AUTOMATION ANYWHERE ENTERPRISE 11.1.2

Control Room - User Guide

Product Version	11.1.2
Document Version	1.0
Date of Publication	6/19/2018
Update(s) to Document Edition	First Edition

Getting started with Control Room

Here are some resources to help you get started with Control Room.

- Control Room overview
- Control Room interface
- Configuring Control Room for the first time
- Logging on to Control Room
- Adding users to your installation of Control Room
- Assigning roles to the users you have created

Control Room overview

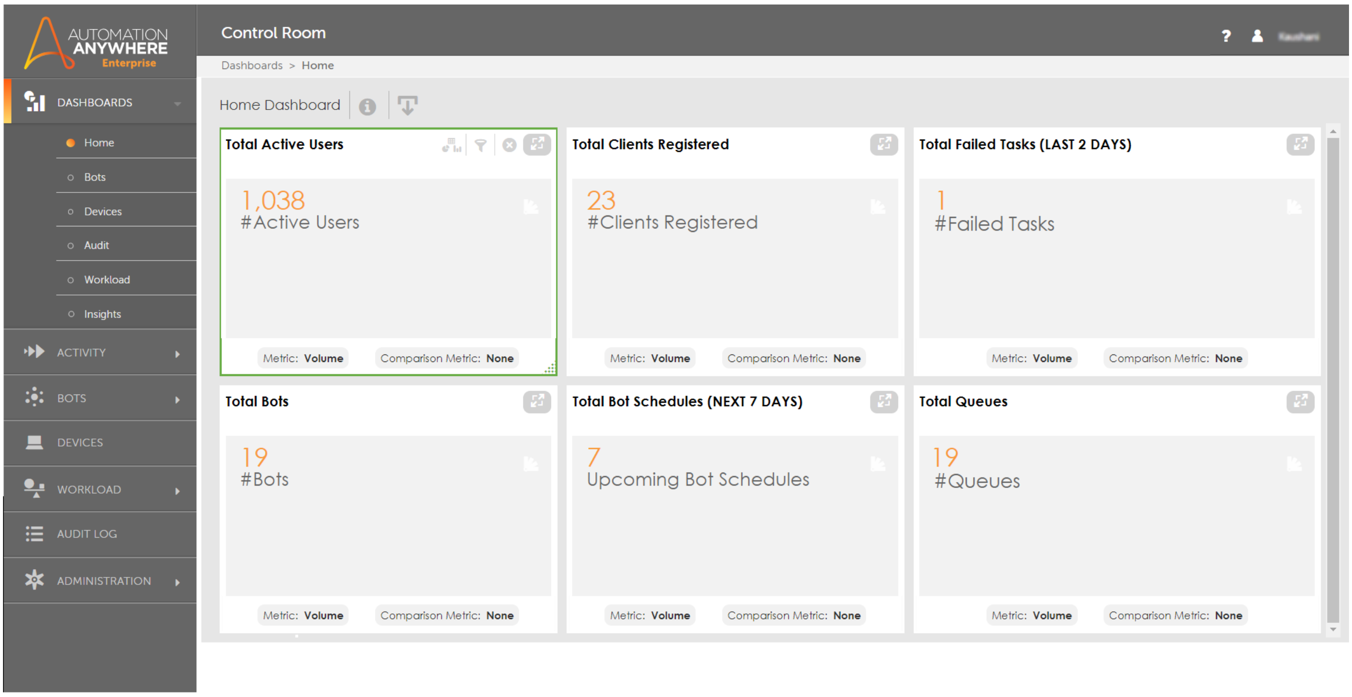
Automation Anywhere's Control Room is a central interface that allows you to manage and monitor all the processes of your RPA infrastructure. In a nutshell, it allows you to manage your bots, monitor activities, create and manage users and roles, monitor connected and disconnected devices, view audit logs, schedule when to run bot, and many more.

Features

- View task relevant activities using the Dashboard
- View the history, tasks in progress and the tasks and activities carried out in control room using the Activity page.
- Manage the automation (bot) files repository and schedule or run tasks using the Bots page
- Manage credentials and lockers using the Credentials page.
- View and manage the statuses of devices using the Bot runners and bot creators page.
- View schedule details using the Scheduled activity page
- Manage various work items using Workload management page
- View recent activities of users and administrators using the Audit Log page.
- Create new and manage existing roles using the Roles page.
- Manage and configure users (client and administrator), assign roles and licenses using the Users page.

Some other features enable you to:

- Manage your own profile details using the profile tray
- Configure CR settings for VCS, SMTP etc.
- Configure email notification to notify users on important events and activities
- Configure version control to enable controlled edits to the bots
- Set up different authentication types - AD, Kerberos and Non-AD

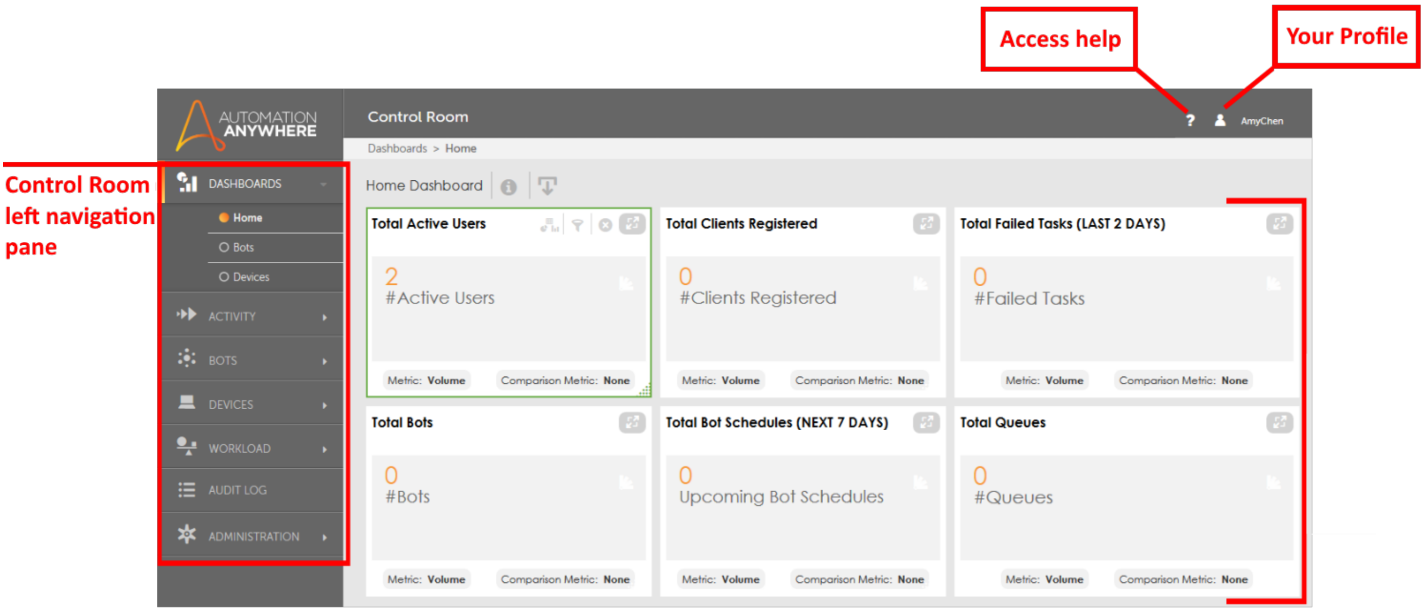


Benefits

- Simplified and improved monitoring and administration of large multi-site complex automation infrastructure using the web based control room.
- Access and manage tasks, clients, and users from anywhere, anytime.
- Monitor task progress and status to enforce internal compliance regulations, as well as prevent tampering with mission-critical processes.
- Facilitate an environment for increased collaboration to optimize productivity.
- Accommodate scaling of multiple users and Client environments (machines).
- Enable an environment to enforce controlled edits using SVN.
- Facilitate uploading and downloading of MetaBots and MetaBot enabled tasks. .
- Facilitate uploading and downloading of IQBots with Vision Skills.
- Provide role-based access to credentials
- Responsive web design helps to run the application in multiple devices such as tablets

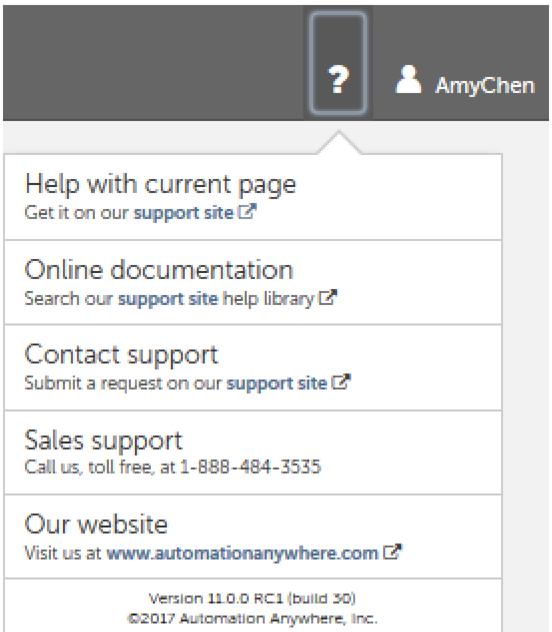
Control Room interface

The interface of Control Room gives you several options to manage and monitor the different components of your RPA infrastructure. This is illustrated in the following figure.



- **Control Room left navigation pane:** This is the first level of navigation. This area on the left holds the components of Control Room. These are Dashboards, Activity, Bots, Devices, Workload, and Administration. The views differ from user to user depending on the assigned roles, permissions, and rights.
- **Details area:** This is the second level of navigation. Depending on the page you are on, it displays a detailed list of users, roles, and bots. It provides you options to perform various actions like create, edit and delete on single or multiple records at a time. It also indicates the current page level in the breadcrumbs at the top. You can use this to navigate back to your previous view.
- **Your profile:** This area allows you to make changes to your profile. This includes changing your password and editing your personal details, such as first name, last name, and e-mail address.

- **Access help:** Clicking this displays a help menu, as shown in the following figure.



This provides you with links to the following resources.

- Help with the page you are currently on
- Access our online knowledge base
- Get support from the Automation Anywhere support team by submitting a support request on our support site
- Call the Automation Anywhere sales team for Sales inquiries
- Visit Automation Anywhere's Website

Log on to Control Room

To log on to Control Room, double-click the Automation Anywhere Control Room icon on your desktop.

The log on screens are different for Control Room hosted in Active directory/Kerberos and Non-Active directory modes. These are explained in the following sections.

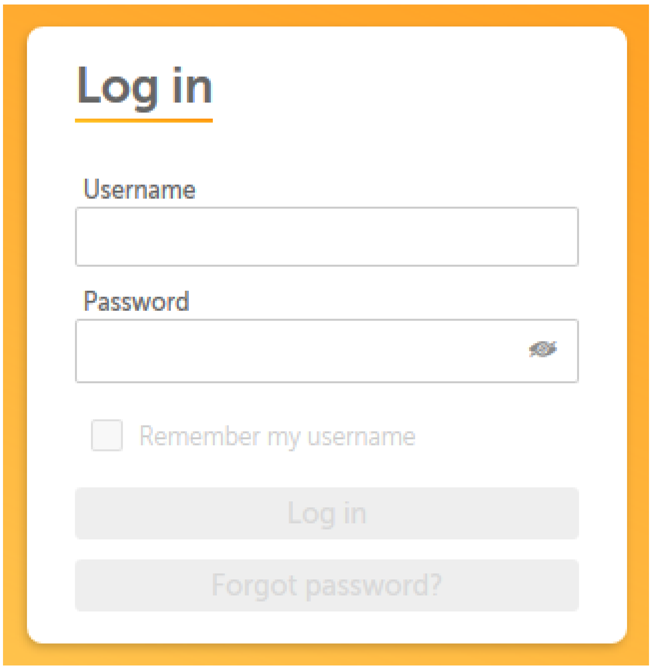
- Log on to Control Room hosted in Active Directory/Kerberos mode
- Log on to Control Room hosted in Non-Active Directory mode
- Log on to Control Room hosted in Single Sign On mode

Note: Control Room does not allow multiple sessions to the same account at the same time.

Log on to Control Room hosted in Non-Active Directory mode

To log on to Control Room hosted in Non-Active Directory mode, perform the following steps.

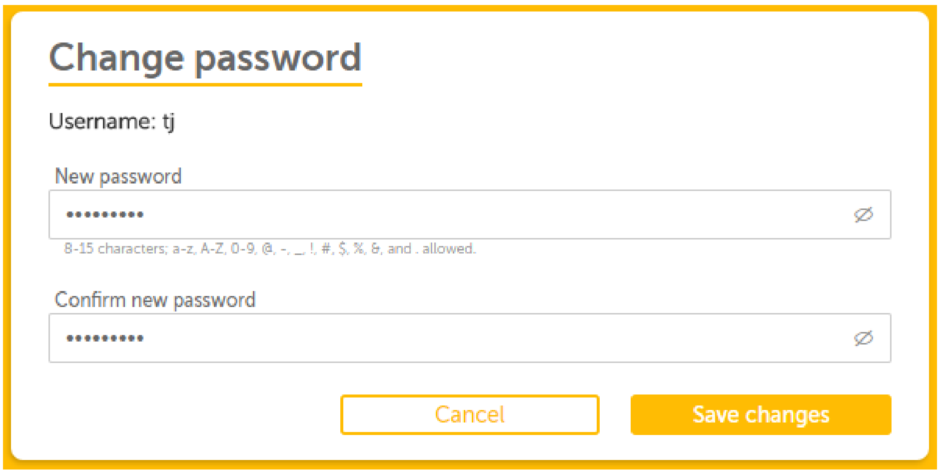
1. Double-click the Automation Anywhere Control Room icon on your desktop or type the Control Room URL on your Web browser and press the Enter key. The Log in screen is displayed.



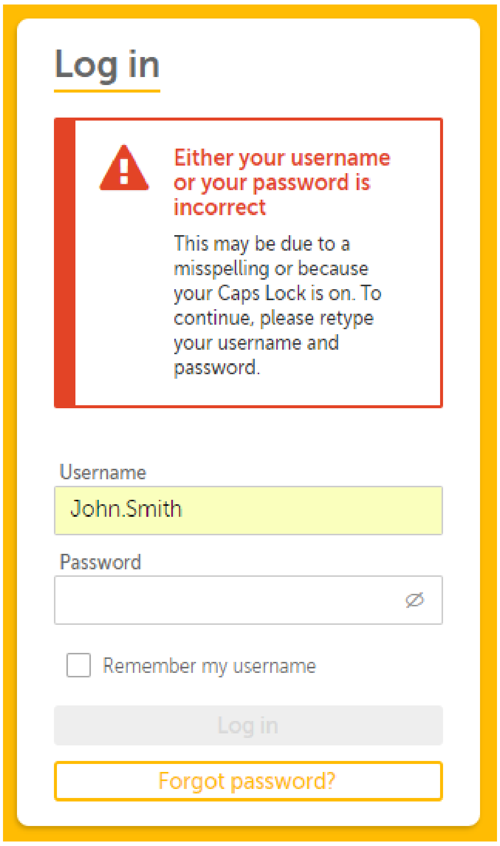
2. In the **Log in** area, do the following.
   - **Username:** Type your Automation Anywhere Enterprise (AAE) user name.
   - **Password:** Type your Automation Anywhere Enterprise (AAE) password to log on.
3. Once the **Log in** button is enabled, click the **Log in** button. The credentials are authenticated directly with CR database.

> **Note:** Your account will be locked if you enter the wrong password for a certain number of times depending on the password policy set by your administrator. For security reasons, failed log in attempts are audited, which allows the administrator to analyze and take appropriate actions.

- You can opt to select **Remember my username** if you want to quickly login to the Control Room.
- Click on **Forgot password?** to reset your password.
  - If you are an admin user, you will have to provide answers to the security questions that were configured during user creation. Once you provide correct answers, you are taken to the navigation page.
  - If a normal user, you are directly taken to the change password page:



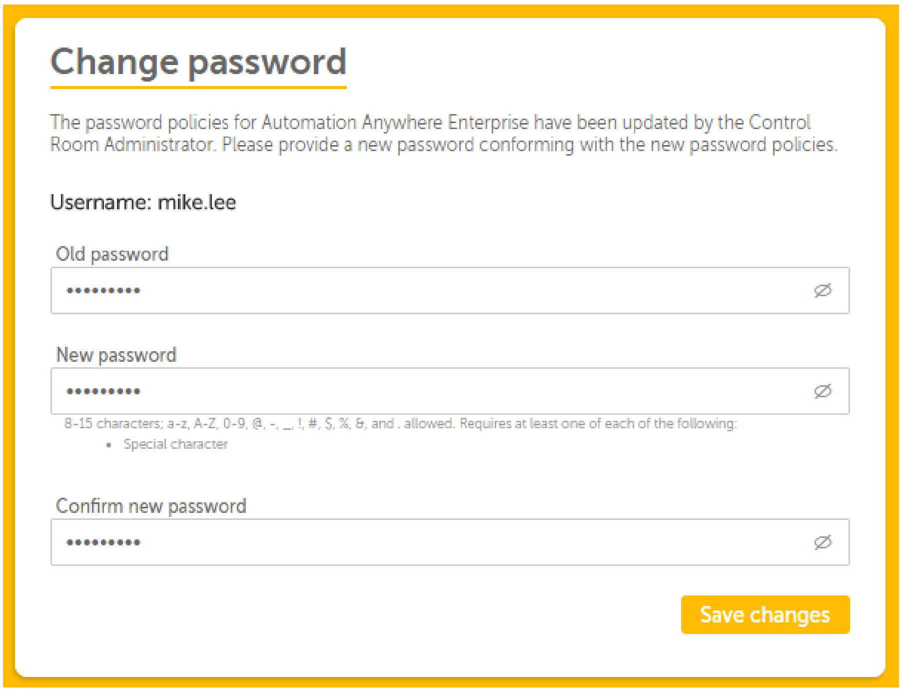
- If you provide incorrect credentials during log in, you are shown:



Re-logon to Control Room when password policy is updated

You will have to change your password when the the Control Room admin updates the password policy in Control Room Settings.

If the policy is updated, next time you login to the Control Room, the Change Password screen is displayed, wherein you can update your password:



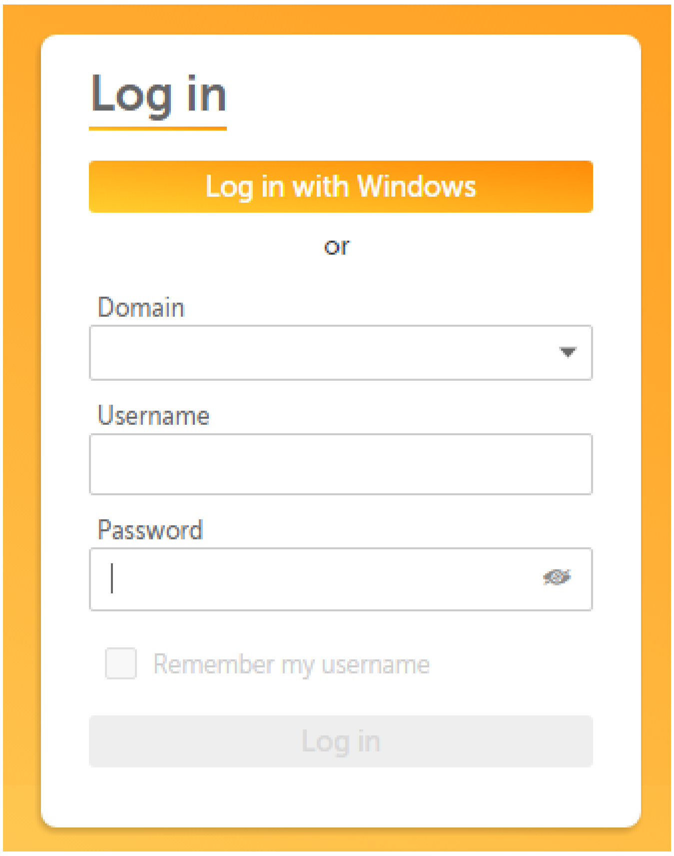
Click 

to login successfully.

Log on to Control Room hosted in Active Directory/Kerberos mode

To log on to Control Room hosted in Active Directory/Kerberos users, perform the following steps.

1. Double-click the Automation Anywhere Control Room icon on your desktop or type the Control Room URL on your Web browser and press the Enter key. The Log in screen is displayed.



2. In the **Log in** area, do the following.
   - **Domain:** Select the domain of the active directory. Note that Automation Anywhere Enterprise Control Room single forest multi-domain environment.
   - **Username:** Type your Active Directory user name.
   - **Password:** Type your Active Directory password.

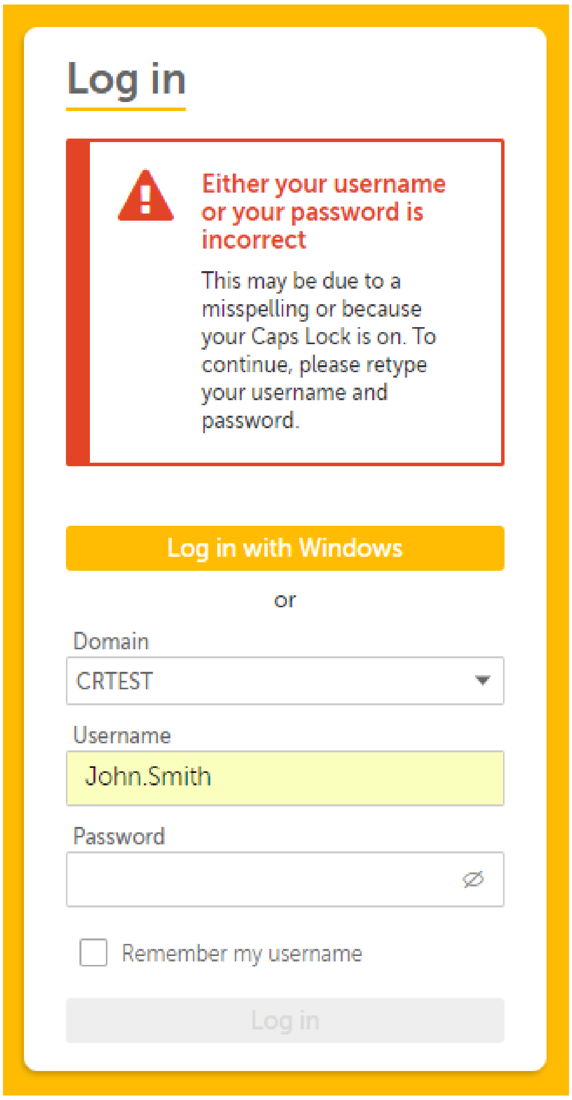
   > **Note:** For Kerberos installation, you do not need to enter your user name and password. Just click the **Log in with Windows** button and you will be logged in with your current Windows account.

3. Once the **Log in** button is enabled, click the **Log in** button. The log in details are authenticated directly with the Active Directory Domain Controller when you log in.

   Note that,

   - Your session will timeout in 20 minutes after you log in and the session is idle for that time period.
   - Multiple sessions of the same user account is not allowed. If you are logged in at one instance and later log to another instance, for example different browser on same machine or different machine, you are allowed to log in with new session. However, when you perform a new request in the earlier session, you will be logged out.

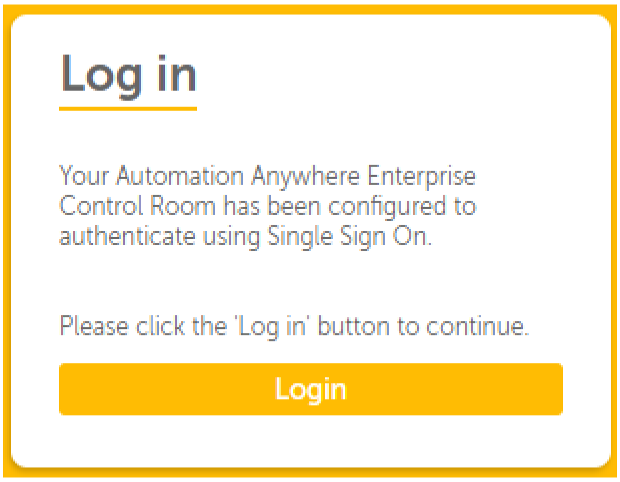
- If you provide incorrect credentials, you are shown:


Log in
Either your username or your password is incorrect
This may be due to a misspelling or because your Caps Lock is on. To continue, please retype your username and password.
Log in with Windows
or
Domain
CRTEST
Username
John.Smith
Password
Remember my username
Log in

Log on to Control Room hosted in Single Sign On mode

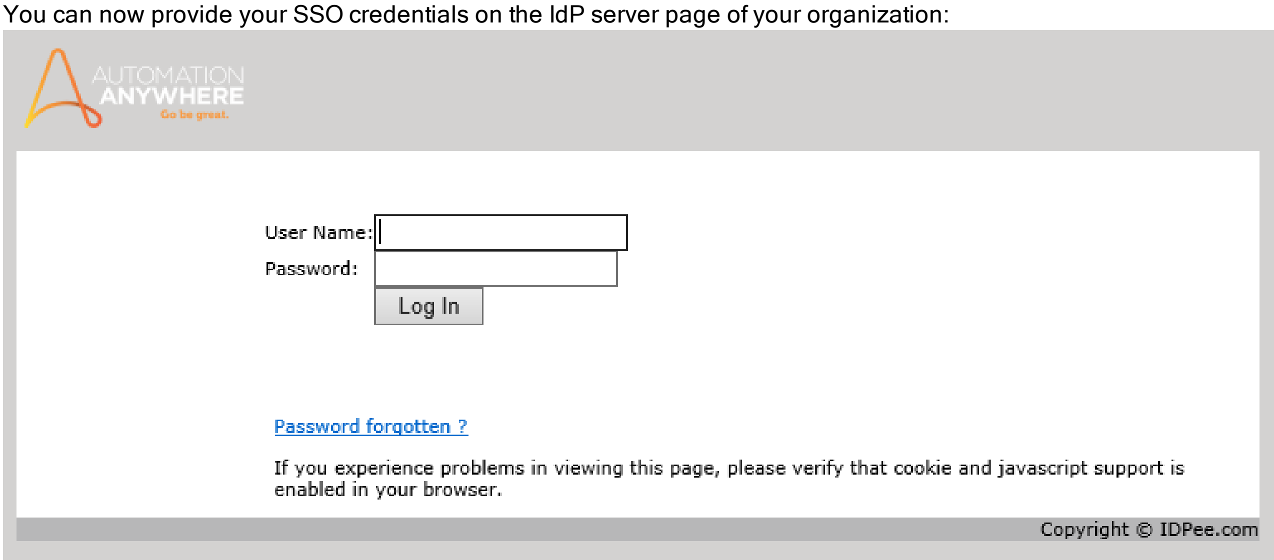
To log on to Control Room hosted in Single Sign On mode, perform the following steps:

1. Double-click the Automation Anywhere Control Room icon on your desktop or type the Control Room URL on your Web browser and press the Enter key. The **Log in** screen is displayed:

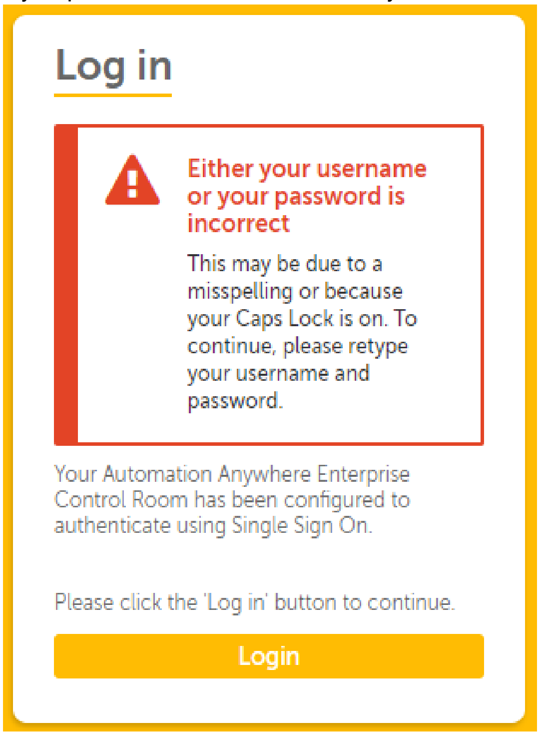


2. Click 

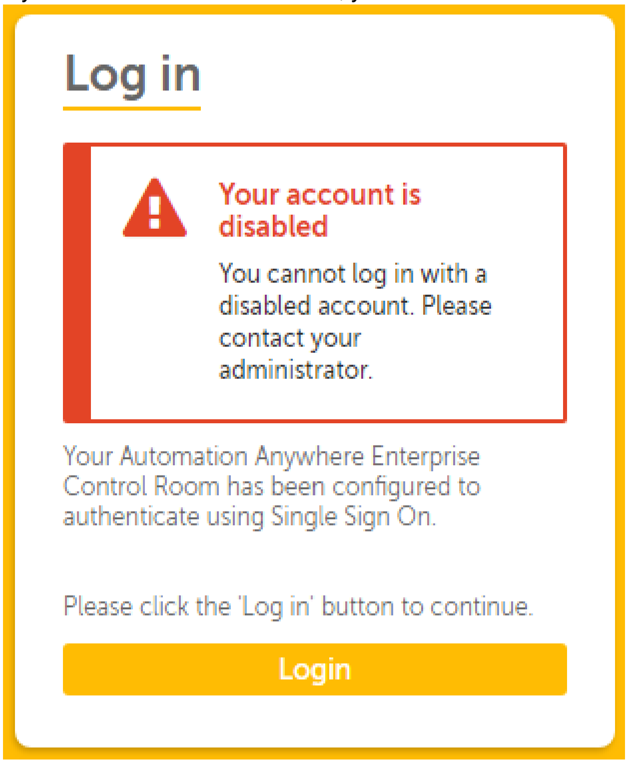
3. You can now provide your SSO credentials on the IdP server page of your organization:



4. Click Log In.
    - If you provide incorrect credentials, you are shown:

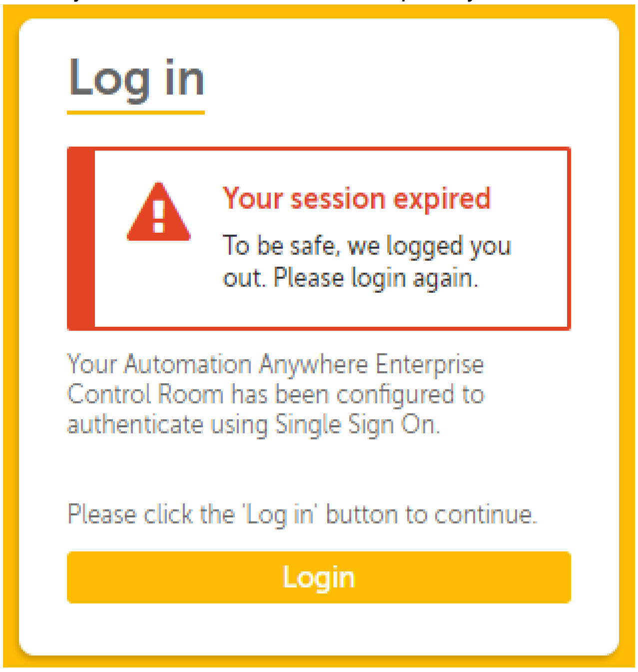


    - If your user account is disabled, you are shown:

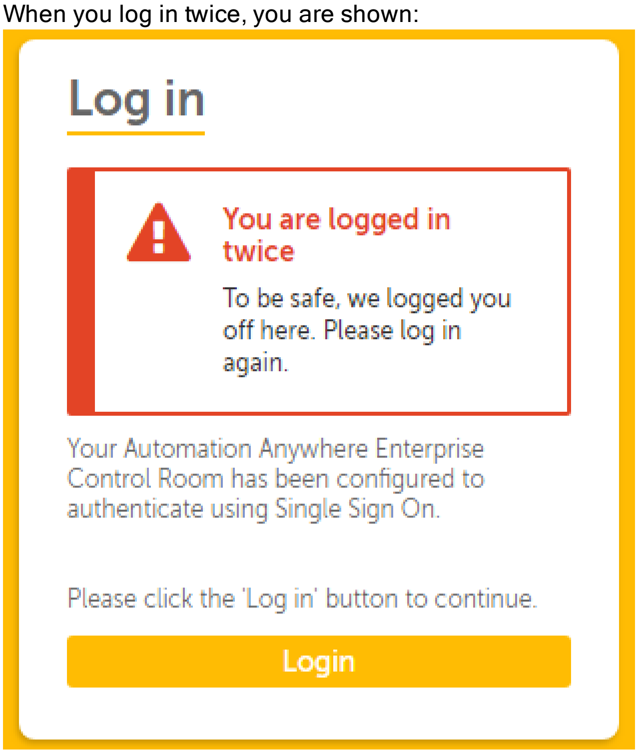


    - If the you input invalid IdP Server credentials, you will not be taken to the Control Room login page.
    - If the IdP Server URL is not valid or the server is down, you are shown appropriate message configured for it. For example, 404 or Bad Gateway.

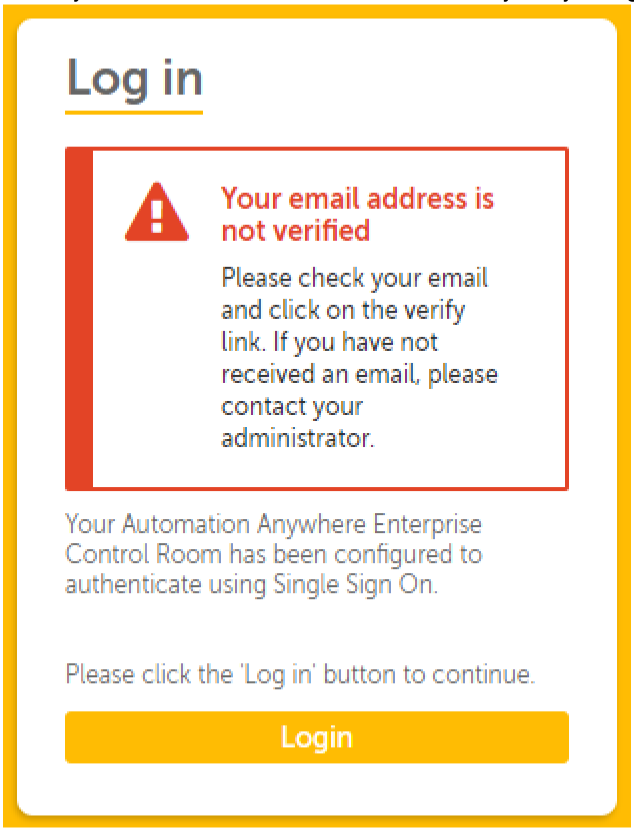
- When your Control Room session expires, you are shown:



- When you log in twice, you are shown:



- When your email address is not verified and if you try to login, you are shown



5. On successful authentication in the IdP server, you are logged into the Control Room.

> **Note:**
>
> - You are automatically logged into the Control Room if you open the Control Room in the same browser or refresh the page as you are already authenticated by the IdP server.
> - When you **Logout** (available when you click <username> in the profile) of the Control Room, you are not logged out of other applications running with the same IdP Server.

Refer Control Room Overview article for a summary on Control Room

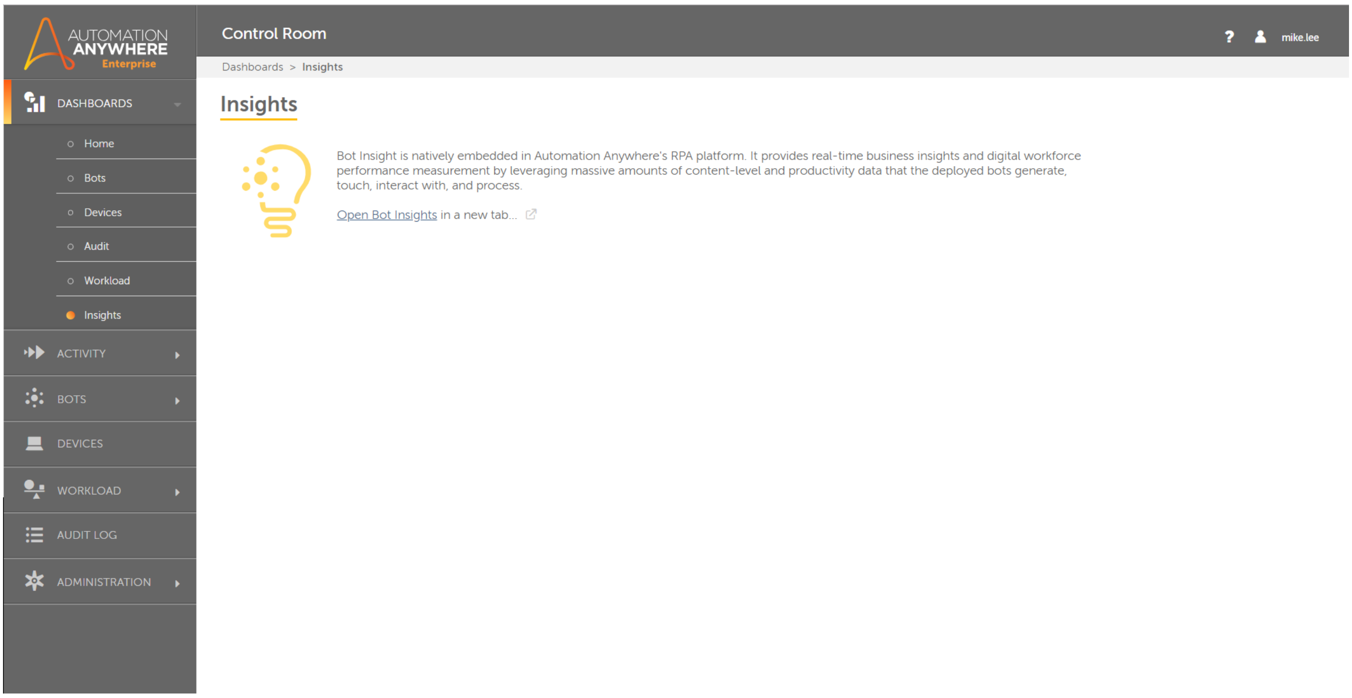
Log on to Bot Insights

Bot Insights helps automation experts to get real-time business insights and digital workforce performance measurement by leveraging massive amounts of content-level and productivity data the deployed bots generate, touch, interact with, and process. It helps the automation experts and consumers to interactively analyze task data and enhance widgets.

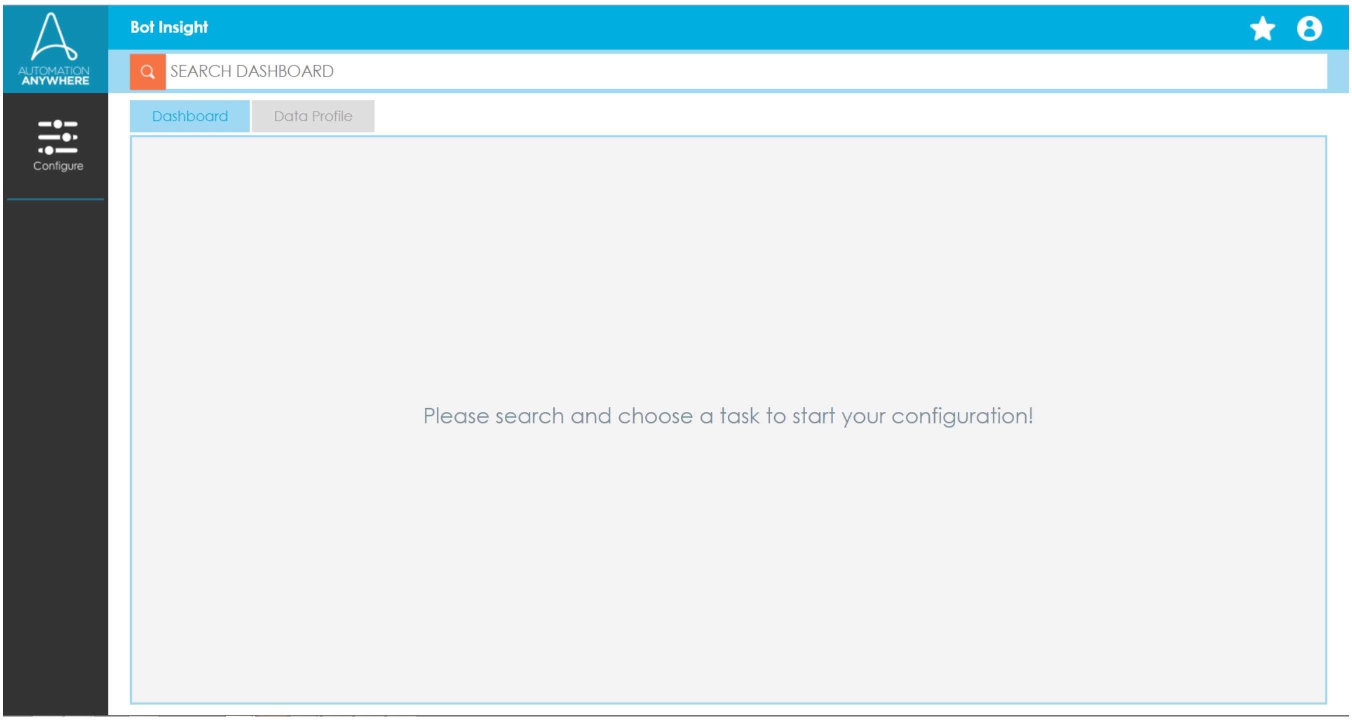
Single Sign-on

When you are logged into one component of Automation Anywhere Enterprise, you do not need to log into the other components. Single Sign-on automatically logs you into all the other components.

In the Control Room, on the left pane, click **DASHBOARDS → Insights**.

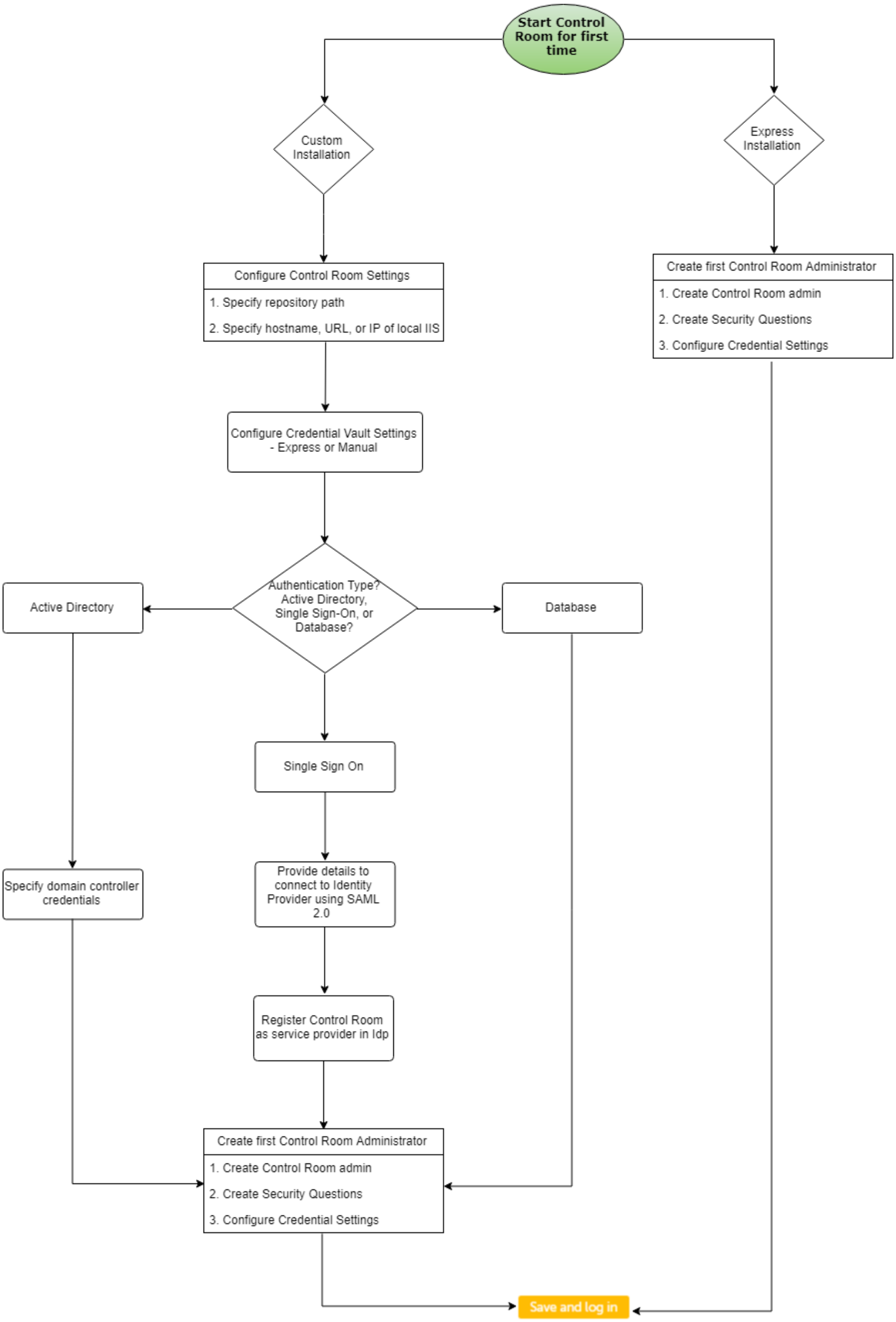


On the right pane, click on the **Open Bot Insights** link. The system opens the Bot Insights application in a separate tab without the need for you to login again into Bot Insights.



Configure Control Room for the first time

Once you have installed Control Room, you must configure it when you launch it for the first time. Depending on the mode of your installation of Control Room, the flow and the pages displayed to you are different when you launch Control Room for the first time. This is illustrated in the following figure.

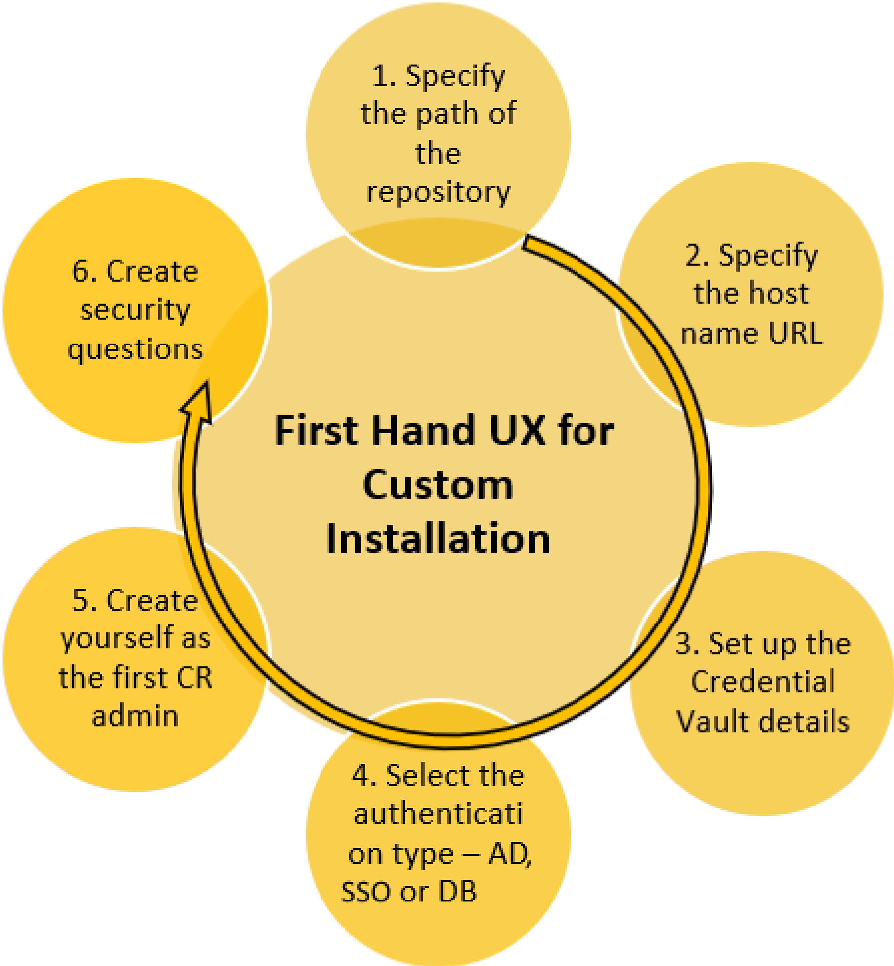


For more information on configuring Control Room for the first time, refer to the following sections.

