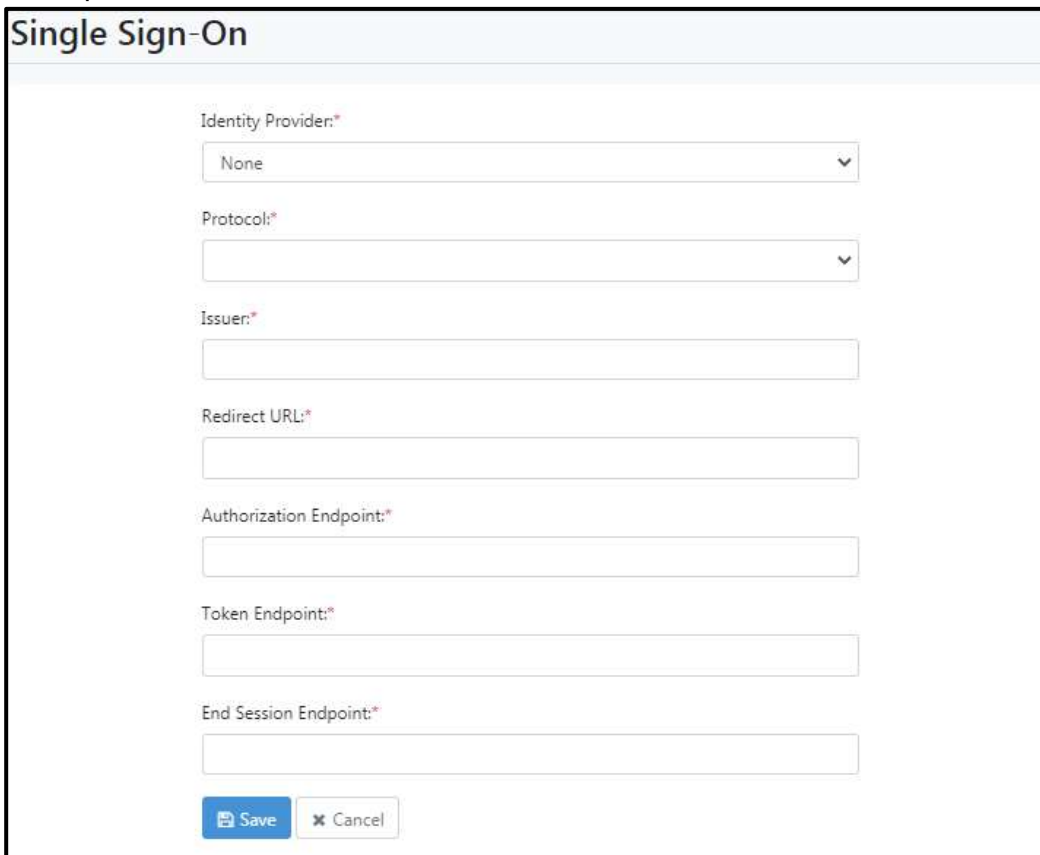
1. Login with a Tenant Administrator Navigate to Settings→Single Sign-On Configuration.
2. Click on Configure button.



Figure 119h: Single Sign-On Configure Button

The Single Sign-On page appears. Notice that unlike the previous sections all the fields are blank. The fields are explained in the Table: Single Sign-On Configuration with OAuth 2.0/OpenID

3. in the previous section.



Figure

119i: Blank Single Sign-On configurations page

4. Select a Protocol from the drop down list. We shall choose OpenID Connect for this configuration.

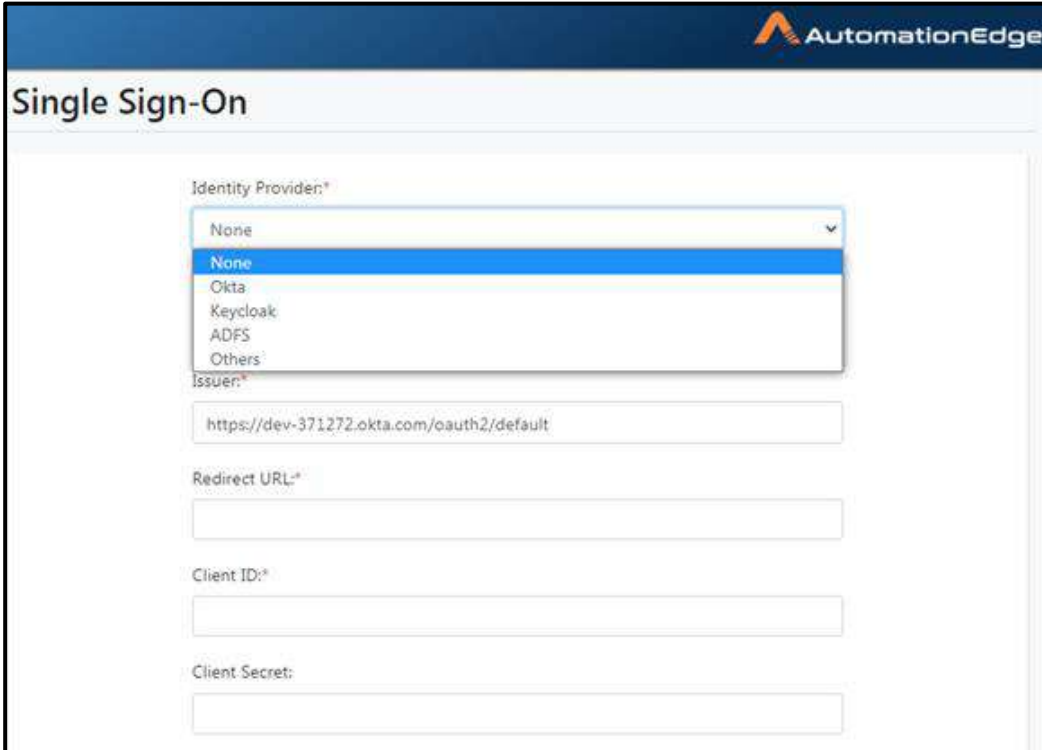


Figure 119j: Single Sign-On Identity Provider

5. Fill in the other Single Sign-On configuration details.
6. You may obtain Identity Provider authorization endpoint, Redirect URL and Client ID from the configurations in the Identity Provider.
7. In this example the identity provider is Okta for SPA(Single Page Application). In case of Okta for Web Application additionally Client Secret is also required. Keycloak supports OpenID Connect as well as OAuth 2.0 protocol.
[Refer Appendix 2: SSO](#) to see how we can fetch these configuration values in Okta and Keycloak.
8. Click Save.

9. Below is a sample configuration of Okta Identity Provider.
10. Click Save.

Single Sign-On

Identity Provider:*
Okta

Protocol:*
OpenID Connect

Issuer:*
`https://dev-371272.okta.com/oauth2/default`

Redirect URL:*
`https://10.51.4.161:8443/aeui`

Client ID:*
`0oakoh32sjxlMy314x6`

Client Secret:

Authorization Endpoint:*
`https://dev-371272.okta.com/oauth2/default/v1/authorize`

Token Endpoint:*
`https://dev-371272.okta.com/oauth2/default/v1/token`

End Session Endpoint:*
`https://dev-371272.okta.com/oauth2/default/v1/logout`




Figure 119k: All Single Sign-On configurations

11. SSO Configuration created successfully message appears as seen below.

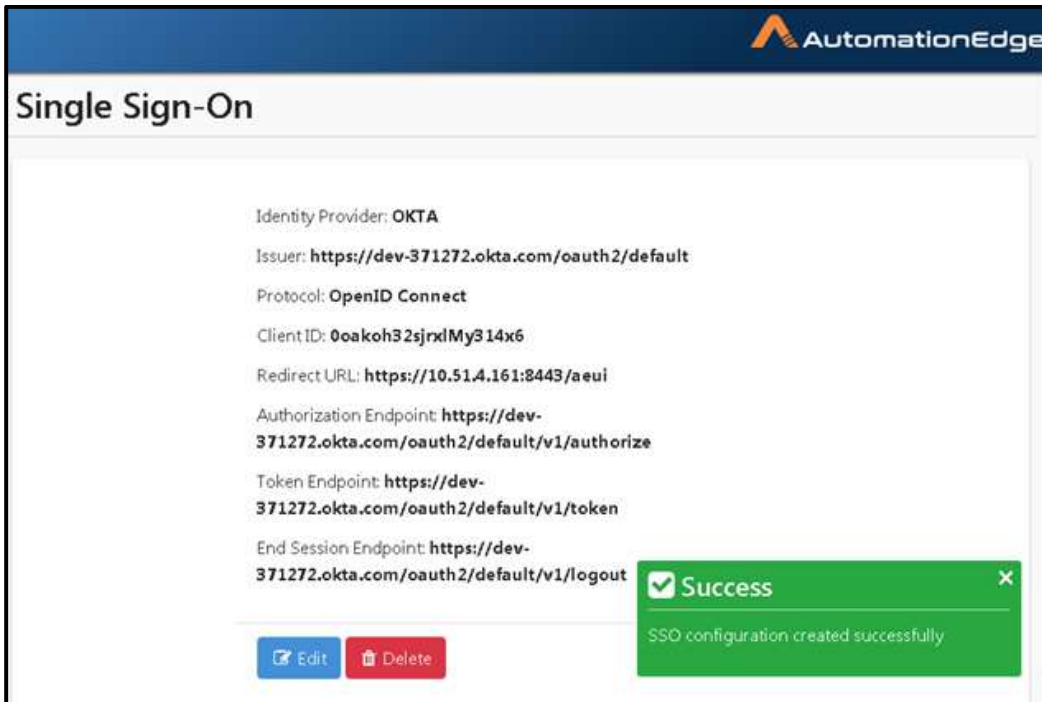


Figure 119: SSO configuration successful

12. This completes the process of SSO configuration with the Configure button for OpenID/OAuth 2.0.
13. You may now create AutomationEdge SSO users by linking users to an Identity Provider user.

17.6.2 Configure AE Single Sign-On for SAML

In this section we will discuss Single Sign-On with SAML. This section applies to Okta/Keycloak/ADFS for SAML protocol.

For SSO with SAML we need to do some changes in at the backend in Tomcat before we configure

17.6.2.1 Configurations in AutomationEdge backend

Before configuring on AutomationEdge UI some changes need to be done for Tomcat. We send SAML request from SP (Service Provider) i.e. AE-Engine to IDP and after authorization IDP sends response. The response sometime may have big header. The current tomcat configuration cannot handle such a big header and we need to increase the header size.

In the Tomcat Directory look for **config** Folder. Open the **server.xml** to change the header size. Check which connector you are using and increase the size of **maxHttpHeaderSize="65536"**

```
<Connector port="8080" protocol="HTTP/1.1"
    connectionTimeout="20000" maxHttpHeaderSize="65536"
    redirectPort="8443" />
```

Need some changes in the webapps aeui folder. If we are using SAML protocol, we need to comment POST request. Follow the steps below:

Navigate to Tomcat home/Webapps/aeui/WEB-INF web.xml

Open web.xml and look for `<http-method>POST</http-method>` and comment it using `<!-- ...->` as seen in the screenshot below.



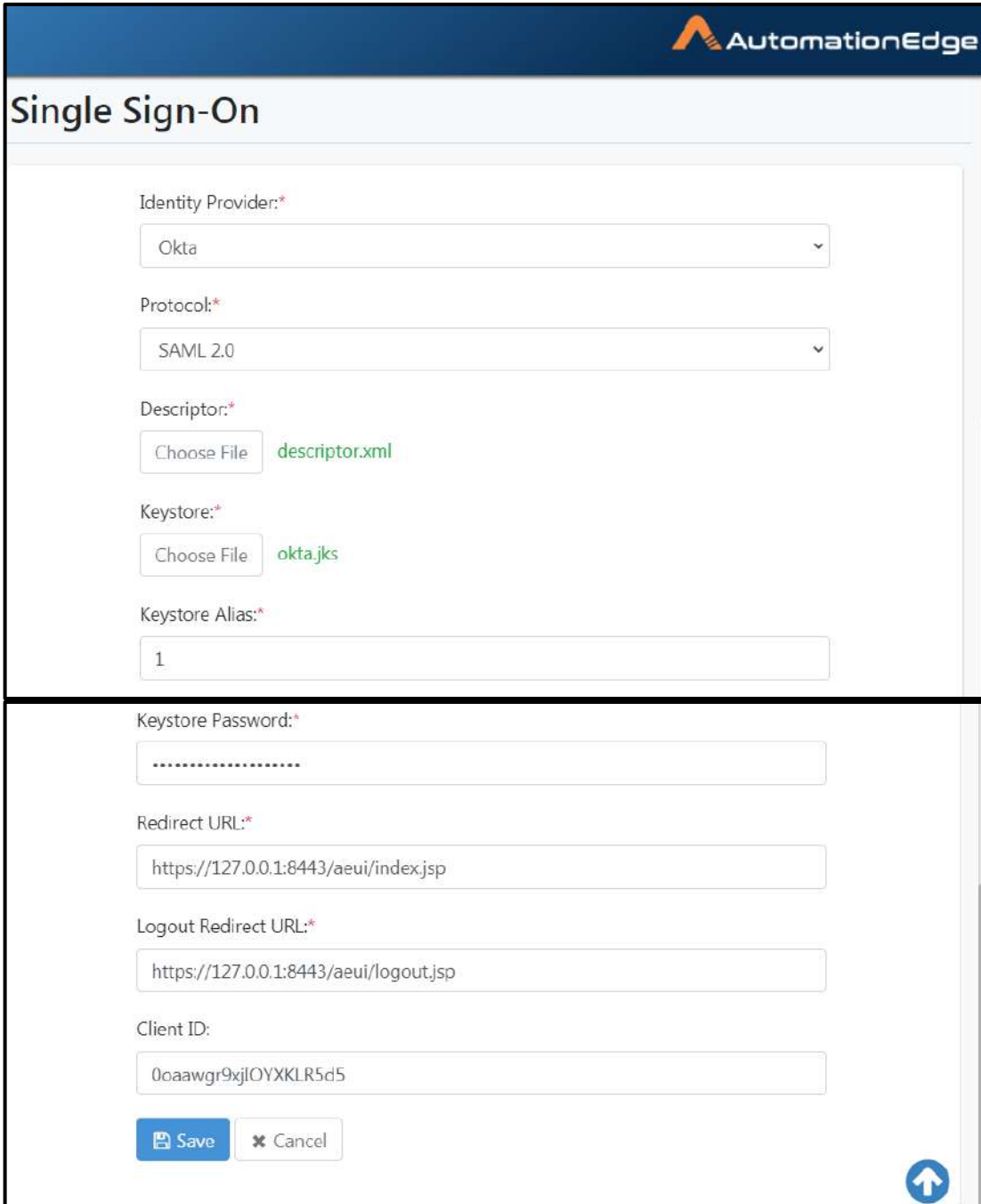
```
<security-constraint>
  <web-resource-collection>
    <web-resource-name>Forbidden Methods</web-resource-name>
    <url-pattern>*/</url-pattern>
    <http-method>OPTIONS</http-method>
    <http-method>TRACE</http-method>
    <http-method>HEAD</http-method>
    <http-method>PATCH</http-method>
    <!-- Comment line below in case of SAML SSO integration -->
    <!--<http-method>POST</http-method>-->
    <http-method>PUT</http-method>
    <http-method>DELETE</http-method>
  </web-resource-collection>
  <auth-constraint/>
</security-constraint>
```

Figure 120a: Comment POST request

17.6.2.2 Configuration on AutomationEdge UI

Following are the Single Sign-On configurations on AutomationEdge UI.

1. Login with a Tenant Administrator and Navigate to Settings→Single Sign-On menu.
2. The following screens show AutomationEdge SSO configuration for SAML 2.0 protocol. The configuration parameters are discussed in the table below.
3. Click Save.



AutomationEdge

Single Sign-On

Identity Provider:*
Okta

Protocol:*
SAML 2.0

Descriptor:*
Choose File descriptor.xml

Keystore:*
Choose File okta.jks

Keystore Alias:*
1

Keystore Password:*
.....

Redirect URL:*
https://127.0.0.1:8443/aeui/index.jsp

Logout Redirect URL:*
https://127.0.0.1:8443/aeui/logout.jsp


Client ID:
00aawgr9xjlOYXKLR5d5

Save Cancel

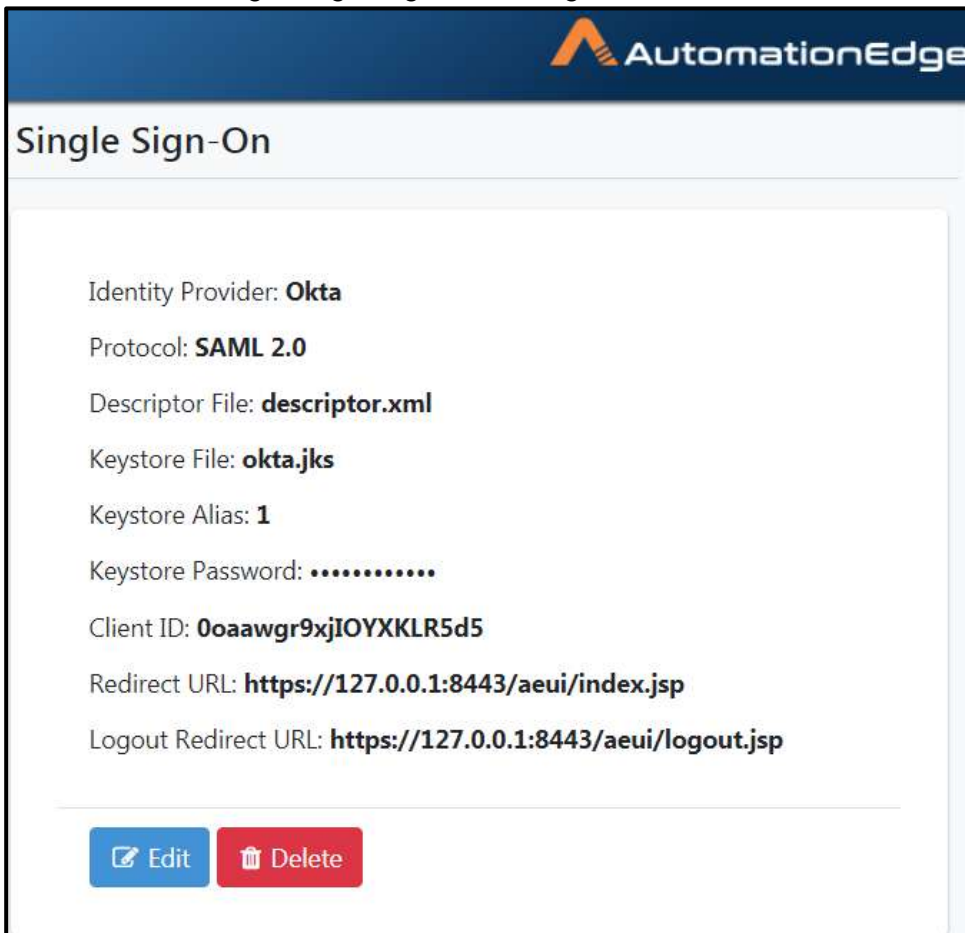
Figure 120b: single Sign-On Configuration

Table: Single Sign-On Configuration with OAuth 2.0/OpenID

Fieldname	Description
Identity Provider	Select an Identity Provider from the drop down list. It contains the following values, <ul style="list-style-type: none"> • None (SSO configuration cannot be saved with None option) • Okta • Keycloak • ADFS • Others
Protocol	The Single Sign-On protocols supported are <ul style="list-style-type: none"> • None (SSO configuration cannot be saved with None Protocol) • OpenID Connect • OAuth 2.0 • SAML 2.0 Select SAML 2.0
Descriptor	Upload the descriptor file (xml). This file is to be created by storing the Identity Provider Metadata.
Keystore	Here we are share public and private key with AE. It is use for xml signature verification. Keystore file (.jks) needs to be uploaded here, it is mandatory. Refer to 2.9 Keystore and Certificate Generation for generating the .jks file.
Keystore Alias	Provide the Keystore Alias you provided while generating Keystore.
Keystore Password	Provide the Keystore Password you provided while generating Keystore.
Redirect URL	Your web application must host a route that Identity Provider sends information to when a user signs in. Redirect URL must be an absolute URI i.e. https://host:port/aeui/. Redirect URL in aeui portal SSO configuration page must be the same as redirect_uri in Identity Provider portal. <p>Note: SSO authentication is supported only for secure sites (https), either with a domain name or IP address. (e.g. https://mydomain:8443/aeui/index.jsp or https://10.51.4.161:8443/aeui/index.jsp).</p> SSO functionality is supported in an HTTPS environment for IE11, Chrome browser and Firefox.
Logout Redirect URL	On logout from SSO Application you are logged out of the application as well as IDP. Specify a Logout Redirect URL as below, (e.g. https://mydomain:8443/aeui/logout.jsp or https://10.51.4.161:8443/aeui/logout.jsp).
Client ID	The public identifier for apps.

 **Note:** Refer [Appendix 2: SSO](#) to create a descriptor file, Keystore and to fetch, Redirect URIs, Client ID for the desired Identity Provider (Okta/Keycloak/ADFS).

4. The AutomationEdge Single Sign-On setting is saved as below.



AutomationEdge

Single Sign-On

Identity Provider: **Okta**

Protocol: **SAML 2.0**

Descriptor File: **descriptor.xml**

Keystore File: **okta.jks**

Keystore Alias: **1**

Keystore Password:

Client ID: **0oaawgr9xjIOYXKLR5d5**

Redirect URL: **https://127.0.0.1:8443/aeui/index.jsp**

Logout Redirect URL: **https://127.0.0.1:8443/aeui/logout.jsp**



 

Figure 120c: Single Sign-On Setting

14. This completes the process of SSO configuration with SAML 2.0.
15. You may now create AutomationEdge SSO users by linking users to an Identity Provider user.

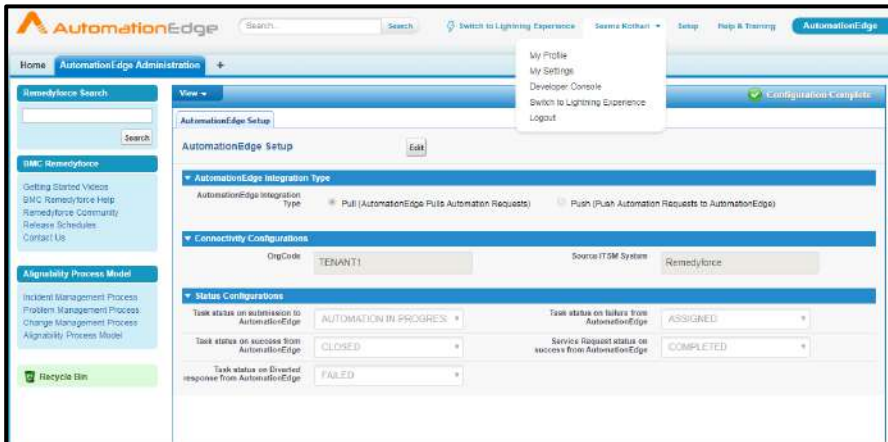
Appendices

1 Appendix 1: Integration with Type Remedifyforce

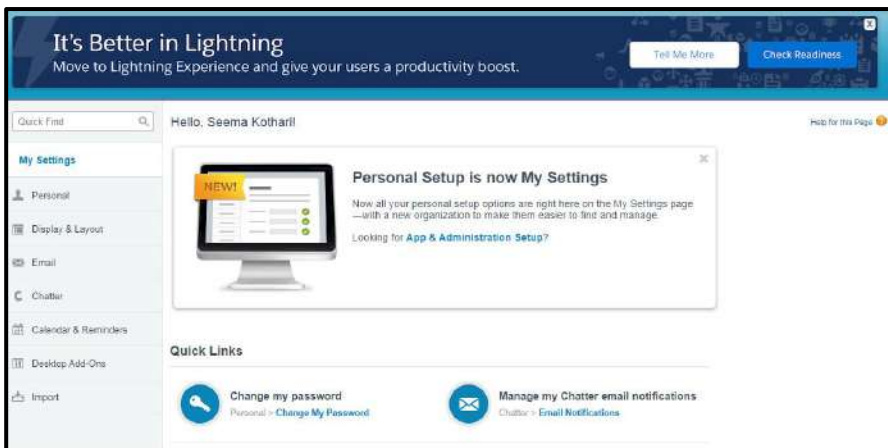
1.1 Setup on Remedifyforce

The following setup is required on Remedifyforce instance to whitelist AutomationEdge server IP Address.

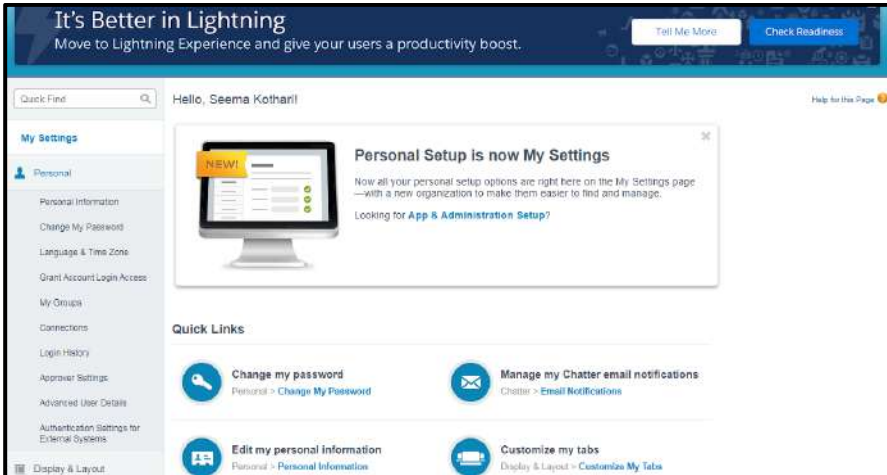
1. Click My Settings under username.



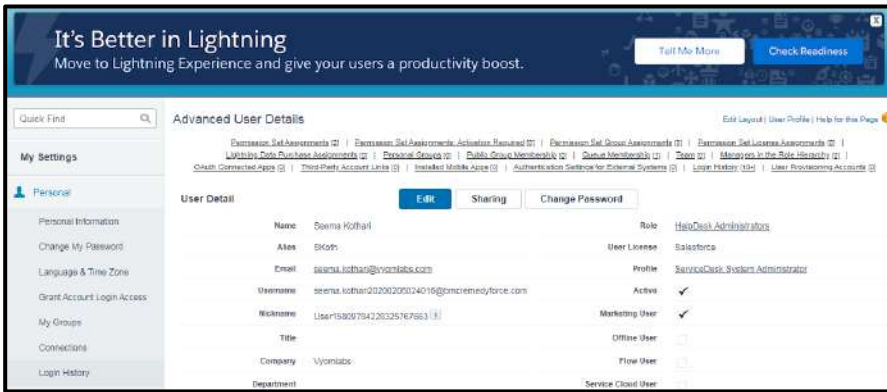
2. Click Personal link.



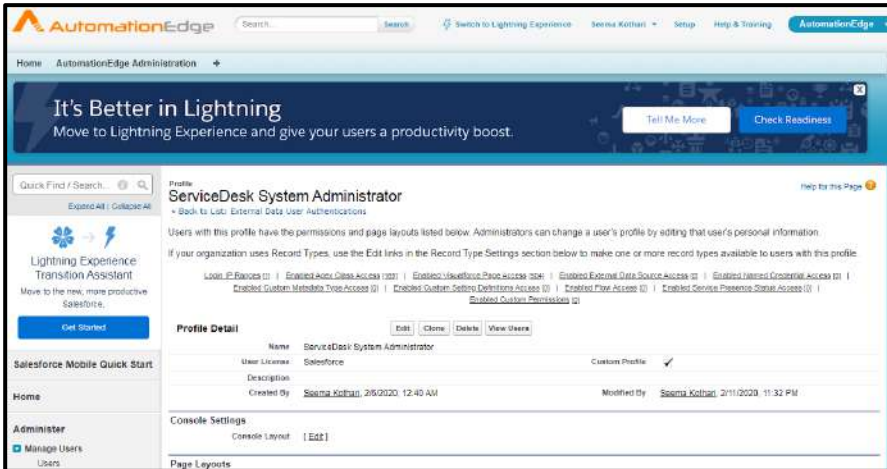
3. Click Advanced User Details



4. Click Profile



5. Click Login IP ranges.



6. Add IP ranges as required.



1.2 Setup on AutomationEdge

1. Setup Integration Services as discussed in AutomationEdge_R7.0.0_Installation_Guide
2. Create Integration Service, Integration Type with Remedyforce (remedyforce-rest.jar) and Integration Type configuration as discussed in the sections above.
3. Upgrade AutomationEdge application on Remedyforce. Configuration steps are the same (detailed document: *AE RF Push Integration Setup - AppVersion 4.03.pdf*).
4. In the Type configuration provide the following parameters,

Parameter Type	Is Secret	Name	Value
String	No	URL	Enter appropriate salesforce URL Sandbox instance: https://test.salesforce.com Production instance: https://login.salesforce.com
Credential	No	Connection Details	Credential object with salesforce username and password in Username and Password fields respectively.

NOTE: The configuration parameter names are case sensitive (including spaces), so make sure to enter the exact values as mentioned.

5. Once the configuration is completed and AutomationEdge Integration Service is running, after a certain interval the polling would start. The interval is configured at integration service level, field 'Update Conf Job Lower Limit (in minutes)'
The related logs can be accessed at location
'<INTEGRATION_TOMCAT_HOME>\logs\intgconf.log'.
6. For debugging change the log settings at location
'<INTEGRATION_TOMCAT_HOME>\webapps\aeintegrationservice\WEB-INF\classes\log4j2.xml'. Change the following line
<Logger name="com.ae.intg" level="INFO">
with
<Logger name="com.ae.intg" level="DEBUG">

2 Appendix 2: SSO – Identity Providers

(Single Sign-On with Identity Providers)

In this Appendix we will demonstrate Identity Provider (IDP) configurations and the navigation to fetch desired IDP configurations for AutomationEdge SSO Setups.

This Appendix includes the following sections,

- [2.1 AE initiated SSO with Okta using OAuth/OpenID](#)
- [2.2 Okta\(IDP\) initiated SSO to AE using OAuth/OpenID](#)
- [2.3 AE initiated SSO with Okta using SAML](#)
- [2.4 Okta\(IDP\) initiated SSO for AE using SAML](#)
- [2.5 AE initiated SSO with Keycloak using OAuth/OpenID](#)
- [2.6 AE initiated SSO with Keycloak using SAML](#)
- [2.7 AE initiated SSO with ADFS using OAuth/OpenID](#)
- [2.8 AE initiated SSO with ADFS using SAML](#)
- [2.9 Keystore and Certificate Generation](#)

The configurations may include some the following for OAuth 2.0/OpenID as well as SAML protocols.

- Identity Provider Issuer
- Identity Provider Endpoints (Authorization, Token, End Session Endpoints)
- Login redirect URIs
Your web application must host a route that Identity Provider sends information to when a user signs in. Redirect URL must be an absolute URI i.e. <https://host:port/aeui/>. Redirect URL in aeui portal must be the same as Redirect_URI in Identity Provider.
- Logout redirect URIs
- Client ID (The public identifier for apps)
- Client Secret (The secret known only to the application and the authorization server)

The configuration additionally includes the following for SAML protocols.

- CSA Certificate (.crt) for SAML IDP configuration
- Keystore File/ Keystore Alias/Keystore Password for SAML AE configuration

The configurations for each Identity Provider and protocol are discussed in the respective sections.

2.1 AE initiated SSO with Okta using OAuth/OpenID

In this section we demonstrate how to get the required parameters and some key configurations to setup AutomationEdge SSO with Okta.

The following are the required parameters for Okta SPA (Single Page Application) –

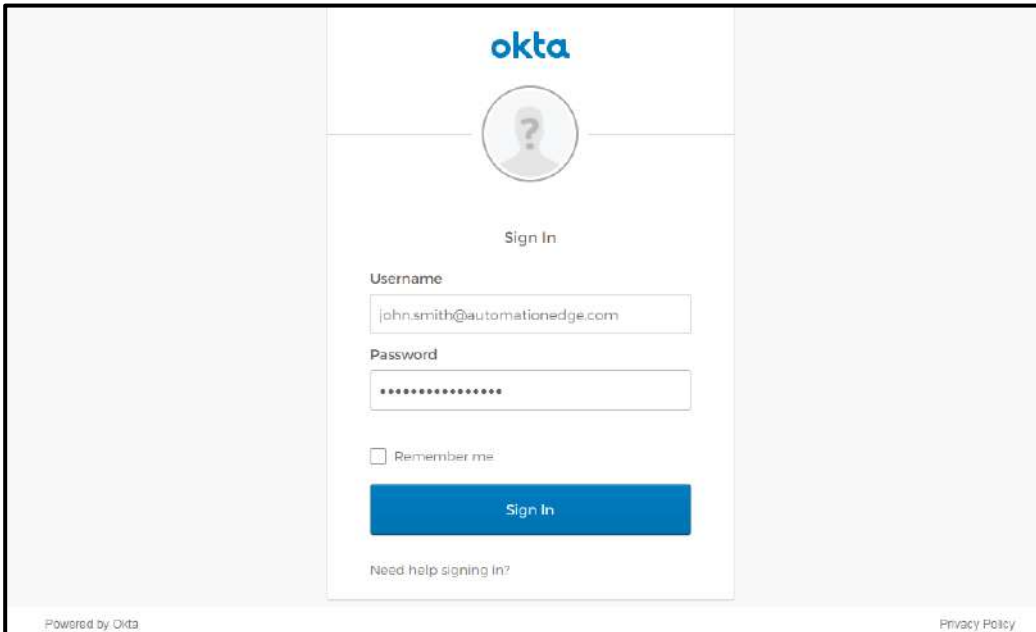
- Identity Provider Issuer
- Identity Provider Endpoints
- Login/Logout redirect URIs
- Client ID

The following parameter is additionally required for Okta Web Application –

- Client Secret

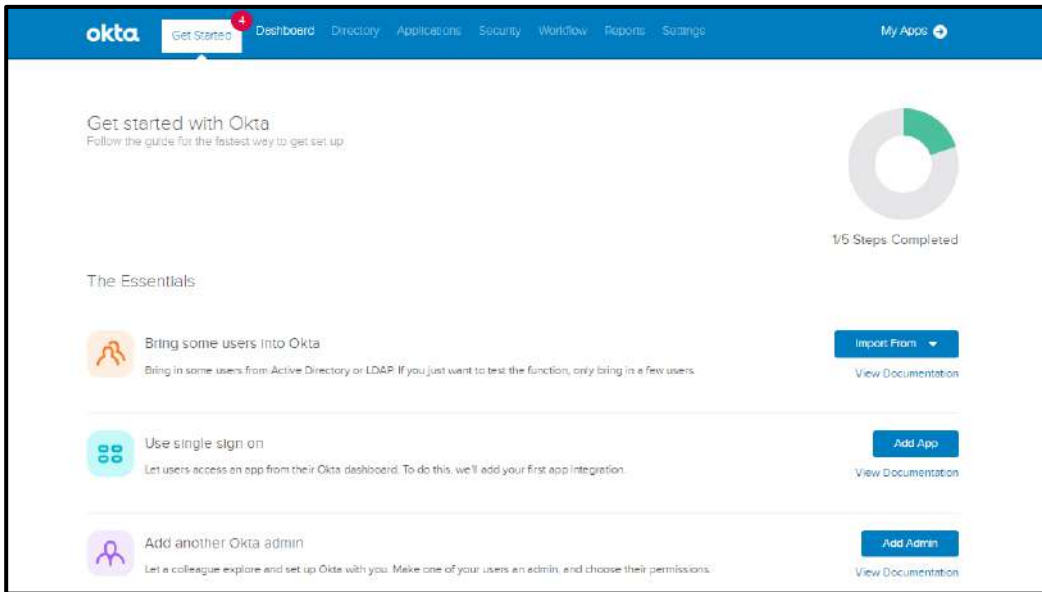
Following are the steps for key configurations for your Identity Provider as Okta and also demonstrates the navigation steps to fetch the parameters mentioned above.

1. Go to the Okta login screen and Sign-In.

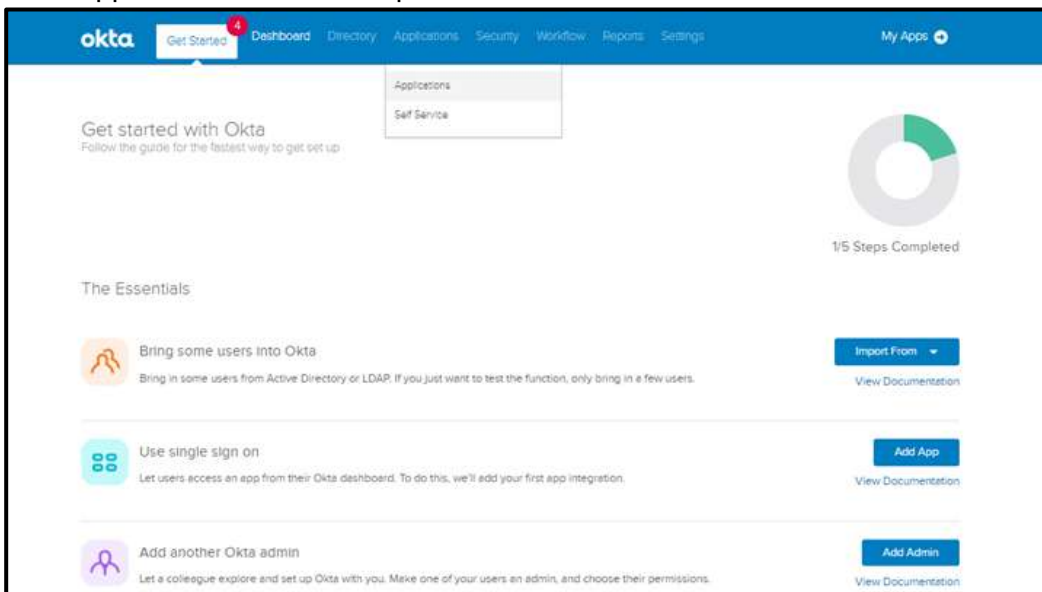


The screenshot shows the Okta Sign In interface. At the top center is the Okta logo. Below it is a circular icon with a question mark. The text "Sign In" is centered below the icon. There are two input fields: "Username" with the value "john.smith@automationedge.com" and "Password" with masked characters. Below the password field is a checkbox labeled "Remember me" which is unchecked. A blue "Sign In" button is positioned below the checkbox. At the bottom left of the form area, there is a link that says "Need help signing in?". At the bottom left of the entire page, it says "Powered by Okta", and at the bottom right, it says "Privacy Policy".

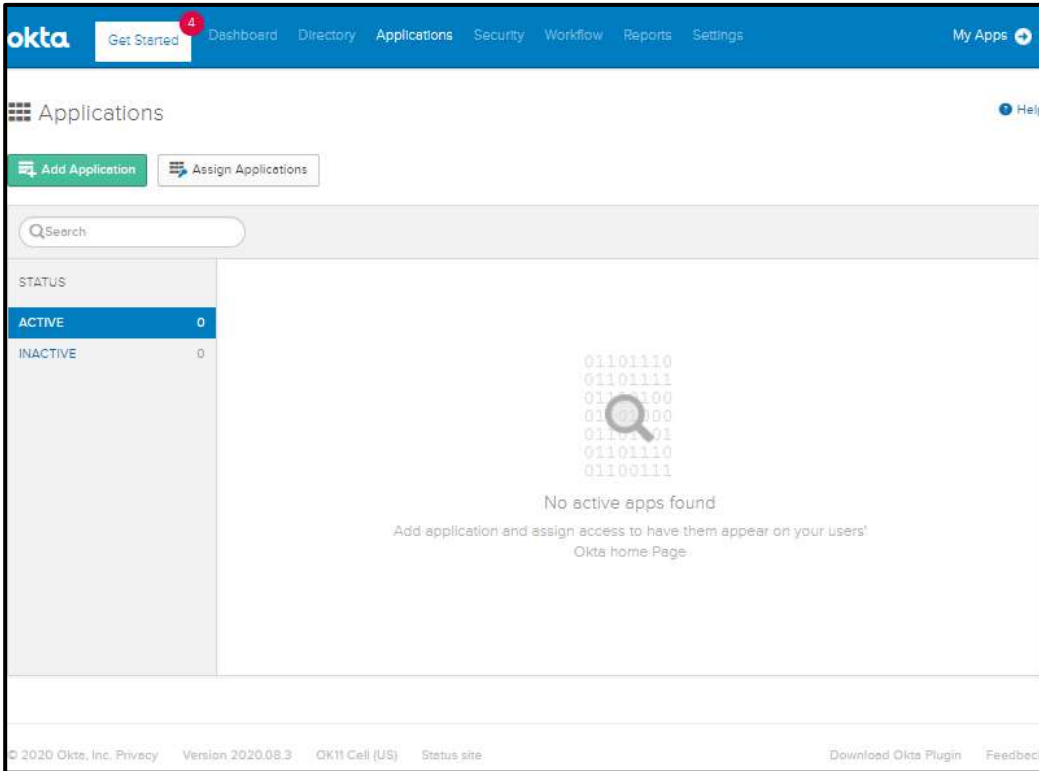
2. The Get Started with Okta page appears.



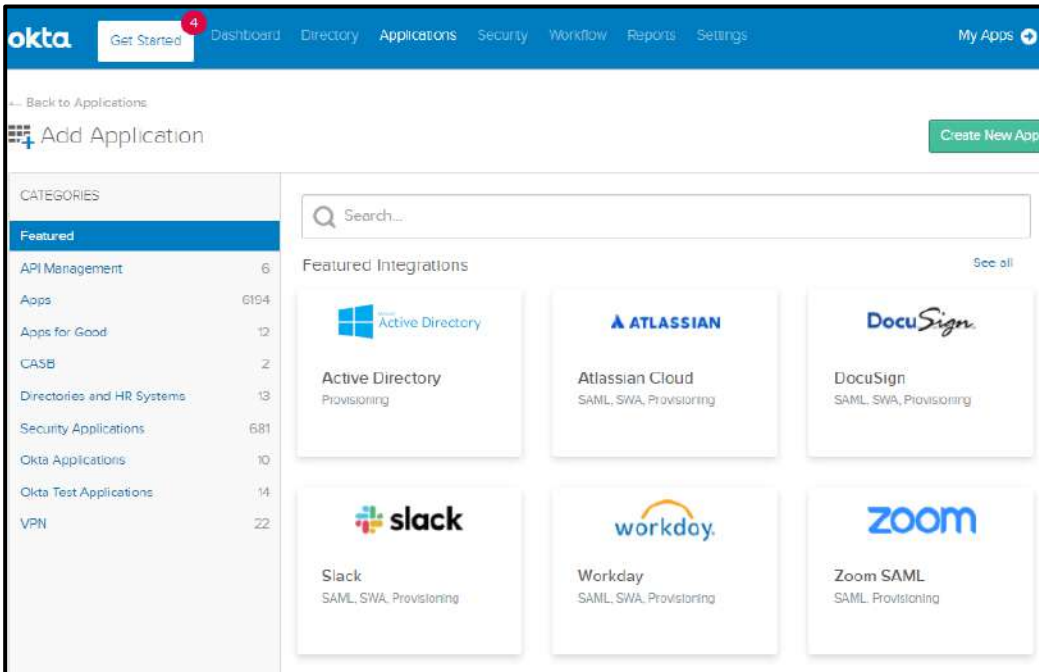
3. Click Applications tab in the top menu bar.



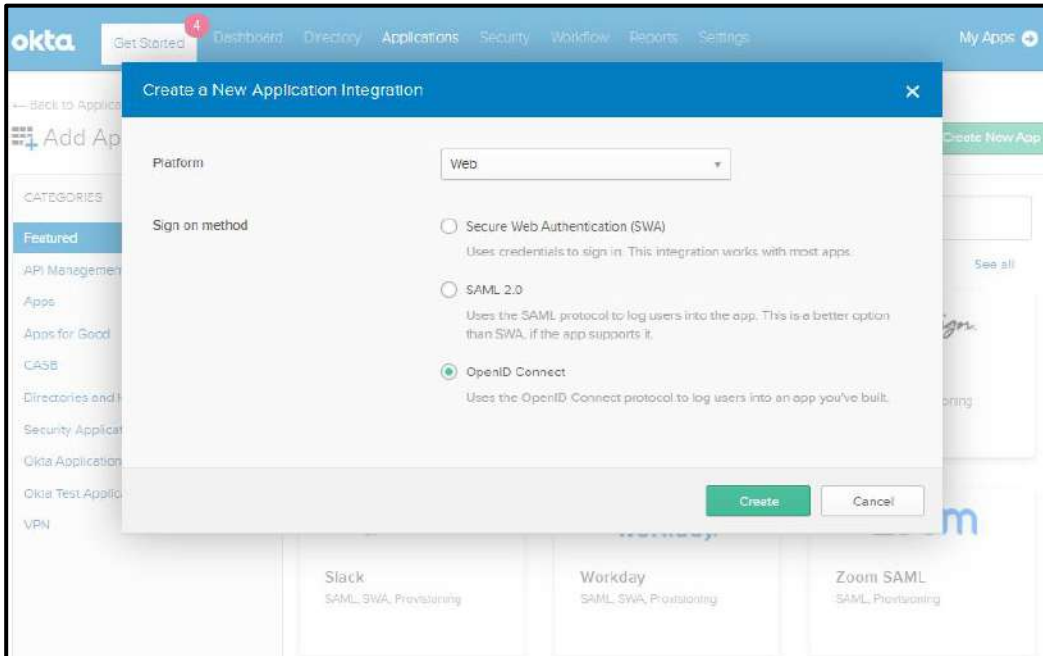
4. Click Add Application button on the left.



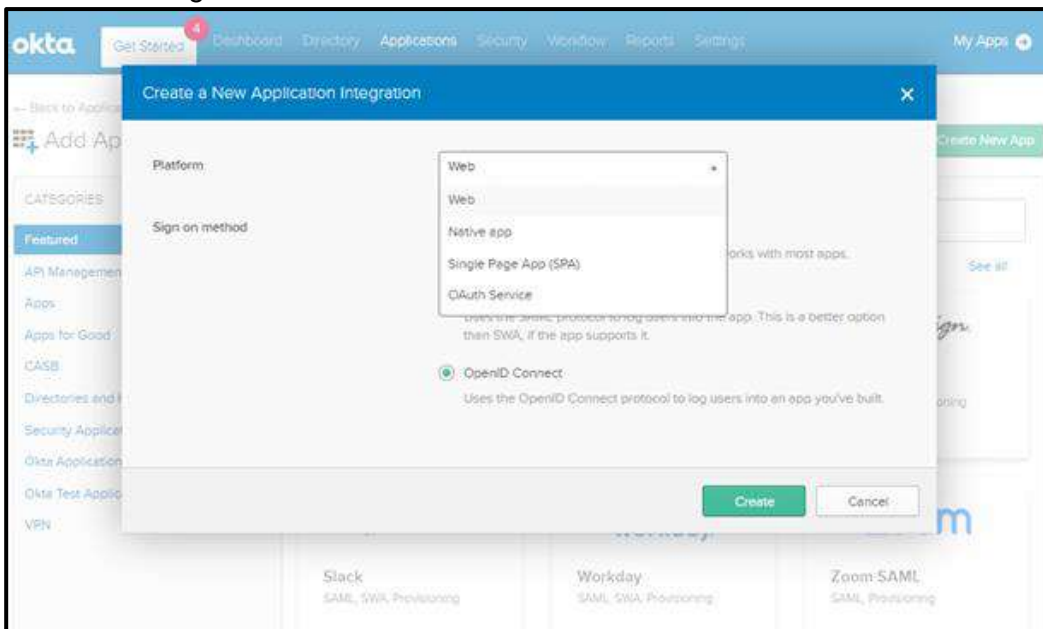
5. Click Create New App button on the right top corner.



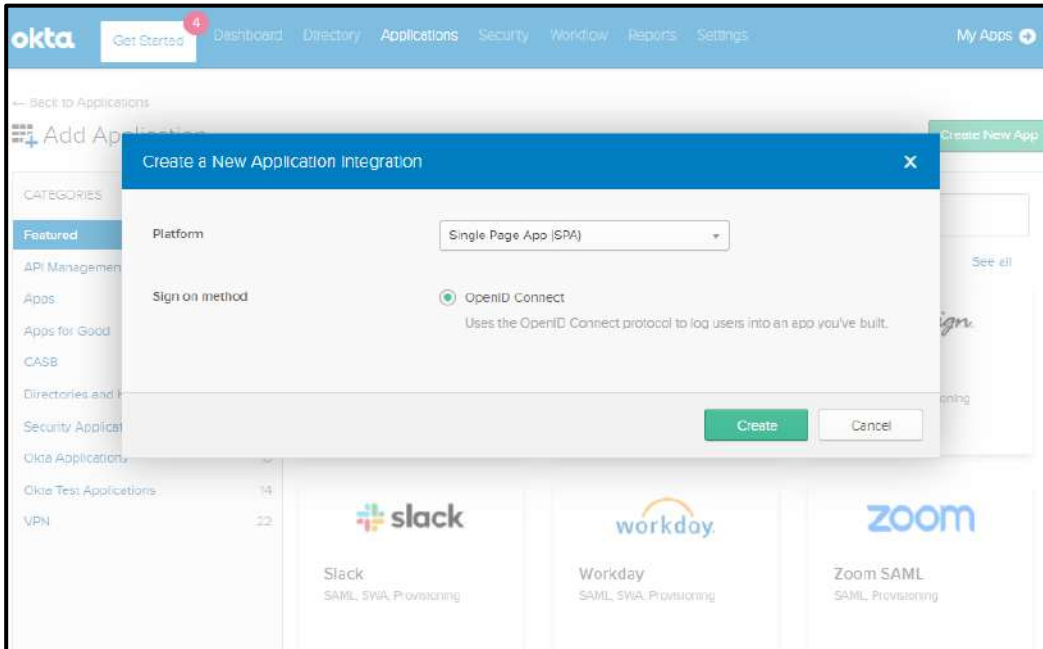
6. Choose the radio button for OpenID Connect.



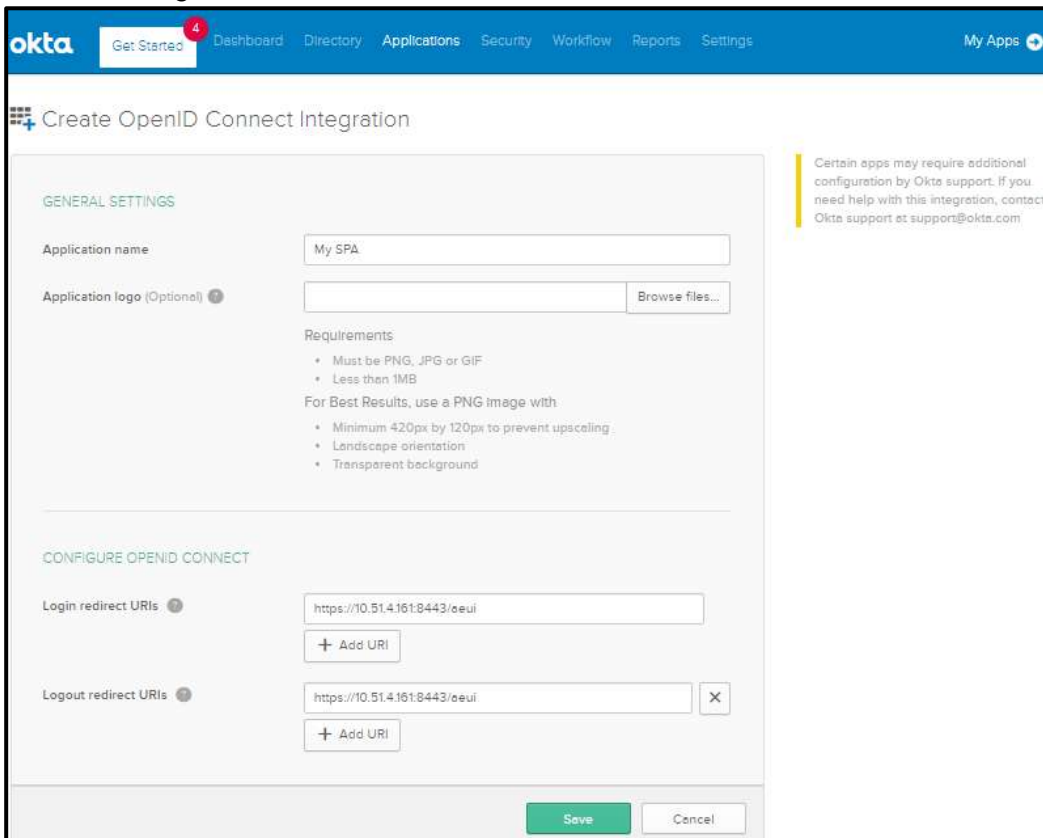
7. Select Web or Single Page App (SPA) applications which are supported for AutomationEdge SSO with Okta.



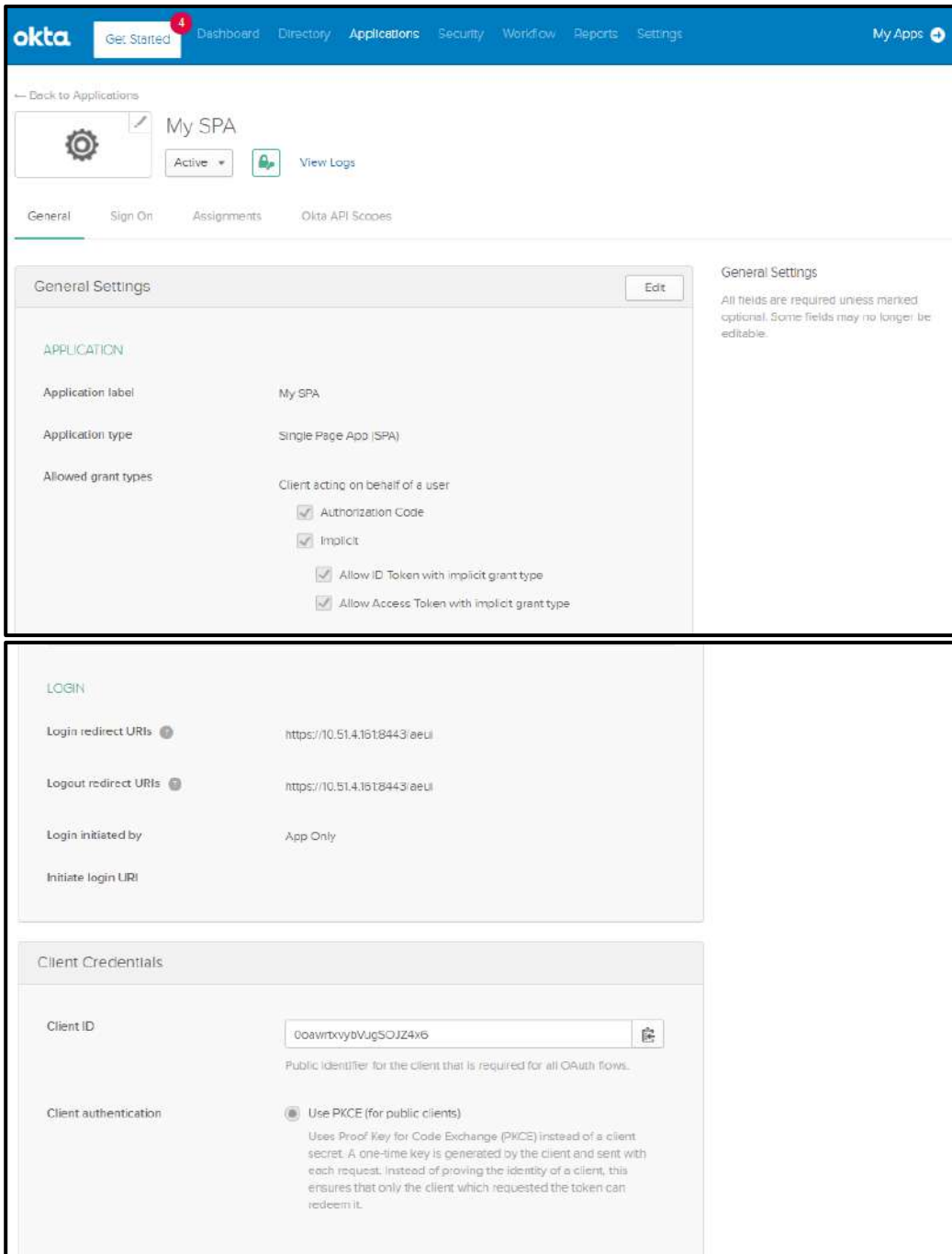
8. In the screenshot below Single Page App (SPA) is selected.



9. Provide configuration details for SPA as seen below. Click save.



10. My SPA Application is created with parameters as seen below. Click Back to Application.



The screenshot displays the Okta Admin Console interface for configuring a My SPA application. The top navigation bar includes 'Get Started', 'Dashboard', 'Directory', 'Applications', 'Security', 'Workflow', 'Reports', 'Settings', and 'My Apps'. The main content area is titled 'My SPA' and includes an 'Active' status indicator and a 'View Logs' button. Below this, there are tabs for 'General', 'Sign On', 'Assignments', and 'Okta API Scopes'. The 'General Settings' section is expanded, showing the following configuration:

- APPLICATION**
 - Application label: My SPA
 - Application type: Single Page App (SPA)
 - Allowed grant types: Client acting on behalf of a user
 - Authorization Code
 - Implicit
 - Allow ID Token with implicit grant type
 - Allow Access Token with implicit grant type

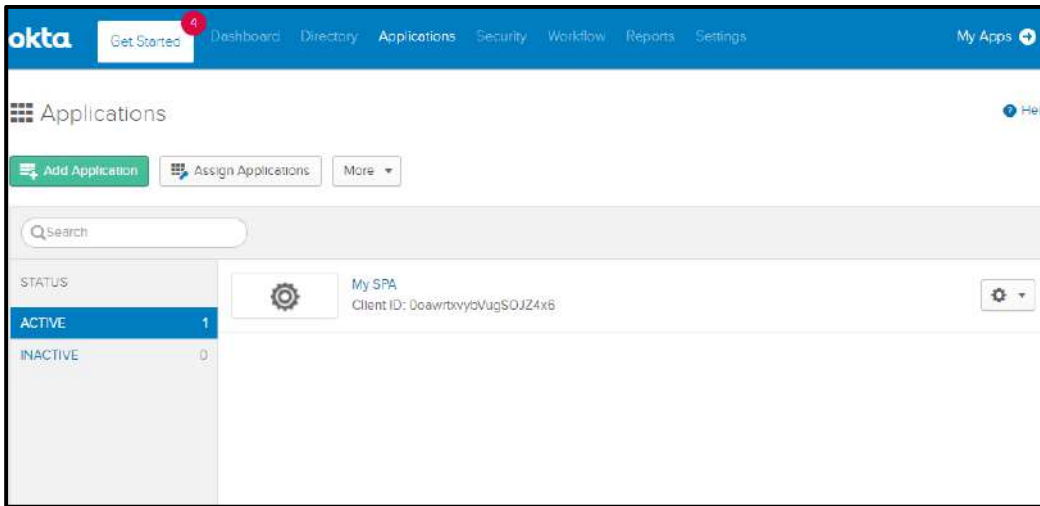
The 'LOGIN' section is also visible, with the following settings:

- Login redirect URIs: <https://10.51.4.151:8443/eeU>
- Logout redirect URIs: <https://10.51.4.151:8443/eeU>
- Login initiated by: App Only
- Initiate login URI: (empty)

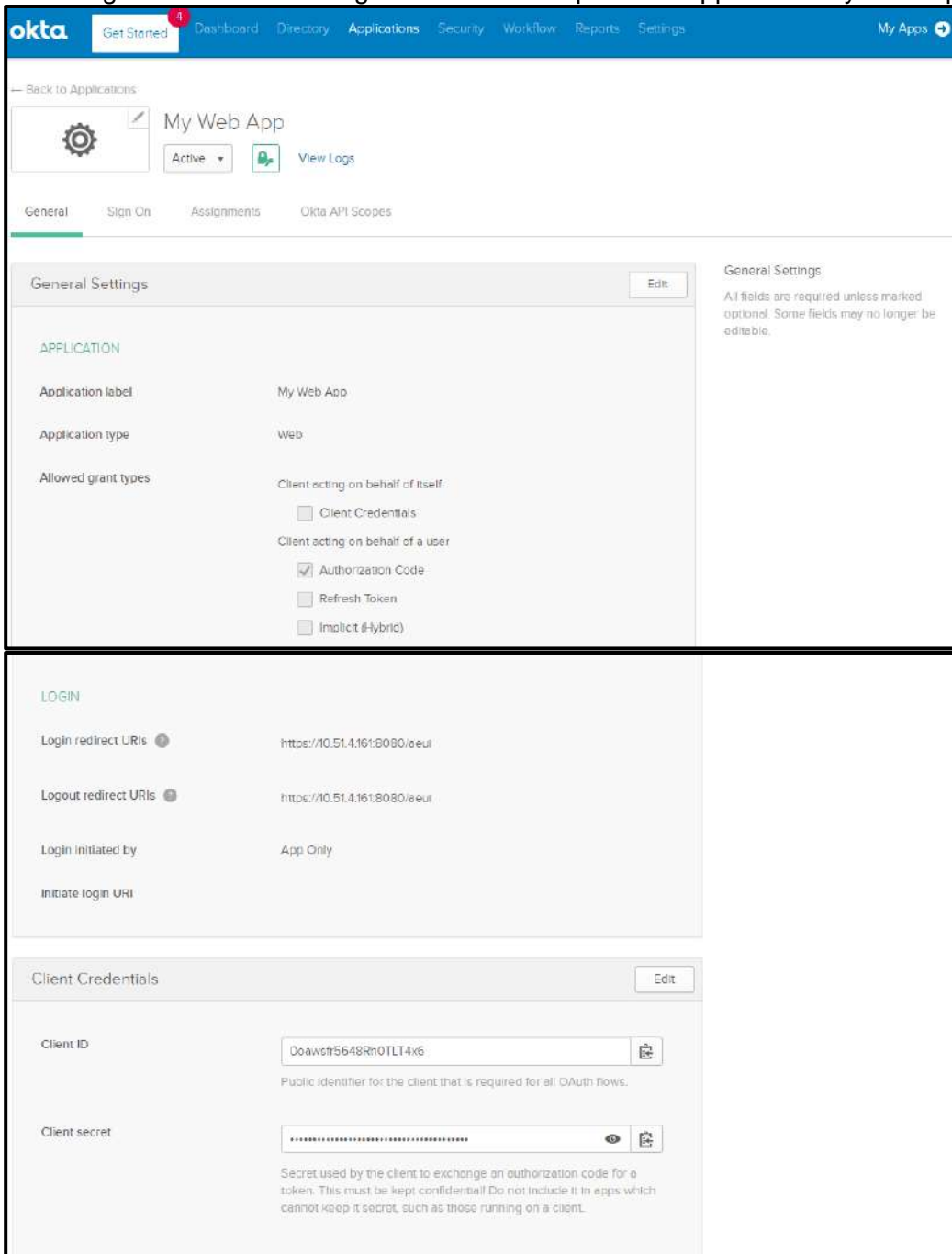
The 'Client Credentials' section shows:

- Client ID: 0oawrtxybVJgSOJZ4x6
- Client authentication: Use PKCE (for public clients)
 - Uses Proof Key for Code Exchange (PKCE) instead of a client secret. A one-time key is generated by the client and sent with each request. Instead of proving the identity of a client, this ensures that only the client which requested the token can redeem it.

11. You can now see MySPA in the Applications.



12. Once again on the menu bar at the top Click Add Applications. This time chose to create a Web Application and create My Web App, similar to how we created a SPA (Single Page Application).
13. Following screen shows configurations of a sample Web Application My Web App.