- Configuring Control Room for the first time - Custom installation
- Configuring Control Room for the first time - Express installation

Configuring Control Room for the first time - Custom installation

A typical work flow for configuring Control Room installed in custom mode is illustrated in the following figure.

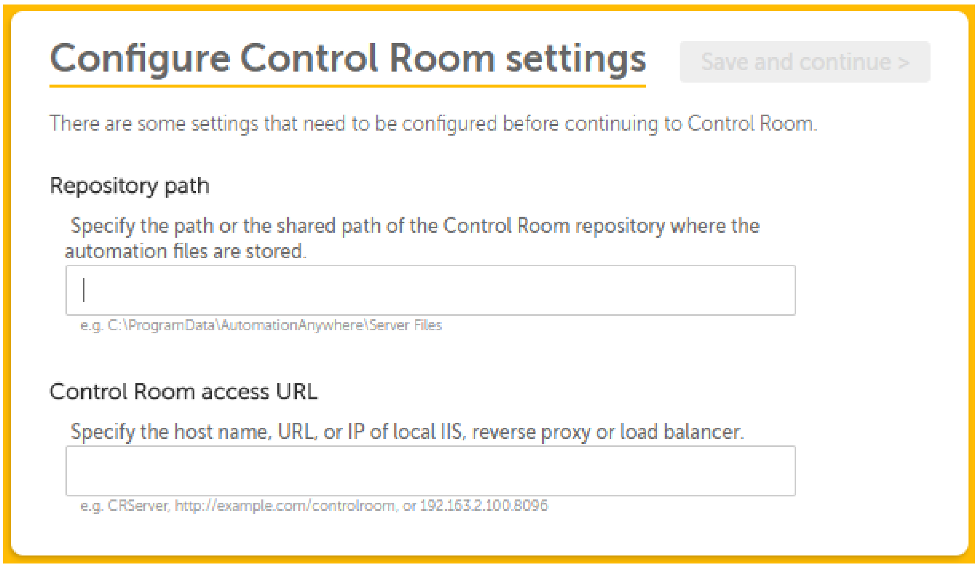


When you install Control Room in Custom mode, the getting started wizard guides you through:

1. Specifying the path of the repository - this is the location where the uploaded automation files, such as meta bots, IQ Bots, and task bots will be stored.
2. Specifying the host name URL - this is the URL that users will use to access your installation of Control Room.
3. Setting up the Credential Vault details
4. Selecting the authentication type - Active Directory, Single Sign-On or Control Room database
5. Creating yourself as the first Control Room administrator
6. Creating security questions in case you lose your password

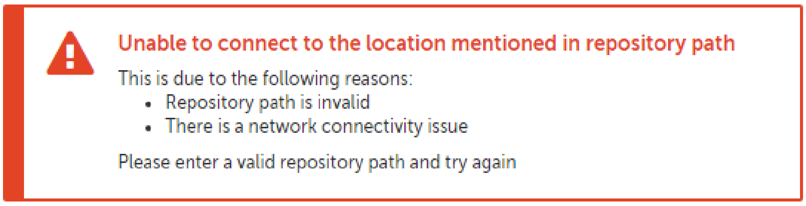
To configure Control Room when you start it for the first time for a custom installation, perform the following steps.

1. Double-click the Automation Anywhere Control Room icon on your desktop. The **Configure Control Room settings** page is displayed.



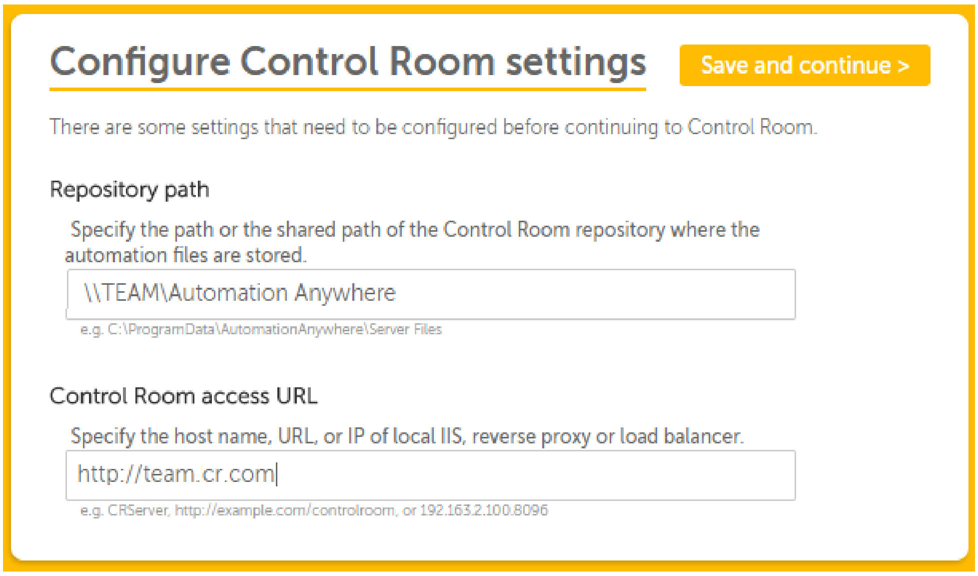
2. On the **Configure Control Room settings** page, do the following.
   - **Repository Path:** Type the location where the uploaded automation files will be stored. For example, Idap\\My-Server-\Server Files.

     > **Note:** If you do not specify the correct location, an error message is displayed, as shown in the following figure.

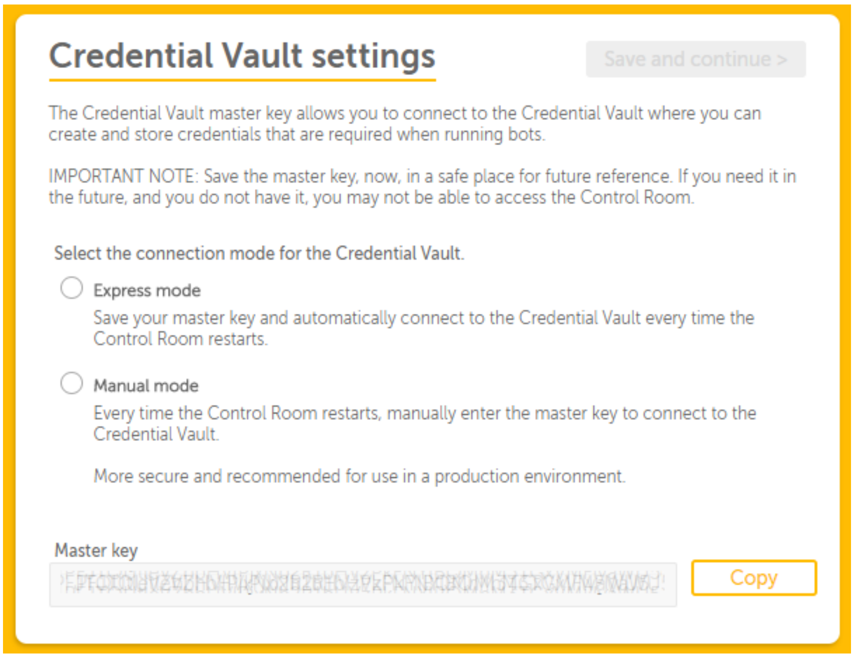
     

   - **Control Room access URL:** Type the URL that users will use to access your installation of Control Room.

> **Note:** This URL is the URL of the load balancer, which routes request to different Control Room instances



3. Once you have typed the **Repository Path** and **Control Room access URL**, click the **Save and continue** button. The **Credential Vault setting** page is displayed.



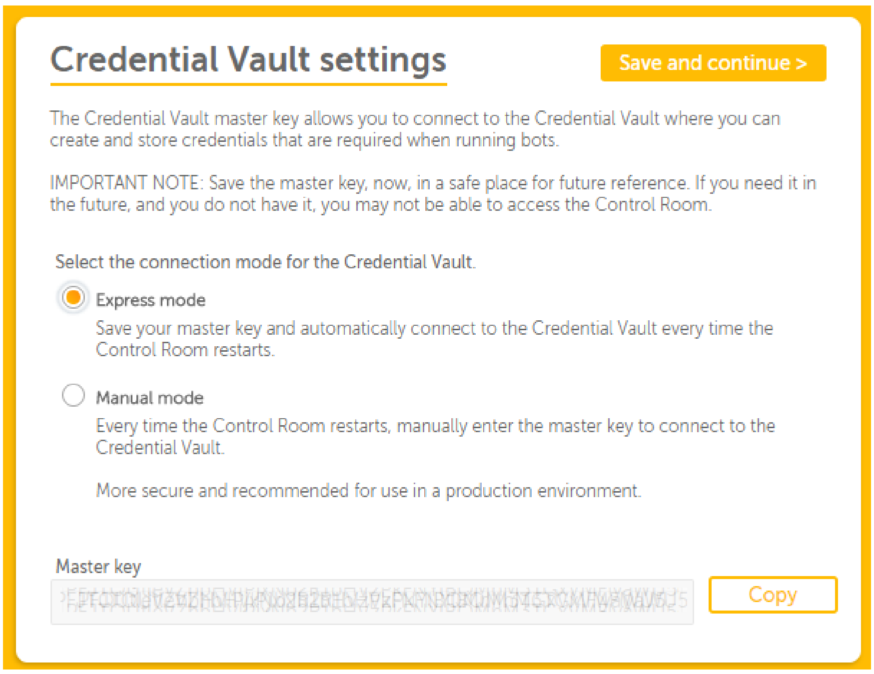
IMPORTANT: The back button of your Web browser is automatically disabled after you type the Repository path and Control Room access URL and click the Save and continue button. This is to ensure that the Credential vault master key that will be generated matches the repository path and Control Room access URL. To go back to the Configure Control Room settings page, press Ctrl+F5 on your keyboard and start over again.

Note: The **Save and continue** button is not enabled if the correct path or URL is not specified.

4. On the **Credential Vault settings** page, do the following.
   - **Express mode:** Select this option if you want the system to store your master key to connect to Credential Vault.

     Note: It is recommended that you do not use this option for a production environment.

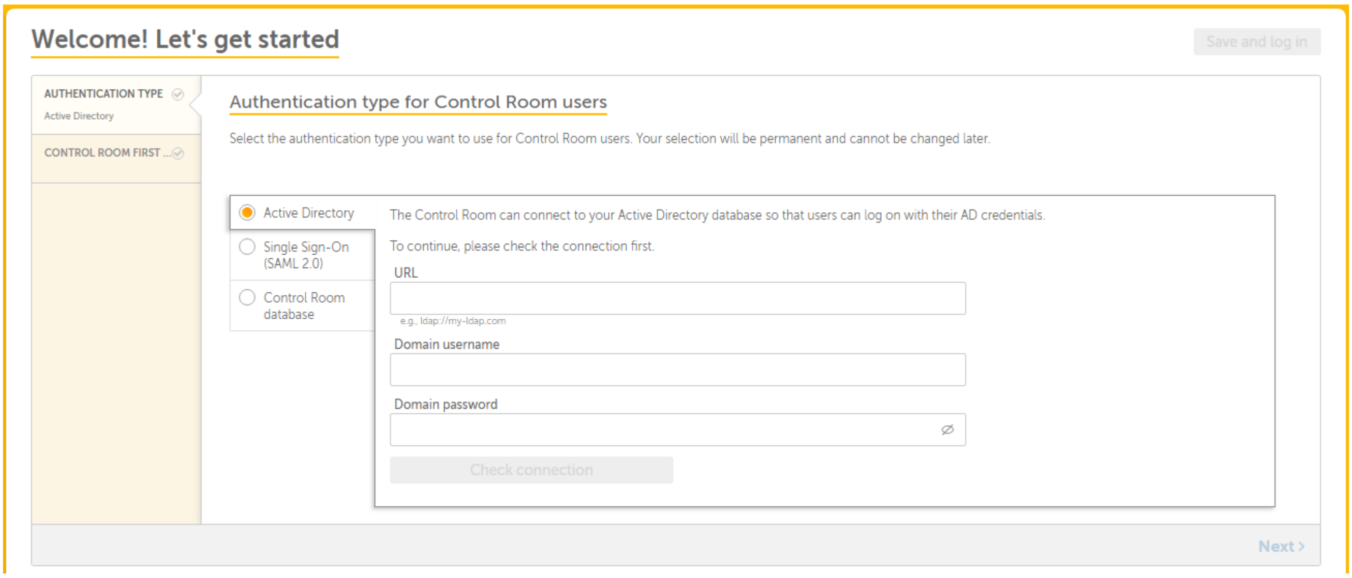
   - **Manual mode:** Select this option if you want to store the master key on your own. When you use this mode, you must enter the master key if the Credential vault is locked. The Master key is used to connect to the Credential Vault so that users can use the vault to secure their credentials and access it in their taskbots. Copy the master key to your Windows clipboard by clicking the **Copy** button and save it in a secure location.



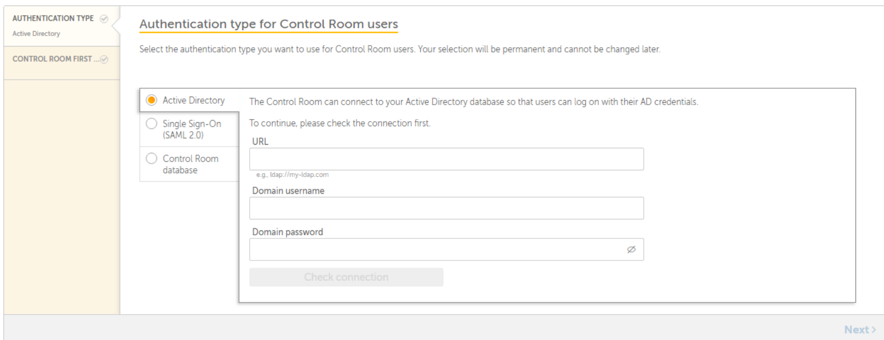
IMPORTANT: As an administrator, you must copy the master key to your clipboard and save it in a secure place. This key is required in the event that the credential vault is closed. If you lose the master key, your access to Control Room is locked.

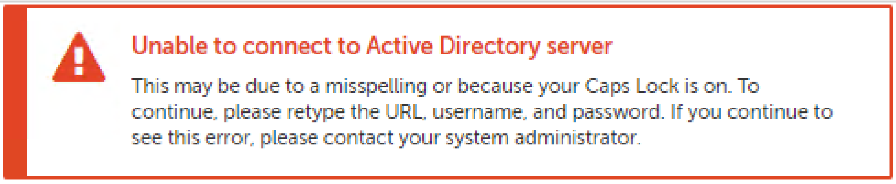
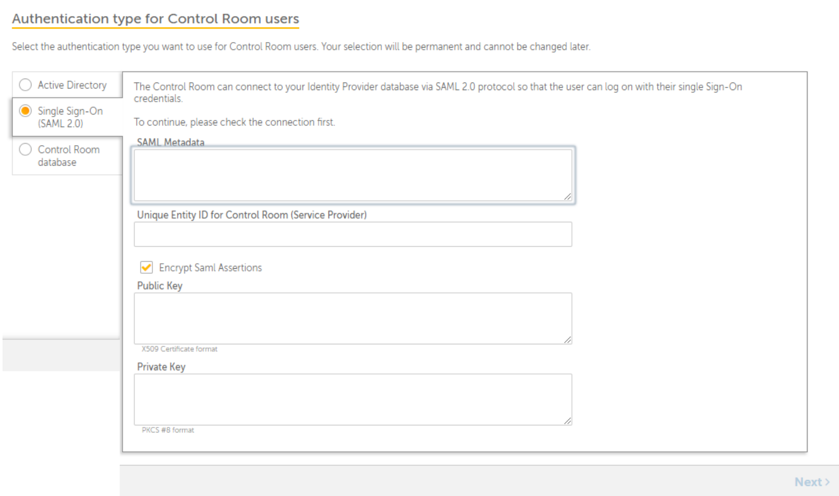
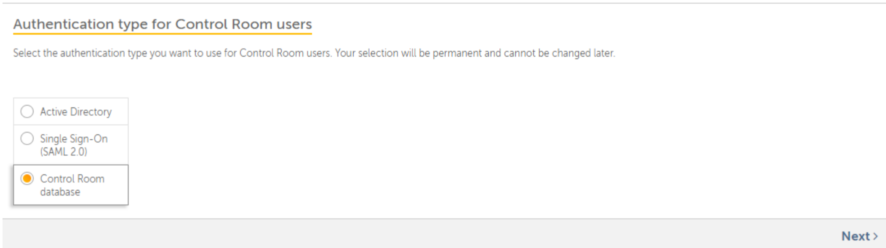
5. Click **Save and Continue**. The **Authentication type for Control Room users** page is displayed. Use this page to specify the type of authentication your Control Room users will use to log on to Control Room.

   IMPORTANT: The back button of your Web browser is automatically disabled after you click the Save and continue button on the Credential Vault settings page and you cannot make any further changes to the Control Room configuration or Credential Vault settings. To make changes, you must reinstall Control Room again.

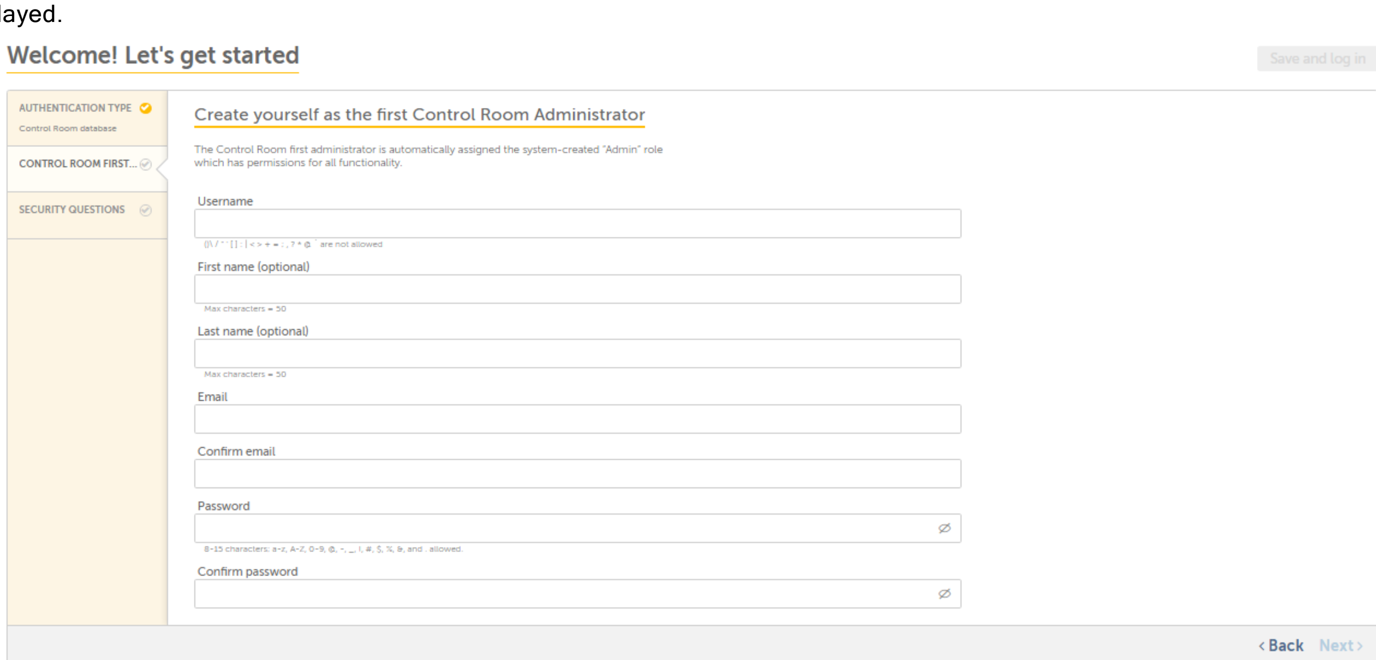


6. On the **Authentication type for Control Room users** page, do one of the following.

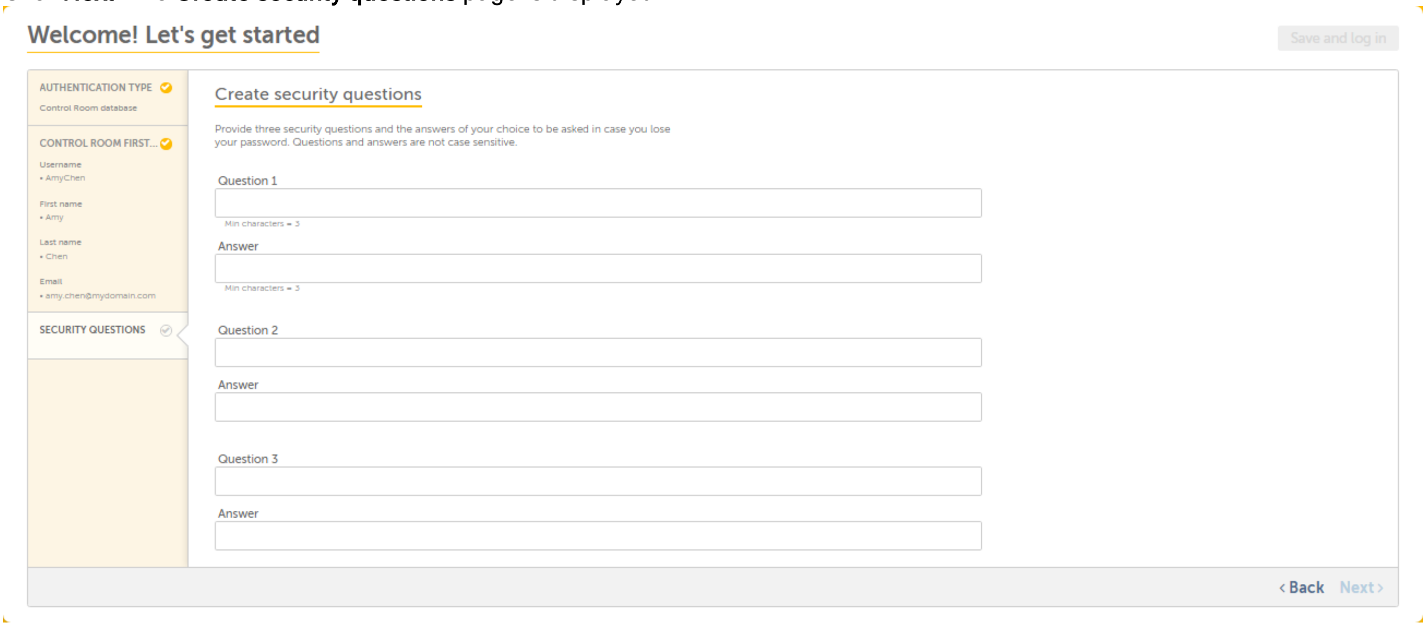
Authentication type	Description
Active Directory	Select this option if you want use Active Directory as the type of authentication. This allows users to log on to Control Room with Active Directory credentials. • **URL:** Type the LDAP URL. For example, ldap://my-ldap.com. This is the URL of the domain controller. • **Username:** Type the user name. This must be a user with domain controller rights (domain administrator.) • **Password:** Type the password for the user.  Type the details for the Active Directory and click the **Check connection** button. If Control Room is unable to connect to the Active Directory database, an error message is displayed, as shown in the following figure.

	
Single Sign On	Select this option if you want to use IdP server for authenticaton.  Refer Configure Control Room for Single Sign On for details.
Control Room database	Select this option if you want to use the Control Room database as the type of authentication. 

7. After selecting the type of authentication. Click **Next**. The **Create yourself as the first Control Room administrator** page is displayed.



8. On the **Create yourself as the first Control Room administrator** page, do the following.
   - **Username:** Type a user name for the administrator.
   - **First name:** Type the first name of the administrator. This is optional.
   - **Last name:** Type the last name of the administrator. This is optional.
   - **Email:** Type an e-mail address for the administrator.
   - **Confirm email:** Confirm the e-mail address.
   - **Password:** Type a password for the administrator.
   - **Confirm password:** Confirm the e-mail address.
9. Click **Next**. The **Create security questions** page is displayed.



10. On the **Create security questions** page, type three security questions and an answer to each. This will be used in case you forget your Control Room password.

> **Note:** Each question must be unique. Set questions and answers that are easy to remember.

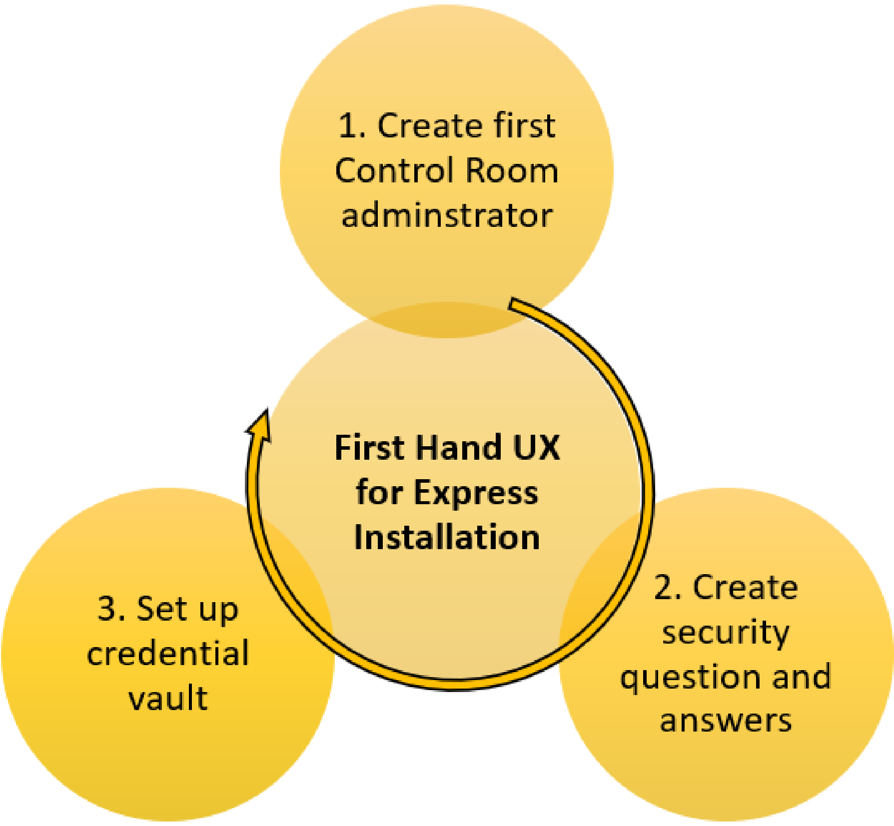
11. Click **Save and log in**. The first administrator user of your Control Room installation is created and you can now configure and manage your overall RPA environment with Control Room and its clients.

> **Note:** For a non-active directory environment, you will be directly logged on to Control Room. However, for an active directory environment, a login dialog is displayed.

Configuring Control Room for the first time - Express installation

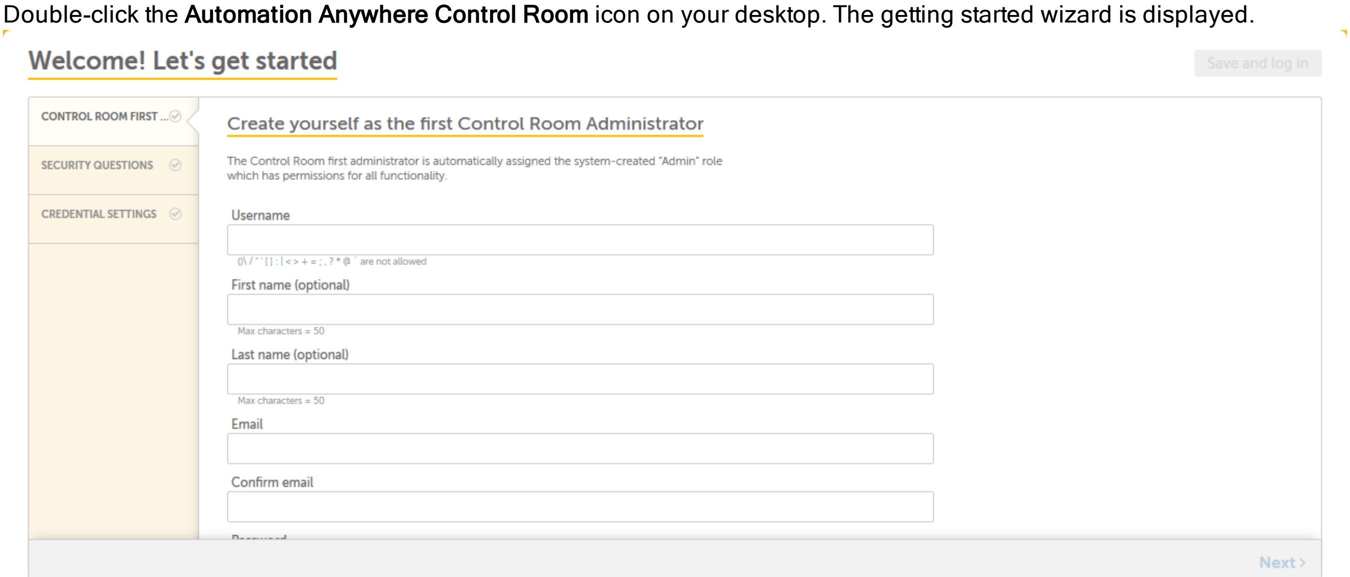
When Control Room is installed in Express mode, the getting started wizard guides you through:

1. Creating yourself as the first Control Room administrator so that you can configure and manage the overall RPA environment of your organization.
2. Creating three security questions in case you forget your password.
3. Setting up your Credential Vault master key.



To configure Control Room for the first time for an express installation, perform the following steps.

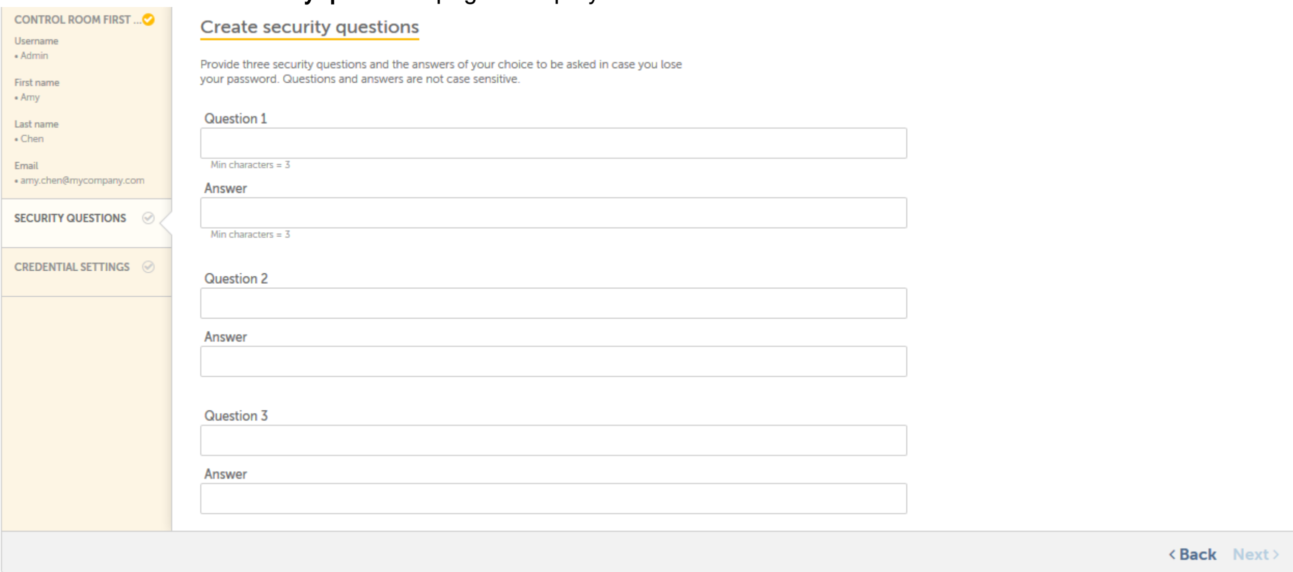
1. Double-click the **Automation Anywhere Control Room** icon on your desktop. The getting started wizard is displayed.



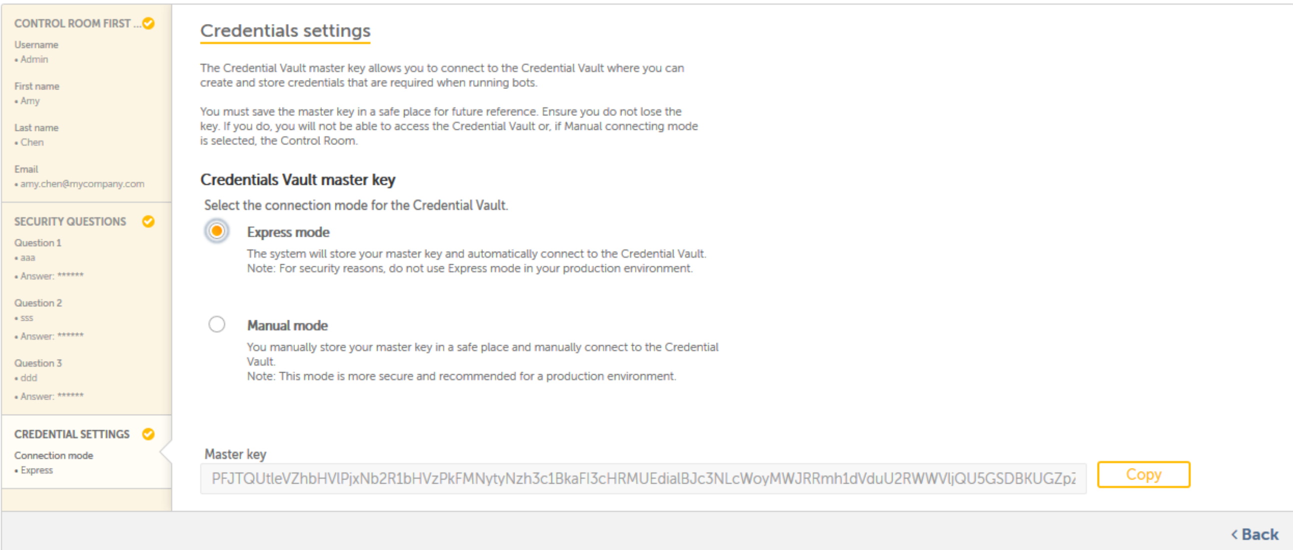
2. On the **Control Room First** tab, do the following.

- **Username:** Type a user name of your choice.
- **First name:** Type your first name (this is optional)
- **Last name:** Type your last name (this is optional)
- **Email:** Type your e-mail address.
- **Password:** Type a password.
- **Confirm password:** Type your password again to confirm.

3. Click **Next**. The **Create security questions** page is displayed.



4. On the **Create security questions** page, type three security questions and an answer to each. This will be used in case you forget your Control Room password.
5. Click **Next**. The **Credential settings** page is displayed.



6. Depending on your requirements, select the **Express mode** or **Manual mode** options.
The Master key is used to connect to the Credential Vault so that users can use the vault to secure their credentials and access it in their taskbots.

> **IMPORTANT:** As an administrator, you must copy the master key to your clipboard and save it in a secure place - use the **Copy** button to do this. This key is required in the event that the credential vault is closed. If you lose the master key, your access to Control Room is locked.

7. Click **Save and log in**. The first administrator user of your Control Room installation is created and you can now configure and manage your overall RPA environment with Control Room and its clients.

Configure Control Room for Single Sign-On

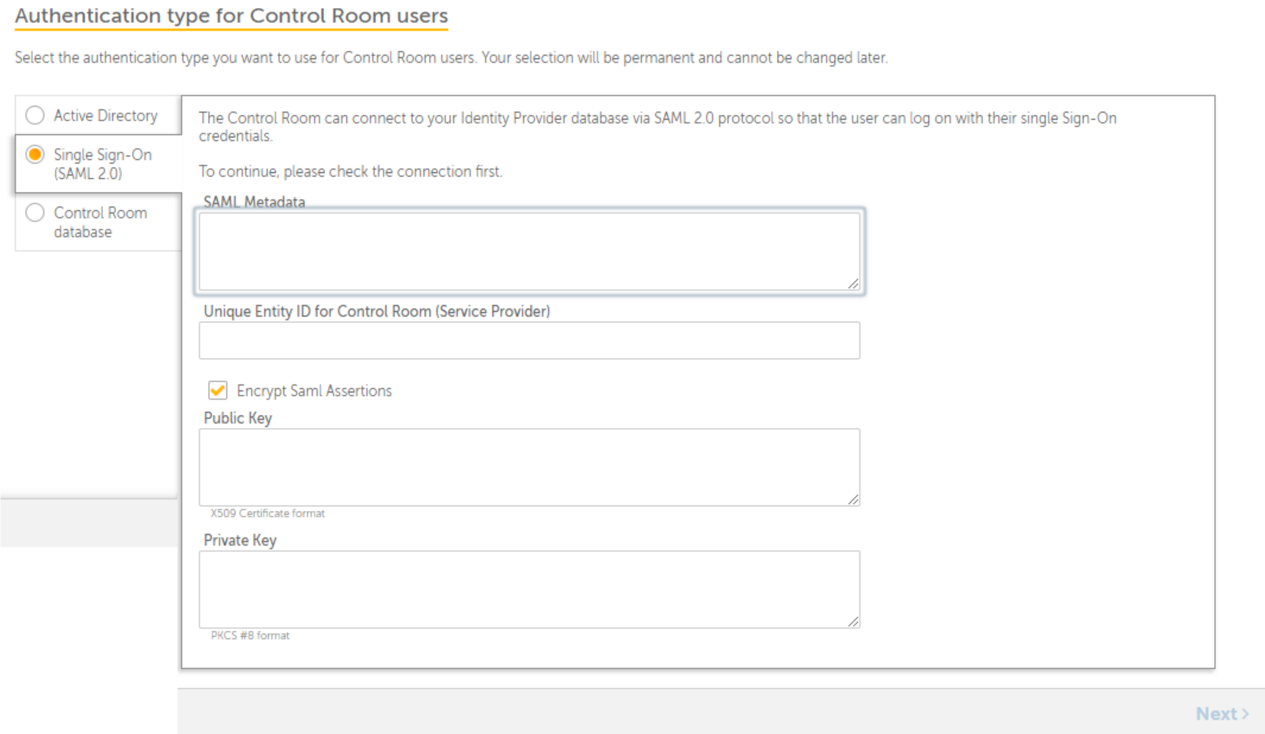
As a Control Room administrator, you can configure the Control Room instance for Single Sign-On (SAML 2.0) if your organization uses IdP server for authentication.

You can select this option once you have specified the repository path, host name URL, and Credential Vault details. Refer Configuring Control Room for the first time - Custom installation for details.

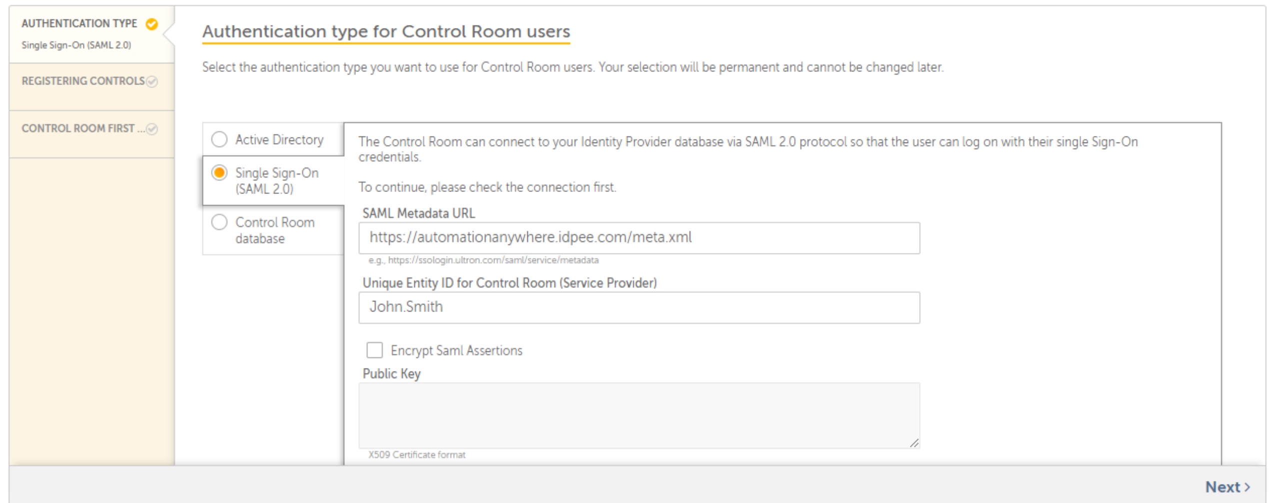
Steps to configure Single Sign-On authentication

Use the Single Sign-On option to allow your Control Room to connect to your identity provider database (Control Room) using SAML 2.0 protocol and log on using Single Sign-On.

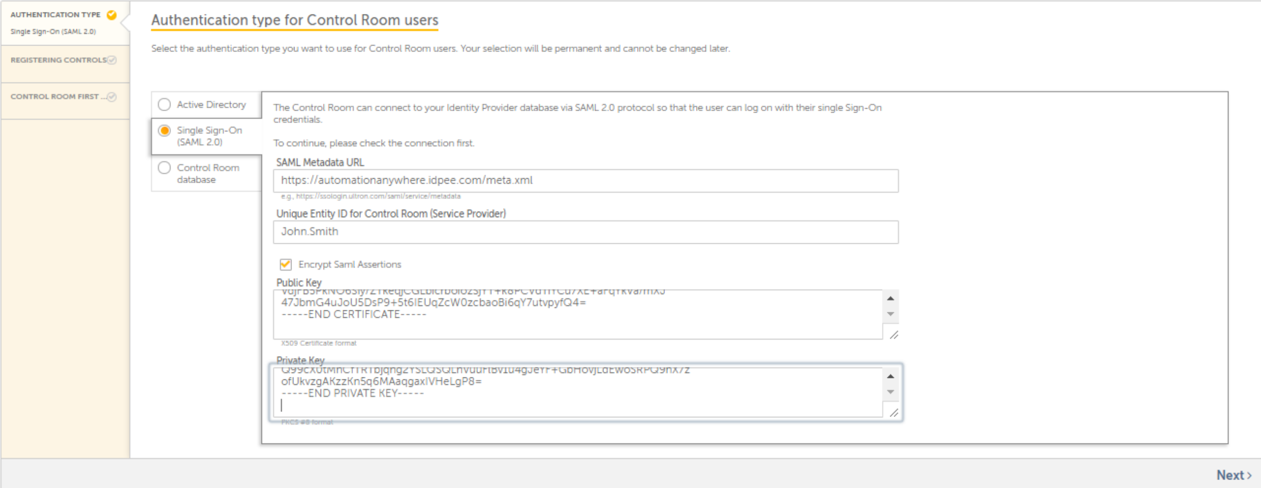
1. On the **Authentication type for Control Room users** page select Single Sign-On (SAML 2.0) option:



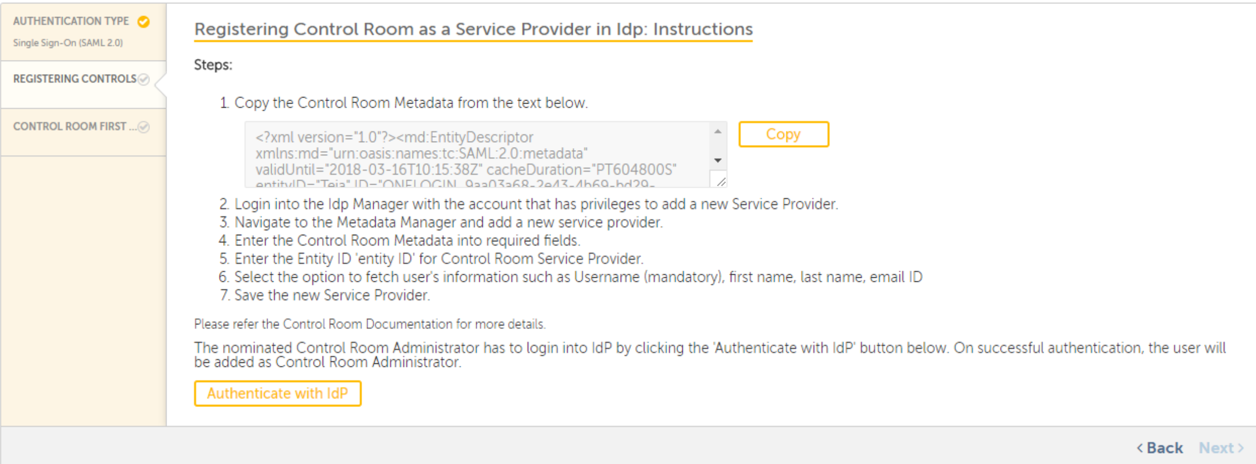
2. You need to check the connection to Control Room for which you need to provide SAML Metadata details.
3. Copy and paste the **SAML Metadata** from an xml file.
4. Provide the **Unique Entity ID for Control Room**. This is basically a user who is the Control Room admin and also has been given an admin role in the IdP Server.



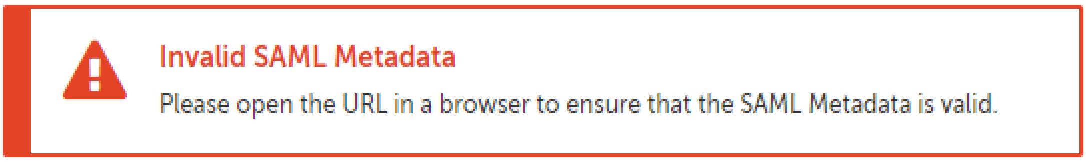
5. Optionally, select **Encrypt SAML Assertions** for enhanced security. For this you will be provided a public and private key by the system admin which you must copy and paste from relevant files.



6. Click **Next.** The **Registering Controls** panel is displayed wherein you need to register your Control Room as a service provider with the IdP.