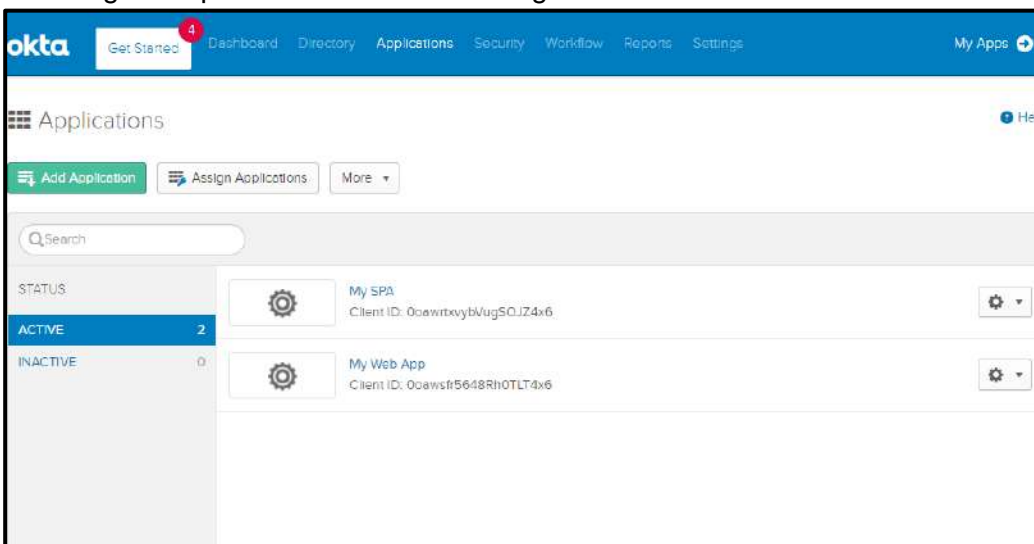


The screenshot displays the Okta Admin Console interface for configuring a web application named "My Web App". The navigation bar at the top includes "Get Started", "Dashboard", "Directory", "Applications", "Security", "Workflow", "Reports", "Settings", and "My Apps". The main content area is divided into several sections:

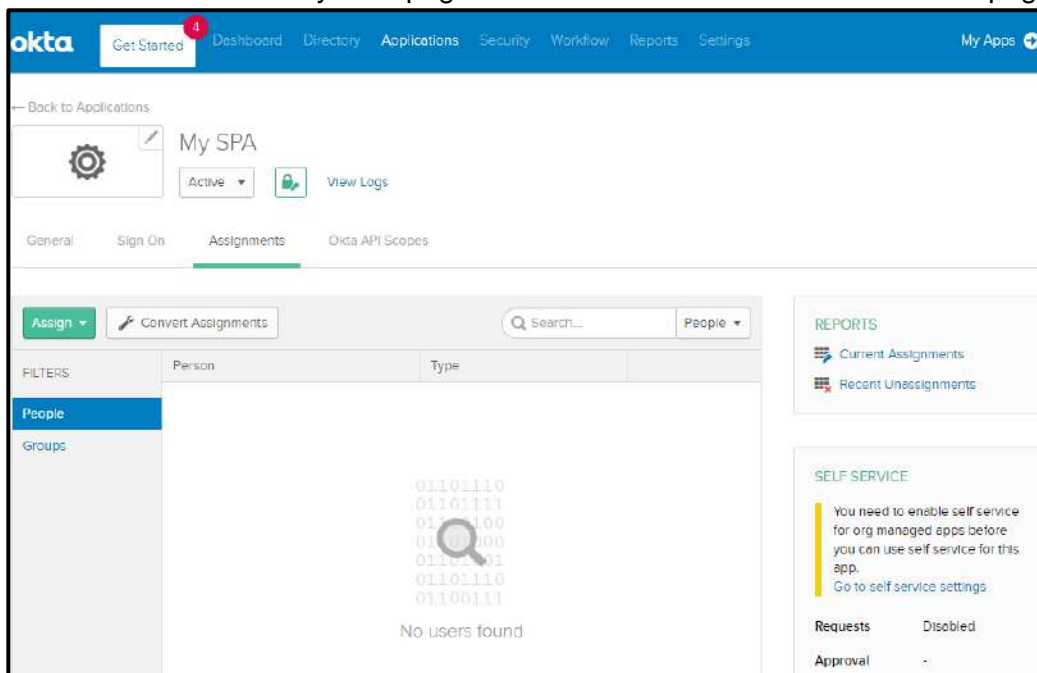
- General Settings:** Contains fields for "Application label" (My Web App), "Application type" (Web), and "Allowed grant types". Under "Client acting on behalf of a user", the "Authorization Code" option is selected, while "Client Credentials", "Refresh Token", and "Implicit (Hybrid)" are unselected.
- LOGIN:** Contains fields for "Login redirect URIs" (https://10.51.4.161:8080/eeul), "Logout redirect URIs" (https://10.51.4.161:8080/eeul), "Login initiated by" (App Only), and "Initiate login URI".
- Client Credentials:** Contains fields for "Client ID" (Doawcfr5648Rh0TLT4x6) and "Client secret" (represented by a masked field).

General Settings: All fields are required unless marked optional. Some fields may no longer be editable.

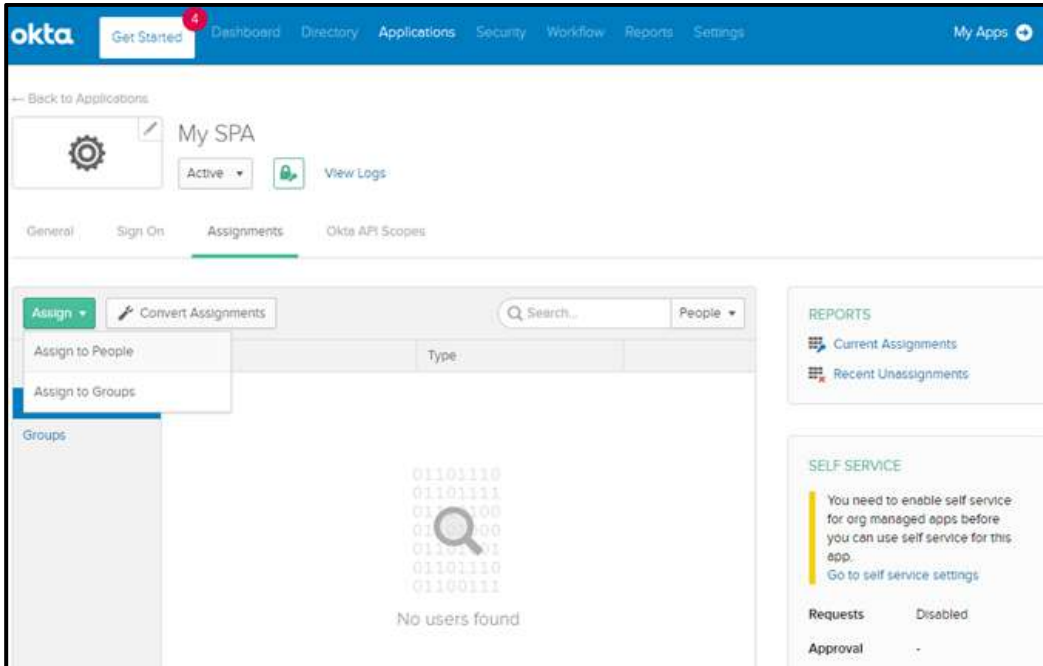
14. Click on your SPA (Single Page Application) or Web Application as desired for which you wish to get the parameters for SSO configuration.



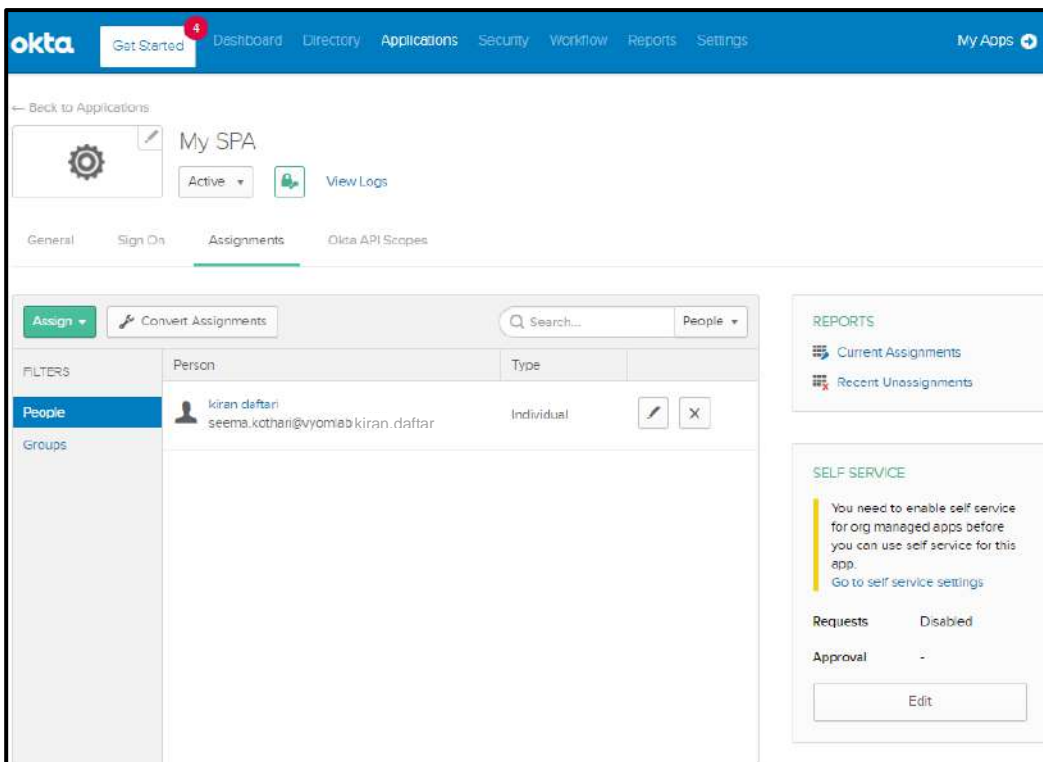
15. In this case we are on My SPA page. Click the General tab on the left of the page.



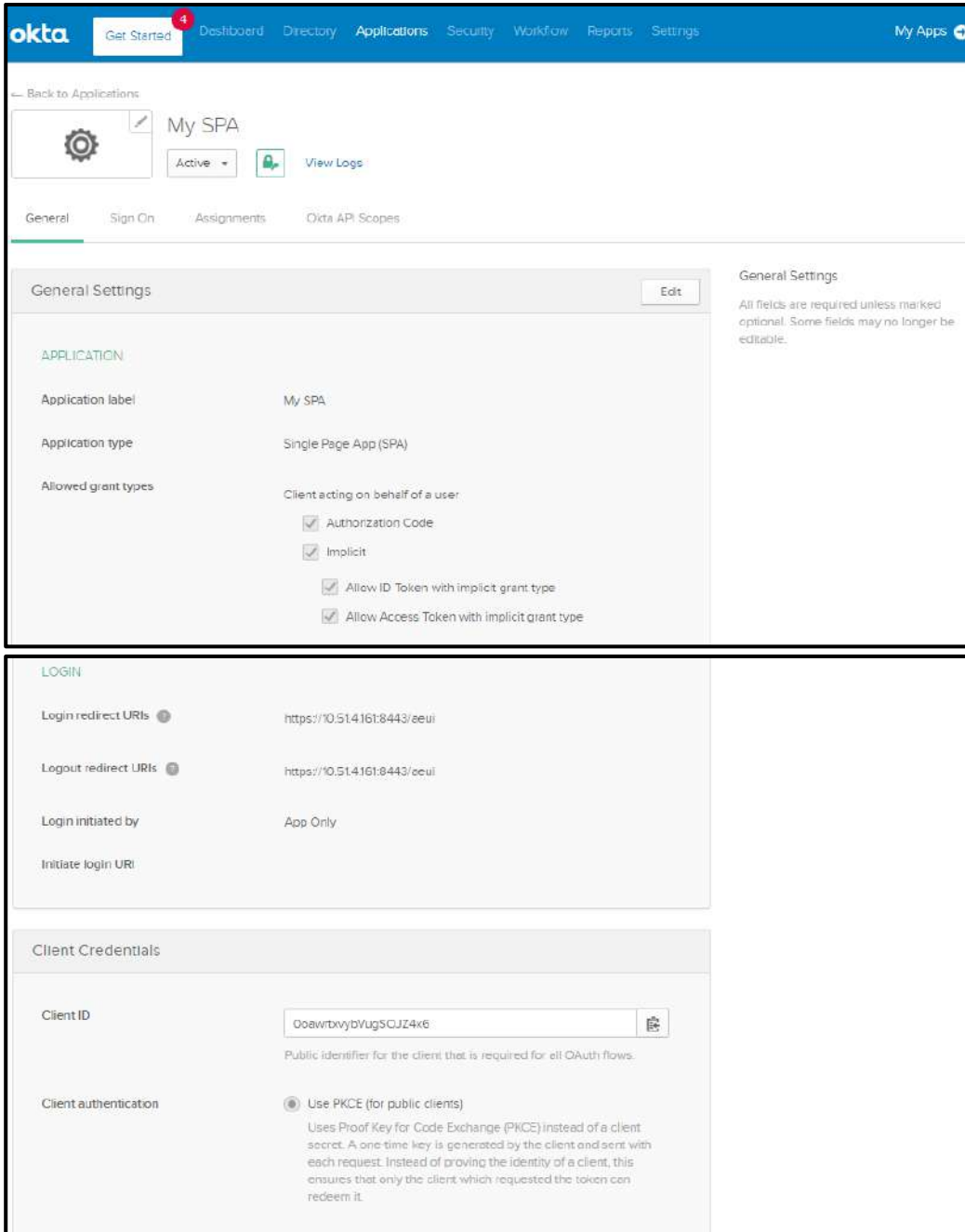
16. Select Assign to people to assign the Okta user to be mapped to AE user.



17. In the screenshot below you can see your user/people assigned My SPA. Click on the General tab.



18. Scroll down to locate Login redirect URIs. Also locate the Client ID



The screenshot displays the Okta Admin Console interface for configuring an application. The top navigation bar includes 'Get Started', 'Dashboard', 'Directory', 'Applications', 'Security', 'Workflow', 'Reports', and 'Settings'. The main content area is titled 'My SPA' and includes an 'Active' status indicator and a 'View Logs' button. Below this, there are tabs for 'General', 'Sign On', 'Assignments', and 'Okta API Scopes'. The 'General Settings' section is expanded, showing the following configuration:

- APPLICATION**
 - Application label: My SPA
 - Application type: Single Page App (SPA)
 - Allowed grant types: Client acting on behalf of a user
 - Authorization Code
 - Implicit
 - Allow ID Token with implicit grant type
 - Allow Access Token with implicit grant type

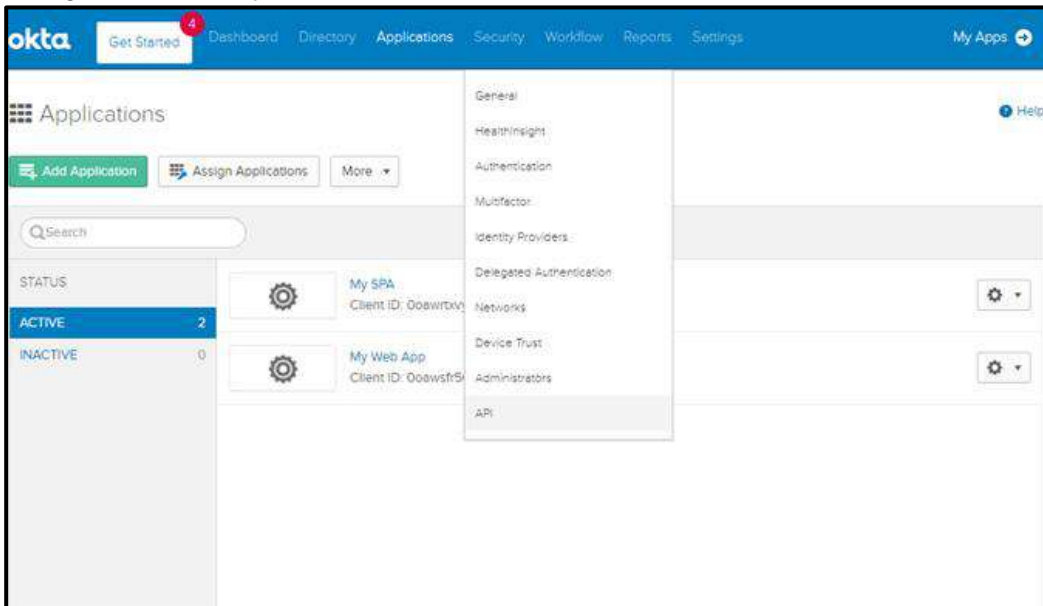
The 'LOGIN' section is also visible, showing:

- Login redirect URIs: <https://10.51.4.161:8443/eeui>
- Logout redirect URIs: <https://10.51.4.161:8443/eeui>
- Login initiated by: App Only
- Initiate login URI: (empty field)

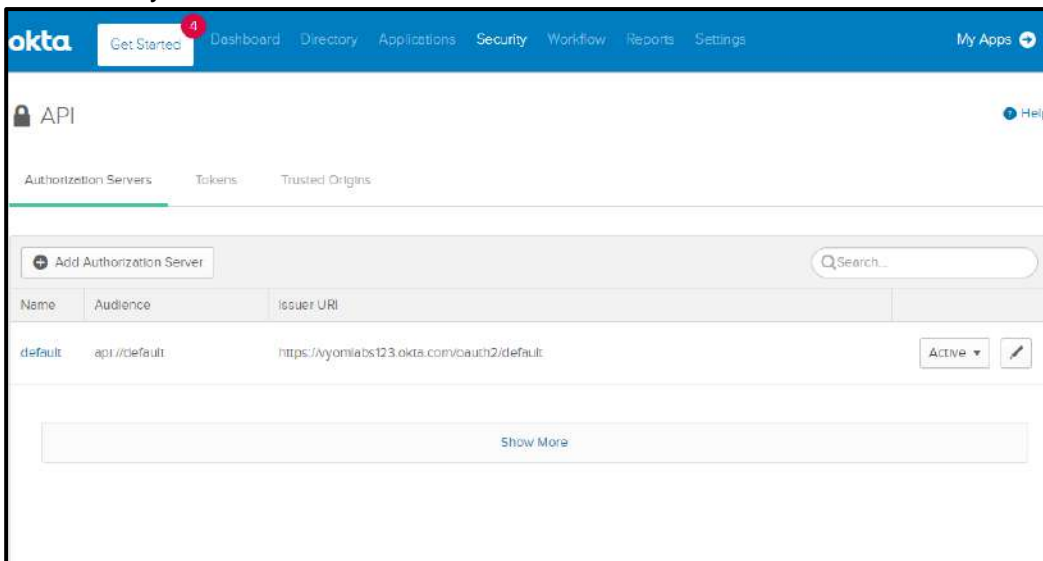
The 'Client Credentials' section is also visible, showing:

- Client ID:
- Client authentication: Use PKCE (for public clients)
 - Uses Proof Key for Code Exchange (PKCE) instead of a client secret. A one-time key is generated by the client and sent with each request. Instead of proving the identity of a client, this ensures that only the client which requested the token can redeem it.

19. Make sure that the login and logout URL are same (e.g. <https://AutomationEdge:{Port}/aeui>)
20. Navigate to Security→API menu.



21. Make sure you are on the Authorization Servers tab. Click the default link.



22. Click on Metadata URI.

The screenshot shows the Okta Admin Console interface. At the top, there is a navigation bar with 'Okta' logo and various menu items like 'Get Started', 'Dashboard', 'Directory', 'Applications', 'Security', 'Workflow', 'Reports', 'Settings', and 'My Apps'. Below the navigation bar, there is a breadcrumb trail: 'Back to Authorization Servers'. The main content area is titled 'default' and has a dropdown menu set to 'Active'. There are several tabs: 'Settings', 'Scopes', 'Claims', 'Access Policies', and 'Token Preview'. The 'Settings' tab is selected, and it shows a list of settings for the 'default' authorization server. The 'Metadata URI' field is highlighted in blue. To the right of the settings, there is a section titled 'Authorization Servers' with a brief description and a 'help page' link.

23. Now click on the Claims tab.

24. Click Add Claim, enter a Name for the claim, and configure the claim details.

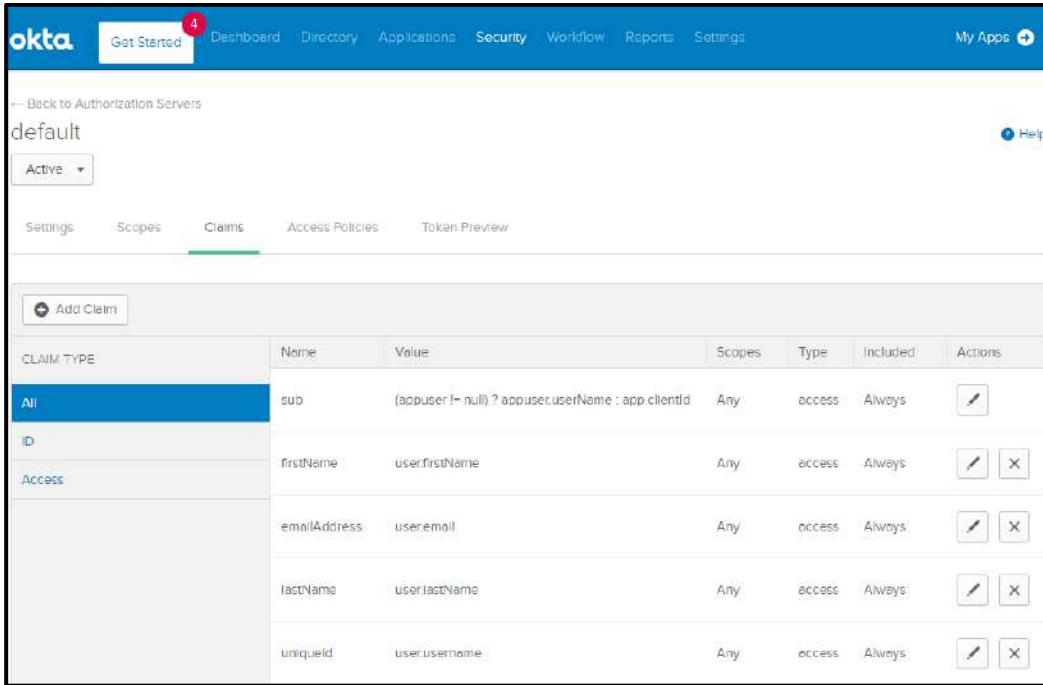
The values expression for the list of claims being used in AutomationEdge may change for different Identity Providers (IDP). The table below shows the claims for Okta IDP.

Name	Values (Case Sensitive)
uniqueId	user.username
firstName	user.firstName
lastName	user.lastName
emailAddress	user.email

It is **mandatory** to specify values for the first 3 attributes - uniqueId, firstName and lastName.

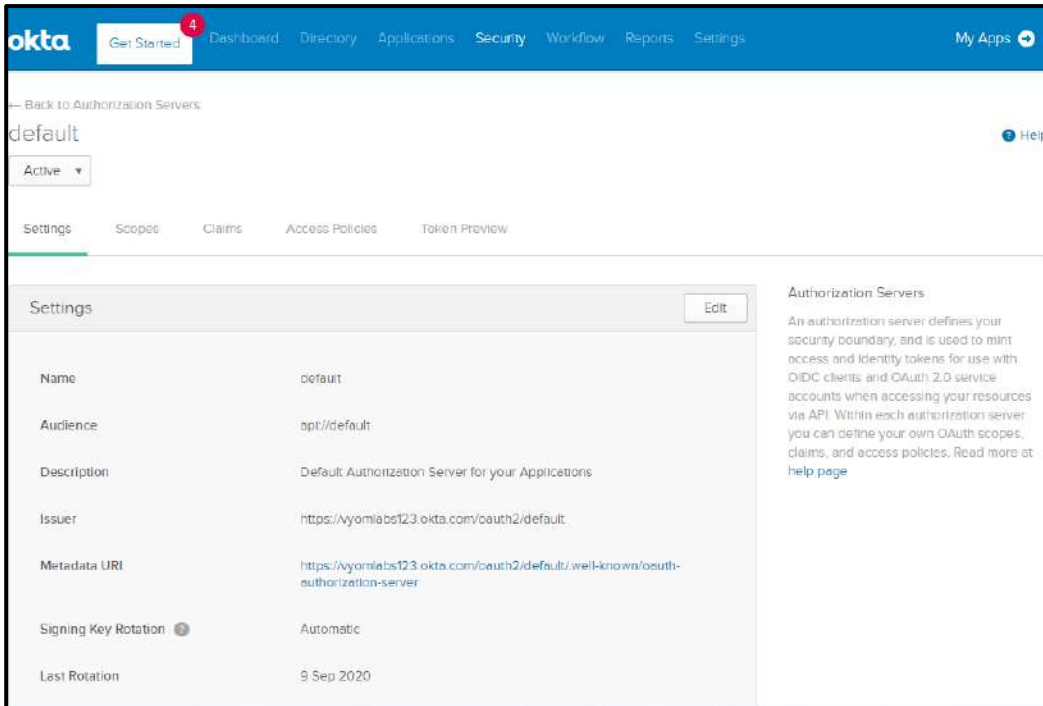
Note: (This is Okta Expression Language syntax to generate values derived from attributes in Universal Directory and app profiles. To validate an expression, use the Token Preview tab).

25. In the snapshot below we can see all the claims.



26. Navigate back to the API→Authorization Servers→default link.

27. In the Settings Tab Click on Metadata URI link.



28. Fetch the value for `authorization_endpoint` key for Identity Provider Authorization Endpoint from the json file displayed as well as other Endpoints (such as Authorization, Token and End Session Endpoints).

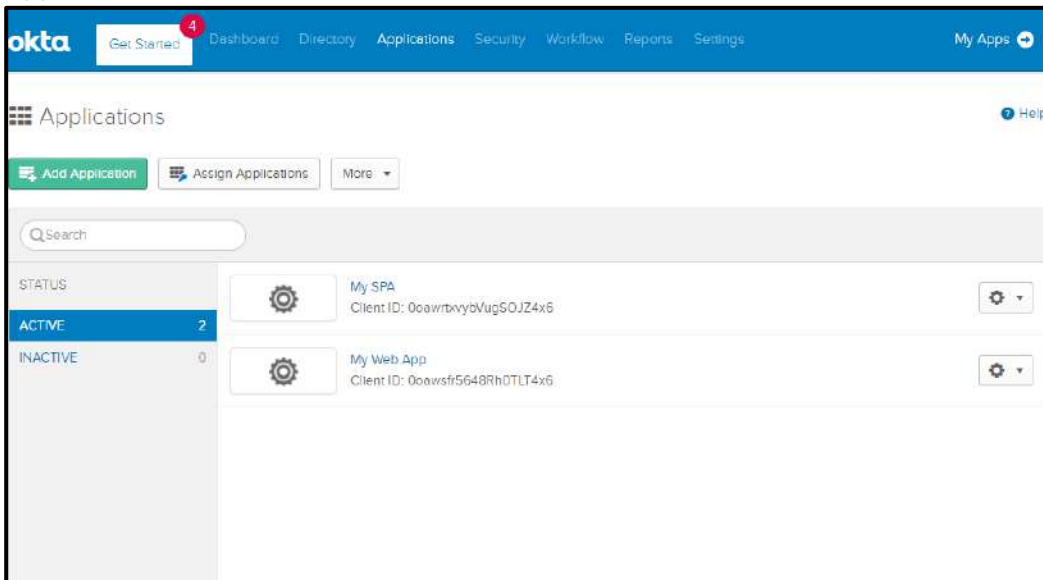
```
{
  "issuer": "https://vyomlabs123.okta.com/oauth2/default",
  "authorization_endpoint": "https://vyomlabs123.okta.com/oauth2/default/v1/authorize",
  "token_endpoint": "https://vyomlabs123.okta.com/oauth2/default/v1/token",
  "registration_endpoint": "https://vyomlabs123.okta.com/oauth2/v1/client_s",
  "jwks_uri": "https://vyomlabs123.okta.com/oauth2/default/v1/keys",
  "response_types_supported": ["code", "token", "id_token", "code_id_token", "code token", "id_token token", "code id_token token"],
  "response_modes_supported": ["query", "fragment", "form_post", "okta_post_message"],
  "grant_types_supported": ["authorization_code", "implicit", "refresh_token", "password", "client_credentials"],
  "subject_types_supported": ["public"],
  "scopes_supported": ["openid", "profile", "email", "address", "phone", "offline_access"],
  "token_endpoint_auth_methods_supported": ["client_secret_basic", "client_secret_post", "client_secret_jwt", "private_key_jwt", "none"],
  "claims_supported": ["ver", "jti", "iss", "aud", "iat", "exp", "cid", "uid", "scp", "sub"],
  "code_challenge_methods_supported": ["S256"],
  "introspection_endpoint": "https://vyomlabs123.okta.com/oauth2/default/v1/introspect",
  "introspection_endpoint_auth_methods_supported": ["client_secret_basic", "client_secret_post", "client_secret_jwt", "private_key_jwt", "none"],
  "revocation_endpoint": "https://vyomlabs123.okta.com/oauth2/default/v1/revocate",
  "revocation_endpoint_auth_methods_supported": ["client_secret_basic", "client_secret_post", "client_secret_jwt", "private_key_jwt", "none"],
  "end_session_endpoint": "https://vyomlabs123.okta.com/oauth2/default/v1/logout",
  "request_parameter_supported": true,
  "request_object_signing_alg_values_supported": ["HS256", "HS384", "HS512", "RS256", "RS384", "RS512", "ES256", "ES384", "ES512"]}

```

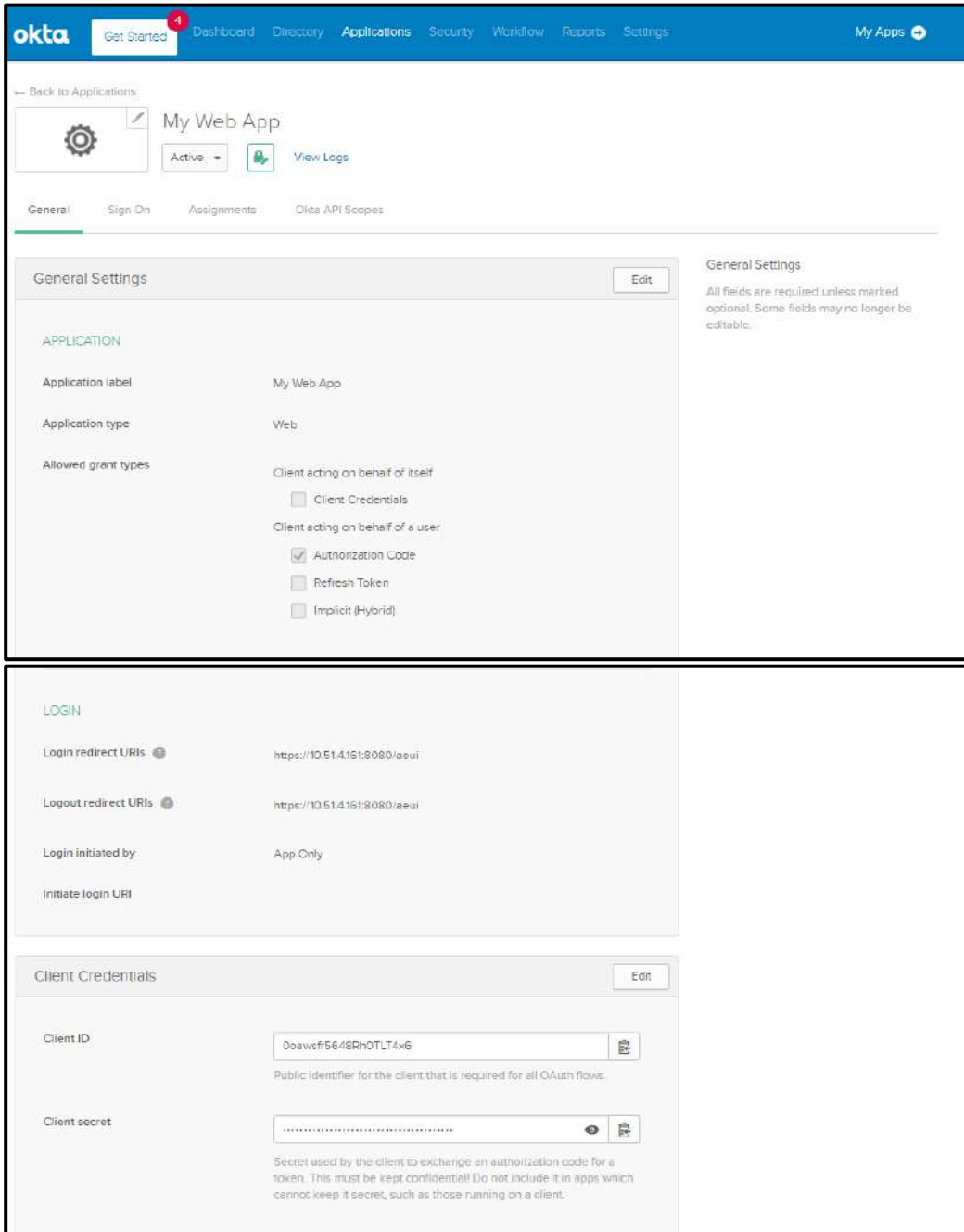
29. In this example Authorization Endpoint is,

```
"authorization_endpoint": "https://vyomlabs123.okta.com/oauth2/default/v1/authorize"
```

30. In summary to fetch Endpoints Json, in the Okta Developer Console, navigate to Security > API > Authorization Servers. Select the default link in the Name column of the authorization server. Click the metadata URL link to display the Endpoints JSON.
31. In case of Web Applications, you additionally need Client Secret. Click on your Web Application.



32. Click the General Tab. Scroll the see the Client Secret along with other configuration parameters.



The screenshot displays the Okta Admin Console interface for configuring an application named "My Web App". The navigation bar at the top includes "Get Started", "Dashboard", "Directory", "Applications", "Security", "Workflow", "Reports", "Settings", and "My Apps". The main content area is divided into several sections:

- General Settings:** This section contains fields for "Application label" (My Web App), "Application type" (Web), and "Allowed grant types". Under "Allowed grant types", there are three options: "Client acting on behalf of itself" (with a checkbox for "Client Credentials"), "Client acting on behalf of a user" (with a checked checkbox for "Authorization Code" and unchecked checkboxes for "Refresh Token" and "Implicit (Hybrid)"), and "Implicit (Hybrid)".
- LOGIN:** This section contains fields for "Login redirect URIs" (https://10.51.4.151:8080/aeui), "Logout redirect URIs" (https://10.51.4.151:8080/aeui), "Login initiated by" (App Only), and "Initiate login URI".
- Client Credentials:** This section contains fields for "Client ID" (0oawsf5648Rh0TLT4v6) and "Client secret" (a masked field). Below the "Client ID" field is a note: "Public identifier for the client that is required for all OAuth flows." Below the "Client secret" field is a note: "Secret used by the client to exchange an authorization code for a token. This must be kept confidential! Do not include it in apps which cannot keep it secret, such as those running on a client."

33. Thus we have seen key Okta setups. We also saw how to capture required configuration parameters from Okta for AE Single Sign-On Settings.

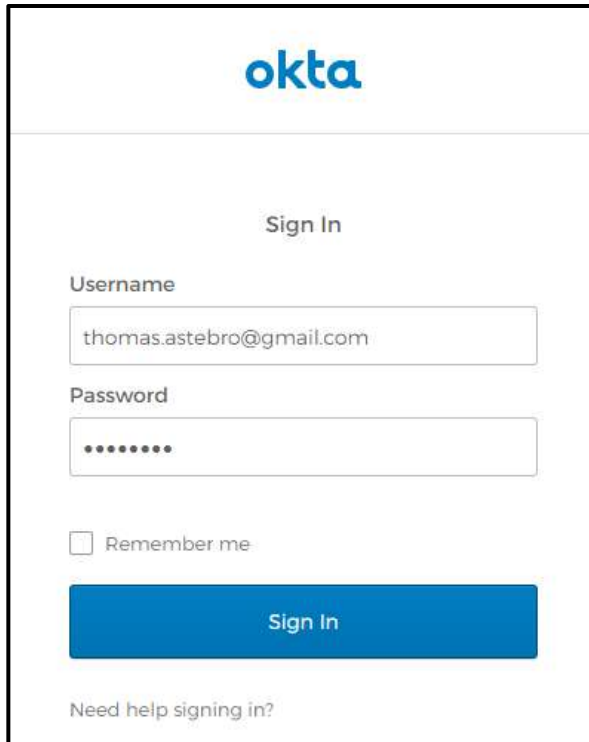
2.2 Okta(IDP) initiated SSO to AE using OAuth/OpenID

In this section we demonstrate setups in Okta and AutomationEdge for IDP initiated SSO for OpenID.

2.2.1 Setups in Okta

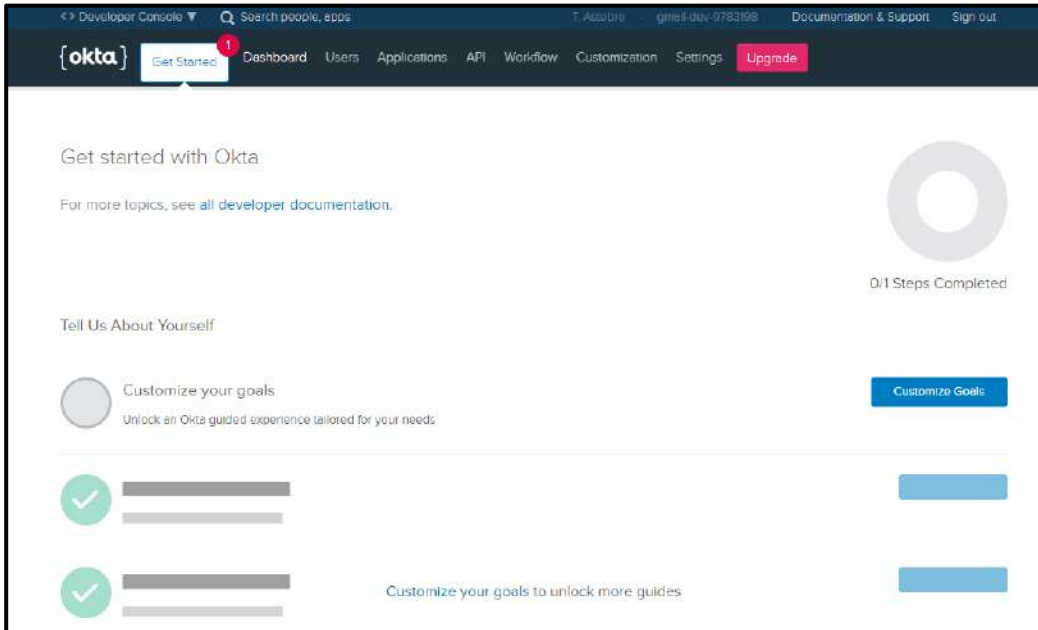
Following are the setups in Okta for IDP initiated SSO for OpenID,

1. Sign in to OKTA.

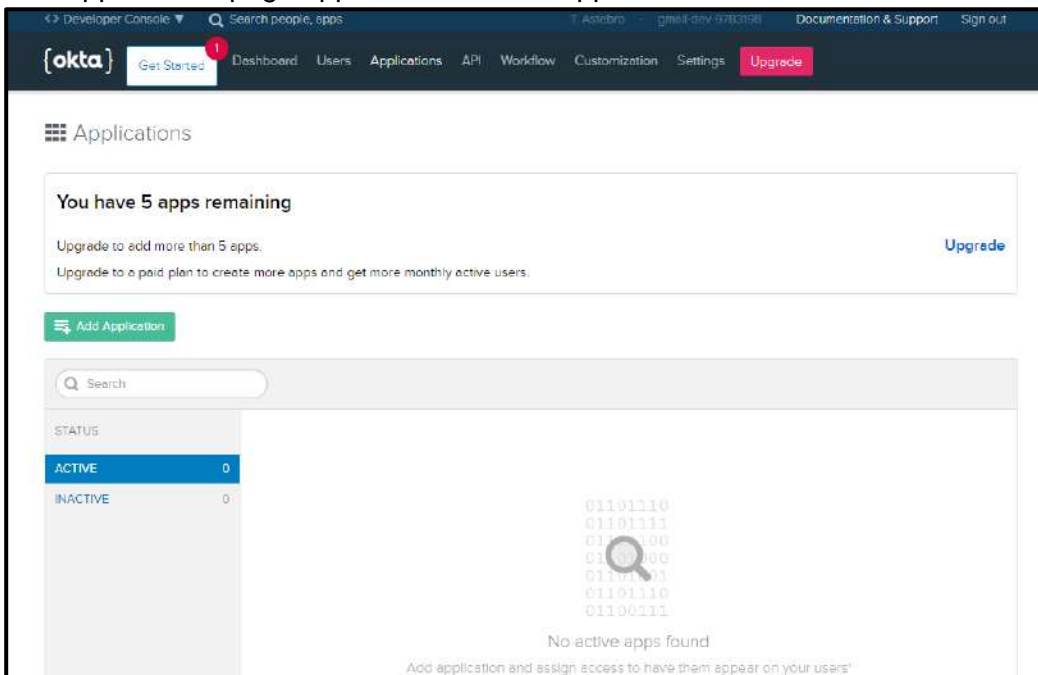


The screenshot shows the Okta Sign In page. At the top is the Okta logo. Below it is the text "Sign In". There are two input fields: "Username" with the value "thomas.astebro@gmail.com" and "Password" with masked characters ".....". Below the password field is a checkbox labeled "Remember me" which is unchecked. At the bottom is a blue "Sign In" button. Below the button is the text "Need help signing in?".

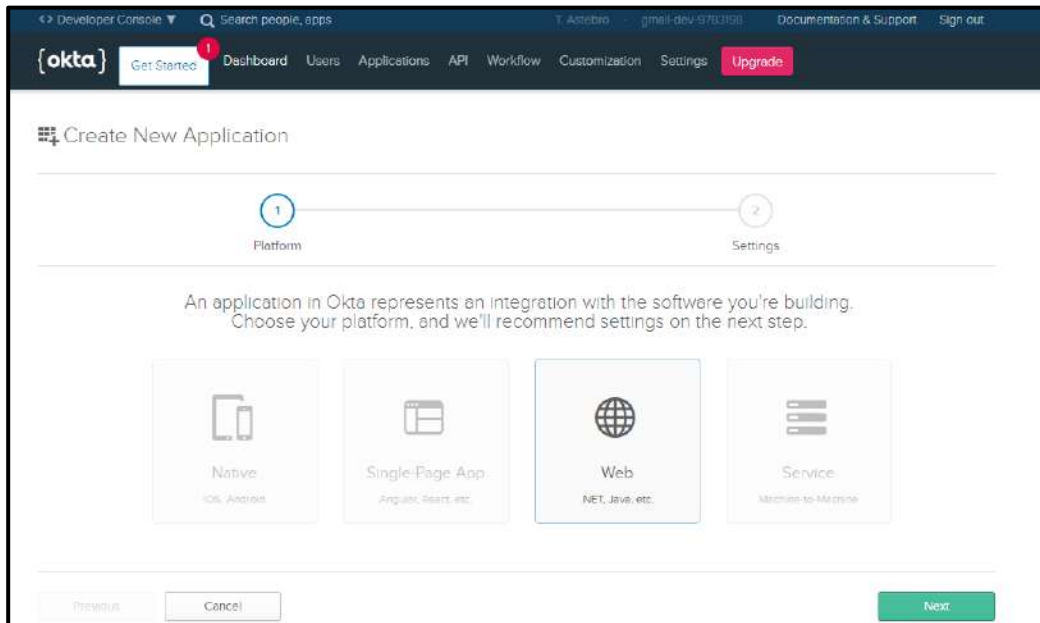
2. The Getting Started page appears. Click on the Applications tab.
3. Click Applications from the drop-down menu.



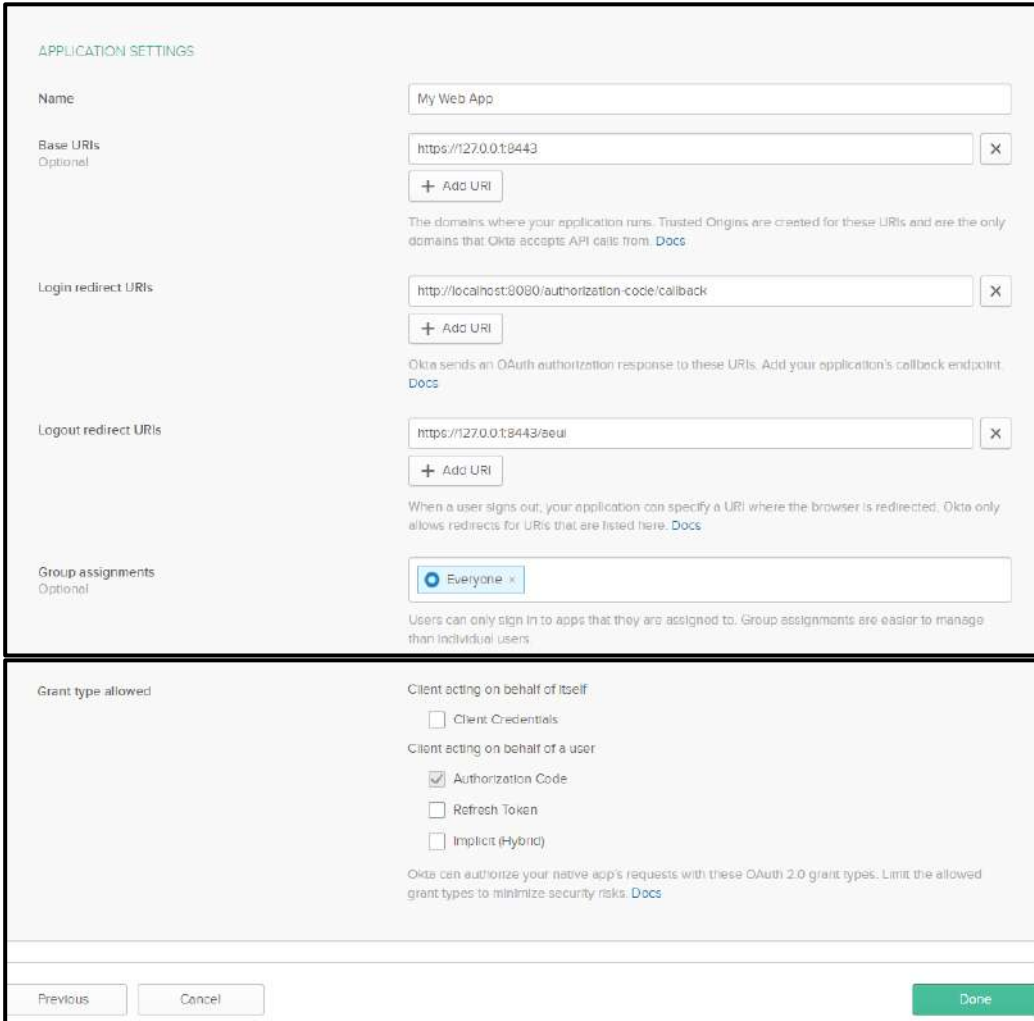
4. The Applications page appears. Click Add Application button.



5. Create a Web application by choosing Web tile.
6. Click Next.



7. On this page you need to configure Application Settings.
8. Create an application with the configurations as seen in the screenshots below. The application name we have provided is 'My Web App'
9. Then add Application name, Login redirect URI and Logout redirect URI as shown in image. Login redirect URI and Logout redirect URI are should be same for AE and it is the base URL for aeui in the form `https://{host}:{port}/aeui`
10. Click Done.



APPLICATION SETTINGS

Name: My Web App

Base URIs (Optional): `https://127.0.0.1:8443`

The domains where your application runs. Trusted Origins are created for these URIs and are the only domains that Okta accepts API calls from. [Docs](#)

Login redirect URIs: `http://localhost:3030/authorization-code/callback`

Okta sends an OAuth authorization response to these URIs. Add your application's callback endpoint. [Docs](#)

Logout redirect URIs: `https://127.0.0.1:8443/aeui`

When a user signs out, your application can specify a URI where the browser is redirected. Okta only allows redirects for URIs that are listed here. [Docs](#)

Group assignments (Optional):
Users can only sign in to apps that they are assigned to. Group assignments are easier to manage than individual users.

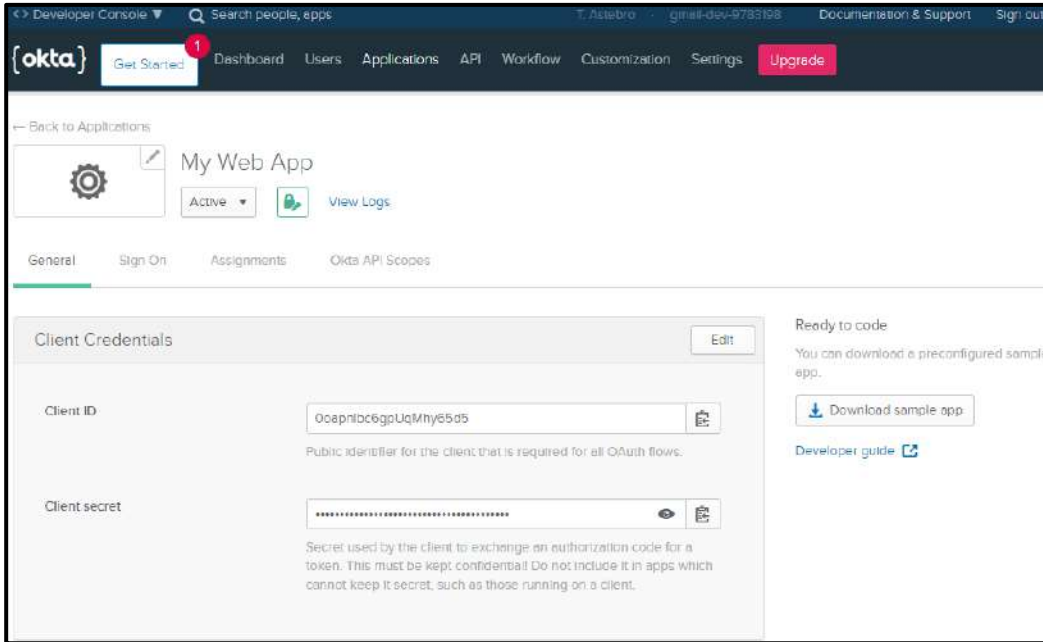
Grant type allowed:

Client acting on behalf of itself
 Client Credentials

Client acting on behalf of a user
 Authorization Code
 Refresh Token
 Implicit (Hybrid)

Okta can authorize your native app's requests with these OAuth 2.0 grant types. Limit the allowed grant types to minimize security risks. [Docs](#)

11. My Web App is now visible as seen below.



12. Scroll down and edit the application just created by clicking on edit button next to General Settings.

General Settings

Okta domain: dev-9783198.okta.com

APPLICATION

Application label: My Web App

Application type: Web

Allowed grant types:

- Client acting on behalf of itself:
 - Client Credentials
- Client acting on behalf of a user:
 - Authorization Code
 - Refresh Token
 - Implicit (Hybrid)
 - Allow ID Token with Implicit grant type
 - Allow Access Token with Implicit grant type

LOGIN

Login redirect URIs:

Logout redirect URIs:

Login initiated by:

Application visibility:

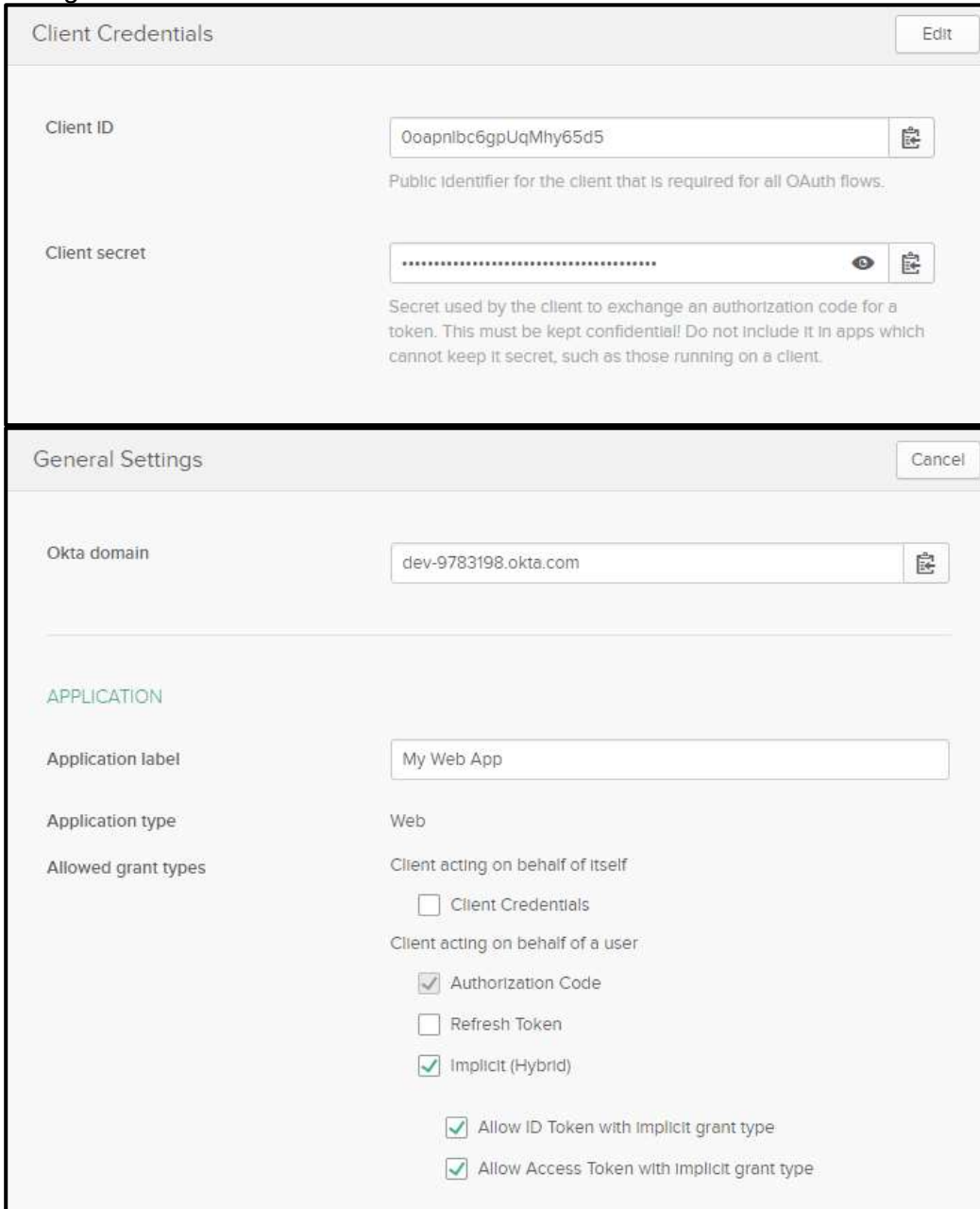
- Display application icon to users
- Display application icon in the Okta Mobile app

Login flow:

- Redirect to app to initiate login (OIDC Compliant)
- Send ID Token directly to app (Okta Simplified)

Initiate login URI:

13. After creating an application then go and edit the application just created by clicking on edit button as shown in image below
14. Check all the checkboxes indicated by an arrow as in images below and fill all the information pointed by arrow. Initiate login URI is important here. It should be **Login redirect URI + `##/sso-login?orgCode=<Your TENANT orgCode>`** (In this example it is `https://127.0.0.1:8443/aeui/#/sso-login?orgCode=TENANTCLOUD`). And save the changes.



The screenshot displays the configuration interface for an application, divided into two main sections: Client Credentials and General Settings.

Client Credentials (Top section, with an 'Edit' button):

- Client ID:** A text input field containing '0oapnlbc6gpUqMhy65d5'. Below it, a note states: 'Public Identifier for the client that is required for all OAuth flows.'
- Client secret:** A text input field with masked characters (dots). Below it, a note states: 'Secret used by the client to exchange an authorization code for a token. This must be kept confidential! Do not include it in apps which cannot keep it secret, such as those running on a client.'

General Settings (Bottom section, with a 'Cancel' button):

- Okta domain:** A text input field containing 'dev-9783198.okta.com'.
- APPLICATION** (Section header):
- Application label:** A text input field containing 'My Web App'.
- Application type:** A dropdown menu set to 'Web'.
- Allowed grant types:** A list of checkboxes:
 - Client acting on behalf of itself
 - Client Credentials
 - Client acting on behalf of a user:
 - Authorization Code
 - Refresh Token
 - Implicit (Hybrid)
 - Allow ID Token with Implicit grant type
 - Allow Access Token with Implicit grant type

LOGIN

Login redirect URIs ⓘ

Logout redirect URIs ⓘ

Login initiated by

Application visibility Display application icon to users
 Display application icon in the Okta Mobile app

Login flow Redirect to app to initiate login (OIDC Compliant)
 Send ID Token directly to app (Okta Simplified)

Initiate login URI

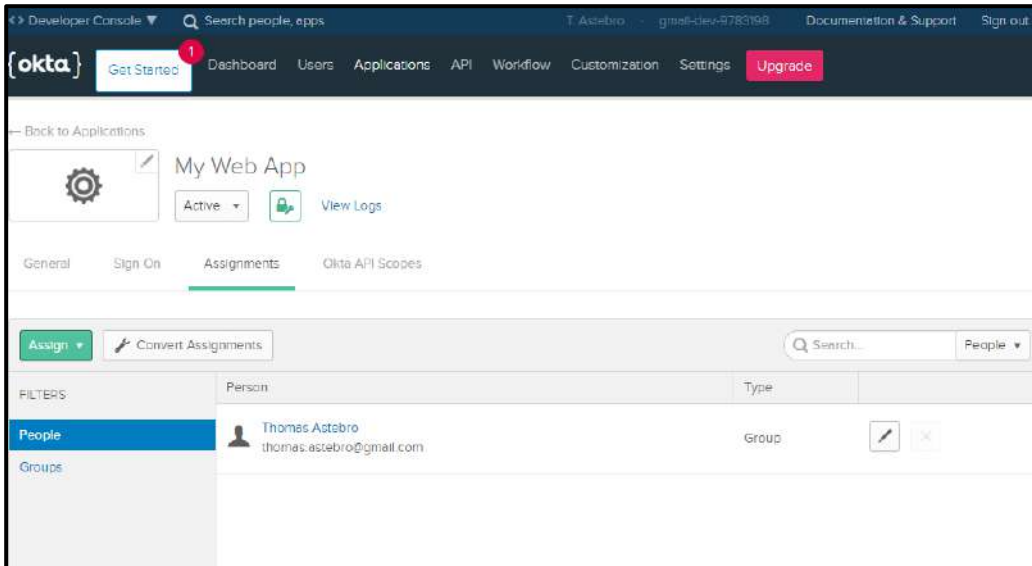
15. At the end of configuration, you will see an App Embed link. If you simply copy and paste this link in browser, it will invoke IDP initiated SSO flow. But there is also another way to do this.

App Embed Link

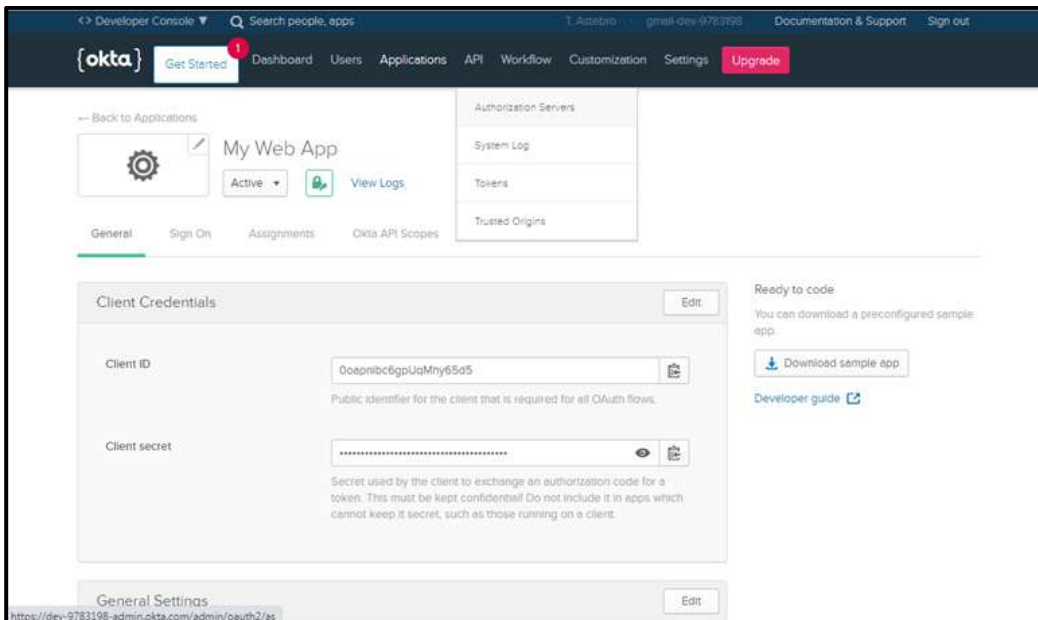
EMBED LINK

You can use the URL below to sign into OpenID Connect Client from a portal or other location outside of Okta.

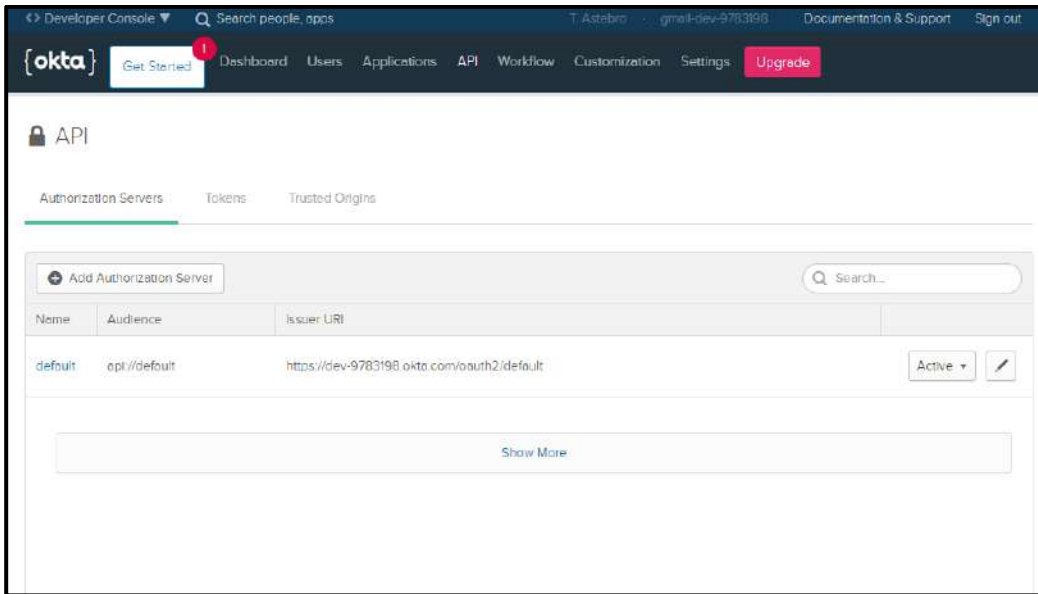
16. On My Web App go to the Assignments tab.
17. You can see that Thomas Astebro is already assigned to My Web App.
18. You may also Search for the people to assign this My Web App application. Once the details for the person are visible below, Click Save and Go Back.