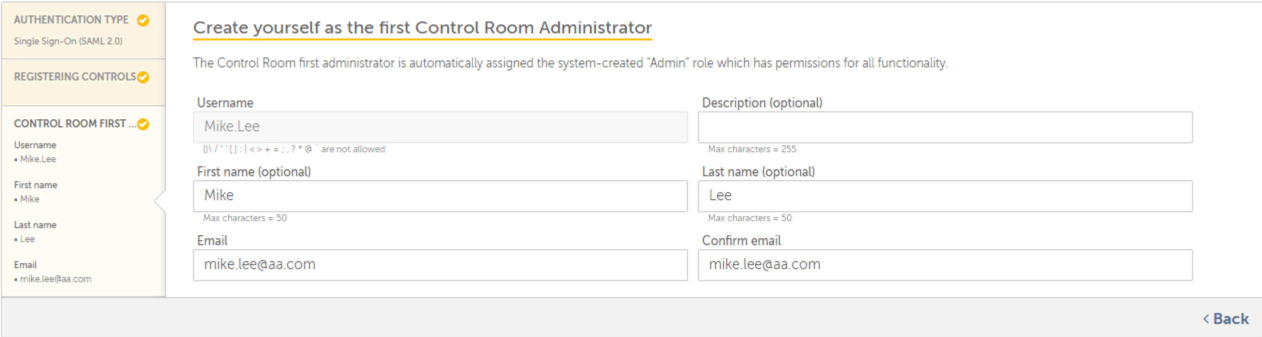


Note: If SAML Metadata URL that your provide is incorrect, you are given an error on this page:



7. To register the Control Room with IdP as service provider, follow the instructions given on the page. To summarize,
   a. Click **Copy** to copy the Control Room metadata to the IdP manager
   b. **Login** to the IdP server as admin or a user with privilege to add a service provider
   c. Click **Manage Metadata** to add a service provider
   d. Select **Attributes** for assertion
   e. Paste the **metadata** that you copied
   f. Click **Submit** to import data
8. Go back to Control Room configuration page
9. Click **Authenticate with IdP**
10. Leave the page to go to IdP login
11. Log on using credentials of the IdP user who provides the Control Room Service Provider credentials.

12. Once you are authenticated, log out of the IdP server. This will take you back to the Control Room First Admin page wherein you can create your first control room admin.

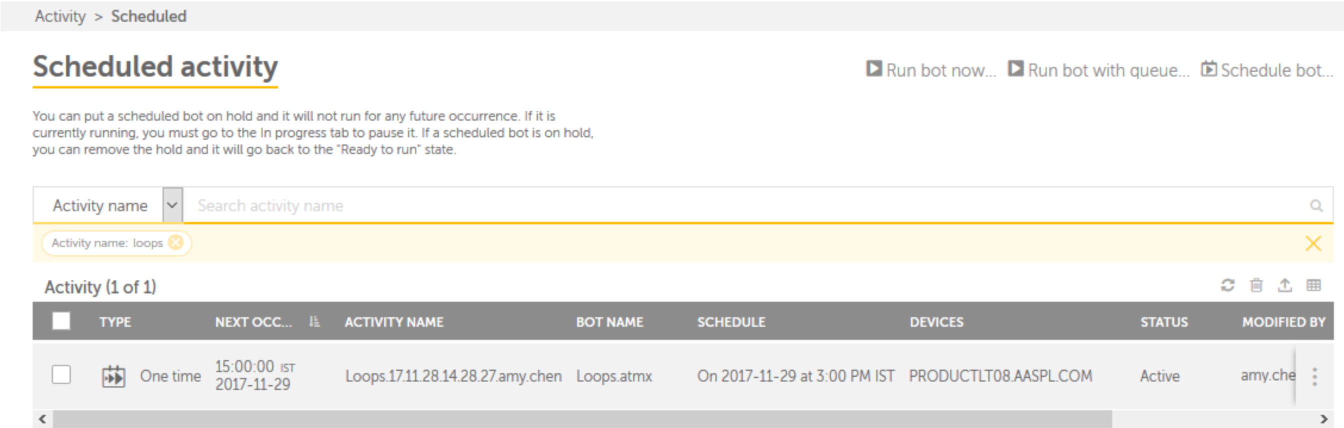


Search and filter data

The search feature in Control Room allows you to search for the information that you are looking for thereby helping you work efficiently. It provides you dynamic suggestions as you type. For example, if you type 'CRM', the suggestion narrows down with every additional character that you type - this suggestion is based on the existing values already available in the database. The count of the auto-populated search terms are displayed and the data is dynamically updated. The search results are displayed in the format of **X of Y**, where:

- X = search result
- Y = total number of records in table

Besides this, you can also reset the search query and Control room remembers the last filter applied by each user per session. The following figure illustrates a search result for the **Scheduled activity** page.



You can use the search feature in the following pages of Control Room.

- Activity tab
- Bots tab
- My bots tab
- Individual folders
- Credentials
- All credentials
- Individual lockers
- Devices tab
- Bot runners and bot creators
- Device pools
- Bot farm images
- Workload tab
- Queues
- Audit log
- Administration
- Users
- Roles

Profile Management

User profiles in Control Room are created by administrators who can change your first name, last name, password, and role depending on the business requirements. If you are a user of Control Room configured with a non-directory environment, you can change the following details of your profile.

- Your password
- Your first name
- Your last name
- Your e-mail address

To personalize and maintain your Control room profile, refer to the following sections.

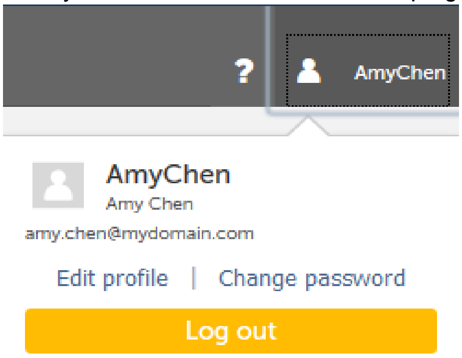
- Changing your password
- Editing and updating your profile

Note: The process of managing your own profile is different for Control Room configured with an active directory and a non-active directory environment. Users cannot configure or make changes to their profile in an active directory environment.

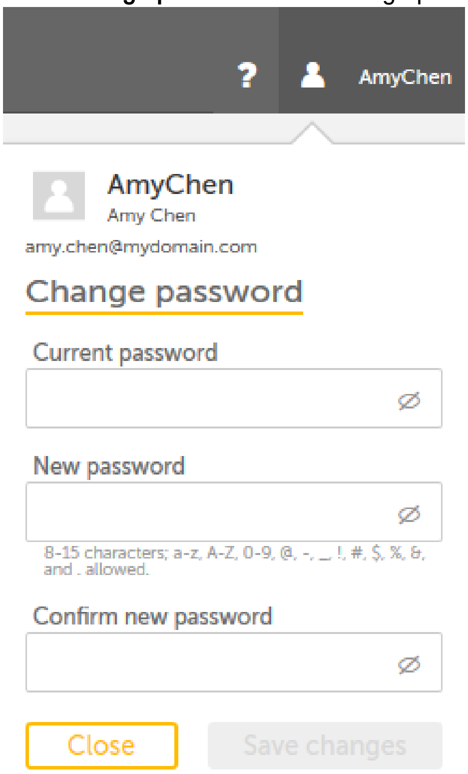
Change your password

To change your password, perform the following steps.

1. Click your user name located at the top right corner of Control Room. The **Edit Profile** and **Change Password** form is displayed.



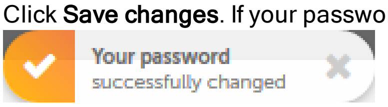
2. Click **Change password**. The Change password form is displayed.



3. On the **Change password** menu, type your current and new password.
   - **Current password:** Type your current password.
   - **New password:** Type your new password.
   - **Confirm New password.** Type your password again for confirmation.

     Note: The new password must be different than the current password and must meet the password policy set up by your Control Room administrator.

4. Click **Save changes**. If your password is successfully changed, a toast message is displayed.



Note: The **Save changes** button remains disabled if the mandatory fields are not filled. You do not need to log in again after changing your password.

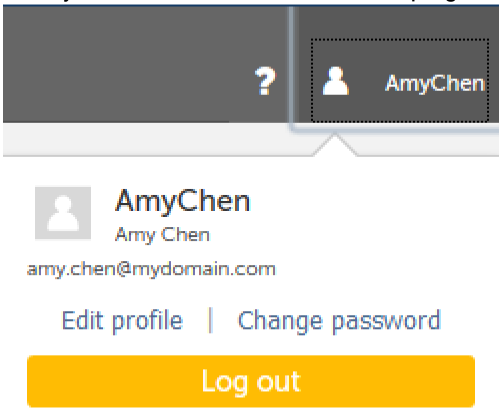
Edit and update your profile

You can change the following details about your profile by clicking your user name located at the top right corner of Control Room.

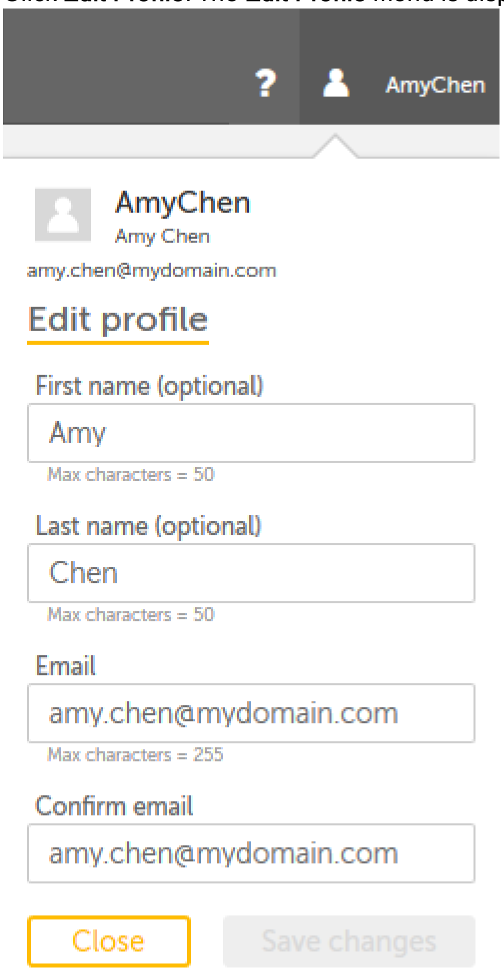
- First name
- Last name
- Email address

For this, perform the following steps.

1. Click your user name located at the top right corner of Control Room. The **Edit Profile** and **Change Password** form is displayed.



2. Click **Edit Profile**. The **Edit Profile** menu is displayed.

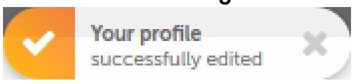


3. On the **Edit Profile** form, do one of the following.

- **First name:** Type your first name. This is optional.
- **Last name:** Type your last name. This is optional.
- **Email:** Type your e-mail. You can use this to reset your password. All important Control Room notifications will be sent to you on this e-mail address.
- **Confirm email.** Type your email again.

> **Tip:** As you start typing and make changes to the fields of the **Edit profile** form, the text of the **Close** button changes to **Cancel** to visually indicate that you have made changes to the form. Clicking **Cancel** closes the **Edit profile** form.

4. Click the **Save changes** button. Your profile is updated and a toast message is displayed.



For information on updating user profiles from the administration page, refer to the following sections.

- Edit active directory user details
- Edit non-active directory user details

Administration Overview

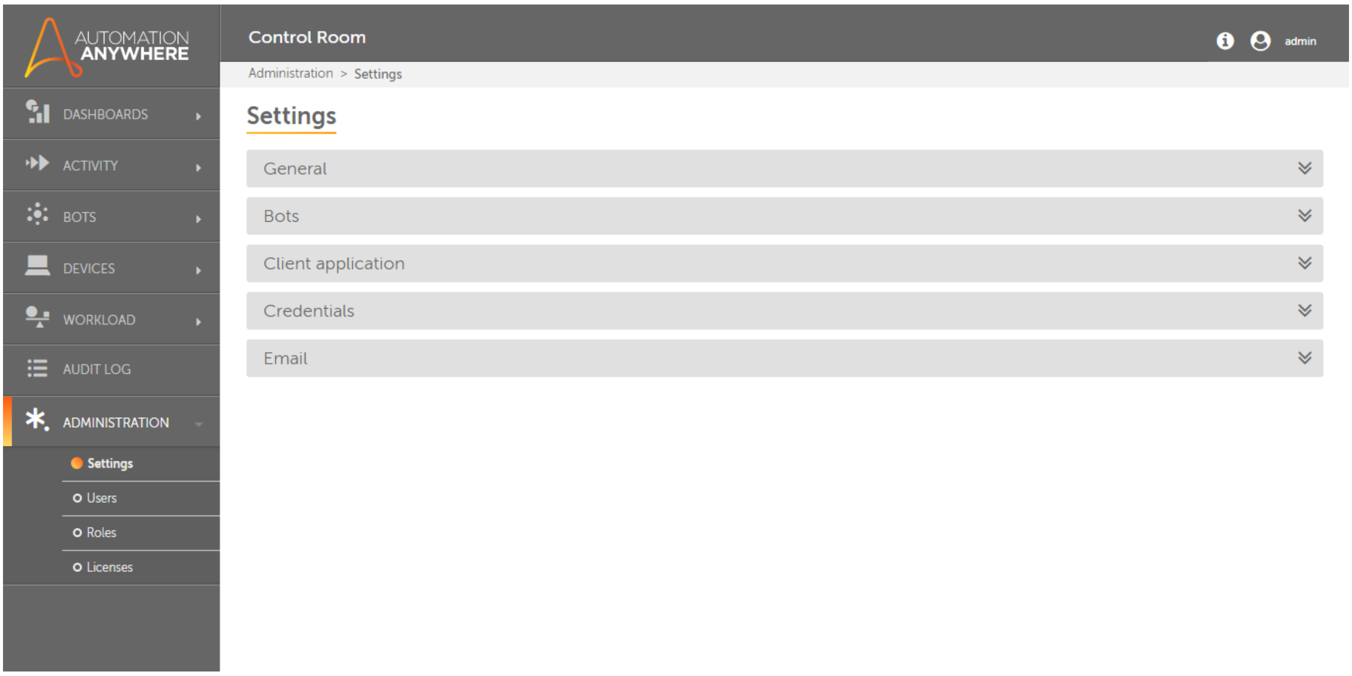
As a Control Room admin you can use the administration module of Control Room to:

- Manage roles by creating, editing, deleting, and viewing existing roles
- Manage users by creating, editing, deleting, and viewing existing users
- Change the general settings of Control Room
- Purchase an extended license or install a new license

Settings - an overview

As a Control Room admin, you can use the Control Room **Settings**, to:

- Configure General Settings and Control Room Database & Software in General
- Enable or disable Version Control in Bots
- Enable or disable Secure recording, set Product help URLs, and configure Device health checks in Client applications
- Configure the connection mode to the Credential Vault in Credentials
- Enable or disable email settings in Email



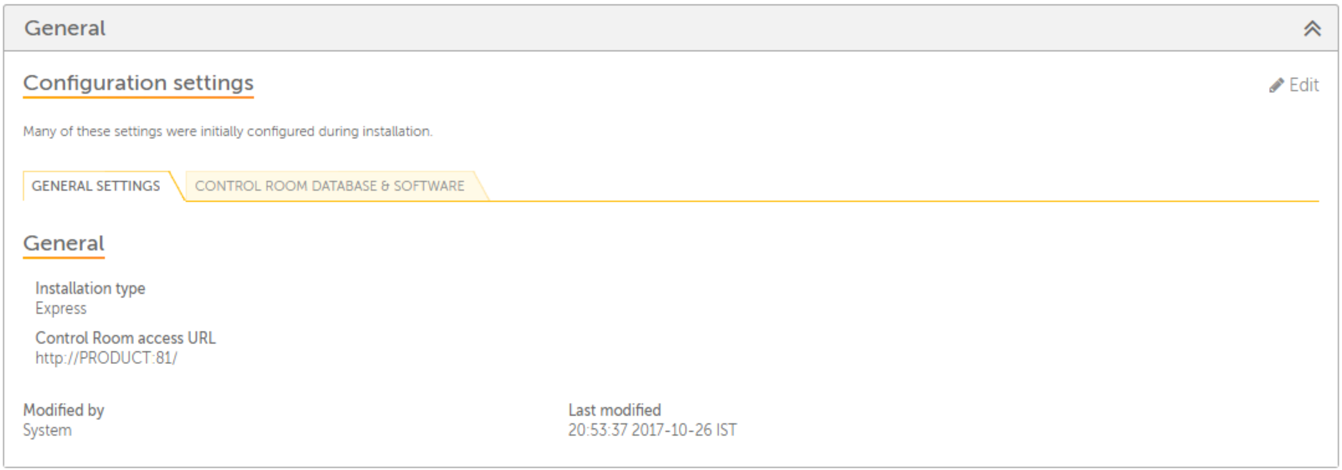
Configuration settings

As a Control Room admin you can view and manage settings that are configured while setting up the Control Room. You can view configuration details of:

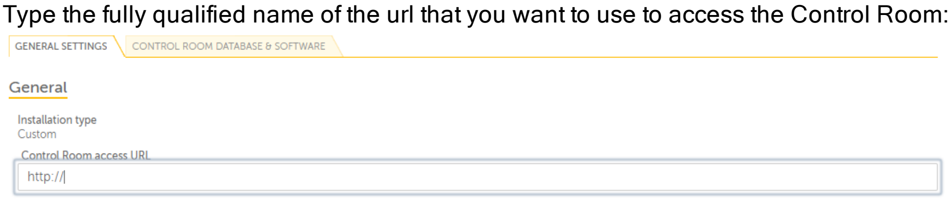
1. Control Room Installation type, access URL, and program files destination folder in General Settings
2. Website Security & Configuration details, Control Room Users, Database, and Repository details, Deployment settings, and Security details in Control Room Database & Software

General settings

The General settings provide information about the installation type, the access URL and program files destination folder. You cannot edit these settings as they are configured during installation.

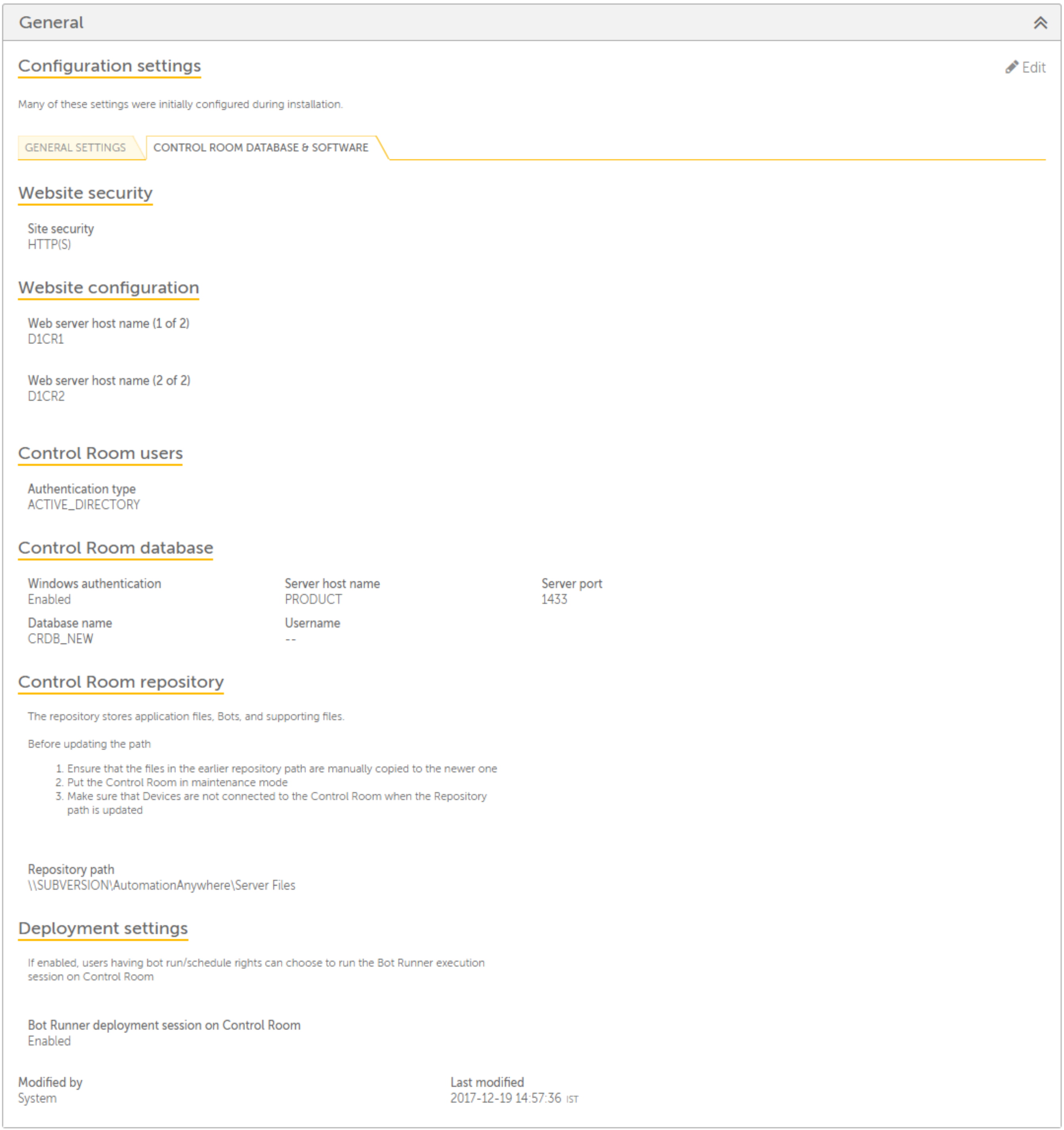


The table below describes the General settings:

Settings	Description
Control Room Installation type	It is the type of setup used to install the Control Room. It can either be **Express** or **Custom.** This setting is configured during installation and is not editable.
Control Room access URL	It is the fully qualified name of the server that is used by Bot Creators, Bot Runners and Users to access the Control Room. You can change the access URL if the Control Room is setup in custom mode. To modify the URL, 1. Click edit 2. The **General Settings** page opens in edit mode. 3. Type the fully qualified name of the url that you want to use to access the Control Room:  4. Click 

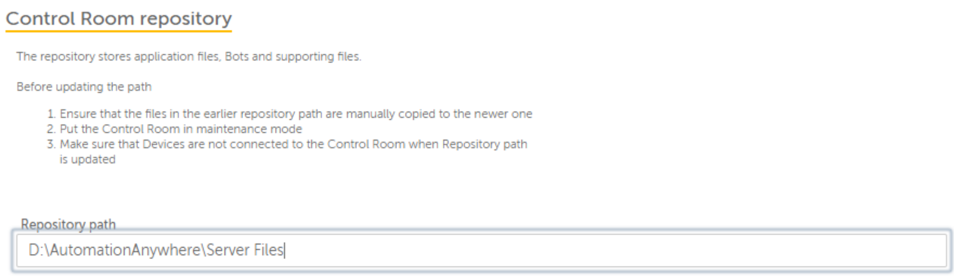
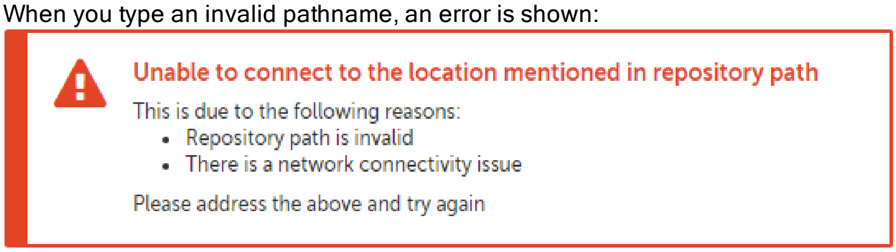
Control Room Database & Software

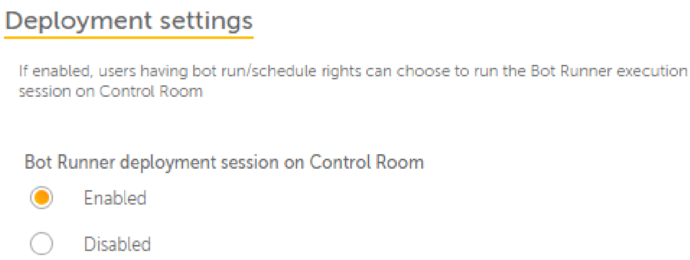
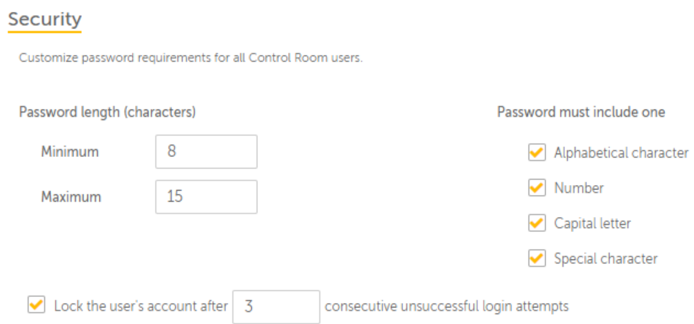
The Control Room database and software settings provide details for website security and configuration, Control room users, database, and repository, deployment, and security settings. You can edit settings for the Control Room repository, Deployment, and Password.

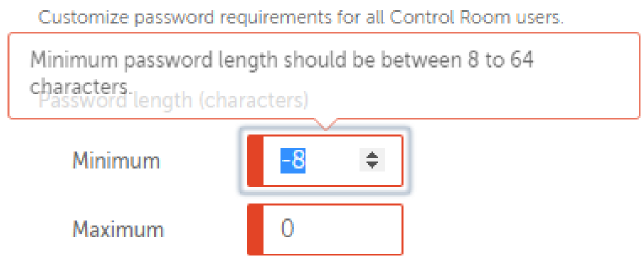


The table below describes the Control Room Database and Software settings:

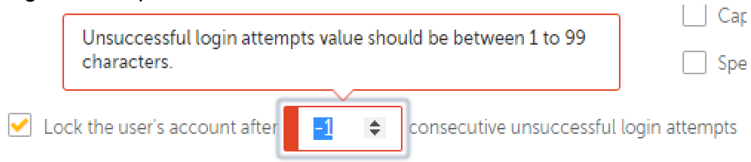
Settings	Description
Website security	It shows the type of security protocol used - http or https. This setting is configured during installation and is not editable.
Website configuration	It shows the website configuration details such as web server host name, If the Control Room is configured for Express installation, only one host name is shown. However, if it is configured for Custom installation, multiple host names are shown. This setting is configured during installation and is not editable.

	Web server host name and port details of all registered and active users are listed. However, note that the username and password values are not shown.
Control Room users	It shows the **Authentication type** used to log on to the Control Room instance by Bots. It could be Active Directory, Single Sign-On (SAML 2.0) or Database. This setting is configured during installation and is not editable. • **Active Directory** users are configured when you want Bots of a specific domain to be authenticated with their Active Directory credentials. • **Single Sign-On (SAML 2.0)** users are configured when you want Bots to be authenticated using SAML 2.0 protocol and log on using the organizations' IdP server credentials. • **Database** users or Non-Active Directory users are configured when you want Bots to be authenticated using the Control Room database.
Control Room database	It shows the settings for : 1. **Windows authentication -** It is the authentication type used to connect to the database server. It shows **Enabled** when Windows Authentication is selected while configuring the database in installation. It shows **Disabled** when default database authentication is used. 2. **Server host name -** It is the fully qualified name of the control room database server. 3. **Server port -** It is the port to which the database is configured. 4. **Database name -** It is the database that will be used to store Control Room data. 5. **Username -** The values are not displayed. This setting is configured during installation and is not editable.
Control Room repository	It shows the location where all Bots, application files, and supporting files are stored. The default path is set to **C:\ProgramData\AutomationAnywhere\Server Files** during installation, if not updated during installation. You can also choose to modify this path post installation here. Before changing the repository path, ensure that you: • Copy the existing files to another location • Put the Control Room in maintenance mode • Inform users to disconnect their devices from the Control Room instance To modify, 1. Click edit 2. The page opens in edit mode. 3. In the **Repository path** field, **type** the location of the repository ending with **Server Files**:  • You can use Network Drive folders for repository path. • When you type an invalid pathname, an error is shown: 

	4. Click Save changes
Deployment settings	It shows whether the users with run and schedule privileges can choose to **Run bot runner session on Control Room** when you deploy or schedule a Bot. Refer Run a bot and Schedule a Bot for details. By default this setting is **Enabled**. To modify, 1. Click edit 2. The page opens in edit mode. 3. Select Enabled or Disabled as required for **Bot Runner deployment session on Control Room:** 
Security	These define the password policy settings for all Control Room users. Here, you can customize the password length, password content, and/or select the number of log on attempts allowed. Note: The password policy is applicable for a Control Room that is configured for **Database authentication type.** To modify, 1. Click edit 2. The page opens in edit mode. 3. Specify the following as per your company policy:  Tip: The user account is disabled in the Control Room when it is locked out. You cannot enter invalid values in the: • Password length field



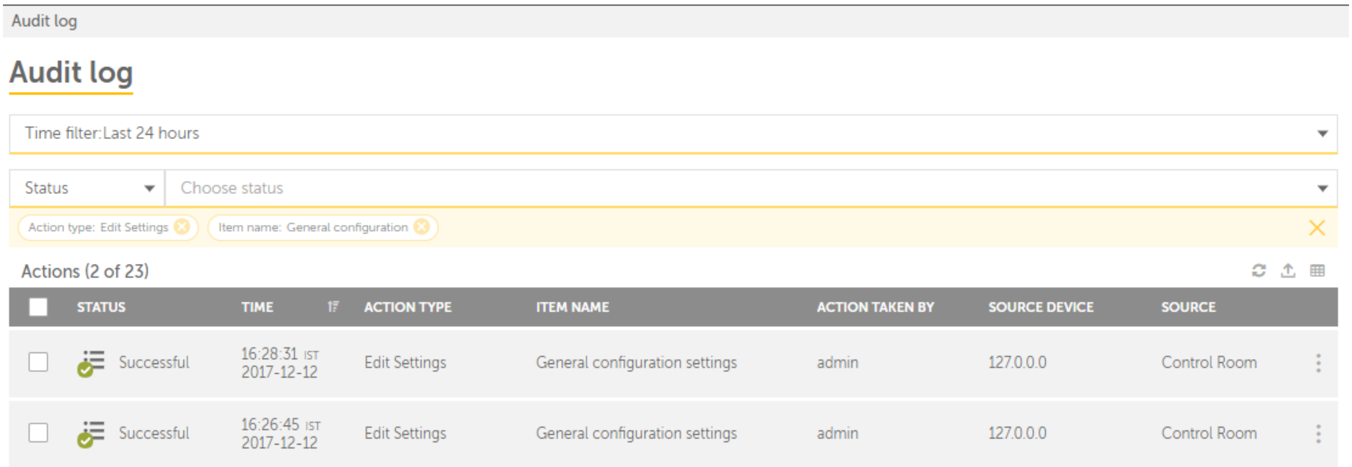
- Log on attempts field



4. Click 

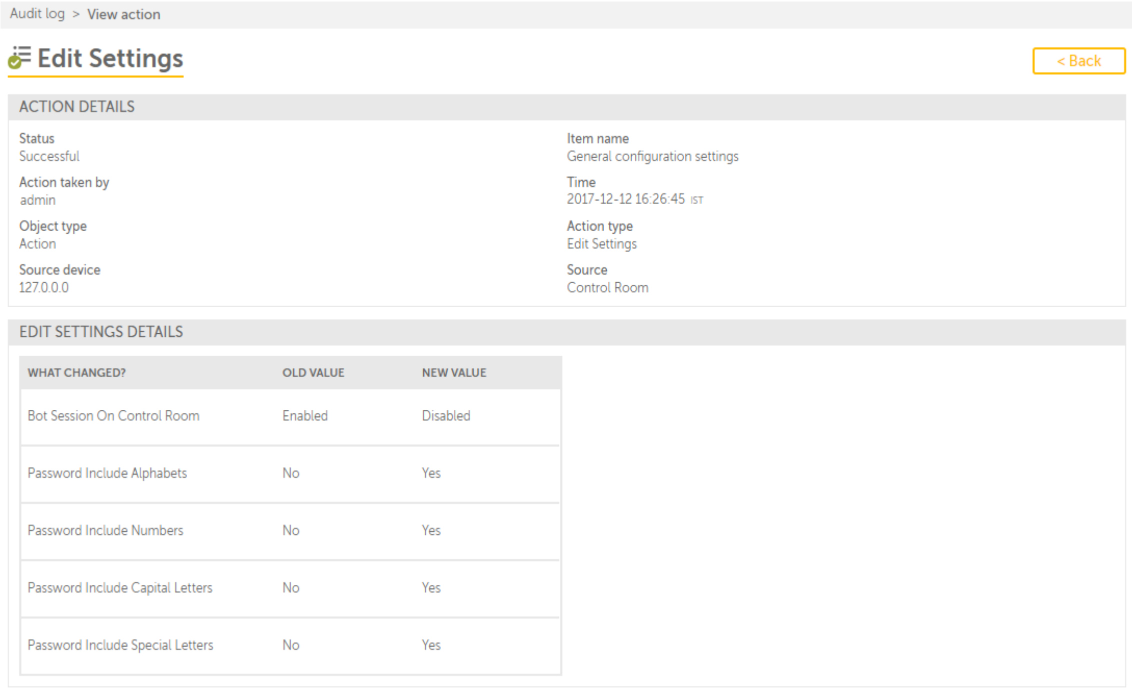
Audit Logs

All updates to the Configuration Settings are captured in the **Audit Log** page. For example, the following illustration lists all actions performed to edit general settings :



To view details of each audit entry:

1. Go to the required data and mouse over
2. Click 
3. The details page is launched where in you can view only those entries that are changed. The illustration below shows details of successful disabling of Bot Session on Control Room and setting of the password policy:



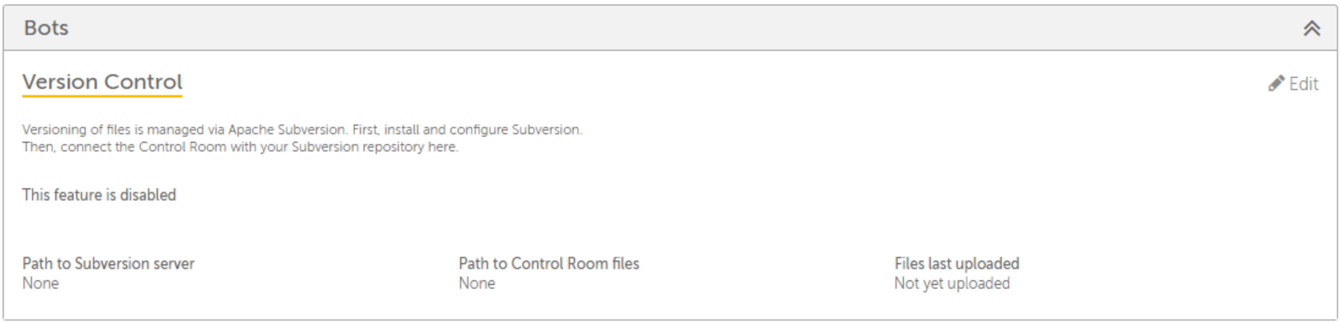
.

Refer View Audit Details for more information.

Bots - Configure Version Control

To manage controlled edits of files that could include TaskBots, MetaBots, Reports, and Workflows, as a Control Room admin you can configure Version Control in Control Room Settings.

The Control Room is tightly integrated with SubVersion version control system so that the version, checkin/checkout, version history and version roll back functionality can be leveraged with ease for all files.



By default, the feature is **disabled**.

Version Control Pre-requisites

- For Version Control to be enabled and integrated from Control Room, it is necessary that SVN (SubVersion) should be installed and configured.

  Note: Automation Anywhere supports Subversion v1.7.2, v1.9.7, and 1.8.15.

- SVN Administrator user should be created with required permissions.
- SVN repository should be created, which can be used to store all version control files.
- Control Room will be the basis of communication with SVN. Clients will not communicate with SVN directly.

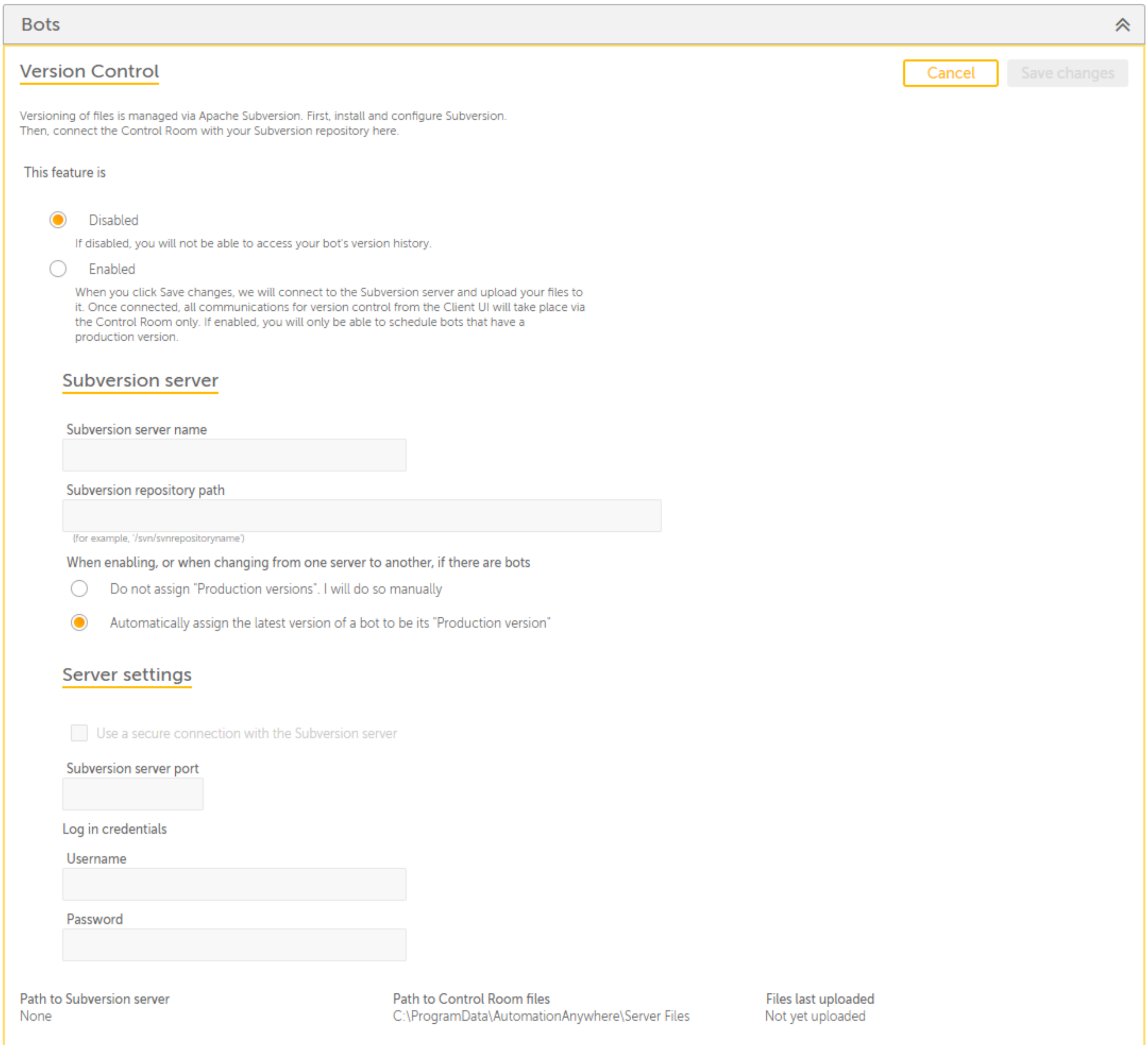
  Note: Once the Control Room integration with SVN is up and running, all communication for version control operations from Enterprise Client to SVN will take place via Control Room only.

Enable Version Control

To enable Version Control for Bots:

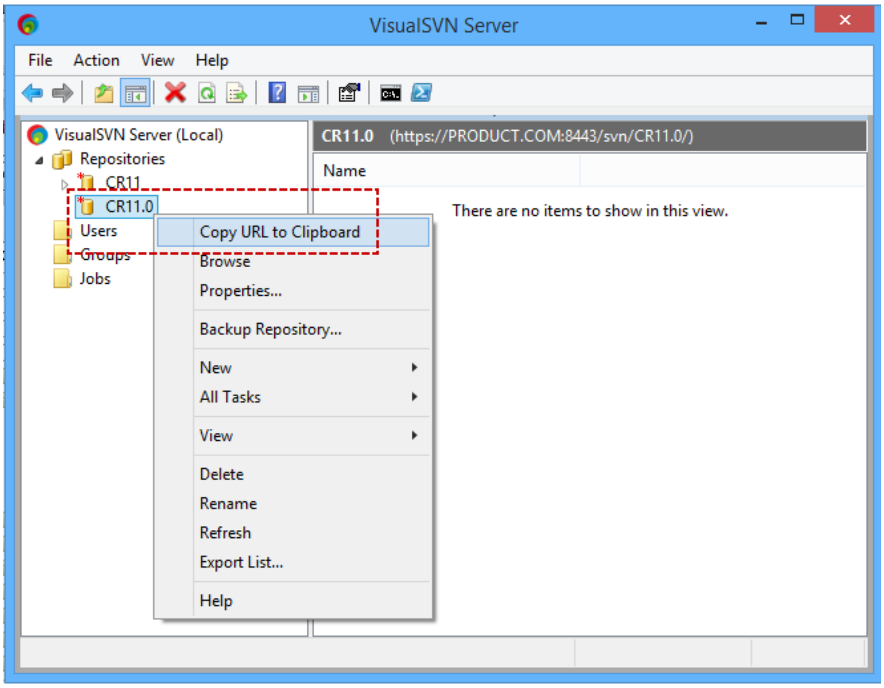
1. Select **Administration** → **Settings** → **Bots**
2. Click **Edit**

3. The page opens in edit mode:



4. Select **Enabled**
5. Enter the following details:
   a. Subversion server name - Provide hostname of subversion server.
   b. Subversion repository path - Provide the SVN repository path.
      - The SVN repository must be empty if you are enabling these settings or switching from an old configured repository to new SVN repository.
      - You can configure only upto three levels of repository path.
      - Refer section on Impact of enabling and disabling VCS settings for details.

      Tip: You can copy these details from the VisualSVN Server Manager as shown:



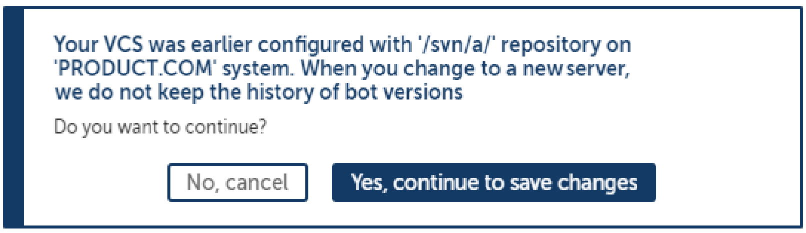
6. Select option for assigning Bot production version manually or automatically when you enable version control or configure version control to another Subversion repository.

   The production version of a Bot is must for a schedule to run on the selected Bot, Your schedules will not be triggered unles the scheduled bots have their production versions set.

   - Use **Do not assign "Production versions". I will do so manually** when you want to manually assign a production version for Bots. Use this option when you want to set production versions in a controlled manner.
   - Use **Automatically assign the latest version of a bot to be its "Production version"** when you want the Control Room to automatically select the latest version of Bots to Production version.
7. Optionally, select **Use a secure connection with the Subversion server**
8. Provide the **Subversion server port** number that is assigned for SVN. It should be between 1 and 65535.
9. Provide your Subversion **Login credentials** - **Username** and **Password**
10. The details for **Subversion path** and **Files last uploaded** are updated once you configure Version Control. The default path of **Control Room files** is also displayed.
11. Click 

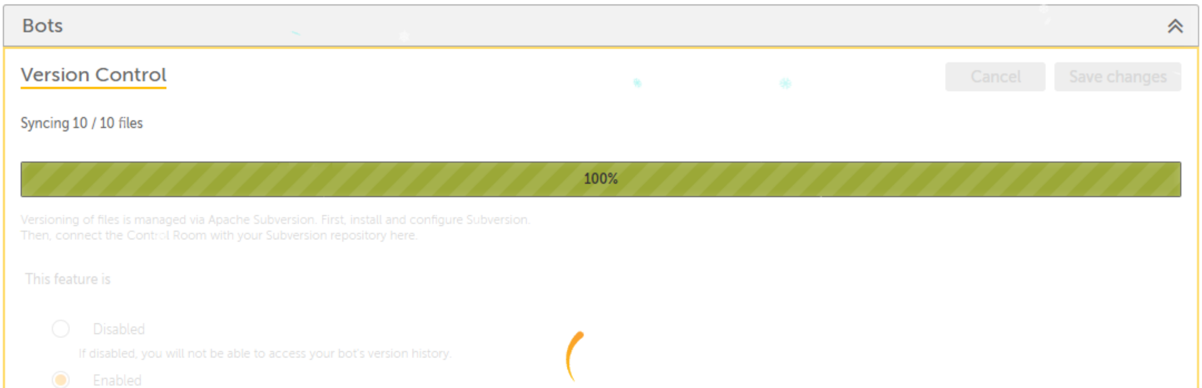
Note: If VCS was earlier configured and you switch to a different Subversion repository, the bot version history is not stored. Refer Impact of enabling and disabling... section for details.

- You must confirm whether you want to continue:

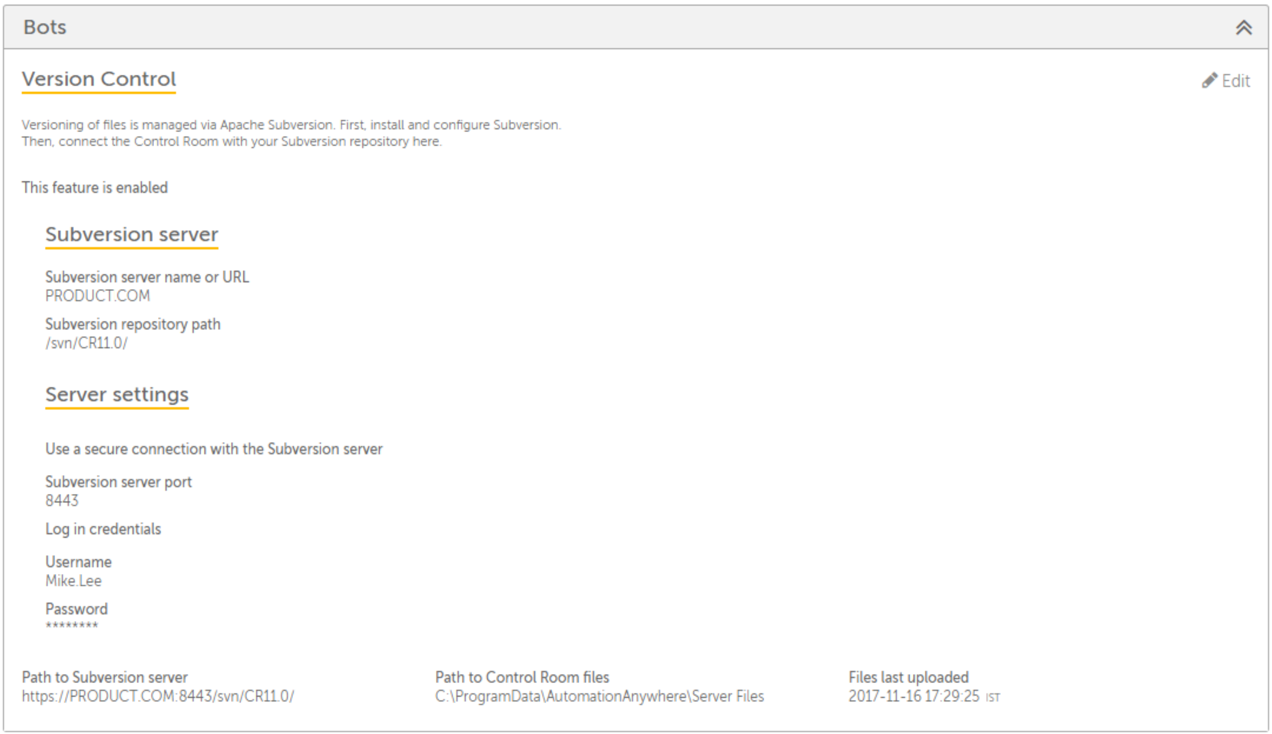


Note: Bots which are deleted after VCS is disabled, will be deleted from SVN too.