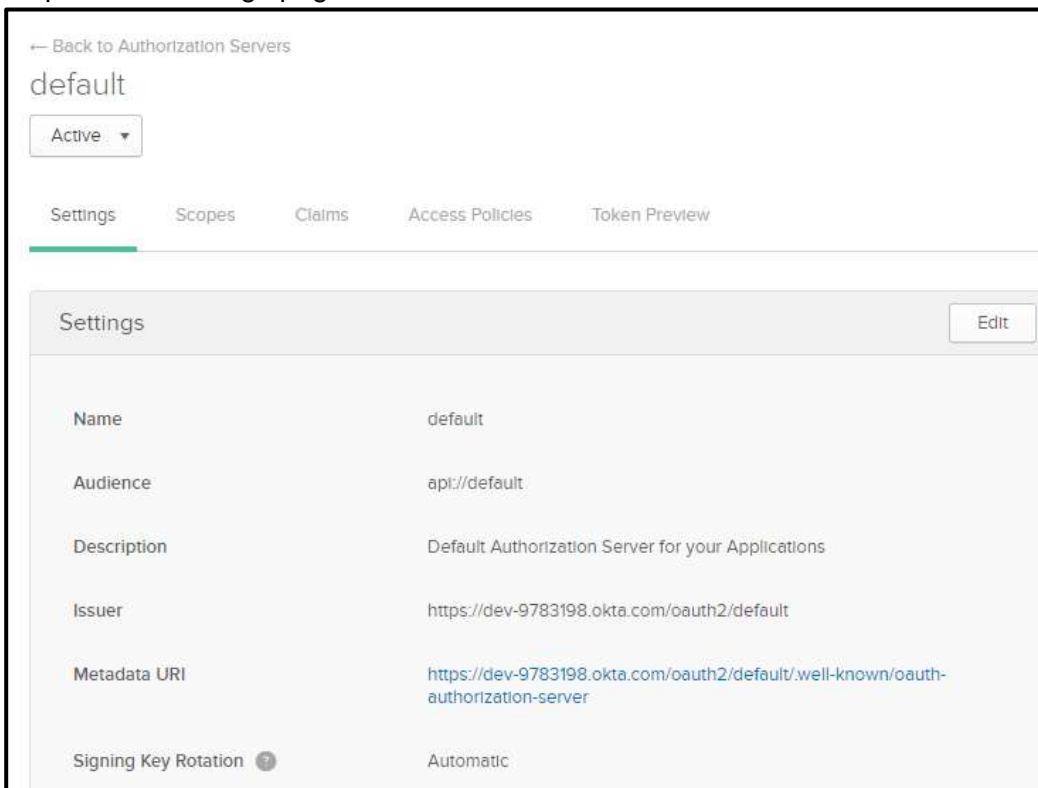
19. Under API click Authorization Servers.



20. Click the default link.



21. It opens the Settings page as seen below. Click the Metadata URI link.



22. It opens Metadata in XML format as seen below.

```
{
  "issuer": "https://dev-9783198.okta.com/oauth2/default",
  "authorization_endpoint": "https://dev-9783198.okta.com/oauth2/default/v1/authorize",
  "token_endpoint": "https://dev-9783198.okta.com/oauth2/default/v1/token",
  "registration_endpoint": "https://dev-9783198.okta.com/oauth2/default/v1/clients",
  "jwks_uri": "https://dev-9783198.okta.com/oauth2/default/v1/keys",
  "response_types_supported": ["code", "token", "id_token", "code id token", "code token", "id_token token", "code id_token token"],
  "response_modes_supported": ["query", "fragment", "form_post", "okta_post_message"],
  "grant_types_supported": ["authorization_code", "implicit", "refresh_token", "password", "client_credentials"],
  "subject_types_supported": ["public"],
  "scopes_supported": ["openid", "profile", "email", "address", "phone", "offline_access"],
  "token_endpoint_auth_methods_supported": ["client_secret_basic", "client_secret_post", "client_secret_jwt", "private_key_jwt", "none"],
  "claims_supported": ["ver", "jti", "iss", "aud", "iat", "exp", "cid", "uid", "scp", "sub"],
  "code_challenge_methods_supported": ["S256"],
  "introspection_endpoint": "https://dev-9783198.okta.com/oauth2/default/v1/introspect",
  "introspection_endpoint_auth_methods_supported": ["client_secret_basic", "client_secret_post", "client_secret_jwt", "private_key_jwt", "none"],
  "revocation_endpoint": "https://dev-9783198.okta.com/oauth2/default/v1/revoke",
  "revocation_endpoint_auth_methods_supported": ["client_secret_basic", "client_secret_post", "client_secret_jwt", "private_key_jwt", "none"],
  "end_session_endpoint": "https://dev-9783198.okta.com/oauth2/default/v1/logout",
  "request_parameter_supported": true,
  "request_object_signing_alg_values_supported": ["HS256", "HS384", "HS512", "RS256", "RS384", "RS512", "ES256", "ES384", "ES512"]}
}
```

23. Since we support claims in the AE, now click on Claims Tab. Add Claims (similar to what was added in AE initiated SSO with Okta using OAuth/OpenID) as listed and discussed below.
24. Add Attributes/Claims by specifying – Name and Value. The values expression for the list of claims being used in AutomationEdge may change for different Identity Providers (IDP). The table below shows the Attributes/ Claims for Okta IDP to be used for OAuth/OpenID.
25. Click Add Claim, enter a Name for the claim, and configure the claim details. The values expression for the list of claims being used in AutomationEdge may change for different Identity Providers (IDP). The table below shows the claims for Okta IDP.

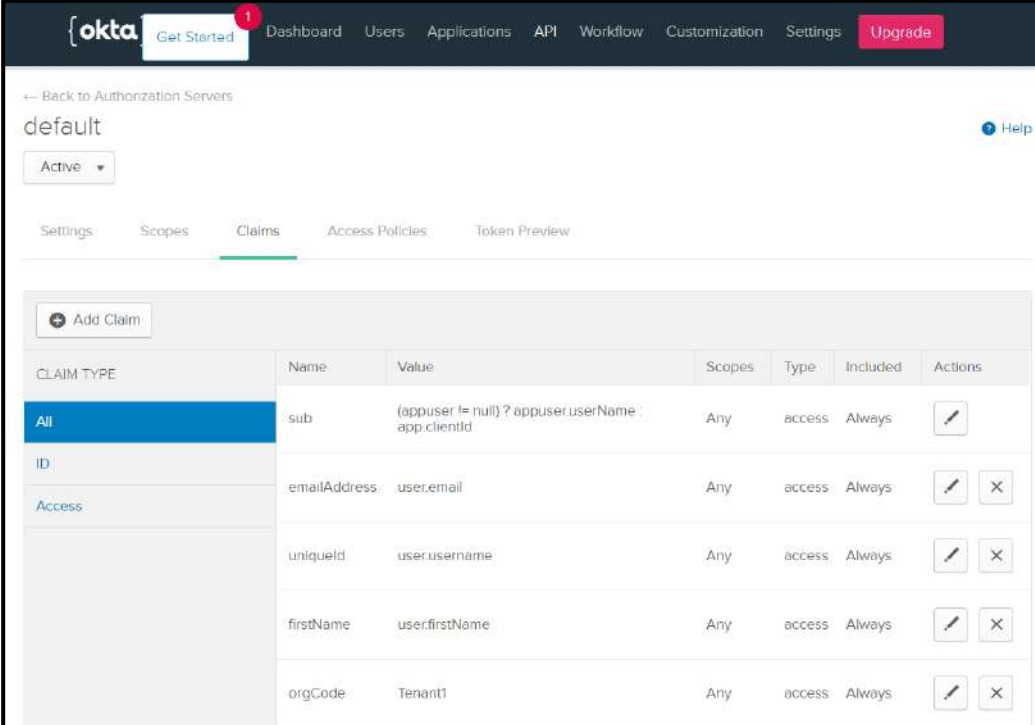
Name	Values (Case Sensitive)
uniqueId	user.username
firstName	user.firstName
lastName	user.lastName
emailAddress	user.email
orgCode	{{OrgCode}}

 **Note:**










It is **mandatory** to specify values for the first attributes - uniqueId and orgCode. It is preferred to provide firstName, lastName and emailAddress for a complete profile view.

(This is Okta Expression Language syntax to generate values derived from attributes in Universal Directory and app profiles. To validate an expression, use the Token Preview tab).

26. In the snapshot below we can see all the claims.



The screenshot shows the Okta Admin Console interface for configuring claims on a default authorization server. The navigation bar includes 'Get Started', 'Dashboard', 'Users', 'Applications', 'API', 'Workflow', 'Customization', 'Settings', and 'Upgrade'. The main content area is titled 'default' and has a status of 'Active'. The 'Claims' tab is selected, showing a table of configured claims. A '+ Add Claim' button is visible at the top left of the table.

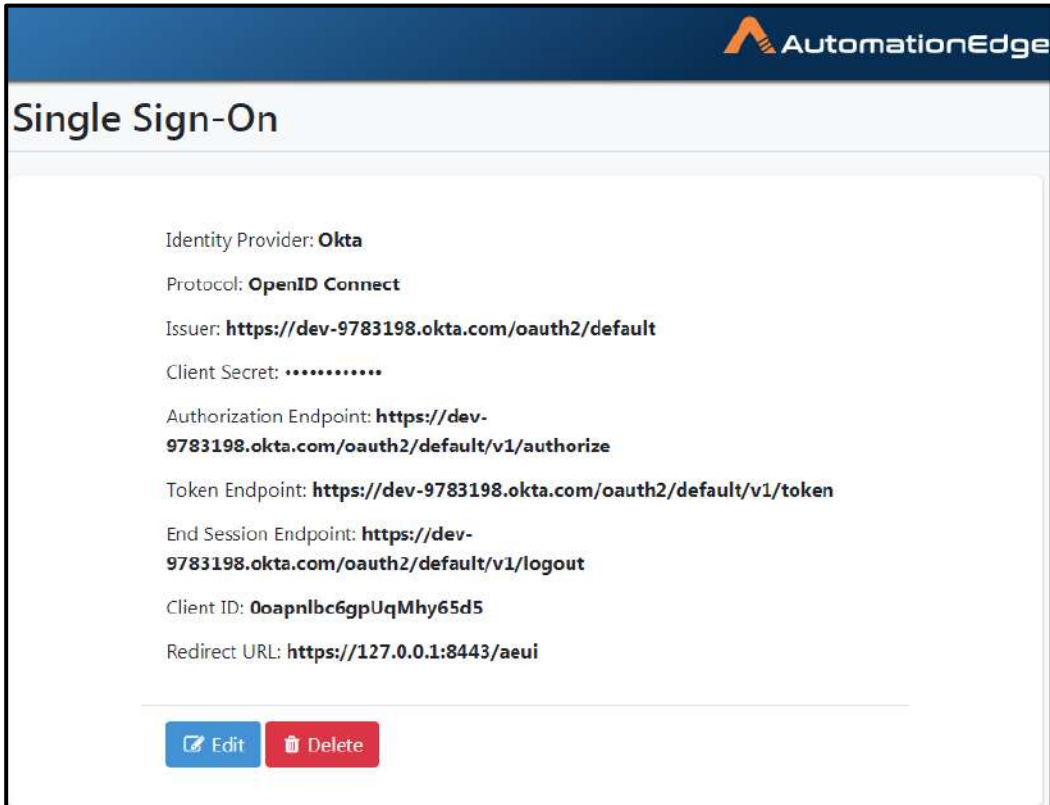
CLAIM TYPE	Name	Value	Scopes	Type	Included	Actions
All	sub	(appuser != null) ? appuser.userName : app.clientId	Any	access	Always	
ID	emailAddress	user.email	Any	access	Always	 
Access	uniqueid	user.username	Any	access	Always	 
	firstName	user.firstName	Any	access	Always	 
	orgCode	Tenant1	Any	access	Always	 

27. This completes Okta setups for IDP initiated SSO.

2.2.2 Setups on AutomationEdge and Single Sign-On

In this section we showcase the AutomationEdge setups.

1. You may import the contents of Metadata URI to setup Single Sign-On in AutomationEdge.

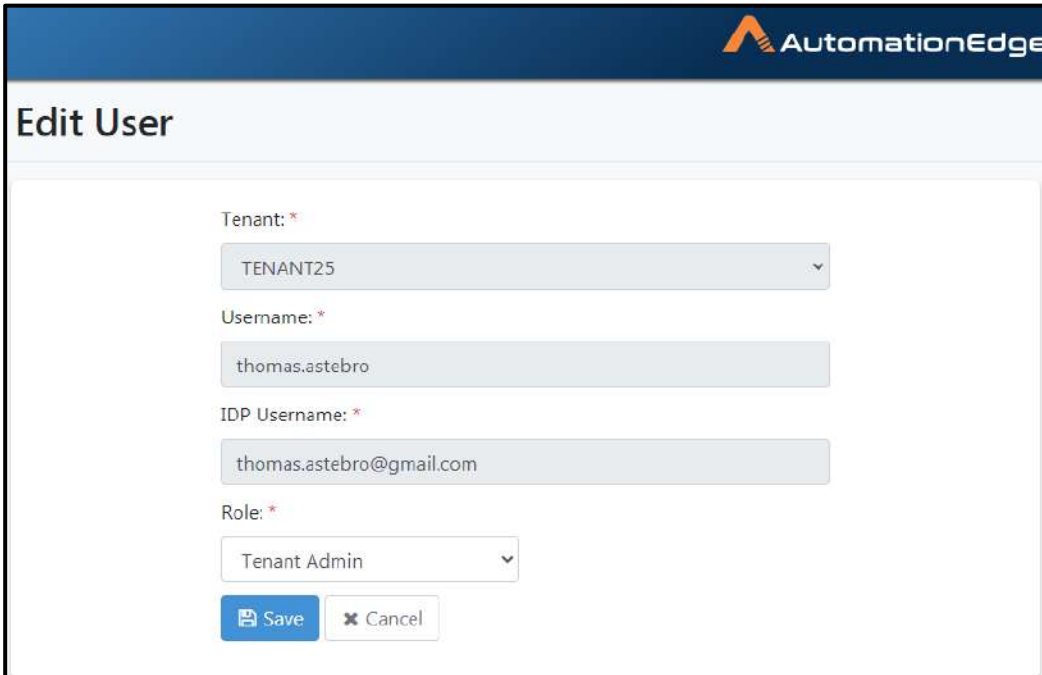


The screenshot shows the AutomationEdge interface for configuring Single Sign-On. The page has a dark blue header with the AutomationEdge logo. Below the header, the title "Single Sign-On" is displayed. The main content area lists the following configuration details:

- Identity Provider: **Okta**
- Protocol: **OpenID Connect**
- Issuer: **https://dev-9783198.okta.com/oauth2/default**
- Client Secret: **.....**
- Authorization Endpoint: **https://dev-9783198.okta.com/oauth2/default/v1/authorize**
- Token Endpoint: **https://dev-9783198.okta.com/oauth2/default/v1/token**
- End Session Endpoint: **https://dev-9783198.okta.com/oauth2/default/v1/logout**
- Client ID: **0oapnlbc6gpUqMhy65d5**
- Redirect URL: **https://127.0.0.1:8443/aeui**

At the bottom of the configuration area, there are two buttons: a blue "Edit" button and a red "Delete" button.

2. Create an SSO user in AutomationEdge mapping it to an IDP user with permissions on IDP application.



Edit User

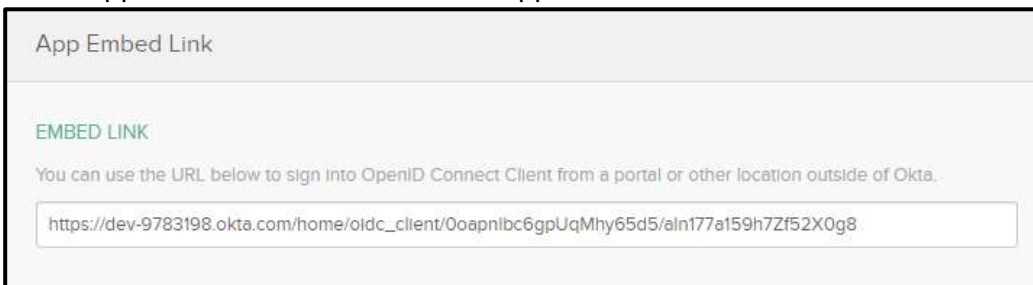
Tenant: *
TENANT25

Username: *
thomas.astebro

IDP Username: *
thomas.astebro@gmail.com

Role: *
Tenant Admin

3. In the Applications General tab locate App Embed Link URL as seen below.



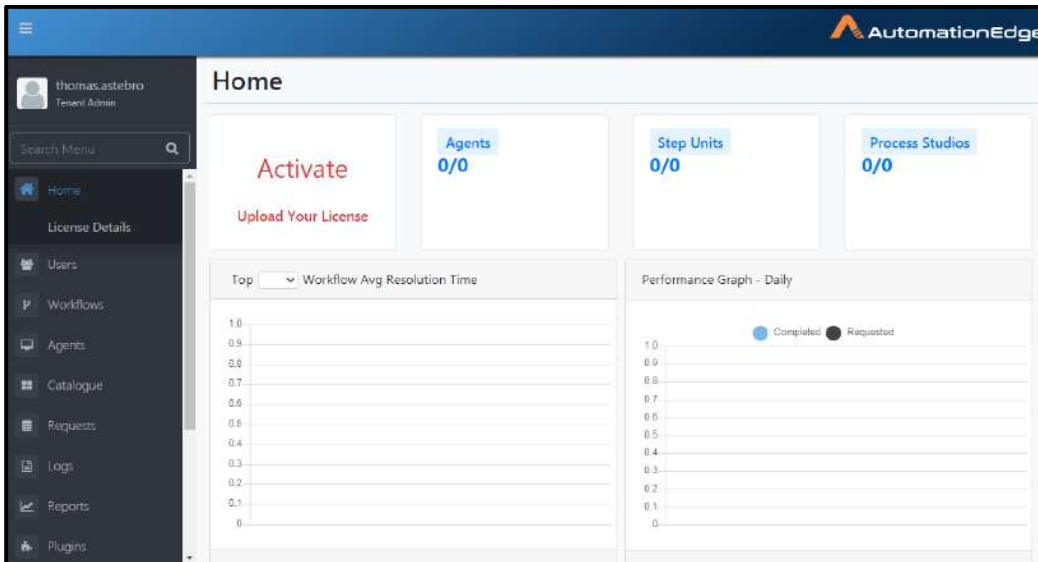
App Embed Link

EMBED LINK

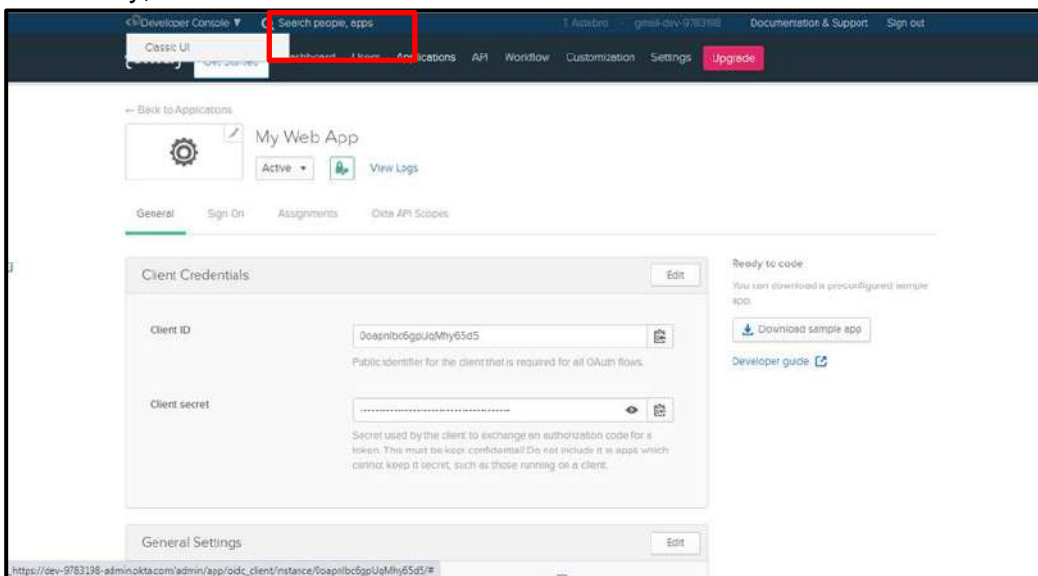
You can use the URL below to sign into OpenID Connect Client from a portal or other location outside of Okta.

https://dev-9783198.okta.com/home/oidc_client/0oapnbc6gpUqMhy65d5/aln177a159h7Zf52X0g8

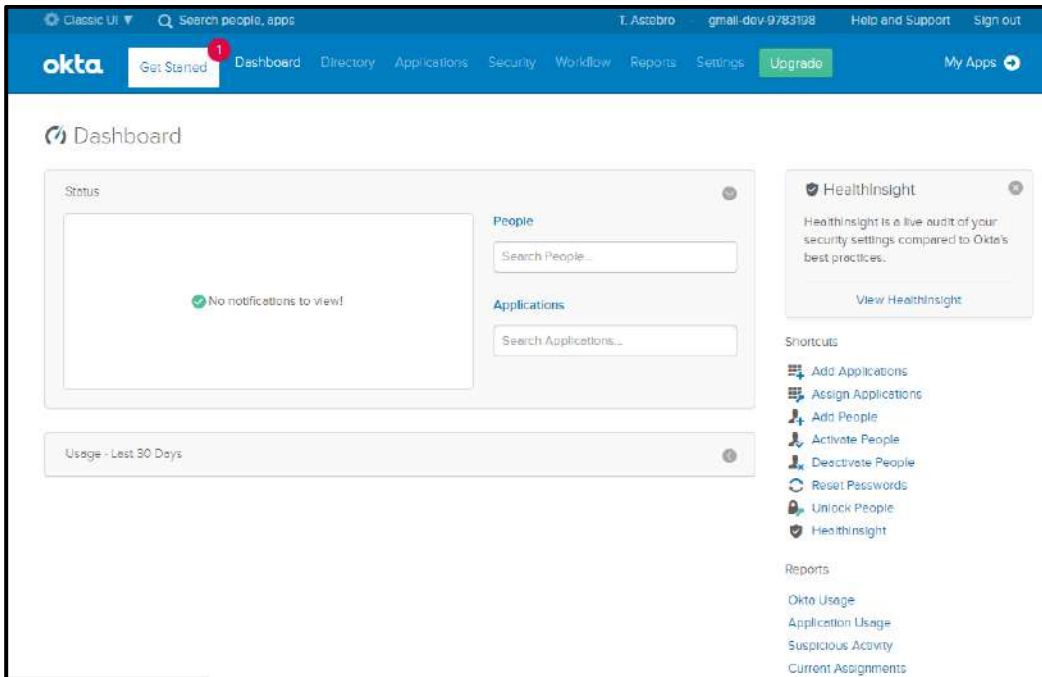
4. Type this URL on the browser and it redirects to AutomationEdge with IDP initiated SSO.



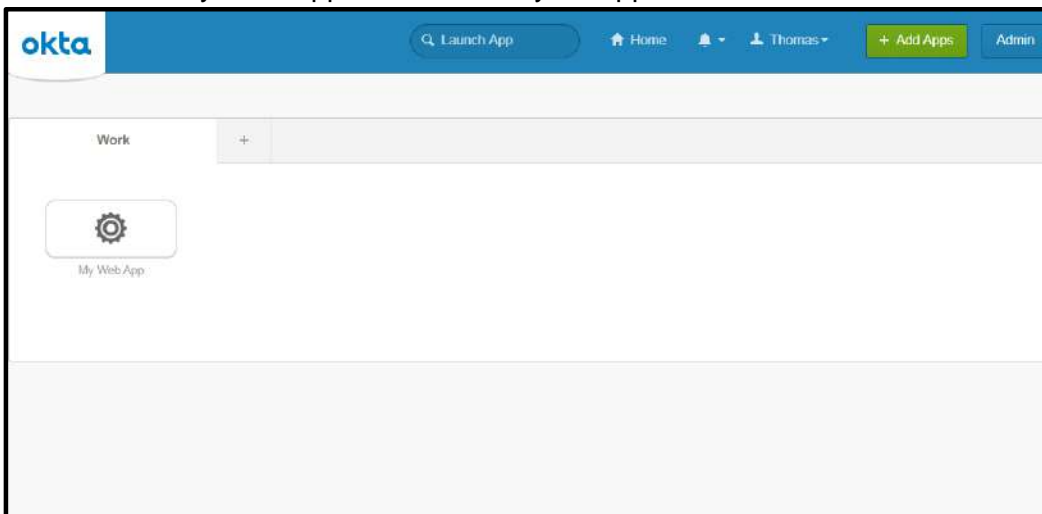
5. Alternately, switch to Okta Classic UI as seen below.



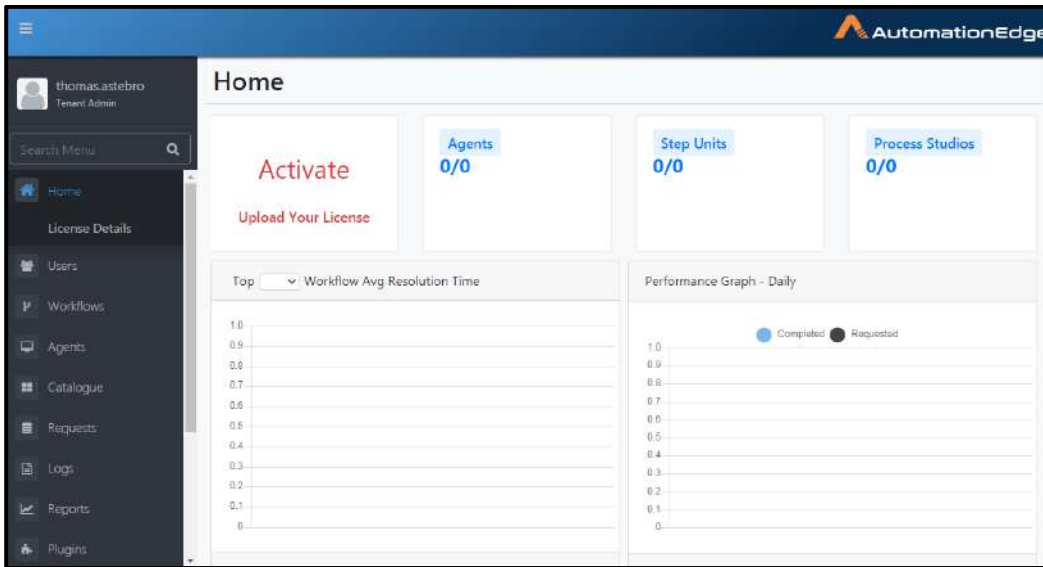
6. Click My Apps on the right hand upper corner.



7. You can see My Web App icon. Click on your application.



8. Clicking on the App takes you to AutomationEdge with IDP initiated SSO.



9. This completes the process of IDP initiated SSO.

2.3 AE initiated SSO with Okta using SAML

Okta Identity Provider supports OAuth 2.0/OpenID Connect and SAML protocols.

In this section we demonstrate configurations to setup AutomationEdge SSO with Okta using SAML protocol.

We will also showcase how to get the required parameters for AutomationEdge – Keycloak Single Sign-On Settings.

The following parameters are obtained from IDP configuration,

- Identity Provider Metadata (store in descriptor.xml)
- Client ID
- Redirect URIs

For AE SSO configurations we need,

- Keystore file, Keystore Alias, Keystore Password

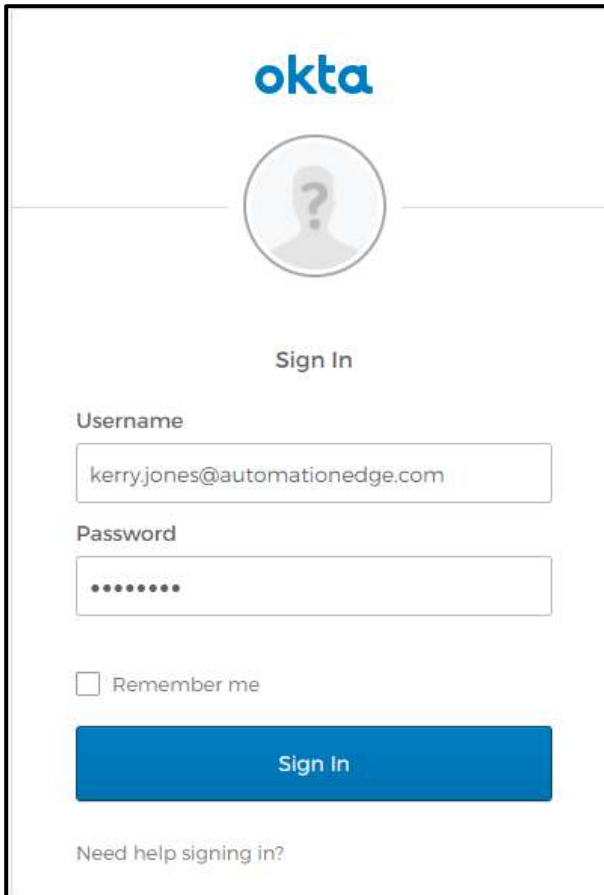
For IDP SSO configurations we need,

- Certificate file (.crt)

 **Note:** For Keystore and Certificate; to generate Self Signed or CA Certificate refer to section [2.9 Keystore and Certificate Generation](#)

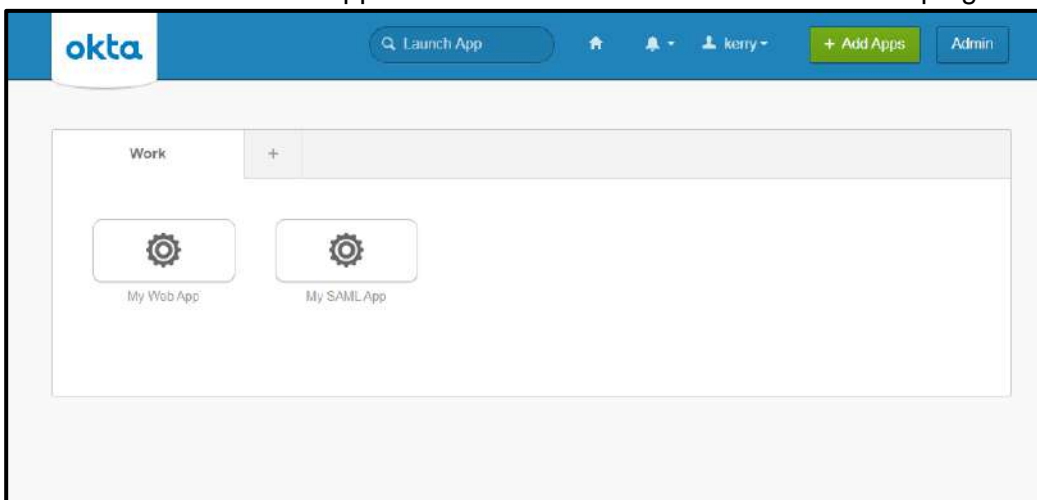
Following are the steps for key configurations for Identity Provider – Okta SAML Application and also demonstrates the navigation steps to fetch the parameters mentioned above.

1. Go to the Okta login screen and Sign-In.

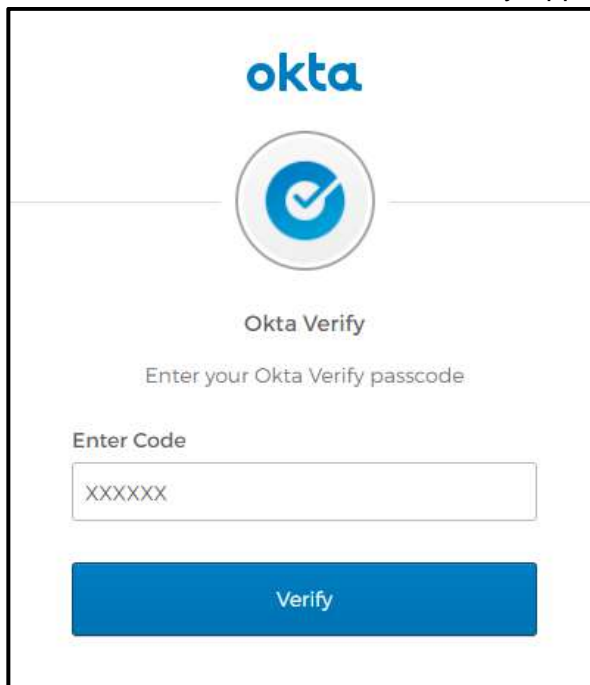


The image shows the Okta Sign In screen. At the top is the Okta logo. Below it is a circular placeholder for a user profile picture with a question mark. Underneath is the text "Sign In". There are two input fields: "Username" with the value "kerry.jones@automationedge.com" and "Password" with masked characters. Below the password field is a checkbox labeled "Remember me". A large blue "Sign In" button is centered below the form. At the bottom left, there is a link that says "Need help signing in?".

2. You can see the current Apps in this account. Click on Admin on the top right corner.

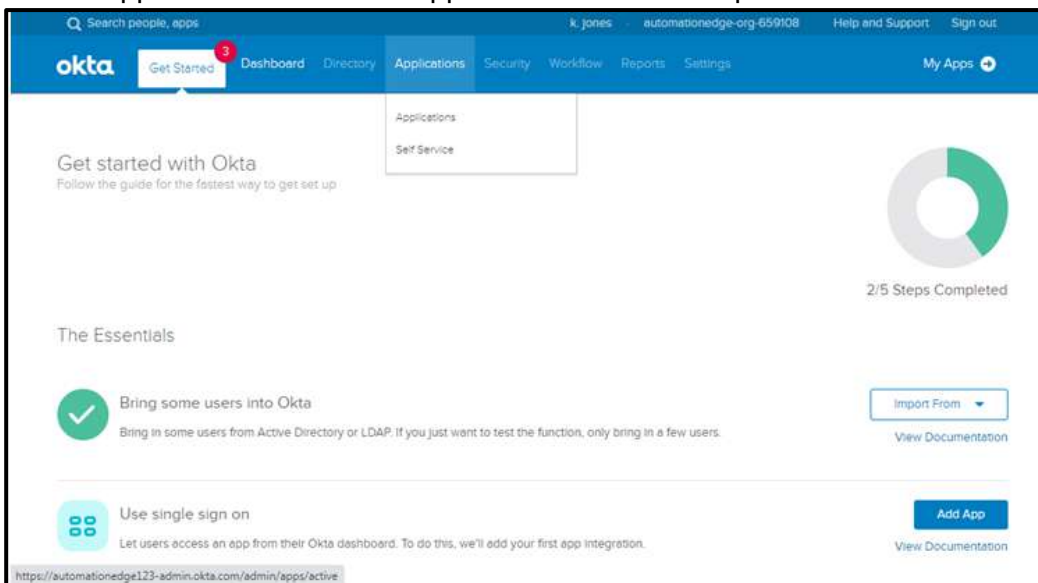


3. If asked for, enter code from Okta Verify App on your mobile here.



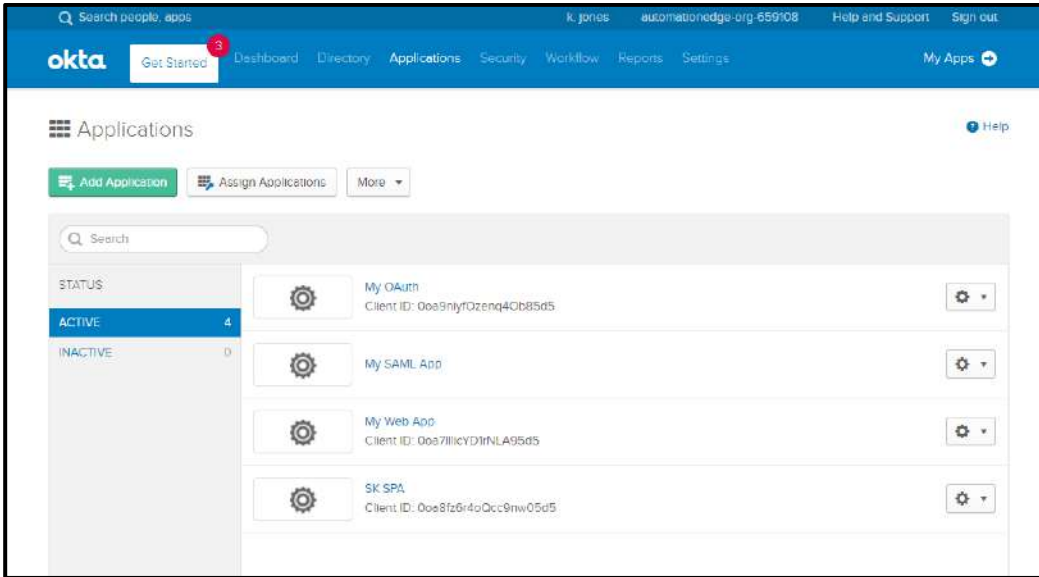
The image shows the Okta Verify mobile app interface. At the top is the Okta logo. Below it is a circular icon with a checkmark. The text reads "Okta Verify" and "Enter your Okta Verify passcode". There is a text input field labeled "Enter Code" containing "XXXXXX". Below the input field is a blue button labeled "Verify".

4. The Get Started with Okta page appears.
5. On the Applications Tab select Applications from the drop down list.

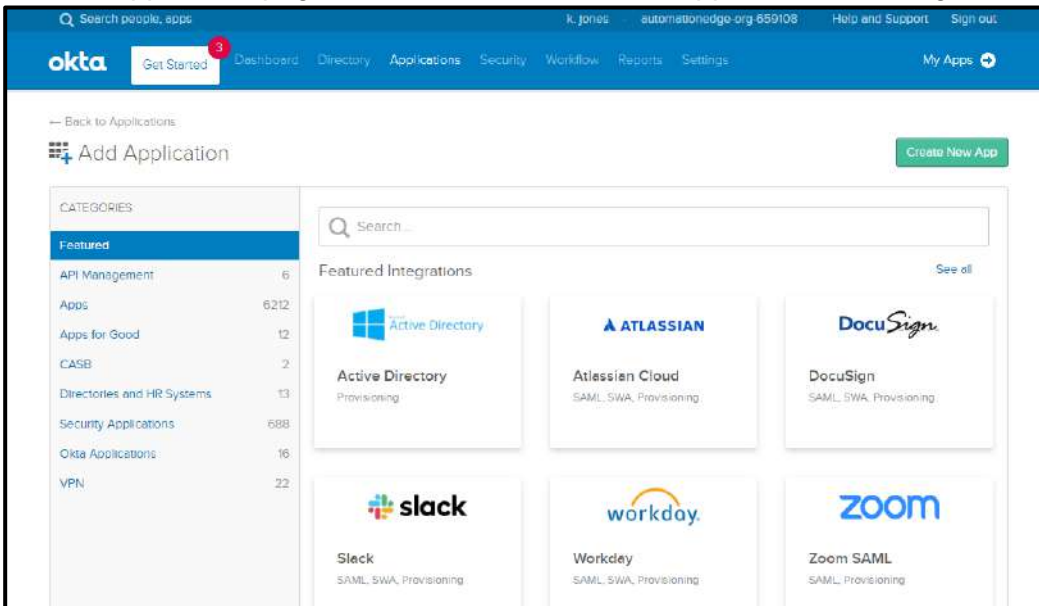


The image shows a screenshot of the Okta Admin Console. The top navigation bar includes "okta", "Get Started" (with a red notification badge), "Dashboard", "Directory", "Applications", "Security", "Workflow", "Reports", "Settings", and "My Apps". The "Applications" tab is selected, and a dropdown menu is open showing "Applications" and "Self Service". The main content area features a "Get started with Okta" section with a progress indicator showing "2/5 Steps Completed". Below this is "The Essentials" section with two items: "Bring some users into Okta" and "Use single sign on". Each item has a "View Documentation" link. The URL at the bottom is <https://automationedge123-admin.okta.com/admin/apps/active>.

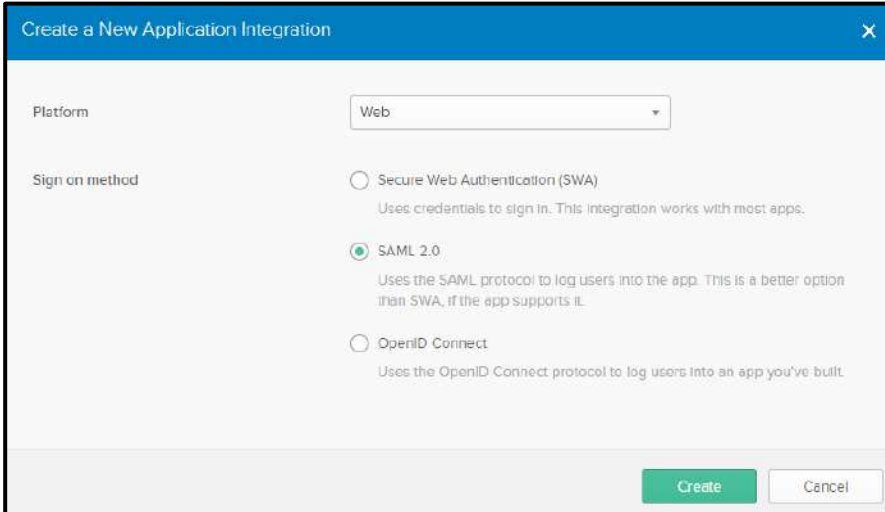
- The Get Started -Applications page appears. Click Add Application button.



- On Add Application page click on Click Create New App button on the right side.



8. We are creating a Web application with Sign on method SAML. Accordingly, select configurations as seen below.

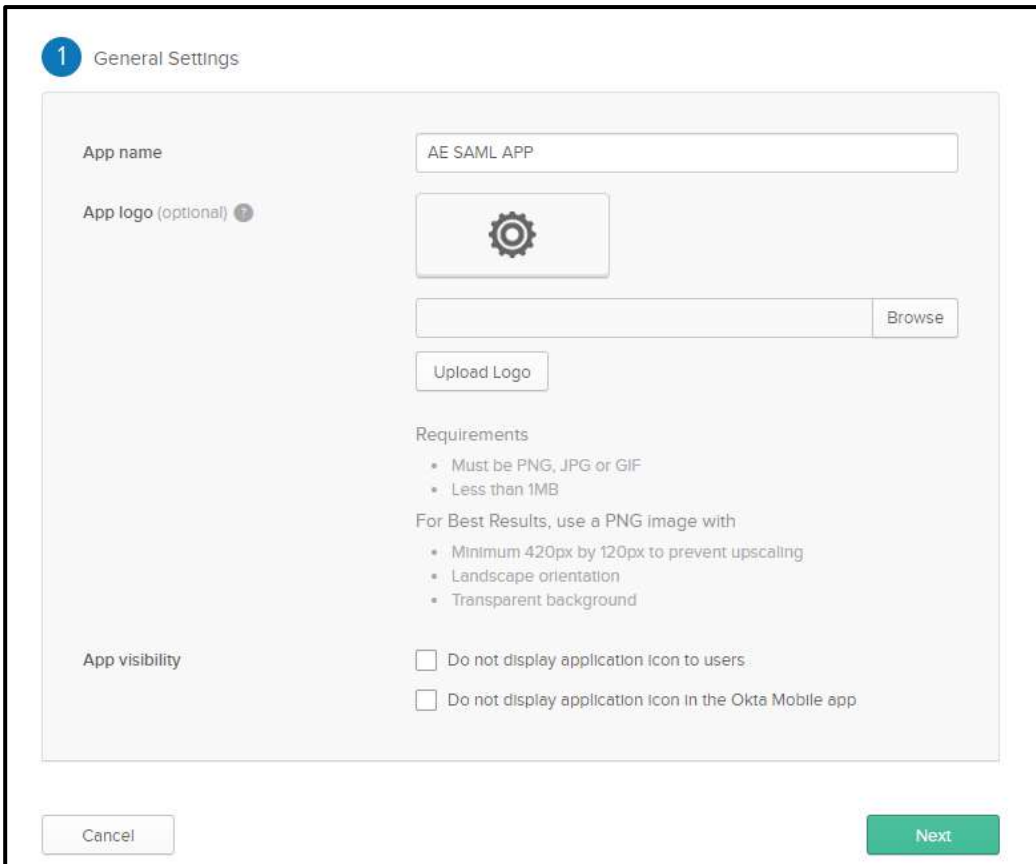


The screenshot shows a dialog box titled "Create a New Application Integration". It has a blue header bar with a close button (X) on the right. The main content area is white and contains the following fields:

- Platform:** A dropdown menu with "Web" selected.
- Sign on method:** Three radio button options:
 - Secure Web Authentication (SWA)
Uses credentials to sign in. This integration works with most apps.
 - SAML 2.0
Uses the SAML protocol to log users into the app. This is a better option than SWA, if the app supports it.
 - OpenID Connect
Uses the OpenID Connect protocol to log users into an app you've built.

At the bottom right, there are two buttons: "Create" (green) and "Cancel" (white).

9. Call your application AE SAML APP as seen in the App name below.
10. Click Next.



The screenshot shows a configuration page titled "1 General Settings". It has a light gray background and contains the following fields and sections:

- App name:** A text input field containing "AE SAML APP".
- App logo (optional):** A section with a gear icon, a text input field, and a "Browse" button.
- Upload Logo:** A button.
- Requirements:**
 - Must be PNG, JPG or GIF
 - Less than 1MB
- For Best Results, use a PNG image with:**
 - Minimum 420px by 120px to prevent upscaling
 - Landscape orientation
 - Transparent background
- App visibility:** Two checkboxes:
 - Do not display application icon to users.
 - Do not display application icon in the Okta Mobile app.

At the bottom, there are two buttons: "Cancel" (white) and "Next" (green).

11. Provide SAML settings as seen below.
12. Specify the Redirect URL for Single sign on URL (as https://<aeui-server>:{Port}/aeui/index.jsp)
13. Make sure your audience URI is also same as sign on URL.
14. Select Name Id format to **Transient** and application username to **Okta Username**.
15. Click Show Advanced Settings.

SAML Settings

GENERAL

Single sign on URL

Use this for Recipient URL and Destination URL

Allow this app to request other SSO URLs

Audience URI (SP Entity ID)

Default RelayState

If no value is set, a blank RelayState is sent

Name ID format

Application username

Update application username on

[Show Advanced Settings](#)


Name	Name format (optional)	Value
<input type="text"/>	<input type="text" value="Unspecified"/>	<input type="text"/>

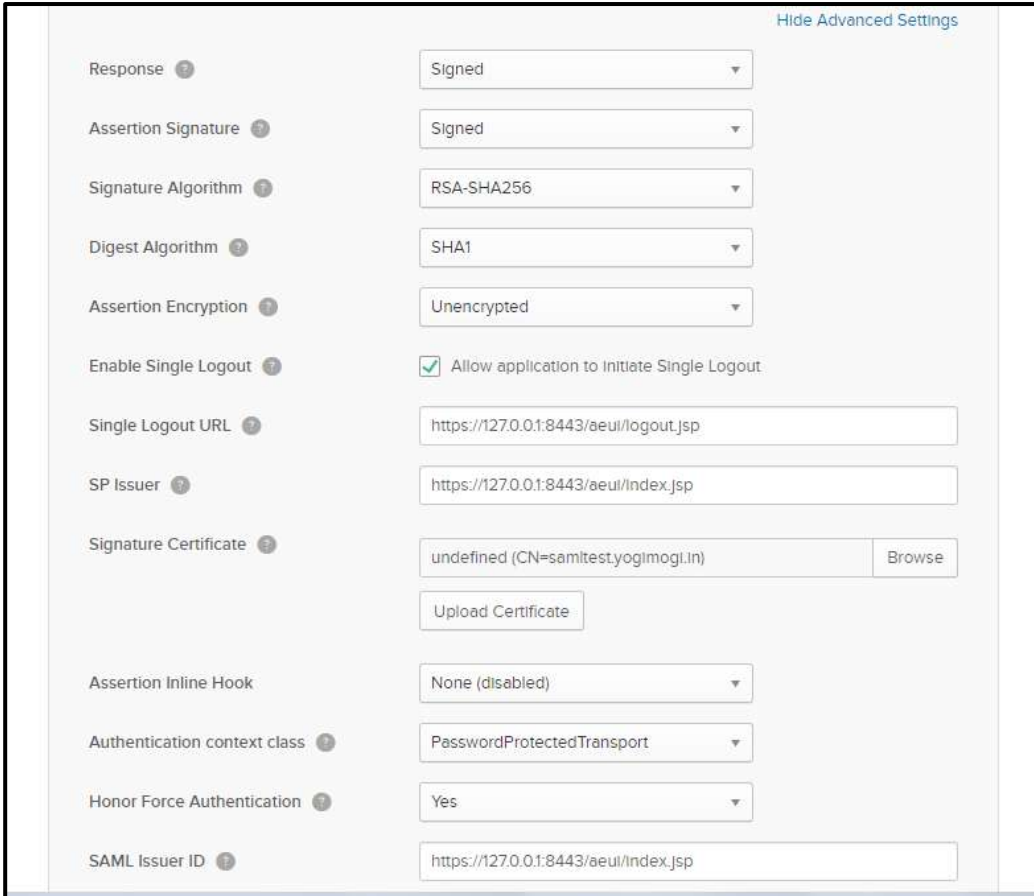
16. Enter Advanced Settings as seen below to enter more OKTA configurations.
17. Set the Response to **Signed** as it will sign the response after successful login.
18. Assertion Signature needs to be **Signed**.
19. The signature algorithm is **RSA-SHA256** even in the backend we are using this algorithm to sign the login request.
20. Set the digest algorithm to **SHA1**.
21. Set Assertion encryption to **Unencrypted**.
22. Check the Enable single logout as we are supporting logout as well. In the Single logout URL specify the logout URL such as http://<aeui-server>/aeui/logout.jsp .
23. Set the SP issuer same as Single sign on URL. As we are signing the xml we need a certificate for it.
24. You can browse and upload the certificate.
25. Even in the SAML Issuer id should be same as single sign on URL.

26. So we have same field value in the following:

- Single Sign on URL
- Audience URL
- SP issuer
- SAML issuer ID

27. Also browse for a Signature Certificate and click Upload.

 **Note:** To generate Self Signed or CA Certificate refer to section [2.9 Keystore and Certificate Generation](#)



Hide Advanced Settings

Response	Signed
Assertion Signature	Signed
Signature Algorithm	RSA-SHA256
Digest Algorithm	SHA1
Assertion Encryption	Unencrypted
Enable Single Logout	<input checked="" type="checkbox"/> Allow application to Initiate Single Logout
Single Logout URL	<input type="text" value="https://127.0.0.1:8443/aeui/logout.jsp"/>
SP Issuer	<input type="text" value="https://127.0.0.1:8443/aeui/index.jsp"/>
Signature Certificate	<input type="text" value="undefined (CN=samitest.yogimogi.in)"/> <input type="button" value="Browse"/> <input type="button" value="Upload Certificate"/>
Assertion Inline Hook	None (disabled)
Authentication context class	PasswordProtectedTransport
Honor Force Authentication	Yes
SAML Issuer ID	<input type="text" value="https://127.0.0.1:8443/aeui/index.jsp"/>

28. AutomationEdge supports the following claims.

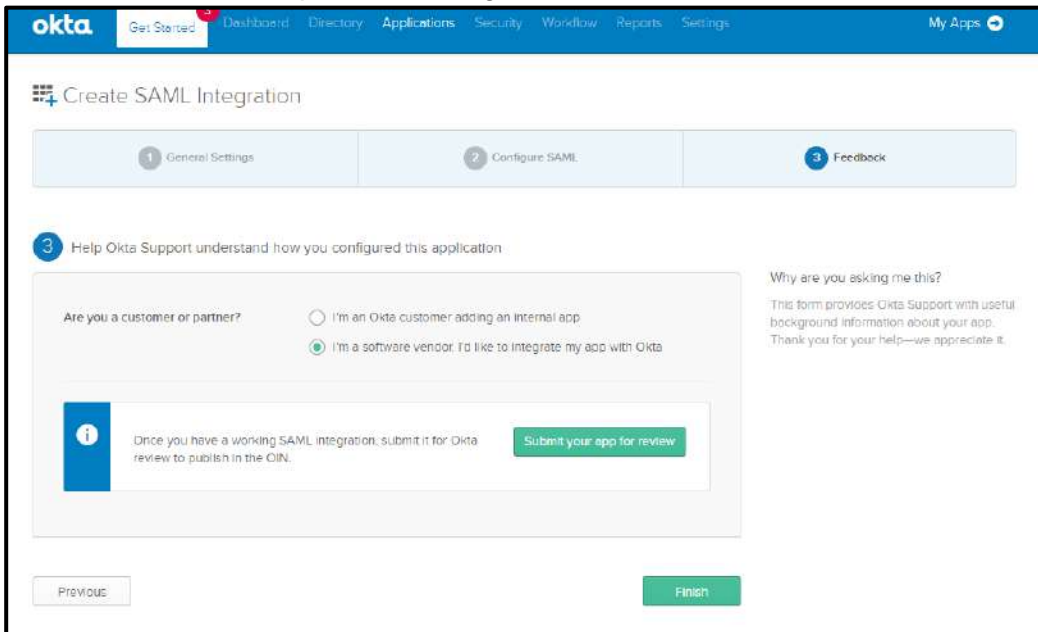
Name	Value
firstName	user.firstName
lastName	User.lastName
emailAddress	User.email
Username	User.login

Hence, add claims as below.

29. There is no change in the GROUP ATTRIBUTE STATEMENTS.

30. Click Next.

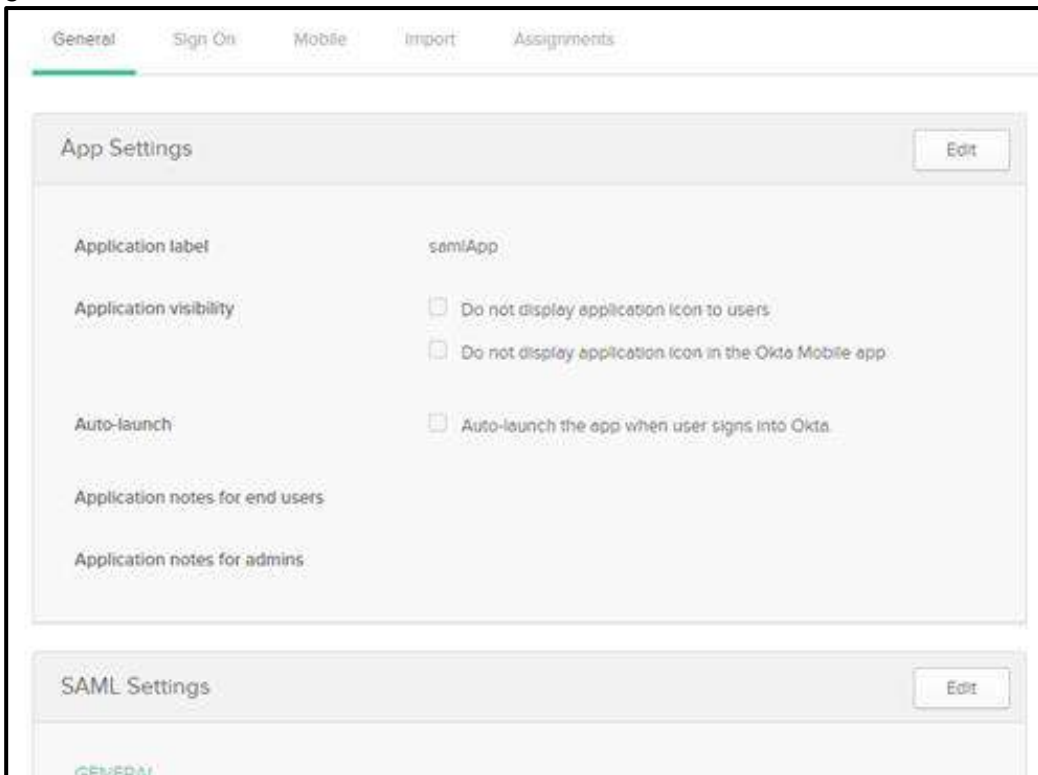
31. Click on **Finish** to complete the configuration.



The screenshot shows the 'Create SAML Integration' wizard in the Okta Admin Console, specifically the 'Feedback' step. The navigation bar at the top includes 'Get Started', 'Dashboard', 'Directory', 'Applications', 'Security', 'Workflow', 'Reports', 'Settings', and 'My Apps'. The main content area has a progress indicator with three steps: '1 General Settings', '2 Configure SAML', and '3 Feedback'. The 'Feedback' step is active and contains a form with the following elements:

- A heading: 'Help Okta Support understand how you configured this application'.
- A question: 'Are you a customer or partner?' with two radio button options:
 - I'm an Okta customer adding an internal app
 - I'm a software vendor. I'd like to integrate my app with Okta
- An information box with an 'i' icon and text: 'Once you have a working SAML integration, submit it for Okta review to publish in the OIN.' A green button labeled 'Submit your app for review' is positioned to the right of this text.
- A 'Previous' button on the bottom left and a green 'Finish' button on the bottom right.
- On the right side, a section titled 'Why are you asking me this?' with explanatory text: 'This form provides Okta Support with useful background information about your app. Thank you for your help—we appreciate it.'

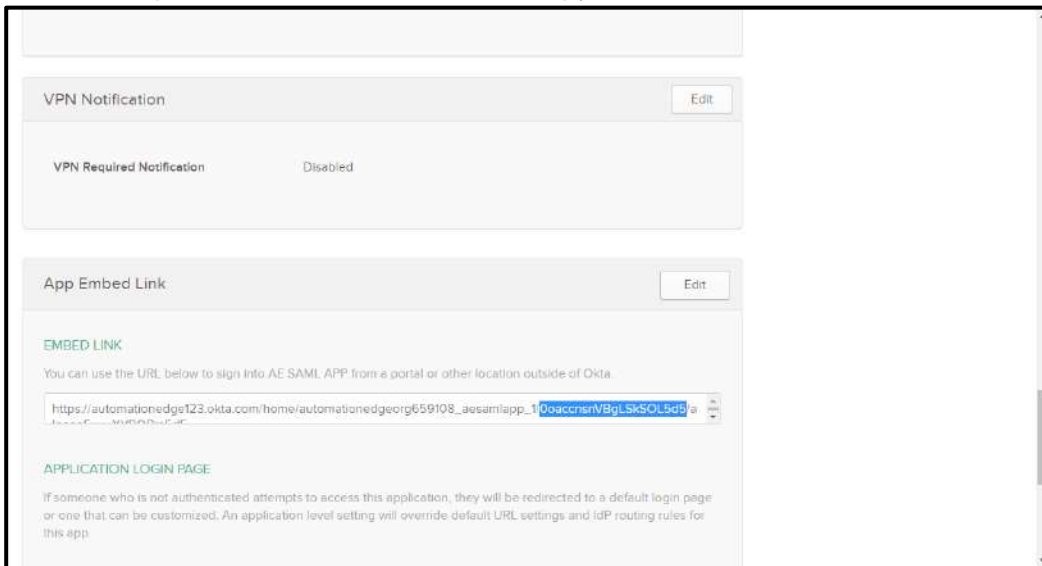
32. Client ID for SAML OKTA is not directly provided in the UI. To fetch Client ID, go to general tab after finish.



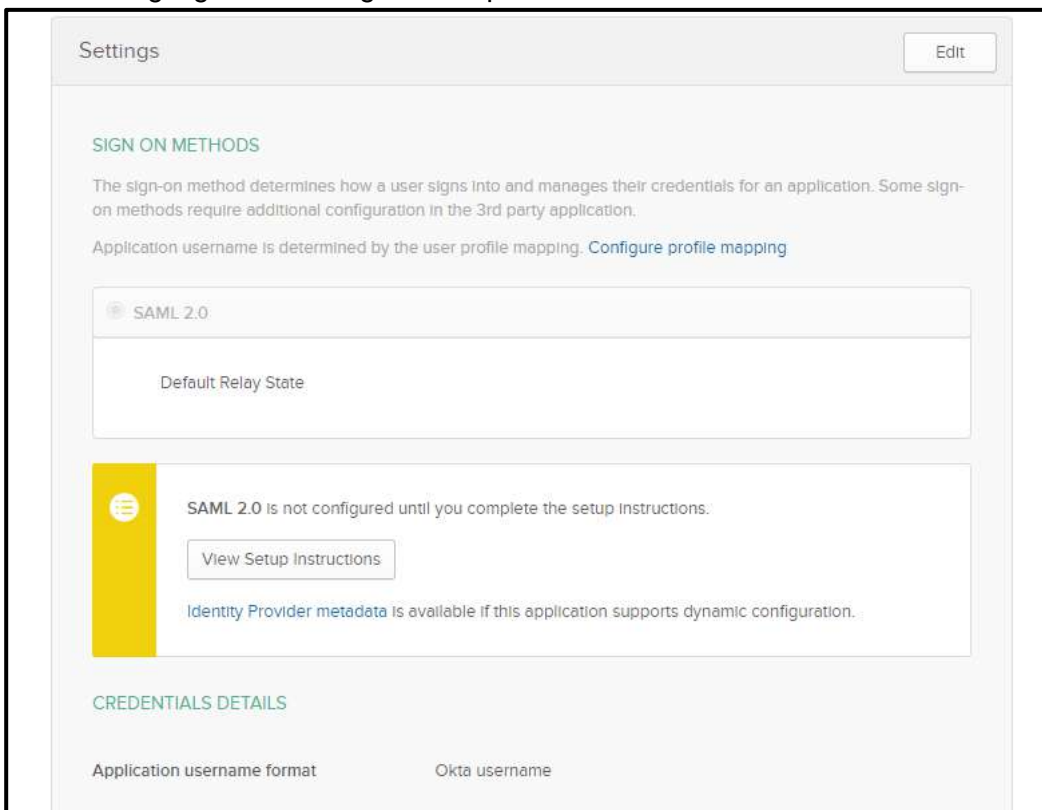
The screenshot shows the 'App Settings' configuration page in the Okta Admin Console. The page has a navigation bar with tabs: 'General', 'Sign On', 'Mobile', 'Import', and 'Assignments'. The 'General' tab is selected and highlighted. The main content area is divided into two sections:

- App Settings**: Contains an 'Edit' button and several configuration options:
 - 'Application label' with the value 'samlApp'.
 - 'Application visibility' with three checkboxes:
 - Do not display application icon to users
 - Do not display application icon in the Okta Mobile app
 - 'Auto-launch' with a checkbox: Auto-launch the app when user signs into Okta.
 - 'Application notes for end users' (text input field).
 - 'Application notes for admins' (text input field).
- SAML Settings**: Contains an 'Edit' button.

33. Scroll down to the App Embed Link section.
34. Client ID is part of the Enbed Link URL. Copy the Client ID.



35. For descriptor.xml navigate to the Application -> {{Your Application Name}} -> Sign On. Click the highlighted link to get descriptor details.