- You can view the repository synching as shown:



12. The details are updated as shown:

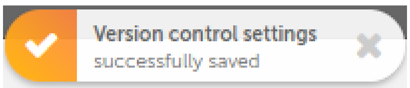


Disable Version Control

You can also choose to disable Version Control.

1. Clear **Enable**
2. Click 

3. A successful switch is denoted with:



Impact of enabling and disabling version control settings

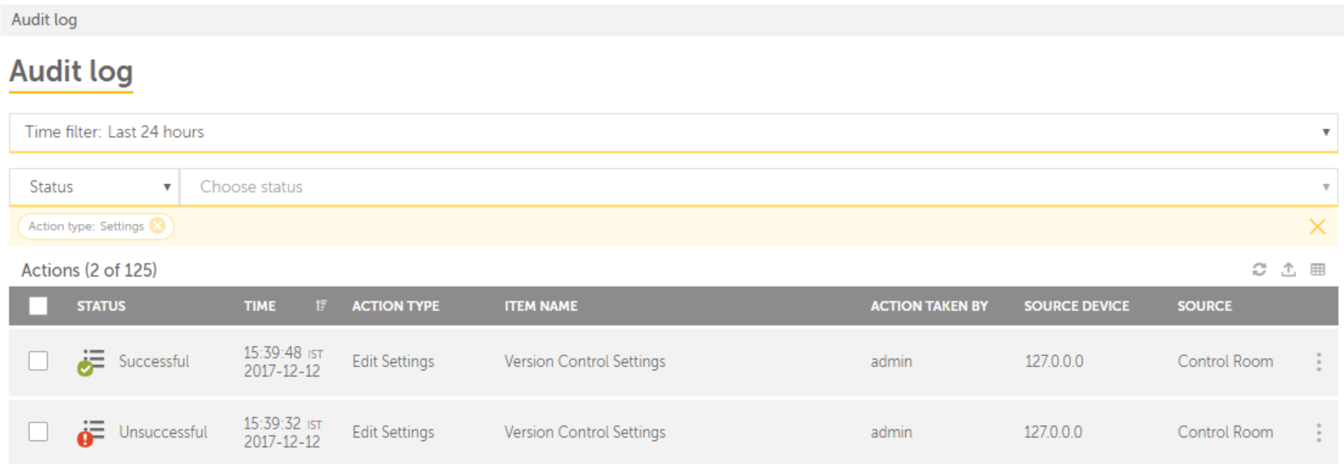
When you enable and disable version control settings in the Control Room, it affects the way a Client can access their Bots in the Client and upload those to the Control Room. While enabling and disabling this setting ensure you are aware about its impact, which is summarized here.

- When you **enable** version control settings, the system uploads the Bots from Control Room repository to SVN repository. During upload the Control Room repository is in read only mode and locked. Hence, you cannot update it. You will not be able to perform actions such as Upload, Delete, Set production version, Checkout /Check in /Undo checkout, and Force unlock.
- When you **disable** version control settings, the files that are in checked out state are listed for force unlock by the Control Room administrator or a user with unlock bots privileges. You are allowed to disable the settings only when you unlock the checked out files.
- When you re-**enable** version control settings, you can:
    a. Connect to the repository that you had uploaded earlier. Version history of existing Bots is also retained. Hence, in this case,
        i. The **version** of the Bots that are not updated **remains the same**.
        ii. A **new version** of updated Bots is **created**.
        iii. **Version 1.0** is allotted to new Bots that have the same name as that of a Bot that was deleted from the earlier repository.
        iv. **Production version is not set** if the option **Do not assign production version. I will do so manually** is selected.
        v. **Production version is set** to latest versions of the Bots if the option **Automatically assign the latest version of bots to production version** is selected
    b. Connect to a new repository that does not have any Bots. Your version history of the earlier repository is not retained. Also, you can choose to set the production version manually or automatically.

> **Note:** You cannot connect to a new repository that is not empty.

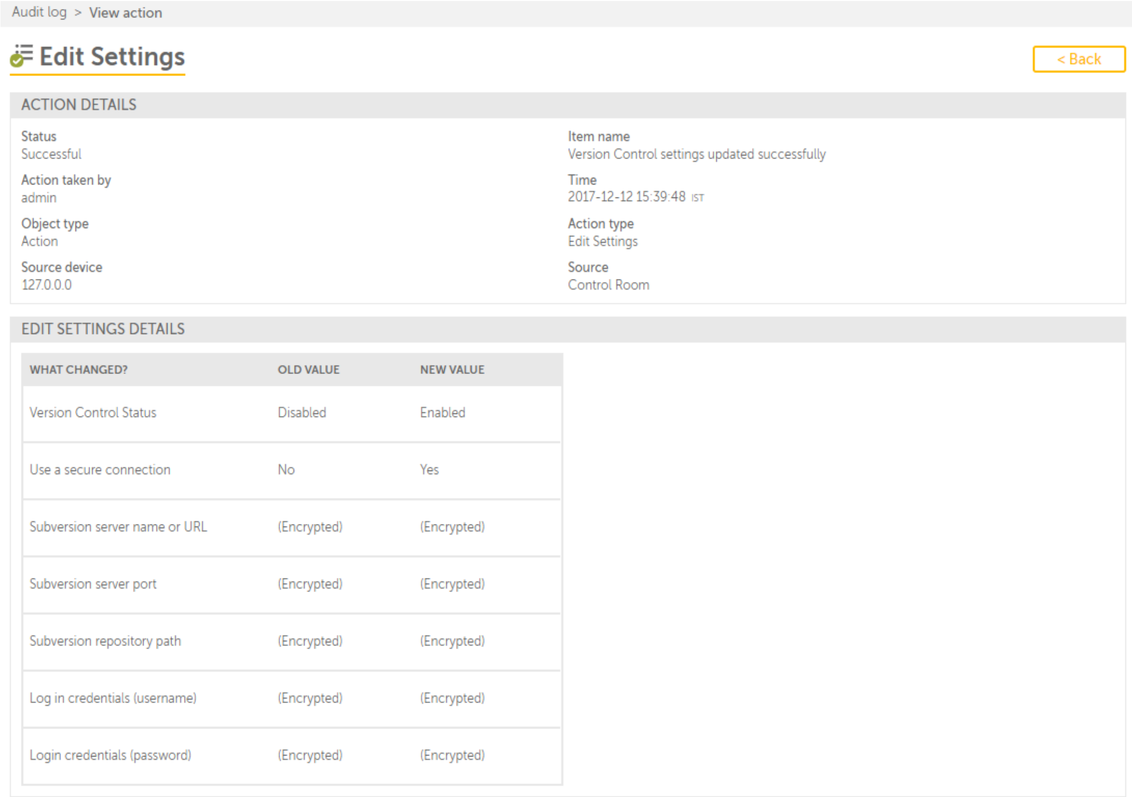
Audit Logs

All updates to the VCS Settings are captured in the **Audit Log** page. For example, the following illustration lists all actions performed to connect and edit VCS settings :



To view details of each audit entry:

1. Go to the required data and mouse over
2. Click
3. The details page is launched where in you can view only those entries that are changed. The illustration below shows details of successful connection of Version Control to a Subversion repository:



Note: Some fields such as Subversion server name, port, repository path, and credentials are shown as **(Encrypted)** because these values are securely stored in the Credential Vault.

.

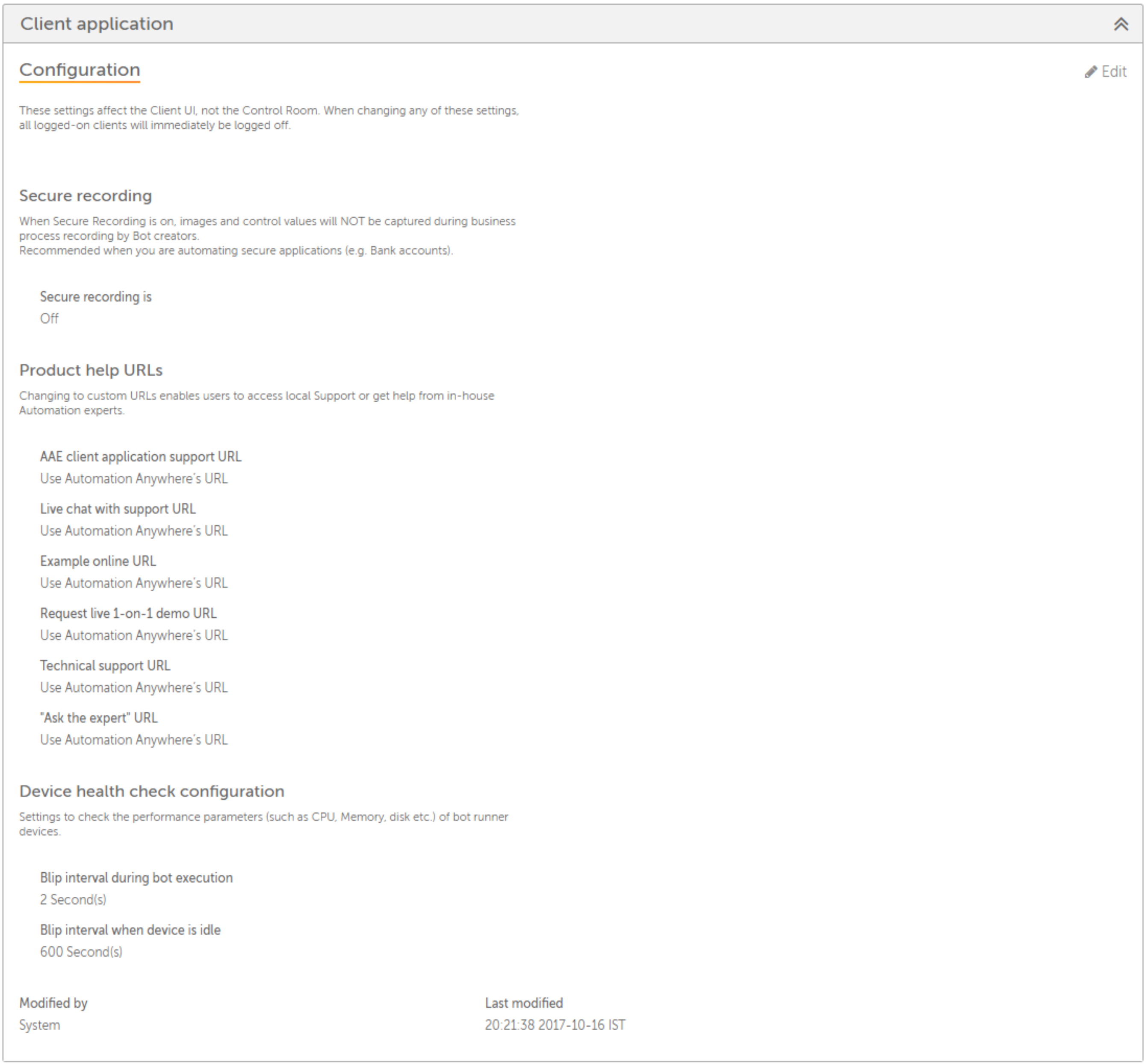
Refer View Audit Details for more information.

Client application

Introduction

As a Control Room admin you can choose to configure the settings relevant to your Automation Anywhere Client in Client application. Here, you can:

- Enable or disable Secure recording
- Change Product help URLs
- Configure Device health checks

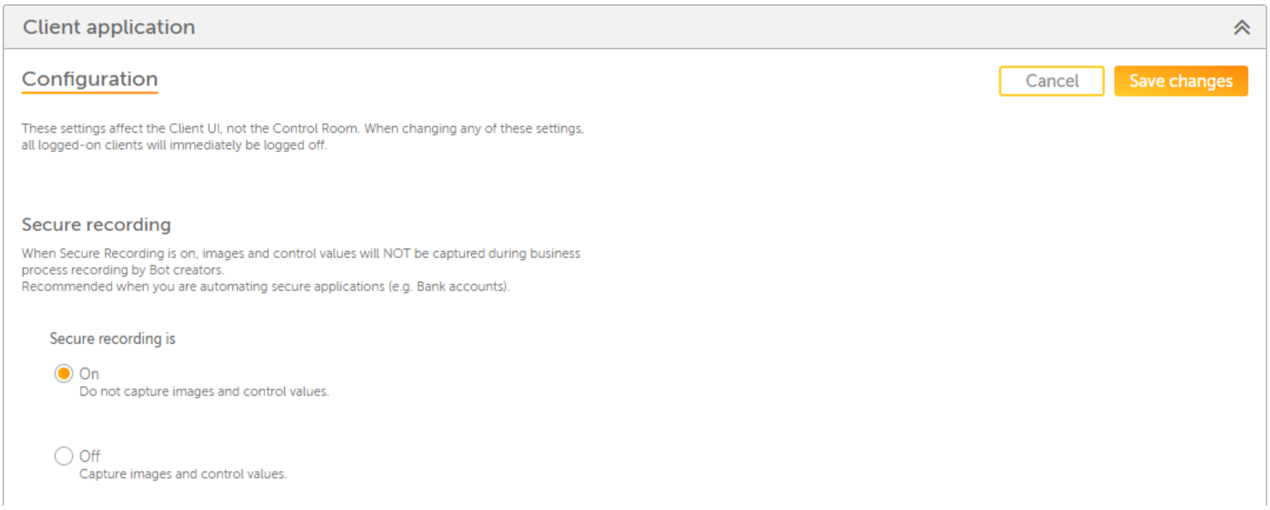


Secure recording

Secure recording offers you a choice between capturing or not capturing images and control values during business process recording by Bot creators. You can enable secure recording when you are automating secure applications such as Bank accounts.

To modify secure recording settings:

1. Select **Client application**
2. Click **Edit**
3. The page opens in edit mode wherein Secure recording is shown **Off** by default.
4. Select **Secure recording is On**



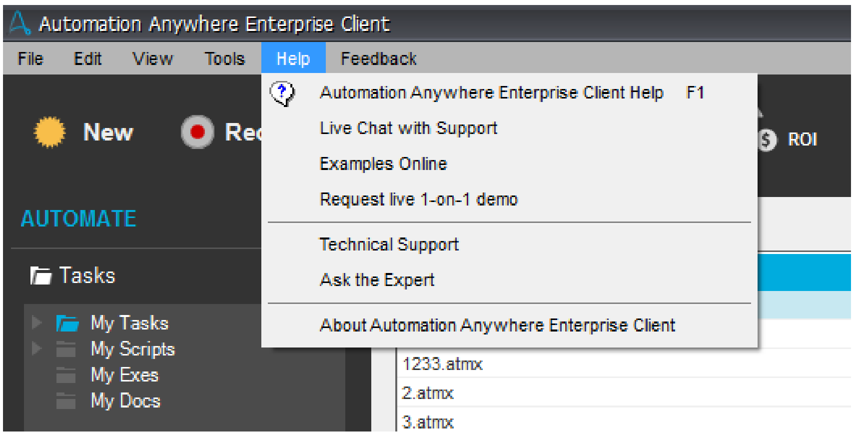
5. Click **Save changes**

Product help URLs

Product help URLs allow you to redirect links to Automation Anywhere Support Site or to any Custom URL of your choice.

- **Use Automation Anywhere's URLs -** Use this to navigate your users to the default Automation Anywhere Support site. This disables all the other options such as Live Chat with Support URL etc.
- **Use Custom URLs -** Use this to navigate your users to your custom defined URLs for Product help. This allows your users to seek help from in-house automation experts.

  The illustration below shows the URL's as seen in Enterprise Client → Help:

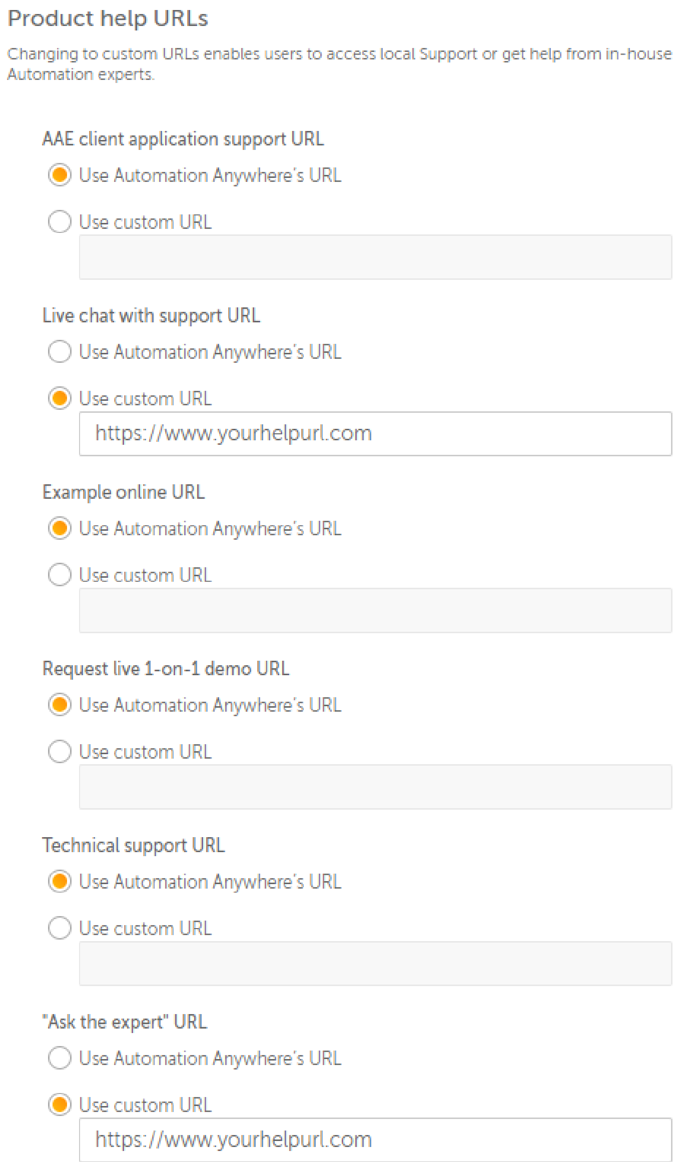


- Table below summarizes Product help URLs:

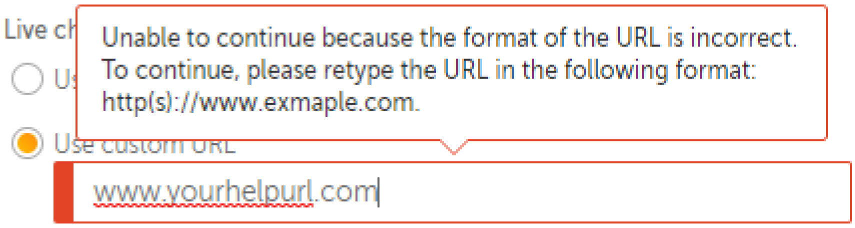
URL	Description
AAE client application support	It allows you to add your customized Product Help URL and re-direct users to your in-house support site.
Live chat with support	It allows you to access in-house Live Chat and speak to online Experts.
Example online	It allows you to look for available Online Examples.
Request live 1-on-1 demo	It allows you to request for live demonstration of features and experts would answer your questions.
Technical support	It allows you to access in-house Technical Support.
Ask the expert	It allows you to speak to an expert and get their expert advice.

To modify Product help URL settings:

1. Select **Client application**
2. Click **Edit**
3. The page opens in edit mode wherein **Use Automation Anywhere URL**s are selected by default.
4. Select **Use Custom URLs** as required. For example, you might want to redirect Live chat support to a specific chat group.



- You must use http(s) protocol in the URLs. If you do not, then your are shown an error:



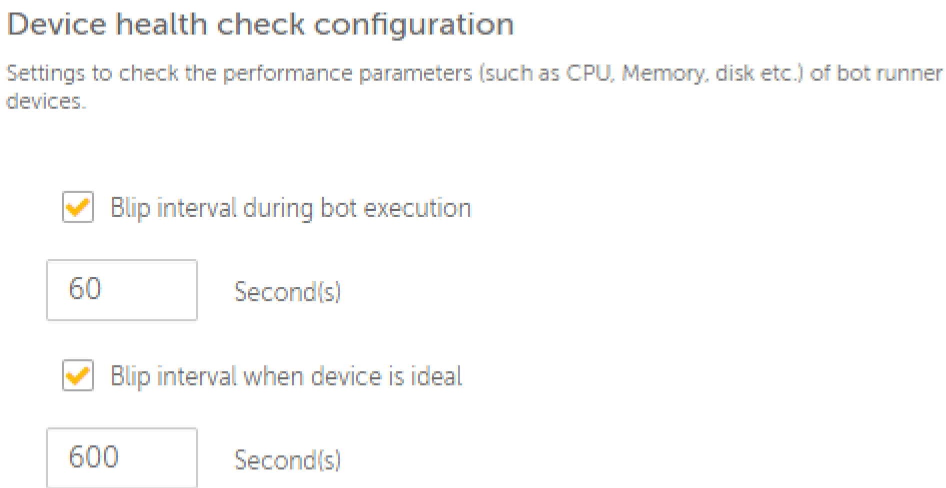
5. Click 

Device health check configuration

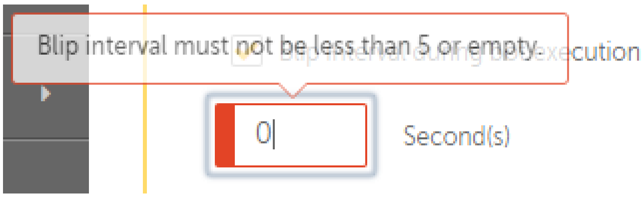
These settings allows you to set the time interval for Device Health check that includes parameters such as CPU, Memory, and Disk usage etc. You can therefore set the frequency at which the data is exchanged between the Control Room and connected Clients.

To modify **Device health check settings**

1. Select **Client application**
2. Click **Edit**
3. The page opens in edit mode wherein the **Blip interval** for **bot execution** and **device** status can be enabled. The default value for:
   - **Bot execution** is set to 60 seconds
   - **device** status i.e. how long it is **idle** is set to 600 seconds.



4. Change the **Blip** interval time as required
   - You cannot input less than 5 or empty value. If you do, then you are shown an error:



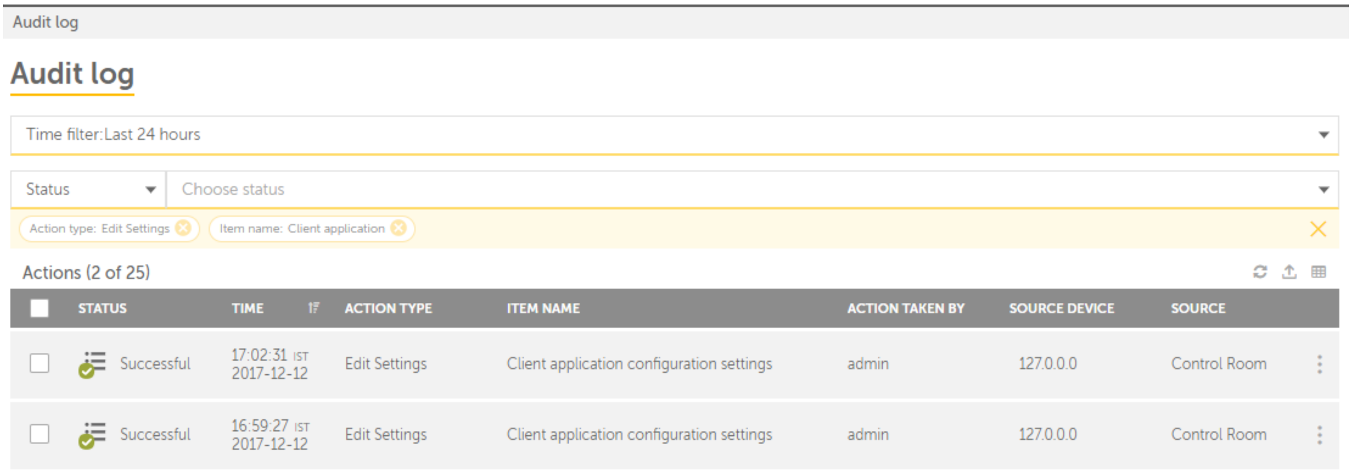
5. Click 

Modification details

The modification details such as **Modified by** and **Last modified** date/time are captured. The Client application tab shows **System** and the Control Room installation/configuration **date and time** by default when you launch the **Settings** page:

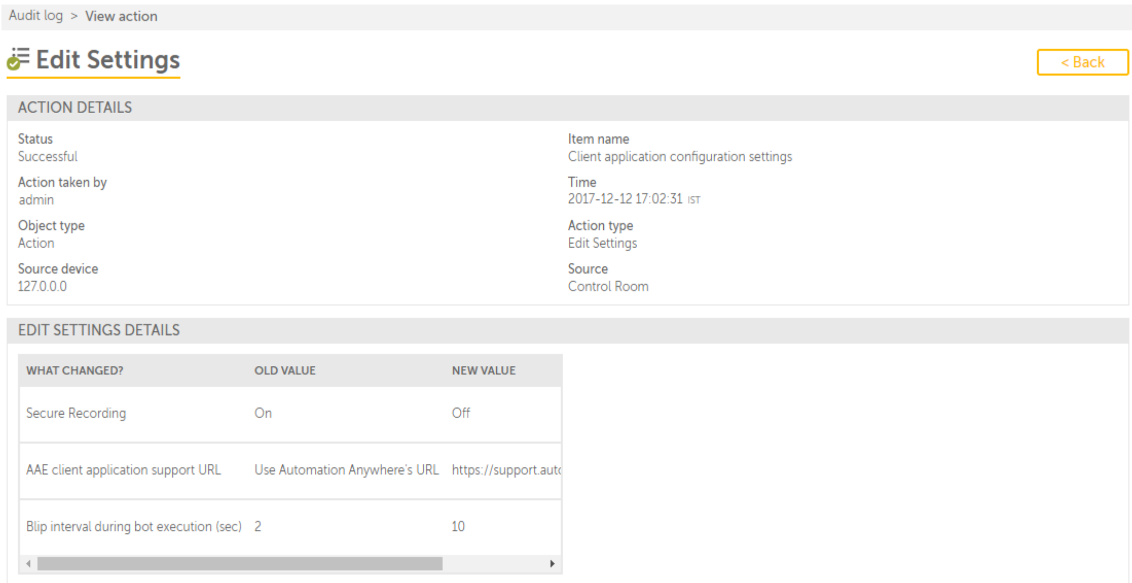
Audit Logs

All updates to the Client application settings are captured in the **Audit Log** page. For example, the following illustration lists all actions performed to update the Client application configuration settings:



To view details of each audit entry:

1. Go to the required data and mouse over
2. Click
3. The details page is launched where in you can view only those entries that are changed. The illustration below shows details of successful disabling of Secure Recording mode, change in Client application support URL, and change in Blip Interval:

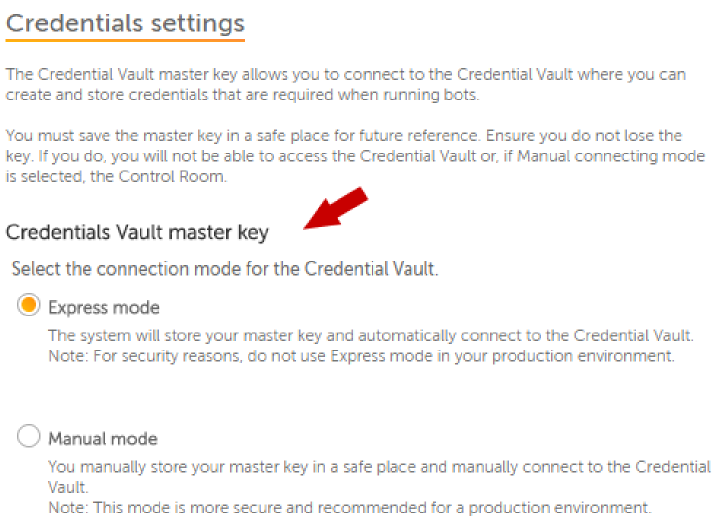


Refer View Audit Details for more information.

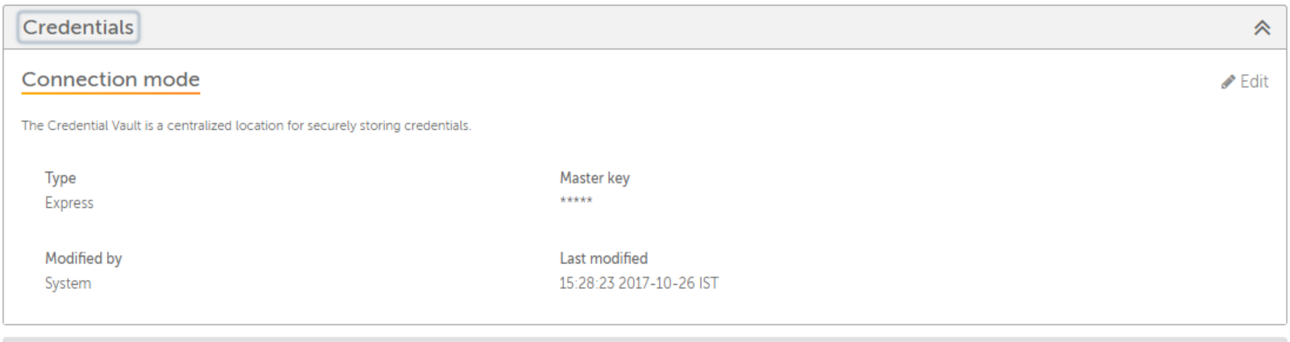
Configure credential vault connection mode

Credential Vault is a centralized location for securely storing credential information used by Bots. As a Control Room admin, you can configure the **Connection mode** that allows you to connect to the Credential Vault using a **Master key**.

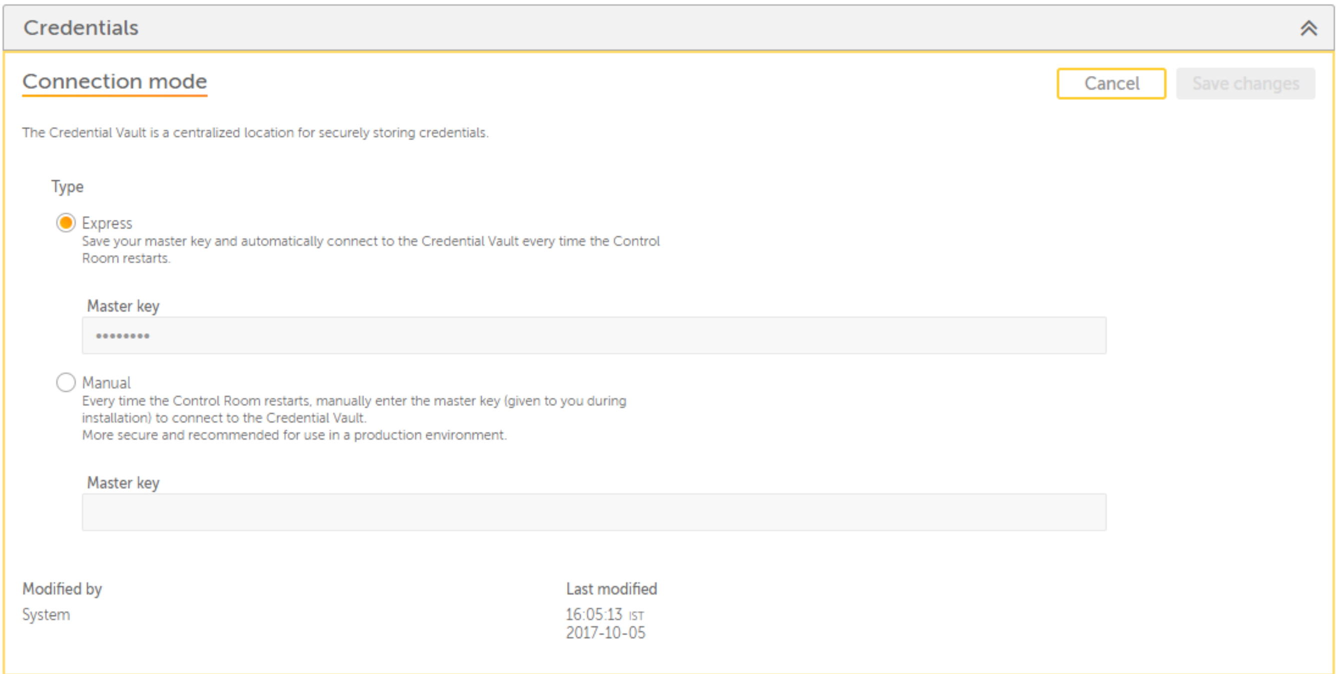
The connection mode is first configured during Control Room's initial setup as illustrated below:



You can view the **Connection mode** details in Settings → Credentials tab



To configure settings for Credential Vault, you have to choose between **Express** or **Manual** mode.

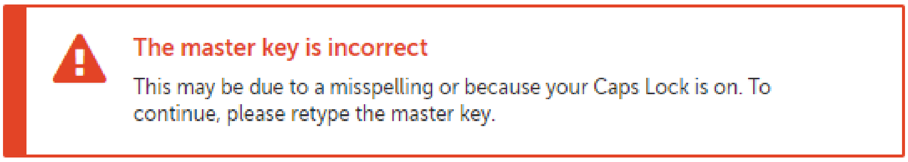


- **Express Mode -** Use this to auto connect to the Credential Vault with the master key that is stored in the system during Control Room configuration.
- **Manual Mode -** Use this to manually connect to the Credential Vault using the master key that was available during Control Room configuration.

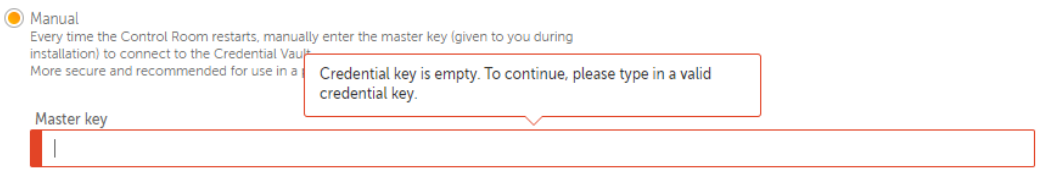
Note: You will have to provide this key every time you start / re-start the Control Room.

Important: Store the master key at a secured location if using the Manual mode. Any modification or loss may result in your losing complete access to the Control Room.

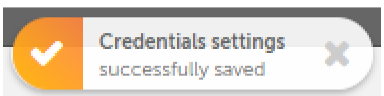
- Compared to **Express**, the **Manual** mode is more secure and recommended for use in production environment.
- While switching modes, you must provide the **Master Key** in the field and click **Save** for the changes to take effect.
- When you do not enter a valid key, you are shown:



- If the field is empty, you are shown:



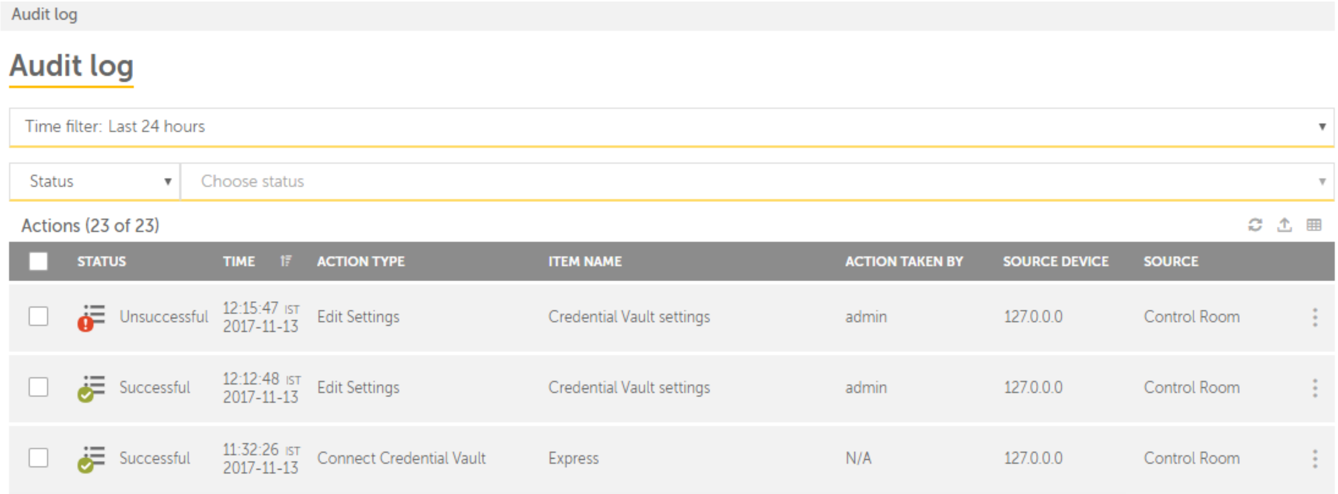
- A successful switch is denoted with:



Tip: Restart the server machine (on which the Control Room is installed) or services to allow changes to take effect.

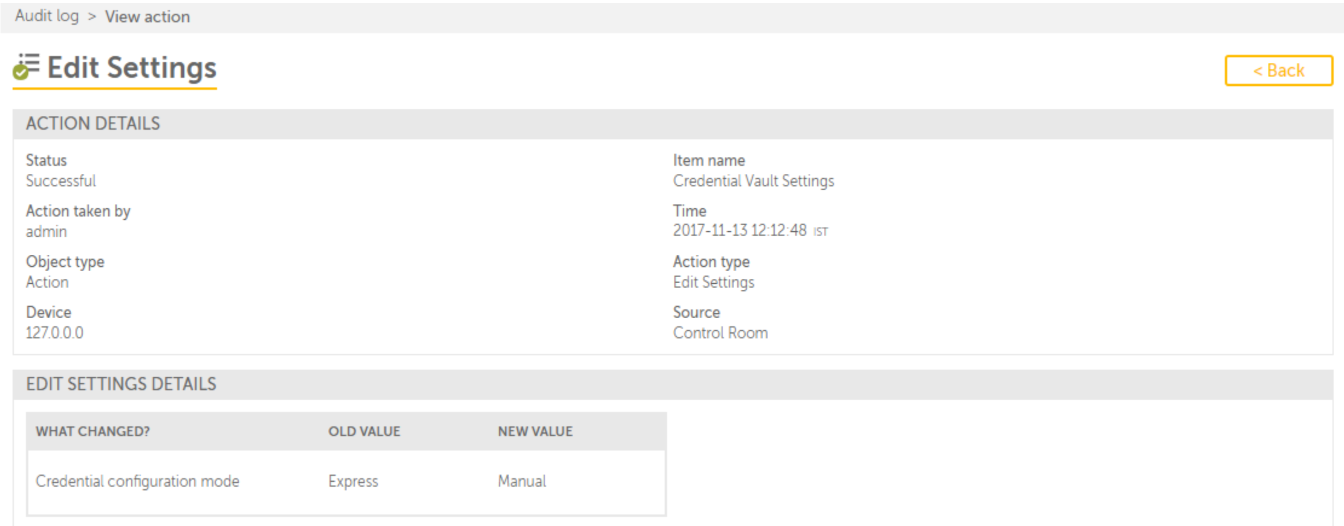
Audit Log

All updates to the Credential Vault connection mode are captured in the **Audit Log** page. For example, the following illustration lists all actions performed to connect and edit connection settings to the Credential Vault :



To view details of each audit entry:

1. Go to the required data and mouse over
2. Click
3. The details page is launched. The illustration below shows details of successful Credential Vault connection switch from **Express** to **Manual** mode:



Refer View Audit Details for more information.

Email-settings

As a Control Room admin, you can opt to send email notifications to other Control Room users when certain activities that affect the users are updated such as user information, account activation/de-activation, TaskBot execution status etc.

Also, when this setting is enabled, all users have to confirm their account by clicking on the confirmation link that they receive in their email account, set the password & security questions, and login to the Control Room.

By default, email notifications are disabled.

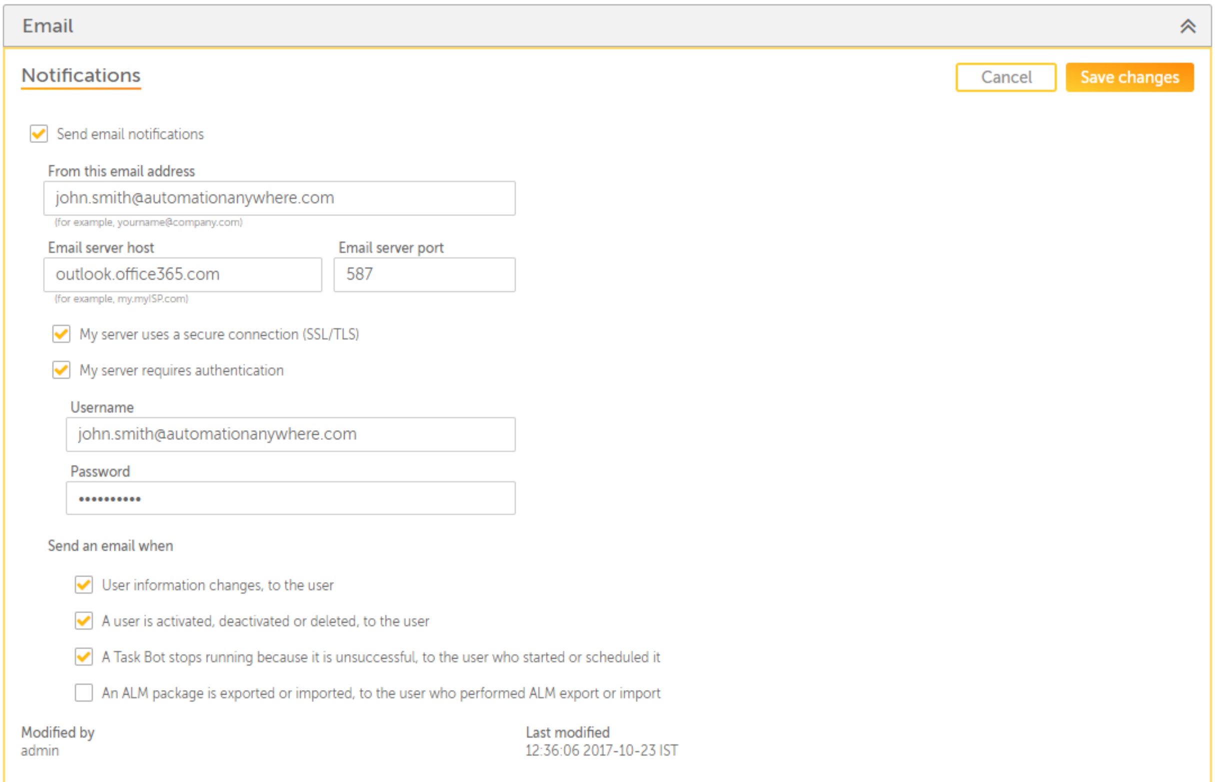
Enable Email notifications

To modify **Email** settings:

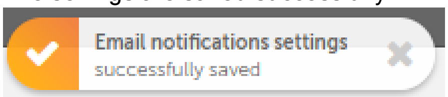
1. Select **Email**
2. Click **Edit**
3. The page opens in edit mode
4. Select **Send email notifications**
5. Enter the following details:
    a. **Email address** - this is the address from which the notification will be sent to the user
    b. **Email server host** - this is the email server host name
    c. **Email server port**.- this should be between 1 and 65535
    d. **My server uses a secure connection (SSL/TLS)** - This is optional. Select this if you have enabled SSL/TLS protocol.
    e. **Username** and **Password** - This is only enabled if you select **My server requires authentication**
6. Select any or all activities for which you want to send the notification to the user when:
    a. **The user information changes**. For example when the Control Room admin updates the Firstname and Lastname of user Mike.Lee, he receives an email notification stating that his user account information has been updated.
    b. **The user is activated, deactivated or deleted.** For example, if the Control Room admin disables the user Mike.Lee, he receives an email stating that his user account has been disabled.
    c. **The Taskbot scheduled or run by the user fails execution.** For example, if Mike.Lee who has scheduling privileges schedules a Bot to run on the Bot Runner Amy.Chen's machine and the Bot fails to,
        - **deploy** to Bot Runner machine
        - **execute** because it was either stopped, timed-out or encountered an error,

        Mike.Lee receives an email notification stating that the Bot scheduled on the Bot Runner Amy.Chen could not finish execution.
    d. **An ALM package is exported or imported by the user.** For example, if Mike.Lee exports or imports an ALM package, he will receive an email notification providing status of the export or import package.

7. Click 



8. The settings are saved successfully

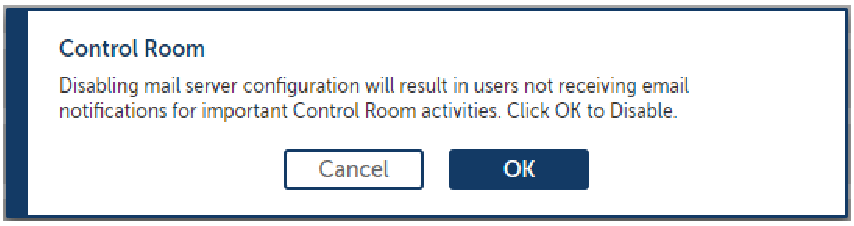


Disable Email notifications

You can also choose to disable the notifications if required.

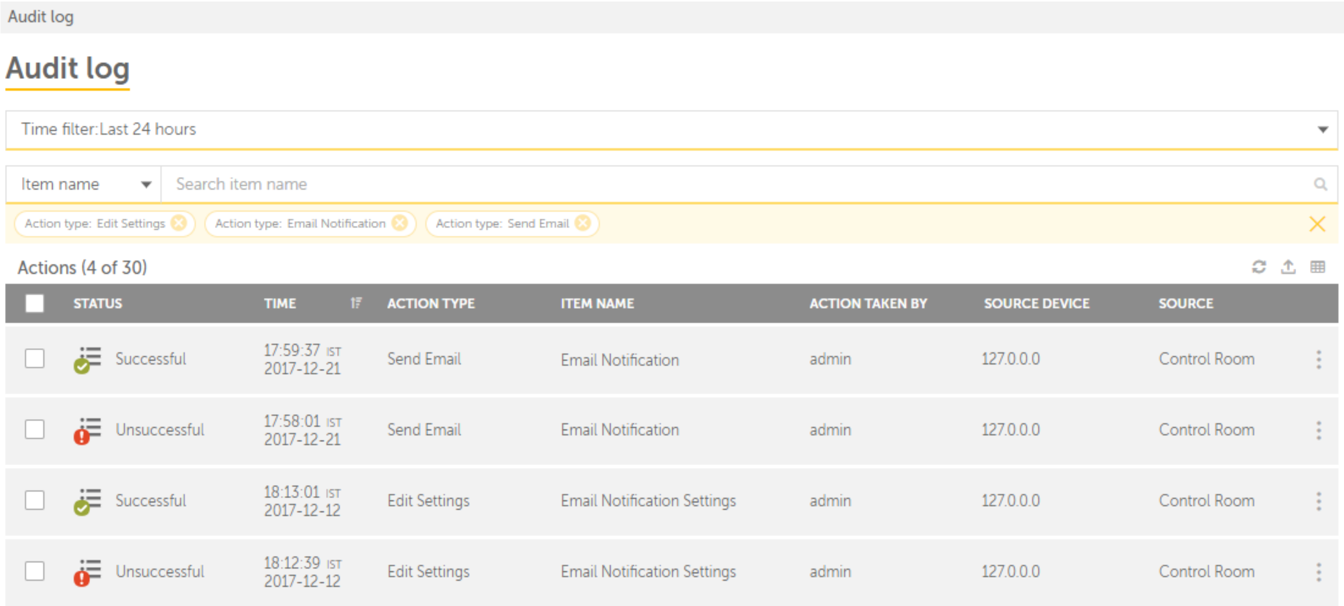
1. Clear the **Send email notifications** option.
2. Click 

3. Click OK



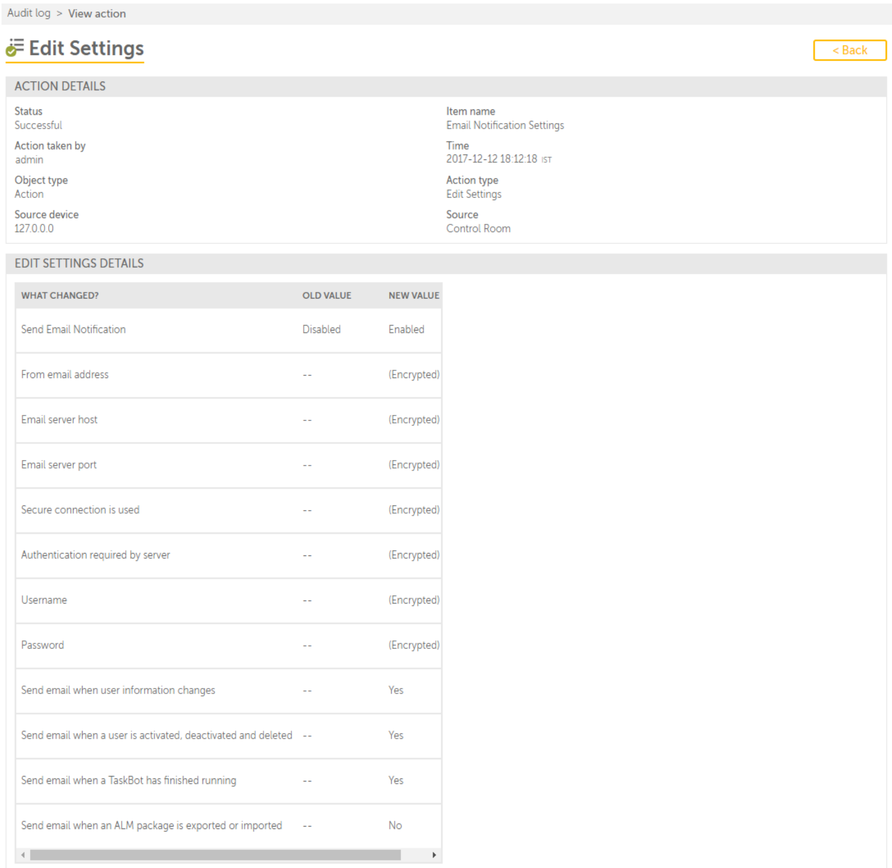
Audit Logs

All updates to the Email notification settings are captured in the **Audit Log** page. For example, the following illustration lists all actions performed to connect to the mail server and edit email notification settings :



To view details of each audit entry:

1. Go to the required data and mouse over
2. Click
3. The details page is launched where in you can view only those entries that are changed. The illustration below shows details of successful enabling of email notification settings, connection to the mail server, email server details, and actions for which notification will be sent:



Note: Some fields such as From email address, server host, port, authentication required or not, and credentials are shown as **(Encrypted)** because these values are securely stored in the Credential Vault.

Refer View Audit Details for more information.

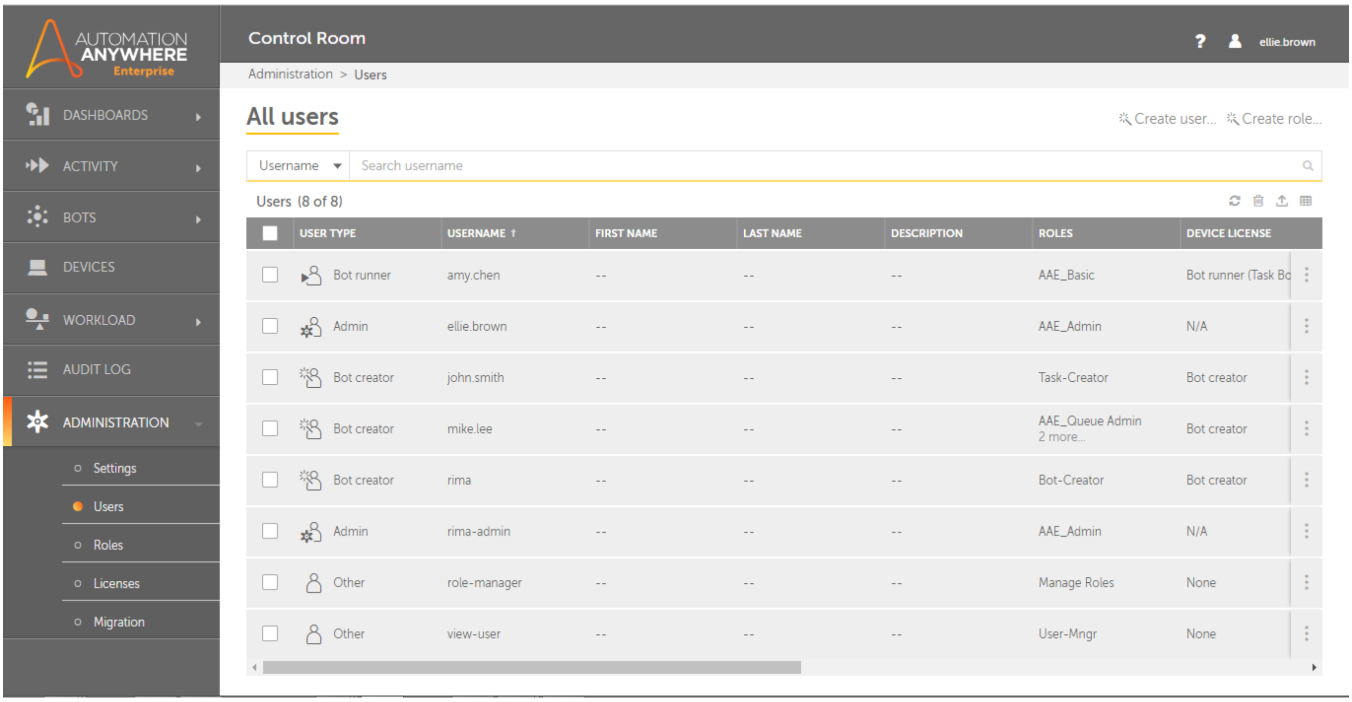
Users - An Overview

The **Users** page of Control Room gives a detailed information of existing users. As a Control Room user with user management privileges, you can view, edit, delete, and enable or disable a user. You can also perform other actions, such as delete multiple users, export the list of users in CSV format, refresh the list in the **Users** table, and show or hide columns in the **Users** table depending on your preferences,

Besides the above tasks, you can:

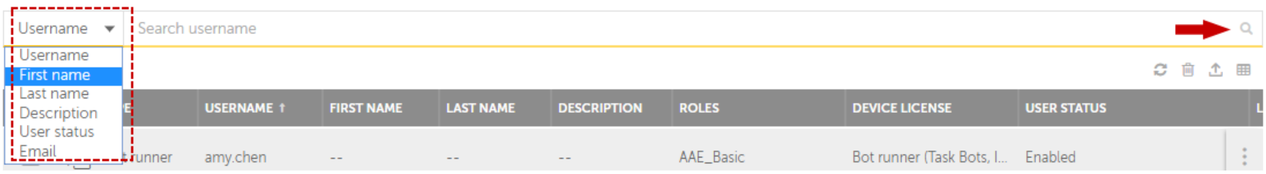
- Create a user
- Create a role

The page is illustrated in the following figure.



For ease of access, you can apply search parameters to Username, First Name, Last Name, Description, User Status, and Email columns.

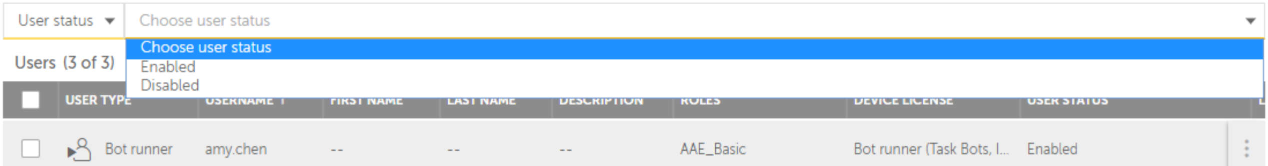
- You can use specify the search parameters in the search bar for Username, First Name, Last Name, Description, and Email columns:



Note: When you specify search parameters for the same column, the system searches using **OR** operator. When you specify search parameters for different columns, the system searches using **AND** operator.

Known Behavior: When you use special keys "-" or "_", the system lists all **Usernames** instead of **Usernames** having these parameters.

- You can choose the search parameters from a list in the search bar for **user status**:



Tip: You can perform the following actions on a column to help you work efficiently.

- Click a column to sort it in ascending and descending order. You can sort up to three columns by holding the Shift key when you click on two more columns. This gives you the option of sorting two additional columns. This way the sorting is done on the entire table and not just the data that is currently visible to you. The last sorting is stored in memory applied by a user per session.
- Use a drag-and-drop operation to move the column left or right.
- Move your mouse cursor at the end of the column and drag to re-size.

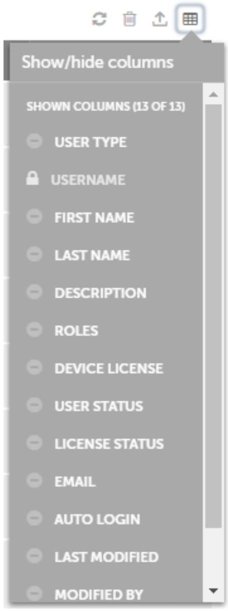
You can perform the following tasks on an individual User by moving your mouse over the Actions icon.

Item	Description
Edit	Click this icon to Edit details about the user . **Note:** • An email is sent when you edit a user if SMTP is enabled. • A non admin user with user management permissions can **only view** the **Admin** and **Locker Admin** users in the Users list but cannot edit these users.
View	Click this icon to view additional information about the user. Refer View user details.
Enable/ Disable	Click this icon to activate or deactivate the user. This is useful in scenarios when you want to temporarily restrict a user's access to Client or Control Room. **Note:** When you activate or deactivate a user, an email is sent to the user if SMTP is enabled.
Delete	Click this icon to delete the user. You can use this feature in scenarios when a user leaves the organization or is moved to another role. This frees the device to which the user was attached and the license allocated to the user is freed. Learn more **Note:** When you delete a user, an email is sent to the user if SMTP is enabled.

You can also perform the following table-level actions for a set of multiple activities.

Note: These actions can be performed only at a table-level and not on individual items.

Table Item	Description
Refresh	Refreshes the table and reflects the latest data.
Delete	Deletes the selected users. Learn more **Note:** You cannot delete a user who is currently logged in.
Export to CSV	Exports the selected items in the table in CSV format.
Show/ Hide columns	Allows you to select the columns that you want to show or hide in the table.

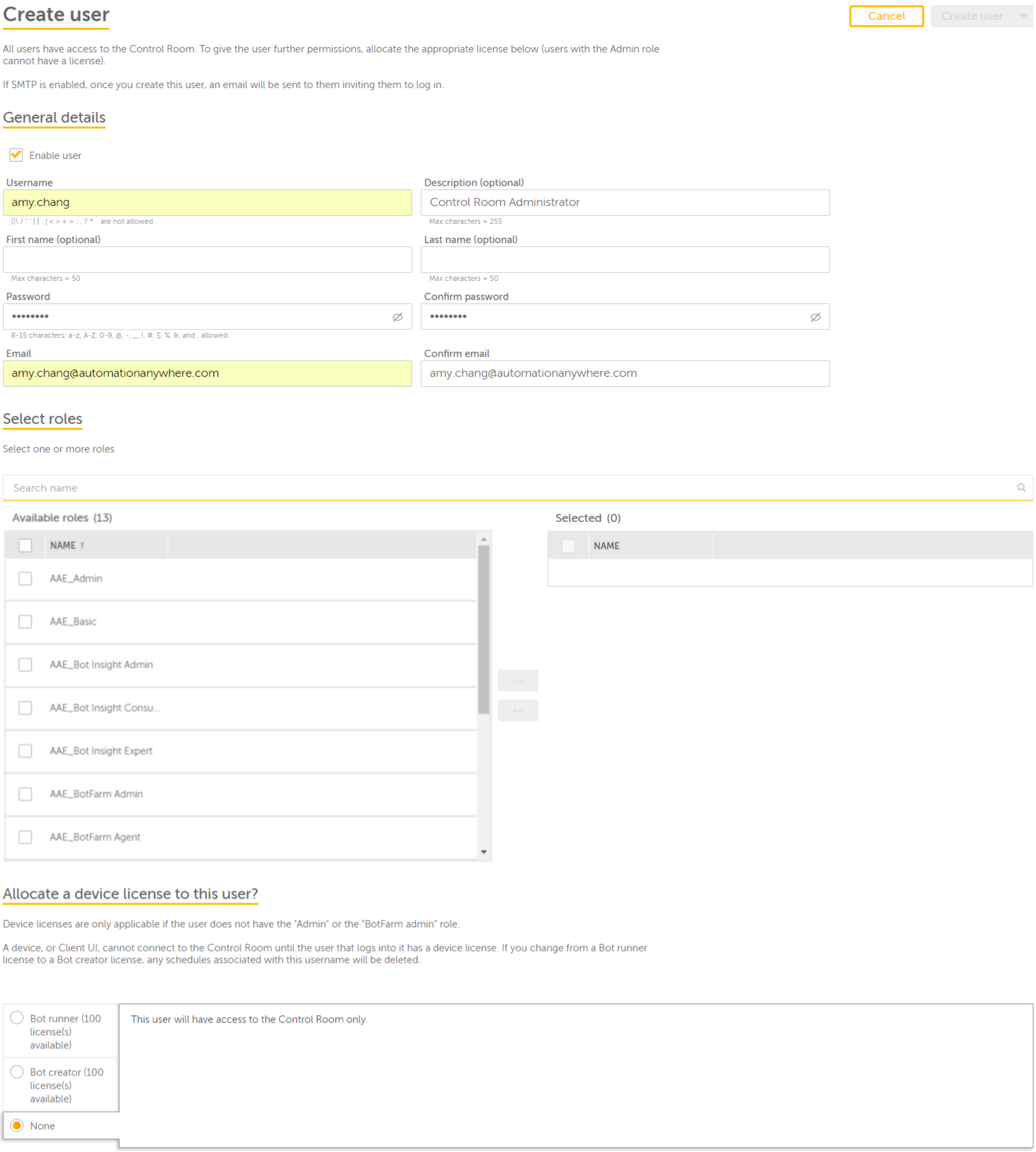
	

Show/hide columns
SHOWN COLUMNS (13 OF 13)
USER TYPE
USERNAME
FIRST NAME
LAST NAME
DESCRIPTION
ROLES
DEVICE LICENSE
USER STATUS
LICENSE STATUS
EMAIL
AUTO LOGIN
LAST MODIFIED
MODIFIED BY

Create a non-active directory user

To create a user, perform the followings steps.

1. Log on to Control Room with administration privileges.
2. Navigate to the users page. The Users page is displayed.
3. Click the Create user link . The **Create user** page is displayed.



4. In the **General details** area, do the following
   - **Username:** Type a user name for the user.

> **Note:** You can use the "@" character to accommodate email user-names.

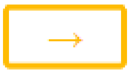
- **Description:** Type a description for the user. This is optional.
- **First name:** Type the first name for the user. This is optional.
- **Last name:** Type the last name for the user. This is optional.

> **Note:** The number of characters allowed in First name and Last name is 50.

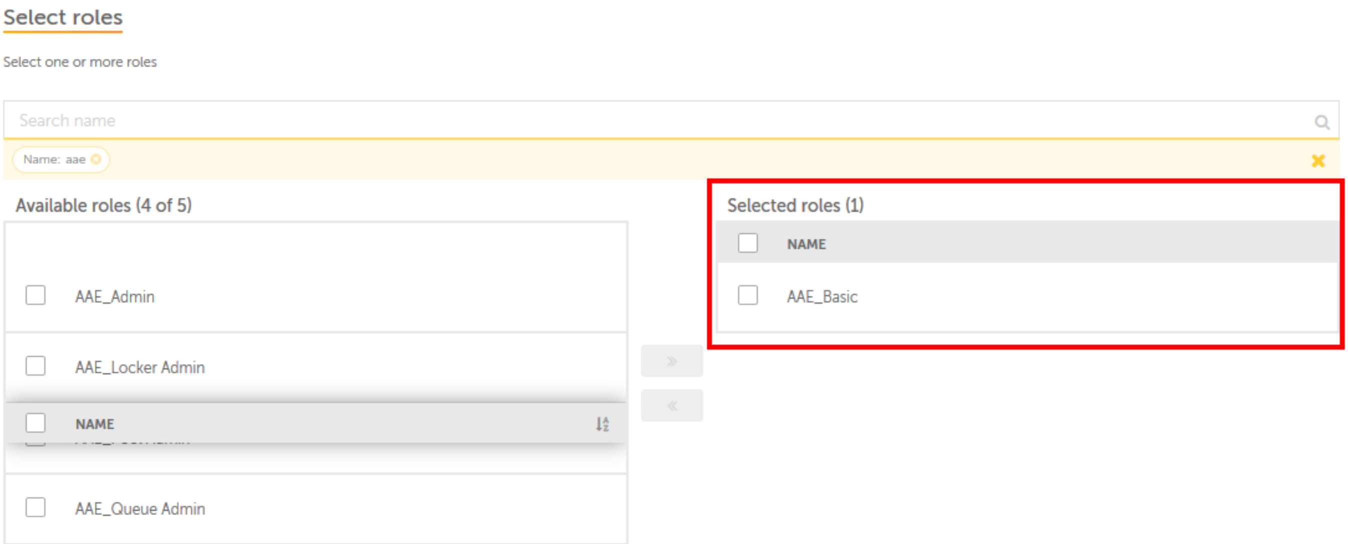
- **Password:** Type a password for the user. Ensure that you are assigning a password that follows the password policy of your organization. For more information on password policy settings, refer **Security** in Configuration Settings.

> **Note:** If Email Notification is enabled then the password field is not displayed to the user; an email is sent to the user to set the password.

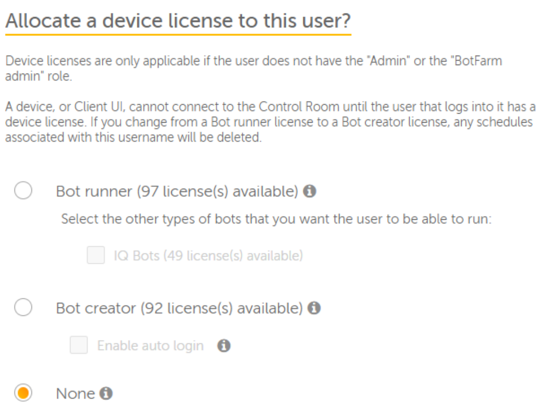
- **Confirm password:** Type the password again. This should be same to what you typed in the **Password** field.
- **Email:** Type the e-mail address for the user. If e-mail setting are enabled, the user is sent an email to this address to confirm the account. All important Control Room notifications will be sent to this e-mail address.
- **Confirm email:** Type the email address again. This should be same to what you typed in the **Email** field.

5. Select a role for the user from the **Available roles** table in the **Select roles** area and click the add button .You can select multiple roles for the user. The role is added to the **Selected roles** area. Depending on the role that you assign to a user, the user will have privileges and permissions to access and perform action in certain areas of Control Room. For example, a user with an AAE_Basic role can view the Dashboard, Activities, Bots, and to manage lockers and queues.

> **Note: View Dashboard, Manage my credentials and locker, View and manage my queues:** These permissions are available to any Control Room user by default. A non-admin user does not have access to **Admin, BotFarm Admin, Pool Admin, Locker Admin** roles.

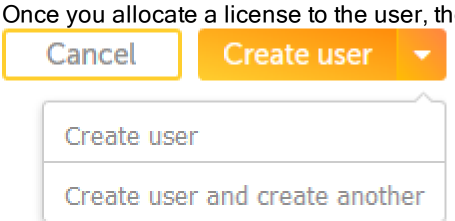


6. Select a license to be allocated to the user from the **Allocate a device license to user** area.



- **Bot runner:** This allows the user to run bots and and requires a run-time license. Additionally, select the **IQ Bots** check box, if you want to grant the user to run Bots.
- **Bot creator:** This allows the user to create and build automation, such as TaskBots, MetaBots, and Workflows and requires a development license. Additionally, you can select the **Enable auto login** check box, if you want the Client UI of the user to remember the credentials of the user. A column in users page is displayed, wherein the value for auto login is either **N/A or Can auto login**. **N/A** is displayed when auto login option is not checked, hence disabled. **Can auto login** is displayed when auto login option is enabled.
- **None:** This allows the user to only access Control Room. Users with this license cannot run or create bots. This option can also be used to release the allocated license.

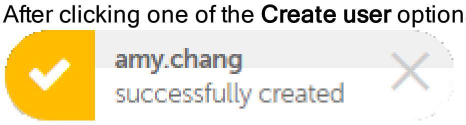
7. Once you allocate a license to the user, the Create user button is enabled.



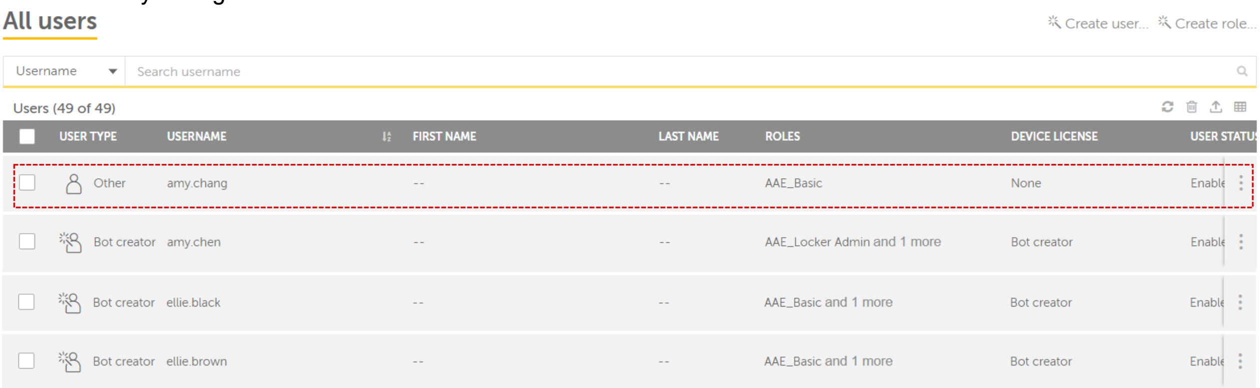
The **Create user** button has two options.

- **Create user:** This creates the user and the **Users** page is displayed.
- **Create user and create another:** This creates the user and the **Create user** page is refreshed so that you can create another user.

8. After clicking one of the **Create user** options, the user is created and the following message is displayed.



The user "amy.chang" is reflected in the **All users** list



Edit non-active directory user details

As a Control Room user having edit user permission, you can modify the details of a user from the Users page. This is useful in scenarios where you may want to change the role of a user or when users forget their password or when their email address is changed.

Note: If roles/ permissions for any user is updated, the user must re-login or refresh the browser for the changes to be immediately reflected on Control Room UI.

You can change the following details for a user.

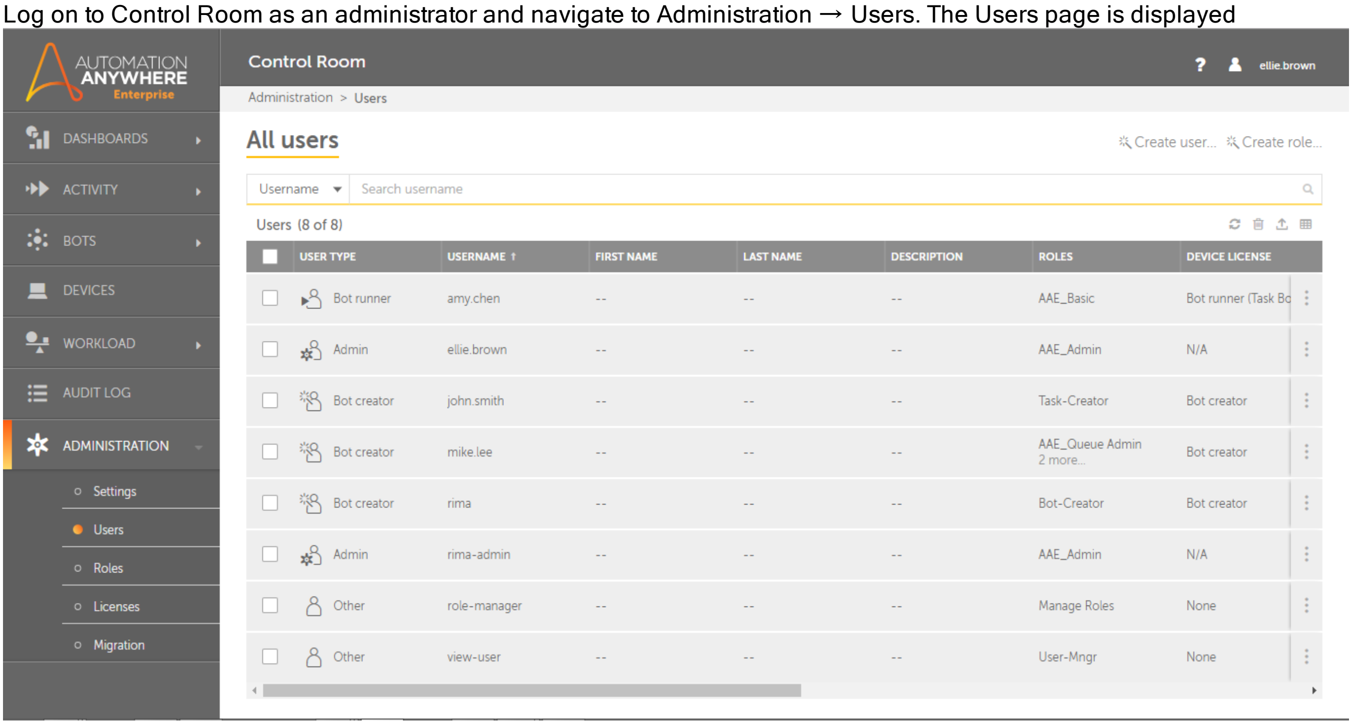
- First name
- Last name
- Password
- Email
- Roles
- Licenses

Note:

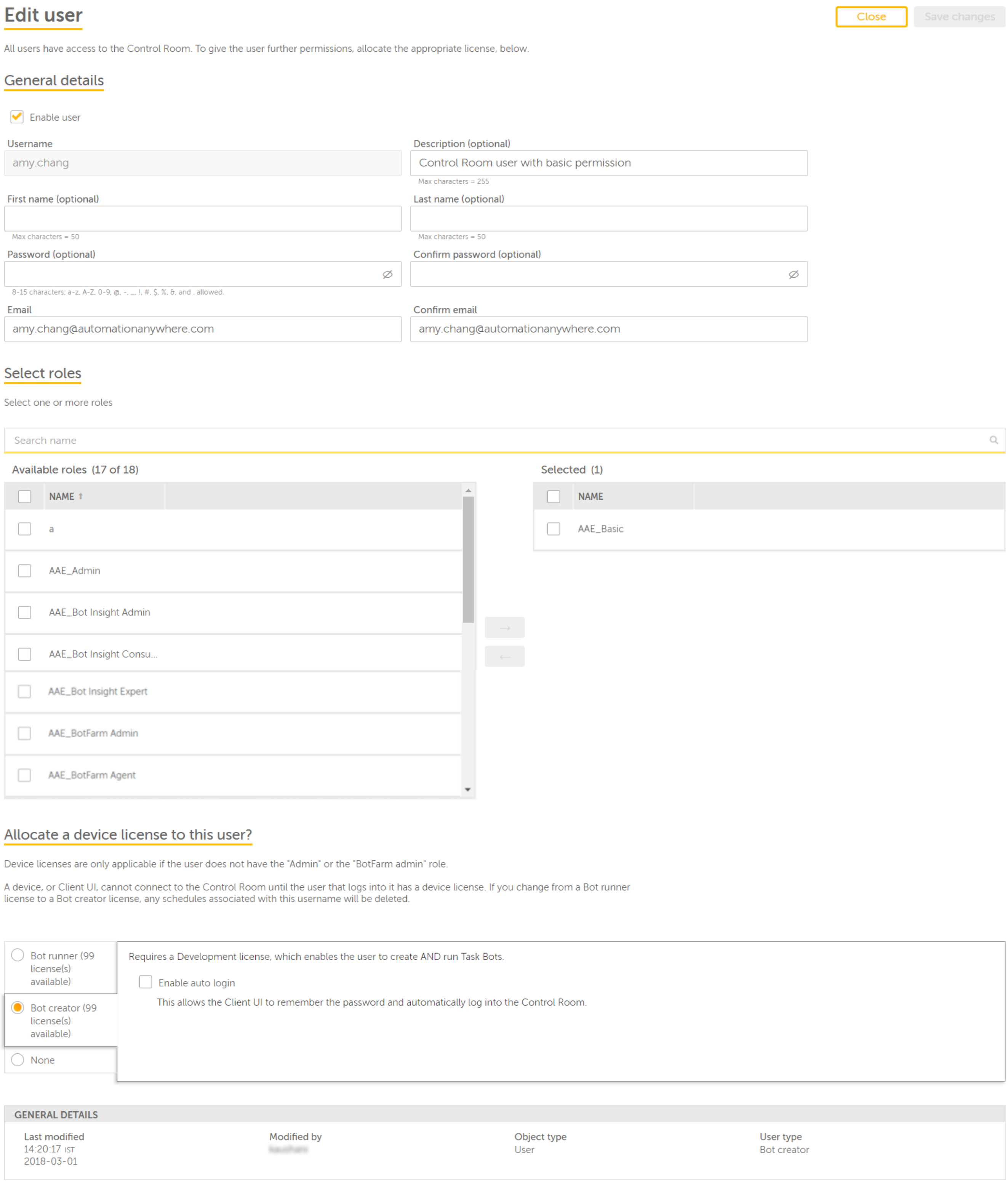
- You cannot change the **User name** for a user.
- You cannot change or edit your own details except from User Profile tray. To change the details of your own profile, refer to Edit and update your profile.
- In case when Email Notification is enabled when you edit the details of a user, an email is sent to the user. Learn more

To edit the details of a user, perform the following steps.

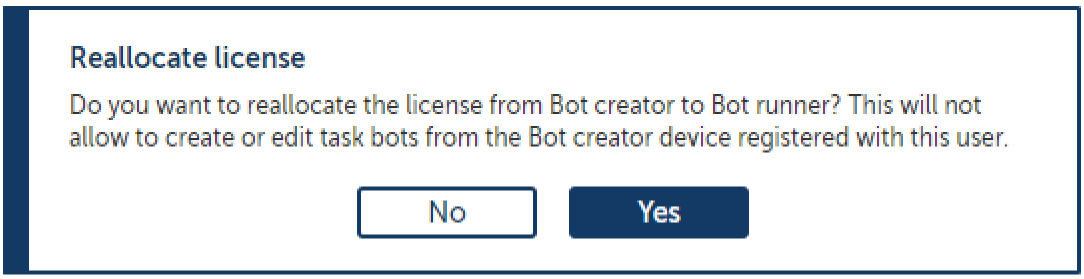
1. Log on to Control Room as an administrator and navigate to Administration → Users. The Users page is displayed



2. Move your mouse over the Actions icon and click the Edit user icon . The **Edit user** page is displayed.



3. Make changes to the fields depending on your requirements. For example, you can reallocate license of a Bot Creator to Bot Runner.



While making any updates, ensure that you are aware as to what changes are applicable.

4. Click the **Save Changes** button. The changes are made and a successfully edited message is displayed.

Note: `These changes are audit logged and authorized users can refer to it in the future.`

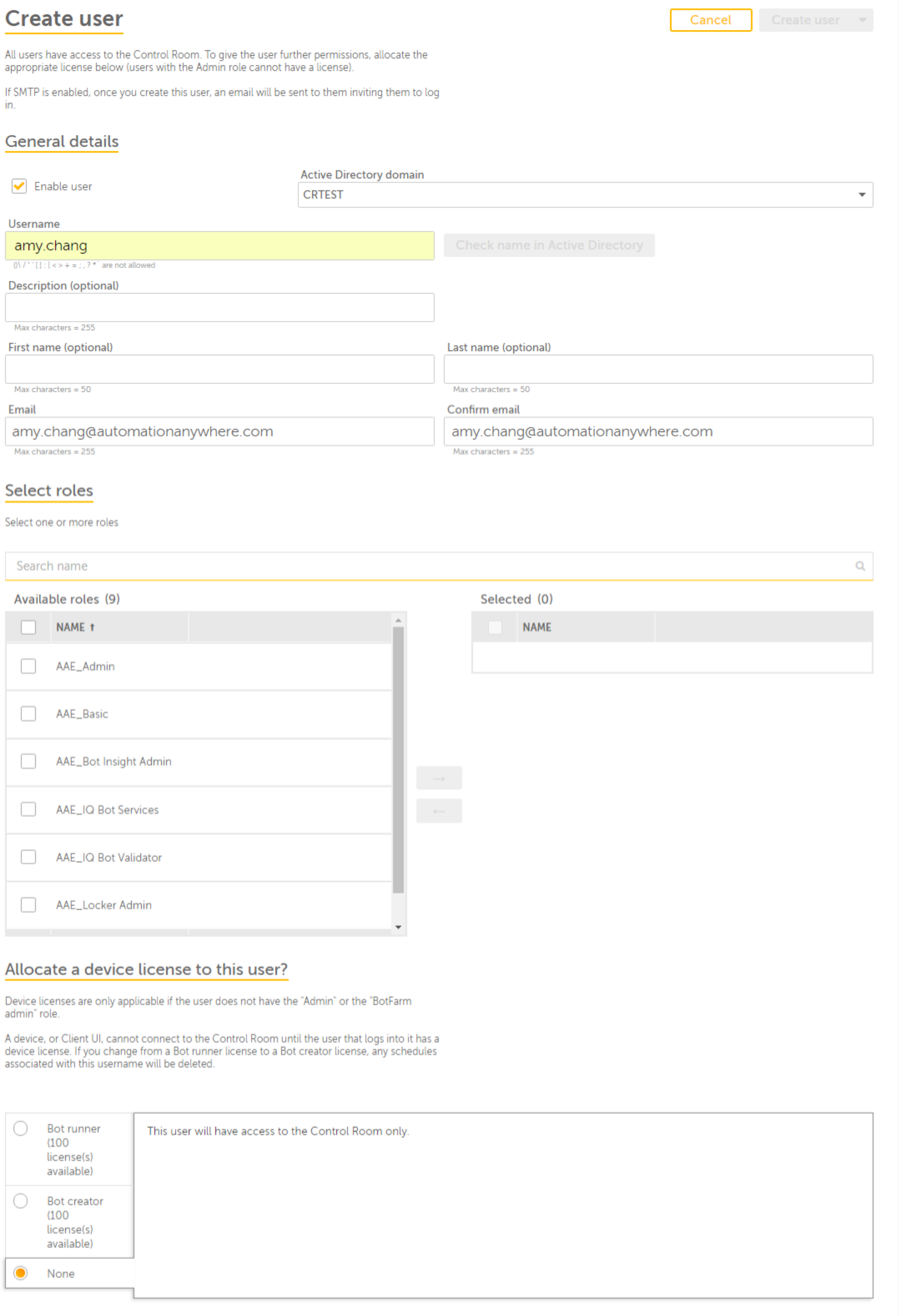
Create an active directory user

The process of creating an active directory user is different from creating a non-active directory user as the user must be a part of an active directory.

To create an active directory user, perform the following steps.

1. Log on to Control Room with administration privileges.
2. Navigate to the Users page. The **Users** page is displayed.

3. Click the Create user link . The **Create user** page is displayed.



4. In the **General details** area, do the following

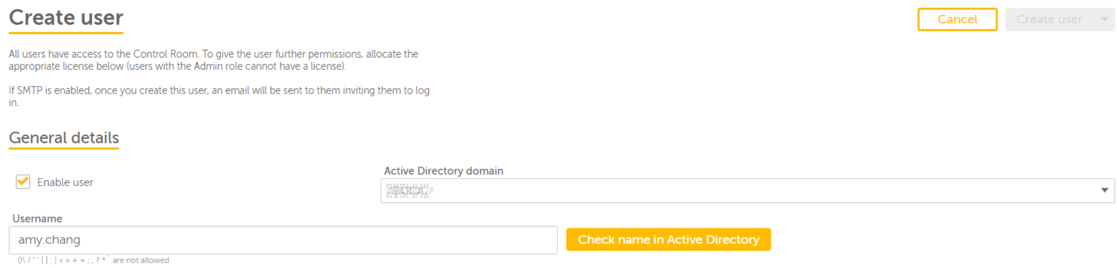
- **Enable user:** Select this check box to enable the user.
- **Active Directory domain:**Select the active directory name for the user. The list displays all domains that are available in AD domain controller.

> **Note:** Control Room Active Directory supports single forest multi-domain environment.

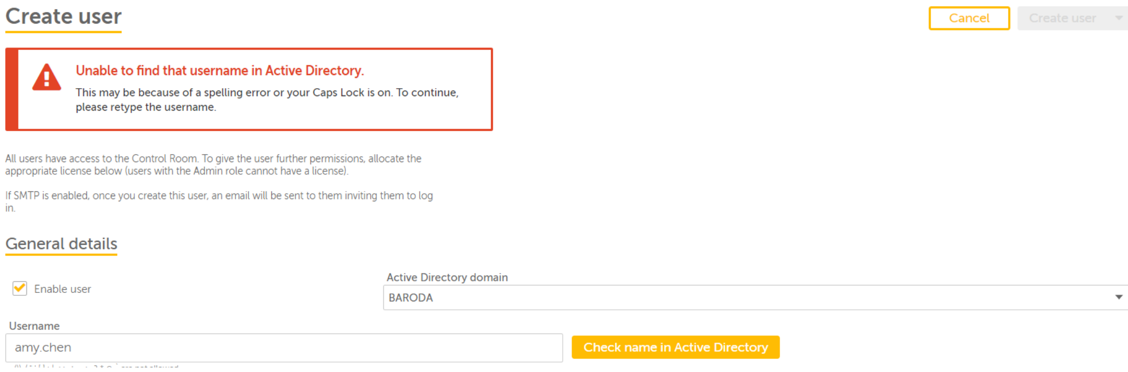
- **Username:** Type a user name for the user, the **CHECK NAME IN ACTIVE DIRETORY** button is enabled. When you click the **CHECK NAME IN ACTIVE DIRETORY** button, one of the following happens.

> **Note:** The "@" character is supported to accommodate email user-names.

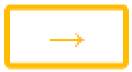
  - If the user name is present in the active directory, the **First name**, **Last name**, **Email**, and **Confirm email** fields are automatically displayed, as shown in the following figure.

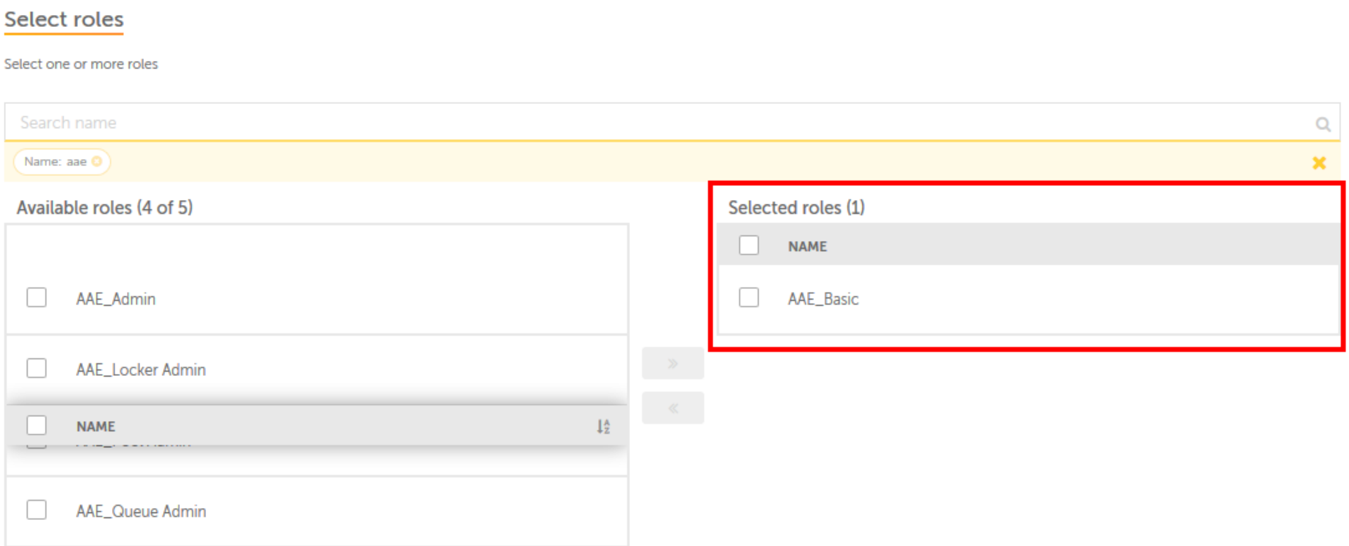


  - If the user name is not present in the active directory, an error message is displayed, as shown in the following figure. Contact your network administrator to resolve the issue.

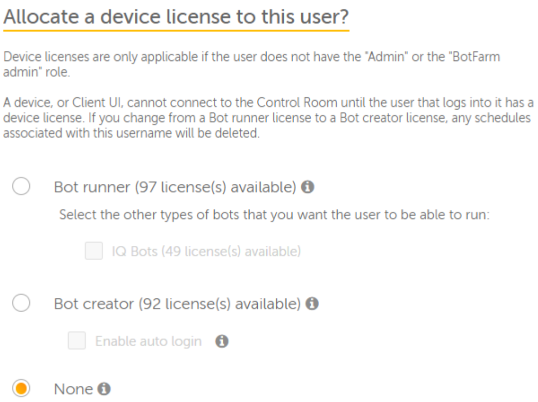


- In Active Directory environment details such as: First Name, Last Name, Email address are auto-populated from AD and hence user does not need to type-in. In case the data is not populated from AD then user must specify the details.

5. Select a role for the user from the **Available roles** table in the **Select roles** area and click the add button . The role is added to the **Selected roles** area.

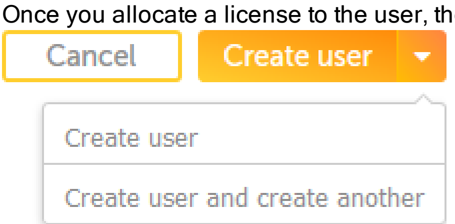


6. Select a license to be allocated to the user from the **Allocate a device license to user** area. By default, there are three licenses available.



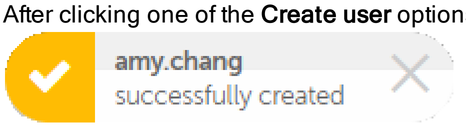
   - **Bot runner:** This allows the user to run bots and and requires a run-time license. Additionally, select the **IQ Bots** check box, if you want to grant the user to run IQ Bots.
   - **Bot creator:** This allows the user to create and run task bots and and requires a development license. Additionally, you can select the **Enable auto login** check box, if you want the Client UI of the user to remember the credentials of the user. A column in users page is displayed, wherein the value for auto login is N/A or Can auto login. **N/A** is displayed when auto login option is not checked and **Can auto login** is displayed when auto login option is enabled.
   - **None:** This allows the user to only access Control Room. Users with this license cannot run or create bots.

7. Once you allocate a license to the user, the **Create user** button is enabled.



   The **Create user** button has two options.
   - **Create user:** This creates the user and the Users page is displayed.
   - **Create user and create another:** This creates the user and the **Create user** page is refreshed so that you can create another user.

8. After clicking one of the **Create user** options, the user is created and the following message is displayed.



Edit active directory user details

As an administrator, you can edit the details of an active directory user from the Users page This is useful in scenarios where you may want to change the role, email address of users or when users forget their password.

Note: If roles/ permissions for any user is updated, the user must re-login or refresh the browser for the changes to be immediately reflected on Control Room UI.

You can change the following details for a user.