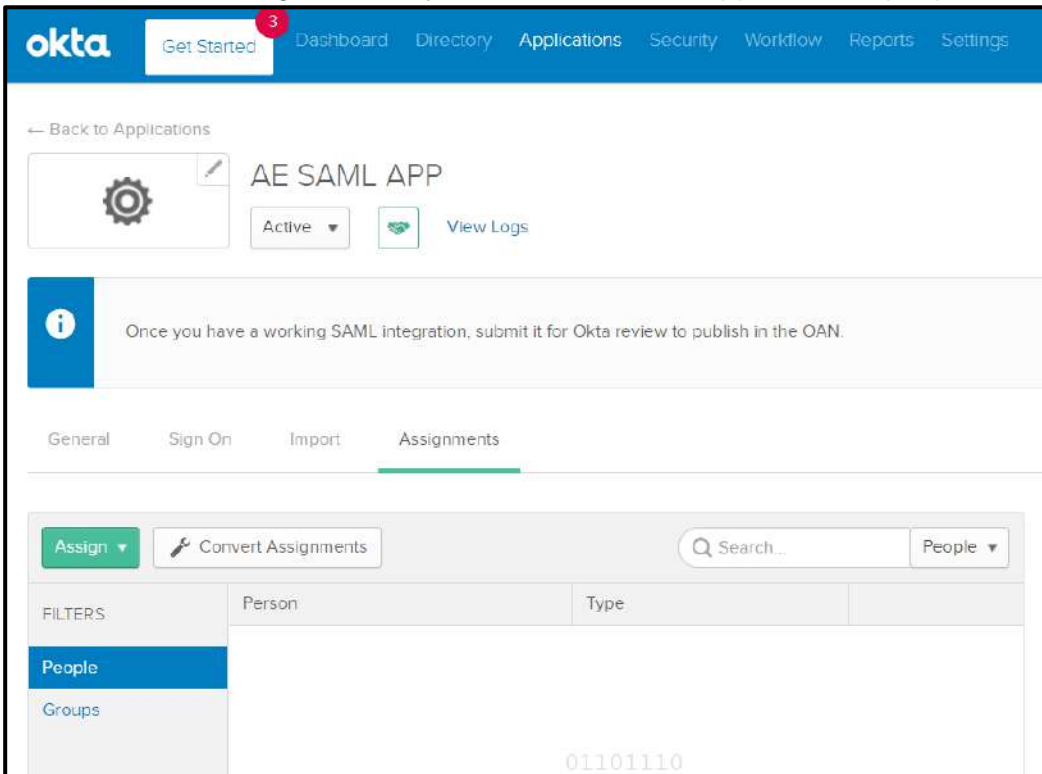


36. Save the descriptor XML into an xml file called descriptor.xml

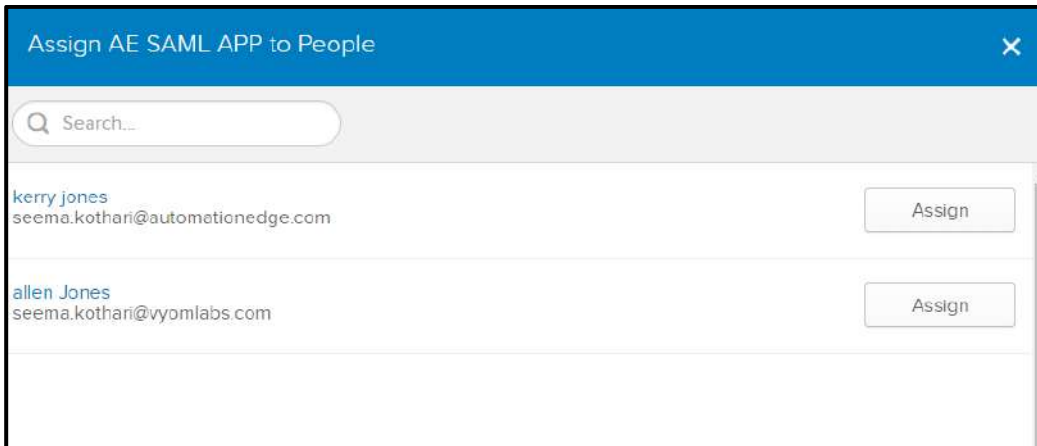
```

This XML file does not appear to have any style information associated with it. The document tree is shown below:
<?xml:entityDescriptor xmlns:mds="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://127.0.0.1:8443/eeui/index.jsp">
  <md:IDPSSODescriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
      <md:keyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>MIIDBTCCAppgwI8AgTGAU8BSC5NAR6CSqgSIb3QDEBChMwTzYwcmQyOQGEw7VUzE7HBE6
          A3UECAWkQZ2sanzvcmSpVTENH8G6AUEBwNU2fUIEZYvU5jAKHbEhNAsgA1UEGgETZ0Y7TEUjPBIGALUECAwLU1MjPHH3Vmd1kZk1x6j4VegWBAWMEHF1dgg+YXRpb251ZGdINTI2PhRwagYkKOZI
          hveNAkEgFgIpbzVQ9BrdEUV28tB4XDTiHTAmizAMHTcyOvXDTNwHTAMizAMHTgyOFoug2kx CzA3BgtWBAyTA1VTRFHwEQYVQZIDApDYHxpZm9ybmZmNjYwYVZlYVQzODAlTlVwagRn3hbmNpc2Nw
          NQ0wCwYDVQKQARPaSRHMQEgYDVQQLDAtU09Qcm92aWRlcjEwRjB6A1UEFAWwRYXV0b21hdGlvbmVhZ2UwHj1wHDAaBggqh1G9w98CQEDLwZm9Ab210Y555b20wgEIPA08CSqGSIb3QDEBAQUA
          A4T8DAAWggRkA0I8AQcP3Dk/F2f7P59lyhZcAYuL2KLR84CUBu657r041vRvN6EXU7P8glu 2Pwaa/rQ16H7K8aR6A+PbmgF5CvFyXn82uMS87/BaIye9aEA30vHPXW5YluwSPFP3yVWQ
          0wMBU2XSP9a939Rnyx0V8TFO0W6YDvGxpk9C0Fvvg7ukcSI0Ej7H+5pkQnPLBn1 qH4y1E8G5JmKZ1YagKc5K1cQ44DZ254Gy8K1wa1Sa77g/2125+wgYkA0d0o18ELz
          DA5T40P541nVvypz8Euf0P222ua9J0cT7T0NHETt8B0tLCH0T1AgHRAAEUQQ3K0ZIHvch AQELBQADggEBAES/OoYx12jLpLjR7FR487KS2Eul4xRRM1pApKcC0XT2ky169QudSTRASCJE
          wQm819o4vaHv5Pv8V5pp2pkW8J5L8CX7d8b5y1FTKRAALrpz4UEBRN7apf6n15TJjQWlp T9FD3+UFe+UQeIK+/o8R7Ee0t5nU0snhu/3T837u81bWLUcNLwylFRzu110dpCInZQ8ttNAzpw
          MB+1+4du1Lp6+D0ed+QaitUc5GFt/GTfeVo239Ghh2IC2s515n1+KML3H41rFnL3h0i0go3 DRD1x++8Fq17KAJCGmtG0u0iYp5XV2PLFn4Eky2CuUMQ3FYkk</ds:X509Certificate>
        </ds:X509Data>
      </ds:keyInfo>
    </md:KeyDescriptor>
    <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="https://autonetionedge123.okta.com/app/autonetionedgeorg59108_aesa1app_1/exkccnm27tcD9fd5d5/slo/saml?"/>
    <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
      Location="https://autonetionedge123.okta.com/app/autonetionedgeorg59108_aesa1app_1/exkccnm27tcD9fd5d5/slo/saml?"/>
    <md:NameIDFormat urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>
    <md:NameIDFormat urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="https://autonetionedge123.okta.com/app/autonetionedgeorg59108_aesa1app_1/exkccnm27tcD9fd5d5/so/saml?"/>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
      Location="https://autonetionedge123.okta.com/app/autonetionedgeorg59108_aesa1app_1/exkccnm27tcD9fd5d5/so/saml?"/>
  </md:IDPSSODescriptor>
</md:EntityDescriptor>
  
```

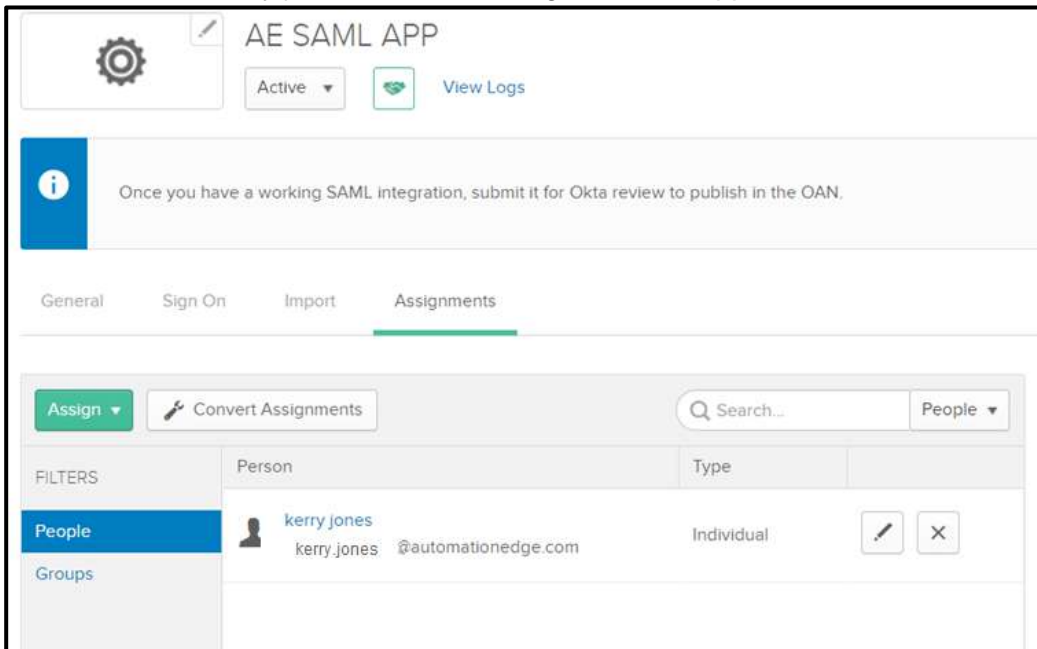
37. Next we need to assign the newly created web SAML application to people. Click Assign.



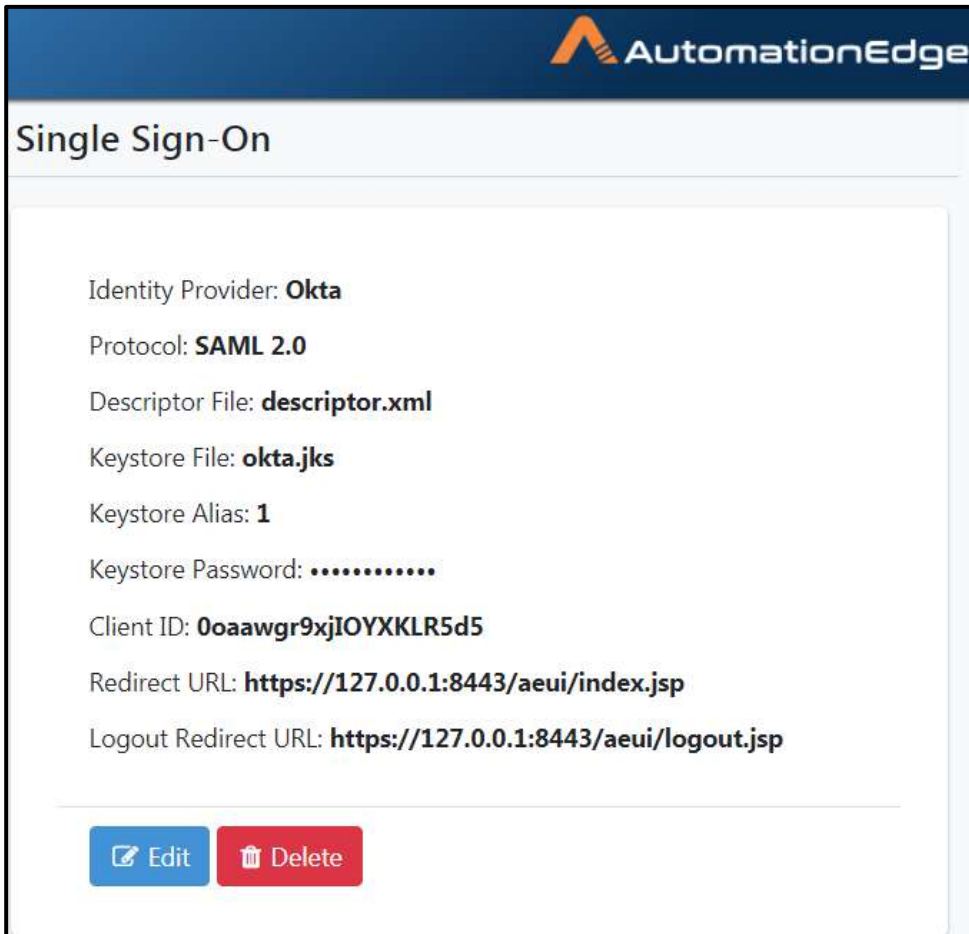
38. Search for the people you wish to assign to the application and click Assign.



39. As seen below, kerry jones has been assigned to the application.



40. Configure Single Sign-On on AutomationEdge UI.



The screenshot displays the AutomationEdge UI for configuring Single Sign-On. The interface has a dark blue header with the AutomationEdge logo. Below the header, the title "Single Sign-On" is displayed. The configuration details are as follows:

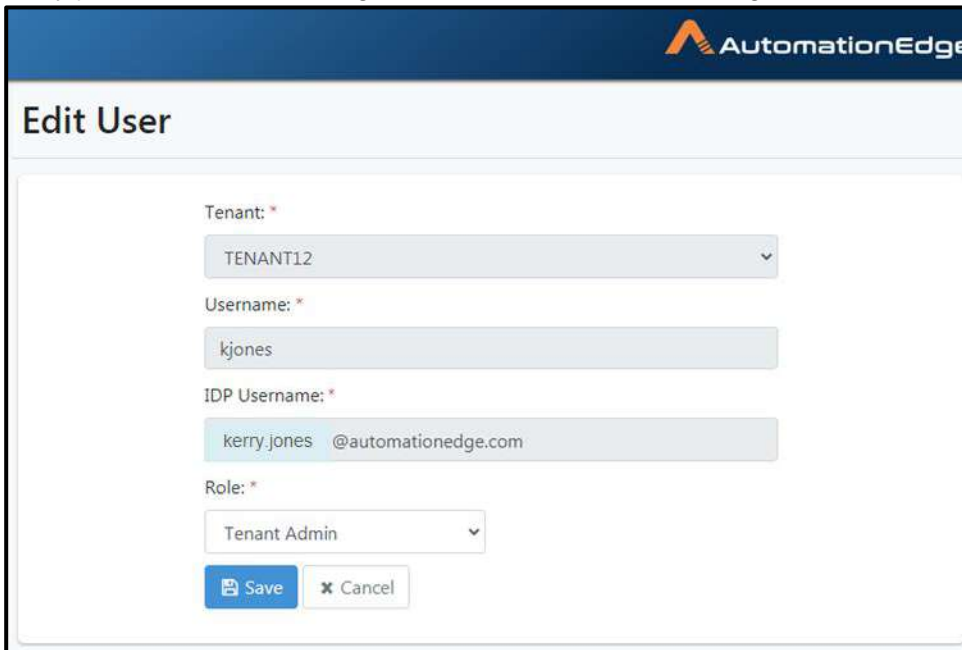
- Identity Provider: **Okta**
- Protocol: **SAML 2.0**
- Descriptor File: **descriptor.xml**
- Keystore File: **okta.jks**
- Keystore Alias: **1**
- Keystore Password: **.....**
- Client ID: **0oaawgr9xjIOYXKLR5d5**
- Redirect URL: **https://127.0.0.1:8443/aeui/index.jsp**
- Logout Redirect URL: **https://127.0.0.1:8443/aeui/logout.jsp**

At the bottom of the configuration area, there are two buttons: a blue "Edit" button and a red "Delete" button.

**Note:**

To generate Keystore refer to section [2.9 Keystore and Certificate Generation](#)

41. Please note the settings in AutomationEdge UI.
42. AutomationEdge username Kerry is mapped to Okta username kerry.jones@automationedge.com seen in AutomationEdge UI as below.



Edit User

Tenant: *
TENANT12

Username: *
kjones

IDP Username: *
kerry.jones @automationedge.com

Role: *
Tenant Admin


43. Now test AutomationEdge SSO.
44. On AutomationEdge login page click Sign In with SSO.



AutomationEdge

AI DRIVEN INTELLIGENT ENTERPRISE RPA

- Unified Automation Platform for both Business and IT Operations
- Automate every department : front office, back office, middle office and IT operations
- Faster RPA product, Fastest Spreadsheet processing

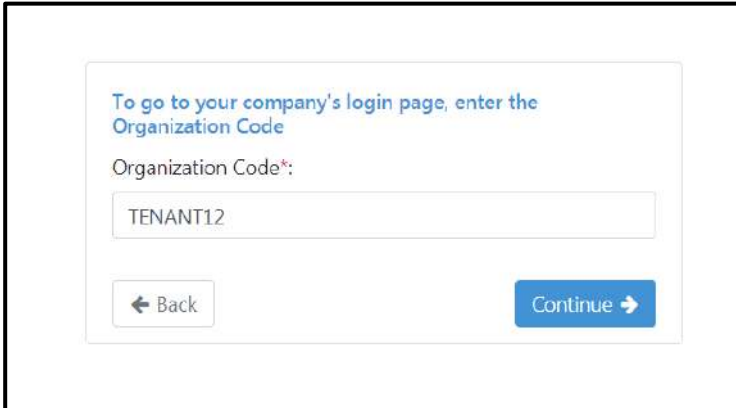


Enter Username
Enter Password

[Forgot Password](#) [Sign In with SSO](#)

© 2019-20 AutomationEdge. All Rights Reserved.

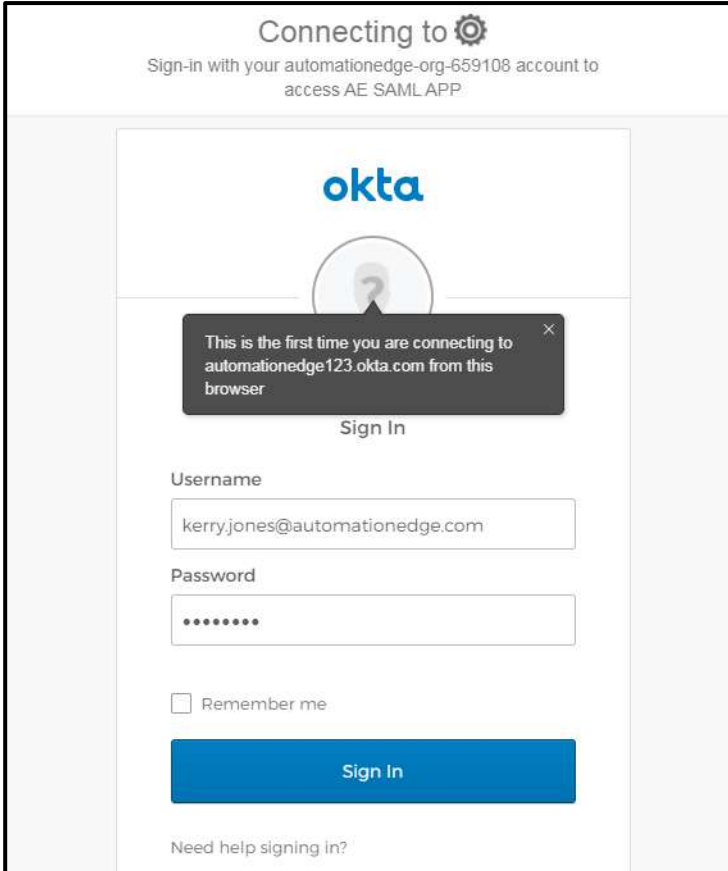
45. Provide the Organization Code of the SSO user in the popup.




To go to your company's login page, enter the Organization Code

Organization Code*:


46. The first time you are connected to Okta for SSO, the Okta login page appears. Provide a username that is mapped to an AutomationEdge user in this organization.



Connecting to 

Sign-in with your automationedge-org-659108 account to access AE SAML APP

okta



This is the first time you are connecting to automationedge123.okta.com from this browser

Sign In

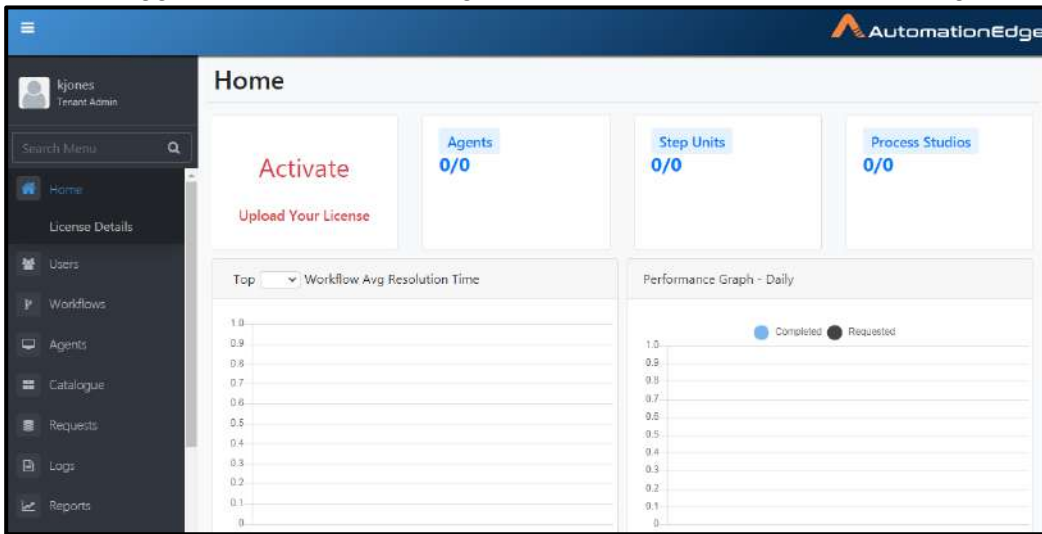
Username

Password

Remember me

Need help signing in?

47. You are logged in to AutomationEdge with SSO and taken AutomationEdge home page.



48. This completes the process of configuring OKTA for SSO with AutomationEdge.

49. You may also fetch the following attributes required to setup Single Sign-On on AutomationEdge UI, as highlighted in section.

- Client ID
- Descriptor file
- Redirect URL

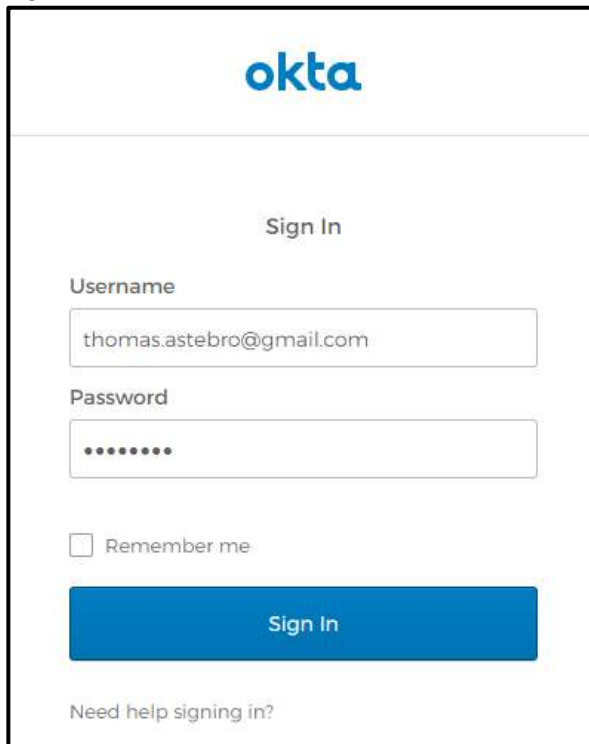
2.4 Okta(IDP) initiated SSO for AE using SAML

This section demonstrates setups in Okta and AutomationEdge for IDP initiated SSO with SAML.

2.4.1 Setups in Okta

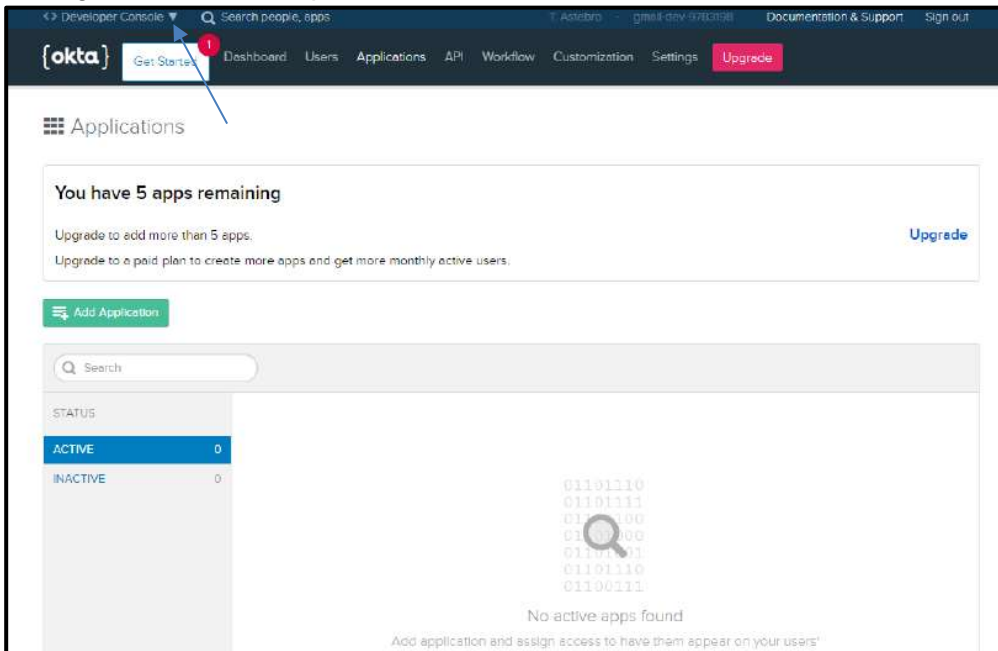
Following are the setups in Okta for IDP initiated SSO with SAML,

1. Sign in to OKTA.

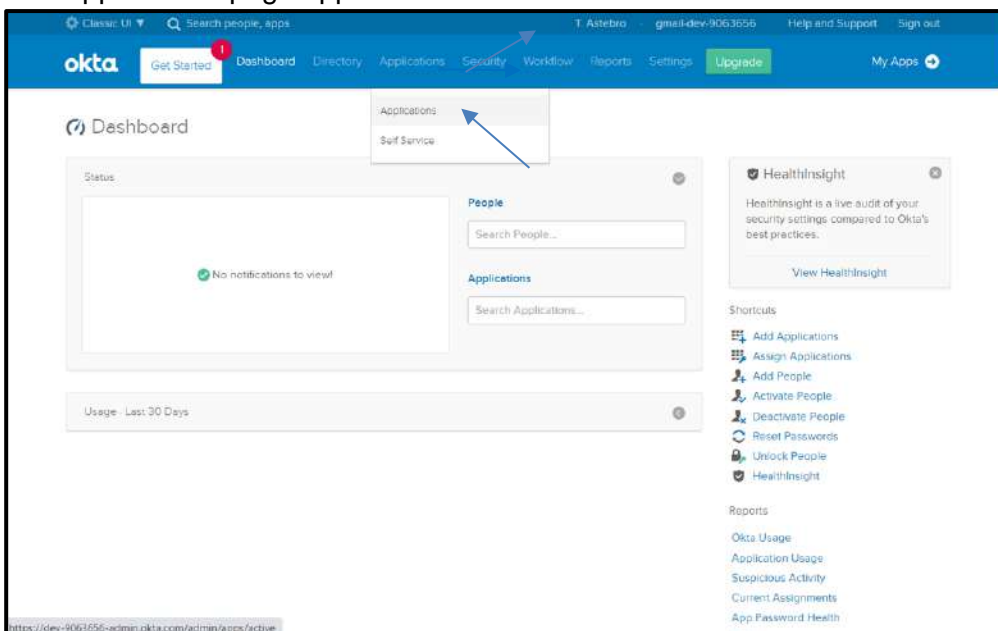


The screenshot shows the Okta Sign In page. At the top is the Okta logo. Below it is the text "Sign In". There are two input fields: "Username" with the value "thomas.astebro@gmail.com" and "Password" with masked characters "••••••". Below the password field is a checkbox labeled "Remember me" which is unchecked. At the bottom is a blue "Sign In" button. Below the button is the text "Need help signing in?".

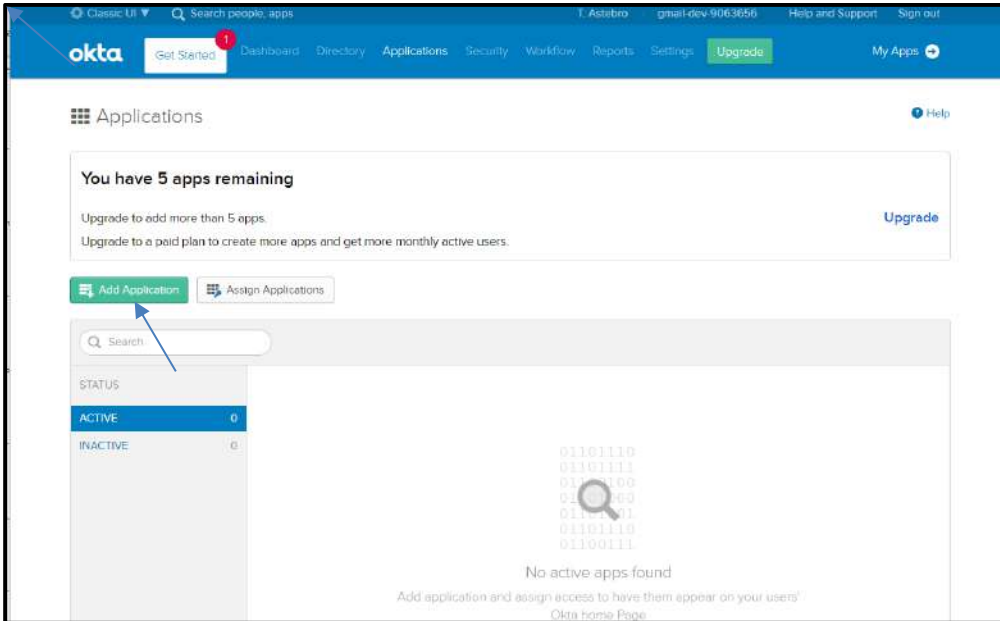
2. The Getting Started page appears.
3. Change UI from Developer Console to Classic UI.



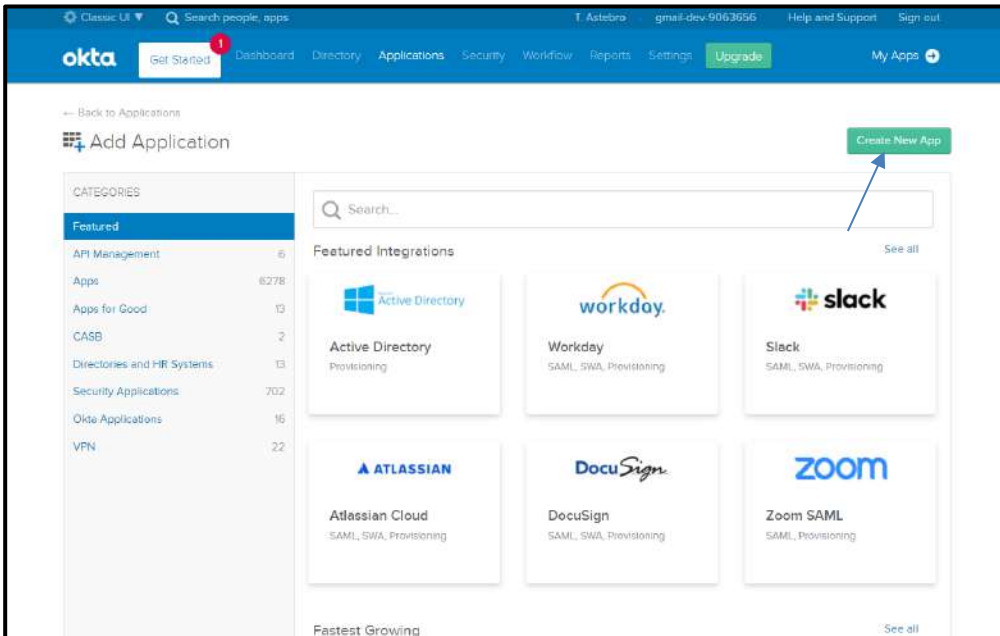
4. Click on Applications Tab and Applications option.
5. The Applications page appears.



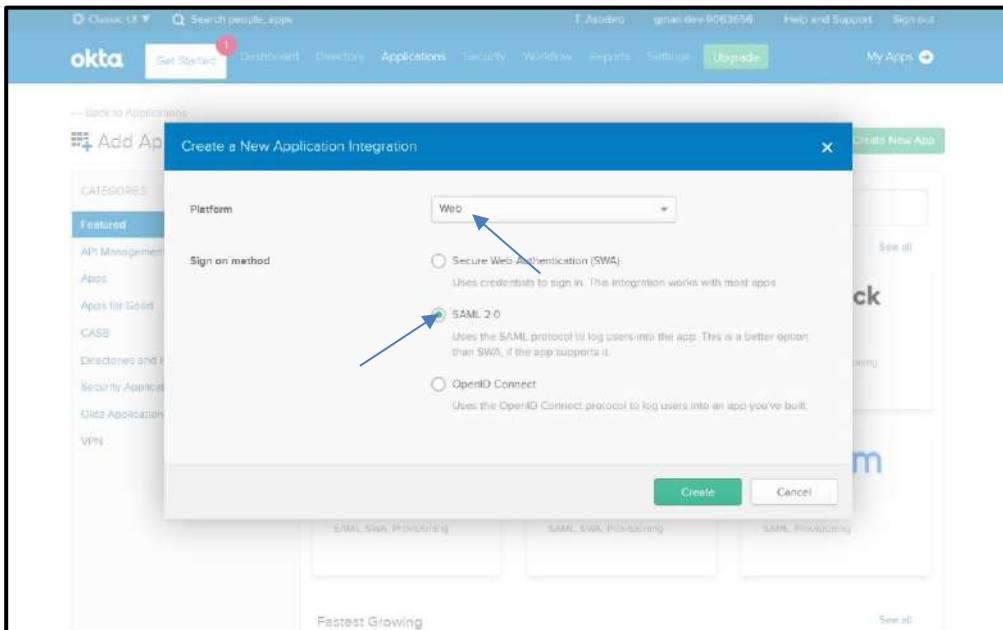
6. Click Add Application button.



7. Click Create New App button.



8. Select Web Platform and SAML 2.0 Sign on method.
9. Click Create.



10. Give a name to the application – MySamlApp. Click next to configure application details.

11. Specify the Single sign on URL (e.g. `https://{host}:{port}/aeui/index.jsp` or `https://<aeui-server>/aeui/index.jsp`)
12. The Audience URI is same as Single sign on URL. Select. Name Id format to **Transient** and application username to **Okta Username**.
13. Click Show Advanced Settings.

14. Add Application name, Login redirect URI and Logout redirect URI as shown in image. Login redirect URI and Logout redirect URI are should be same for AE and it is the base URL for aeui in the form `https://{host}:{port}/aeui`.
15. Configure Advanced Settings as seen below.
16. The below screen shot is an example what all need to be done in Okta configuration. Set the Response to **Signed** as it will sign the response after successful login. Assertion Signature need to be **Signed**. The signature algorithm is **RSA-SHA256** even in the backend we are using this algorithm to sign the login request. Set the digest algorithm to **SHA1**. Set Assertion encryption to **Unencrypted**. **Check** Enable Single Logout to allow application to initiate single logout as well. In the Single Logout URL specify the **Logout URL** such as `http://<aeui-server>/aeui/logout.jsp` . Set the SP issuer same as Single sign on URL. As we are signing the Request Descriptor xml file we need a certificate for it. In the Signature Certificate Browse and Upload the certificate (To generate certificate refer to section [2.9 Keystore and Certificate Generation](#)). Even in the SAML Issuer ID provide the same value as Single sign on URL.
17. So, we have same values for the following:
 - Single Sign on URL
 - Audience URL
 - SP issuer
 - SAML issuer ID
18. Also add Attributes by specifying - Name, Name format and Value as discussed in the next point.

The screenshot shows the 'Advanced Settings' section of an Okta configuration page. The settings are as follows:

- Response:** Signed
- Assertion Signature:** Signed
- Signature Algorithm:** RSA-SHA256
- Digest Algorithm:** SHA1
- Assertion Encryption:** Unencrypted
- Enable Single Logout:** Allow application to initiate Single Logout
- Single Logout URL:** `https://techedge.automationedge.com:8443/aeui/logout.jsp`
- SP Issuer:** `https://techedge.automationedge.com:8443/aeui/index.jsp`
- Signature Certificate:** `keystore.jks` (with a 'Browse' button) and an 'Upload Certificate' button.
- Authentication context class:** PasswordProtectedTransport
- Honor Force Authentication:** Yes
- SAML Issuer ID:** `https://techedge.automationedge.com:8443/aeui/index.jsp`

At the bottom, there is a table for adding attributes:

Name	Name format (optional)	Value
<input type="text"/>	Unspecified	<input type="text"/>

An 'Add Another' button is located below the table.

19. Since we support claims in the AE, add Attributes/Claims (similar to what was added in AE initiated SSO with Okta using OAuth/OpenID), as listed and discussed below.
20. Add Attributes/Claims by specifying - Name, Name format and Value.
21. The values expression for the list of claims being used in AutomationEdge may change for different Identity Providers (IDP). The table below shows the Attributes/ Claims for Okta IDP to be used for SAML App.

Name	Values (Case Sensitive)
firstName	user.firstName
lastName	user.lastName
emailAddress	user.email
username	user.login
orgCode	{{OrgCode}}

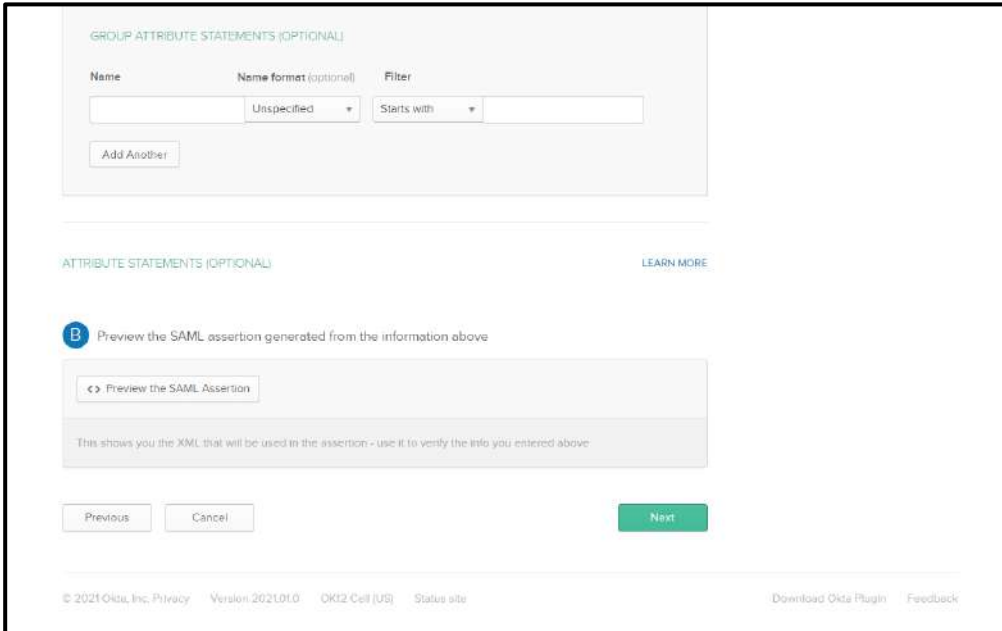
 **Note:**

It is **mandatory** to specify values for `username` and `orgCode`. It is preferable to provide values for `firstName`, `lastName` and `emailAddress` Attributes also for a complete profile view. (This is Okta Expression Language syntax to generate values derived from attributes in Universal Directory and app profiles. To validate an expression, use the Token Preview tab).

22. Add the Attributes by clicking Add Another.

Name	Name format (optional)	Value
firstName	Unspecified	user.firstName
lastName	Unspecified	user.lastName
emailAddress	Unspecified	user.email
Username	Unspecified	user.login
Orgcode	Unspecified	TENANT1
Add Another		

23. Note: There are no configurations required in the GROUP ATTRIBUTE STATEMENTS.
24. Scroll down and click Next.



GROUP ATTRIBUTE STATEMENTS (OPTIONAL)

Name Name format (optional) Filter

Unspecified Starts with

Add Another

ATTRIBUTE STATEMENTS (OPTIONAL) [LEARN MORE](#)

B Preview the SAML assertion generated from the information above

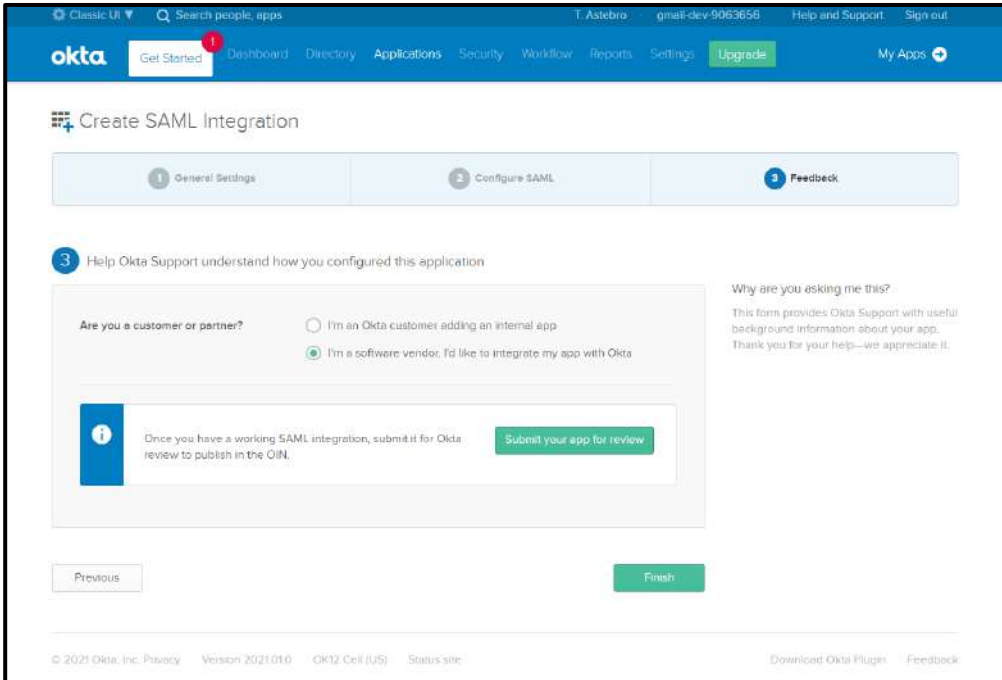
Preview the SAML Assertion

This shows you the XML that will be used in the assertion - use it to verify the info you entered above

Previous Cancel Next

© 2021 Okta, Inc. Privacy Version 2021.01.0 OK12 Cell (US) Status site Download Okta Plugin Feedback

25. Click Finish to complete the configuration.



Classic UI Search people, apps T. Astebro gmail-dev-9063656 Help and Support Sign out

okta Get Started Dashboard Directory Applications Security Workflow Reports Settings Upgrade My Apps

Create SAML Integration

1 General Settings 2 Configure SAML 3 Feedback

3 Help Okta Support understand how you configured this application

Are you a customer or partner?

I'm an Okta customer adding an internal app

I'm a software vendor, I'd like to integrate my app with Okta

Submit your app for review

Once you have a working SAML integration, submit it for Okta review to publish in the OIN.

Why are you asking me this?
This form provides Okta Support with useful background information about your app. Thank you for your help—we appreciate it.

Previous Finish

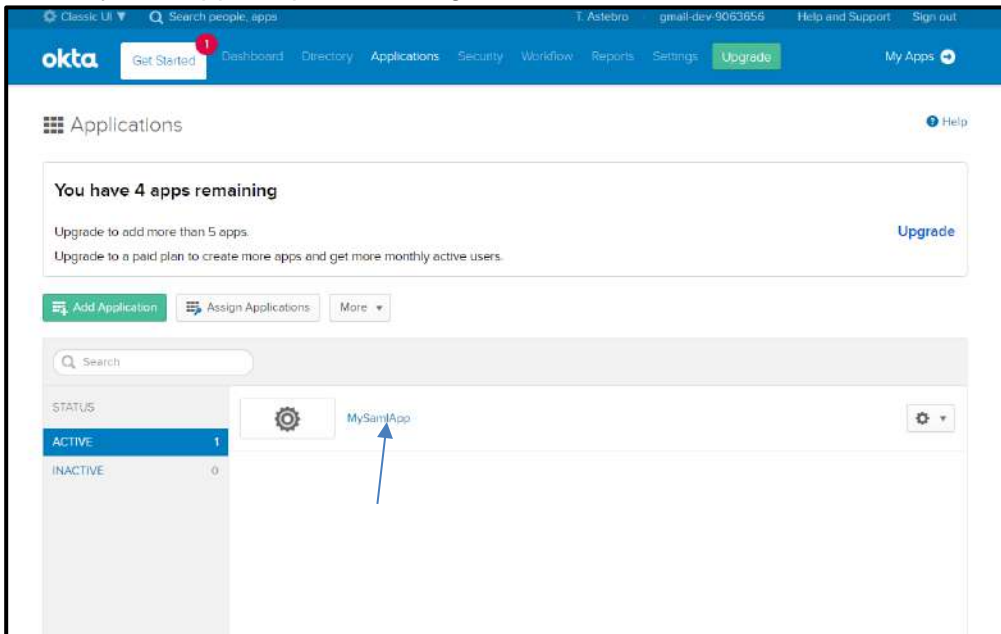
© 2021 Okta, Inc. Privacy Version 2021.01.0 OK12 Cell (US) Status site Download Okta Plugin Feedback

2.4.1.1 Fetch Descriptor File and Client ID for AE SSO setup

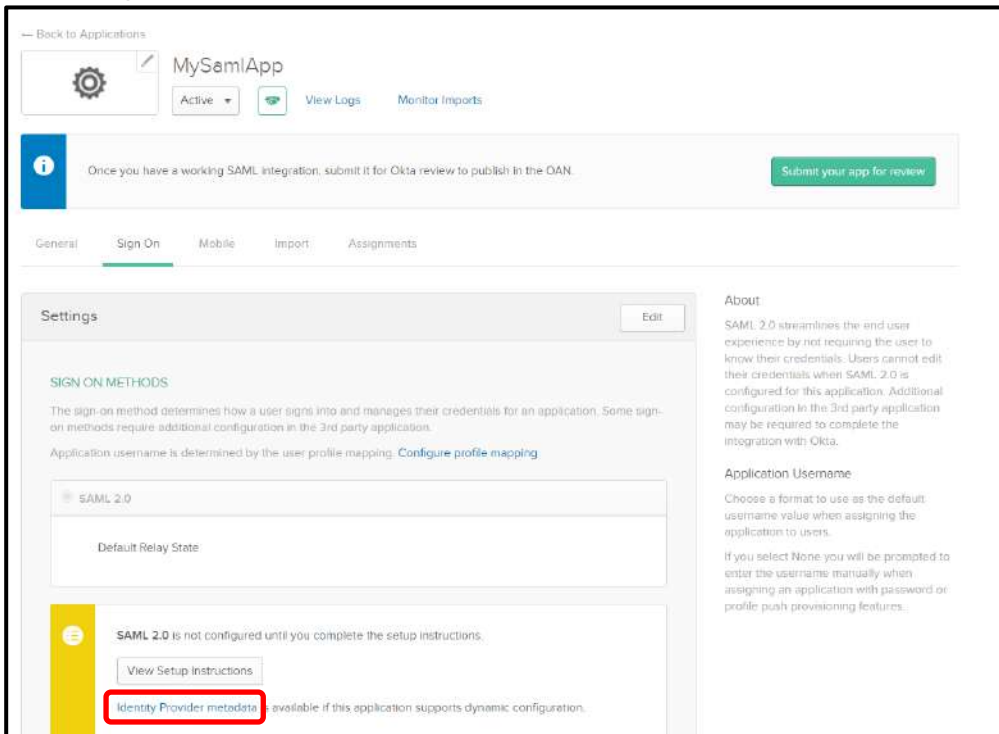
In this section we shall fetch a descriptor file and Client ID to be used in AE SSO setup.

26. Upon finish in the previous section, you are taken back to the Applications page.

27. Click MySamlApp to open its configurations.



28. On your MySamlApp go to Sign On tab.
29. The Identity Provider Metadata as marked in red below provides the descriptor details. Click to open Metadata.xml on a new tab.



— Back to Applications

MySamlApp

Active View Logs Monitor Imports

Once you have a working SAML integration, submit it for Okta review to publish in the DAN. [Submit your app for review](#)

General **Sign On** Mobile Import Assignments

Settings [Edit](#)

SIGN ON METHODS

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. [Configure profile mapping](#)

SAML 2.0

Default Relay State

SAML 2.0 is not configured until you complete the setup instructions. [View Setup Instructions](#)

Identity Provider metadata available if this application supports dynamic configuration.

About

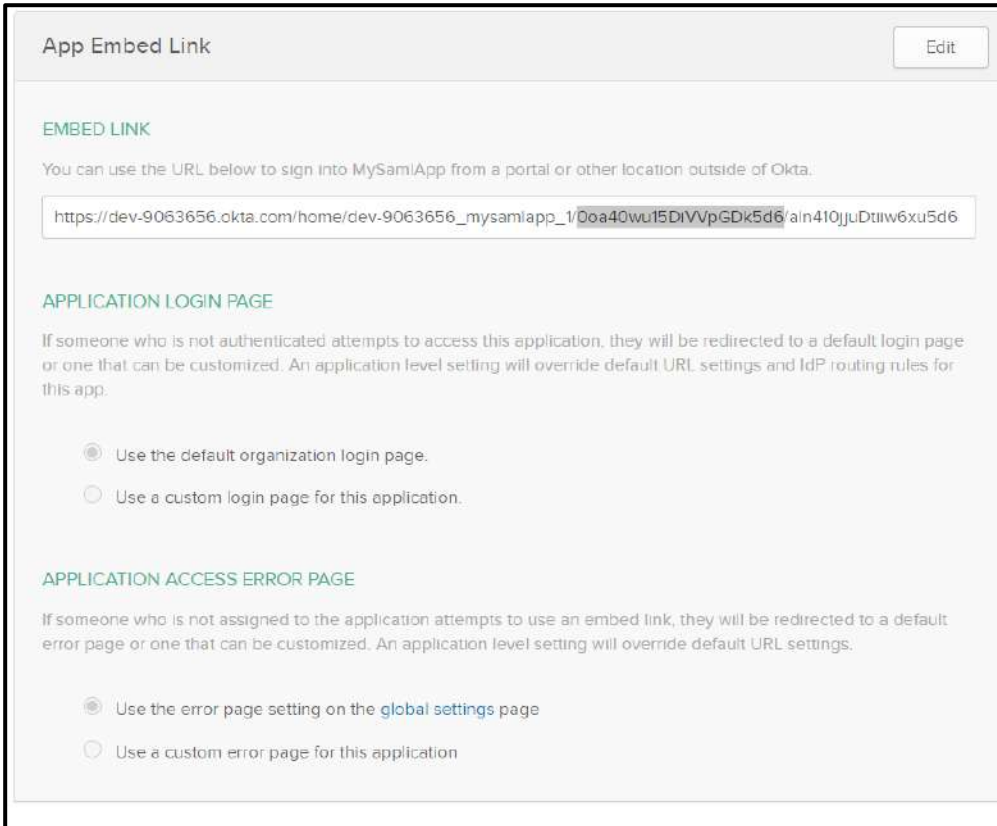
SAML 2.0 streamlines the end user experience by not requiring the user to know their credentials. Users cannot edit their credentials when SAML 2.0 is configured for this application. Additional configuration in the 3rd party application may be required to complete the integration with Okta.

Application Username

Choose a format to use as the default username value when assigning the application to users.

If you select None you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.

32. Next go back to the General Tab.
33. Client ID for SAML Okta is not directly provided in the UI. To fetch Client ID, go to General Tab after finish. Scroll down to the App Embed link section to fetch Client ID.
34. Client ID is part of the Embed link. It is highlighted within the Embed Link as seen below.



App Embed Link Edit

EMBED LINK

You can use the URL below to sign into MySamiApp from a portal or other location outside of Okta.

`https://dev-9063656.okta.com/home/dev-9063656_mysamiapp_1/00a40wu15DiVVpGDk5d6/ain410jjuDtiiw6xu5d6`

APPLICATION LOGIN PAGE

If someone who is not authenticated attempts to access this application, they will be redirected to a default login page or one that can be customized. An application level setting will override default URL settings and IdP routing rules for this app.

Use the default organization login page.

Use a custom login page for this application.

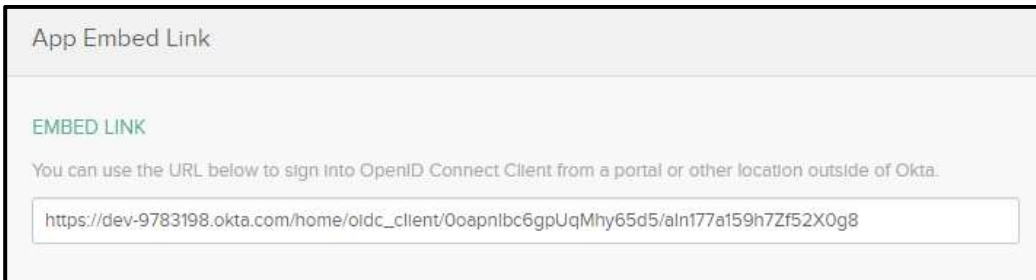
APPLICATION ACCESS ERROR PAGE

If someone who is not assigned to the application attempts to use an embed link, they will be redirected to a default error page or one that can be customized. An application level setting will override default URL settings.

Use the error page setting on the [global settings](#) page

Use a custom error page for this application

35. In the App Embed Link section, you will see an Embed link. If you simply copy and paste this link in browser, it will invoke IDP initiated SSO flow - after all the configurations as discussed in the following sections are completed. This one of the methods of IDP initiated SSO.



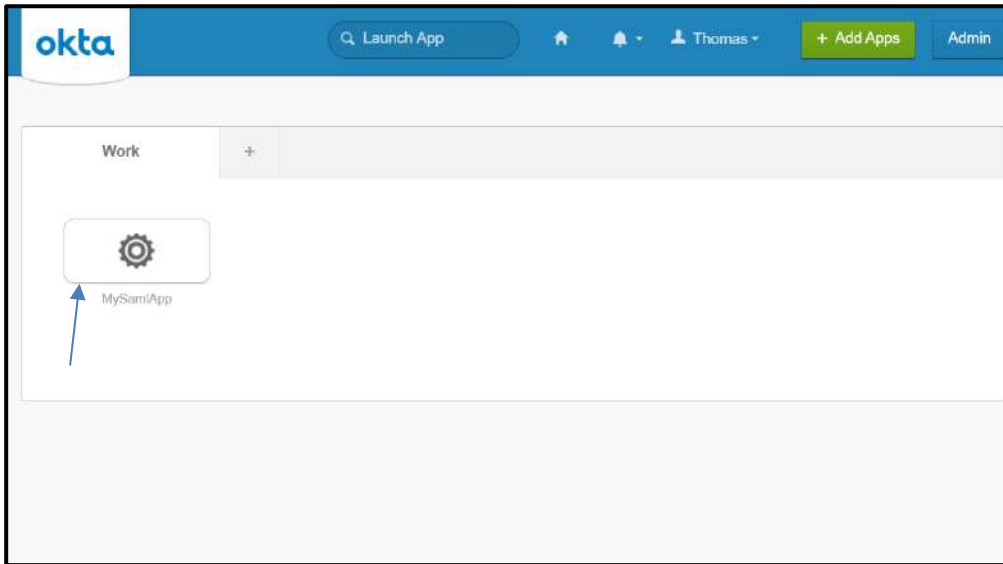
App Embed Link

EMBED LINK

You can use the URL below to sign into OpenID Connect Client from a portal or other location outside of Okta.

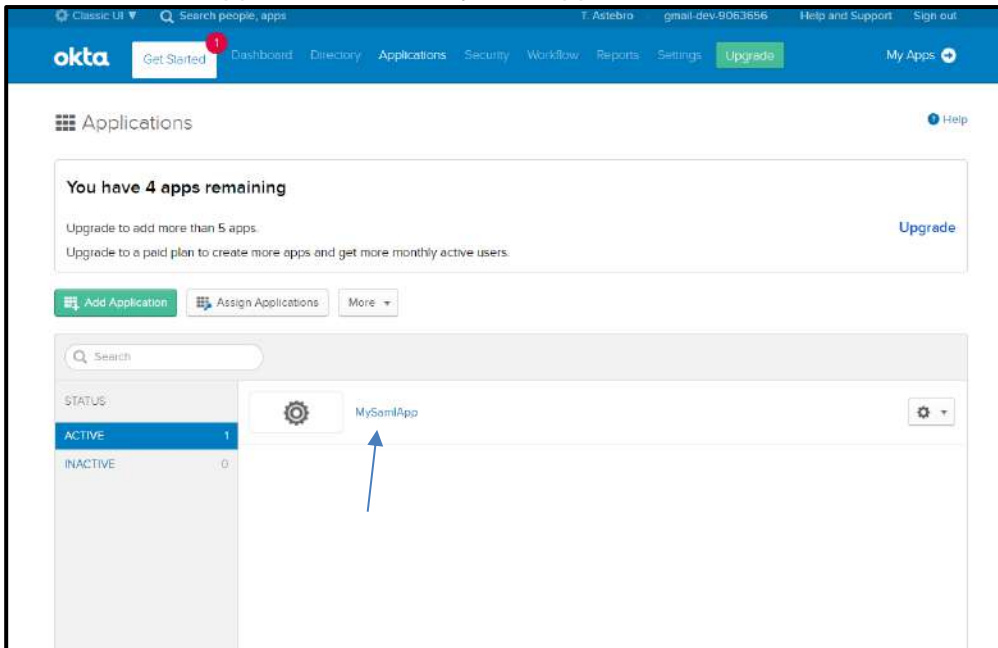
`https://dev-9783198.okta.com/home/oidc_client/00apn1bc6gpUqMhy65d5/ain177a159h7Zf52X0g8`

36. On Okta Classic UI, click MyApps which is the tab on the extreme right. MySamlApp is now visible as seen in the screenshot below. You may click on the App for Single sign on to AE (you will be redirected to AEUI Home page), once all the settings are completed as discussed in further sections.



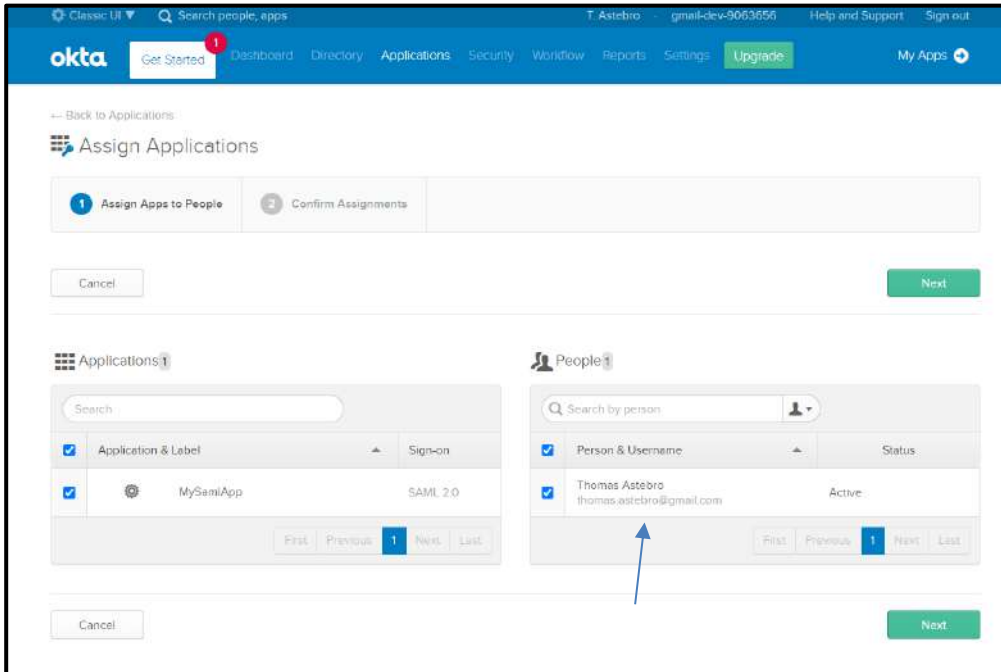
2.4.1.2 Assign Okta Users to SAML App

37. Go back to the Applications Tab. MySamlApp visible as seen below.

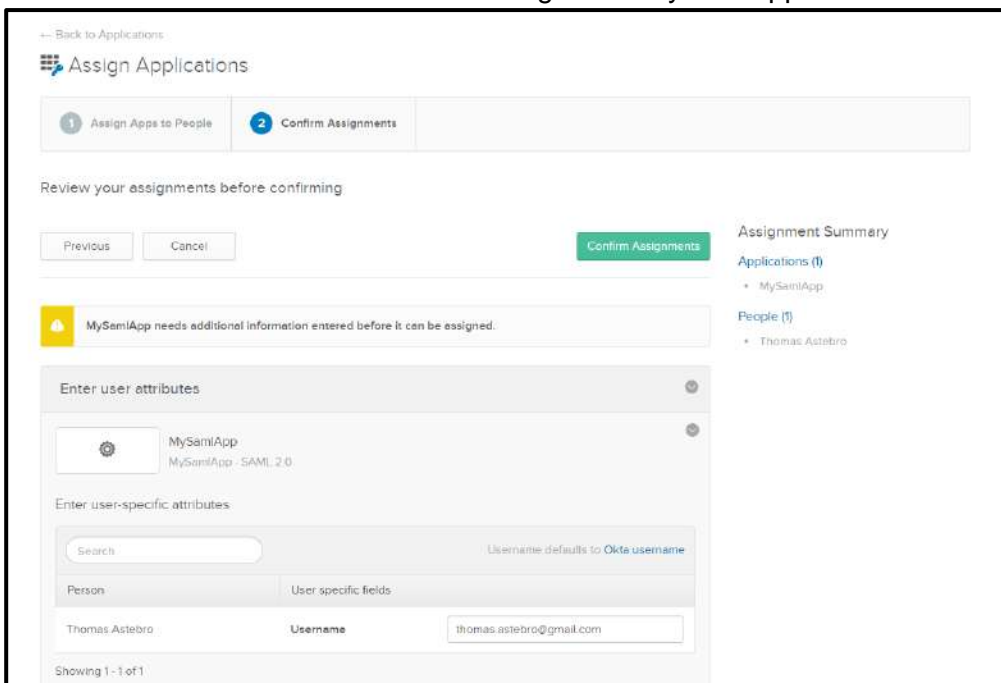


38. On My Web App go to the Assignments Tab. Click on Assign Apps to People.
 39. Enable checkbox next to MySamlApp and the user (i.e. Thomas Astebro) on the right. Click Next.

40. You may also Search for the people to assign this My Web App application. Once the details for the person are visible below, Click Save and Go Back.



41. Click Confirm Assignments button.
42. You can see that Thomas Astebro is assigned to MySamlApp.



43. This completes Okta setups for IDP initiated SSO with SAML App

2.4.2 Setup on AE Tomcat Server for SAML Apps

For SAML Apps the following setup is required on Tomcat server,

1. Stop Tomcat Server
2. Navigate to the <Tomcat home>/webapps\aeui\WEB-INF folder (e.g. D:\AutomationEdge\tools\apache-tomcat-9.0.36\webapps\aeui\WEB-INF)
3. You will see the Web.xml file as seen below.

Name	Date modified	Type	Size
web	1/20/2021 12:43 PM	XML Document	2 KB

4. Edit Web.xml.
5. Comment the line below this comment - <!-- Comment line below in case of SAML SSO integration -->.

i.e. comment - <http-method>POST</http-method> as seen below.

```

<filter-mapping>
  <filter-name>httpHeaderSecurity</filter-name>
  <url-pattern>/*</url-pattern>
  <dispatcher>REQUEST</dispatcher>
</filter-mapping>
<security-constraint>
  <web-resource-collection>
    <web-resource-name>Forbidden Methods</web-resource-name>
    <url-pattern>/*</url-pattern>
    <http-method>OPTIONS</http-method>
    <http-method>TRACE</http-method>
    <http-method>HEAD</http-method>
    <http-method>PATCH</http-method>
    <!-- Comment line below in case of SAML SSO integration -->
    <http-method>POST</http-method>
    <http-method>PUT</http-method>
    <http-method>DELETE</http-method>
  </web-resource-collection>
  <auth-constraint/>
</security-constraint>
</web-app>

```

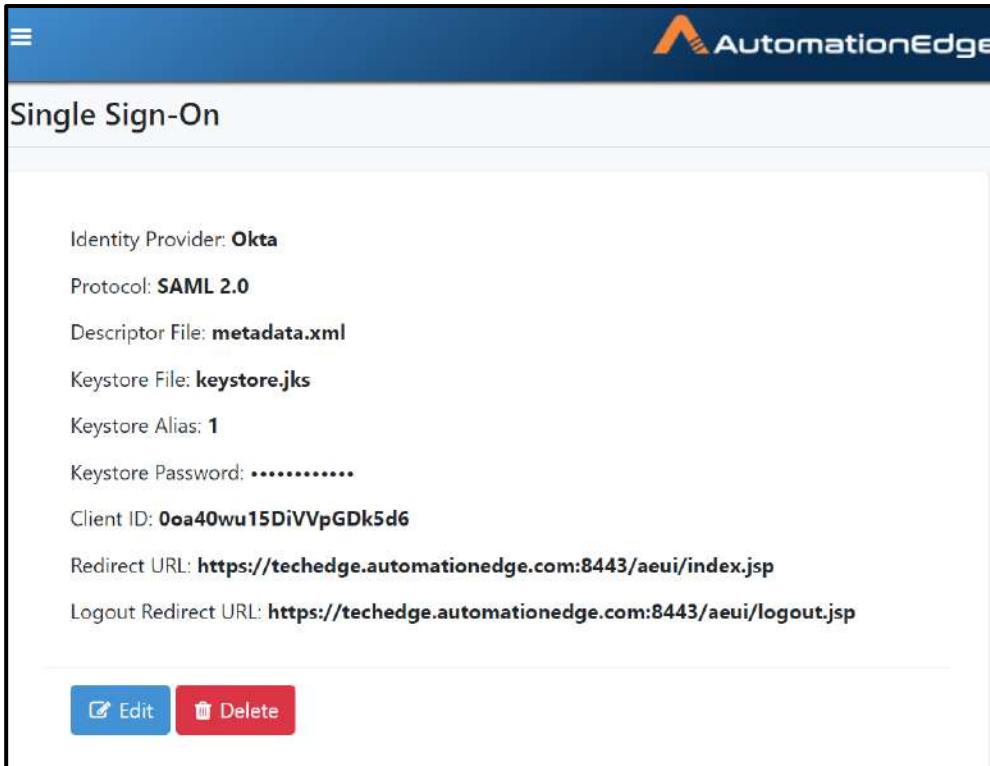
6. Restart Tomcat server.
7. This completes setups on AE Tomcat server

2.4.3 Setups on AE UI for Single Sign-On using SAML

In this section we showcase the AutomationEdge setups.

1. Configure Single Sign-On in AutomationEdge.

(Note: For SAML App import option **is not** used to fetch Metadata URI)

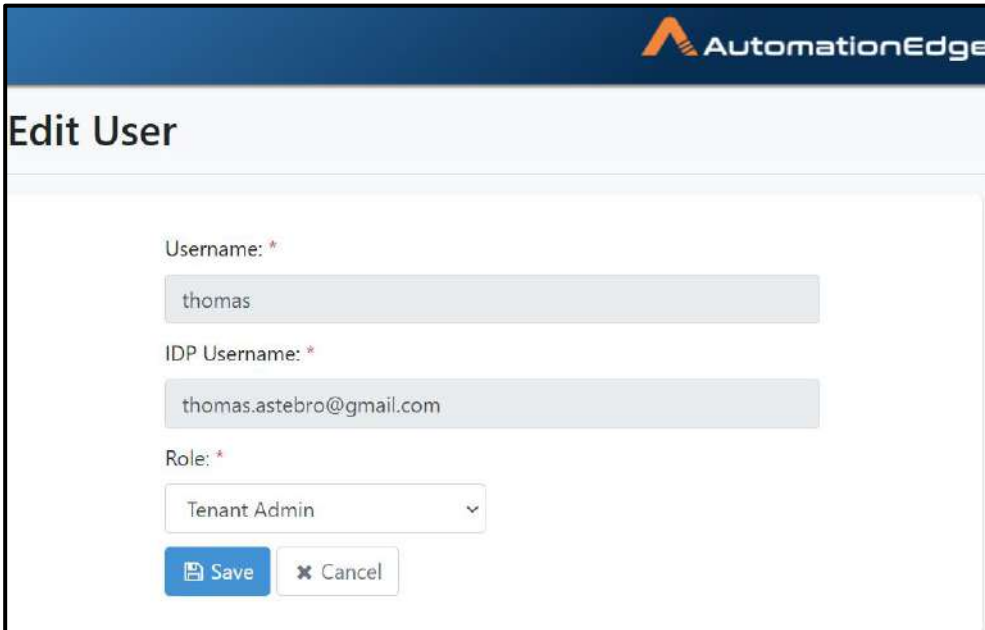


The screenshot displays the AutomationEdge interface for configuring a Single Sign-On (SSO) setup. The page title is "Single Sign-On". The configuration details are as follows:

- Identity Provider: **Okta**
- Protocol: **SAML 2.0**
- Descriptor File: **metadata.xml**
- Keystore File: **keystore.jks**
- Keystore Alias: **1**
- Keystore Password: **••••••••**
- Client ID: **00a40wu15DiVVpGDk5d6**
- Redirect URL: **https://techedge.automationedge.com:8443/aeui/index.jsp**
- Logout Redirect URL: **https://techedge.automationedge.com:8443/aeui/logout.jsp**

At the bottom of the configuration area, there are two buttons: a blue "Edit" button and a red "Delete" button.

2. Create an SSO user in AutomationEdge mapping it to an IDP user with permissions on IDP application.



AutomationEdge

Edit User

Username: *

IDP Username: *

Role: *

2.4.4 Invoke IDP (Okta) initiated SSO using SAML

3. In the Applications General tab locate App Embed Link URL as seen below.

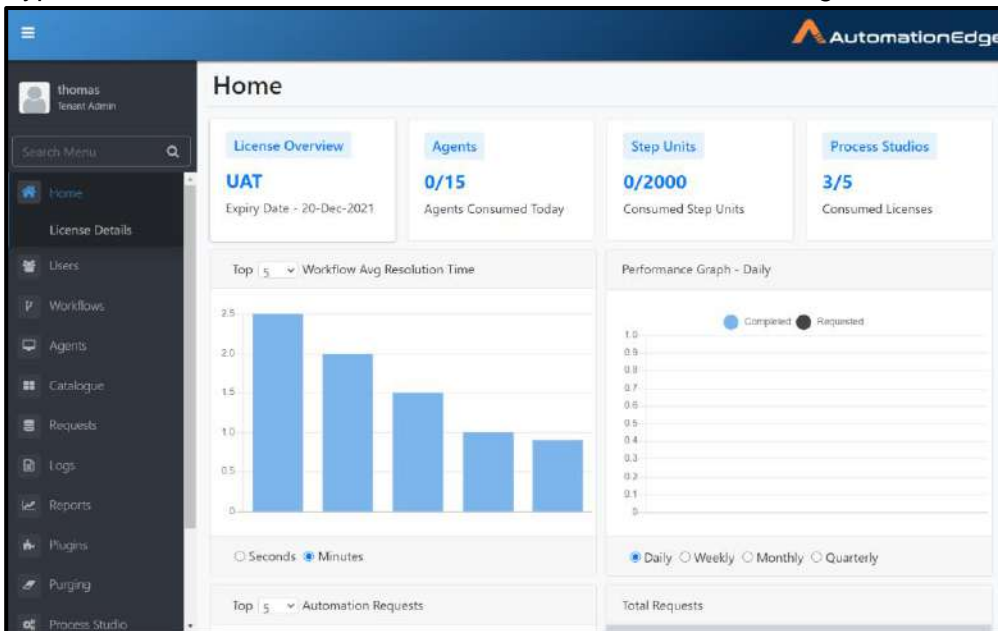
App Embed Link Edit

EMBED LINK

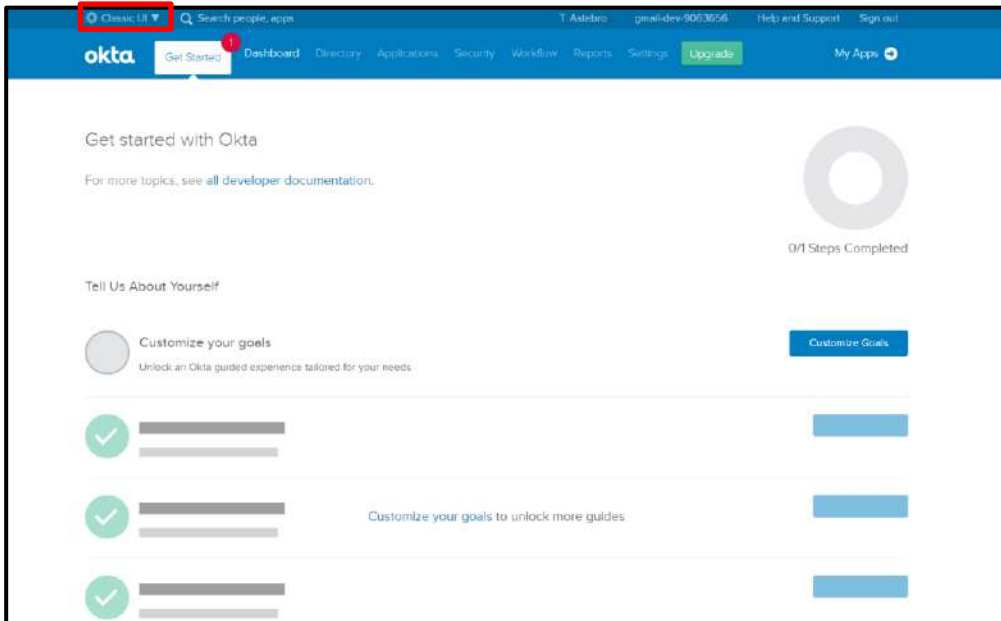
You can use the URL below to sign into MySamlApp from a portal or other location outside of Okta.

`https://dev-9063656.okta.com/home/dev-9063656_mysamlapp_1/0oa40wu15DiVVpGDk5d6/aln410jjuDtiw6xu5d6`

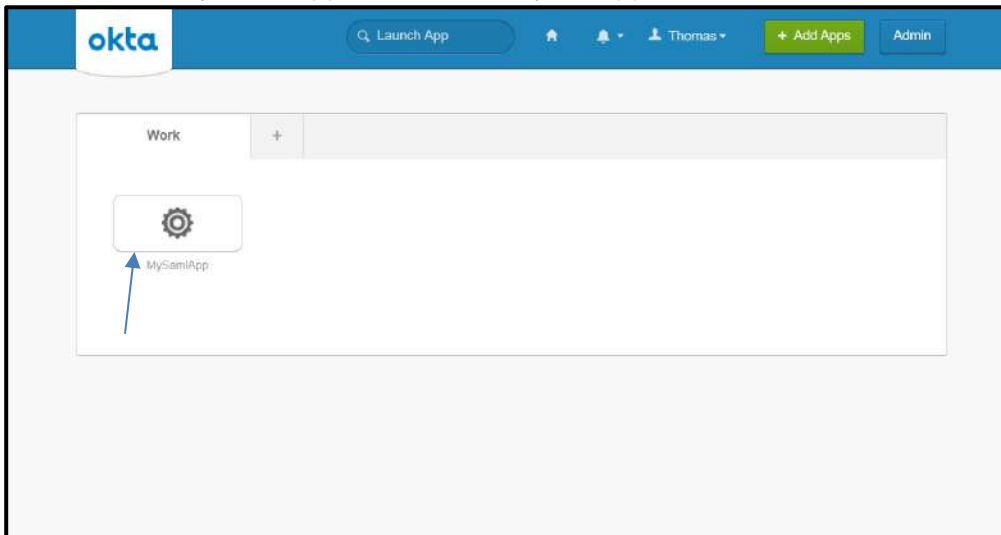
4. Type this URL on the browser and it redirects to AutomationEdge with IDP initiated SSO.



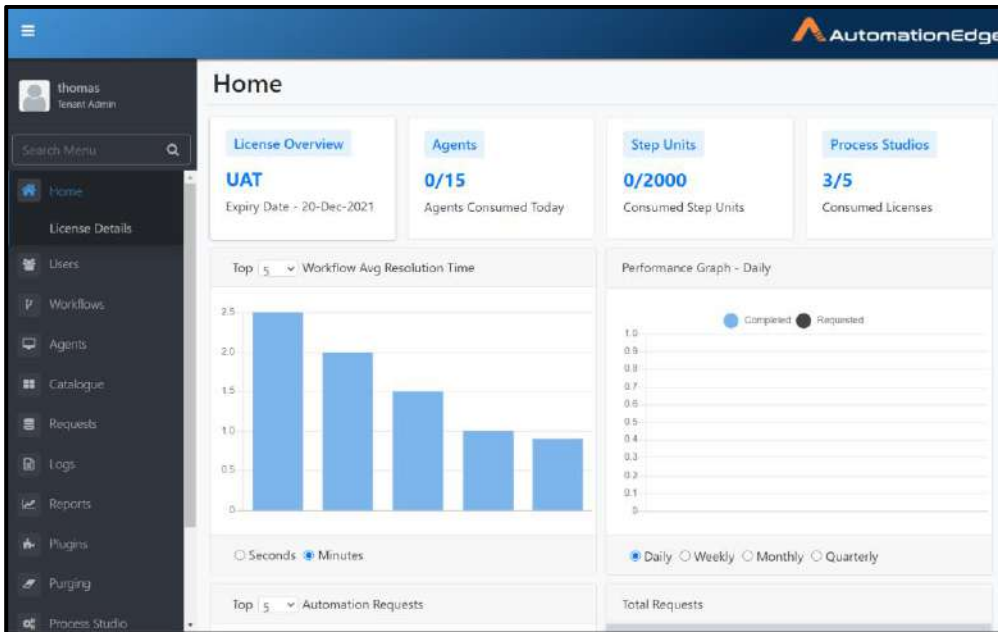
5. Alternately, in Okta Classic UI as seen below, click My Apps on the right hand upper corner.



6. You can see My Web App icon. Click on your application.



7. Clicking on the App takes you to AutomationEdge with IDP initiated SSO.



8. Since Single Logout URL has been set, logout from AE also logs out IDP (Okta).
9. This completes the process of IDP initiated SSO.

2.5 AE initiated SSO with Keycloak using OAuth/OpenID

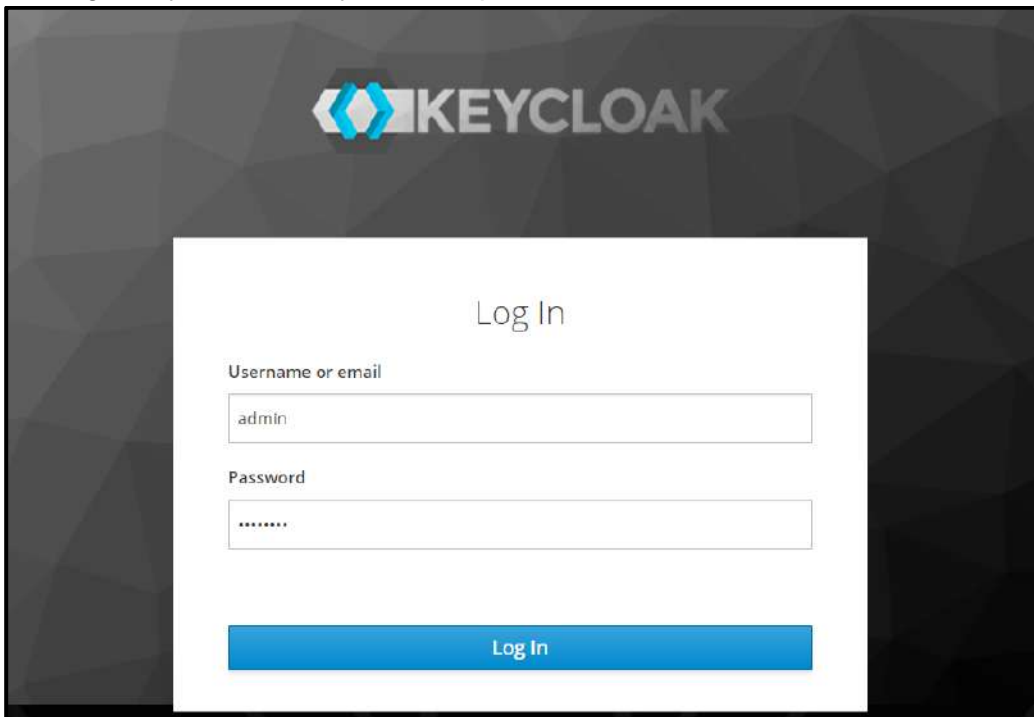
Keycloak Identity Provider supports OpenID Connect and OAuth 2.0 protocols.

In this section we demonstrate how to get the required parameters and some key configurations to setup AutomationEdge SSO with Keycloak.

The following are the required parameters for Keycloak IDP SSO configuration in AutomationEdge,

- Identity Provider Issuer
- Identity Provider Endpoints (Authorization, Token & End Session Endpoints)
- Login redirect URIs
- Client ID

1. Login Keycloak Identity Provider portal.



2. Add Realm if not added.

The screenshot shows the Keycloak Admin Console interface for the 'Master' realm. The left sidebar contains navigation options: Master, Add realm, Realm, Settings, Clients, Client, Scopes, Roles, Identity, Providers, User, Federation, Authentication, Manage, and Groups. The main content area is titled 'Master' and includes tabs for General, Login, Keys, Email, Themes, Cache, Tokens, and Client Registration. Under the 'Security Defenses' section, the following fields are visible:

- Name:** master
- Display name:** Keycloak
- HTML Display name:** <div class="kc-logo-text">Keycloak</div>
- Frontend URL:** (empty)
- Enabled:** ON
- User-Managed Access:** OFF
- Endpoints:** OpenID Endpoint Configuration, SAML 2.0 Identity Provider Metadata

Buttons for 'Save' and 'Cancel' are located at the bottom of the form.

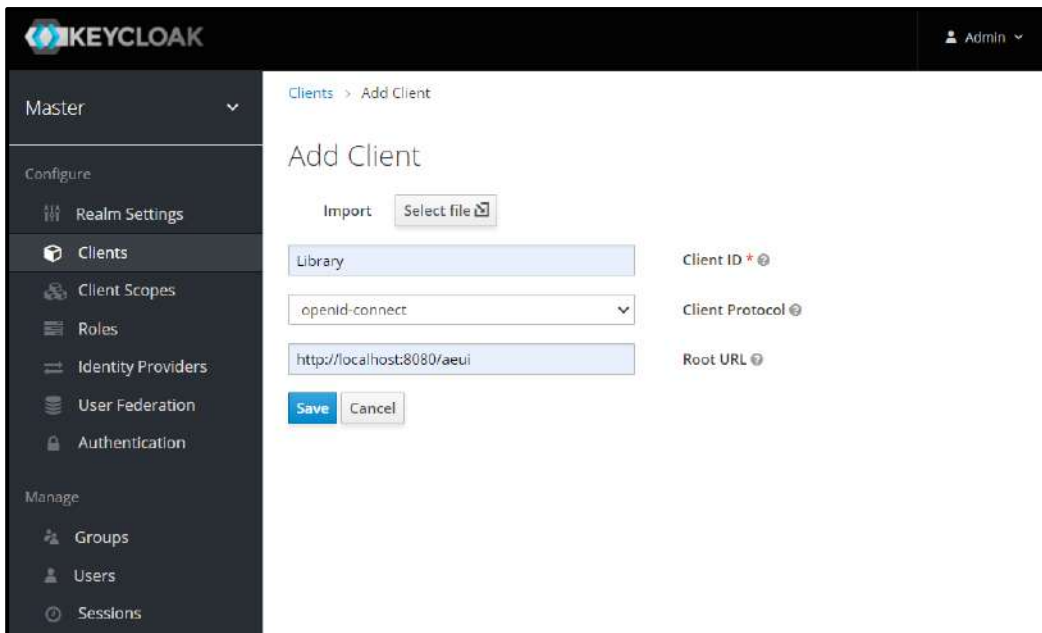
3. Go to the “Clients” section and click the “create” button. We will create a client called “Library”.

The screenshot shows the Keycloak Admin Console interface for the 'Clients' section. The left sidebar contains navigation options: Master, Configure, Realm Settings, Clients, Client Scopes, Roles, Identity Providers, User Federation, Authentication, Manage, Groups, Users, and Sessions. The main content area is titled 'Clients' and includes a 'Lookup' search bar. Below the search bar is a table with the following data:

Client ID	Enabled	Base URL	Actions
account	True	https://localhost:8543/auth/realms/master/account/	Edit Export Delete
account-console	True	https://localhost:8543/auth/realms/master/account/	Edit Export Delete
admin-cli	True	Not defined	Edit Export Delete
broker	True	Not defined	Edit Export Delete
master-realm	True	Not defined	Edit Export Delete
security-admin-console	True	https://localhost:8543/auth/admin/master/console/	Edit Export Delete

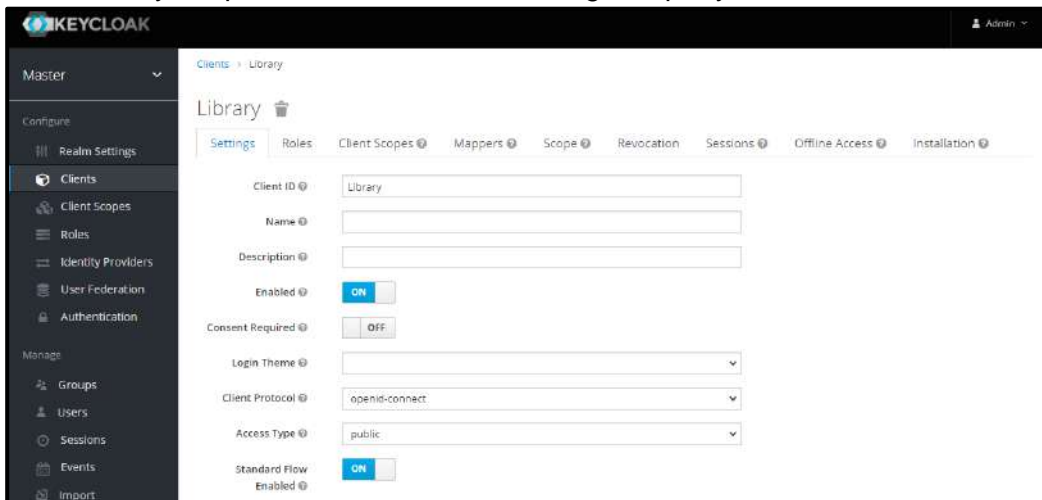
A 'Create' button is located in the top right corner of the table area.

4. Select appropriate Client Protocol and Access Type as public.
5. Specify a valid redirect URL https://Automationedge:{Port}/aeui.



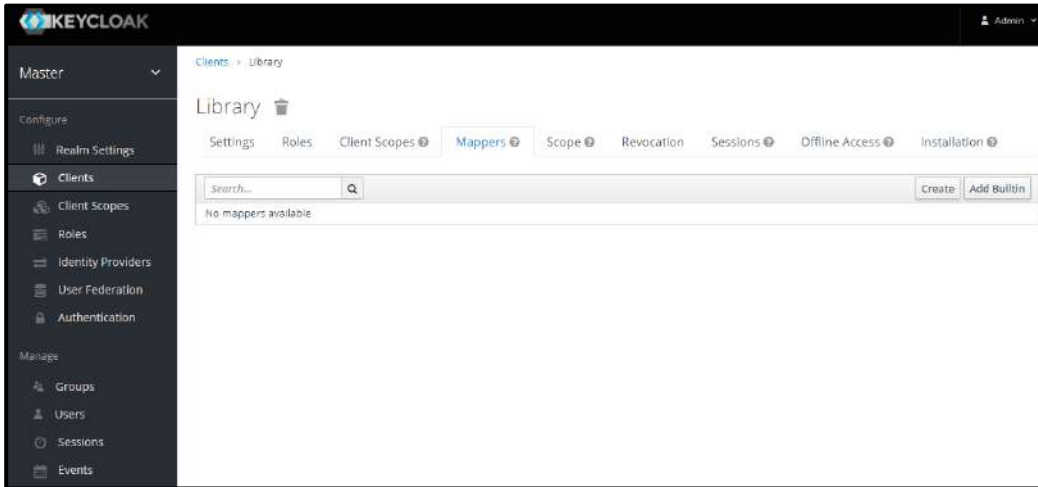
The screenshot shows the Keycloak administration console. The left sidebar contains navigation options: Master, Configure (Realm Settings, Clients, Client Scopes, Roles, Identity Providers, User Federation, Authentication), and Manage (Groups, Users, Sessions). The main content area is titled 'Add Client' and includes an 'Import' button with a 'Select file' icon. Below this are three input fields: 'Library' (text), 'openid-connect' (dropdown), and 'http://localhost:8080/aeui' (text). To the right, there are three labels: 'Client ID', 'Client Protocol', and 'Root URL'. At the bottom of the form are 'Save' and 'Cancel' buttons.

6. You may keep the default values or change as per your need.

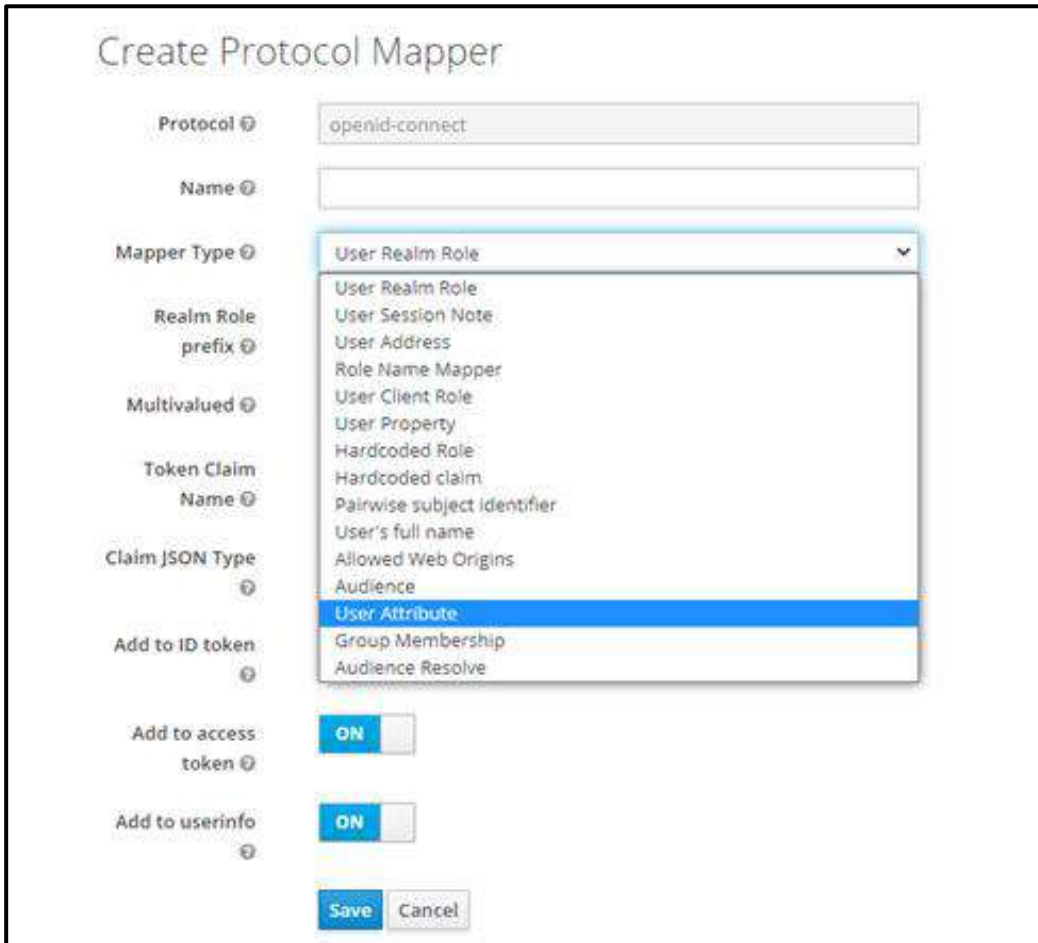


The screenshot shows the Keycloak administration console for the 'Library' client. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Library' and has a trash icon. Below the title are several tabs: 'Settings', 'Roles', 'Client Scopes', 'Mappers', 'Scope', 'Revocation', 'Sessions', 'Offline Access', and 'Installation'. The 'Settings' tab is active, showing various configuration options: 'Client ID' (text field with 'Library'), 'Name' (text field), 'Description' (text field), 'Enabled' (toggle switch set to 'ON'), 'Consent Required' (toggle switch set to 'OFF'), 'Login Theme' (dropdown menu), 'Client Protocol' (dropdown menu with 'openid-connect'), 'Access Type' (dropdown menu with 'public'), and 'Standard Flow Enabled' (toggle switch set to 'ON').

- In Client menu click on the Mappers tab. Click Create button to open the Create Protocol Mapper for creating claims.



- On the Create Protocol Mapper page, select Mapper Type as User Attribute.



- Enter details to create the first User Attribute uniquely as seen below. Click Save.

[Clients](#) > [Library](#) > [Mappers](#) > Create Protocol Mappers

Create Protocol Mapper

Protocol	<input type="text" value="openid-connect"/>
Name	<input type="text" value="uniqueid"/>
Mapper Type	<input type="text" value="User Attribute"/>
User Attribute	<input type="text" value="uniqueid"/>
Token Claim Name	<input type="text" value="uniqueid"/>
Claim JSON Type	<input type="text" value="Select One..."/>
Add to ID token	<input checked="" type="checkbox"/> ON
Add to access token	<input checked="" type="checkbox"/> ON
Add to userinfo	<input checked="" type="checkbox"/> ON
Multivalued	<input type="checkbox"/> OFF
Aggregate attribute values	<input type="checkbox"/> OFF

10. Success! Mapper has been created message appears at the top as seen below.

The screenshot shows the 'UniquelId' mapper configuration page. At the top, a green success message reads 'Success! Mapper has been created.' The configuration fields are as follows:

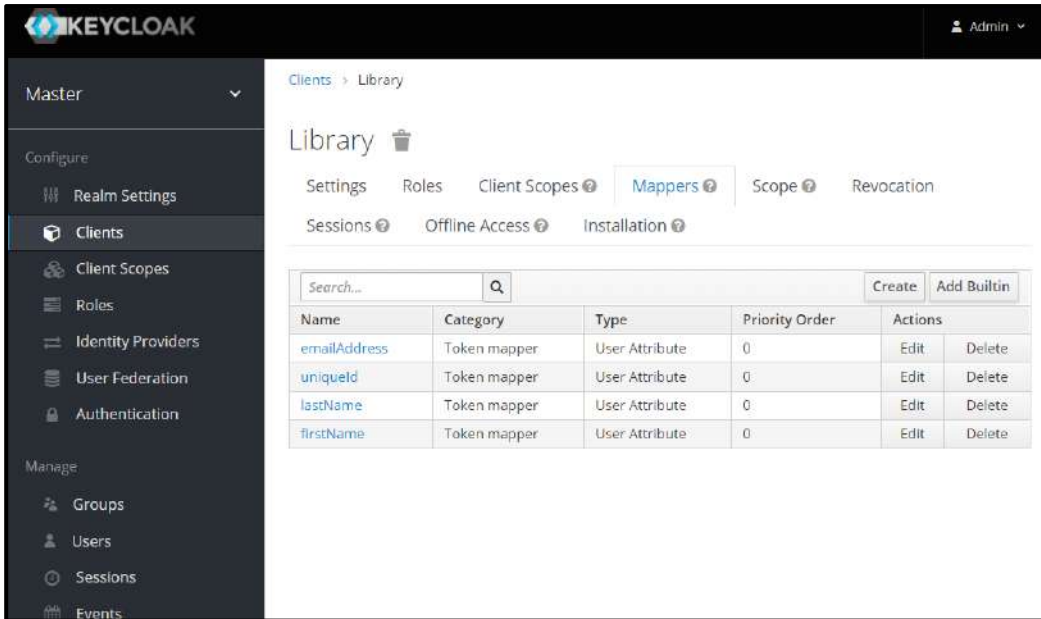
- Protocol: openId-connect
- ID: 64aa176d-fb44-4b53-9b4b-8e7fe7fc90d
- Name: uniquelId
- Mapper Type: User Attribute
- User Attribute: uniquelId
- Token Claim Name: uniquelId
- Claim JSON Type: Select One...
- Add to ID token: ON
- Add to access token: ON
- Add to userinfo: ON
- Multivalued: OFF
- Aggregate attribute values: OFF

Buttons for 'Save' and 'Cancel' are located at the bottom of the form.

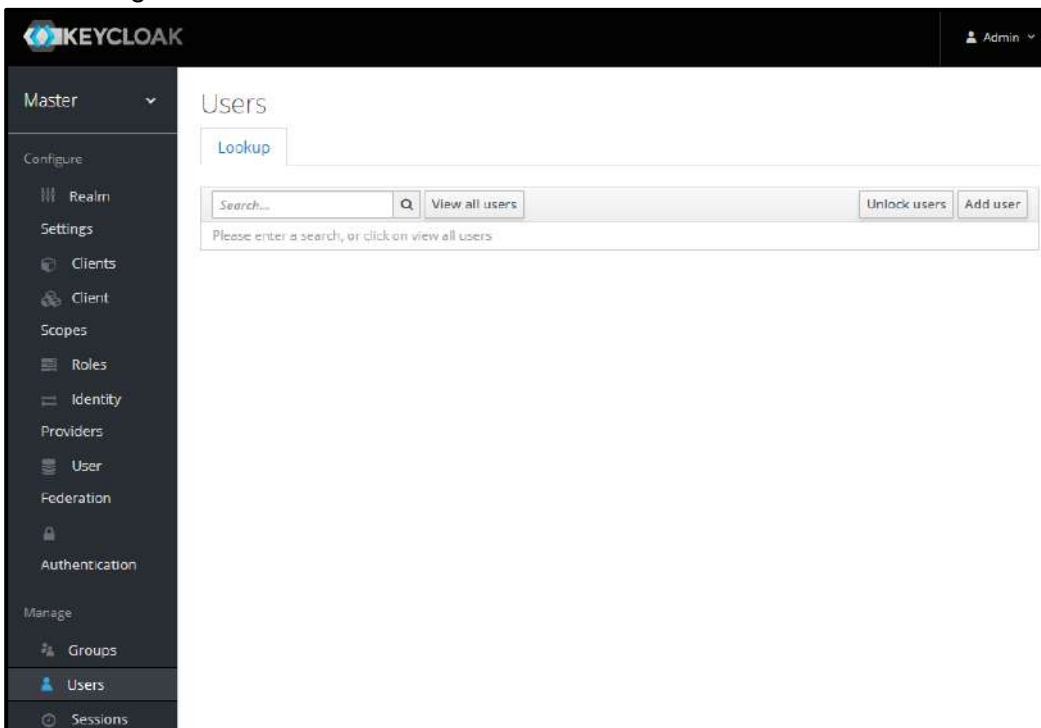
11. Complete creating the following Mappers (Claims) for JWT (Access) token; to be used by Service Provider (in this case AutomationEdge).

Name	Uses Attribute	Token Claim Name
uniqueId	uniqueId	uniqueId
firstName	firstName	firstName
lastName	lastName	lastName
emailAddress	emailAddress	emailAddress

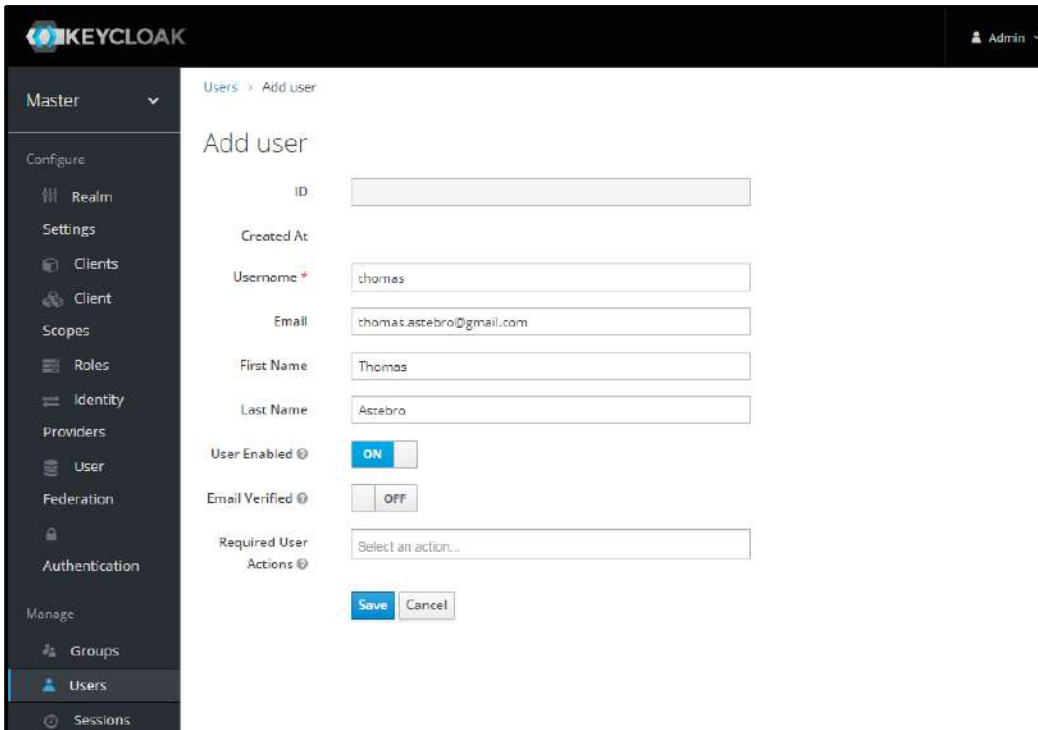
12. Create four Mappers in the client. After creating Mappers, it looks as shown below,



13. Now create a user. Specify the First Name, Last Name and Email. To set user credentials, go to the credentials tab and choose a password, we have used “password” for the rest of this article. Turn off the “Temporary” flag unless you want the user to change password on first login.



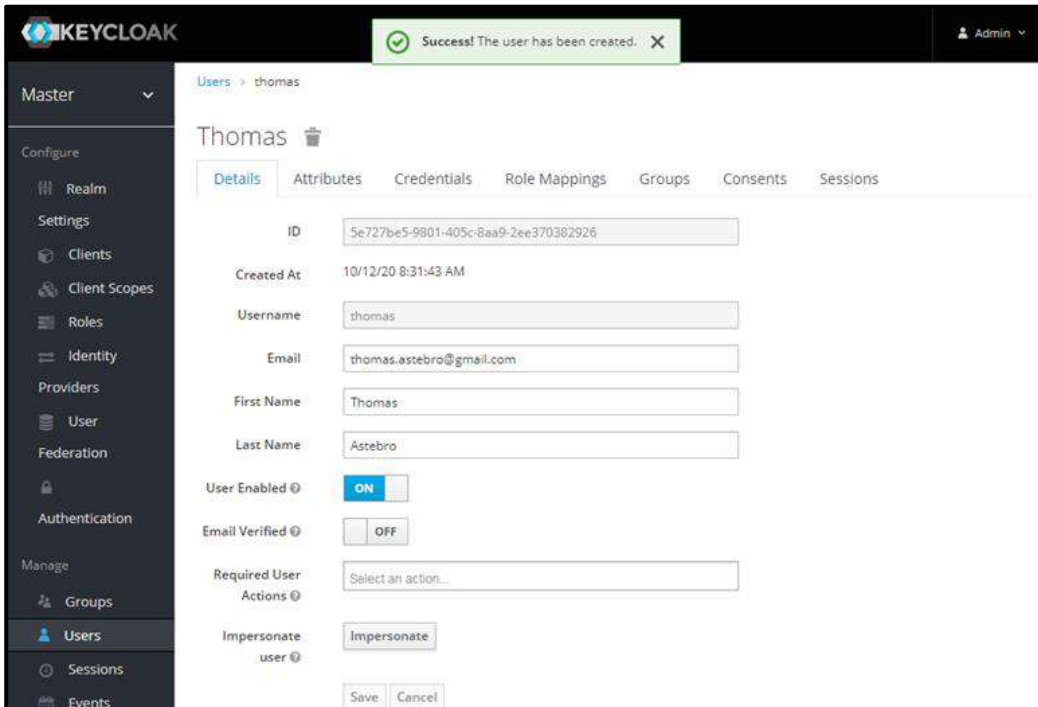
14. Configure User details. Click Save.



The screenshot shows the Keycloak administration interface for adding a new user. The left sidebar contains navigation menus for 'Configure' (Realm, Settings, Clients, Client Scopes, Roles, Identity, Providers, User, Federation), 'Authentication', and 'Manage' (Groups, Users, Sessions). The main content area is titled 'Add user' and contains the following fields and controls:

- ID:
- Created At:
- Username:
- Email:
- First Name:
- Last Name:
- User Enabled:
- Email Verified:
- Required User Actions:
- Buttons:

15. Success! User has been created message appears at the top.



The screenshot shows the Keycloak administration interface for the user 'thomas'. A green success message is displayed at the top: 'Success! The user has been created. X'. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Thomas' and contains the following fields and controls:

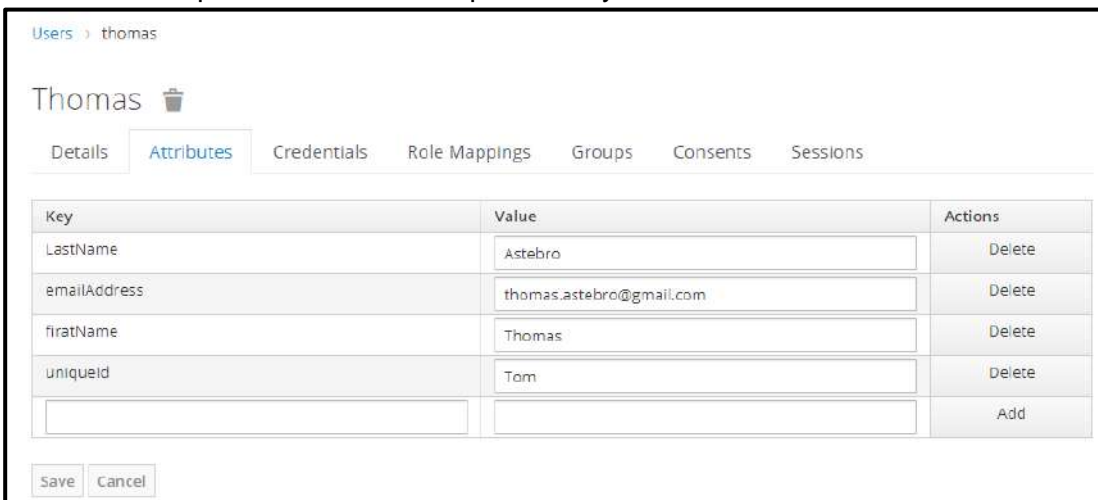
- ID:
- Created At:
- Username:
- Email:
- First Name:
- Last Name:
- User Enabled:
- Email Verified:
- Required User Actions:
- Impersonate user:
- Buttons:

16. Click Attributes tab to add the following four attributes for the user. Provide the actual values in the Value.


Key	Value
uniqueId	{username}
firstName	{first-Name}
lastName	{last-Name}
emailAddress	{email}

 **Note:** It is **mandatory** to specify actual values for the first 3 attributes: uniqueId, firstName and lastName

17. Below are sample values for the respective keys.



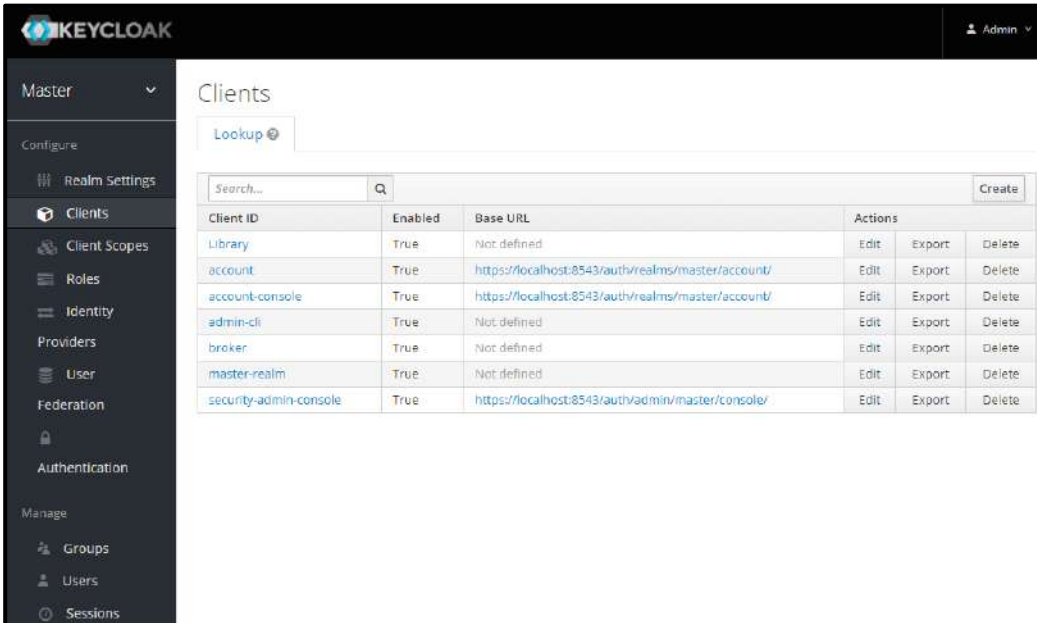
Users > thomas

Thomas 

Details **Attributes** Credentials Role Mappings Groups Consents Sessions

Key	Value	Actions
LastName	<input type="text" value="Astebro"/>	Delete
emailAddress	<input type="text" value="thomas.astebro@gmail.com"/>	Delete
firstName	<input type="text" value="Thomas"/>	Delete
uniqueId	<input type="text" value="Tom"/>	Delete
<input type="text"/>	<input type="text"/>	Add

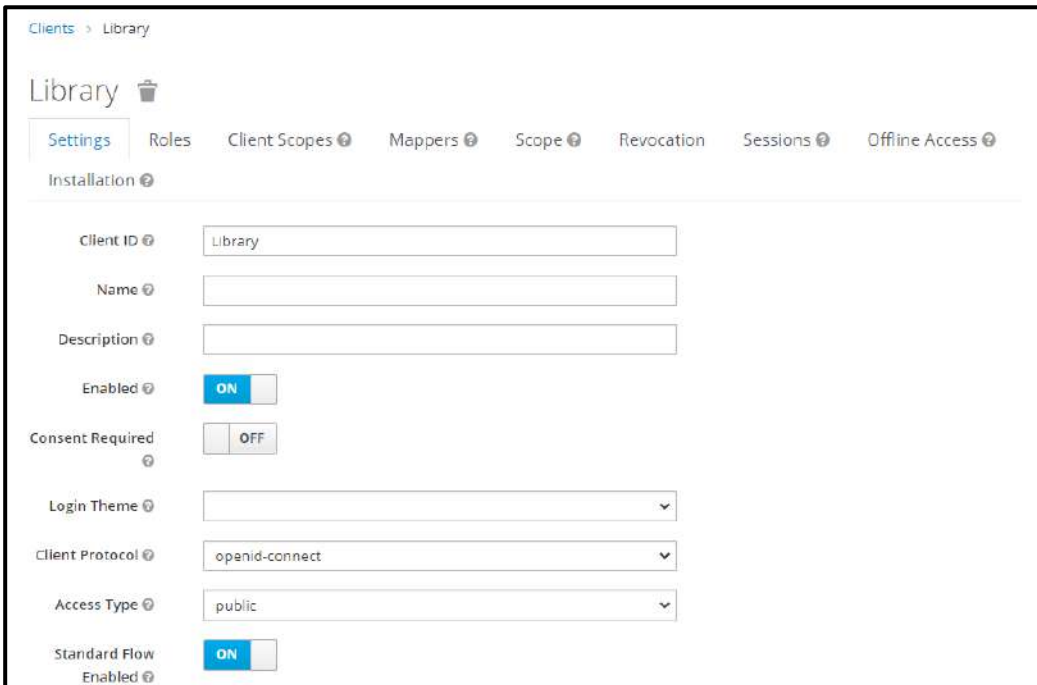
18. Next, we wish to fetch the Client ID, Redirect URLs.
19. Click on the Clients link the left Navigation menu. Click on Library link in the list.



The screenshot shows the Keycloak Admin Console interface. The left navigation menu is expanded to 'Clients'. The main content area displays a table of clients. The table has columns for Client ID, Enabled, Base URL, and Actions. The 'Library' client is highlighted.

Client ID	Enabled	Base URL	Actions
Library	True	Not defined	Edit Export Delete
account	True	https://localhost:8543/auth/realms/master/account/	Edit Export Delete
account-console	True	https://localhost:8543/auth/realms/master/account/	Edit Export Delete
admin-cli	True	Not defined	Edit Export Delete
broker	True	Not defined	Edit Export Delete
master-realm	True	Not defined	Edit Export Delete
security-admin-console	True	https://localhost:8543/auth/admin/master/console/	Edit Export Delete

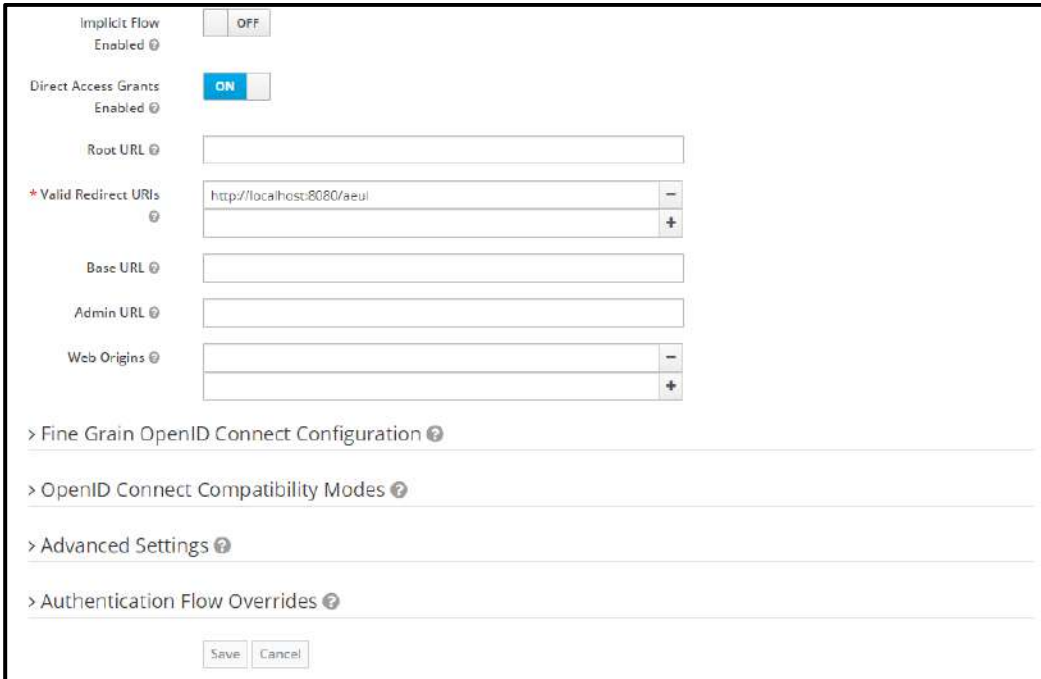
20. Get the Client ID.



The screenshot shows the configuration page for the 'Library' client in the Keycloak Admin Console. The 'Settings' tab is selected. The configuration includes the following fields:

- Client ID: Library
- Name: (empty)
- Description: (empty)
- Enabled: ON
- Consent Required: OFF
- Login Theme: (empty)
- Client Protocol: openid-connect
- Access Type: public
- Standard Flow Enabled: ON

21. You can now get the Valid Redirect URIs as seen below.



The screenshot shows a configuration page for OpenID Connect. It includes several sections with toggle switches and input fields:

- Implicit Flow**: Enabled OFF
- Direct Access Grants**: Enabled ON
- Root URL**:
- * Valid Redirect URIs**:
- Base URL**:
- Admin URL**:
- Web Origins**:

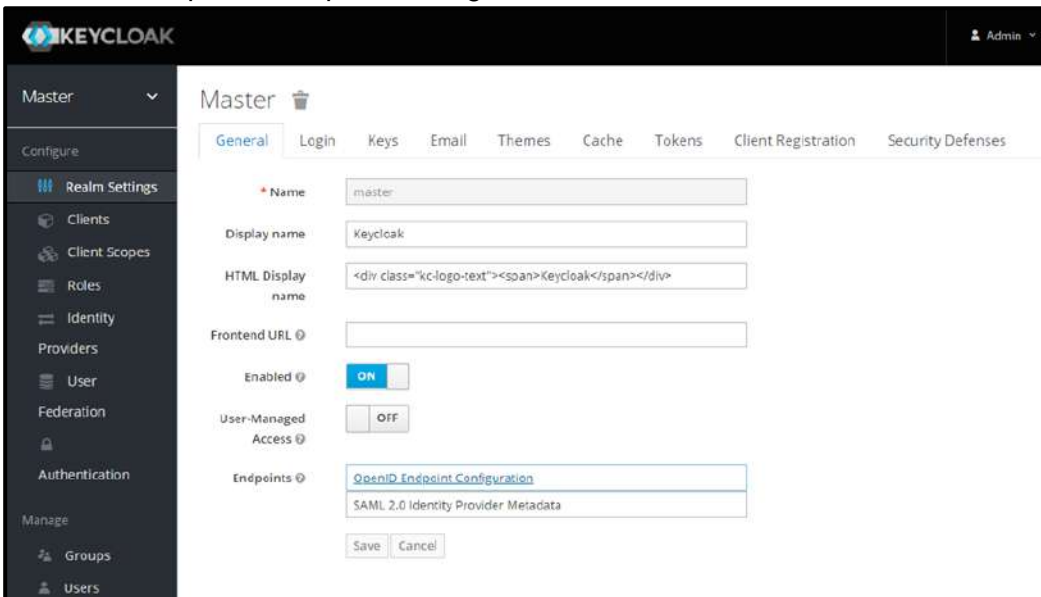
Below these fields are expandable sections:

- > Fine Grain OpenID Connect Configuration
- > OpenID Connect Compatibility Modes
- > Advanced Settings
- > Authentication Flow Overrides

At the bottom are and .

22. Go back to the Realm Settings menu.

23. Click on the OpenID Endpoint Configuration.



The screenshot shows the Keycloak Admin Console for the 'master' realm. The left sidebar contains a navigation menu with 'Realm Settings' selected. The main content area shows the 'OpenID Endpoint Configuration' for the 'master' realm.

Configuration details:

- Name**: master
- Display name**: Keycloak
- HTML Display name**: `<div class="kc-logo-text">Keycloak</div>`
- Frontend URL**:
- Enabled**: ON
- User-Managed Access**: OFF
- Endpoints**:
 - [OpenID Endpoint Configuration](#)
 - SAML 2.0 Identity Provider Metadata

At the bottom are and .

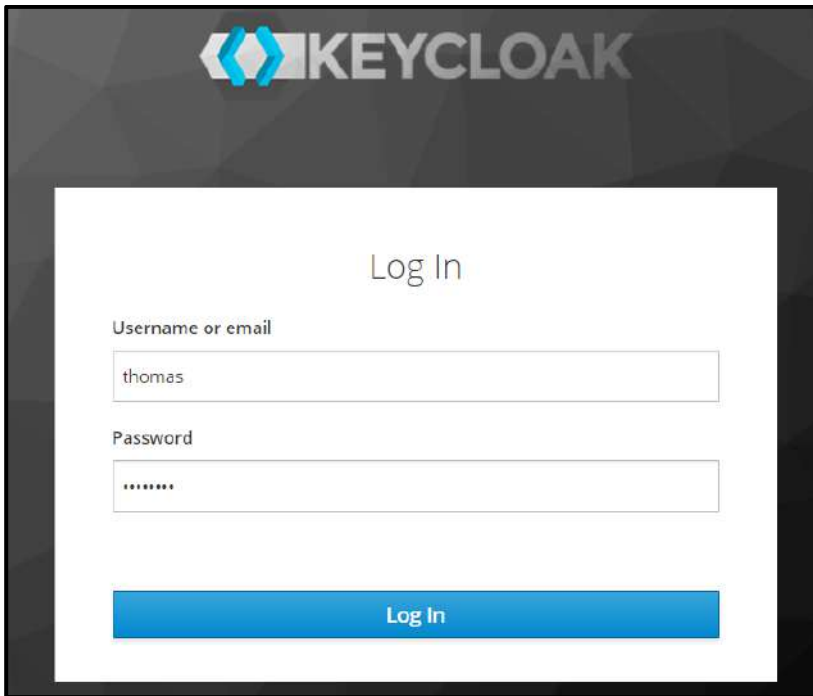
24. You can fetch the `authorization_endpoint` key value and other Endpoints from the Endpoints JSON below.

```
{
  "issuer": "https://localhost:8543/auth/realms/master",
  "authorization_endpoint": "https://localhost:8543/auth/realms/master/protocol/openid-connect/auth",
  "token_endpoint": "https://localhost:8543/auth/realms/master/protocol/openid-connect/token",
  "introspection_endpoint": "https://localhost:8543/auth/realms/master/protocol/openid-connect/token/introspect",
  "userinfo_endpoint": "https://localhost:8543/auth/realms/master/protocol/openid-connect/userinfo",
  "end_session_endpoint": "https://localhost:8543/auth/realms/master/protocol/openid-connect/logout",
  "jwks_uri": "https://localhost:8543/auth/realms/master/protocol/openid-connect/certs",
  "check_session_iframe": "https://localhost:8543/auth/realms/master/protocol/openid-connect/login-status-iframe.html",
  "grant_types_supported": [
    "authorization_code",
    "implicit",
    "refresh_token",
    "password",
    "client_credentials"
  ],
  "response_types_supported": [
    "code",
    "none",
    "id_token",
    "token",
    "id_token token",
    "code id_token",
    "code id_token token"
  ],
  "subject_types_supported": [
    "public",
    "pairwise"
  ],
  "id_token_signing_alg_values_supported": [
    "PS384",
    "ES384",
    "RS384",
    "HS256",
    "HS512",
    "ES256",
    "RS256",
    "HS384",
    "ES512",
    "PS256",
    "PS512",
    "RS512"
  ],
  "id_token_encryption_alg_values_supported": [
    "RSA-OAEP",
    "RSA1_5"
  ],
  "id_token_encryption_enc_values_supported": [
    "A256GCM",
    "A192GCM",
    "A128GCM",
    "A128CBC-HS256",
    "A192CBC-HS384",
    "A256CBC-HS512"
  ],
  "userinfo_signing_alg_values_supported": [
    "PS384",
    "ES384",
    "RS384",
    "HS256",
    "HS512",
    "ES256",
    "RS256",
    "HS384",
    "ES512",
    "PS256",
    "PS512",
    "RS512",
    "none"
  ],
  "request_object_signing_alg_values_supported": [
    "PS384",
    "ES384",
    "RS384",
    "HS256",
    "HS512",
    "ES256",
    "RS256",
    "HS384",
    "ES512",
    "PS256",
    "PS512",
    "RS512",
    "none"
  ],
  "response_modes_supported": [
    "query",
    "fragment",
    "form_post"
  ],
  "registration_endpoint": "https://localhost:8543/auth/realms/master/clients-registrations/openid-connect",
  "token_endpoint_auth_methods_supported": [
    "private_key_jwt",
    "client_secret_basic",
    "client_secret_post",
    "tls_client_auth",
    "client_secret_jwt"
  ],
  "token_endpoint_auth_signing_alg_values_supported": [
    "PS384",
    "ES384",
    "RS384",
    "HS256",
    "HS512",
    "ES256",
    "RS256",
    "HS384",
    "ES512",
    "PS256",
    "PS512",
    "RS512"
  ],
  "claims_supported": [
    "aud",
    "sub",
    "iss",
    "auth_time",
    "name",
    "given_name",
    "family_name",
    "preferred_username",
    "email",
    "acr"
  ],
  "claim_types_supported": [
    "normal"
  ],
  "claims_parameter_supported": false,
  "scopes_supported": [
    "openid",
    "address",
    "email",
    "microprofile-jwt",
    "offline_access",
    "phone",
    "profile",
    "roles",
    "web-origins"
  ],
  "request_parameter_supported": true,
  "request_uri_parameter_supported": true,
  "code_challenge_methods_supported": [
    "plain",
    "S256"
  ],
  "tls_client_certificate_bound_access_tokens": true
}
```

25. In summary to fetch Endpoints Json: In the Keycloak Console, navigate to Realm Settings. Copy the Endpoints Link (i.e. OpenId Endpoint Configuration) to open the Endpoint JSON.
26. Thus we have seen how to get Client ID, Redirect URIs and Identity Provider Endpoints (Authorization, Token and End Session Endpoints) in Keycloak.
27. On AutomationEdge UI you can now complete configurations under Settings→Single Sign-On; by entering the values or by importing the endpoints authorization file.
28. Create an SSO user in AutomationEdge UI. The username should be the same as the uniqueid of an IDP user (In this example the uniqueid for username thomas is tom). So create a claims parameter with username tom.
29. Now Sign In with SSO link on AutomationEdge UI. Provide the Organization Code.

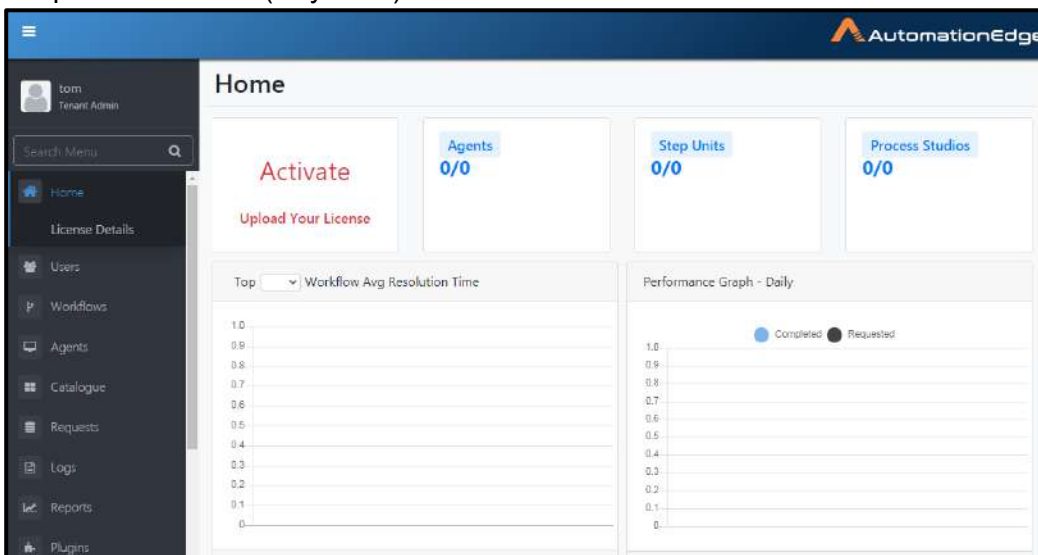
The screenshot shows a web form for entering an organization code. At the top, it says "To go to your company's login page, enter the Organization Code". Below this is a text input field containing "XXXXXX". At the bottom of the form, there are two buttons: a "Back" button with a left-pointing arrow and a "Continue" button with a right-pointing arrow.