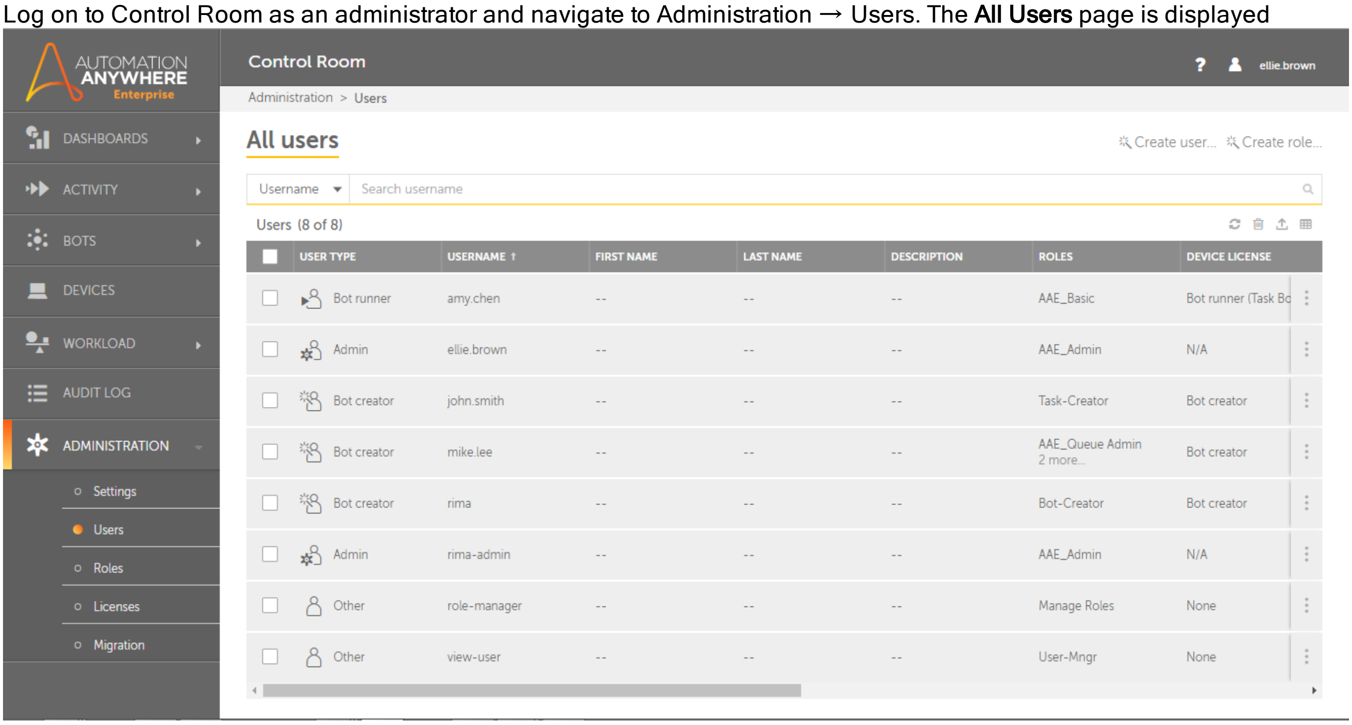
- First name
- Last name
- Password
- Roles and Licenses

Notes:

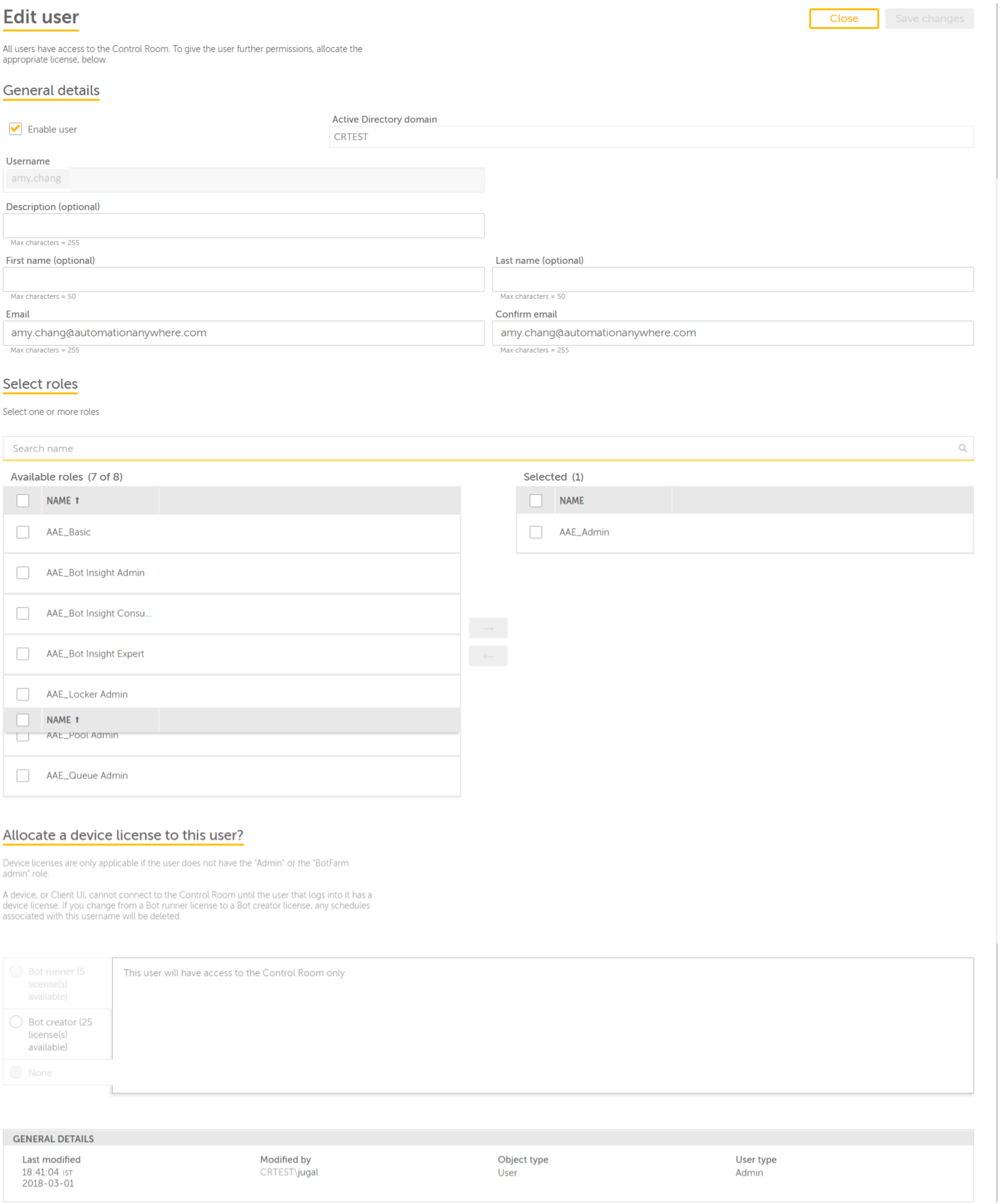
- You cannot change the **User name** and **Active Directory domain** for a user.
- You cannot change or edit your own profile. Contact you administrator to make the changes.
- When you edit the details of a user, an email is sent to the user.

To edit the details of a user, perform the following steps.

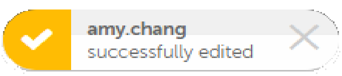
1. Log on to Control Room as an administrator and navigate to Administration → Users. The **All Users** page is displayed



2. Move your mouse over the Actions icon and click the Edit user icon . The **Edit user** page is displayed.



3. Make changes to the fields depending on your requirements.
4. Click the **Save Changes** button. The changes are made and a successfully edited message is displayed.

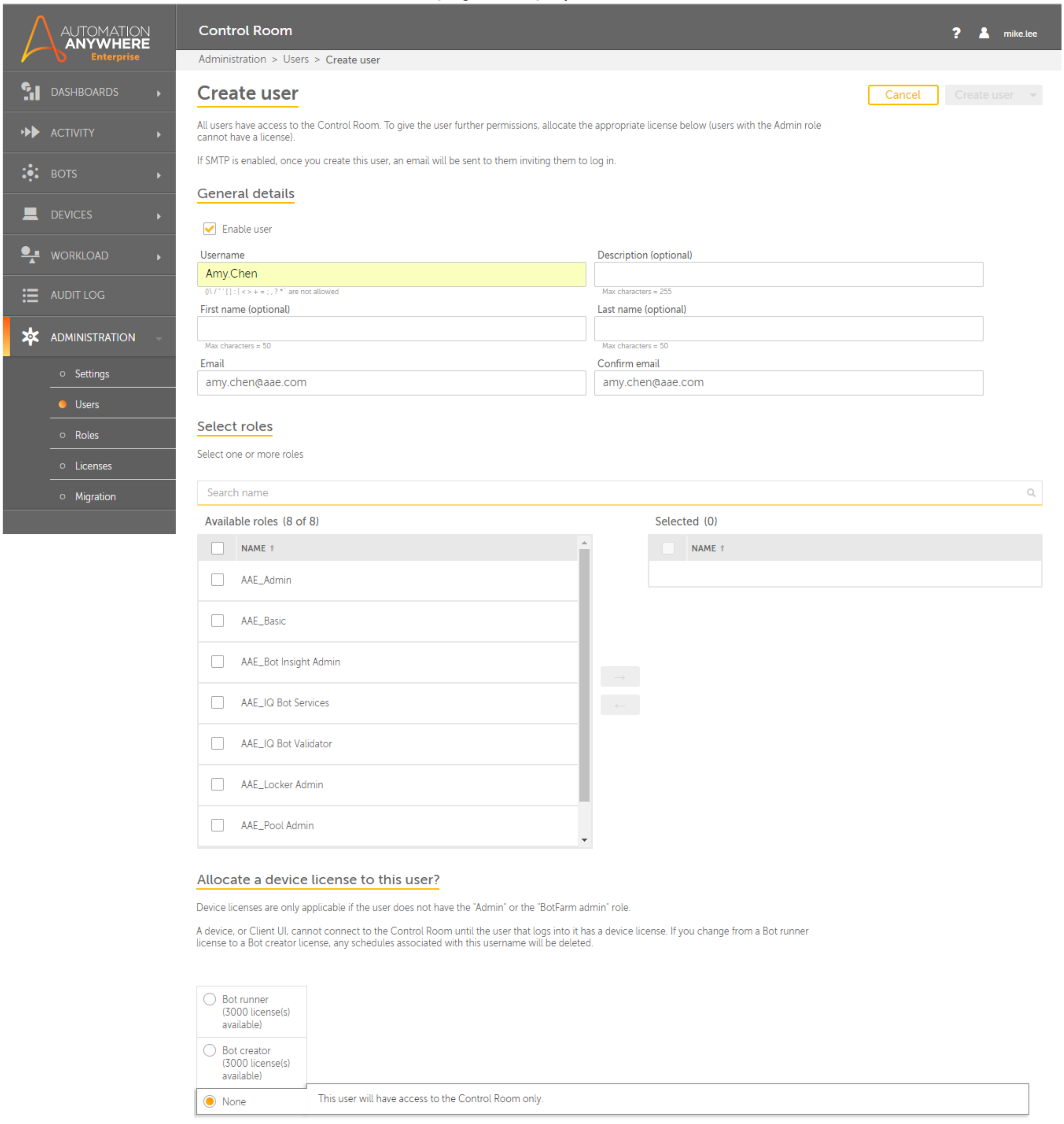


Add user from IdP server for single sign on

The process of adding a user from the IdP server in a Control Room that is configured for Single Sign On is similar to creating an active directory user.

To create an sso user, perform the following steps.

1. Log on to Control Room with administration privileges.
2. Navigate to the Users page. The **Users** page is displayed.
3. Click the Create user link . The **Create user** page is displayed.



4. In the **General details** area, do the following

- **Username:** Type a user name for the user.

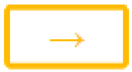
Tip: Ensure that the **Username** is the same as provided in the **IdP Server**.

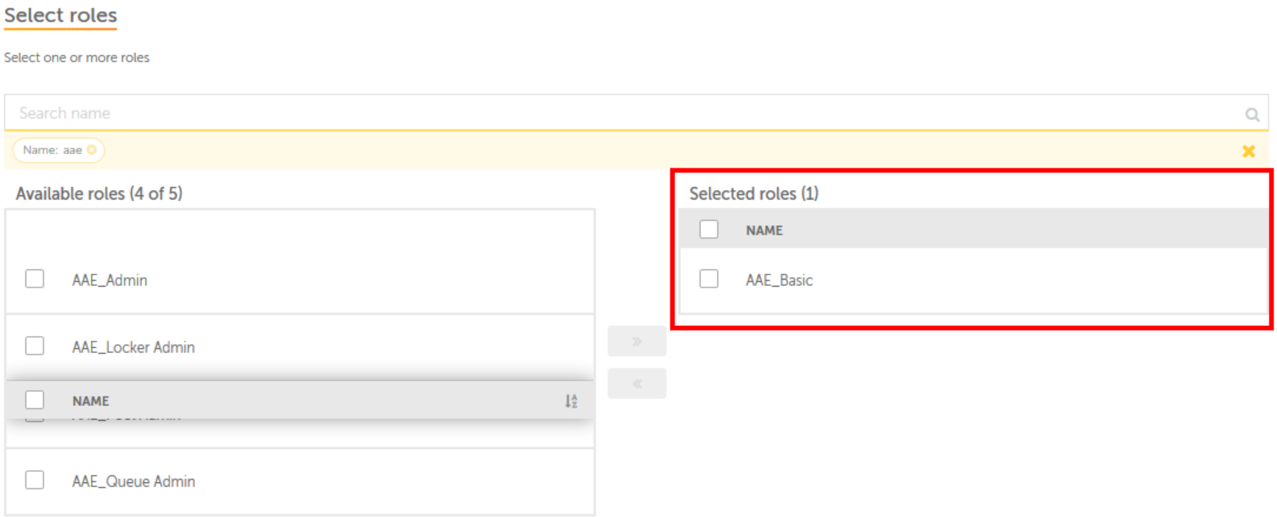
> **Note:** The "@" character is supported to accommodate email user names.

- **Description:** Type a description for the user. This is optional.
- **First name:** Type the first name for the user. This is optional.
- **Last name:** Type the last name for the user. This is optional.

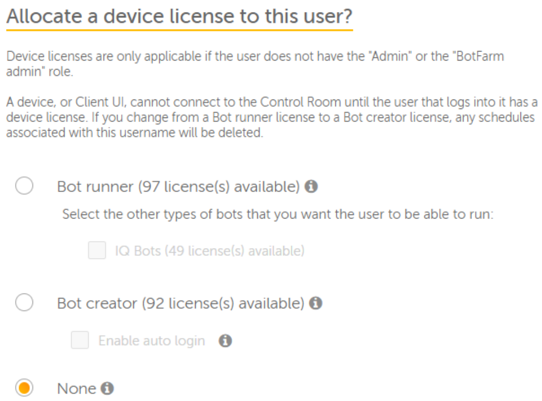
> **Note:** The number of characters allowed in First name and Last name is 50.

- **Email:** Type the e-mail address for the user. If e-mail setting are enabled, the user is sent an email to this address to confirm the account. All important Control Room notifications will be sent to this e-mail address.
- **Confirm email:** Type the email address again. This should be same to what you typed in the **Email** field.

7. Select a role for the user from the **Available roles** table in the **Select roles** area and click the add button . The role is added to the **Selected roles** area.



8. Select a license to be allocated to the user from the **Allocate a device license to user** area. By default, there are three licenses available.



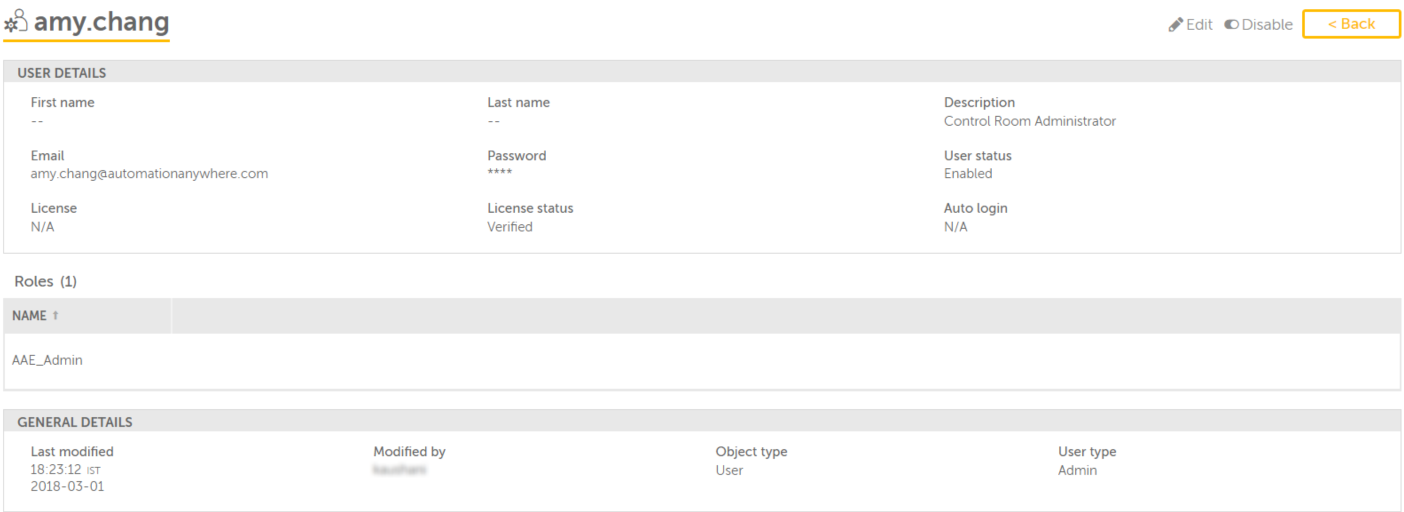
- **Bot runner:** This allows the user to run bots and and requires a run-time license. Additionally, select the **IQ Bots** check box, if you want to grant the user to run IQ Bots.
- **Bot creator:** This allows the user to create and run task bots and and requires a development license. Additionally, you can select the **Enable auto login** check box, if you want the Client UI of the user to remember the credentials of the user. A column in users page is displayed, wherein the value for auto login is N/A or Can auto login. **N/A** is displayed when auto login option is not checked and **Can auto login** is displayed when auto login option is enabled.
- **None:** This allows the user to only access Control Room. Users with this license cannot run or create bots.

View user details

A Control Room user with view user permission, you have access to **View users** page.

When you click the **View** icon for an individual user in the **All users** page, the **View user** page is opened in read only mode. It provides information, such as the user details, roles, and general details, such as Last modified, Modified by, Object type, and User type. Besides this, you can also edit details of the user and enable or disable the user using the enable/ disable toggle button.

> **Note:** `For Active Directory users, the password field is not displayed.`



The different areas of the **View user** page are explained in the following table.

Area	Description
User details	Use this area to view the following details of the folder • **First name:** The first name of the user. • **Last name:** The last name of the user • **Description:** The description of the user. • **Email:** The email address of the user • **Password:** The password of the user • **User status:** The status of user, whether enabled or disabled. • **License:** The license type of the user, such as bot runner, bot creator and other license types. • **License status:** The status of the license for the user. This may be verified or unverified.
Roles	The roles assigned to the user.
General details	Use this area to view the following details for the folder. • **Last Modified:** Displays the last time changes were made to the user in date and time. • **Modified by:** Displays the name of the user who last made changes to the user in date and time. • **Object type:** Displays the type of the bot, such as Task Bot, Meta Bot, or IQ Bot. • **User type:** The type of user, such as Bot creator, Bot runner, Admin or Other.

Edit idp user details

As a Control Room user having edit user permission, you can modify the details of a user from the Users page. This is useful in scenarios where you may want to change the role of a user or when users forget their password or when their email address is changed.

Note: If roles/ permissions for any user is updated, the user must re-login or refresh the browser for the changes to be immediately reflected on Control Room UI.

You can change the following details for a user.

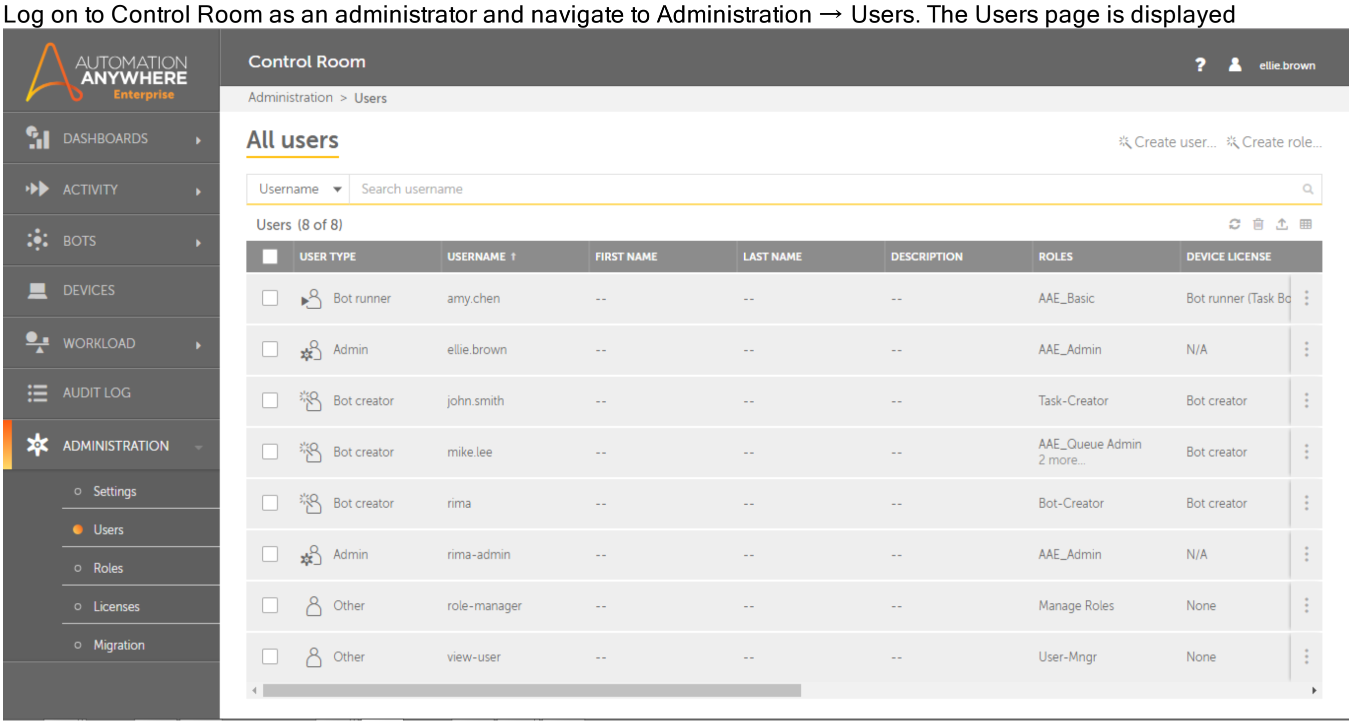
- First name
- Last name
- Email
- Roles
- Licenses

Note:

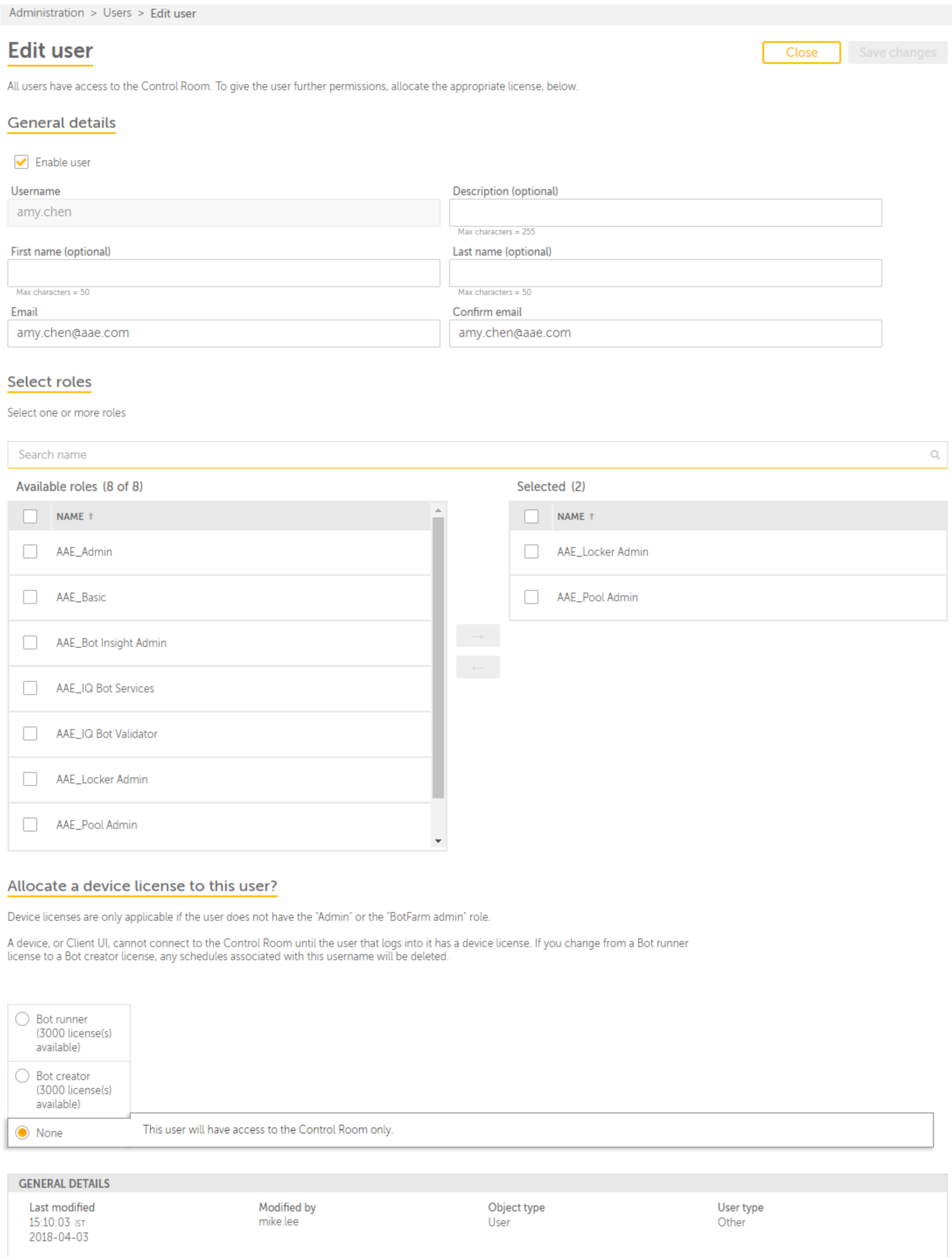
- You cannot change the **User name** for a user.
- You cannot change or edit your own details except from User Profile tray. To change the details of your own profile, refer to Edit and update your profile.
- In case when Email Notification is enabled when you edit the details of a user, an email is sent to the user. Learn more

To edit the details of a user, perform the following steps.

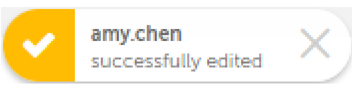
1. Log on to Control Room as an administrator and navigate to Administration → Users. The Users page is displayed



2. Move your mouse over the Actions icon and click the Edit user icon . The **Edit user** page is displayed.



3. Make changes to the fields depending on your requirements.
4. Click the **Save Changes** button. The changes are made and a successfully edited message is displayed.



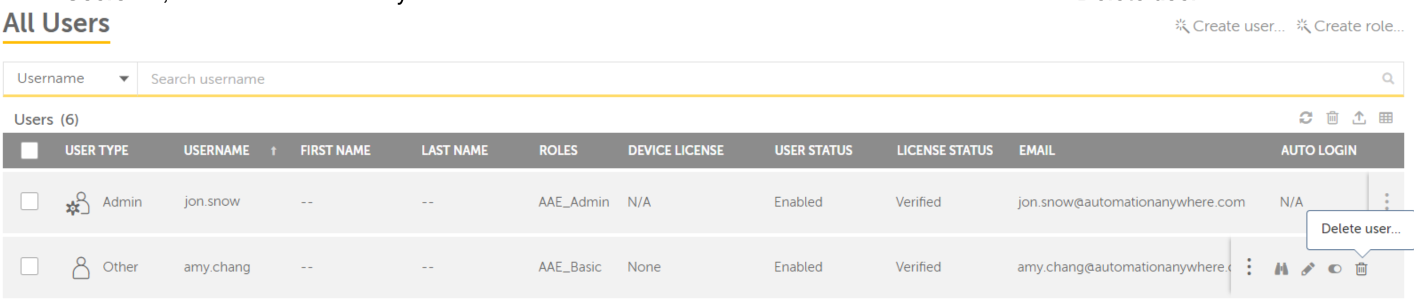
Note: These changes are audit logged and authorized users can refer to it in the future.

Delete a user

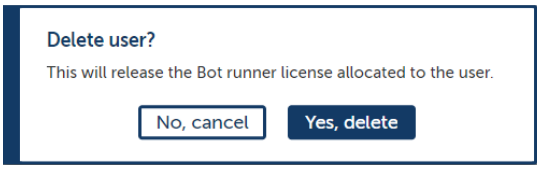
To remove redundant users, and free allocated license, a Control Room Admin user can Delete users.

To Delete a user, follow the steps mentioned below:

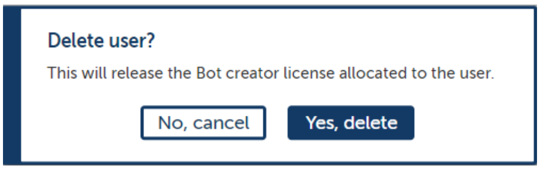
1. Go to Administration → Users
2. In the **Users** list, choose the user that you wish to delete. Then mouse over to the actions list and click **Delete user**



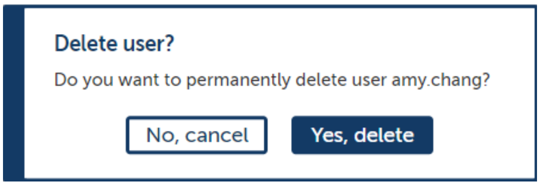
3. The following messages are displayed if the user is assigned:
   - **Bot Runner license**



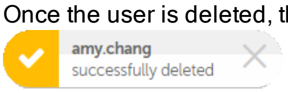
   - **Bot Creator license**



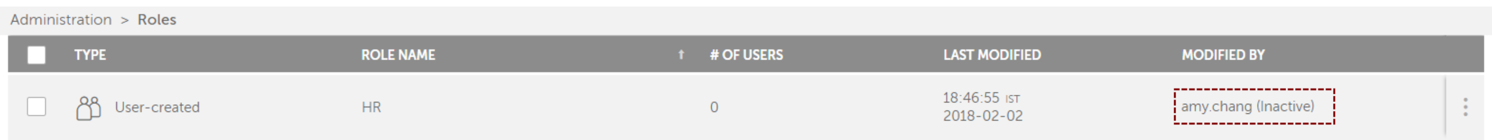
   - **None**



4. Once the user is deleted, the following notification is displayed:



5. When an admin user deletes "amy.chang" from Control Room,"amy.chang" is displayed as **Inactive**. As shown in the below mentioned screen shot. The deleted users are shown as Inactive appended to their name. This helps to identify the users that are not in use any more and have left the organization.



Roles - An Overview

This page allows an admin or user with roles permission to perform actions such as: Create, Edit, Delete roles for various features and operations in Control Room. RBAC (role based access control) grants access to users based on the assigned roles and the accessibility provided to the user.

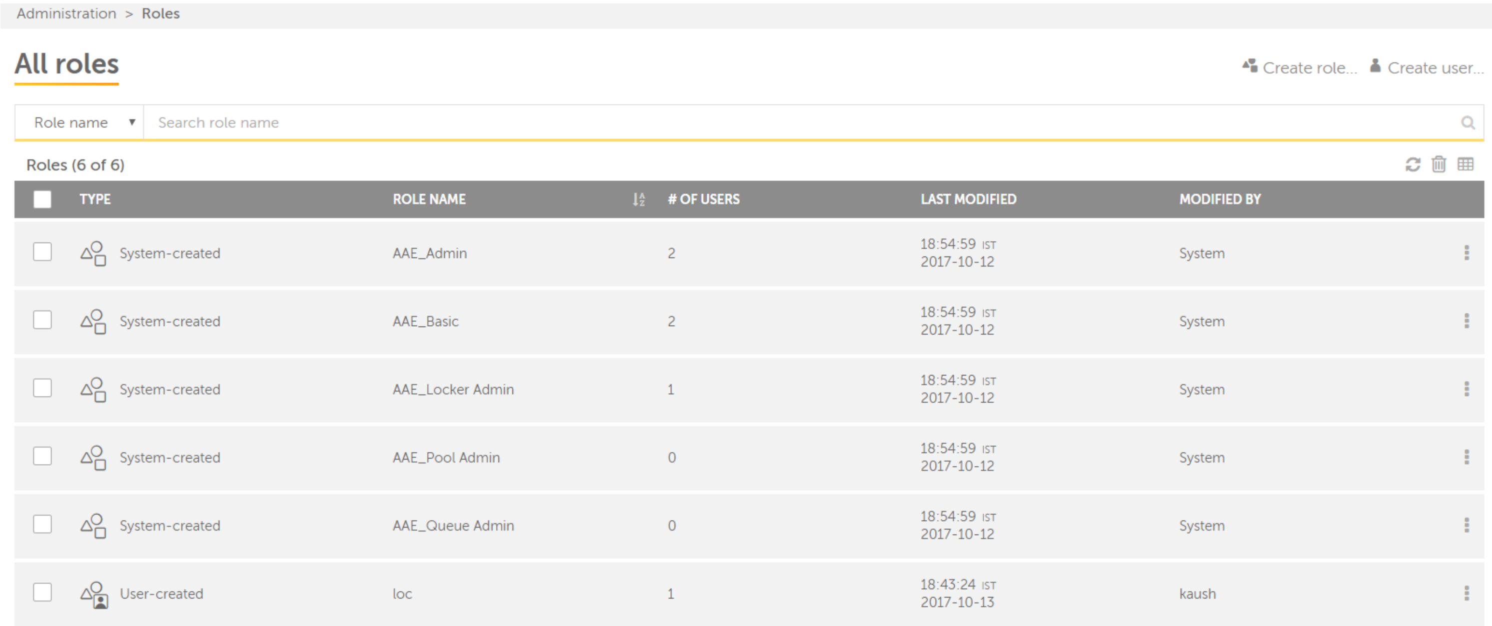
Benefits of creating roles

- Increased security by controlling users access according to their specified roles.
- Decreased need of customer support
- Easy and accurate monitoring of the use and access of data by higher management, leading to better research management.

In Control Room you can see two types of roles:

- **System- created**: These roles are pre-configured during Control Room installation.
- **User- created**: These roles are created by user themselves and can be customized accordingly.

> **Note:** If a **custom role /user-created role** is created with all Control Room permission then it is not considered as a Control Room Admin role. Only system created Admin role has this privilege.



- **Create role**: Allows user to create roles. Learn More
- **Create user**: Allows to create users in Control Room. Learn More
- In the search pane you can filter roles according to role name and role type.

> **Note:** When you specify search parameters for the same column, the system searches using **OR** operator. When you specify search parameters for different columns, the system searches using **AND** operator.

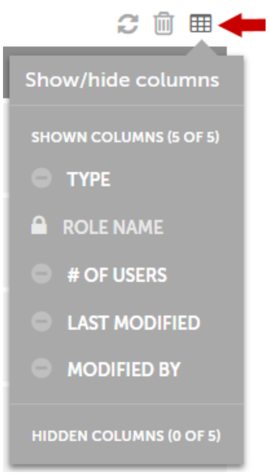
> **Tip:** You can perform the following actions on a column to help you work efficiently.
> - Click a column to sort it in ascending and descending order. You can sort up to three columns by holding the Shift key when you click on two more columns. This gives you the option of sorting two additional columns. This way the sorting is done on the entire table and not just the data that is currently visible to you. The last sorting is stored in memory applied by a user per session..
> - Use a drag-and-drop operation to move the column left or right.
> - Move your mouse cursor at the end of the column and drag to re-size.

The following describes the list of items that can be viewed in the table:

Table Item	Description
Type	Shows the type of role as system-created or user-created.
Role Name	Shows name of the role.
# of Users	Shows number of users accessing the role.
Last Modified	Shows date and time of role when it was last modified.
Modified By	Shows name of the user who last modified the role.

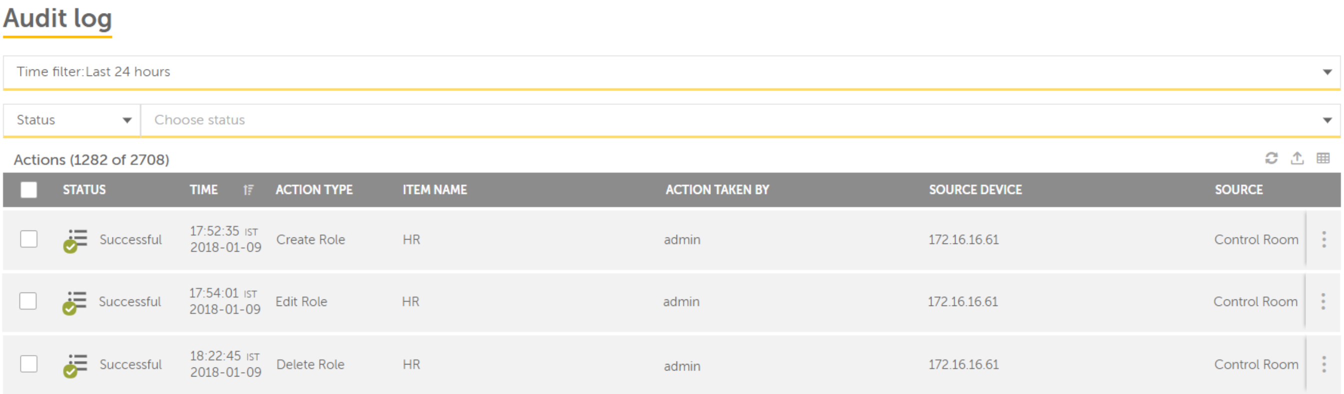
Table Item	Description
View	Allows you to view role details. Learn More
Edit	Allows you to edit a role. Learn More
Delete	Allows you to delete a role. Learn More
Copy	Allows you to copy a role. Learn More

Alternatively, you can select all roles and perform the following actions:

Table Item	Description
Refresh	Allows you to refresh the list of roles.
Delete	Allows you to delete selected roles from the list.
Show/ hide columns	Allows you to show or hide specific columns. By default, all the columns are displayed.  Tip: To **hide** a column, click the column name.

Audit Logs

All the **Create, Update, Delete** actions are tracked in audit log for record keeping and future use. You can refer those entries in the Audit Log page:

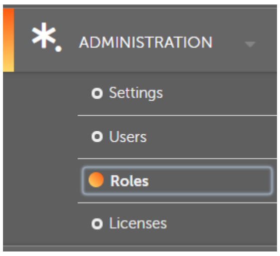


Create a role

Activities and access to Control Room for Users (Administrators, Clients, and non-Clients) are governed by the role defined for each. The role based accessibility model ensures each User has privileges to view information or data that is relevant to the role assigned by the Control Room Administrator. Therefore, only an admin or Control Room user with roles permission can assign roles to users and provide access to them for various features and operations.

To create a role, follow the steps mentioned below:

1. Go to *Administration → Roles*.



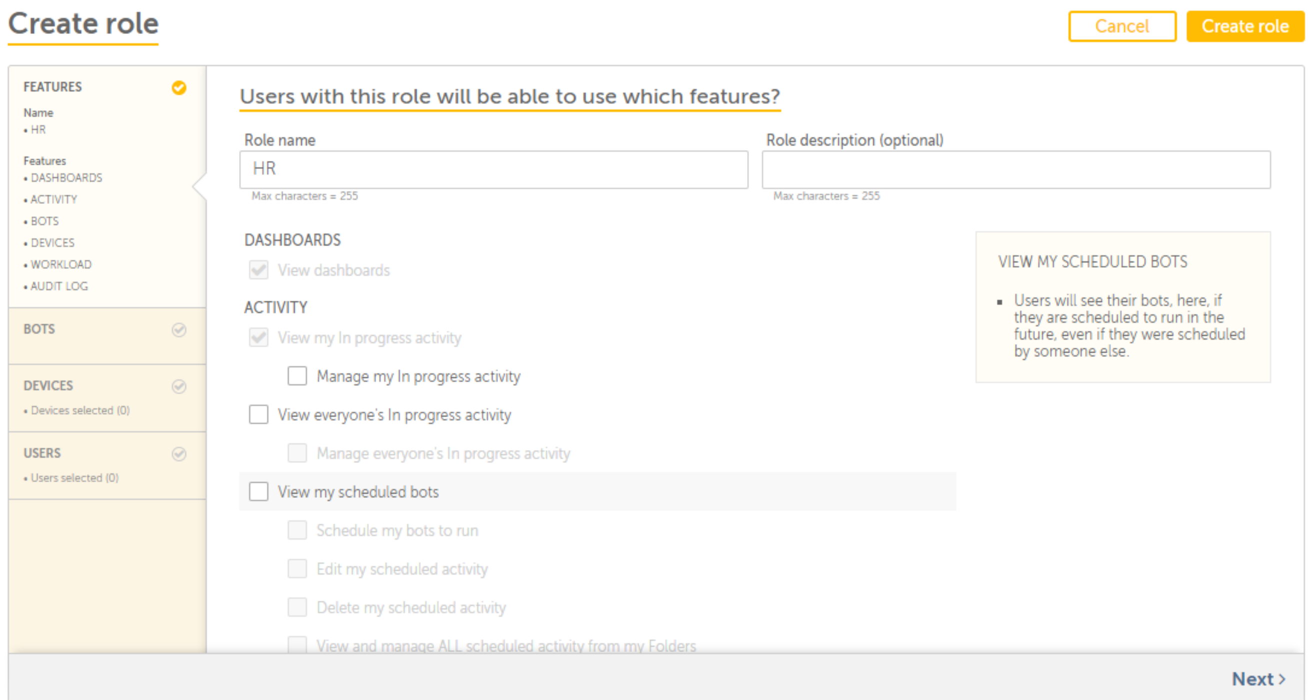
2. Click on Create Role.

3. Input the following information:
   - Name and description of the role.
   - Click individual sub-tabs such as: **Features, Bots, Devices, Users**and select required permissions that are relevant to the role you are creating.

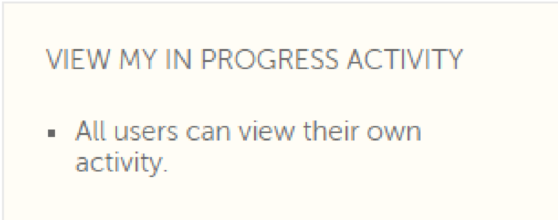
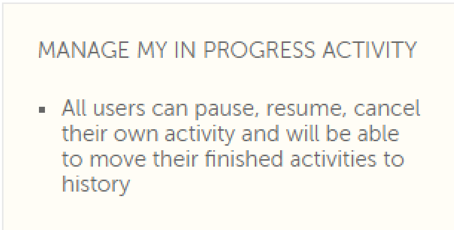
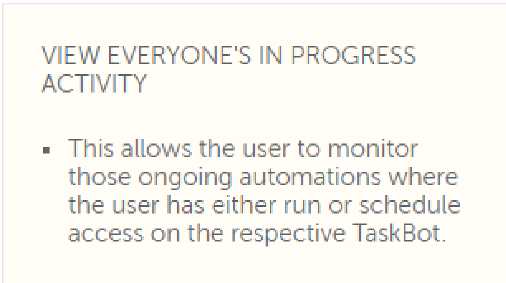
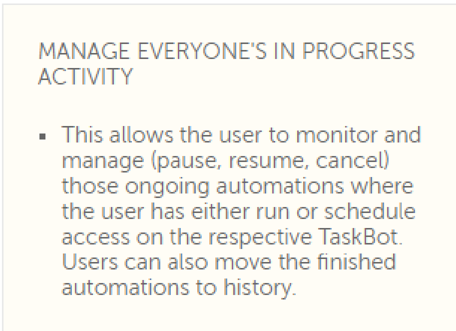
   > **Note: Bots and Devices** sub-tabs are displayed only if the required permission is selected from the Features sub-tab.

4. Input required information such as- role name, description, and check desired permissions. Click next, if you wish to add users.

> **Note:** Bot Insight, BotFarm, and IQ Bot roles are displayed only if you have respective licenses.



- You can **assign the following permissions** to your role:

Features	Permissions
Dashboard	• **View dashboards** **Note:** This permission is checked and disabled by default since it is available to all users.
Activity	• **View my In progress activity** **Note:** This permission is checked and disabled by default since it is available to all users.  • **Manage my In progress activity**  • **View everyone's In progress activity**  • **Manage everyone's In progress activity**  • **View my scheduled bots** • **Schedule my bots to run**

	SCHEDULE MY BOTS TO RUN ▪ This requires the ability to view and manage Bot runners ▪ Therefore, if you select this feature, the following features will automatically be selected ▪ View and manage my Bot runners and Bot creators • **Edit my scheduled activity** EDIT MY SCHEDULED ACTIVITY ▪ Users can edit their scheduled bots, even if they were scheduled by someone else. • **Delete my scheduled activity** DELETE MY SCHEDULED ACTIVITY ▪ Users can delete their scheduled bots, even if they were scheduled by someone else. • **View and manage ALL scheduled activity from my Folders** VIEW AND MANAGE ALL SCHEDULED ACTIVITY FROM MY FOLDERS ▪ Users can view, edit and delete all the schedules on the bot Folders which the user has access to. This includes the schedules that the user has created and also created by others. • **View and manage ALL scheduled activity** VIEW AND MANAGE ALL SCHEDULED ACTIVITY ▪ Users can view, edit and delete all the schedules in the system. This includes the schedules that the user has created and also created by others.
Bots	• **View my bots** VIEW MY BOTS ▪ This allows users to view bots that you will choose on the next page of the wizard • **Run my bots**

RUN MY BOTS

- This requires the ability to view and manage Bot runners
- Therefore, if you select this feature, the following features will automatically be selected
  - View and manage my Bot runners and Bot creators

- **Export bots**

  EXPORT BOTS

  - This allows user to export bots and their dependencies from Control Room. User can export only those bots and dependencies on which user has download permission.

- **Import bots**

  IMPORT BOTS

  - This allows user to import bots and their dependencies into Control Room. User can import only those bots and dependencies on which user has upload permission.

- **Create Folders**

  CREATE FOLDERS

  - This allows user to create folders within the folders that they have access to

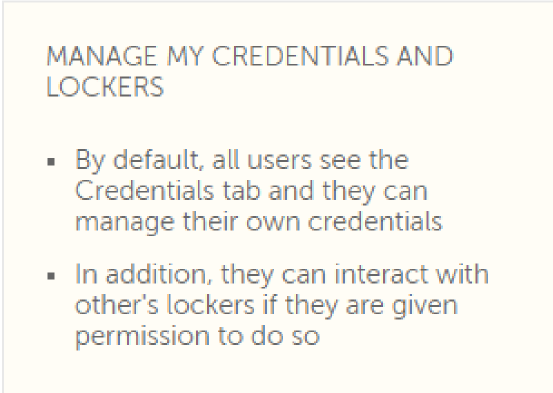
- **Rename Folders**

  RENAME FOLDERS

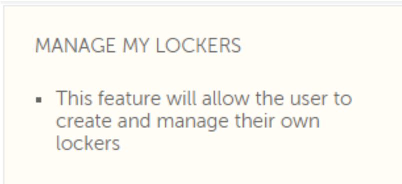
  - This allows user to rename folders within the folders that they have access to. Note that only empty folders can be renamed

- **Manage my credentials and lockers**

  Note: This permission is checked and disabled by default since it is available to all users.

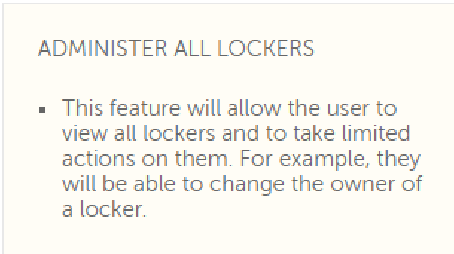
<table>
<tr>
<td></td>
<td>


Manage my lockers



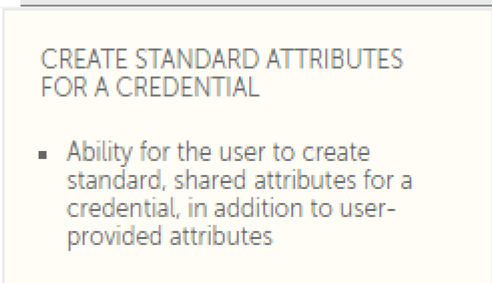
Administer all lockers

Note: This permission is available only for Locker Admin role and cannot be granted to any other roles.