30. You are redirected to the Keycloak login page.



The image shows the Keycloak login page. At the top, the Keycloak logo is displayed. Below the logo, the text "Log In" is centered. There are two input fields: "Username or email" with the value "thomas" and "Password" with a masked password "*****". A blue "Log In" button is positioned below the password field.

31. You logged in to AutomationEdge. Note that the user logged in is the same as the uniqueid of the IDP (Keycloak) user 'tom'.



The image shows the AutomationEdge Home dashboard. The top navigation bar includes the AutomationEdge logo and the user name "tom Terence Admin". The main content area is titled "Home" and features several widgets:

- Activate**: A red button labeled "Upload Your License".
- Agents**: A blue box showing "0/0".
- Step Units**: A blue box showing "0/0".
- Process Studios**: A blue box showing "0/0".
- Workflow Avg Resolution Time**: A line graph with a y-axis from 0 to 1.0 and a dropdown menu set to "Top".
- Performance Graph - Daily**: A line graph with a y-axis from 0 to 1.0, showing data for "Completed" (blue) and "Requested" (black).

32. This completes the process of configuring Keycloak and AutomationEdge for SSO using OpenID Connect protocol for Web applications.

2.6 AE initiated SSO with Keycloak using SAML

Keycloak Identity Provider supports OAuth 2.0/OpenID Connect and SAML protocols.

In this section we demonstrate configurations to setup AutomationEdge SSO with Keycloak using SAML protocol.

We will also showcase how to get the required parameters for AutomationEdge – Keycloak Single Sign-On Settings.

The following parameters are obtained from IDP configuration,


- Identity Provider Metadata (store in descriptor.xml)
- Client ID
- Redirect URIs

For IDP SSO configurations we need,

- Keystore file, Keystore Alias, Keystore Password

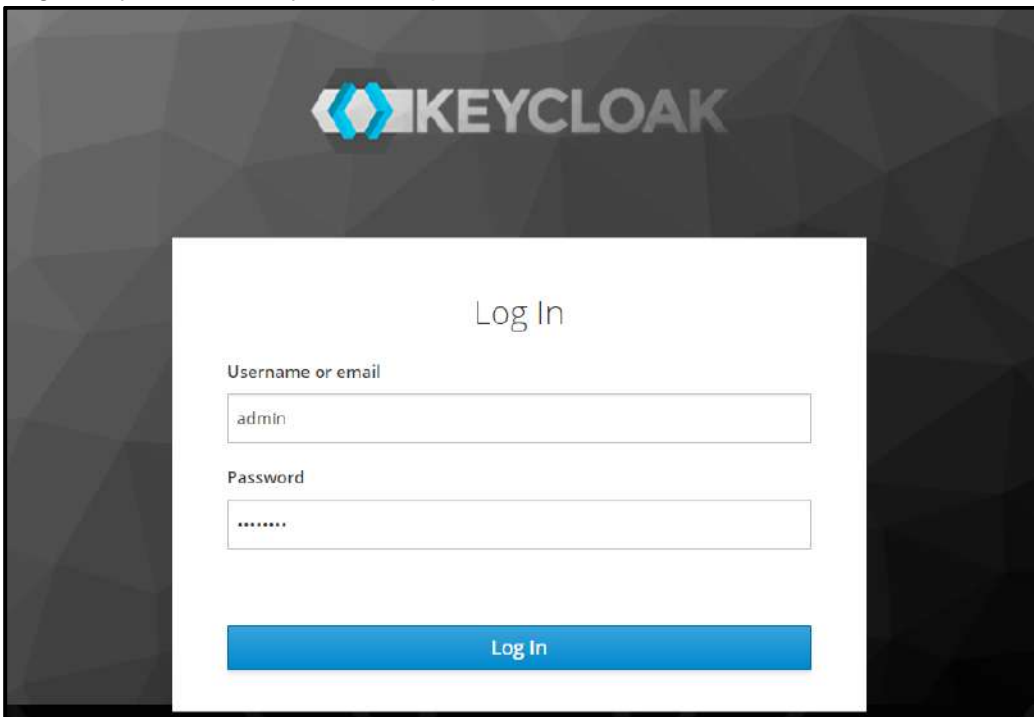
Additionally, for IDP SSO configurations we need,

- Certificate file (.crt)

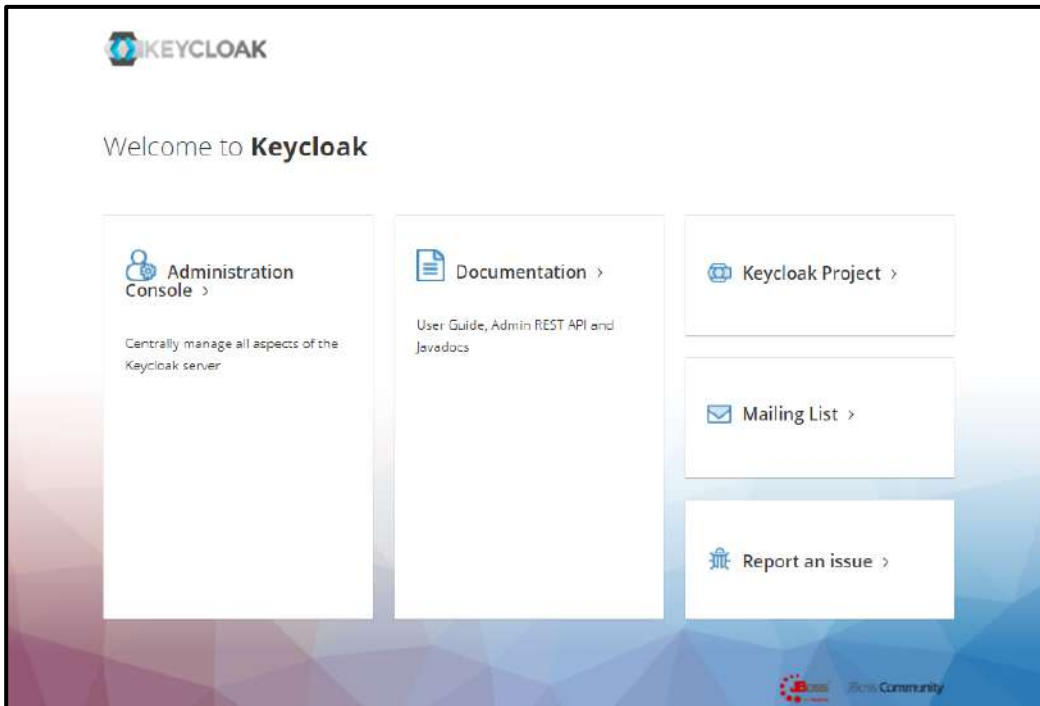
 **Note:** For Keystore and Certificate; to generate Self Signed or CA Certificate refer to section [2.9 Keystore and Certificate Generation](#)

Follow the steps below to configure Keycloak,

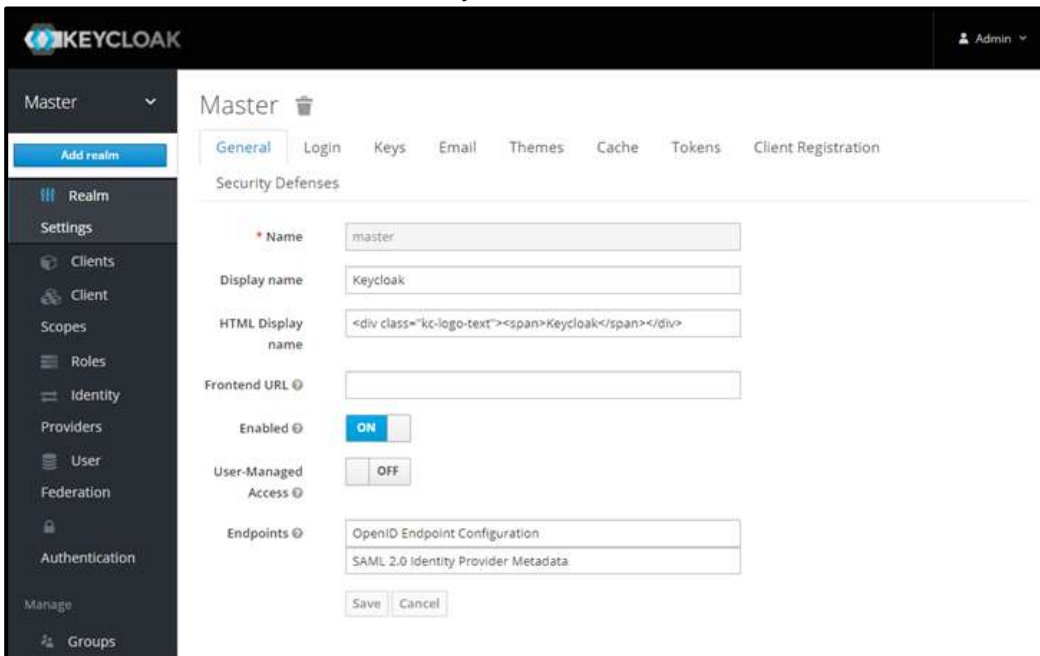
1. Login Keycloak Identity Provider portal.



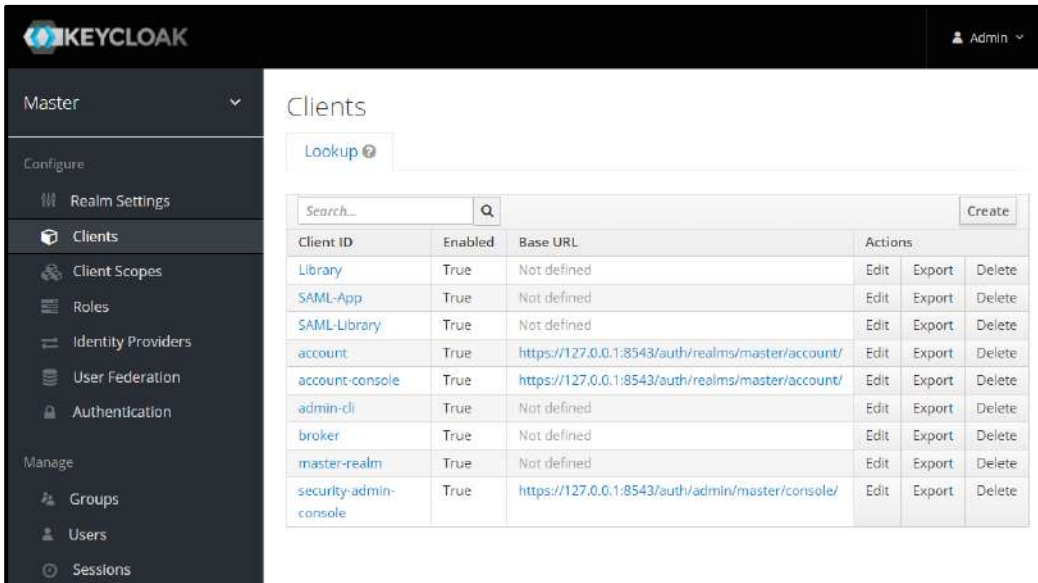
2. You are taken to the Home page. Click on Administration Console



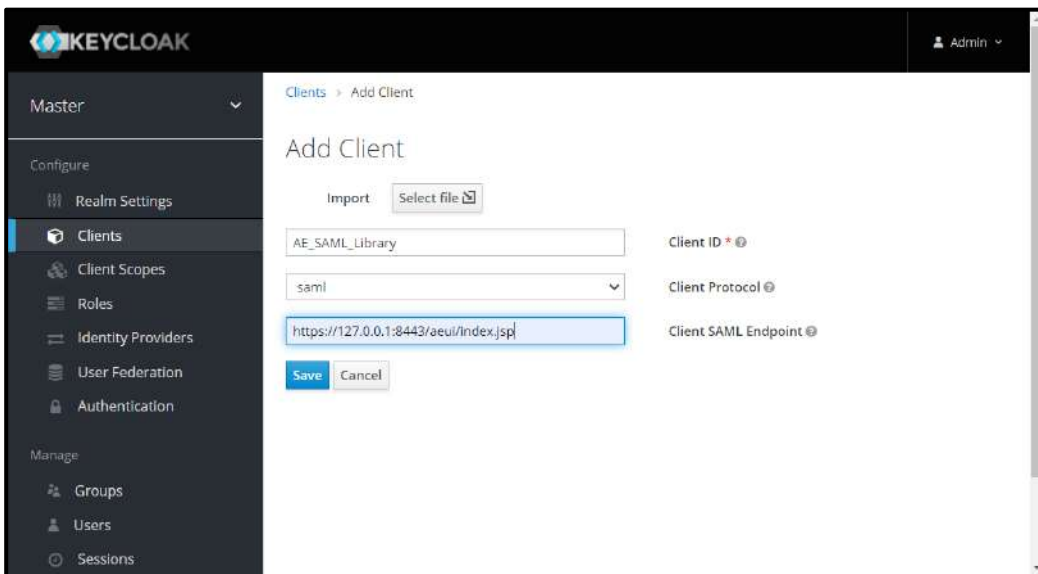
3. Add Realm if not added. We already have a Realm named master.



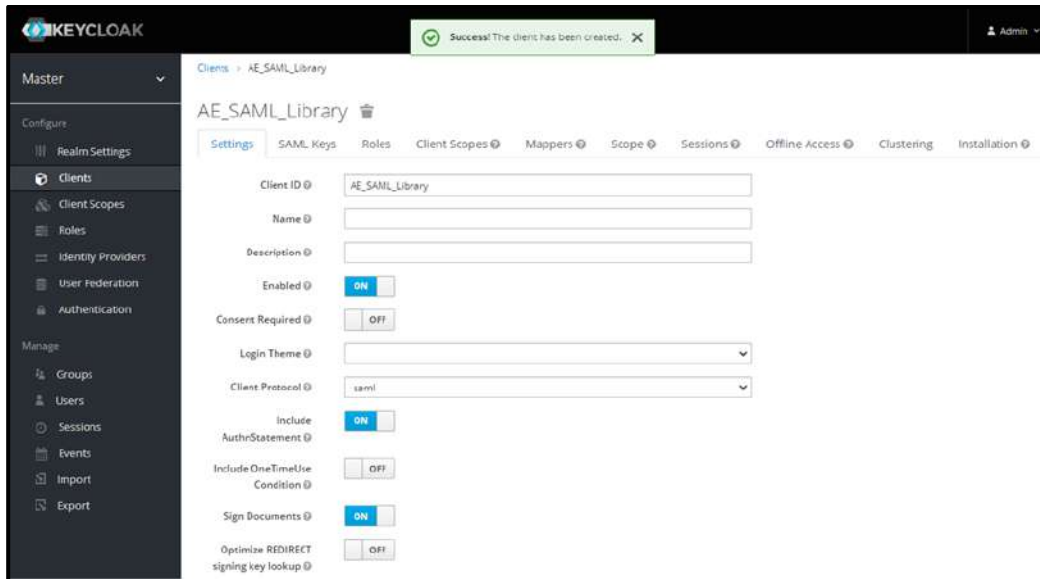
- Go to the “Clients” section and click the Create button.



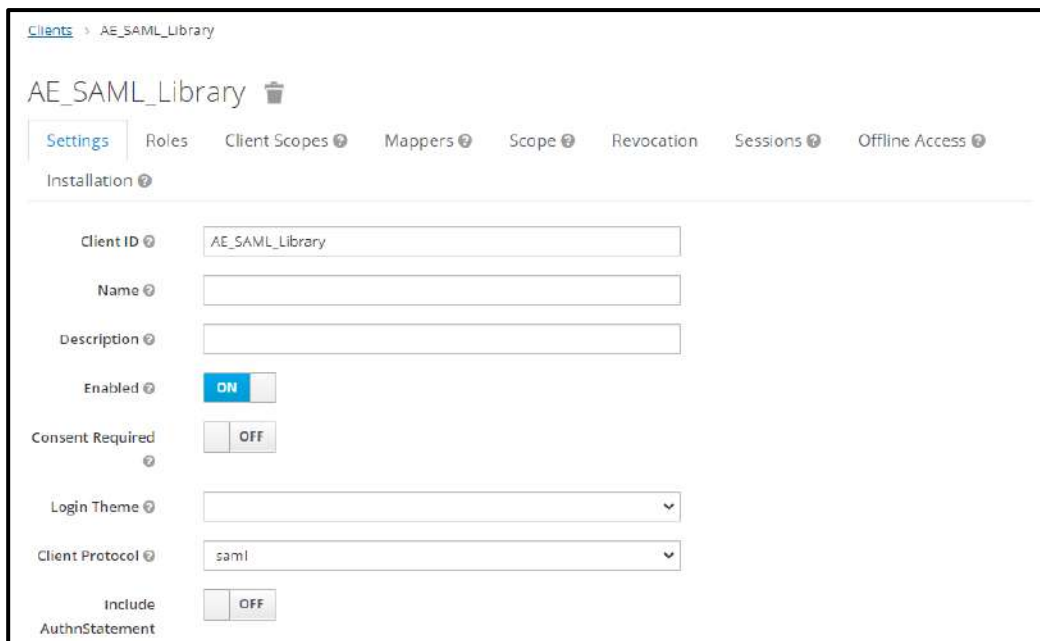
- Give a name to the Client - “AE_SAML_Library”.
- Select appropriate Client Protocol in this case SAML.
- Set Client SAML Endpoint (valid redirect URIs) as https://<aeui-server>:{Port}/aeui/index.jsp.
- Click Save.



9. The Client has been created message appears.



10. You are taken to the page with more Settings.
11. You may change the configurations as in the below screens.
12. Click Save.



Include OneTimeUse Condition ⓘ	<input type="checkbox"/> OFF
Sign Documents ⓘ	<input checked="" type="checkbox"/> ON
Optimize REDIRECT signing key lookup ⓘ	<input type="checkbox"/> OFF
Sign Assertions ⓘ	<input type="checkbox"/> OFF
Signature Algorithm ⓘ	<input type="text" value="RSA_SHA256"/>
SAML Signature Key Name ⓘ	<input type="text" value="NONE"/>
Canonicalization Method ⓘ	<input type="text" value="EXCLUSIVE"/>
Encrypt Assertions ⓘ	<input type="checkbox"/> OFF
Client Signature Required ⓘ	<input type="checkbox"/> OFF
Force POST Binding ⓘ	<input type="checkbox"/> OFF

Front Channel Logout ⓘ	<input type="checkbox"/> OFF
Force Name ID Format ⓘ	<input type="checkbox"/> OFF
Name ID Format ⓘ	<input type="text" value="transient"/>
Root URL ⓘ	<input type="text"/>
Valid Redirect URIs ⓘ	<input type="text" value="https://127.0.0.1:8443/aeui/index.jsp"/> <input type="button" value="-"/> <input type="button" value="+"/>
Base URL ⓘ	<input type="text"/>
Master SAML Processing URL ⓘ	<input type="text"/>
IDP Initiated SSO URL Name ⓘ	<input type="text"/>
IDP Initiated SSO Relay State ⓘ	<input type="text"/>

▼ Fine Grain SAML Endpoint Configuration ?

Assertion Consumer Service POST Binding URL

Assertion Consumer Service Redirect Binding URL

Logout Service POST Binding URL

Logout Service Redirect Binding URL

> Advanced Settings ?

> Authentication Flow Overrides ?

The SAML App configurations to be applied are also listed in the table below.

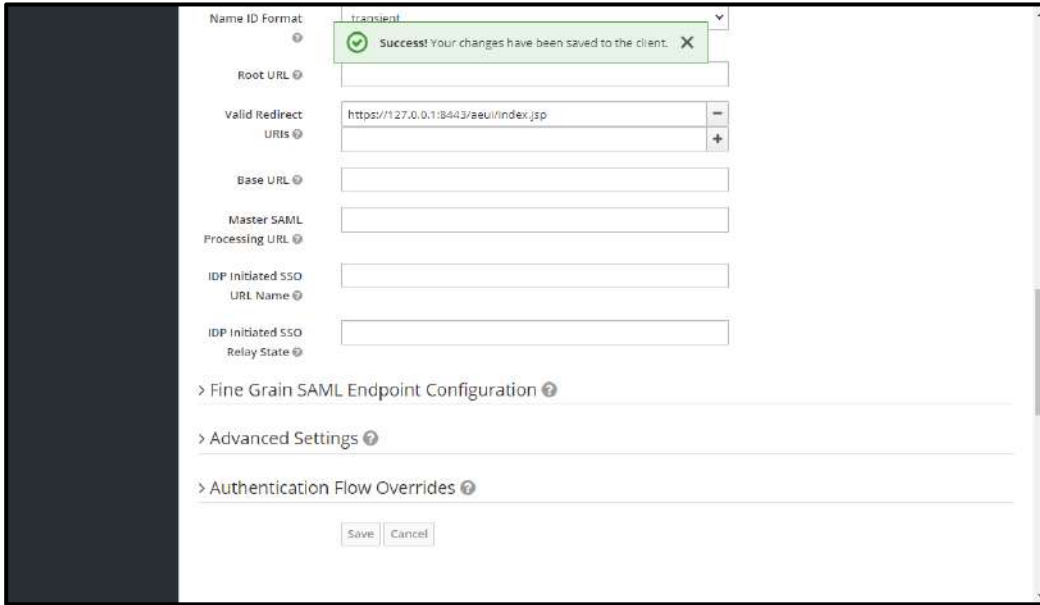
Enabled	On
Consent Required	off
Login Theme	
Client Protocol	Saml
Include AuthnStatement	off
Include OneTimeUse Condition	off
Sign Documents	On
Optimize REDIRECT signing key lookup	off
Sign Assertions	off
Signature Algorithm	RSA-SHA256
Saml Signature Key Name	None
Canonicalization Method	EXCLUSIVE
Encrypt Assertions	off
Client Signature Required	off
Force POST Binding	off
Front Channel Logout	off
Force Name ID Format	off
Name Id Format	transient
Root URL	
Valid Redirect URIs	http://<aeui-server>/aeui/index.jsp
Base URL	
Master SAML Processing URL	
IDP Initiated SSO URL Name	
IDP Initiated SSO Relay State	
Assertion Consumer Service	https://<AutomationEdgeServer/IP>:port/aeui/index.jsp

Logout Service Post Binding URL	https://AutomationEdge Server/IP:port/aeui/logout.jsp
---------------------------------	---

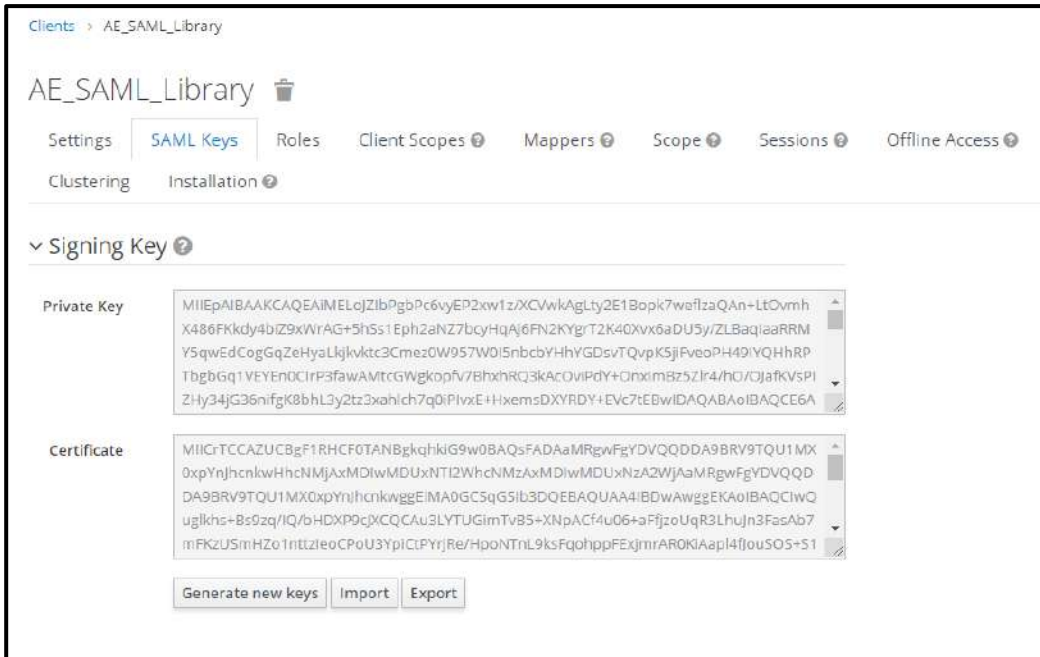
Note:

- Valid Redirect URL is used after successful login to the IDP.
- We are using post binding in our application. So the 'Assertion Consumer Service' and 'Logout service Post Binding URL' should have valid URLs. Redirect URL and Assertion Consumer Service root URL should be same.

13. Upon save a Success message appears as below.



14. Now go to the SAML Keys tab.



15. A screen appears as below.



Clients > AE_SAML_Library > SAML Keys > SAML Signing Key Import

Import SAML Key AE_SAML_Library

Archive Format  JKS

Key Alias 

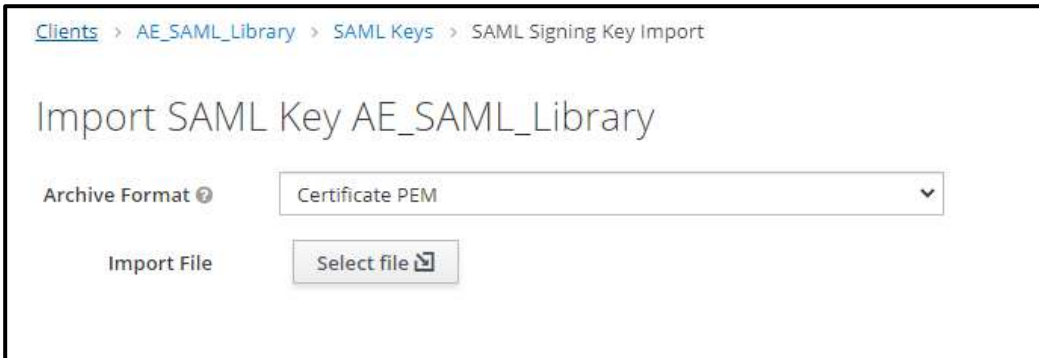
Store Password  

Import File

16. Select Archive format at Certificate PEM from the drop down list.


 **Note:** To generate Self Signed or CA Certificate refer to section [2.9 Keystore and Certificate Generation](#)

17. Click Select file to browse your certificate file.



Clients > AE_SAML_Library > SAML Keys > SAML Signing Key Import

Import SAML Key AE_SAML_Library

Archive Format  Certificate PEM

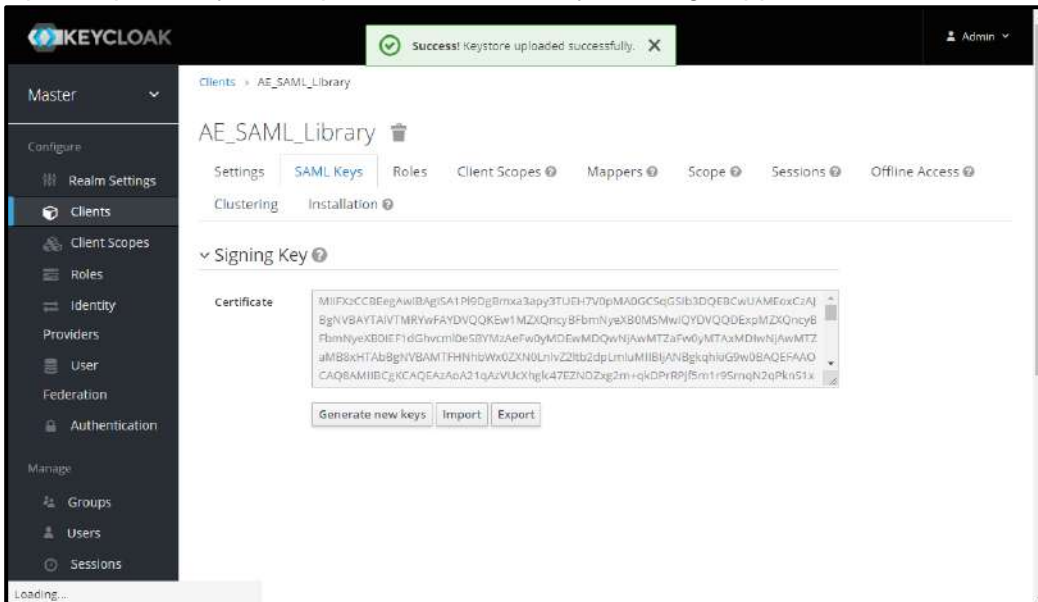
Import File

18. The screen shot below shows the browsed Certificate file.

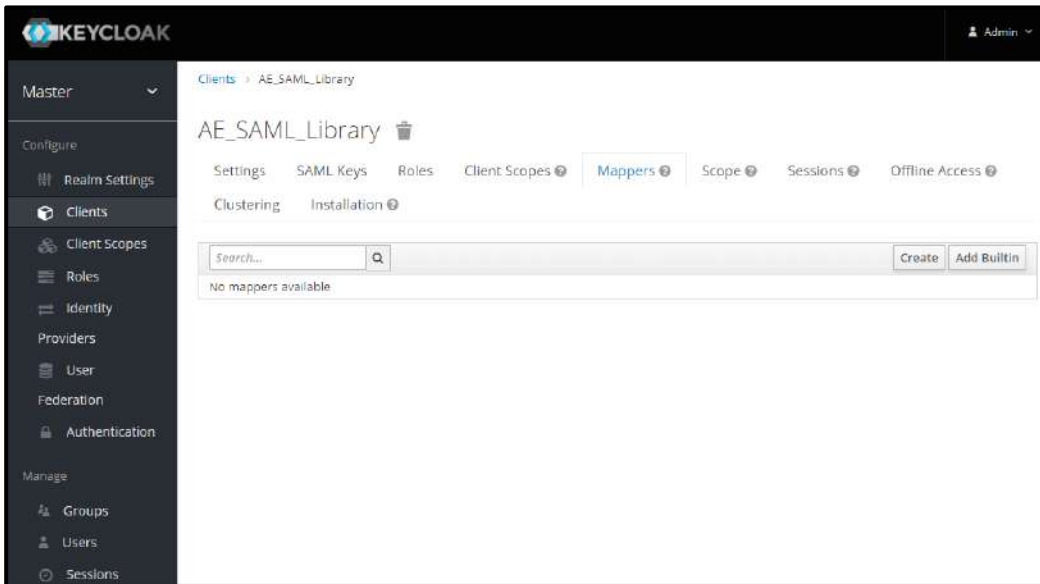
19. Click Import.



20. Upon import, Keystore uploaded successfully message appears as seen below.



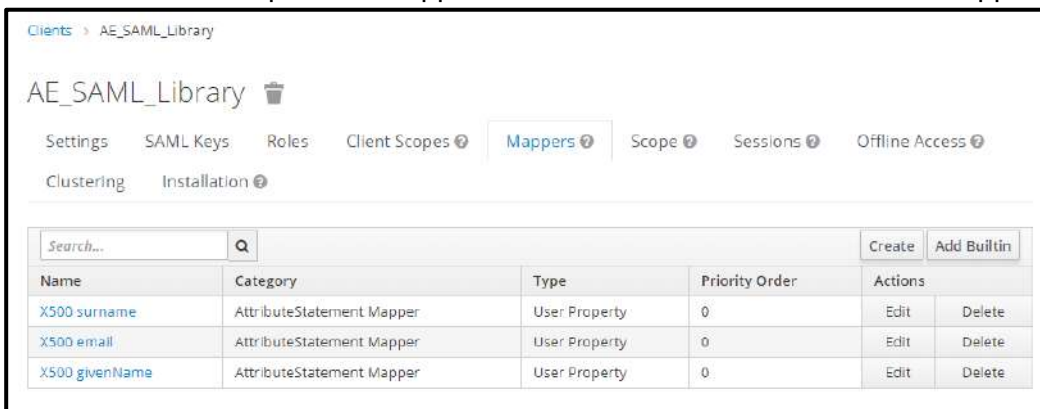
21. Next we will enable some built-in Protocol Mappers and create a new Protocol Mapper.
22. In Client menu click on the Mappers tab.
23. In the same client setting section move on to **Mapper** click on Add Builtin.



24. Include Build-in email, givenName and surname by enabling checkbox next to them.



25. The selected Builtin protocol Mapper attributes are now available under Mappers tab.



26. We got the three attribute only left with username attribute.
27. Click Create button to open the Create Protocol Mapper for creating username claim.
28. Set Name, User Attribute, Friendly Name, SAML Attribute Name as **username**. And also set Mapper Type to **User Attribute**. Next click on **Save**.

Clients > AE_SAML_Library > Mappers > Create Protocol Mappers

Create Protocol Mapper

Protocol

Name

Mapper Type

User Attribute

Friendly Name

SAML Attribute Name

SAML Attribute NameFormat

Aggregate attribute values OFF

29. The Client Protocol Mapper for username claim is successfully created.

KEYCLOAK Success! Mapper has been created. X Admin

Clients > AE_SAML_Library > Mappers > username

Username

Protocol

ID

Name

Mapper Type

User Attribute

Friendly Name

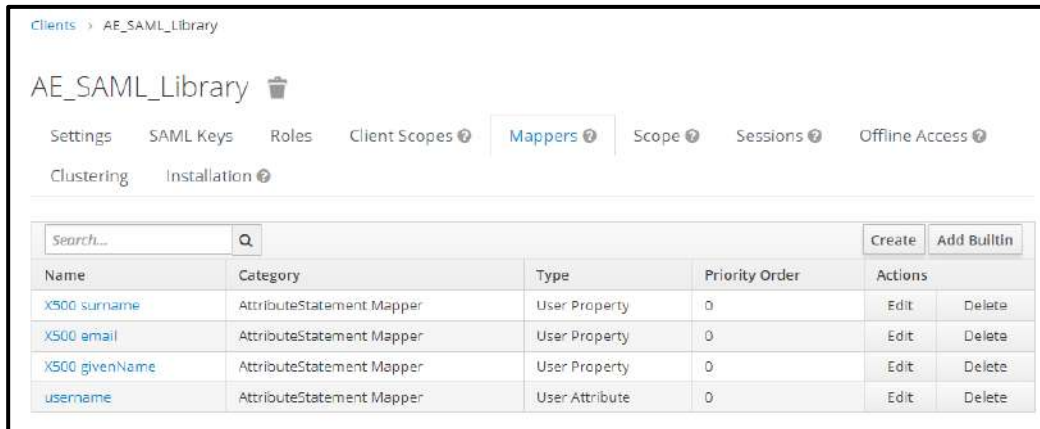
SAML Attribute Name

SAML Attribute NameFormat

Aggregate attribute values OFF

Loading...

30. The Protocol Mappers (claims) for the Client is now as seen below.

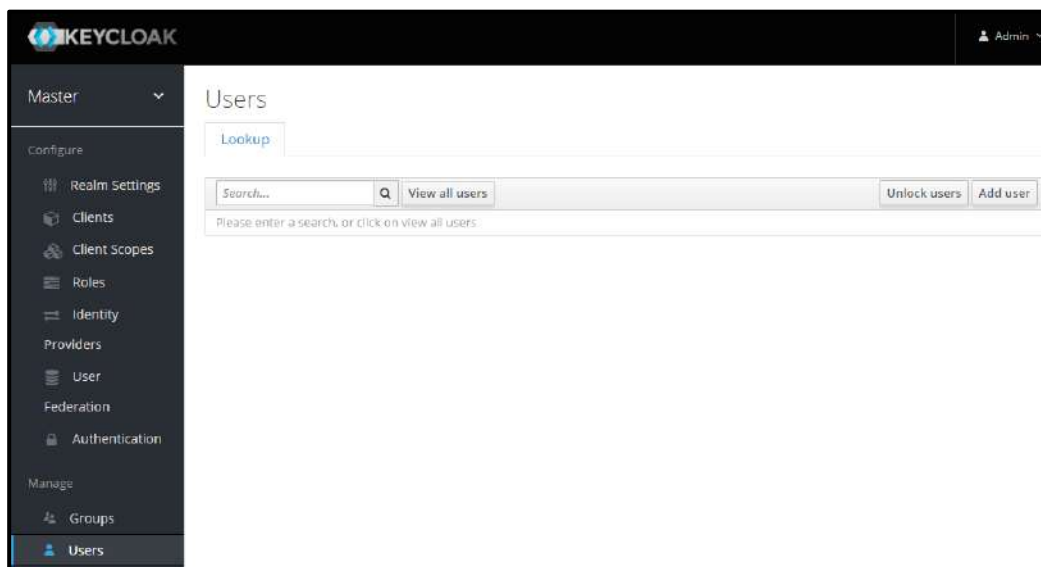


Name	Category	Type	Priority Order	Actions
X500 surname	AttributeStatement Mapper	User Property	0	Edit Delete
X500 email	AttributeStatement Mapper	User Property	0	Edit Delete
X500 givenName	AttributeStatement Mapper	User Property	0	Edit Delete
username	AttributeStatement Mapper	User Attribute	0	Edit Delete

2.6.1 Add User

If user is not added to the realm, following are the steps to view and Add new users.

1. Navigate to the Users menu in the left navigation pane.
2. Click on View all users.



3. The following is the current list of users.

Users

Lookup

Search...

ID	Username	Email	Last Name	First Name	Actions
F34e04e0-81c3-42...	admin				Edit Impersonate Delete
614bf386-9c16-47...	jane	seema.kothari@g...	Webster	Jane	Edit Impersonate Delete
4caa9ab1-abfa-41...	tom	thomas.astebro@...	Astebro	Thomas	Edit Impersonate Delete

4. Click Add User button to create a new user.

5. Specify the First Name, Last Name and Email. Configure User details as seen below.

6. Click Save.

Users > Add user

Add user

ID

Created At

Username *

Email

First Name

Last Name

User Enabled ON

Email Verified OFF

Required User

Actions

7. A user is created and an ID is generated a seen below, with a success message.

Users > anne

Anne

Details | Attributes | Credentials | Role Mappings | Groups | Consents | Sessions

ID	<input type="text" value="b3c3bcad-fc7c-446d-b962-b5d532bd4d50"/>
Created At	10/21/20 2:08:46 AM
Username	<input type="text" value="anne"/>
Email	<input type="text" value="i@gmail.com"/>
First Name	<input type="text" value="Anne"/>
Last Name	<input type="text" value="Jonas"/>
User Enabled	<input checked="" type="checkbox"/> ON
Email Verified	<input type="checkbox"/> OFF
Required User Actions	<input type="text" value="Select an action..."/>
Impersonate user	<input type="button" value="Impersonate"/>

8. To set user credentials, go to the credentials tab and choose a password. Turn off the Reset Password- “Temporary” flag unless you want the user to change password on first login.

The screenshot shows the 'Users > anne' page with the 'Credentials' tab selected. The 'Manage Credentials' table is empty. The 'Set Password' section contains two password input fields, a 'Temporary' toggle set to 'OFF', and a 'Set Password' button. The 'Credential Reset' section includes a 'Reset Actions' dropdown menu, an 'Expires In' field set to '12 Hours', and a 'Send email' button.

9. Now we will set the Protocol Mapper user attributes, provided in the table below for this user.

Key	Value
username	{{username}}
firstName	{{firstname}}
lastName	{{lastname}}
emailAddress	{{email}}

- Click Attributes tab to add the following four attributes for the user. Provide the actual values in the Value field.

Key	Value	Actions
emailAddress	@gmail.com	Delete
firstName	Anne	Delete
lastName	Jonas	Delete
username	anne	Delete
		Add

Save Cancel

Note: It is **mandatory** to specify actual values for the first 3 attributes: uniqueId, firstName and lastName

2.6.2 Fetch parameters for AutomationEdge SSO Settings

- Next, we wish to fetch the Client ID, Redirect URLs. Click on the Clients link the left Navigation menu. Click on the Client link in the list (in this case AE_SAML_Library). Get the Client ID.
- Get the Valid Redirect URLs by scrolling further down.
- Navigate to the Realm Settings. Click on SAML 2.0 Identity Provider Metadata.

KEYCLOAK Admin

Master

Configure: General, Login, Keys, Email, Themes, Cache, Tokens, Client Registration, Security Defenses

Realm Settings

Name: master

Display name: Keycloak

HTML Display name: <div class="kc-logo-text">Keycloak</div>

Frontend URL

Enabled: ON

User-Managed Access: OFF

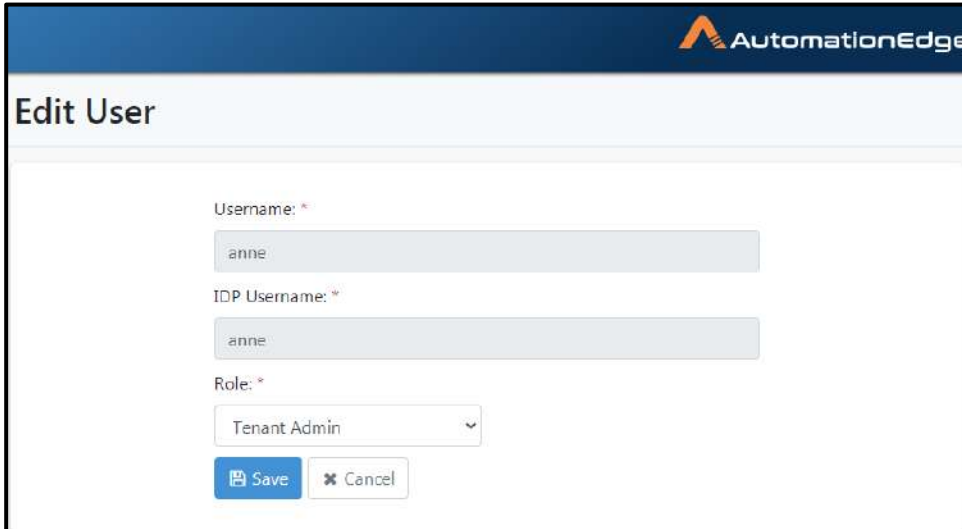
Endpoints: OpenID Endpoint Configuration, SAML 2.0 Identity Provider Metadata

Save Cancel

https://127.0.0.1:8543/auth/realms/master/protocol/saml/descriptor

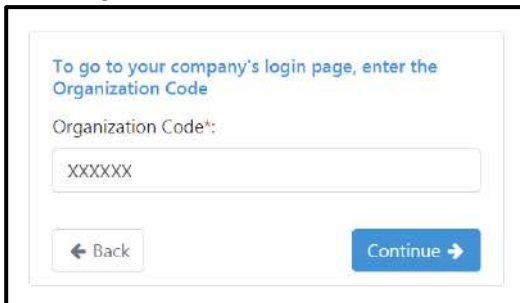
@ Note: To generate Keystore as well as Self Signed or CA Certificate refer to section [2.9 Keystore and Certificate Generation](#)

8. Create an SSO user in AutomationEdge UI. The username should be mapped to a unique IDP user.

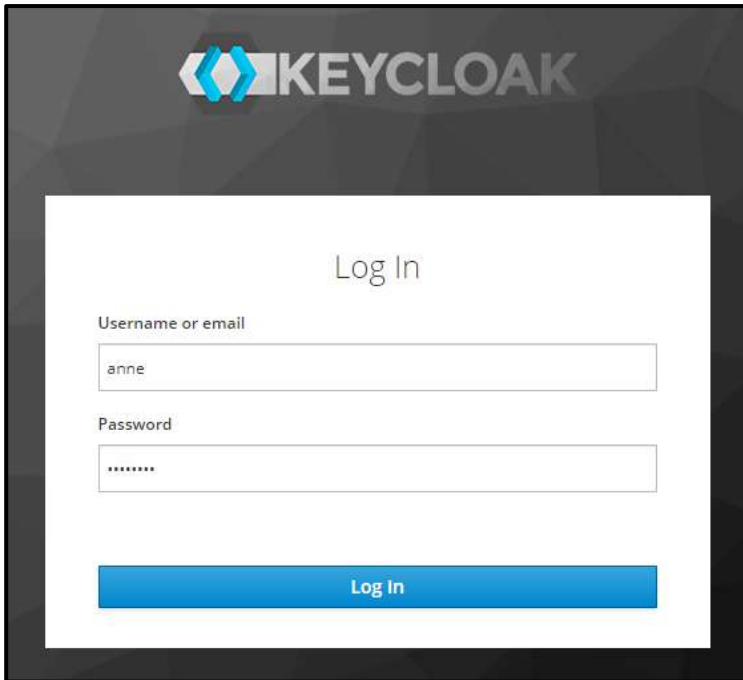


2.6.3 AE initiated SSO

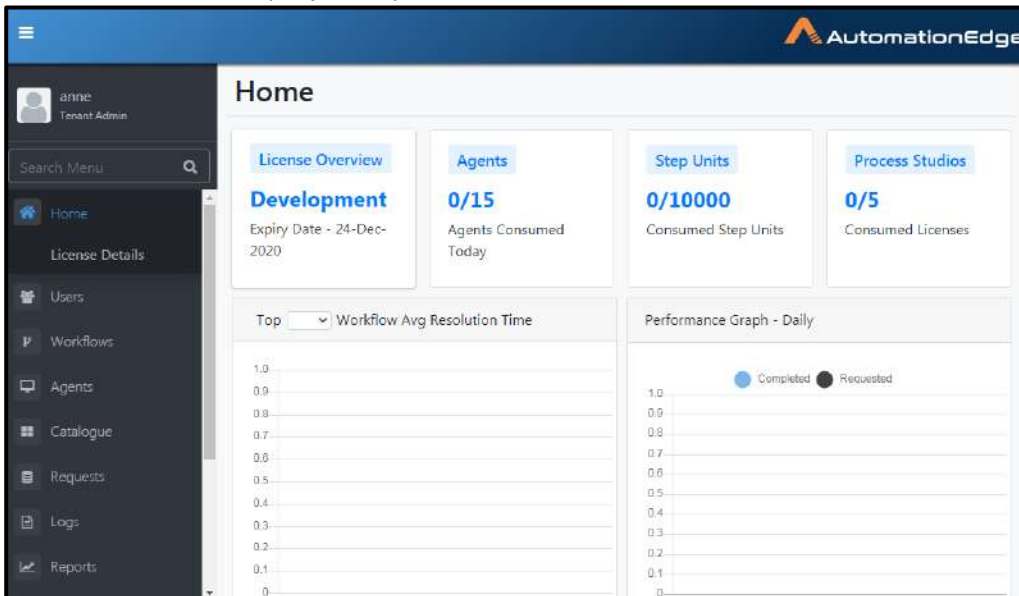
1. Now Sign In with SSO link on AutomationEdge UI. Provide the Organization Code.



2. The first time you try to login with SSO, you are redirected to the Keycloak login page (Make sure you login with the right user).
3. In case you are already logged with another user you need to first logout and login with this user.



4. You logged in to AutomationEdge. Note that the user logged in is the same as the uniqueid of the IDP (Keycloak) user 'tom'.



5. This completes the process of configuring Keycloak and AutomationEdge for SSO using OpenID Connect protocol for Web applications.

2.7 AE initiated SSO with ADFS using OAuth/OpenID

ADFS Identity Provider supports OAuth 2.0/ OpenID Connect and SAML protocols.

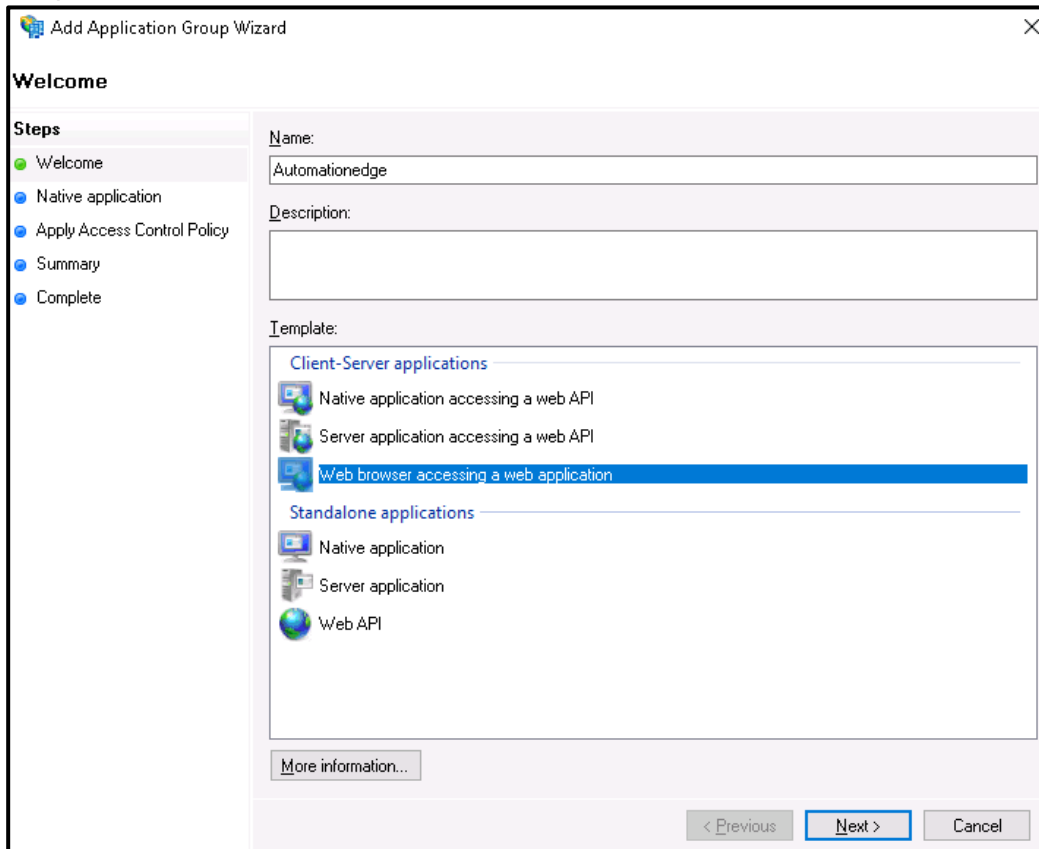
In this section we demonstrate some key configurations to setup ADFS and fetch the required parameters for AutomationEdge SSO.

- Identity Provider Issuer
- Identity Provider Endpoints (Authorization, Token & End Session Endpoints)
- Login redirect URIs
- Client ID

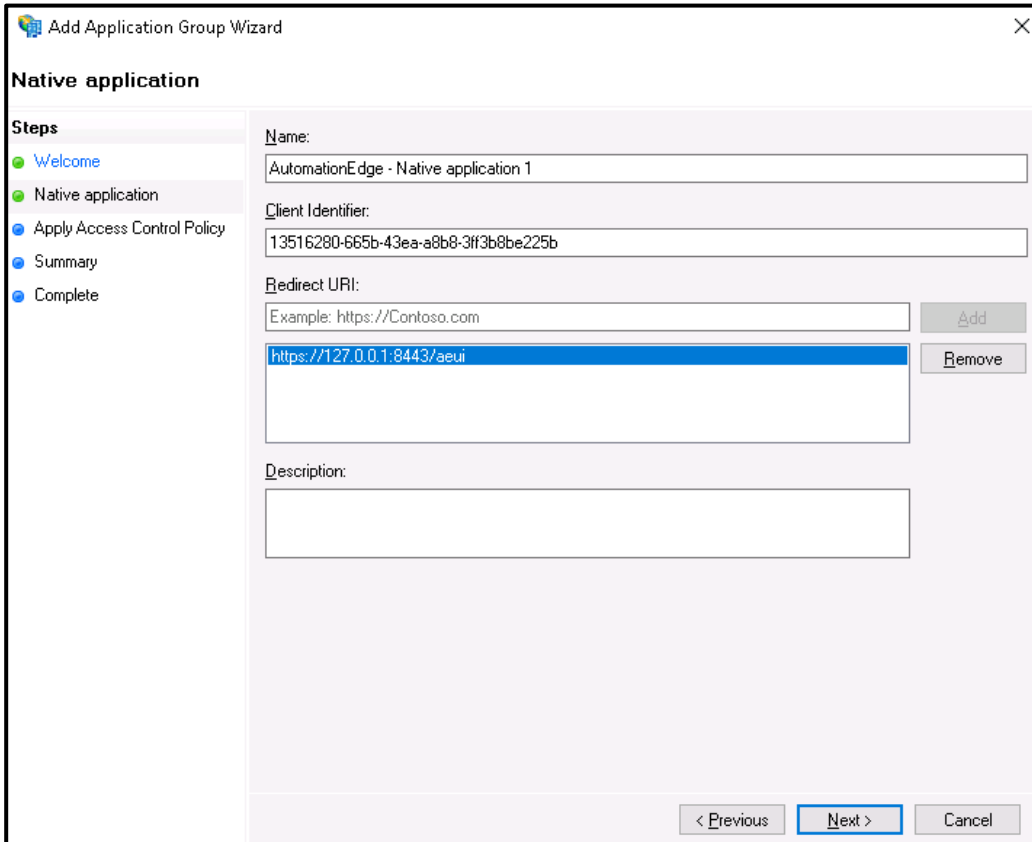
1. Open ADFS console and go to Application Group. Click on Add Application Group.



2. Type a Name for a new Application Group. We shall provide the name 'Automationedge'.
3. Select Web browser accessing a web application as the Client-Server application template.



4. Add Application Group Wizard starts.
5. In the Welcome step a new Client Identifier (to be used for Client ID in AutomationEdge SSO configuration) is generated. You may change it, but it is not necessary. Copy the Client Identifier.
6. In the Redirect URI section, add all the URLs for AutomationEdge as the client application.
7. Click Next.

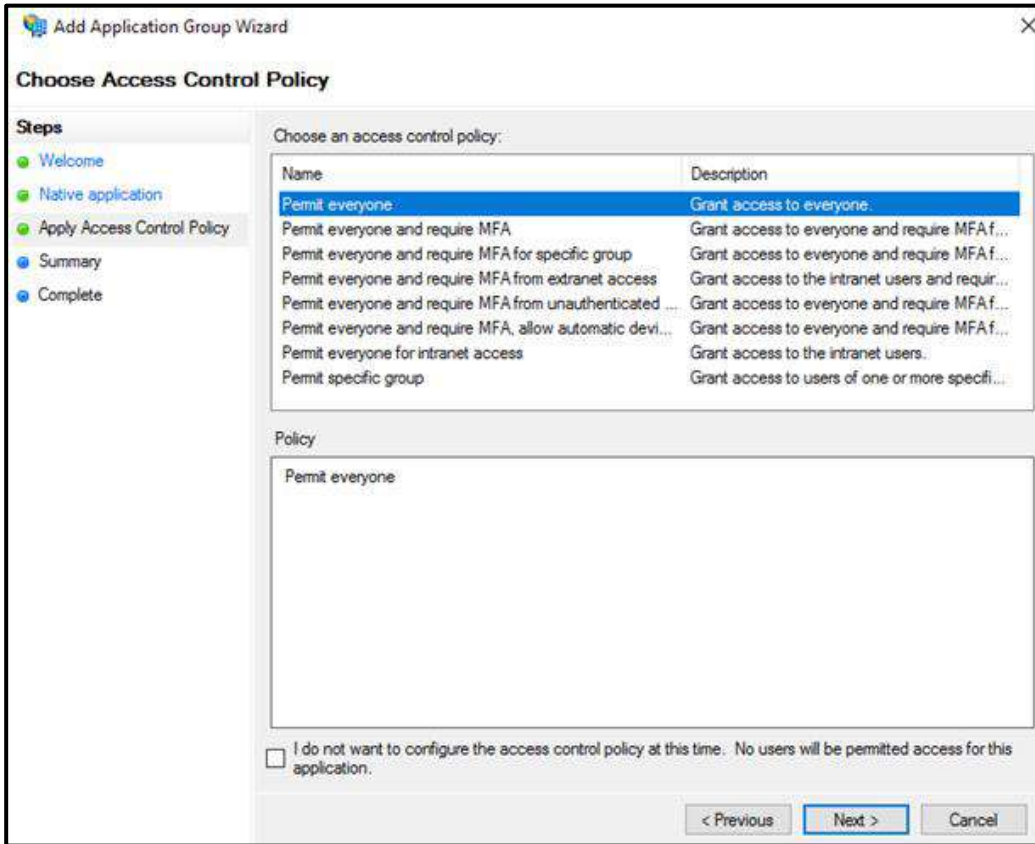


The screenshot shows the 'Add Application Group Wizard' dialog box, specifically the 'Native application' step. The dialog has a title bar with a close button (X) and a 'Steps' sidebar on the left. The 'Steps' sidebar lists: Welcome (selected), Native application (current), Apply Access Control Policy, Summary, and Complete. The main area contains the following fields:

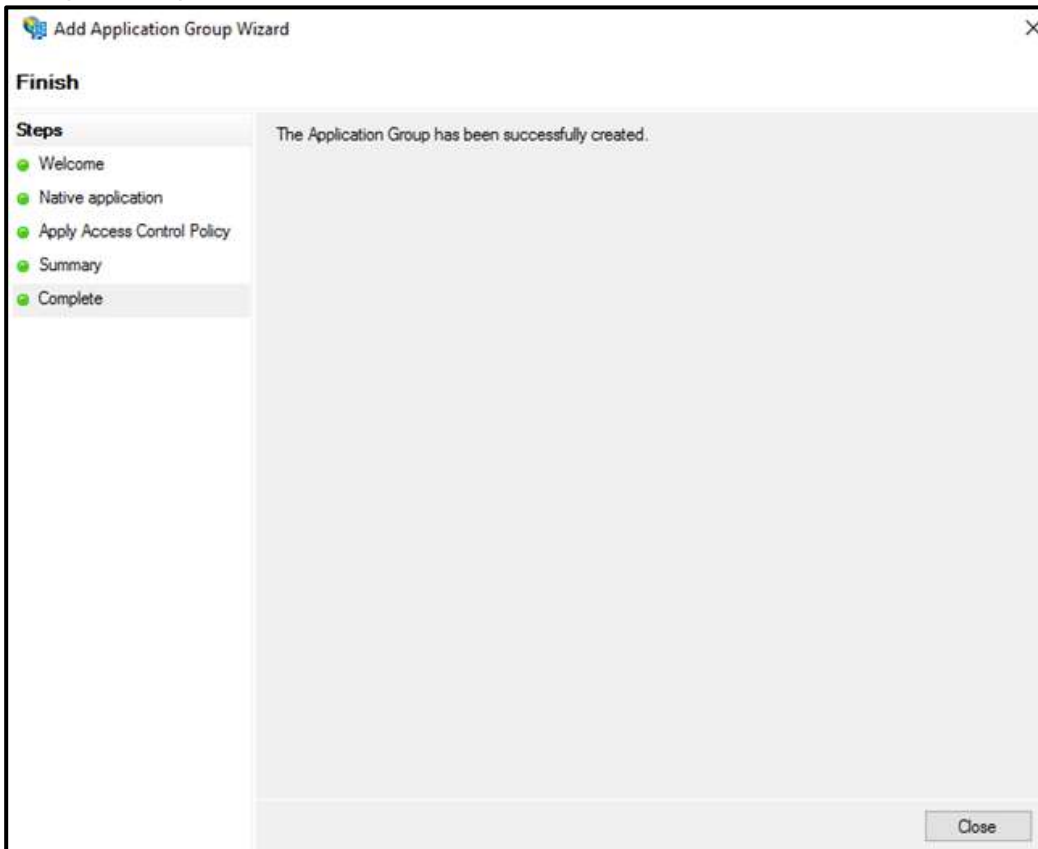
- Name:** AutomationEdge - Native application 1
- Client Identifier:** 13516280-665b-43ea-a8b8-3f3b8be225b
- Redirect URI:** A list of URIs. The first is 'https://127.0.0.1:8443/aeui', which is highlighted in blue. There are 'Add' and 'Remove' buttons next to the list.
- Description:** An empty text box.

At the bottom of the dialog, there are three buttons: '< Previous', 'Next >' (highlighted), and 'Cancel'.

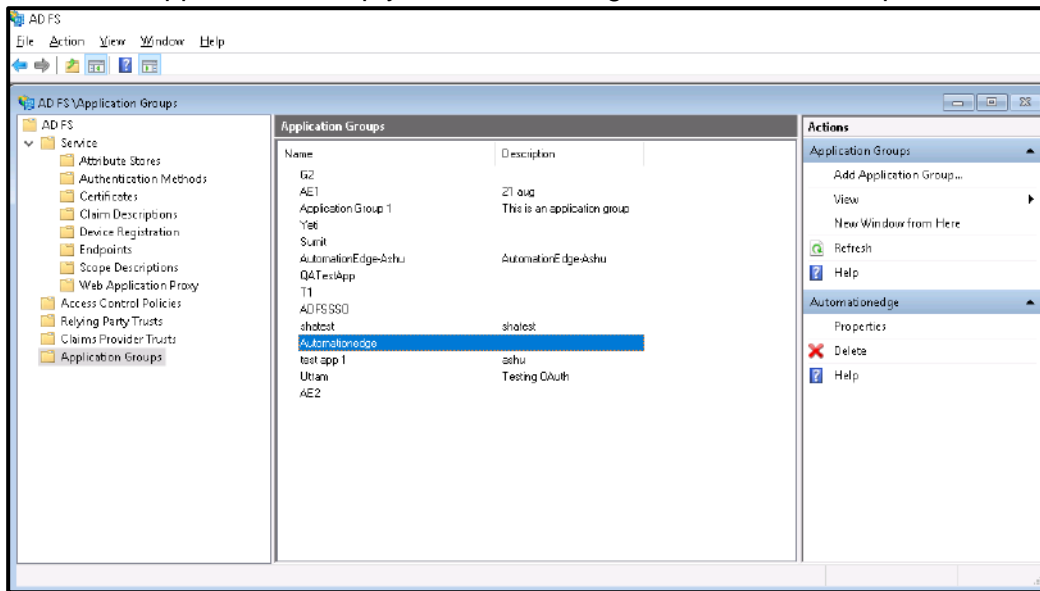
8. In the Apply Access Control policy step Permit everyone option is selected but you may select as per need. Click Next.



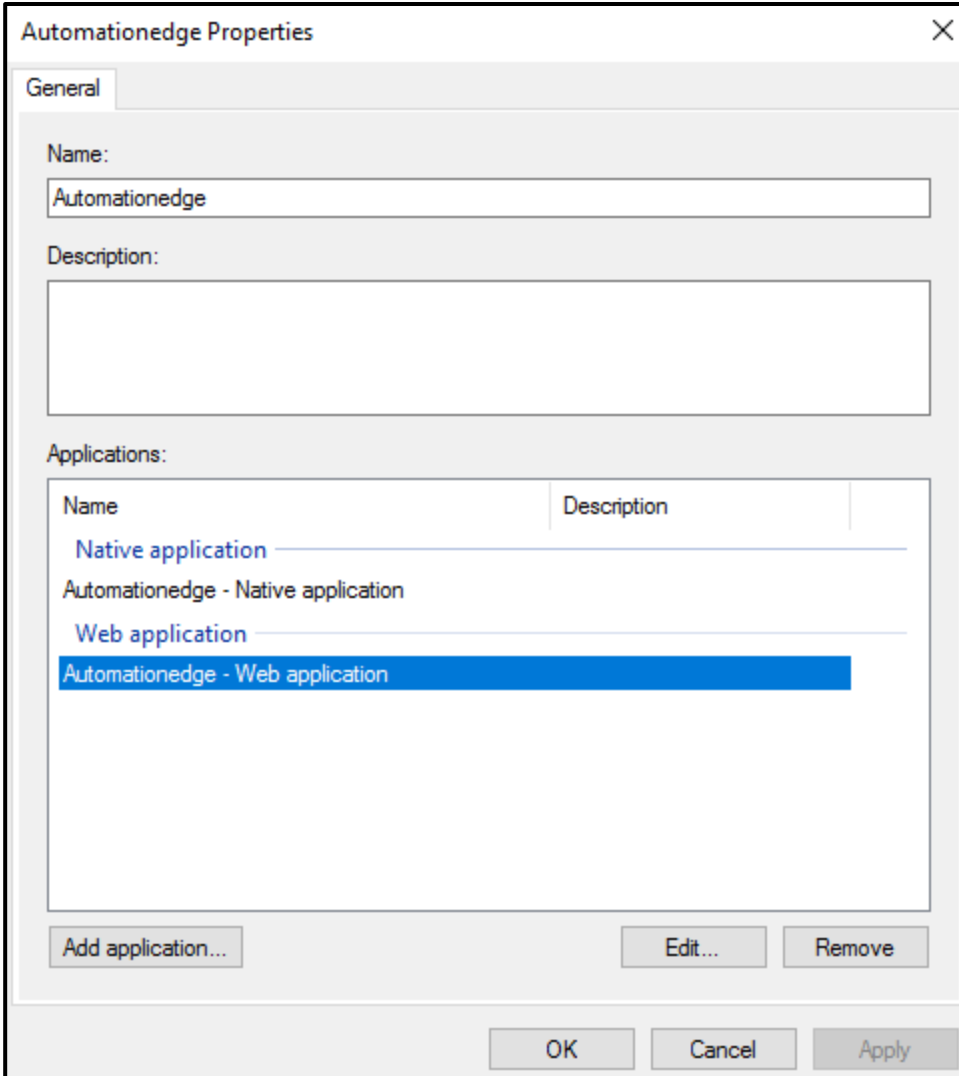
9. Review settings in the Summary step and click Next button.
10. The Application Group has been successfully created message can be seen in the Complete step. Click Close.



11. You can now see the ADFS console.
12. The new Application Group is now listed in the Application Groups interface where once there were no Application Groups.
13. Select the Application Group you want to configure and click on Properties.



14. The newly created Application Group's Properties window opens. The two Applications for Client Application and Server have been created by the Application Group creation Wizard.
15. Now select the 'Automationedge' Web Application as seen below for additional configurations. Click Edit.



Automationedge Properties

General

Name:
Automationedge

Description:

Applications:

Name	Description
Native application	Automationedge - Native application
Web application	Automationedge - Web application

Add application... Edit... Remove

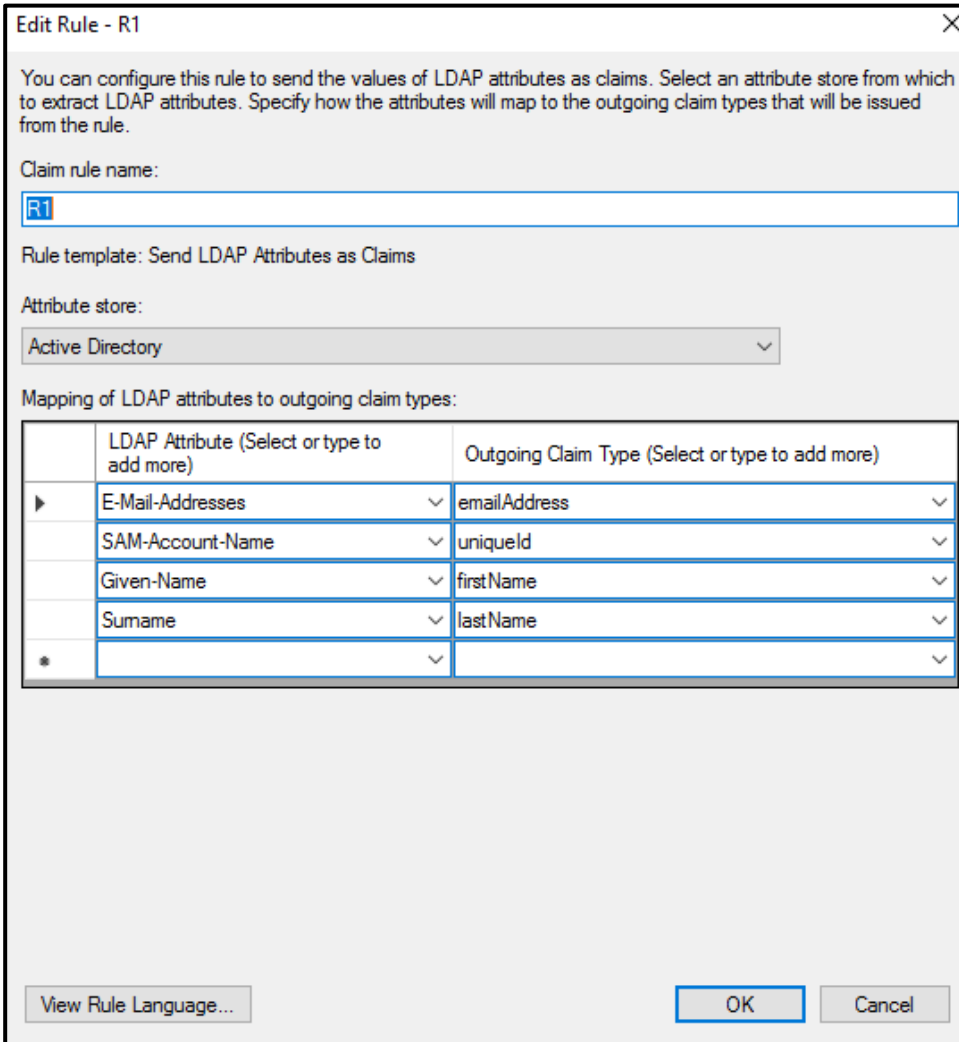
OK Cancel Apply

16. Add Claims for the Access Token.
17. Keep the Notes and Access control policy tab as they are.
18. Go to the Issuance Transform Rules tab which is empty! Once you see the windows like in the snapshot below, click the Add Rule button. Select the 'Send LDAP Attributes as Claims'. Add the LDAP Attributes as mentioned in the table below.

LDAP Attribute	Outgoing Claim Type –case sensitive
E-Mail-Addresses	emailAddress
SAM-Account-Name	uniqueId
Given-Name	firstName
Surname	lastName

 **Note:** It is **mandatory** to map LDAP attributes to the three outgoing claim types - uniqueId, firstName and lastName

19. Click Next.



Edit Rule - R1

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Rule template: Send LDAP Attributes as Claims

Attribute store:

Mapping of LDAP attributes to outgoing claim types:

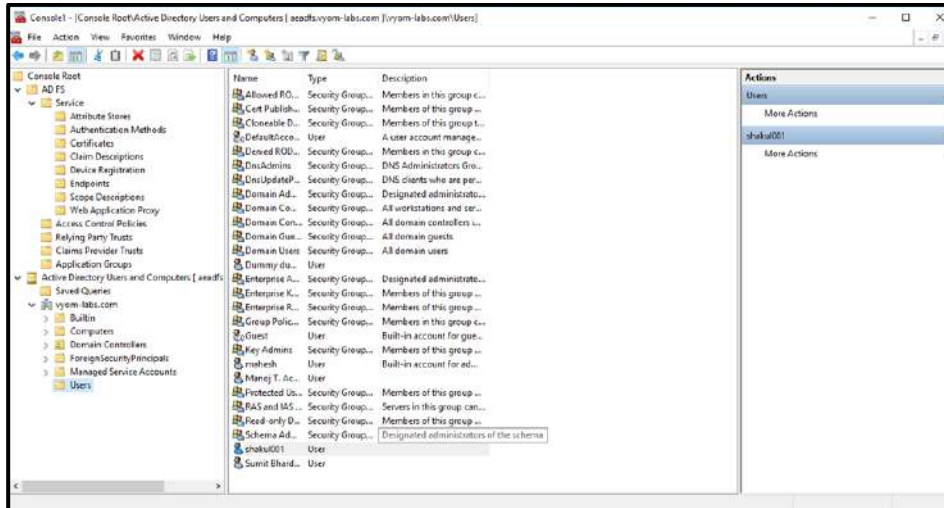
	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	E-Mail-Addresses	emailAddress
	SAM-Account-Name	uniqueId
	Given-Name	firstName
	Surname	lastName
*		

20. For AutomationEdge Web Application Configurations, finally, click on Client Permissions.

In our case we have selected the three scopes below:

- OpenID: request use of the OpenID Connect authorization protocol;

21. After selecting Client Permissions, click OK button.
22. Next add a user in ADFS server Active Directory. Following are the steps for Adding new user in ADFS server Active Directory.
 - In the ADFS console click on Active Directory Users and Computer s
 - Navigate to Organization -> User-> New -> User



- Provide details of the user to be created.

The screenshot shows the 'New Object - User' dialog box. The 'Create in:' field is set to 'vyom-labs.com/Users'. The 'First name' field contains 'shaku001', the 'Last name' field is empty, and the 'Full name' field contains 'shaku001'. The 'User logon name' field contains 'shaku001' and the domain dropdown is set to '@vyom-labs.com'. The 'User logon name (pre-Windows 2000):' field contains 'VYOM-LABS\' and 'shaku001'. The 'Next >' button is highlighted.

6. Once the user is created to fetch the Identity Provider Endpoints (Authorization, Token and End Session Endpoints) in ADFS follow the steps below,
 - Open Windows Power Shell and type the command: Get-AdfsEndpoint
 - Search for OpenID Connect Discovery.

```

Administrator: Windows PowerShell
Protocol           : Device Registration
SecurityMode       : Transport
AddressPath        : /EnrollmentServer/
Version            : default

ClientCredentialType : Anonymous
Enabled            : True
FullUrl            : https://[redacted]adfs/.well-known/openid-configuration
Proxy              : True
Protocol           : OpenID Connect Discovery
SecurityMode       : Transport
AddressPath        : /adfs/.well-known/openid-configuration
Version            : default
  
```

- Copy the Full URL (e.g. https://xxxxx.com/adfs/.well-known/openid-configuration)
- Open the URL to get the Endpoints text in JSON format as seen in the snapshot below.

```

{"issuer": "https://vyom-labs.com/adfs", "authorization_endpoint": "https://vyom-labs.com/adfs/oauth2/authorize/", "token_endpoint": "https://vyom-labs.com/adfs/oauth2/token/", "jwks_uri": "https://vyom-labs.com/adfs/discovery/keys", "token_endpoint_auth_methods_supported": ["client_secret_post", "client_secret_basic", "private_key_jwt", "windows_client_authentication"], "response_types_supported": ["code", "id_token", "code id_token", "id_token token", "code token", "code id_token token"], "response_modes_supported": ["query", "fragment", "form_post"], "grant_types_supported": ["authorization_code", "refresh_token", "client_credentials", "urn:ietf:params:oauth:grant-type:jwt-bearer", "implicit", "password", "srv_challenge", "urn:ietf:params:oauth:grant-type:device_code", "device_code"], "subject_types_supported": ["pairwise"], "scopes_supported": ["openid", "logon_cert", "user_impersonation", "allatclaims", "aza", "offline_access", "email", "vpn_cert", "winhello_cert", "profile"], "id_token_signing_alg_values_supported": ["RS256"], "token_endpoint_auth_signing_alg_values_supported": ["RS256"], "access_token_issuer": "http://vyom-labs.com/adfs/services/trust", "claims_supported": ["aud", "iss", "iat", "exp", "auth_time", "nonce", "at_hash", "c_hash", "sub", "upn", "unique_name", "pwd_url", "pwd_exp", "mfa_auth_time", "sid"], "microsoft_multi_refresh_token": true, "userinfo_endpoint": "https://vyom-labs.com/adfs/userinfo", "capabilities": [], "end_session_endpoint": "https://vyom-labs.com/adfs/oauth2/logout", "as_access_token_token_binding_supported": true, "as_refresh_token_token_binding_supported": true, "resource_access_token_token_binding_supported": true, "op_id_token_token_binding_supported": true, "rp_id_token_token_binding_supported": true, "frontchannel_logout_supported": true, "frontchannel_logout_session_supported": true, "device_authorization_endpoint": "https://vyom-labs.com/adfs/oauth2/devicecode"}
  
```

23. This completes ADFS configurations and fetching desired parameters for AutomationEdge SSO.
24. You may now create an AutomationEdge SSO user mapped to the newly created user in ADFS Windows server Active Directory for AutomationEdge initiated Single Sign-On.

2.8 AE initiated SSO with ADFS using SAML

ADFS Identity Provider supports OAuth2.0/OpenID Connect and SAML protocols.

In this section we demonstrate configurations to setup AutomationEdge SSO with ADFS using SAML protocol.

We will also showcase how to get the required parameters for AutomationEdge – Keycloak Single Sign-On Settings.

The following parameters are obtained from IDP configuration,

- Identity Provider Metadata (store in descriptor.xml)
- Client ID
- Redirect URIs

Additionally, for IDP SSO configurations we need,

- Keystore file, Keystore Alias, Keystore Password

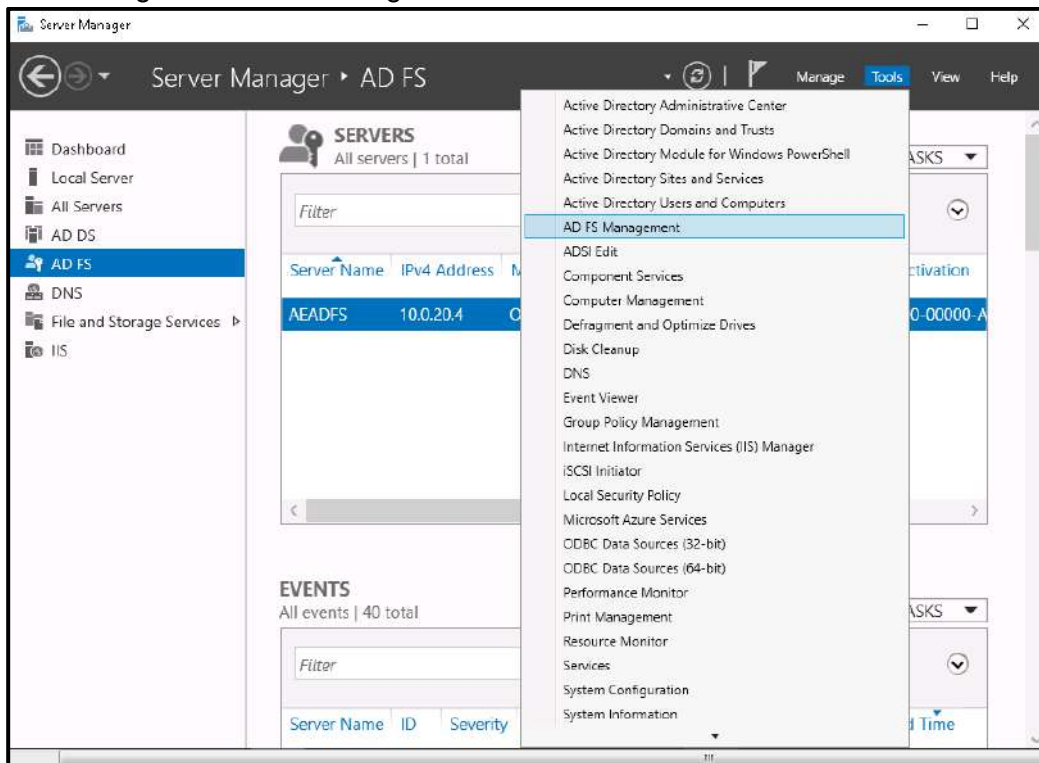
Additionally, for IDP SSO configurations we need,

- Certificate file (.crt)

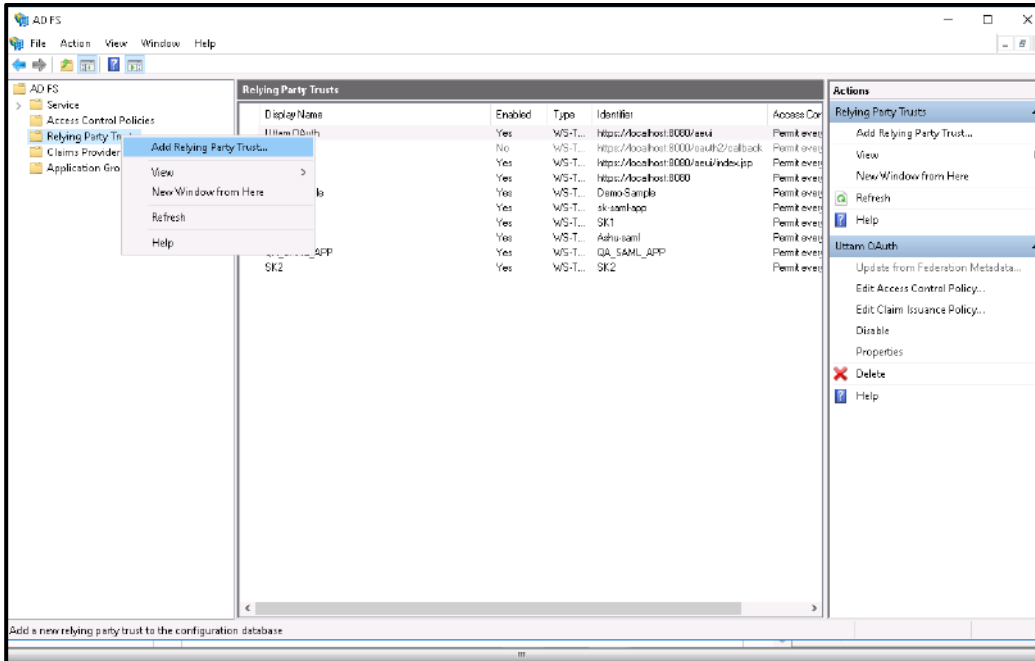
Note: For Keystore and Certificate; to generate Self Signed or CA Certificate refer to section [2.9 Keystore and Certificate Generation](#)

Follow the steps below to configure ADFS for SAML,

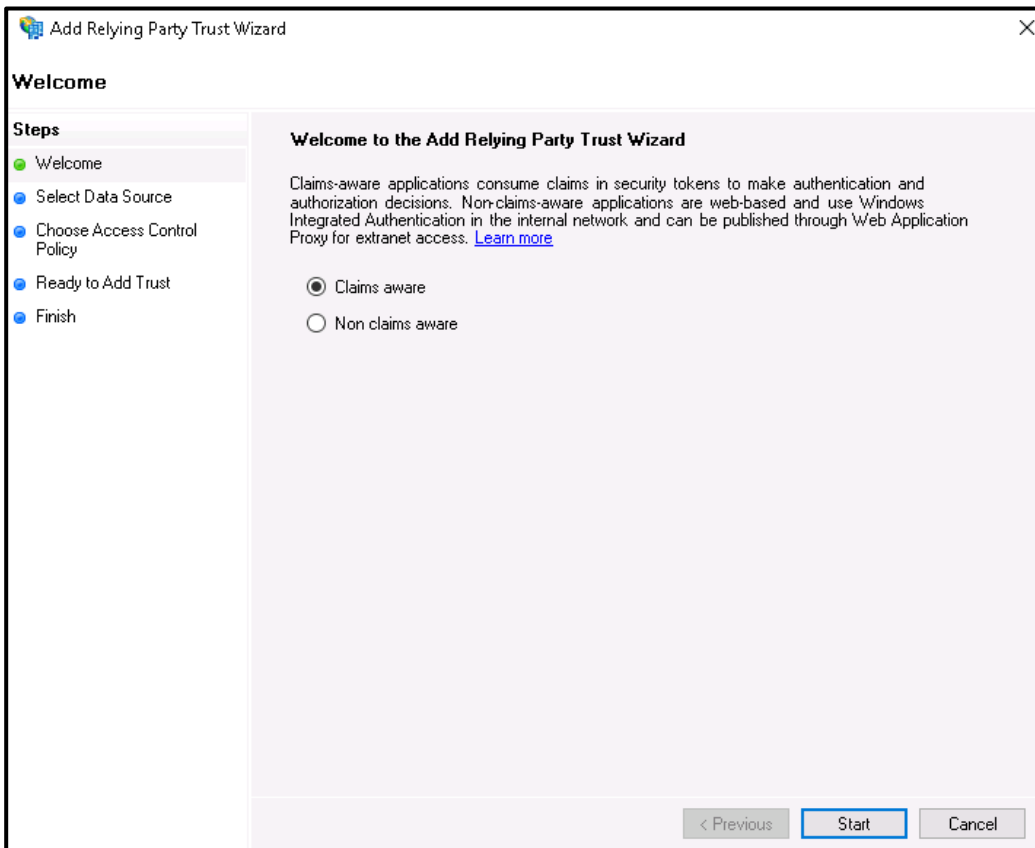
1. In Window Server 2016 go for Server Manager Section and look out for Tools tab. In the Tools tab go for AD FS Management.



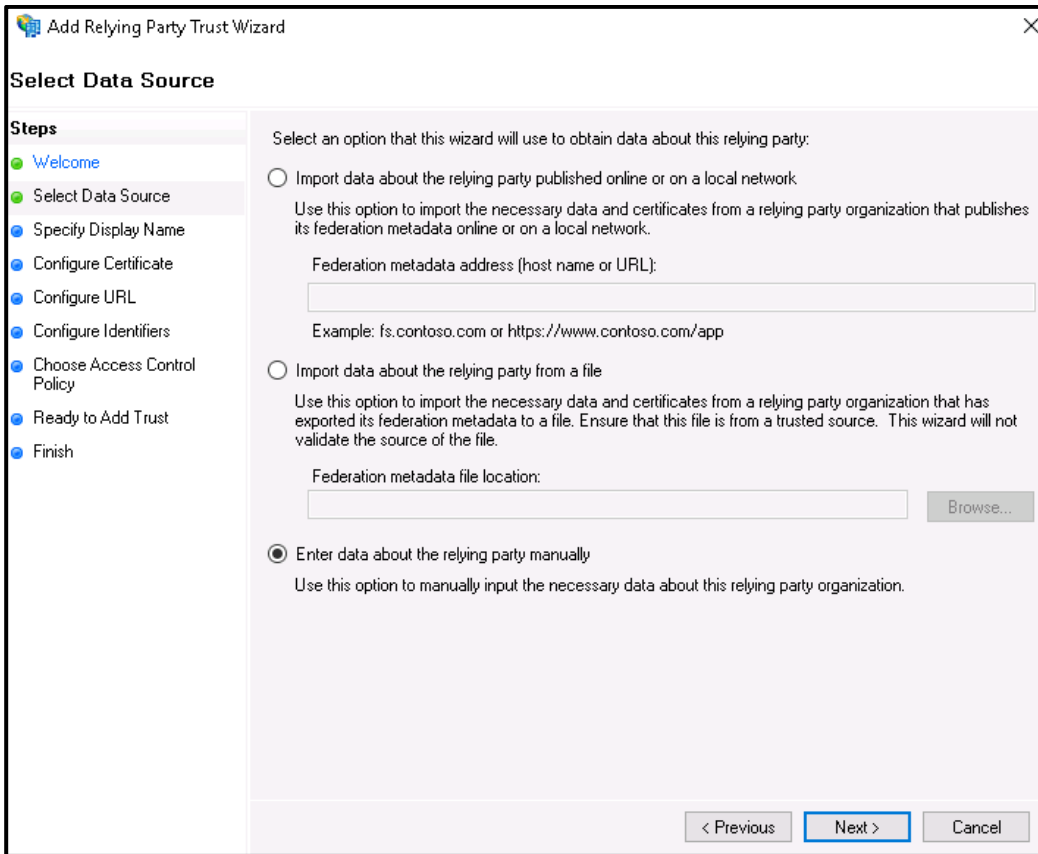
2. Look out for Relying Party Trusts and go for add party trust



3. Make sure u check on Claims Aware and click on next



4. In the next section click on Enter data about the relying party manually and click on next.

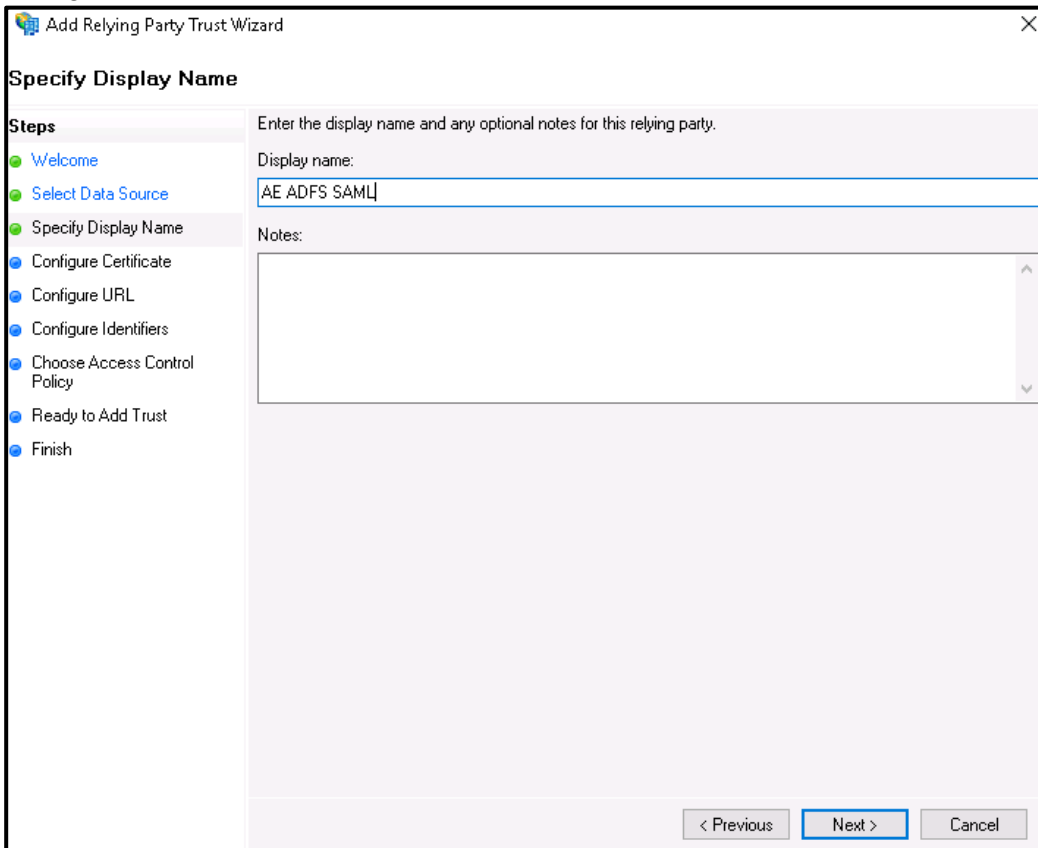


The screenshot shows the 'Add Relying Party Trust Wizard' dialog box, specifically the 'Select Data Source' step. The dialog has a title bar with a close button (X) and a 'Steps' list on the left. The 'Steps' list includes: Welcome, Select Data Source (highlighted), Specify Display Name, Configure Certificate, Configure URL, Configure Identifiers, Choose Access Control Policy, Ready to Add Trust, and Finish. The main area contains three radio button options for selecting data source information:

- Import data about the relying party published online or on a local network. Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network. Federation metadata address (host name or URL): [text box]. Example: fs.contoso.com or https://www.contoso.com/app
- Import data about the relying party from a file. Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file. Federation metadata file location: [text box] [Browse...]
- Enter data about the relying party manually. Use this option to manually input the necessary data about this relying party organization.

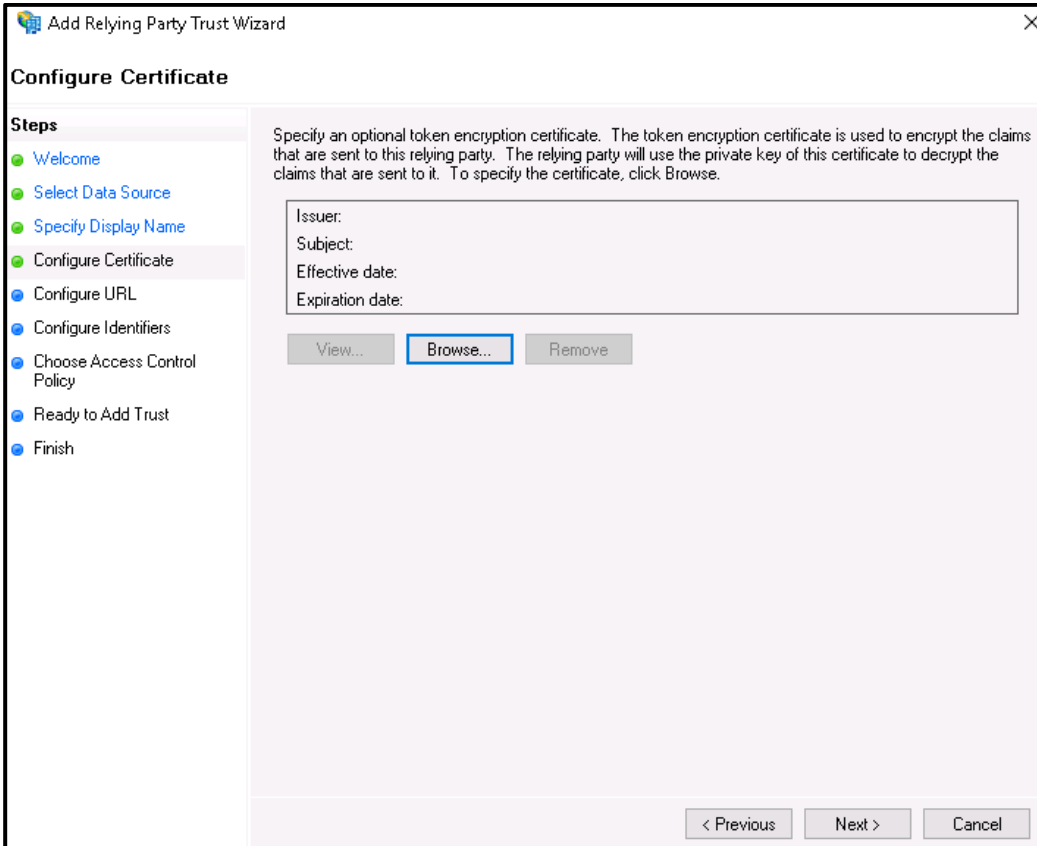
At the bottom right, there are three buttons: '< Previous', 'Next >' (highlighted with a blue border), and 'Cancel'.

5. Give a Display name to that relying trust name which will be displayed after the configuration is done. Click Next.



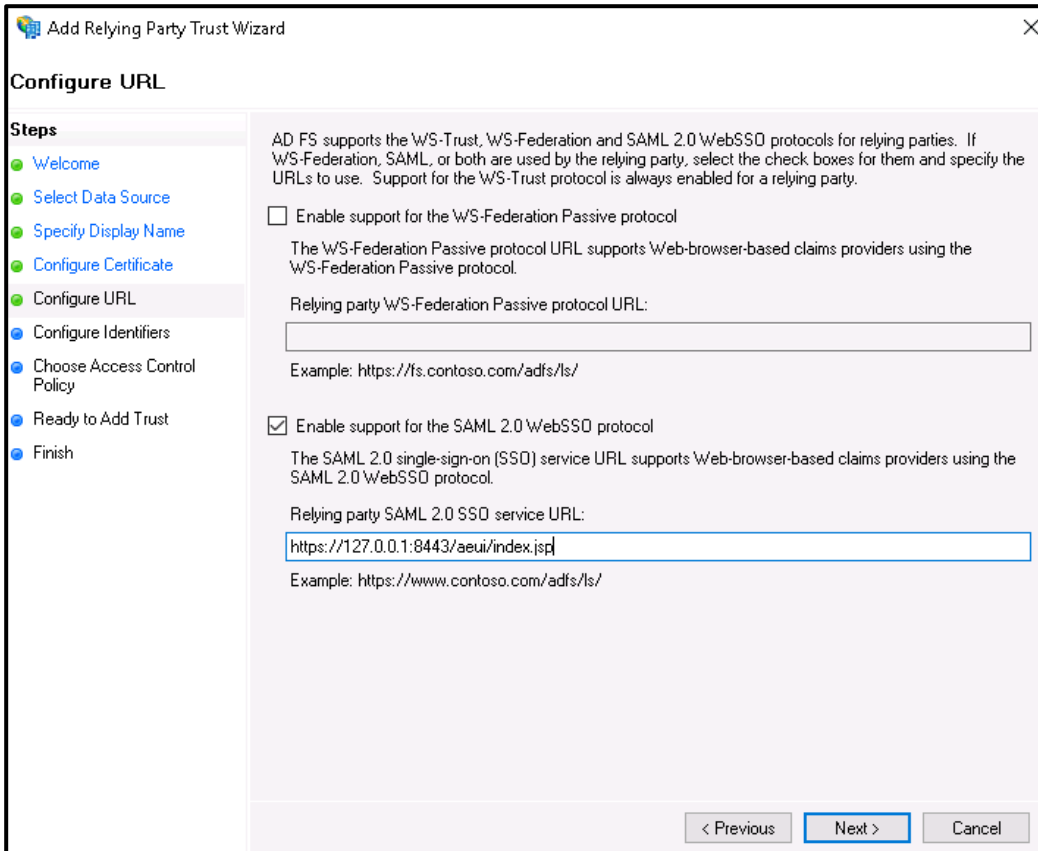
The screenshot shows the 'Add Relying Party Trust Wizard' dialog box, specifically the 'Specify Display Name' step. The dialog has a title bar with a close button (X) and a subtitle 'Add Relying Party Trust Wizard'. Below the title bar, the main heading is 'Specify Display Name'. On the left side, there is a 'Steps' list with the following items: 'Welcome', 'Select Data Source', 'Specify Display Name' (which is highlighted with a green dot), 'Configure Certificate', 'Configure URL', 'Configure Identifiers', 'Choose Access Control Policy', 'Ready to Add Trust', and 'Finish'. The main area of the dialog contains the instruction 'Enter the display name and any optional notes for this relying party.' Below this instruction, there is a 'Display name:' label followed by a text input field containing the text 'AE ADFS SAML'. Below the input field is a 'Notes:' label followed by a large, empty text area with a vertical scrollbar. At the bottom right of the dialog, there are three buttons: '< Previous', 'Next >' (which is highlighted with a blue border), and 'Cancel'.

6. We shall configure the Certificate later, for now Click Next.



The screenshot shows the 'Add Relying Party Trust Wizard' dialog box, specifically the 'Configure Certificate' step. The window title is 'Add Relying Party Trust Wizard'. The main heading is 'Configure Certificate'. On the left, there is a 'Steps' list with the following items: Welcome, Select Data Source, Specify Display Name, Configure Certificate (highlighted), Configure URL, Configure Identifiers, Choose Access Control Policy, Ready to Add Trust, and Finish. The main area contains the following text: 'Specify an optional token encryption certificate. The token encryption certificate is used to encrypt the claims that are sent to this relying party. The relying party will use the private key of this certificate to decrypt the claims that are sent to it. To specify the certificate, click Browse.' Below this text is a form with four labels: 'Issuer:', 'Subject:', 'Effective date:', and 'Expiration date:'. Below the form are three buttons: 'View...', 'Browse...' (highlighted with a blue border), and 'Remove'. At the bottom right of the dialog are three buttons: '< Previous', 'Next >', and 'Cancel'.

7. In this window make a check on Enable support for the SAML 2.0 WebSSO protocol. And in the service URL provide the redirect URL. If you are using AE redirect URL then `https://Automationedge:Port/aeui/index.jsp`. Make sure you r using https because AD FS need secure communication. Click on Next.



The screenshot shows the 'Add Relying Party Trust Wizard' dialog box, specifically the 'Configure URL' step. The window title is 'Add Relying Party Trust Wizard' and it has a close button (X) in the top right corner. The 'Steps' pane on the left lists the following steps: Welcome, Select Data Source, Specify Display Name, Configure Certificate, Configure URL (highlighted), Configure Identifiers, Choose Access Control Policy, Ready to Add Trust, and Finish. The main area contains the following text and controls:

AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party.

Enable support for the WS-Federation Passive protocol

The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol.

Relying party WS-Federation Passive protocol URL:

Example: `https://fs.contoso.com/adfs/ls/`

Enable support for the SAML 2.0 WebSSO protocol

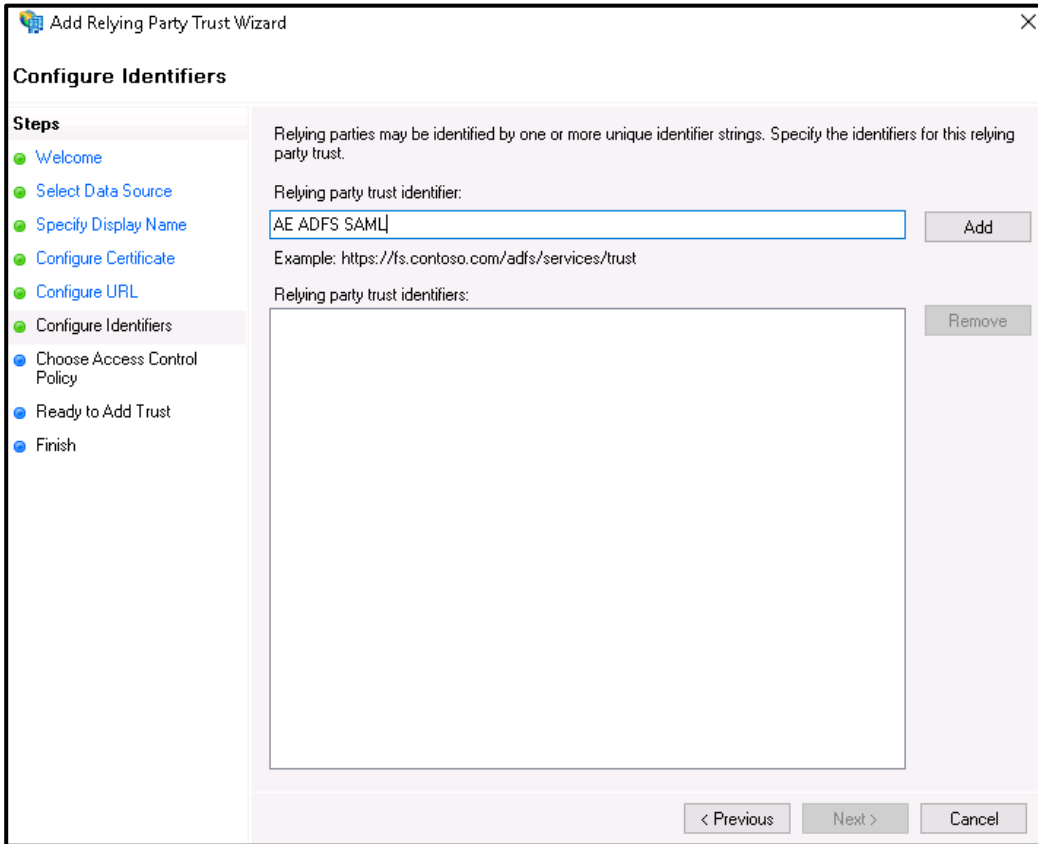
The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol.

Relying party SAML 2.0 SSO service URL:

Example: `https://www.contoso.com/adfs/ls/`

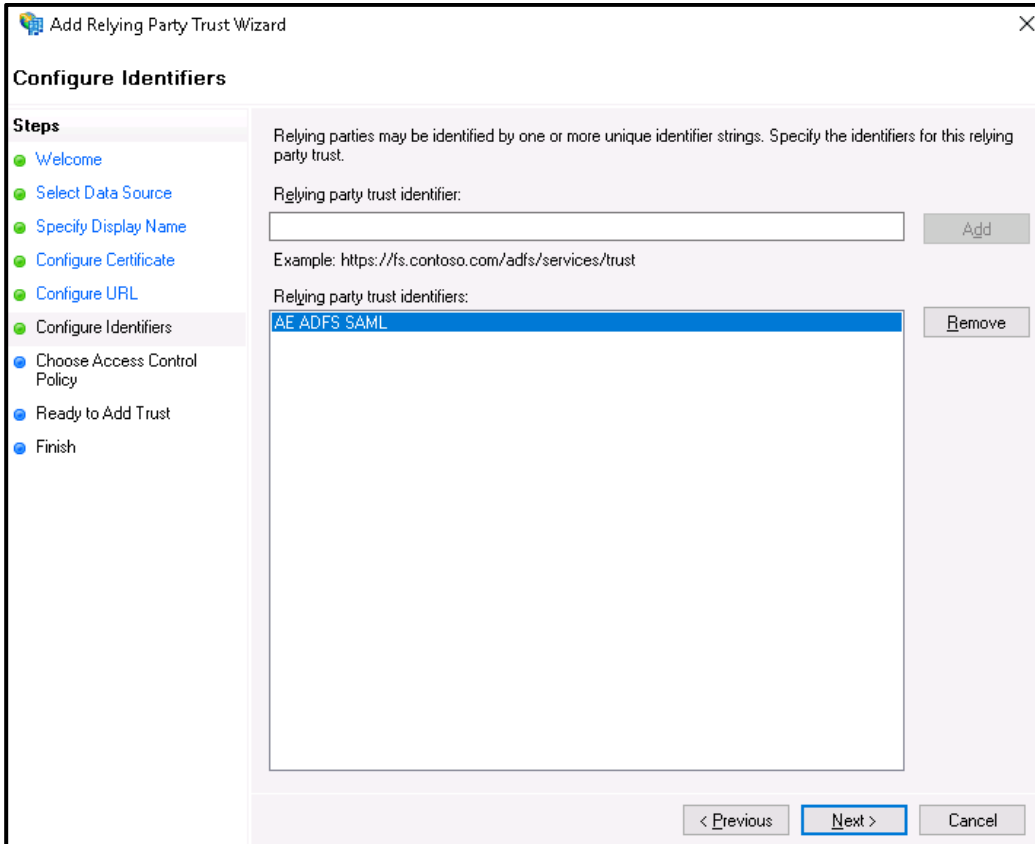
At the bottom right, there are three buttons: '< Previous', 'Next >' (highlighted), and 'Cancel'.

8. In the next window under identifier make sure you have same relying trust display name. Then Add the identifier.



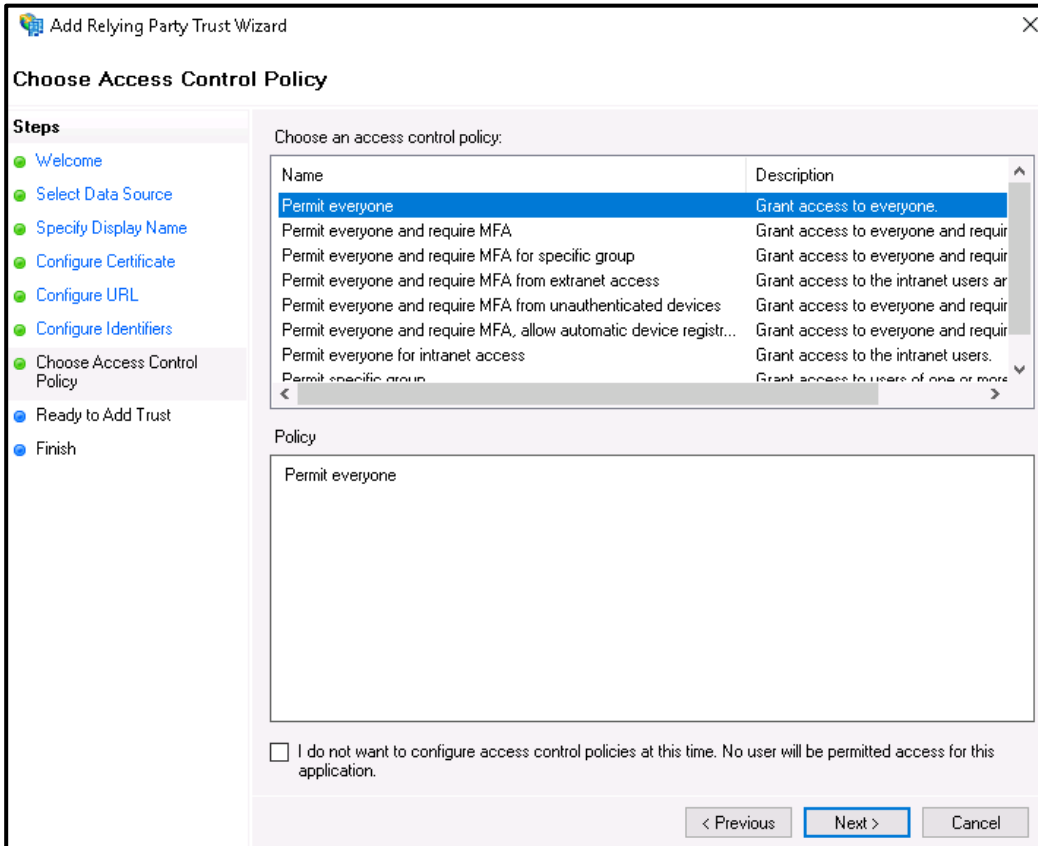
The screenshot shows the 'Add Relying Party Trust Wizard' window, specifically the 'Configure Identifiers' step. The window title is 'Add Relying Party Trust Wizard'. The main heading is 'Configure Identifiers'. On the left, there is a 'Steps' list with the following items: Welcome, Select Data Source, Specify Display Name, Configure Certificate, Configure URL, Configure Identifiers (highlighted), Choose Access Control Policy, Ready to Add Trust, and Finish. The main area contains the following text: 'Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust.' Below this, there is a 'Relying party trust identifier:' label, a text input field containing 'AE ADFS SAML', and an 'Add' button. An example URL is provided: 'Example: https://fs.contoso.com/adfs/services/trust'. Below the input field, there is a 'Relying party trust identifiers:' label and a large empty list box. To the right of the list box is a 'Remove' button. At the bottom of the window, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

9. Once Relying Party Trust Identifier is added, click Next.

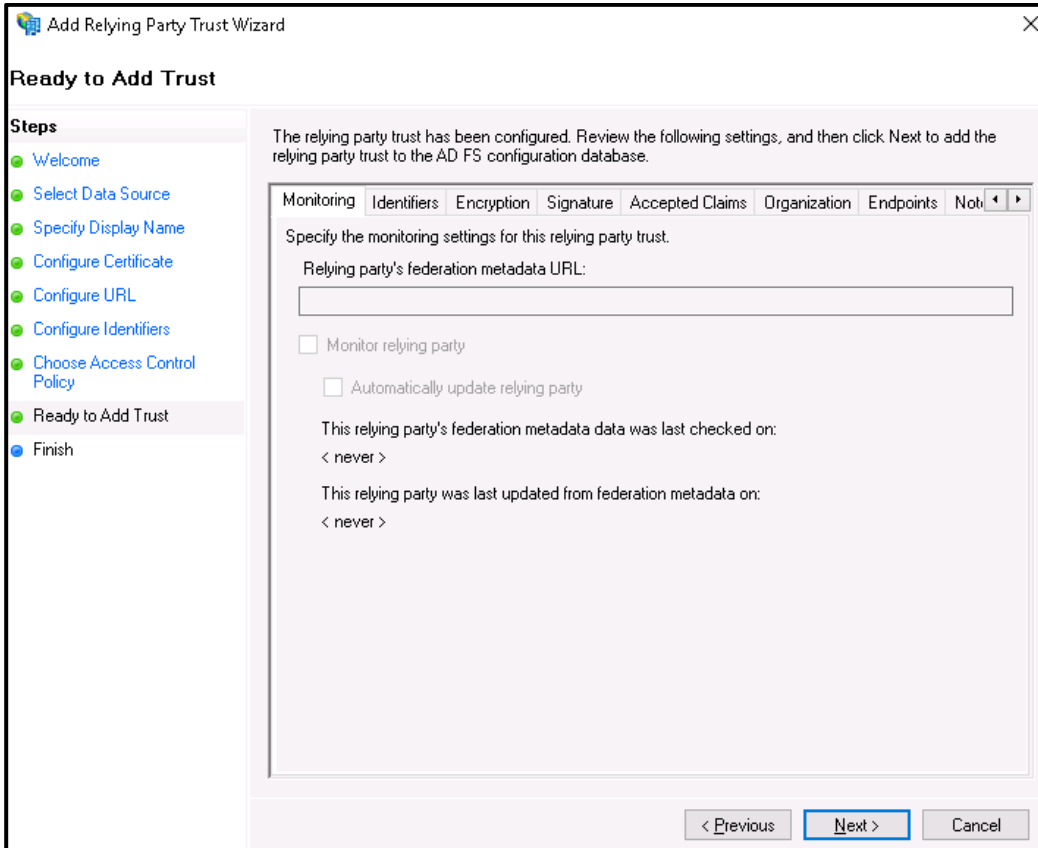


The screenshot shows the 'Add Relying Party Trust Wizard' dialog box, specifically the 'Configure Identifiers' step. The window title is 'Add Relying Party Trust Wizard'. On the left, a 'Steps' pane lists the following steps: Welcome, Select Data Source, Specify Display Name, Configure Certificate, Configure URL, Configure Identifiers (highlighted), Choose Access Control Policy, Ready to Add Trust, and Finish. The main area contains the following text: 'Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust.' Below this is a text input field labeled 'Relying party trust identifier:' with an 'Add' button to its right. An example URL is provided: 'Example: https://fs.contoso.com/adfs/services/trust'. Below the example is a list box labeled 'Relying party trust identifiers:' containing the entry 'AE ADFS SAML', which is currently selected. A 'Remove' button is located to the right of the list box. At the bottom of the dialog, there are three buttons: '< Previous', 'Next >' (highlighted), and 'Cancel'.

10. Give access control policy according to your need. In the below screenshot we have selected Permit everyone policy. Then click on Next.



11. Review the settings and click Next.



Add Relying Party Trust Wizard

Ready to Add Trust

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Configure Certificate
- Configure URL
- Configure Identifiers
- Choose Access Control Policy
- Ready to Add Trust
- Finish

The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.

Monitoring | Identifiers | Encryption | Signature | Accepted Claims | Organization | Endpoints | Notif

Specify the monitoring settings for this relying party trust.

Relying party's federation metadata URL:

Monitor relying party

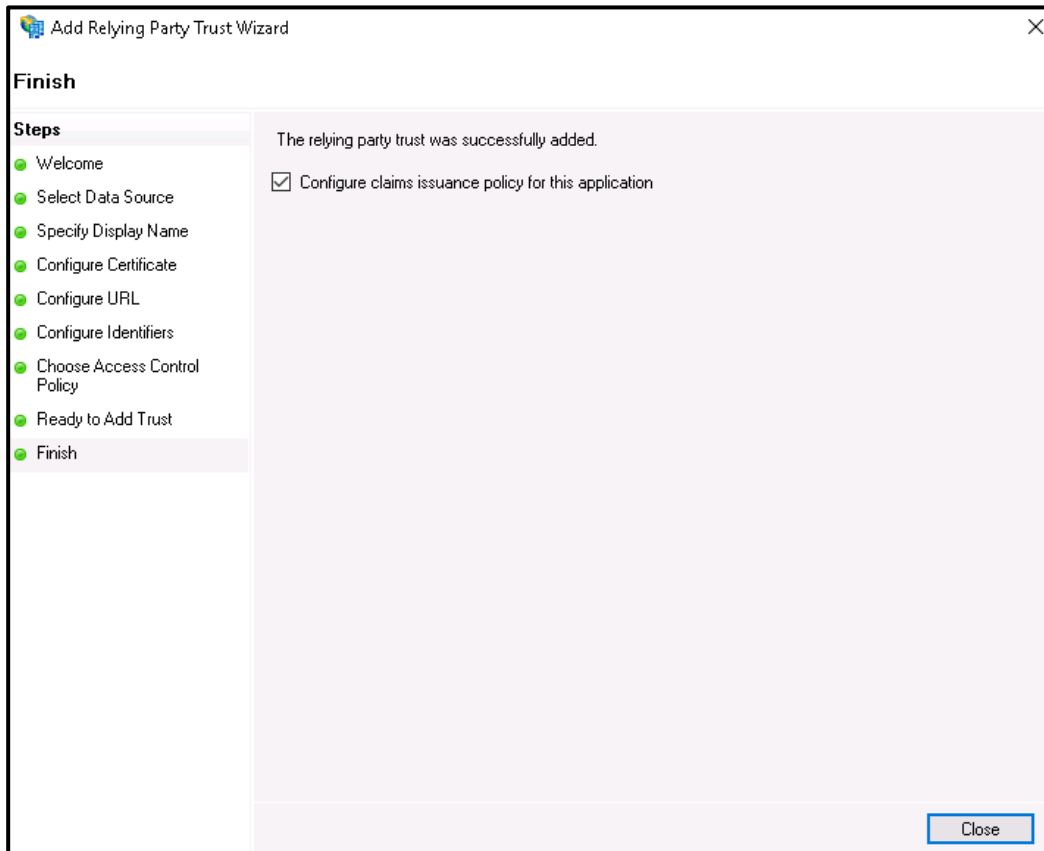
Automatically update relying party

This relying party's federation metadata data was last checked on:
< never >

This relying party was last updated from federation metadata on:
< never >

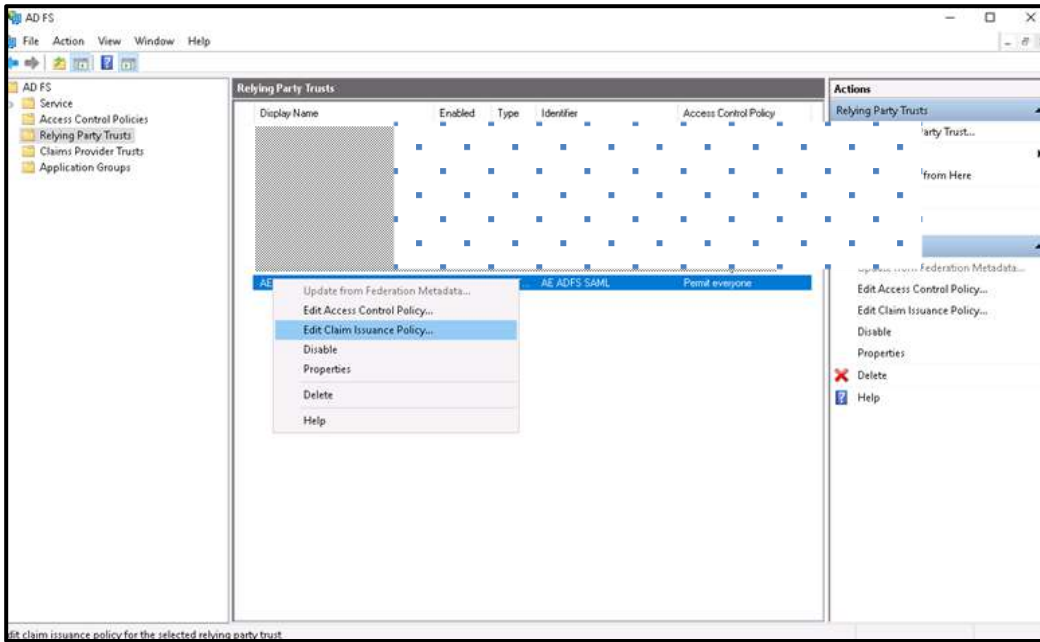
< Previous **Next >** Cancel

12. Make a check on Configure Claims issuance policy for the application. As we still need to configure claims and upload a certificate.
13. Click Close.

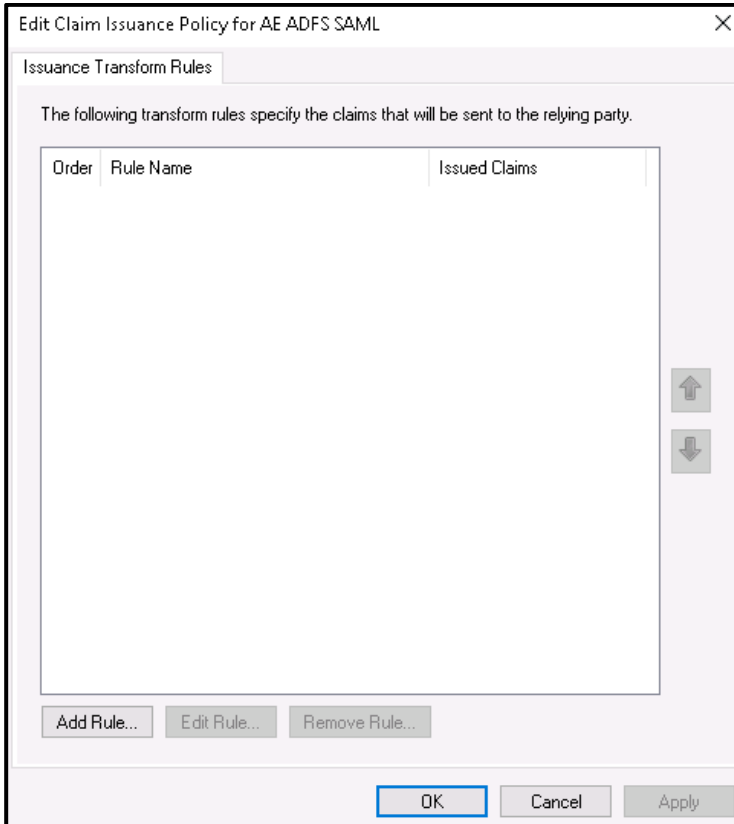


Claim Issuance Policy

14. We need to add claims for the party trust. Highlight your party trust and look out for **Edit Claim Issuance Policy**.

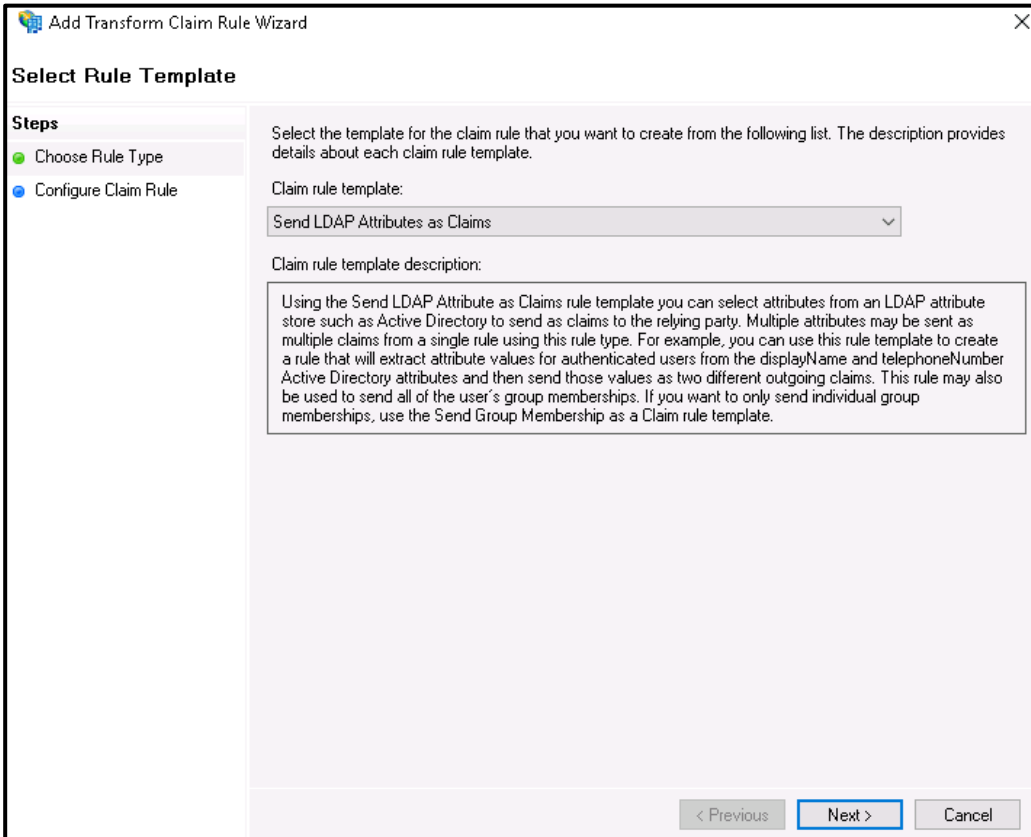


15. The below window will pop-up, click on add rules



Rule 1

16. In the next window select on Send LDAP Attributes as Claims and click on next.



The screenshot shows a dialog box titled "Add Transform Claim Rule Wizard" with a close button (X) in the top right corner. The dialog is divided into two main sections. On the left, under the heading "Steps", there are two items: "Choose Rule Type" (indicated by a green circle) and "Configure Claim Rule" (indicated by a blue circle). The right section is titled "Select Rule Template" and contains the following text: "Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template." Below this text, there is a label "Claim rule template:" followed by a dropdown menu that has "Send LDAP Attributes as Claims" selected. Underneath the dropdown is a label "Claim rule template description:" followed by a text box containing the following text: "Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template." At the bottom right of the dialog, there are three buttons: "< Previous" (disabled), "Next >" (active/highlighted), and "Cancel" (disabled).

17. Add Transform Claim Rule Wizard appears.
18. Give a name to Claim and in the Attribute Store click on Active Directory
19. Use the following attribute mapping

LDAP Attribute	Outgoing Claims
User-Principal-Name	username
E-Mail-Addresses	emailAddress
Given-Name	firstName
Surname	lastName

Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name: Rule1

Rule template: Send LDAP Attributes as Claims

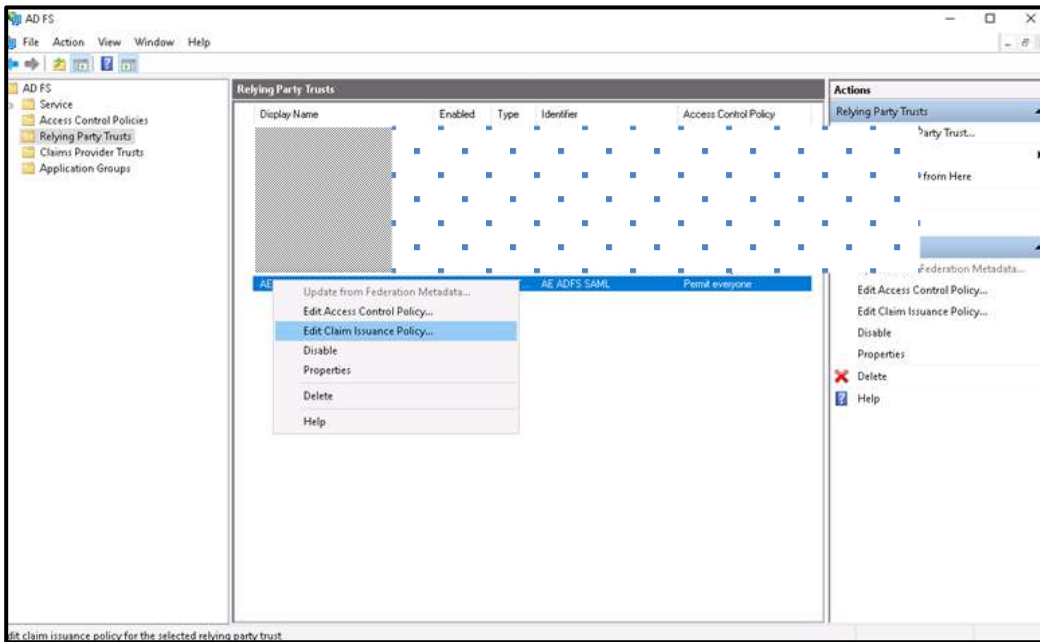
Attribute store: Active Directory

Mapping of LDAP attributes to outgoing claim types:

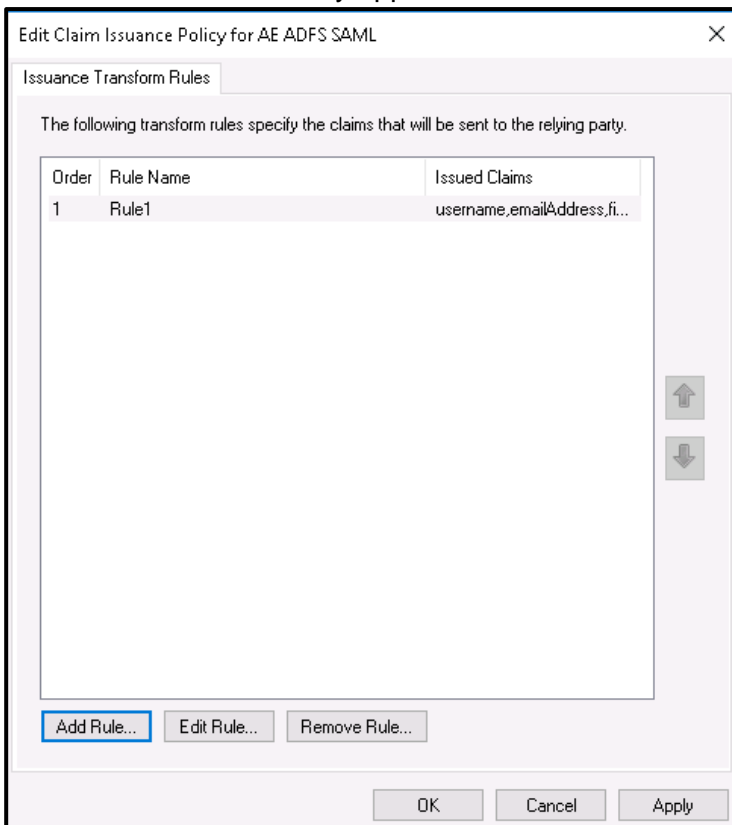
	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
	User-Principal-Name	username
	E-Mail-Addresses	emailAddress
	Given-Name	firstName
▶	Surname	lastName
*		

< Previous Finish Cancel

20. Click Finish.
21. We need to add claims for the party trust. Highlight your party trust and look out for **Edit Claim Issuance Policy**.