Create Standard Attributes for a Credential

Note: This permission is available only for Locker Admin role and cannot be granted to any other roles.



</td>
</tr>
<tr>
<td>Devices</td>
<td>
View and manage my Bot runners, and device pools

Note: This permission is checked and enabled by default since it is available to all users.
</td>
</tr>
</table>

	VIEW AND MANAGE MY BOT RUNNERS, BOT CREATORS AND DEVICE POOLS ▪ This feature is required if the user will need to run bots or schedule bots • **Create device pools** CREATE DEVICE POOLS ▪ This feature will allow the user to create and manage their own pools • **Administer all device pools** **Note:** This permission is available only for Locker Admin role and cannot be granted to any other roles. ADMINISTER ALL DEVICE POOLS ▪ This feature will allow the user to manage all pools in the system. • **View and manage BotFarm** VIEW AND MANAGE BOTFARM ▪ Only users with the system-created Admin role can view and manage BotFarm functionality
Workload	• **View and manage my queues** **Note:** This permission is checked and disabled by default since it is available to all users. VIEW AND MANAGE MY QUEUES ▪ This feature will allow the user to create and manage queues • **Create queue** CREATE QUEUES ▪ This feature will allow the user to create and manage their own queues • **Administer all queues**

	ADMINISTER ALL QUEUES ▪ This feature will allow the user to manage all queues in the system. • **SLA Calculator** SLA CALCULATOR ▪ This feature will allow the user to calculate SLA.
Audit Log	• **View everyone's audit log actions** VIEW EVERYONE'S AUDIT LOG ACTIONS ▪ This feature allows the user to view everyone's actions in the Audit Log, not just their own • **Archive audit log actions** ▪ This allows the user to archive selected audit log records. Archived audit log will be removed from Audit Log table and stored separately.
Administration	• **View and manage settings** **Note:** This permission is available only for Control Room Admin role and cannot be granted to any other roles VIEW AND MANAGE SETTINGS ▪ Only users with the system-created Admin role can view and manage Settings • **View users** VIEW USERS ▪ This will allow the user to View all users in the system, although they will not be able to edit them • **Create users** • **Edit users**

	EDIT USERS ▪ This will allow the user to Edit all users in the system, even if they did not create them • **Delete users** DELETE USERS ▪ This will allow the user to Delete any user in the system, even if they did not create them • **View and manage roles** • **View and manage Migration** VIEW AND MANAGE MIGRATION ▪ Only users with the system-created Admin role can view and manage migration • **View licenses** VIEW LICENSES ▪ This will allow the user to view the license details • **Manage user's device licenses** MANAGE USER'S DEVICE LICENSES ▪ This allows to assign device licenses to users. • **Install License** INSTALL LICENSES ▪ This allows the user to install Automation Anywhere Enterprise licenses from Control Room
API	• **Bot Auto-Login Credentials API** BOT AUTO-LOGIN CREDENTIALS API ▪ This allows the user to set the Auto-Login Credentials of other users via API. • **Bot Insight Data API**

	BOT INSIGHT DATA API ▪ This feature will allow access to Bot Insight RESTful APIs to the data logged by the Control Room, and by a task during 'Production' runs.
IQ Bot	• **Validator** VALIDATOR ▪ Permissions to access IQ Bot Validator screen for reviewing documents with exceptions. Limited access to Control Room features. • **Console** CONSOLE ▪ Permissions to manage Learning Instances and Bots on the IQ Bot Platform along with Dashboard access. Limited access to Control Room features.

- **System- created roles:** These roles are pre-configured during Control Room installation

> Note: System-created roles cannot be deleted or edited, except assigning or removing users from the role.

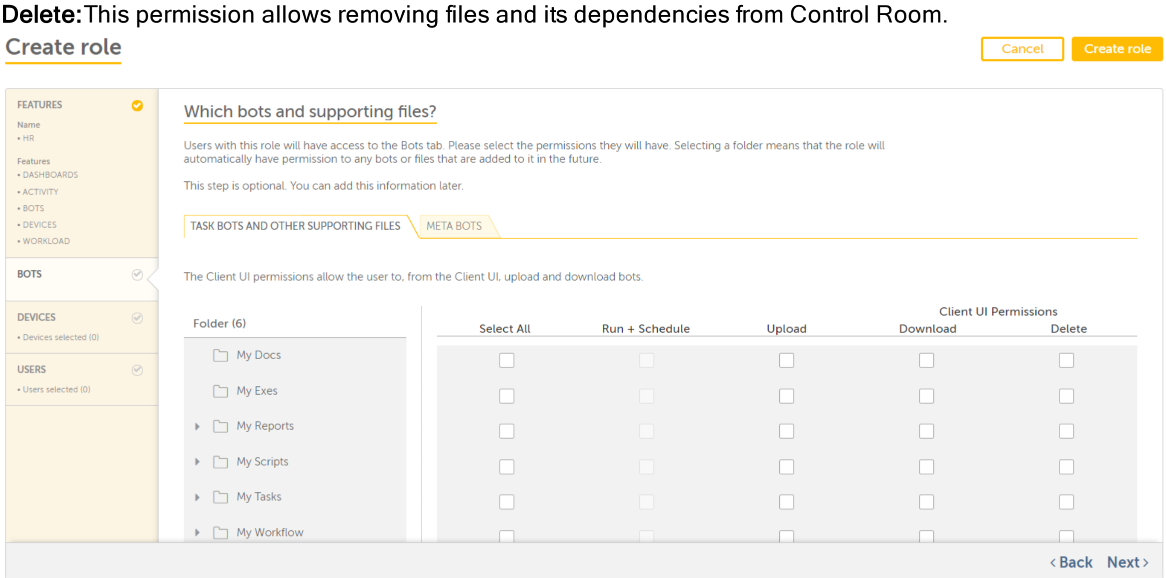
Default Roles	Description
AAE_Admin	This role allows access to all features, including creating other Admin users and access to all folders and files. The only role that can access Control Room settings.
AAE_Locker Admin	This role allows to view all credentials and all lockers. A Locker Admin can change the owner of a credential that they do not own. For lockers they do not own, they can delete the locker, edit permissions, and remove credentials. **Note:** This permission is not applicable to Control Room Admin role.
AAE_Basic	This role provides permissions to upload and download Task Bots in the My Tasks folder. Limited access to other features.
AAE_Pool Admin	This role allows user to view and manage all device pools. **Note:** Users with AAE_Pool Admin do not have permission to see any bots and supporting files.

AAE_Queue Admin	This role allows user to view and manage all queues.
AAE_Bot Insight Admin	This role provides permission to view and manage data in Bot Insight. Limited access to Control Room features. (If Bot Insight license is installed). It allows a user to access BotInsight RESTful APIs to get access to the data logged by the Control Room, and by a task during 'Production' run.
AAE_Bot Insight Consumer	This role allows permissions to view data in Bot Insight. Limited access to Control Room features. (If Bot Insight license is installed)
AAE_Bot Insight Expert	This role provides permission to manage data in Bot Insight. Limited access to Control Room features. (If Bot Insight license is installed)
AAE_BotFarm Admin	This role provides BotFarm admin privileges to the user.
AAE_BotFarm Agent	This role provides view and manage privileges to the user.
AAE_IQ Bot Validator	This role allows user to install Automation Anywhere Enterprise licenses from Control Room
AAE_IQ Bot Services	This role grants a user the permissions to access IQ Bot Validator screen for reviewing documents with exceptions. Limited access to Control Room features.

5. In the **Bots tab**, you can check permissions for the following:

> **Note:** `Bots tab is visible only if` **`'View my bots'`**`permission is selected in Features tab.`

- **TaskBots and other supporting files** - You can check the following permissions:
- **Select all -** This permission includes upload, download, execute, delete, Run + Schedule actions.
- **Run + Schedule -** This permission includes run and schedule permission for TaskBots i.e. allows user to run and/or schedule Bots. This permission is enabled only if user has either **Run my bots** or **Schedule my bots to run** permission.
  - This permission is termed as **Run** when the user has **Run my bots** feature permission. You can explicitly select Run permission on a specific folder to allow the user to run all bots that belong to this folder.
  - Similarly, this permission is termed as **Schedule** when the user has **Schedule my bots to run** feature permission. You can explicitly select Run permission on a specific folder to allow the user to schedule all bots that belong to this folder.
  - It is termed as **Run + Schedule** when user has both feature permissions. This allows the user to run and schedule bots that belong to this specific folder on which the permission is selected.
- **Upload:** This permission allows uploading TaskBot files/ folder to Control Room from Client.
- **Download:**This permission allows downloading TaskBot from Control Room.
- **Delete:**This permission allows removing files and its dependencies from Control Room.

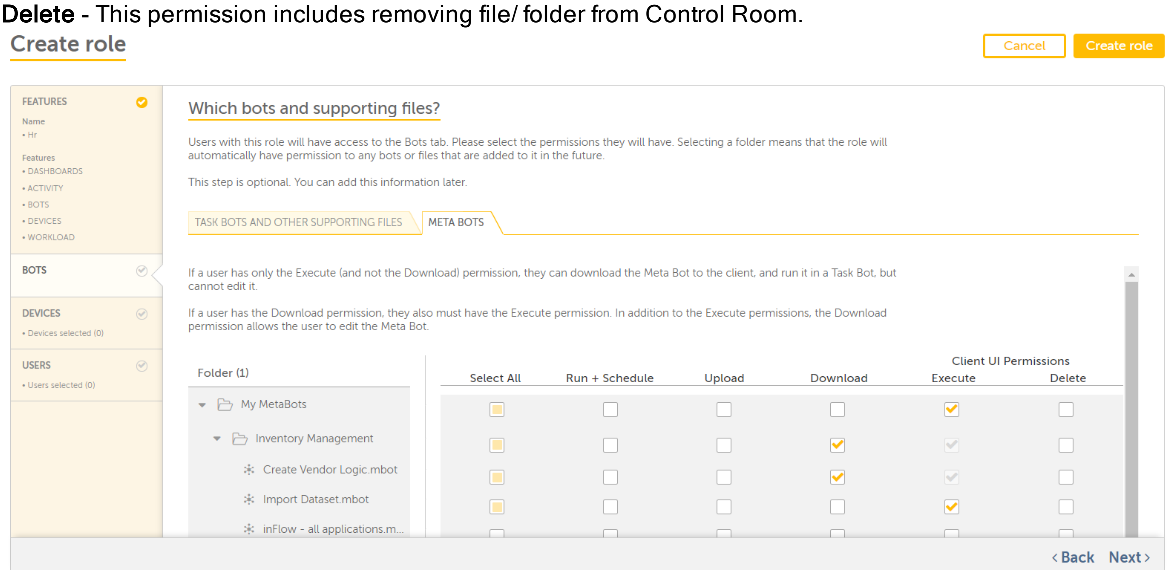


- **MetaBots**- MetaBot supports role based access control (RBAC) on individual MetaBot files, and folders containing MetaBots. When a MetaBot is uploaded to Control Room, it inherits permission of the immediate parent folder. To change or modify permission on individual MetaBot file, you must perform the action manually.

> **Note:**If the applied permissions are different on a MetaBot file and its folder, precedence is given to permission applied at the MetaBot file level.

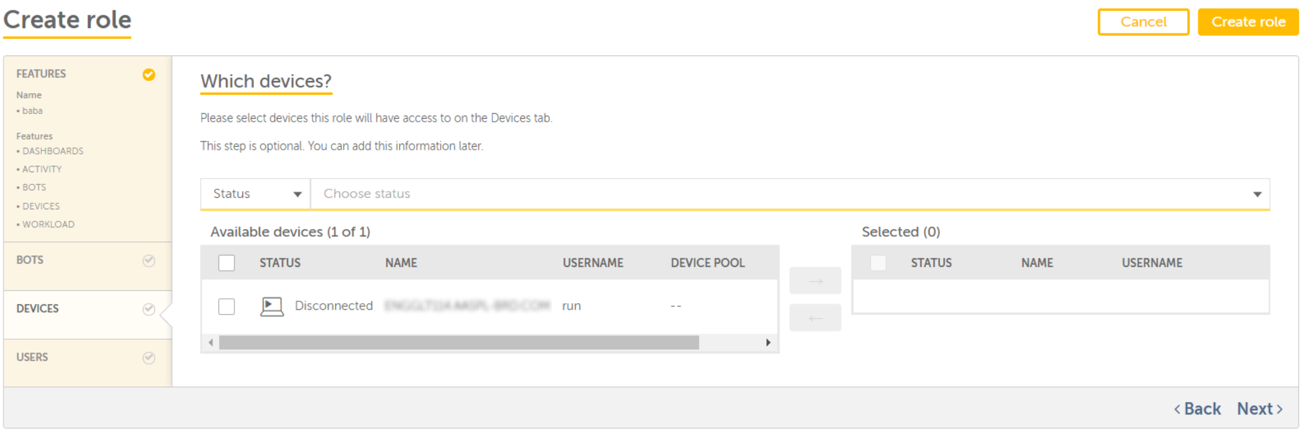
You can check the following permissions:

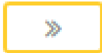
- **Select all** - This permission includes upload, download, execute, delete, run + schedule actions.
- **Run + Schedule -** This permission includes run and schedule permission for MetaBots i.e. allows user to run and/or schedule Bots. This permission is enabled only if user has either **Run my bots** or **Schedule my bots to run** permission.
  - This permission is termed as **Run** when the user has **Run my bots** feature permission. You can explicitly select Run permission on a specific folder to allow the user to run all bots that belong to this folder.
  - Similarly, this permission is termed as **Schedule** when the user has **Schedule my bots to run** feature permission. You can explicitly select Run permission on a specific folder to allow the user to schedule all bots that belong to this folder.
  - It is termed as **Run + Schedule** when user has both feature permissions. This allows the user to run and schedule bots that belong to this specific folder on which the permission is selected.
- **Upload** - This permission includes uploading MetaBot files/ folder to Control Room.
- **Download** - This permission includes downloading MetaBot files/ folder from Control Room to Client. **Please note**, if download is selected then execute is auto-selected.
- **Execute** - This permission includes using MetaBot in a task.
- **Delete** - This permission includes removing file/ folder from Control Room.



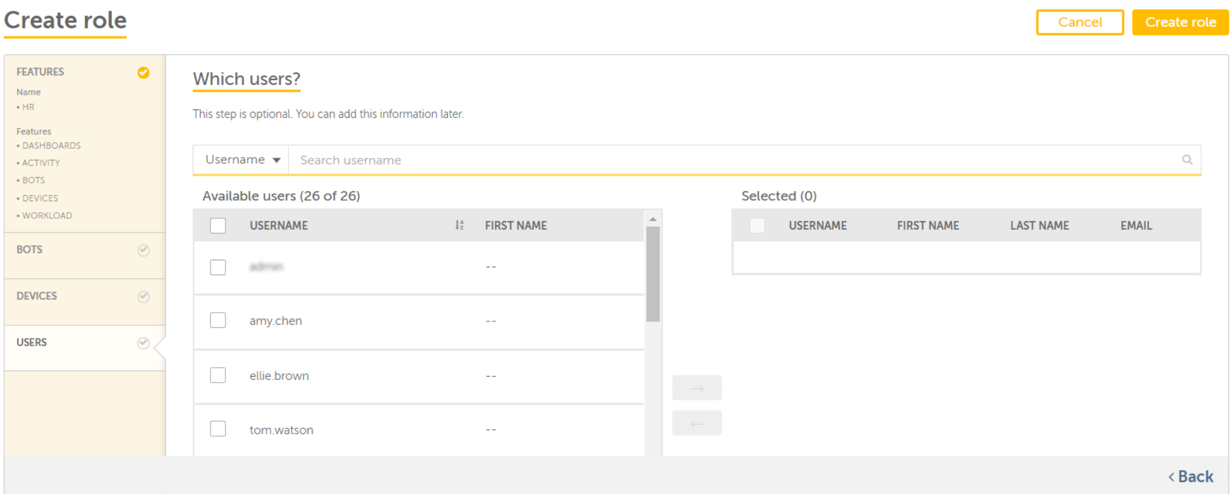
> Note: The **Run + Schedule** permission replaces the earlier behaviour of 11.0 where user was allowed to run or schedule a bot when the user had download permission for a folder.

3. In **Devices tab**, you can select the devices your role will have access to. A non-admin user will have access to Bot runners that are tagged to user's role.



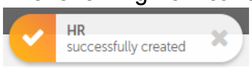
4. In **Users tab**, you can assign your role to existing users, select users from the list of available users and click on . After you complete selecting users for your role, click on **Create role**.

Tip: You can select multiple users for your role in users tab. This allows more than one user to be assigned the same role at a time, which reduces the effort unlike the Users landing page.



Note: Users that are shown **disabled** cannot be selected if they have been deactivated by an Admin user. Also, your own user is reflected as disabled in the users' list and it cannot be removed.

5. The following notification indicates that your role has been successfully created:



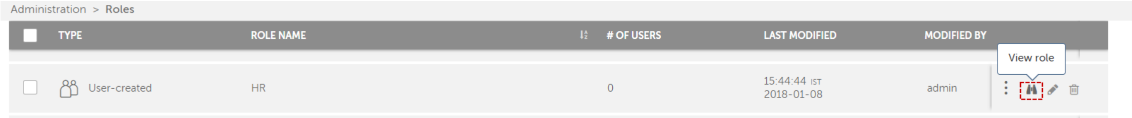
Next...

Create users in Control Room based on the roles and permissions assigned. Learn More

View a role

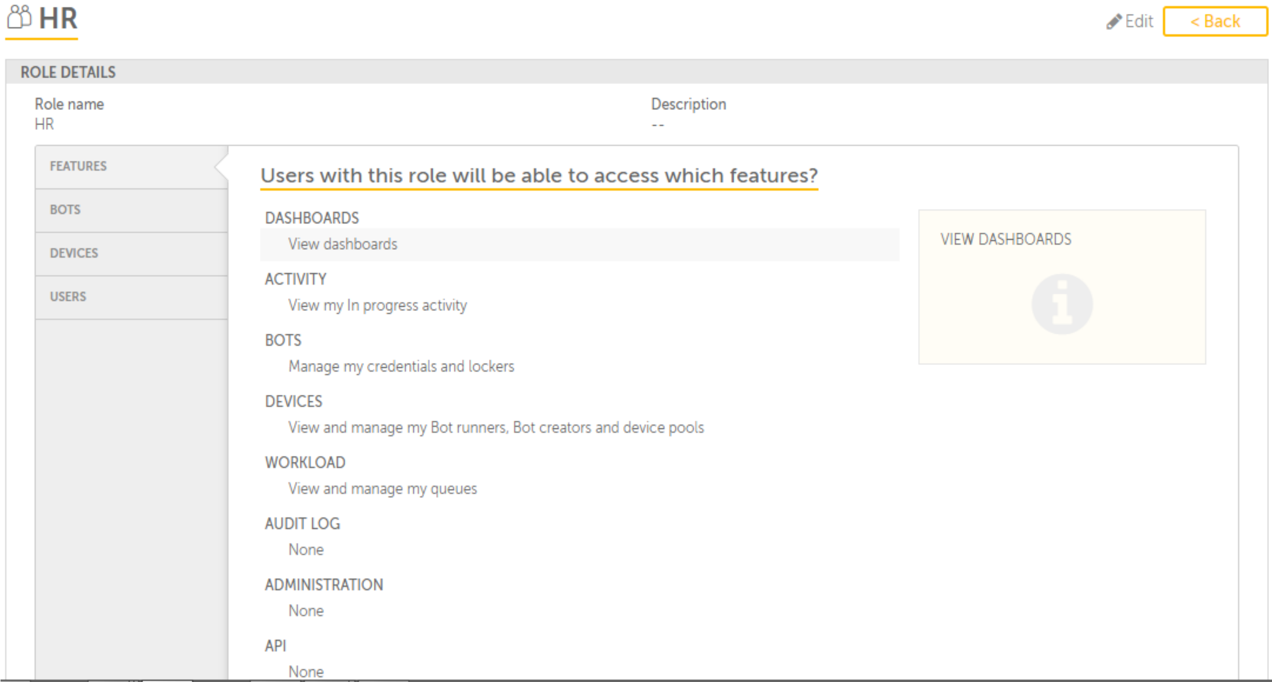
An admin user, or a user with permission to view and/or manage role can access **View role** page.

1. Go to Administration → Roles
2. In the roles page, choose the role that you wish to view. Go to the actions list and click **View Role**.

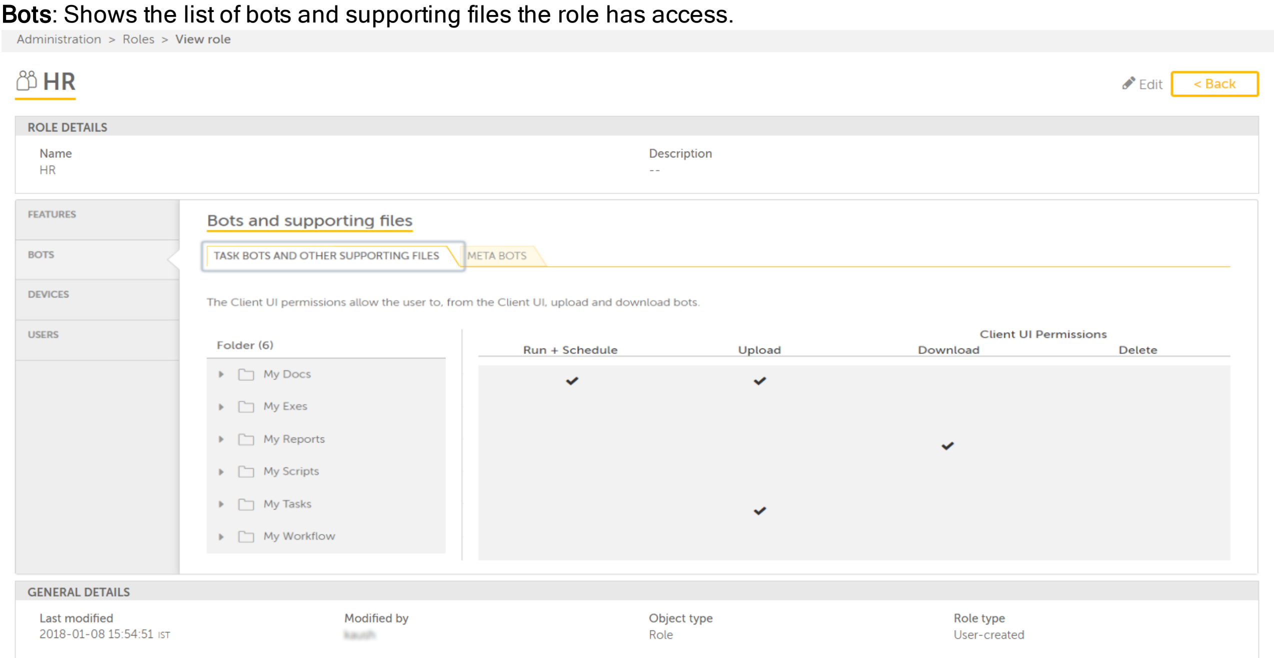


3. The following page is displayed with information such as selected: Features, Bots, Devices, and Users for the role in read-only mode:

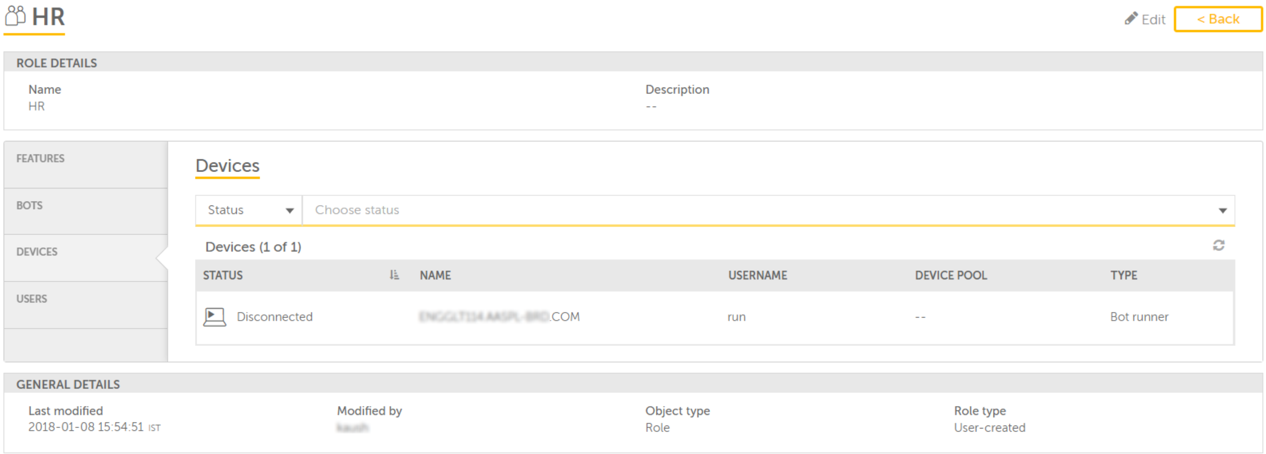
- **Features**: Shows the list of features and permissions the role has access.



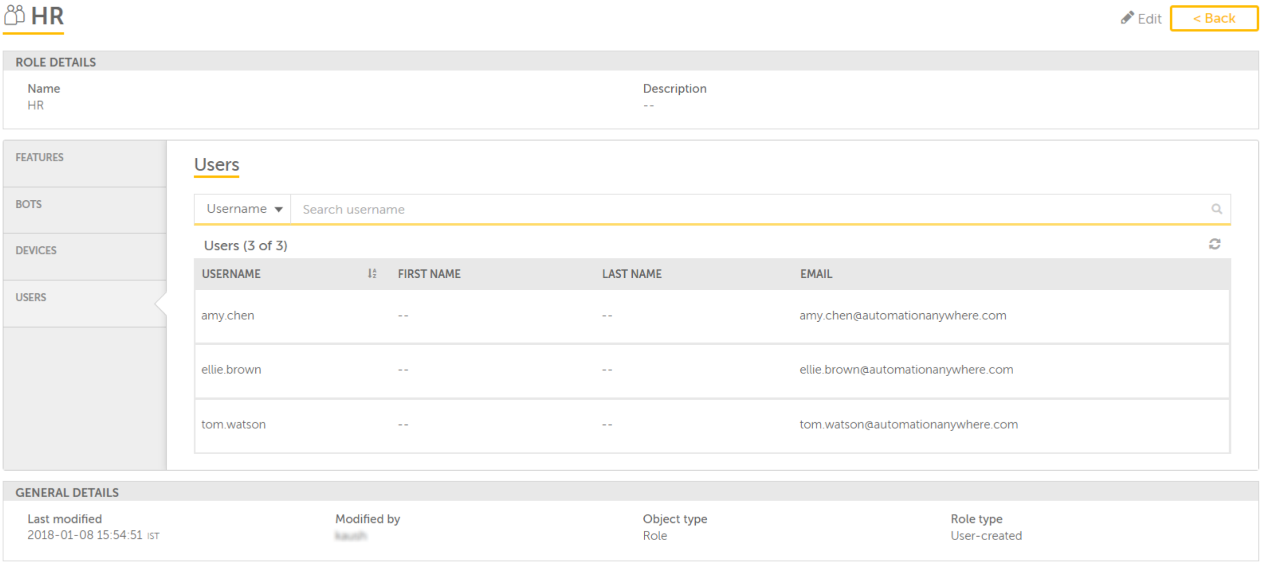
- **Bots**: Shows the list of bots and supporting files the role has access.



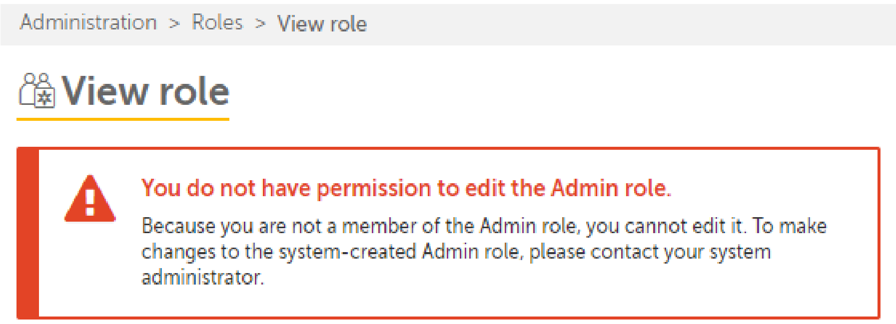
- **Devices**: Shows the list of devices the role has access.



- **Users**: Shows the list of users having access to the respective role.



Note: A user with **View and Manage Role** permission can view all the roles. However, the user cannot view details of Admin and Locker Admin roles. When the user clicks , the view page is launched with an error:

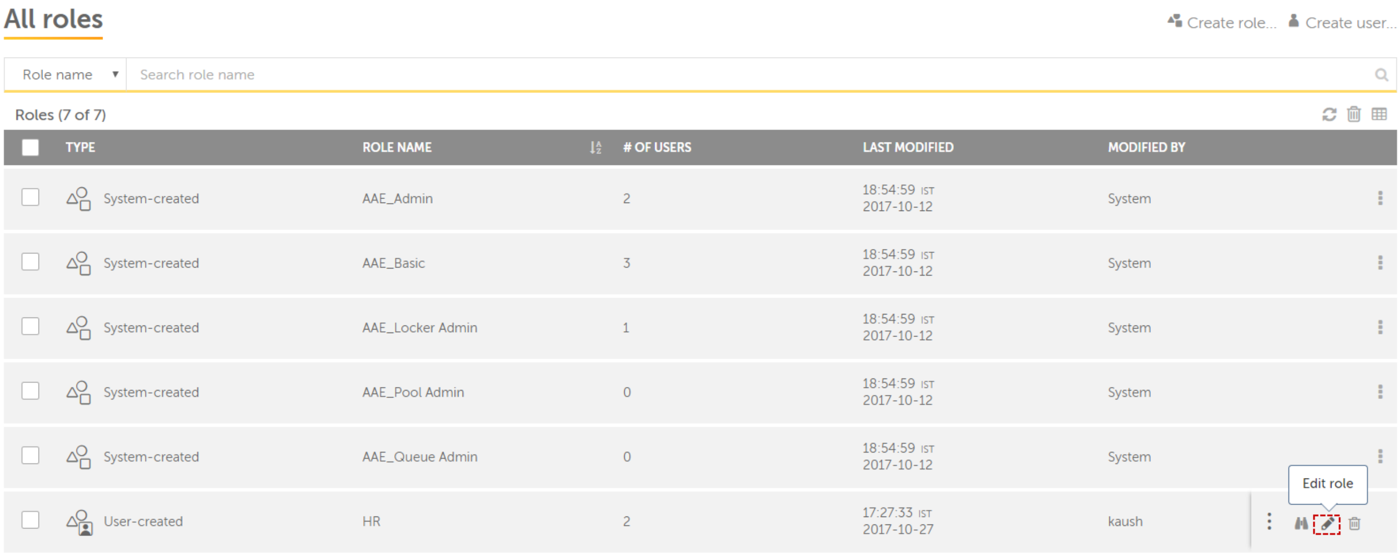


Edit a role

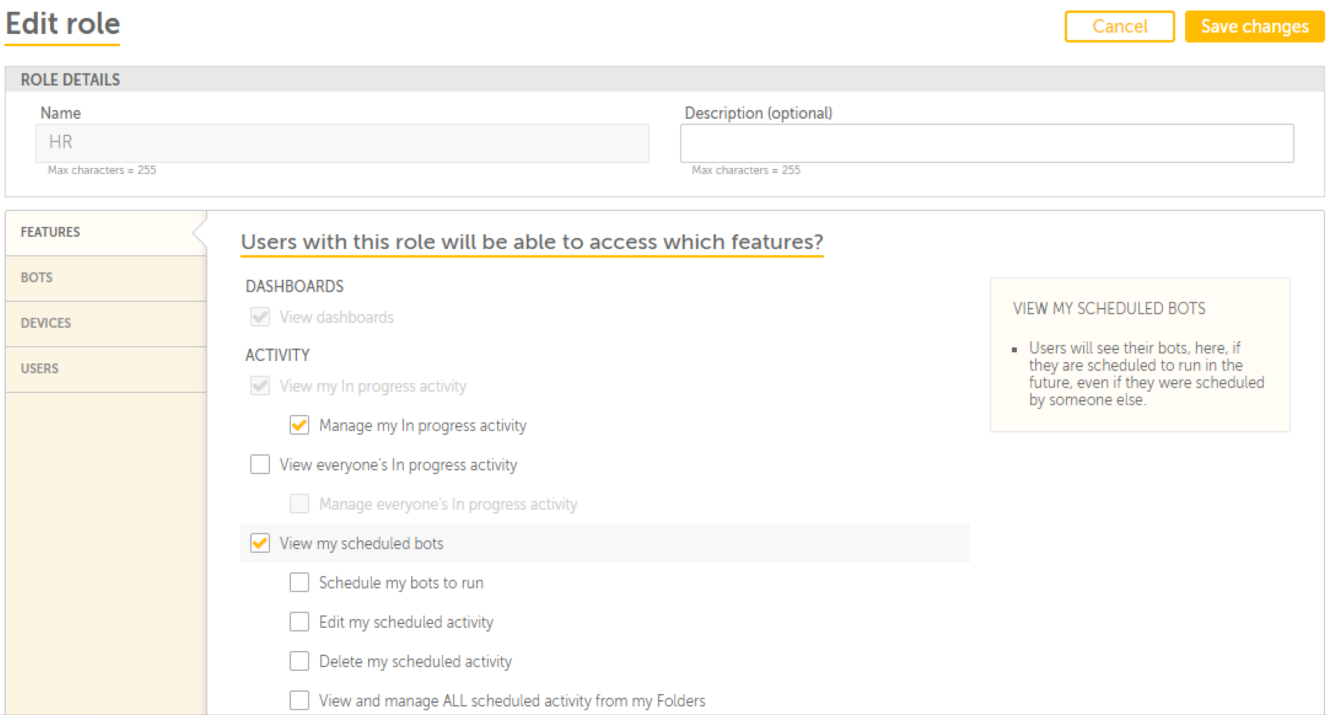
When you click the **Edit** icon for a role in the **Roles** table of the **All roles** page, the Edit role page is opened. Only an admin user, or a user with permission to edit role can access Edit role option. User has access to modify information, such as feature permissions, bots, devices and users

Note: If a role/ permission for a user is updated, the user must re-login or refresh the browser for the changes to be immediately reflected on Control Room UI.

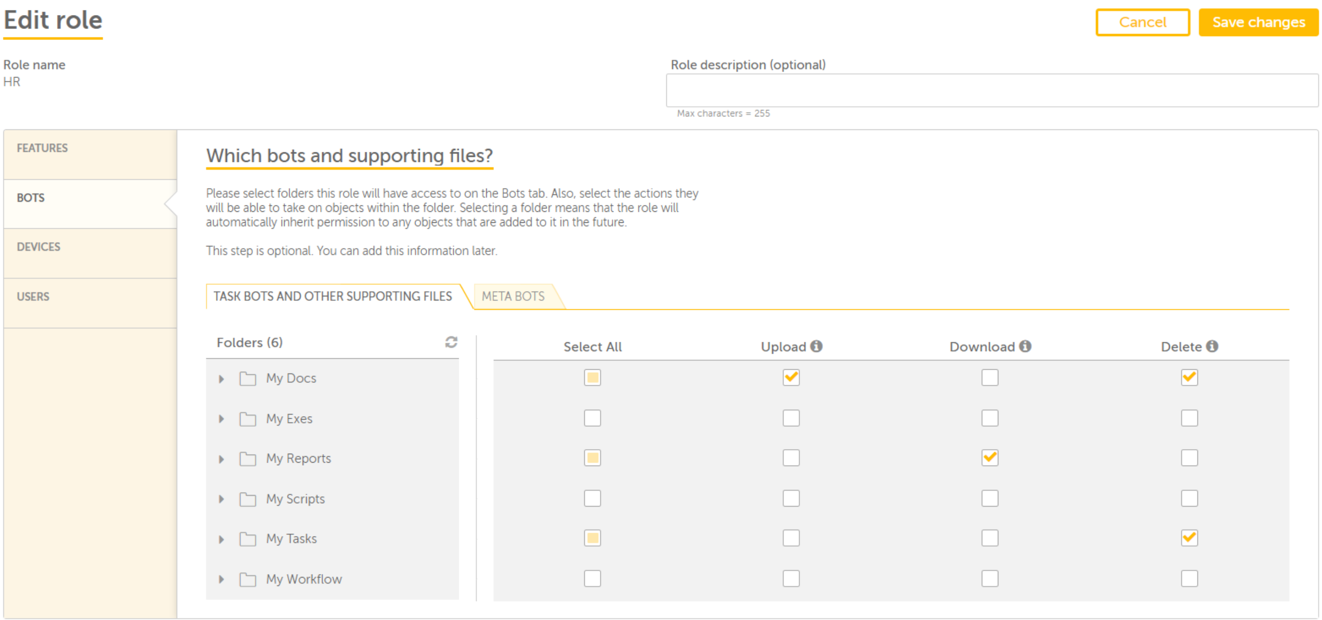
1. Go to Administration → Roles
2. In the roles list, choose the role that you wish to edit. Then mouse over to the Actions list and click **Edit role**.



3. In the Edit role page, user can make changes : Features, Bots, Devices, and Users
   - **Features:** Allows you to add or revoke role permissions.

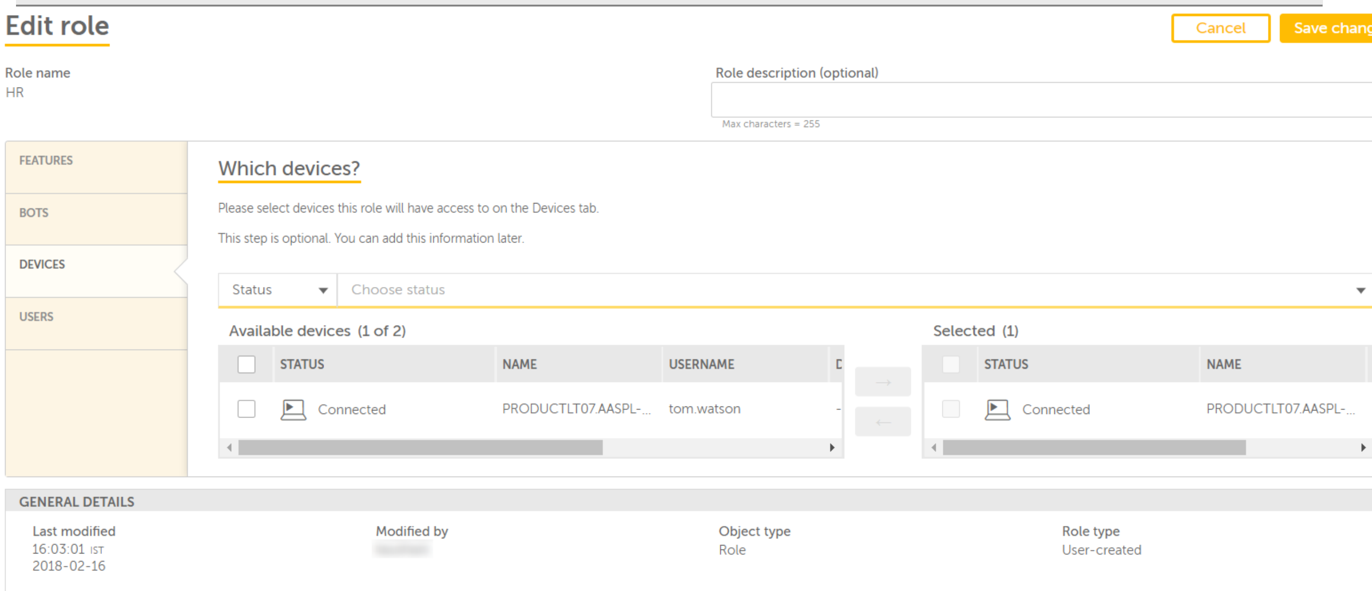


- **Bots**: Allows you to add or revoke access to folders on the Bots tab. Also, you can select the actions a user can perform on files within the folder.

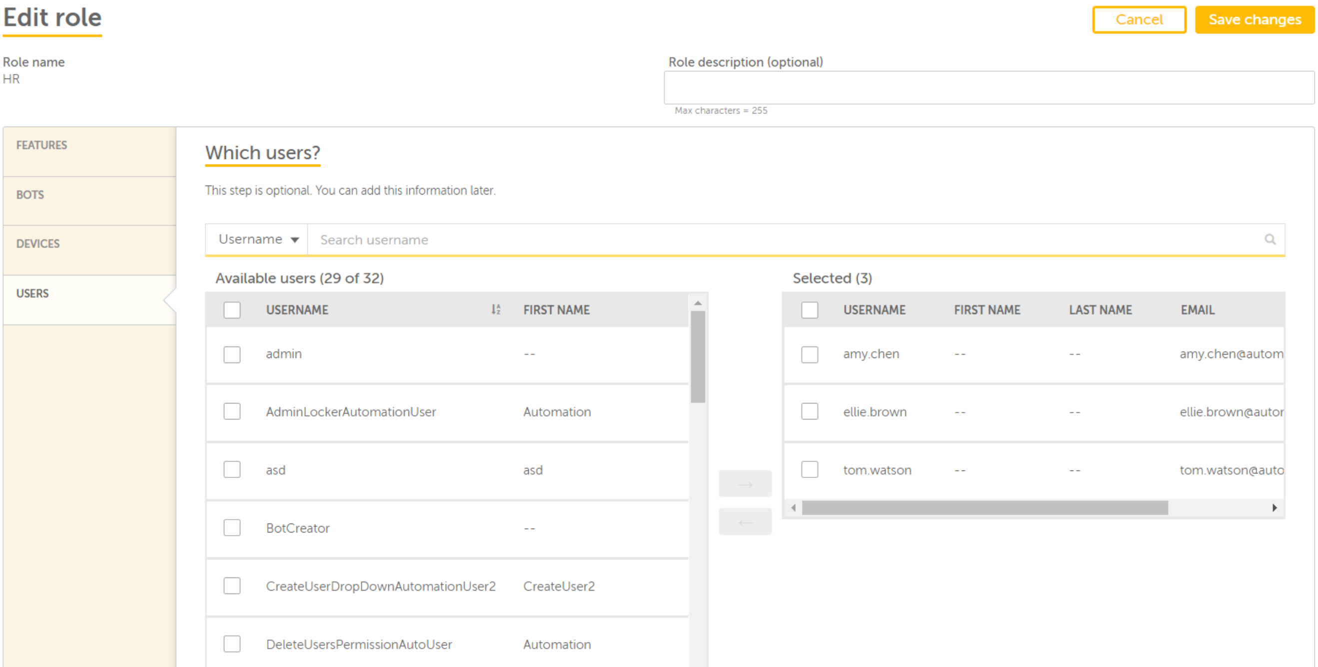


Devices: Allows you to add or remove devices a role has access to on the Devices tab.

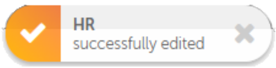
> **Note:** If a Bot is scheduled on a device, the device is shown disabled in the "selected" area.



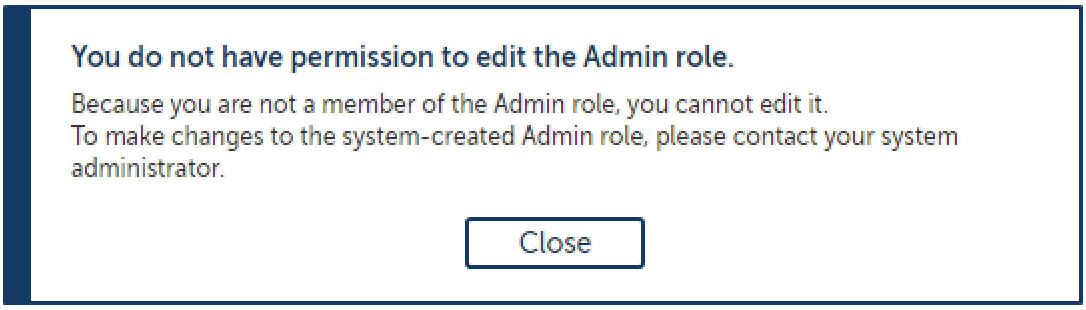
- **Users**: Allows you to add or remove users who have permission to access the role.



4. Once the changes are done, click **Save changes**. Your role is successfully edited.



Note: A user with **View and Manage Role** permission can view all the roles. However, the user cannot edit details of **Admin** and **Locker Admin** roles. When the user clicks , the following message is displayed:



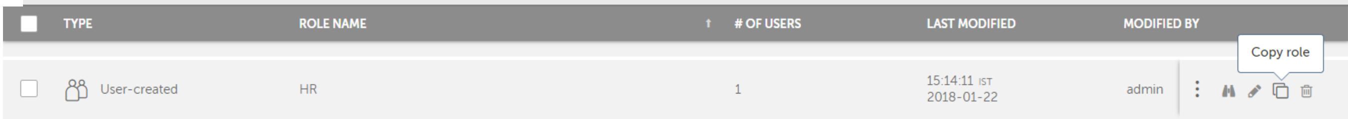
Copy a role

An admin user, has permission to select **Copy** role option in Control Room. This ensures that user can create similar roles in the system without having to perform the action manually.

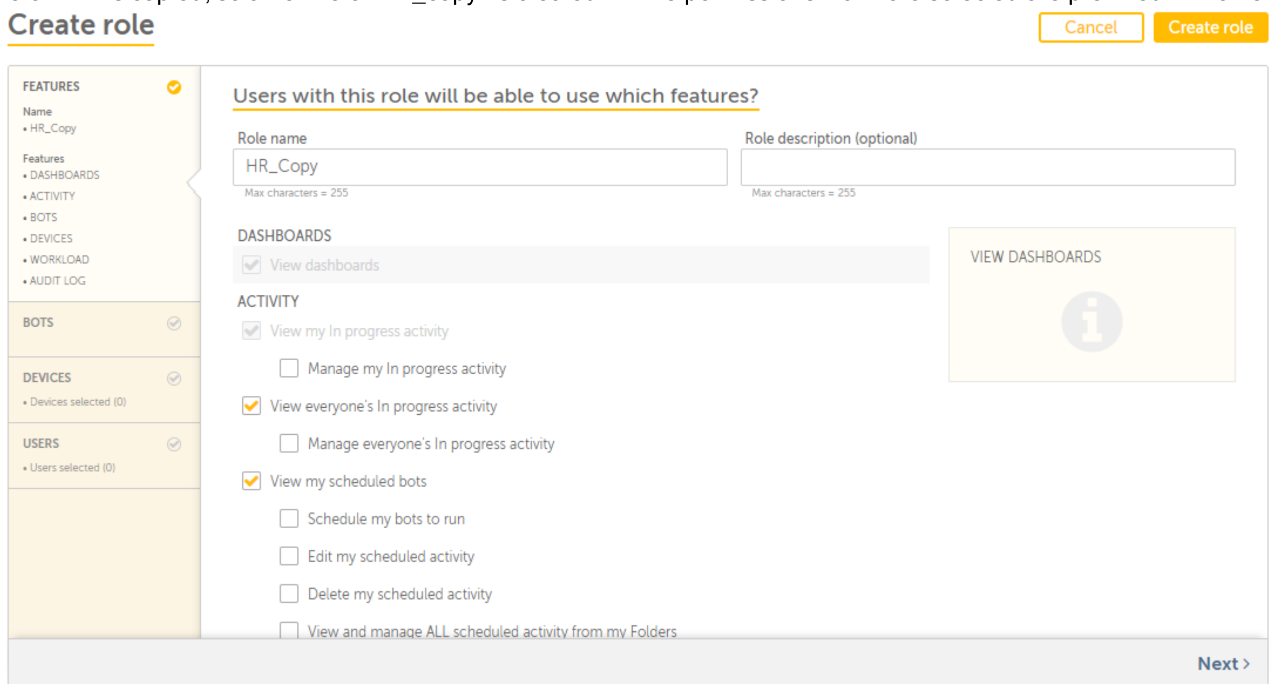
To copy a role, follow the steps mentioned below:

1. Go to Administration → Roles
2. In the roles list, choose the role that you wish to copy. Mouse over to the actions list and click **Copy role.**

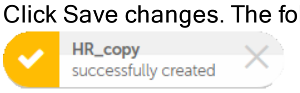
   Note: System-created roles cannot be copied. These roles are pre-configured during Control Room installation.