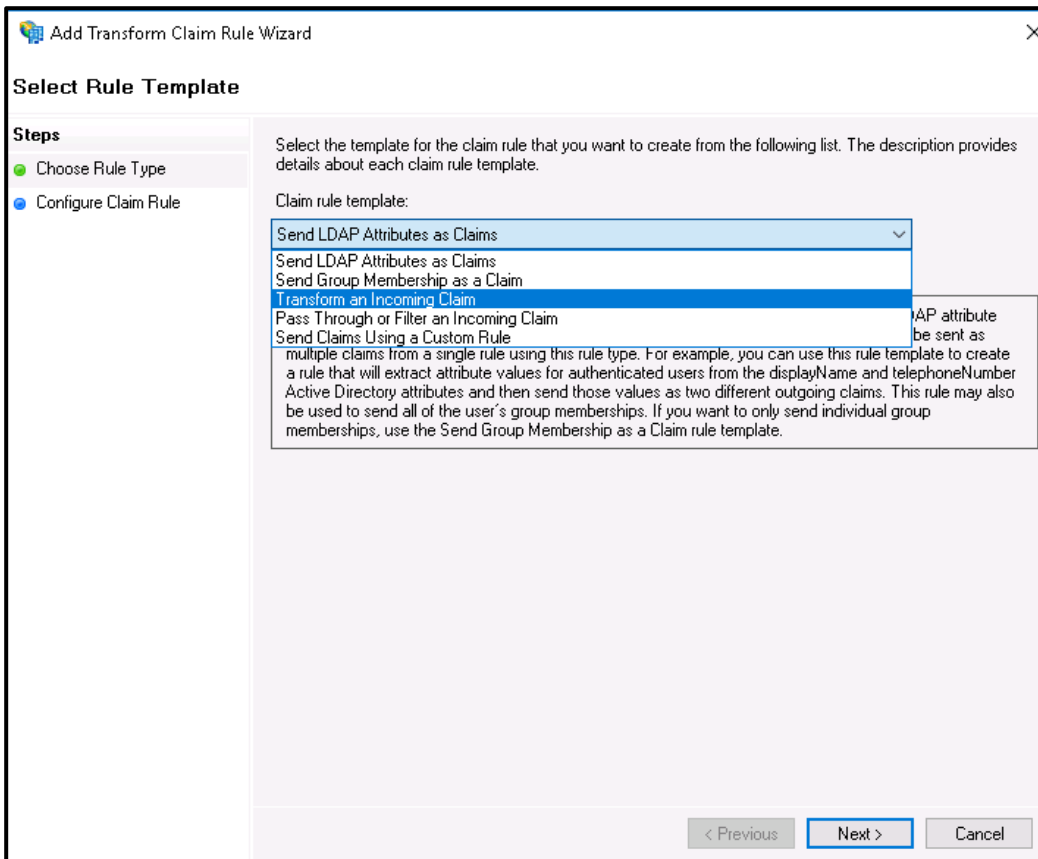


22. Edit Claim Issuance Policy appears. Click Add Rule.

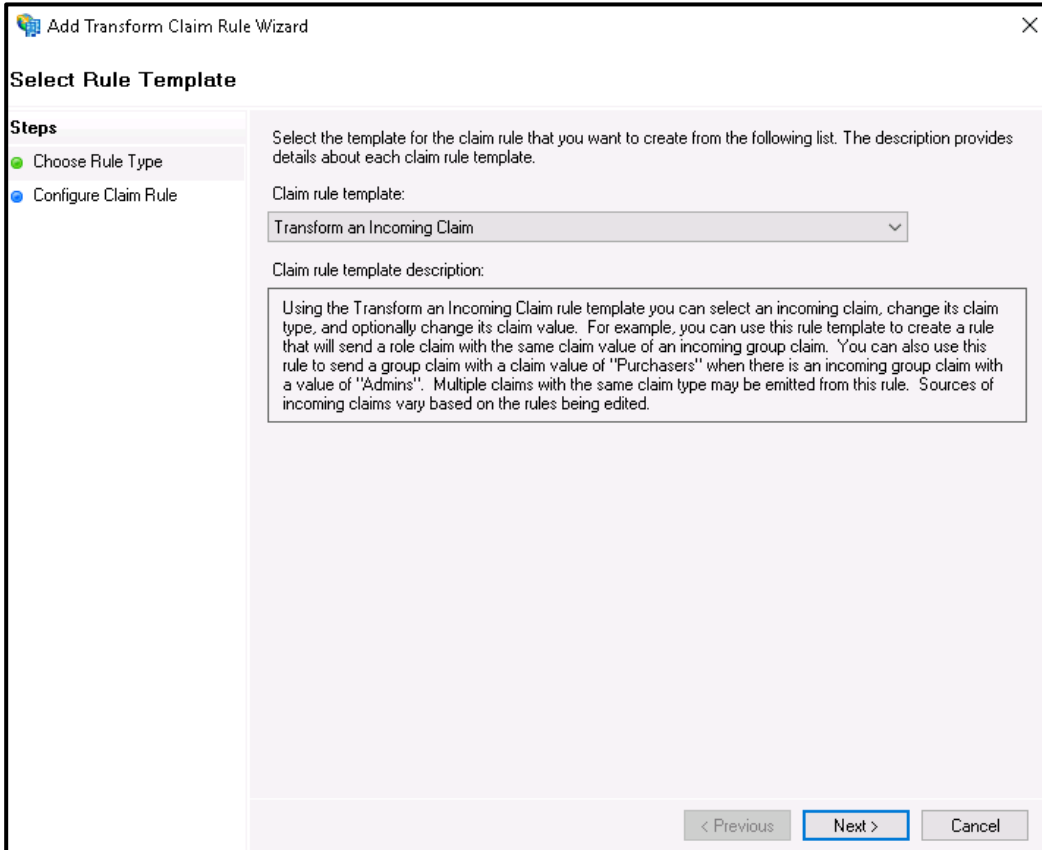


Rule 2

23. We need to add one more incoming claims for the following party trust. Highlight your party trust and look out for Edit Claim Issuance Policy. The below window will pop-up, click on add rules



24. We need to add one more incoming claims for the following party trust. Highlight your party trust and look out for Edit Claim Issuance Policy. The below window will pop-up, click on add rules. Click Next.



Add Transform Claim Rule Wizard

Select Rule Template

Steps

- Choose Rule Type
- Configure Claim Rule

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template:

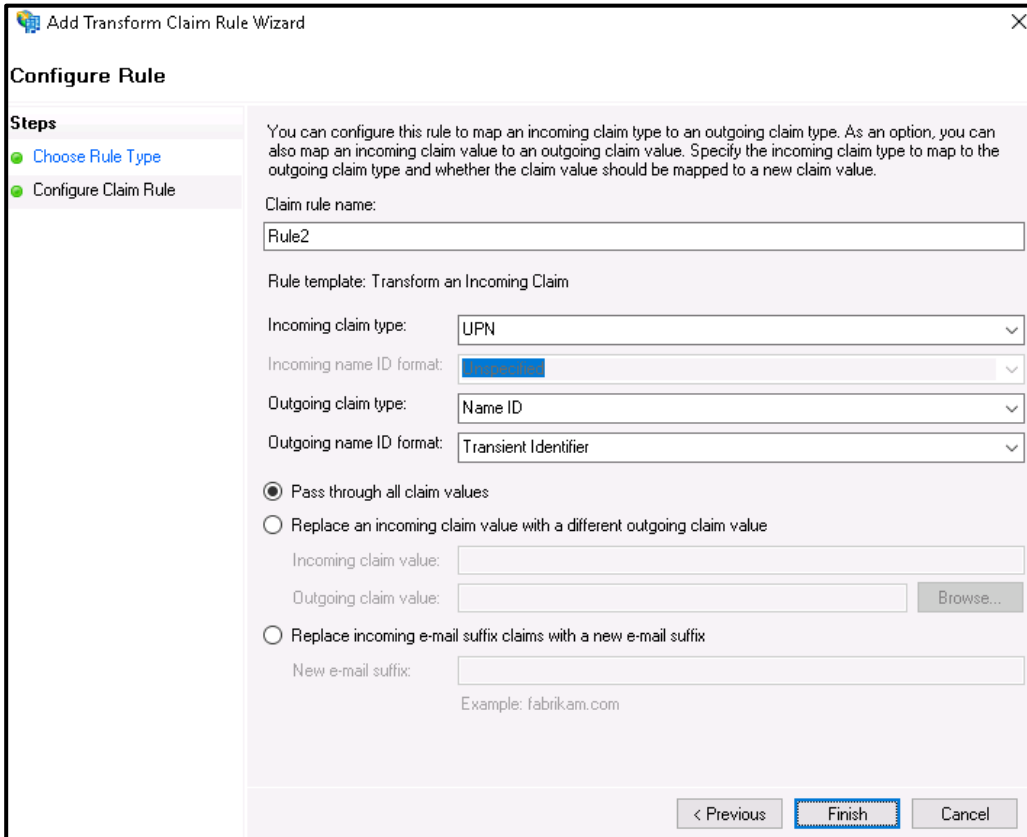
Transform an Incoming Claim

Claim rule template description:

Using the Transform an Incoming Claim rule template you can select an incoming claim, change its claim type, and optionally change its claim value. For example, you can use this rule template to create a rule that will send a role claim with the same claim value of an incoming group claim. You can also use this rule to send a group claim with a claim value of "Purchasers" when there is an incoming group claim with a value of "Admins". Multiple claims with the same claim type may be emitted from this rule. Sources of incoming claims vary based on the rules being edited.

< Previous **Next >** Cancel

25. Select Incoming claim type to **UPN**, Outgoing Claim type to **Name ID** and Outgoing name ID format to **Transient Identifier**. Click Finish.



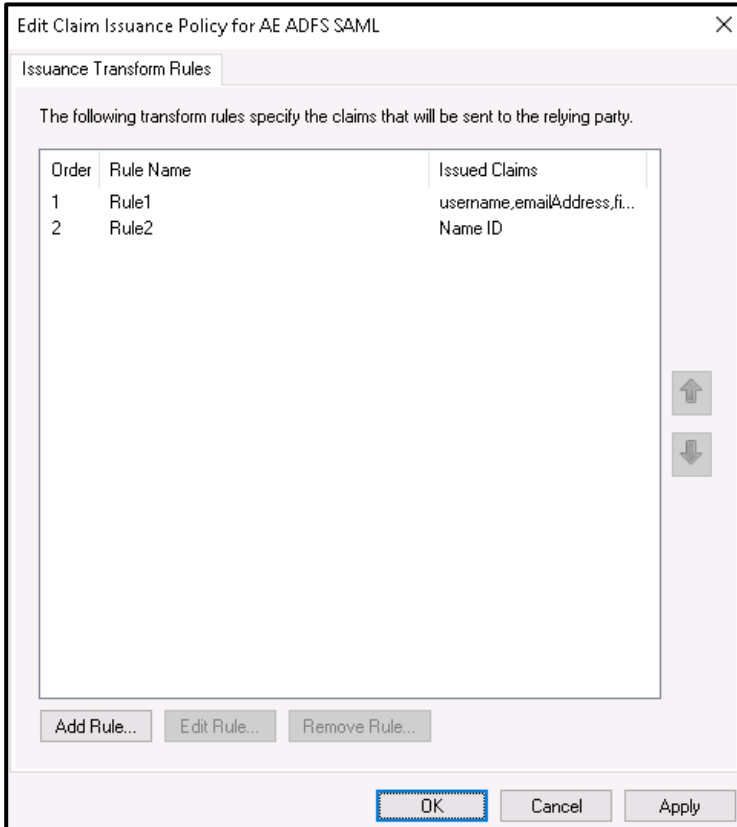
The screenshot shows the 'Add Transform Claim Rule Wizard' dialog box, specifically the 'Configure Rule' step. The window title is 'Add Transform Claim Rule Wizard'. On the left, there is a 'Steps' pane with two items: 'Choose Rule Type' (highlighted in blue) and 'Configure Claim Rule' (highlighted in green). The main area contains the following configuration options:

- Claim rule name:** A text box containing 'Rule2'.
- Rule template:** 'Transform an Incoming Claim'.
- Incoming claim type:** A dropdown menu set to 'UPN'.
- Incoming name ID format:** A dropdown menu set to 'Name ID'.
- Outgoing claim type:** A dropdown menu set to 'Name ID'.
- Outgoing name ID format:** A dropdown menu set to 'Transient Identifier'.
- Options:** Three radio button options:
 - Pass through all claim values
 - Replace an incoming claim value with a different outgoing claim value
 - Incoming claim value:** An empty text box.
 - Outgoing claim value:** An empty text box with a 'Browse...' button to its right.
 - Replace incoming e-mail suffix claims with a new e-mail suffix
 - New e-mail suffix:** An empty text box.
 - Example: fabrikam.com

At the bottom right, there are three buttons: '< Previous', 'Finish' (highlighted with a blue dashed border), and 'Cancel'.

26. You can now see the two rules created. You may edit rules if desired by selecting them.

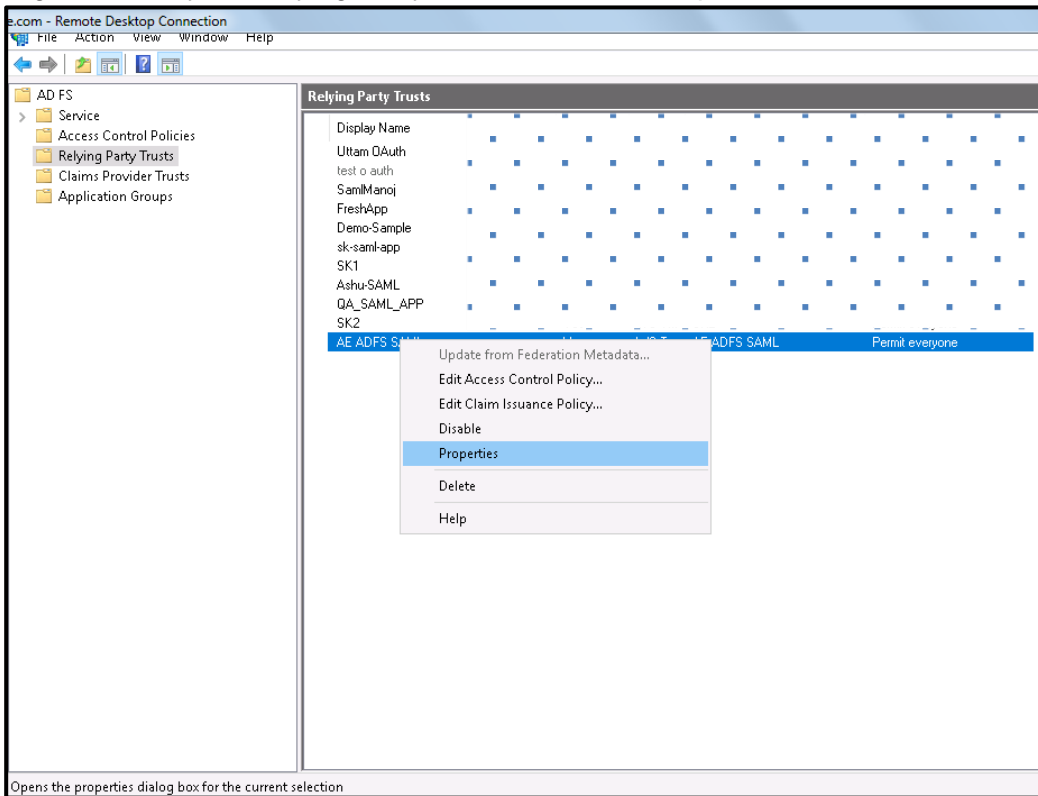
27. Also at any later time, you may right click on your Relying Party Trust and Edit Claim Issuance Policy to open this screen.



Upload RSA Certificate for Relying Party Trust

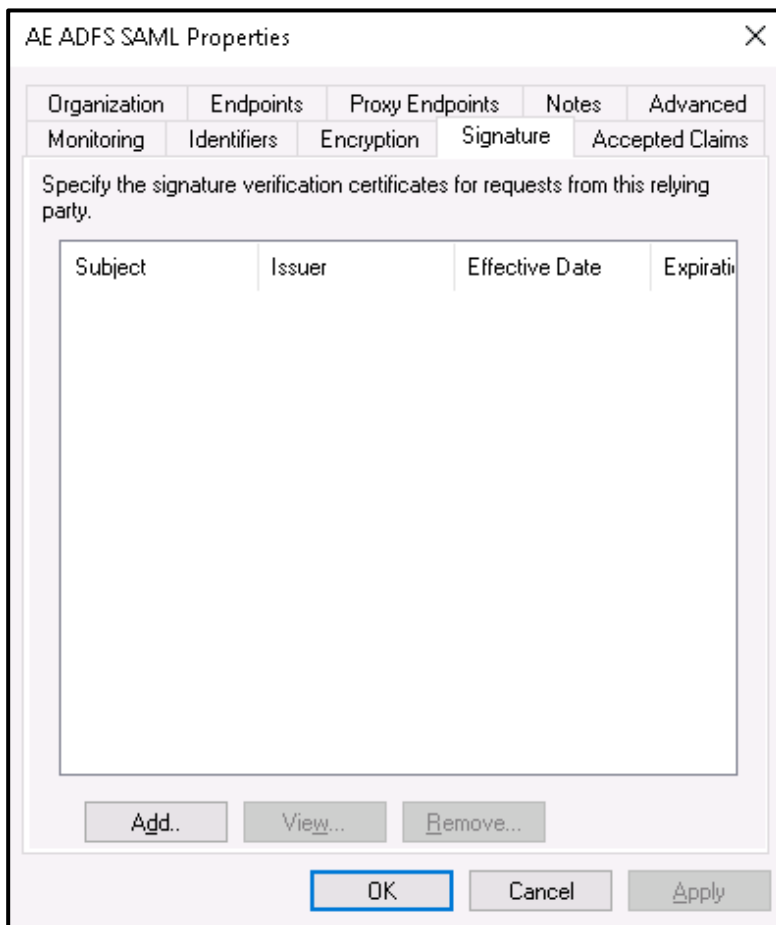
28. Once again let us go to the Windows Server Manager console and open AD FS tool.

29. Right click on your Relying Party Trust and select Properties

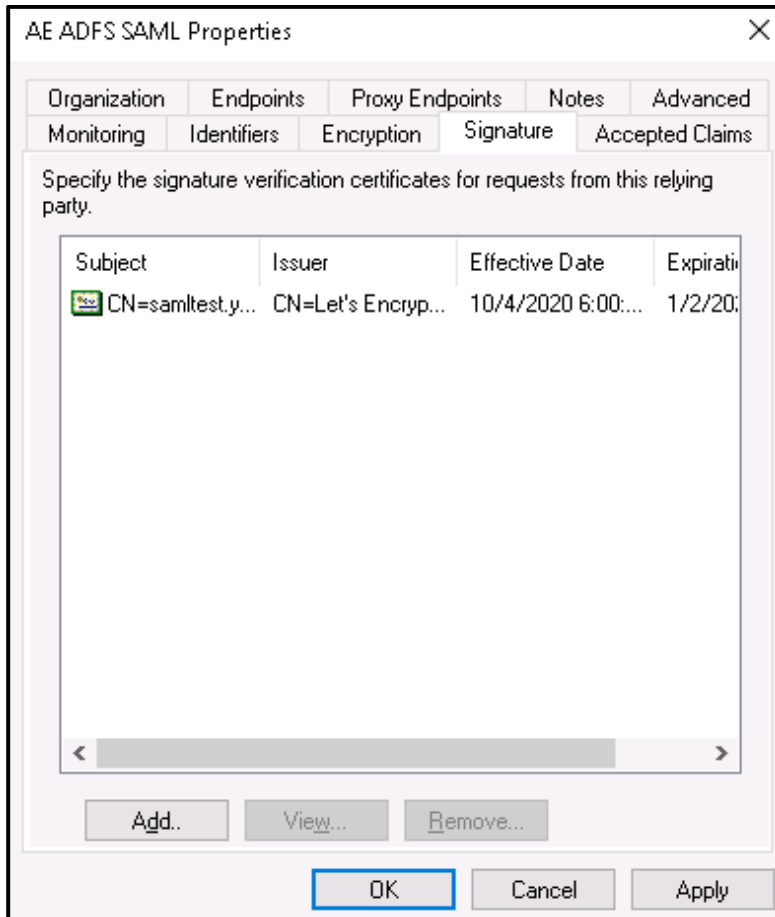


30. Look out for signature tab and click on Add and browse for your RSA certificate.

 **Note:** To generate Self Signed or CA Certificate refer to section [2.9 Keystore and Certificate Generation](#).

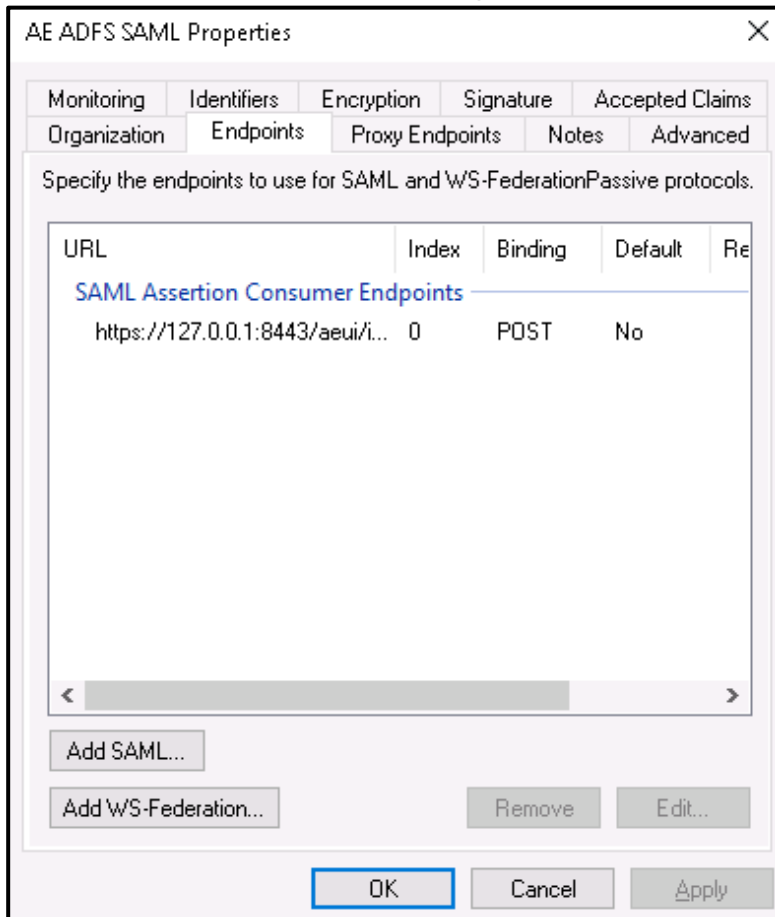


31. The RSA certificate is now uploaded. Click Apply



Endpoints

32. In the same window look out for endpoint tab and click on **Add SAML...**



33. In this step we configure for logout. So select the endpoint type to SAML Logout, under binding go for post. Internally we are using post binding for logout request.

For the Trusted URL, create a URL using:

- i. The web address of your ADFS server
- ii. The ADFS SAML endpoint you noted earlier
- iii. The string '?wa=wsignout1.0'

The URL should look something like this:

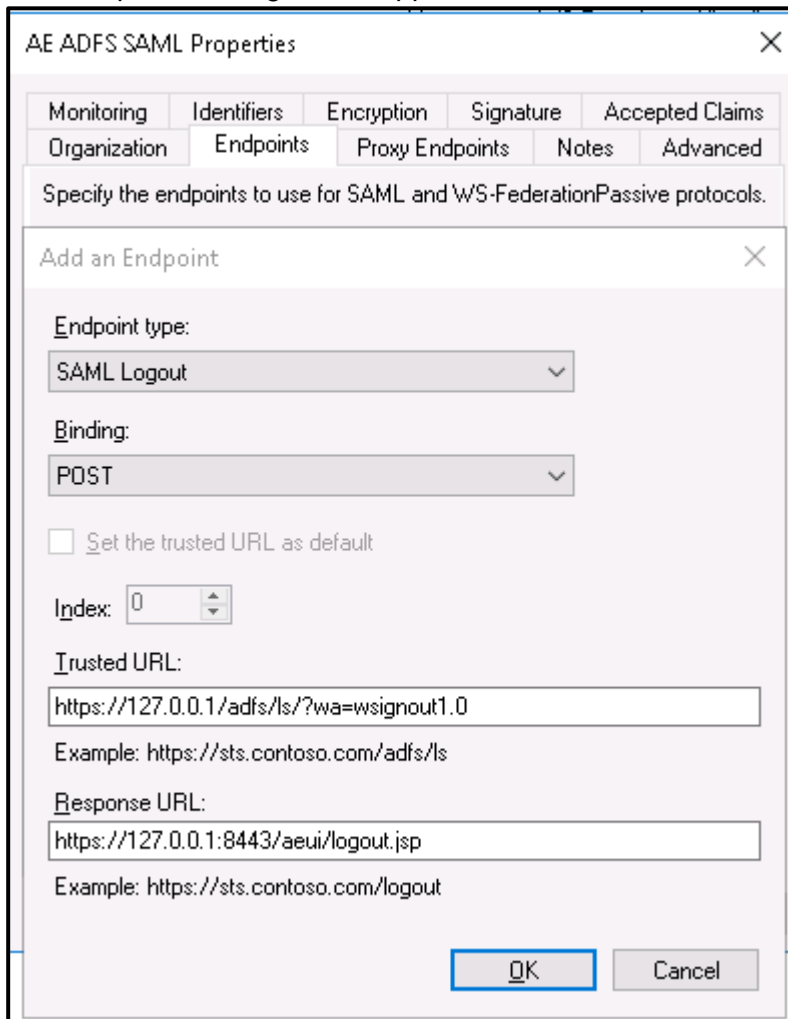
`https://<sso.yourdomain.tld>/adfs/ls/?wa=wsignout1.0`

In the response URL section specify the redirect after logout e.g.

`https://automationedge.port/aeui/logout.jsp`

34. Click on OK.

35. The Endpoints configuration appears as below.

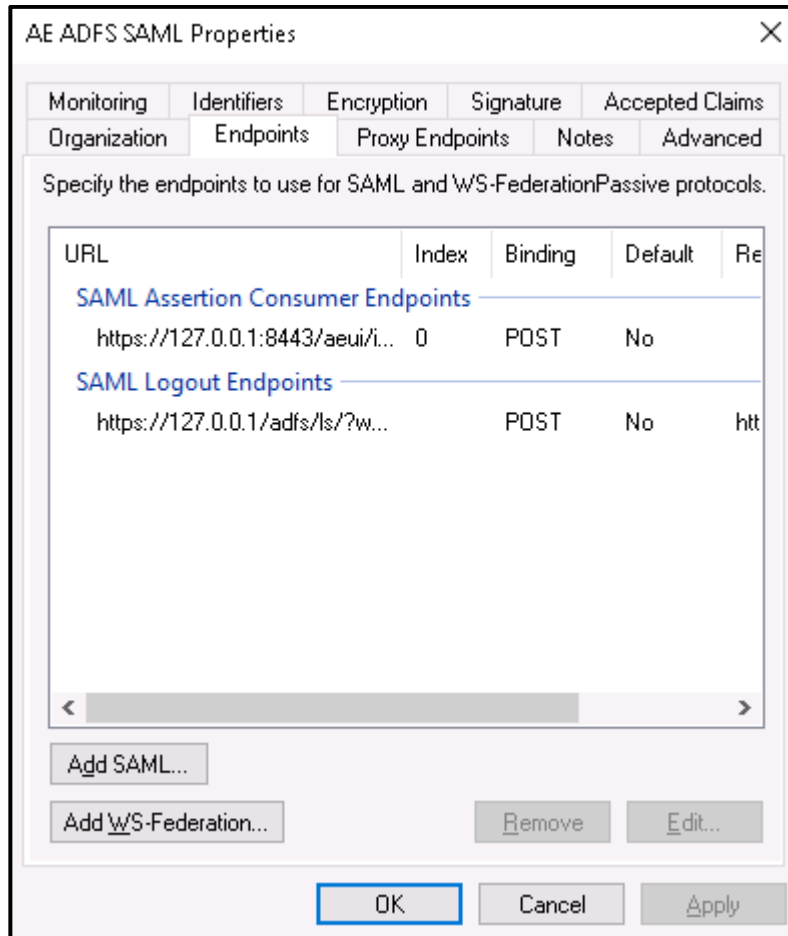


The screenshot shows the 'AE ADFS SAML Properties' dialog box with the 'Endpoints' tab selected. The 'Add an Endpoint' sub-dialog is open, displaying the following configuration:

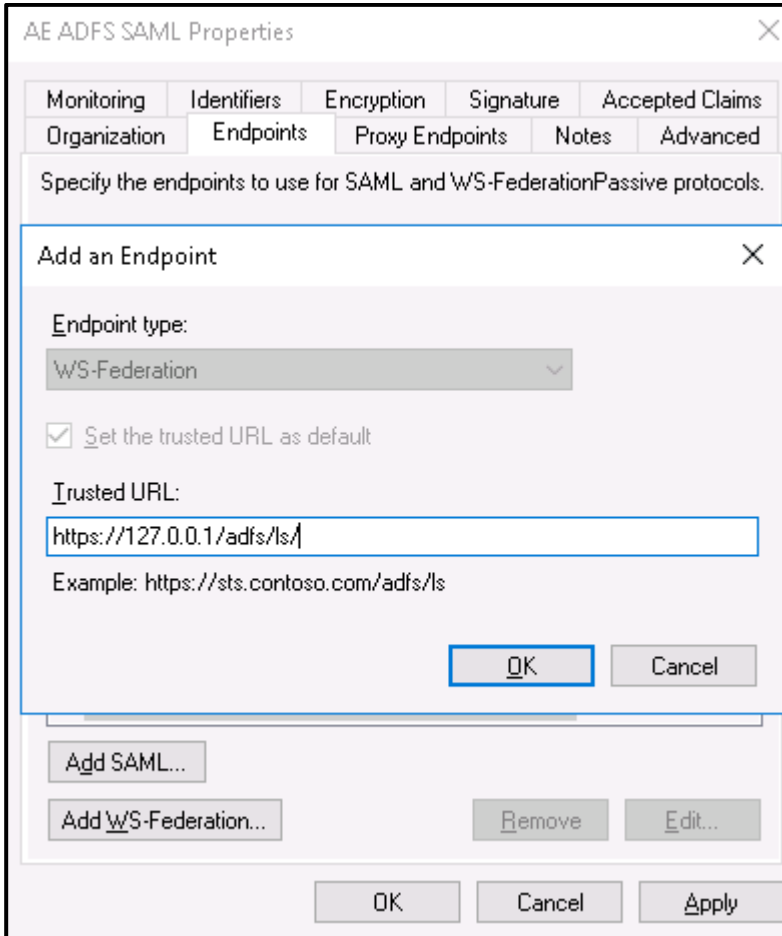
- Endpoint type: SAML Logout
- Binding: POST
- Set the trusted URL as default
- Index: 0
- Trusted URL: `https://127.0.0.1/adfs/ls/?wa=wsignout1.0`
Example: `https://sts.contoso.com/adfs/ls`
- Response URL: `https://127.0.0.1:8443/aeui/logout.jsp`
Example: `https://sts.contoso.com/logout`

Buttons for 'OK' and 'Cancel' are visible at the bottom of the sub-dialog.

36. Then click **Add WS-Federation** button as shown in image below.



37. Add `https://sso.yourdomain.tld/adfs/ls/` as a trusted URL and click Ok.



AE ADFS SAML Properties

Monitoring Identifiers Encryption Signature Accepted Claims
Organization Endpoints Proxy Endpoints Notes Advanced

Specify the endpoints to use for SAML and WS-FederationPassive protocols.

Add an Endpoint

Endpoint type:
WS-Federation

Set the trusted URL as default

Trusted URL:
`https://127.0.0.1/adfs/ls/`

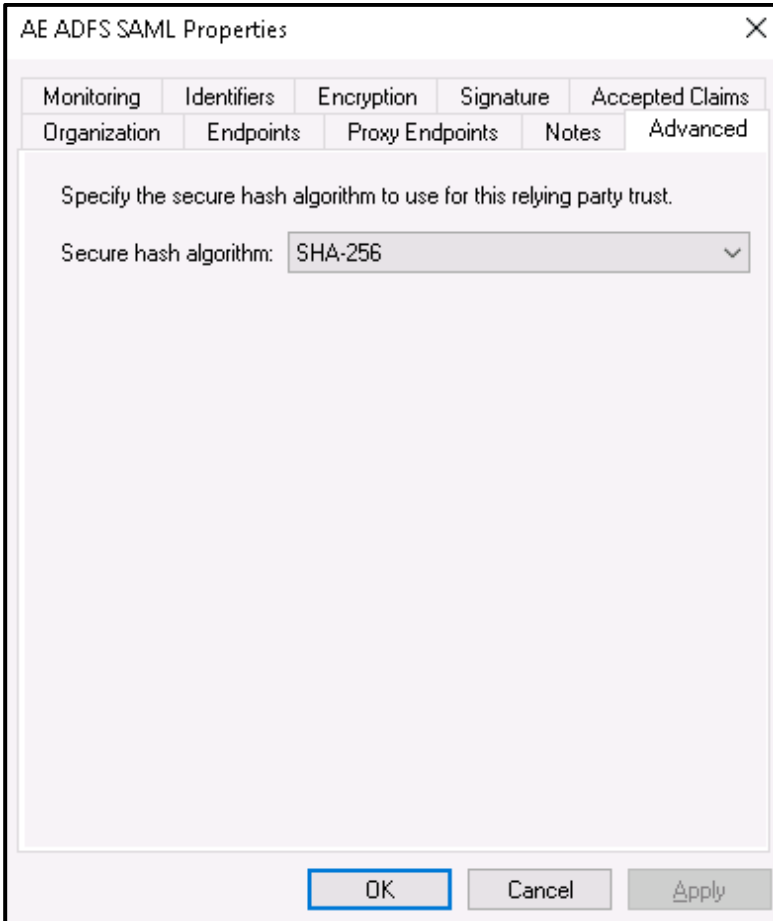
Example: `https://sts.contoso.com/adfs/ls`

OK Cancel

Add SAML...
Add WS-Federation... Remove Edit...

OK Cancel Apply

38. In the Advanced tab, make sure SHA-256 is specified as the secure hash algorithm.

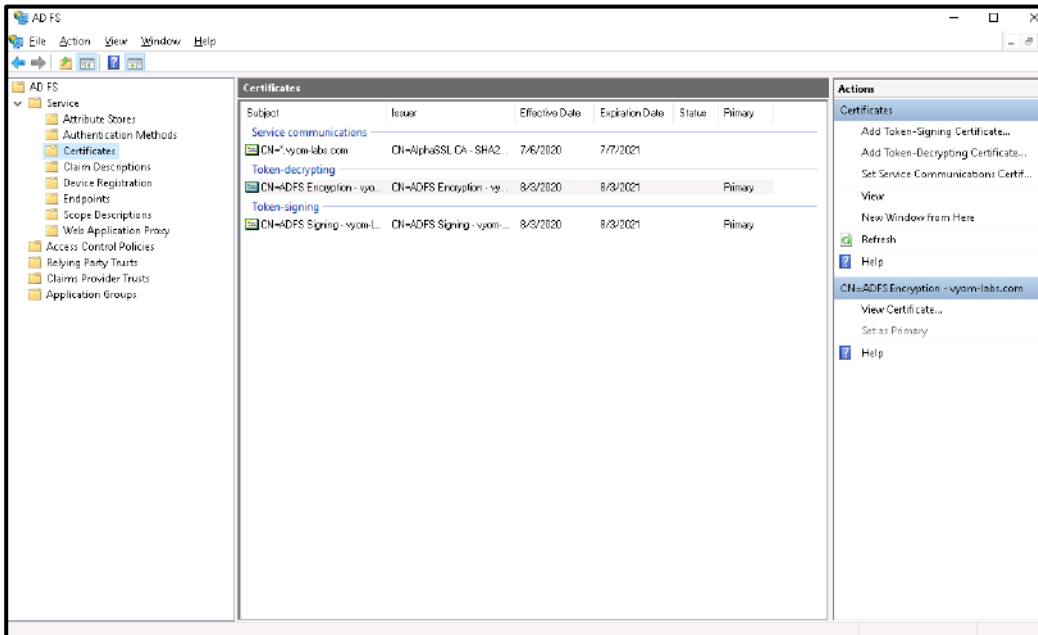


The screenshot shows a dialog box titled "AE ADFS SAML Properties" with a close button (X) in the top right corner. The dialog has two rows of tabs. The first row contains "Monitoring", "Identifiers", "Encryption", "Signature", and "Accepted Claims". The second row contains "Organization", "Endpoints", "Proxy Endpoints", "Notes", and "Advanced". The "Advanced" tab is selected. Below the tabs, the text "Specify the secure hash algorithm to use for this relying party trust." is displayed. Underneath this text is a label "Secure hash algorithm:" followed by a dropdown menu that currently shows "SHA-256". At the bottom of the dialog, there are three buttons: "OK", "Cancel", and "Apply". The "OK" button is highlighted with a blue border.

Upload RSA certificate in AD FS:

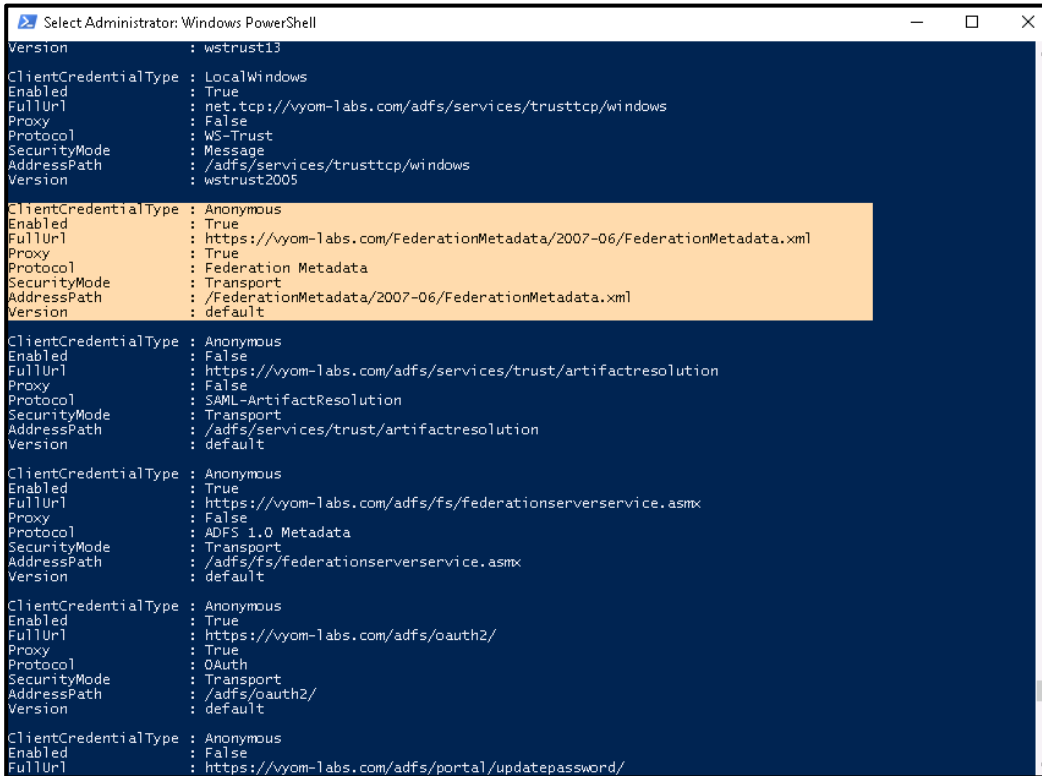
Note: To generate Self Signed or CA Certificate refer to section [2.9 Keystore and Certificate Generation](#)

39. In AD FS console window look out for **Certificate** and move on to **Add Token Signing Certificate**. Upload the certificate.
40. If there are multiple certificates uploaded, mark an appropriate certificate the primary certificate for signing. Right click on the Certificate and select the option 'Set as Primary'.



descriptor.xml:

41. To get descriptor.xml you need to open power shell and type the following command:
Get-AdfsEndpoint
42. Scroll a little and search for Protocol: **Federation Metadata**. Copy the Full URL and past in the browser for federation details. Copy the XML data in a file and save as descriptor.xml.
43. descriptor.xml is required for Single Sign-on configuration in AutomationEdge.



```

Select Administrator: Windows PowerShell
Version           : wstrust13
ClientCredentialType : LocalWindows
Enabled           : True
FullUrl           : net.tcp://vyom-labs.com/adfs/services/trusttcp/windows
Proxy             : False
Protocol          : WS-Trust
SecurityMode      : Message
AddressPath       : /adfs/services/trusttcp/windows
Version           : wstrust2005

ClientCredentialType : Anonymous
Enabled           : True
FullUrl           : https://vyom-labs.com/FederationMetadata/2007-06/FederationMetadata.xml
Proxy             : True
Protocol          : Federation Metadata
SecurityMode      : Transport
AddressPath       : /FederationMetadata/2007-06/FederationMetadata.xml
Version           : default

ClientCredentialType : Anonymous
Enabled           : False
FullUrl           : https://vyom-labs.com/adfs/services/trust/artifactresolution
Proxy             : False
Protocol          : SAML-ArtifactResolution
SecurityMode      : Transport
AddressPath       : /adfs/services/trust/artifactresolution
Version           : default

ClientCredentialType : Anonymous
Enabled           : True
FullUrl           : https://vyom-labs.com/adfs/fs/federationsservice.asmx
Proxy             : False
Protocol          : ADFS 1.0 Metadata
SecurityMode      : Transport
AddressPath       : /adfs/fs/federationsservice.asmx
Version           : default

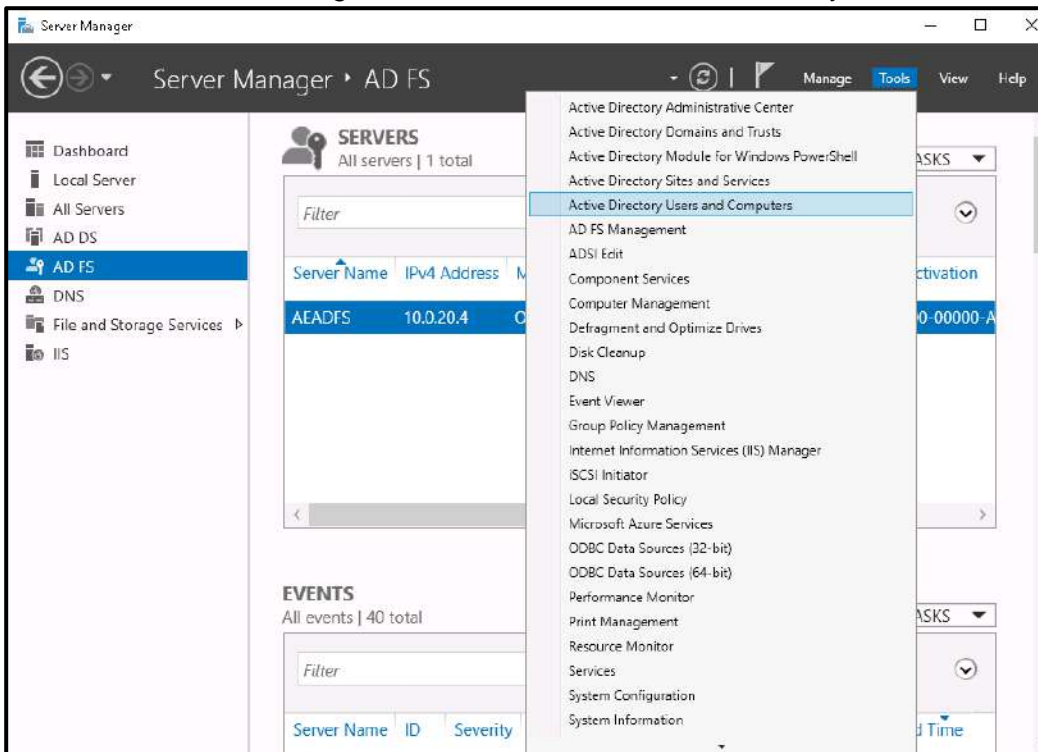
ClientCredentialType : Anonymous
Enabled           : True
FullUrl           : https://vyom-labs.com/adfs/oauth2/
Proxy             : True
Protocol          : OAuth
SecurityMode      : Transport
AddressPath       : /adfs/oauth2/
Version           : default

ClientCredentialType : Anonymous
Enabled           : False
FullUrl           : https://vyom-labs.com/adfs/portal/updatepassword/

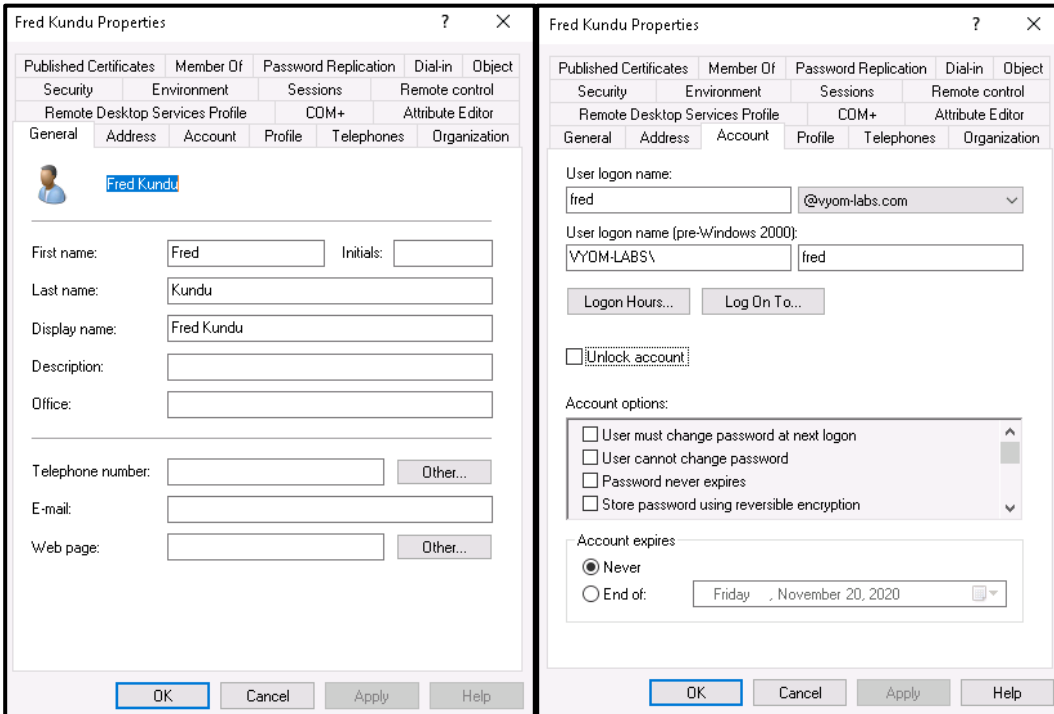
```

Create User

44. You may use an existing user or create a new user to be mapped with AutomationEdge user for SSO.
45. In Windows Server Manager under Tools, select Active Directory Users and Computers.



46. Create a new user as seen below. Configure the new user with General and Account tabs as displayed below.



The image displays two screenshots of the 'Fred Kundu Properties' dialog box, showing the configuration for a new user.

Left Screenshot (General Tab):

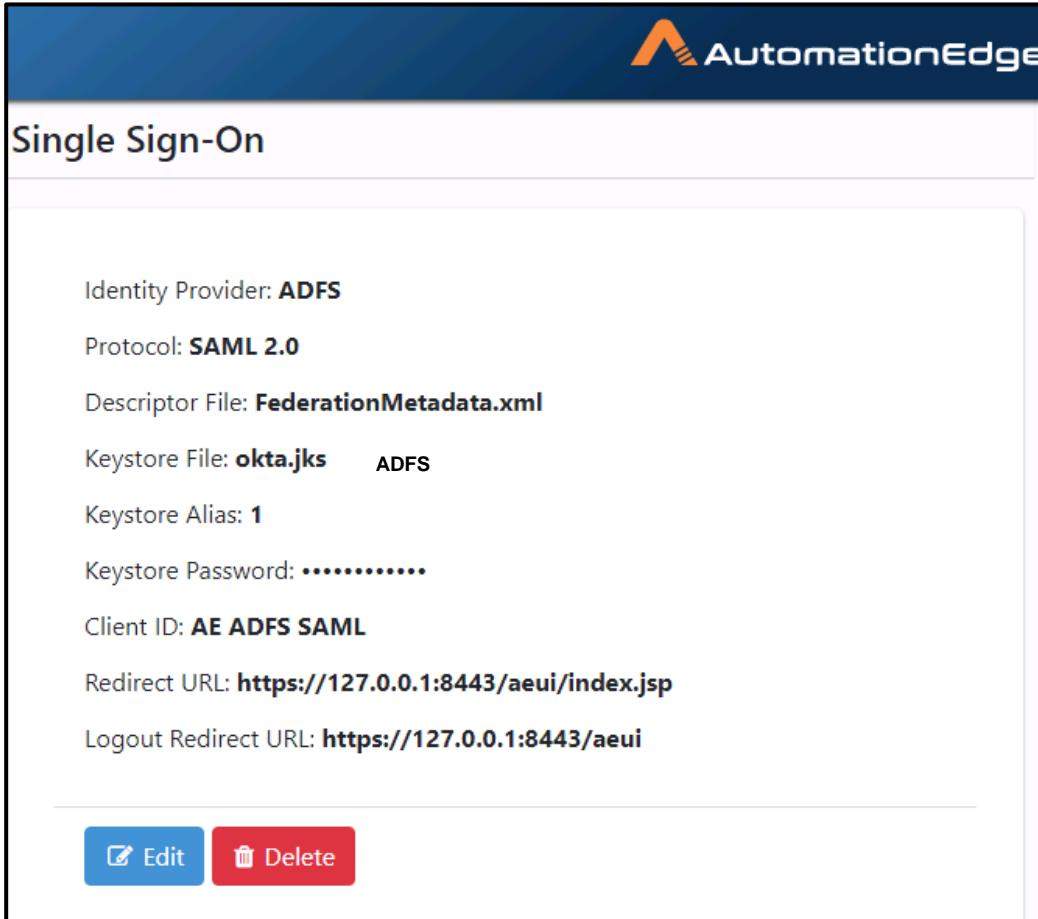
- Published Certificates: Member Of, Password Replication, Dial-in, Object
- Security: Environment, Sessions, Remote control
- Remote Desktop Services Profile: COM+, Attribute Editor
- General: Address, Account, Profile, Telephones, Organization
- User icon: Fred Kundu
- First name: Fred, Initials: []
- Last name: Kundu
- Display name: Fred Kundu
- Description: []
- Office: []
- Telephone number: [], Other... []
- E-mail: []
- Web page: [], Other... []
- Buttons: OK, Cancel, Apply, Help

Right Screenshot (Account Tab):

- Published Certificates: Member Of, Password Replication, Dial-in, Object
- Security: Environment, Sessions, Remote control
- Remote Desktop Services Profile: COM+, Attribute Editor
- General: Address, Account, Profile, Telephones, Organization
- User logon name: fred, @vyom-labs.com
- User logon name (pre-Windows 2000): VYOM-LABS\fred
- Logon Hours... [], Log On To... []
- Unlock account
- Account options:
 - User must change password at next logon
 - User cannot change password
 - Password never expires
 - Store password using reversible encryption
- Account expires:
 - Never
 - End of: Friday, November 20, 2020
- Buttons: OK, Cancel, Apply, Help

AutomationEdge SSO Configuration

47. Single Sign-On is configured under AutomationEdge Settings tab as seen below.



AutomationEdge

Single Sign-On

Identity Provider: **ADFS**

Protocol: **SAML 2.0**

Descriptor File: **FederationMetadata.xml**

Keystore File: **okta.jks** **ADFS**

Keystore Alias: **1**


Keystore Password: **.....**

Client ID: **AE ADFS SAML**

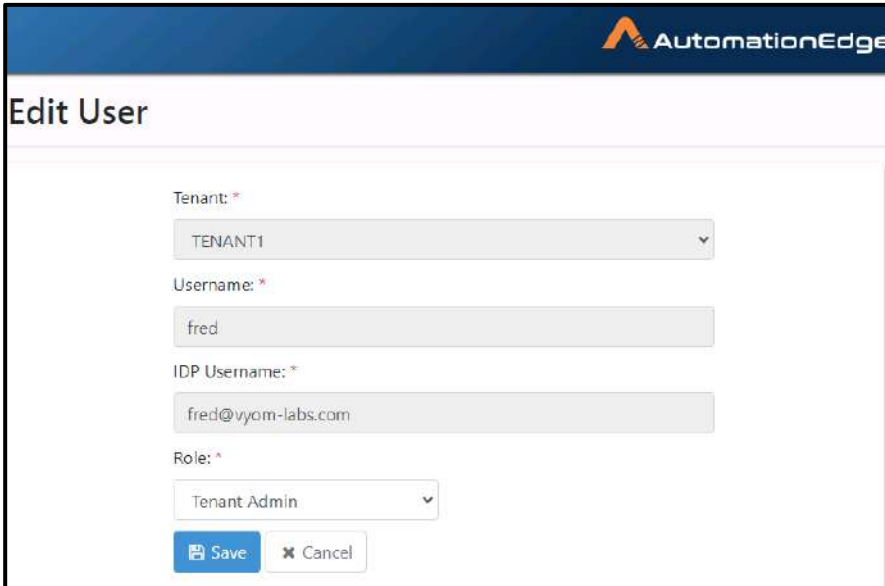
Redirect URL: **https://127.0.0.1:8443/aeui/index.jsp**

Logout Redirect URL: **https://127.0.0.1:8443/aeui**

[Edit](#) [Delete](#)

 **Note:** To generate Keystore and Self Signed or CA Certificate refer to section [2.9 Keystore and Certificate Generation](#)

48. An AutomationEdge SSO user is created as seen below.



AutomationEdge

Edit User

Tenant: *
TENANT1

Username: *
fred

IDP Username: *
fred@vyom-labs.com

Role: *
Tenant Admin

49. On AutomationEdge Login page click 'Sign In with SSO'.



AutomationEdge

AI DRIVEN INTELLIGENT ENTERPRISE RPA

- Unified Automation Platform for both Business and IT Operations
- Automate every department : front office, back office, middle office and IT operations
- Faster RPA product, Fastest Spreadsheet processing

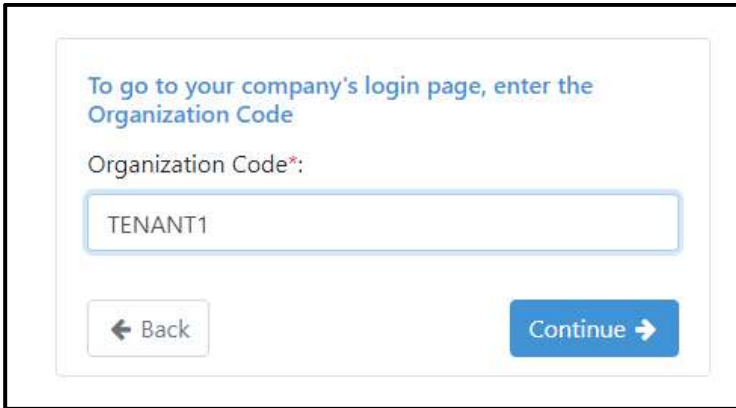


Enter Username
Enter Password

[Forgot Password](#) [Sign In with SSO](#)

© 2019-20 AutomationEdge. All Rights Reserved.

50. Provide Organization code as below.

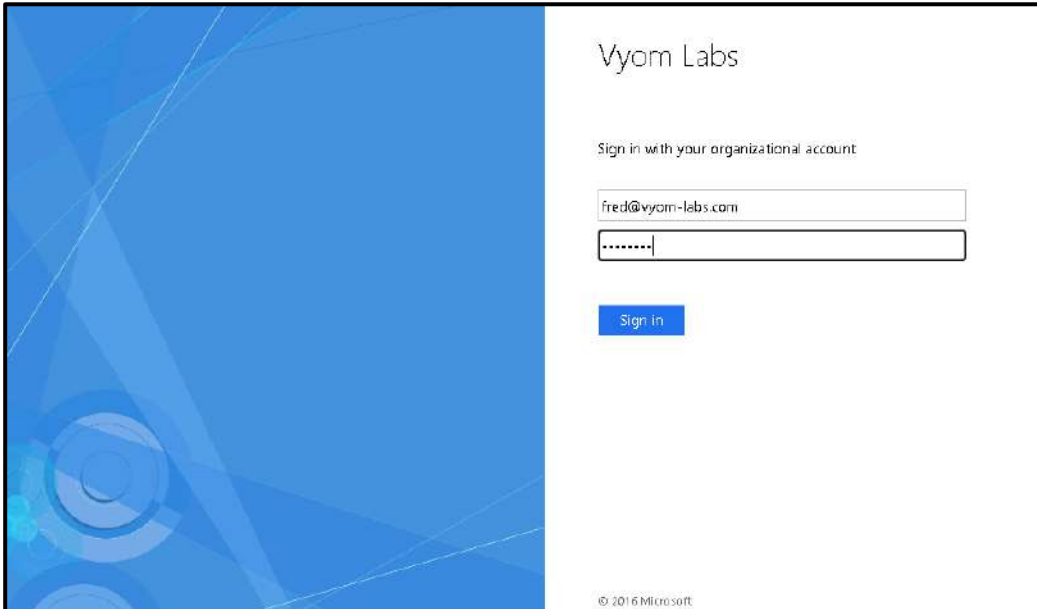


To go to your company's login page, enter the Organization Code

Organization Code*:

← Back Continue →

51. It takes you to the ADFS login page the first time you login.



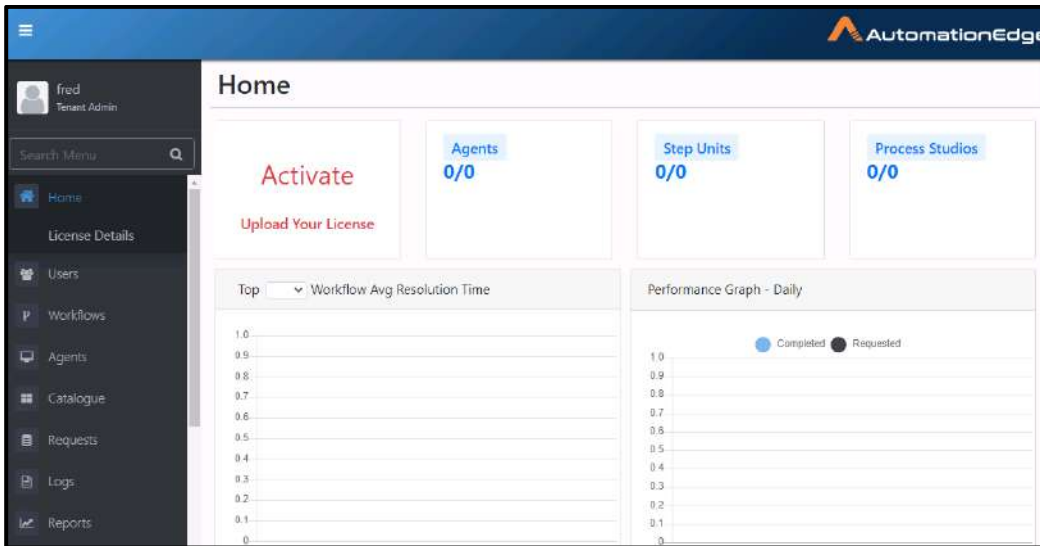
Vyom Labs

Sign in with your organizational account

Sign in

© 2016 Microsoft

52. The following screen shows we have logged in to AutomationEdge with SSO user fred.



53. This completes the process of AutomationEdge initiated Single Sign-On with ADFS using SAML protocol.

2.9 Keystore and Certificate Generation

In this section we have showcased the following methods of Certificate generation. You may choose the method as per your need.

- Generating Self-Signed Certificate
- Generating CA signed Certificate

2.9.1 Generating Self-Signed Certificate

Generate a self-signed Certificate for xml signature verification purposes.

A Java KeyStore (JKS) is a repository of security certificates – either authorization certificates or public key certificates – plus corresponding private keys, used for instance in SSL encryption. Use a tool for public/private key generation.

- keytool is one of the utilities that can be used to generate a new public/private keypair in the default keystore file. Oracle has a good reference which can be accessed at - <https://docs.oracle.com/cd/E19798-01/821-1841/gjrgy/>

Perform the following steps,


- Execute the keytool command to generate a new keypair in the keystore file with keysize **2048**, signature algorithm **SHA256withRSA** and storetype **PKCS**.
- The generated keystore file contains both private and certificate information. For IDP we need only certificate information, so extract the certificate information from the keystore file by executing the export command.
Execute the command to export the keystore (keystore.jks) to extract the certificate information into a file (<filename>.crt). Make sure that you add the same alias and password for the command to extract the certificate, as was used for keystore generation.

Upload the generated file keystore.jks file on AE UI SSO configuration settings and the certificate information file (e.g. client.crt) file on IDP configuration settings.

2.9.2 CA Signed Certificate

Configure Tomcat with TLS(HTTPS), refer to

- The Apache Tomcat documentation, <https://tomcat.apache.org/tomcat-9.0-doc/index.html>.
- Apache Tomcat SSL/TLS Configuration, <https://tomcat.apache.org/tomcat-9.0-doc/ssl-howto.html>

 **Note:** During TLS configurations while generating a new keypair in the keystore file make sure to generate it with keysize **2048**, signature algorithm **SHA256withRSA** and storetype **PKCS**.

Upload the generated file keystore.jks file on AE UI SSO configuration settings and the issued certificate file (<filename>.crt or any file type supported by IDP) on IDP configuration settings.



Contact

AutomationEdge Technologies Inc



General: info@automationedge.com

Support: support@automationedge.com

Trainings: training.support@automationedge.com



Website: <https://automationedge.com>



India: +91-20-6632-1000

USA: +1-281-220-1057