3. A new role page is launched, wherein the role is created with "copy" appended to the Role Name. **Example**: In the previous image, role "HR" is copied, so a new role "HR_copy" is created. All the permissions that were selected are pre-filled in the new role.



4. Click Save changes. The following success notification is displayed:



Delete a role

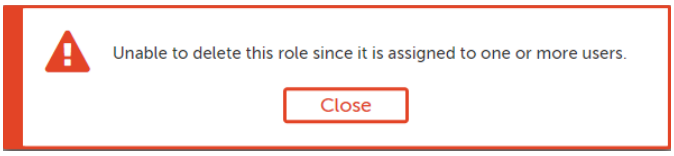
An admin user, or a user with permission to delete role can select **Delete** option to remove redundant roles from the system.

To delete a role, follow the steps mentioned below:

1. Go to Administration → Roles
2. In the roles list, choose the role that you wish to delete. Then mouse over to the actions list and click **Delete role**

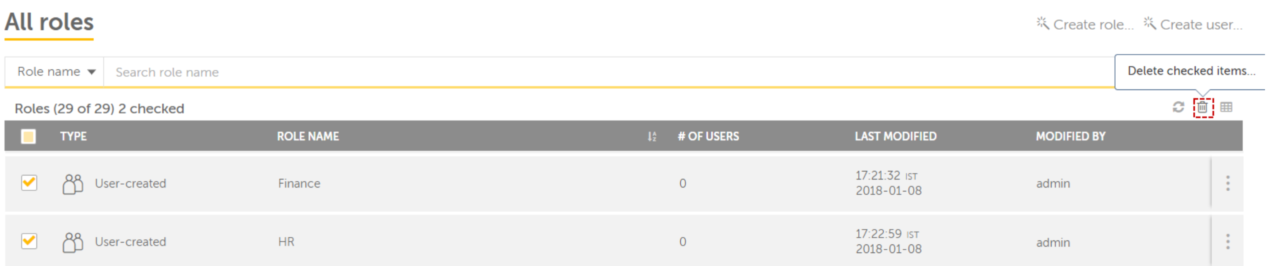
> **Note:** `System-created roles cannot be deleted.`

- If users are assigned to your role, then the following message is displayed:



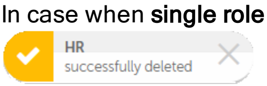
- If users are not assigned to your role, then the following message is displayed. Click **Yes, delete** to delete your role and **No, cancel** to cancel deletion:

3. You can also delete multiple roles . Check the roles that you wish to delete and click on **Delete Checked Items** icon

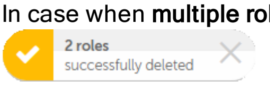


4. A success notification is displayed as follows:

- In case when **single role** is deleted:



- In case when **multiple roles** are deleted:



Licenses- An Overview

Control Room License page provides detailed information about the current license that is installed. It also gives the Admin user privilege to monitor license details and usage statistics. Therefore, an Admin user can view these details any time and avail information about the number of products purchased, the number of device licenses purchased, and number of licenses that are exactly in use. A first time user has access to trial license for a period of 30 days, after which a user can continue with an extended trial license or install a new license.

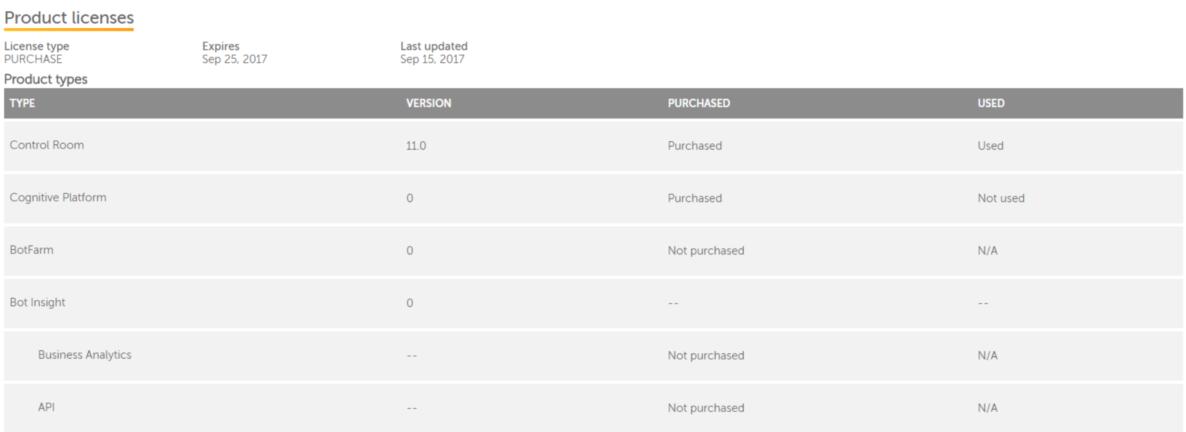
Benefits of purchasing a license

- Genuine license ensures reliable support system
- Enables user to utilize the product features for the license period they have purchased
- Helps gain access to latest updates, upgrades, security patches, hot fixes.

Product licenses

Control Room integrates with other Automation Anywhere products such as BotFarm, Bot Insight and Cognitive Platform. The **product license details** shows the list of purchased products, along with license version and product license status as used, not used, or N/A.

Note: If you have Bot Insight license, Operational Analytics is available by default with Control Room v11.0


Product licenses

License type: PURCHASE
Expires: Sep 25, 2017
Last updated: Sep 15, 2017

Product types

TYPE	VERSION	PURCHASED	USED
Control Room	11.0	Purchased	Used
Cognitive Platform	0	Purchased	Not used
BotFarm	0	Not purchased	N/A
Bot Insight	0	--	--
Business Analytics	--	Not purchased	N/A
API	--	Not purchased	N/A

Column	Value
Type	Product Name
Version	Latest version no. of the current installed product
Purchased	Product has been purchased or not purchased
Used	Product is in used, not used, or N/A status

Bot user licenses

Bot user license detail shows the number of device licenses that have been purchased and are currently in use.

Bot user licenses

Bot user types

TYPE	PURCHASED	USED
Bot creator (Development)	100	29
Bot runner (Run time with TaskBots)	100	3
IQ Bots	50	0
BotFarm (Run time)	00:00:00 hours	00:00:00 hours
Bot Insight	--	--
Business Analytics	0	0
API	0 rows	0 rows

Bot creator (Development): Users with privilege to automate Bot(s) in Client.

Bot runner (Runtime): Users with privilege to run Bot(s).

BotFarm (Runtime) : Bot user count of licenses is measured in number of hours used by all runtime clients within BotFarm to execute a Bot.

BotInsight: It shows the number of user count having Business Analytics role -Bot Insight Consumer or Expert. And API count is measured in number of rows that API fetches from Bot Insight database.

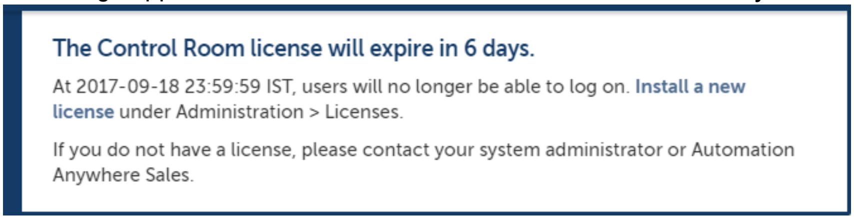
Column	Value
Type	Type of license
Purchased	No. of licenses purchased
Used	No. of licenses in use

Trial license

Automation Anywhere Control Room ships trial License with an evaluation period of 30 days. This provides the user with an ability to assess the product and make an informed decision. Trial license offers 3 Bot Creators and 2 Bot Runners to begin with; also a user can contact System Administrator or Automation Anywhere Sales to purchase a new license or extend the existing trial license.

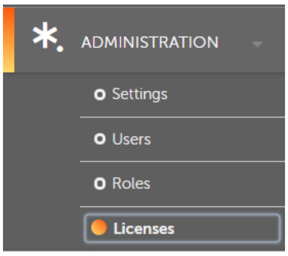
To purchase an extended license or to install a new license, follow the below mentioned steps:

1. Login to Control Room as an Admin and the Dashboard homepage is displayed.
2. A notification is displayed with remaining days for license expiry. Click Show details.


3. A message appears with a link to **Install a new license** or to **contact System Administrator or Automation Anywhere Sales**


To view Bot license and usage statistics, follow the below mentioned steps:

Note: Product and Bot user license statistics is only visible to users with Admin role and users with License management permission,

1. Go to Administrations Tab → Click Licenses.


2. The License page shows Product and Bot User license statistics with details.

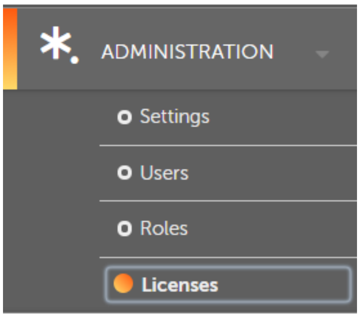
For detailed information, refer Install a new license.

Install a license

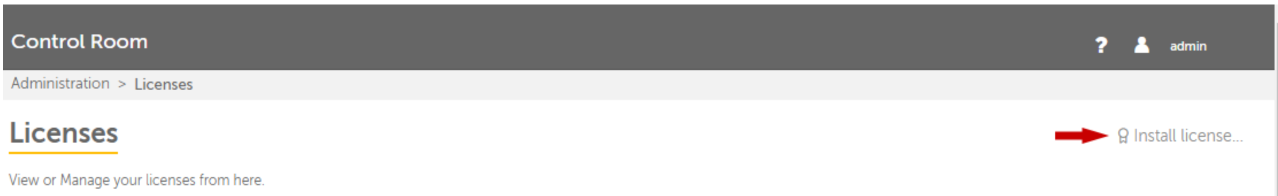
A Control Room Admin or a user with License management permission can install a license, and evaluate Control Room version 11.0. A trial license is shipped with validity of 30 days; on expiry of Trial license the user must contact System Administrator or Automation Anywhere Sales to purchase a new license.

To install a license, follow the steps mentioned below:

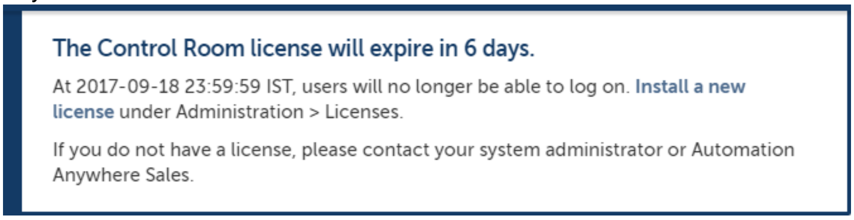
1. Go to Administration Tab → Click Licenses.



2. Click Install license button.



or you can click on Show details on the notification bar in Control Room header and then click Install a new license link.



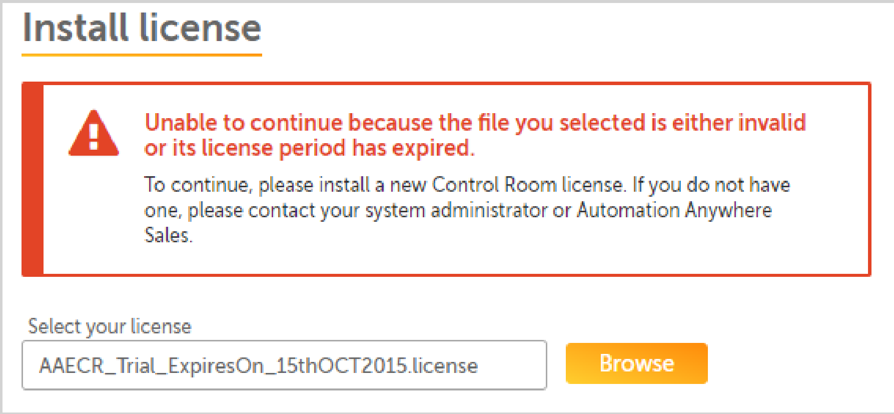
3. Click on browse to select a '.license' file from the list of licenses. Make sure you select a valid '.license' file.

4. Click Install license button.

5. The following message indicates that your license is successfully updated:

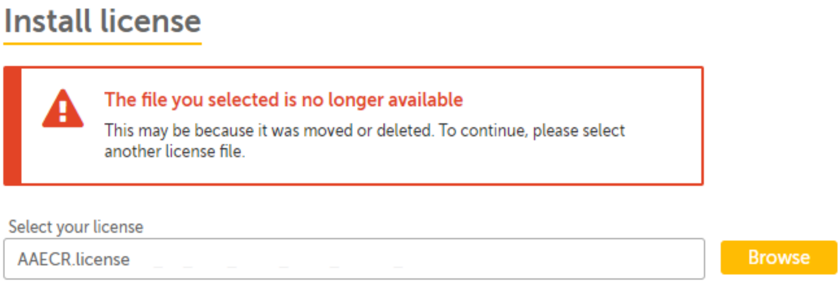
Errors

- If a user has **invalid or an expired license** file, then the following error is displayed:



- If user selects a **file with a different extension** other than ".license", then the following error is displayed:

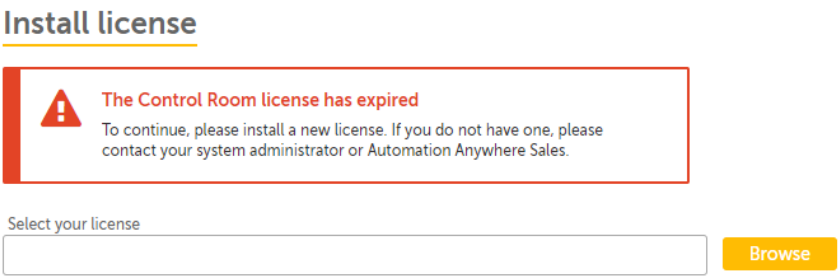
- If user selects a file that is either **deleted or moved to another location**, then the following error is displayed:



License Expiry

You would be unable to access Control Room, if your current license has expired. You must install a new license or contact system administrator or Automation Anywhere Sales.

- The following message is displayed when your current license expires:



Migration - an overview

Use the **Migration** page to migrate data from a previous Control Room version 10.x to the current version - 11 LTS. You should be a Control Room administrator with **View and Manage Migration** permission to be able to use the migration tool - Migration wizard. The wizard can be launched anywhere in a browser from Control Room version 11 LTS.

You can use the tool to migrate data either on the basis of **Roles** or **Users** in phases depending on your business requirements. Dependent data such as licenses, credentials, bots, and schedules are also migrated automatically when you migrate roles or users.

Prerequisites

To ascertain whether you can initiate migration of data, ensure the following prerequisites are met:

1. You should have
    a. Access to Control Room v10.x* repository path via a shared drive
    b. Credentials to connect to Control Room v10.x* SQL database
    c. Master key to connect to Credential Vault of Control Room v10.x*
    d. Credentials to connect to Bot Insight SQL database (applicable only if using Bot Insight with Control Room v10.x*)
    e. URL of Bot Insight meta-data database
2. A new infrastructure (that is separate from 10.x* environment) with Automation Anywhere Enterprise v11.1 already installed
3. It is recommended that you backup,
    - Control Room v10.x* SQL database
    - Control Room v10.x* shared repository
    - Control Room v10.x* SVN database (if applicable)
    - Bot Insight SQL database (if applicable)
    - Bot Insight meta-data database (if applicable)
4. It is recommended that if a migration is already in progress, you do not initiate another migration process.

** Includes Automation Anywhere Enterprise 10 LTS, 10 SP2, and hot-fixes with these as base version. Refer Installation Guide of particular versions on how to install.*

Important Considerations

1. The Automation Anywhere Enterprise 10.x environment should be strictly controlled and monitored once the migration process is initiated. Hence, it is recommended that you,
    - Do not,
        a. Create users, roles, and permissions
        b. Create and upload any meta data. For example, new automation bots
        c. Create new schedules
        d. Check out bots (if version control is enabled)
    - Schedule and deploy only on demand bots.
2. If you are using a version less than 10 LTS, you should first migrate to 10 LTS using the 10 LTS Migration Utility and then migrate from 10 LTS to 11 LTS.

    ```
    Note: The hot fixes on 10 LTS are supported for migration to 11 LTS.
    ```

3. You cannot migrate from Automation Anywhere Enterprise version 9.x. For this you should first migrate to 10 LTS. Refer AAE 10 LTS Installation Guide and AAE 10 LTS Data Migration Utility Guide.
4. Migrating data from 11 GA (11.0) to 11 LTS is NOT supported
5. Migration of data includes,
    a. Repository data
    b. Meta-data available in database
    c. Users, roles, licenses, and permissions

d. Automation schedules

e. System defined credentials

f. Application settings

g. Automation bots with version history if applicable

h. Bot Insight data

6. Migration of data excludes,

   a. Devices/Clients

   b. Audit logs

   c. License information of source Control Room

   d. User defined credentials

   e. Version Control Settings

   f. Schedule history

7. If Version Control is enabled in 10.x Control Room then you must enable the same in 11 LTS Control Room manually since the settings for Version Control is not migrated. It is mandatory to use a fresh SVN database for 11 LTS which is different than 10.x SVN database.

8. Ensure the SQL database service is running during the migration process.

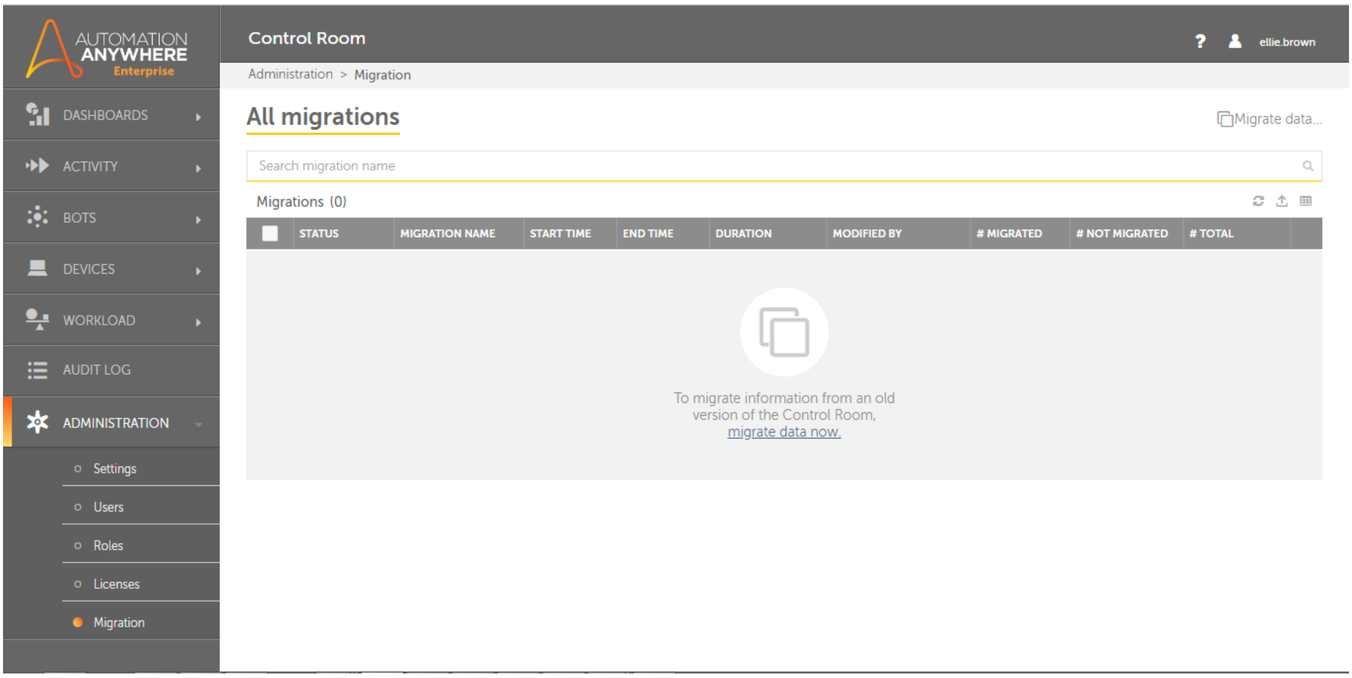
9. Data from source Control Room configured for one user type cannot be migrated to destination Control Room configured for another user type. For example, data for Control Room configured for Active Directory cannot be migrated to Control Room with either Non Active Directory or Single Sign On users.

10. Migration of SAML configuration data is NOT supported.

Refer the article on Frequently asked questions (FAQs) for other details.

Role-based access to Migration tool

You can access the migration tool from **Administration → Migration** page as illustrated:



Note: Only a Control Room admin can access the Migration page as the admin user is granted View and Manage Migration permission. Refer Create a role for details.

For ease of access, you can search the entries based on the unique **Migration Name**

Search migration name

The following describes the list of items that can be viewed in the table:

Table Item	Description
Status	Shows the status of the saved migration - successful or unsuccessful
Migration Name	Shows the name of the migration for the corresponding migration run i.e. <timestamp>.<username>
Start Time	Shows the time and date when the migration process began
End Time	Shows the time and date when the migration process ended
Duration	Shows the time it took for the migration to run
Modified by	Shows name of the user who initiated the migration i.e. name of the Control Room administrator
# Migrated	Shows the number of entities that were migrated successfully
# Not Migrated	Shows the number of entities that failed to migrate
# Total	Shows the total number of entities that were attempted for migration

Tip: You can perform the following actions on a table column:

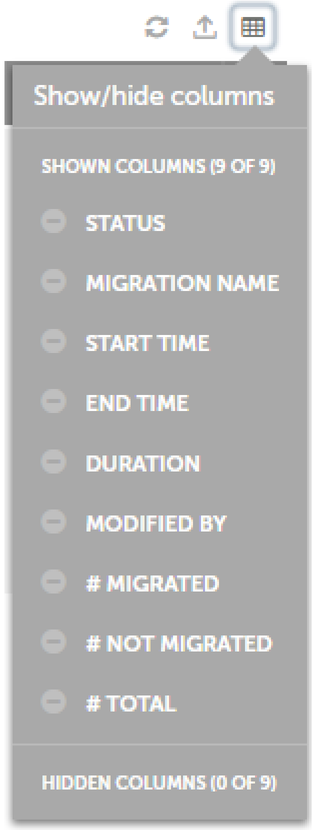
- Click a column to sort it in ascending and descending order. You can sort up to three columns by holding the Shift key when you click on two more columns. This gives you the option of sorting two additional columns. This way the sorting is done on the entire table and not just the data that is currently visible to you. The last sorting is stored in memory applied by a user per session.
- Use a drag-and-drop operation to move the column left or right
- Move your mouse cursor at the end of the column and drag to re-size

The following describes the tasks that you can perform on an individual migration:

Table Item	Description
View details	Allows you to view details of the selected migration run

At table level you can perform the following actions:

Table Item	Description
Refresh	Allows you to refresh the table contents so that you can view the latest migration status
Export to CSV	Allows you to export the selected data to a csv file. You can export data based on: • Filters • Selection
Show / Hide columns	Allows you to show or hide specific columns. By default, all columns are displayed:

	 Tip: To **hide** a column, click on the column name.

Migrating Data

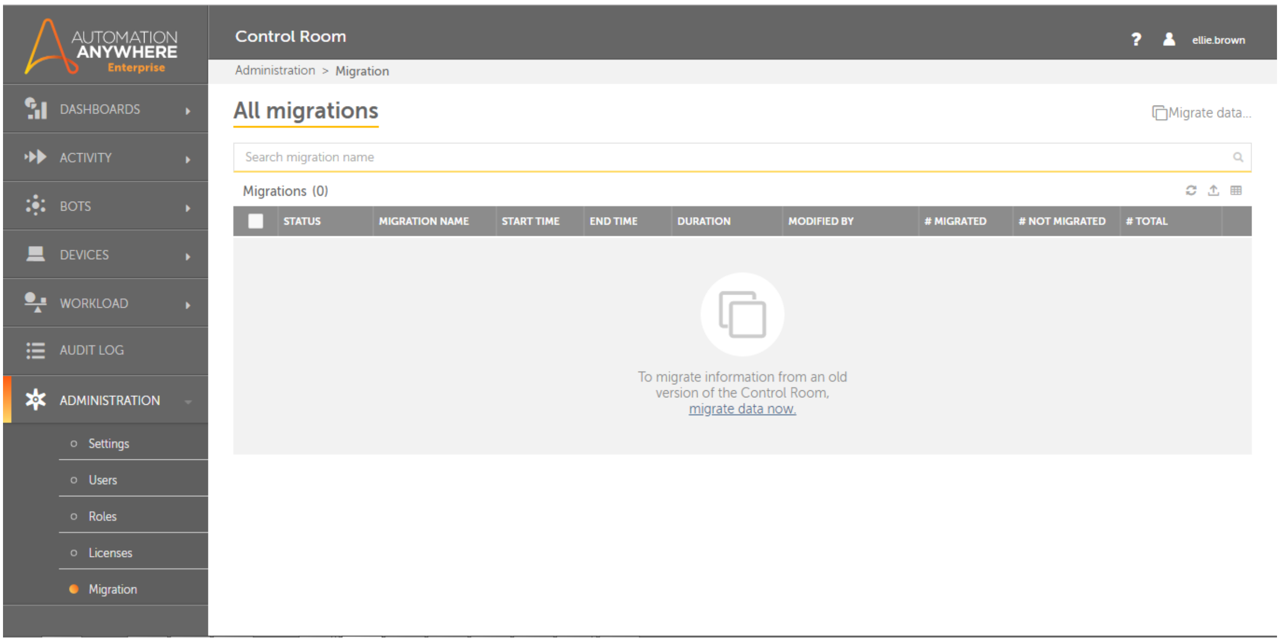
To migrate date, first ensure following preconditions are met,

1. Control Room 11 LTS must be installed
2. First Control Room Admin user is created
3. Credential Vault is configured
4. Control Room 11 LTS license is installed.
5. If using Version Control, the Version Control Settings should be configured under Administration → Settings. Refer Control Room settings for details.
6. If using Windows Authentication to connect to source database, the user who is configured to run all destination Control Room Windows Services has access on source database.
7. If using Secure Connection, the source Control Room certificates is imported to the Java trust store. To import the certificate,
    a. Run command prompt in administrator mode
    b. Go to the AAE installation path - for example, C:\Program Files\Automation Anywhere\Enterprise
    c. Type or paste the following command at the prompt:

```
jre\bin\java -jar certmgr.jar -appDir "C:\Program Files\Automation Anywhere\Enterprise" -
importTrustCert "<Certificate Path>"
```

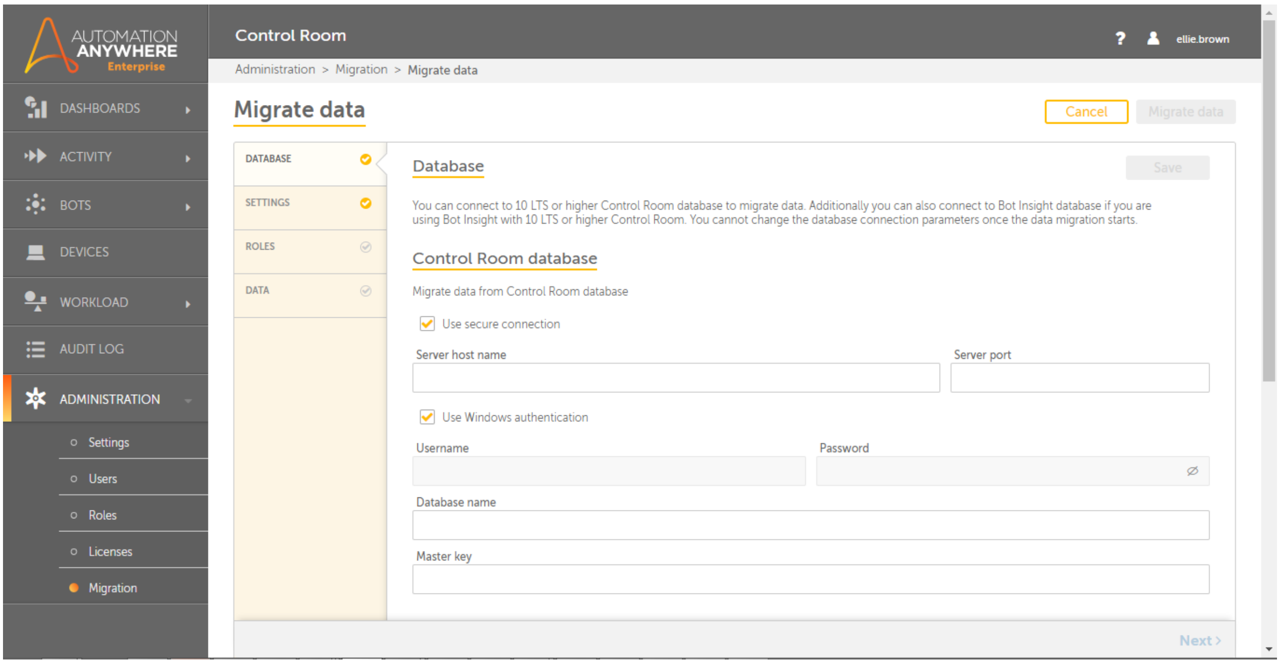
Once the above is done, follow below steps to start the migration process:

1. Launch the 11 LTS Control Room
2. Login using your first admin credentials
3. Go to **Administration** → **Migration** tab
4. Click  available above the **Migrations** table or the **Migrate data now** link in the **Migrations** table.



Note: The migrate data now link is visible only if no migration process has been done.

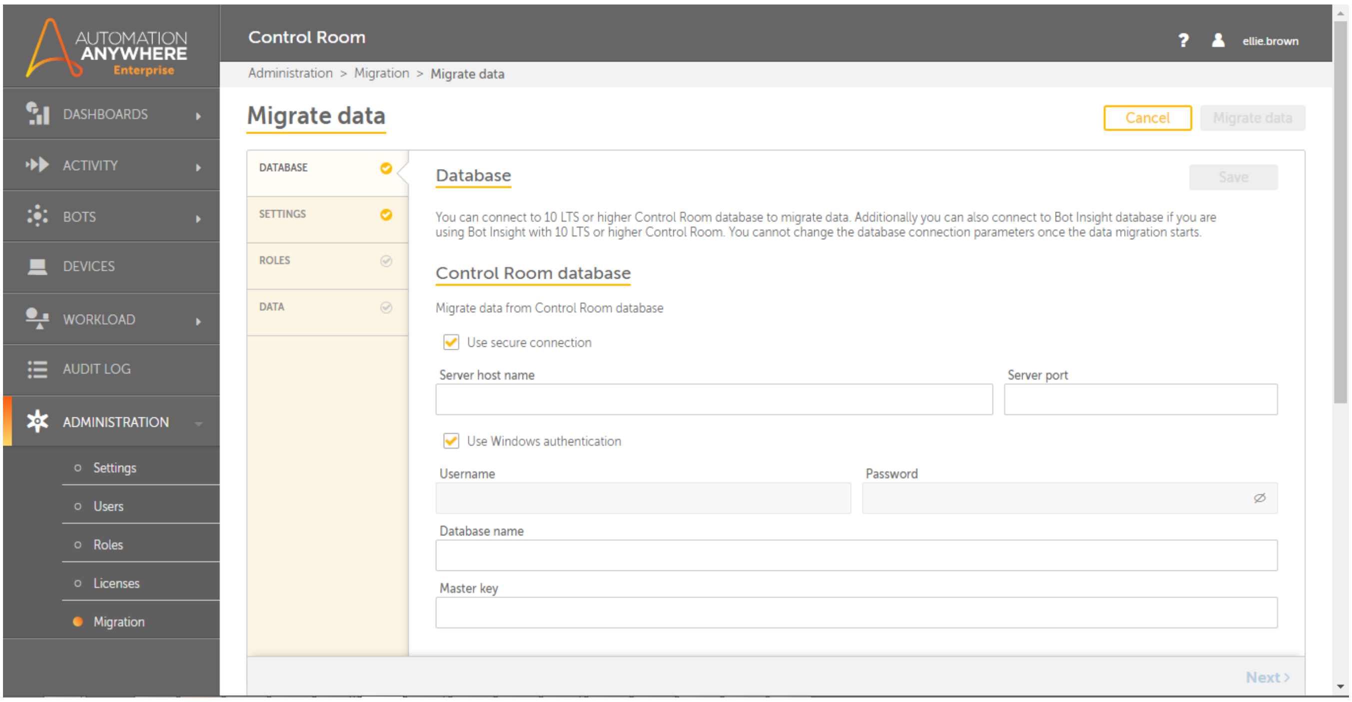
5. The **Migration wizard** is launched



6. The Migration wizard comprises of following tabs,
   1. Database
   2. Settings
   3. Roles/Users
   4. Data

Migration wizard

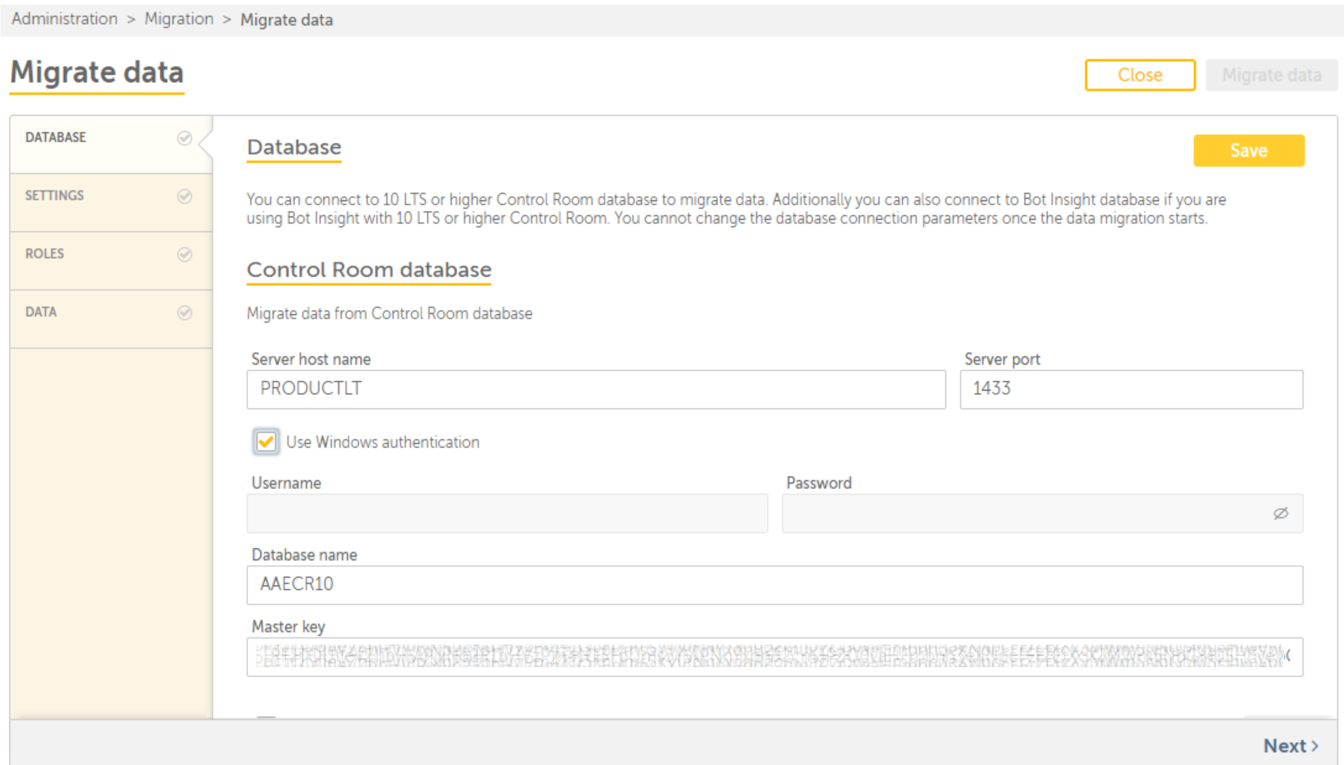
As a Control Room administrator with **View and Manage Migration** privileges you can use the **Migrate data** wizard to migrate data from Automation Anywhere Enterprise v10.x to v11.1 in a systematic and phased manner.



Database

The system allows you to connect to the source Control Room and migrate data from the source database to the destination Control Room database. You can also migrate your Bot Insight data if it is installed in the source Control Room.

Control Room database



To migrate Control Room database from 10.x, you must first connect to 10.x source Control Room and follow the steps given below:

1. Keep the **Use secure connection** selected if the SQL instance hosting 10.x Control Room database is configured with a secure connection. Clear this if the source SQL Server is not configured with secure connection.
2. Provide the **host name** and **port** number of the SQL Server where v10.x Control Room database is hosted. For example, PRODUCTLT and 1433
3. Keep the **Use Windows authentication** selected if the source SQL Server is configured using Windows authentication. Alternatively, **clear** the option and provide **Username** and **Password** if SQL Server is configured with SQL authentication**.**
4. Type the source Control Room database name. For example, AAECR10
5. Copy the source Control Room master key and paste it in the **Master key** field. This allows you to connect to the credential vault of the source Control Room. This is shown encrypted once you save the migration process.
6. Click Save at this juncture if you do not want to migrate Bot Insight database and move on to the next step of migrating data.

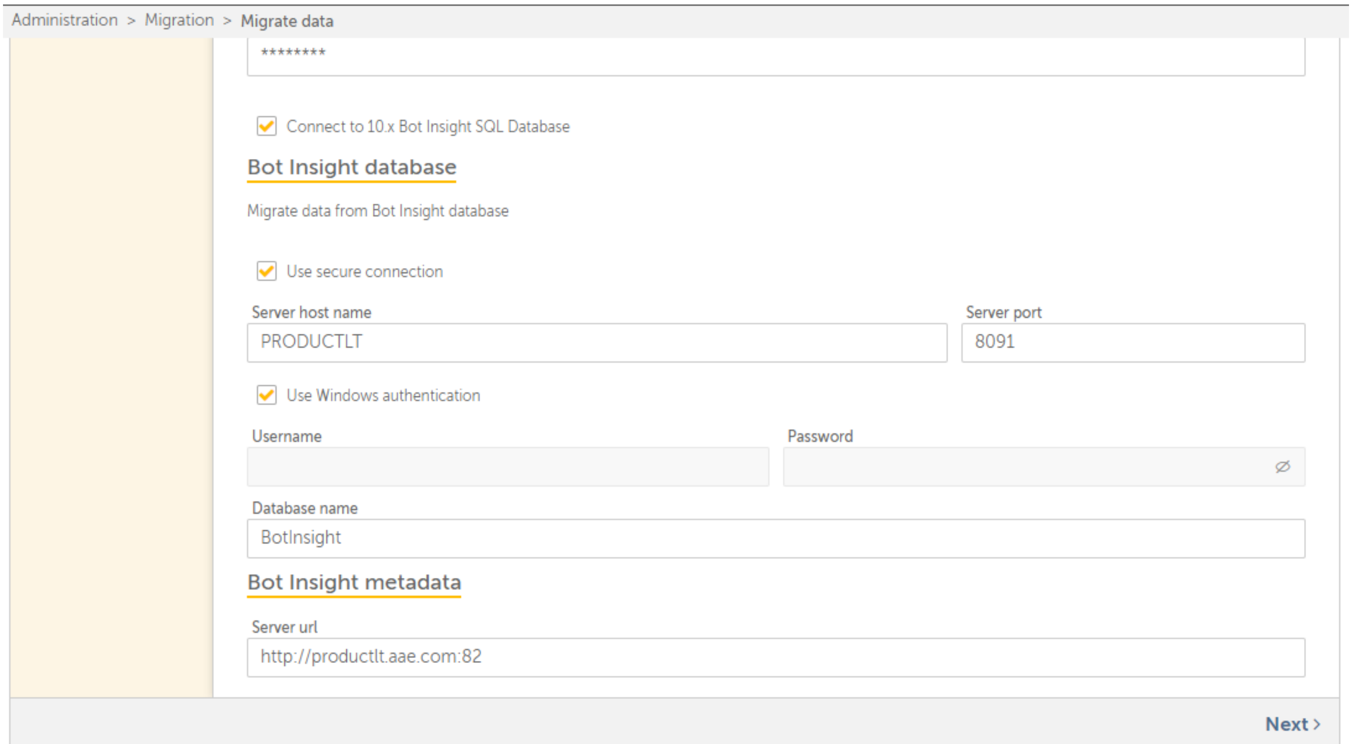
   > **Tip:** You can Close the page if you do not provide any data or Cancel if you want to go back to the Migration page without saving the data.

   > **Note:** You can change the **Database** connection settings until the migration process is started. The database tab is disabled once the process starts.

7. Click Next >

Bot Insight Database

Applicable only if Bot Insight is installed on source Control Room 10.x



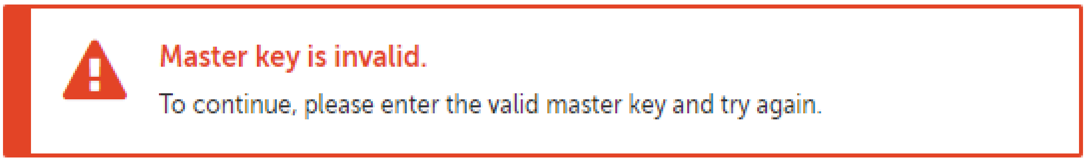
To migrate data from source Bot Insight database,

1. Select **Connect to 10.x Bot Insight SQL Database**. This enables all other fields for Bot Insight database connection.
2. Keep the **Use secure connection** selected if the SQL instance hosting 10.x Bot Insight database is configured with a secure connection. Clear this if the source SQL Server is not configured with secure connection.
3. Provide the **host name** and **port** number of the SQL Server where v10.x Bot Insight database is hosted. For example, PRODUCTLT and 8091

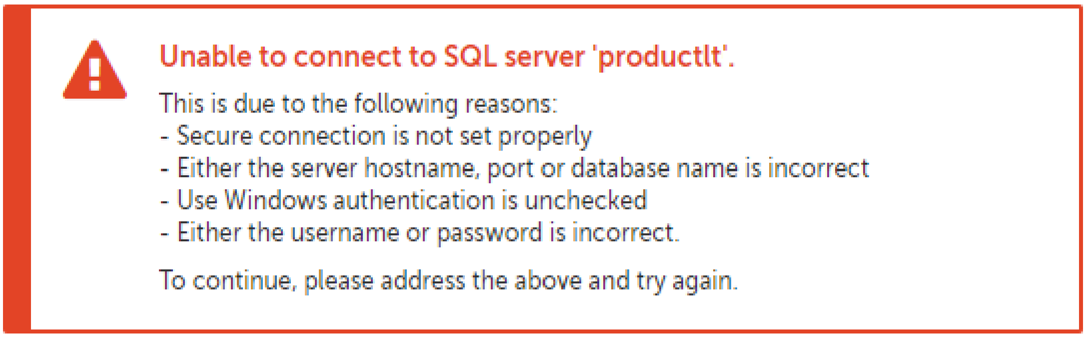
4. Keep the **Use Windows authentication** selected if the source SQL Server is configured using Windows authentication. Alternatively, **clear** the option and provide **Username** and **Password** if SQL Server is configured with SQL authentication.
5. Type the source Control Room Bot Insight database name. For example, BOTINSIGHT10
6. Type the Server URL where Bot Insight Visualization ServerPort is configured. For example, http://productlt.aae.com:82/analytics
7. Click **Save** to connect to the database. When the connection is established, you can move to the next step.
8. Click **Next >** to select migration of data based on roles or users.

Errors

1. If the master key is invalid, you are shown:

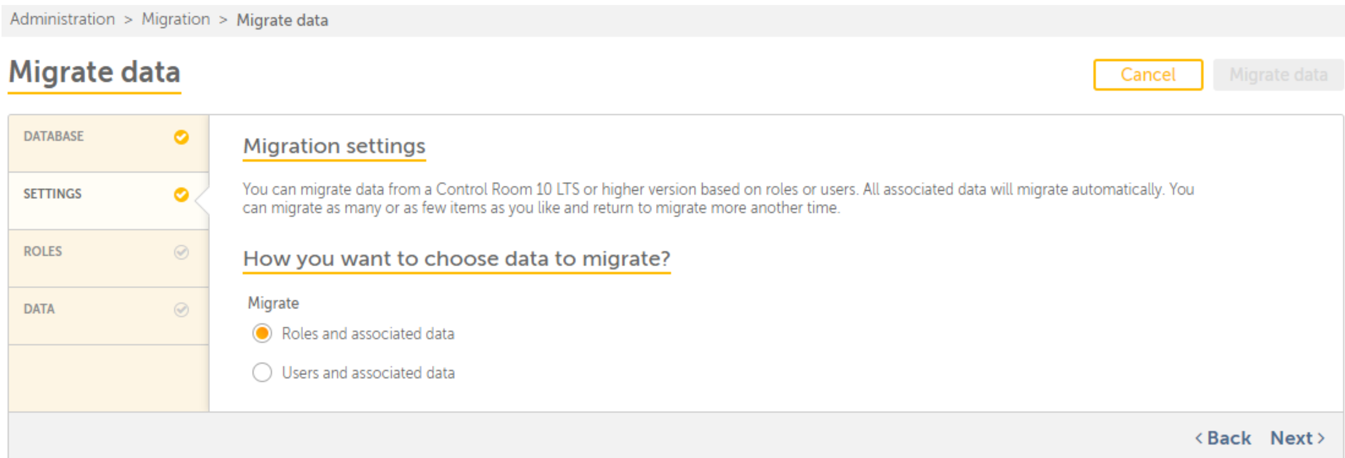


2. If a connection could not be established, you are shown:



Settings

You can choose to migrate data from your source Control Room based on roles or users in the **Settings** page. Though it is possible to migrate entire data at one go, this method is not recommended. Hence, you can migrate selected data in different phases.



Migration of data can be done using two options,

1. Migrate data based on **Roles**. This option allows you to migrate selected roles data from source Control Room database. When you migrate the roles, data associated with those roles such as users, license, bots, credentials, and schedules are also migrated.
2. Migrate data based on **Users**. This option allows you to migrate selected user data from source Control Room database. When you migrate the users, data associated with those users such as roles, license, bots, credentials, and schedules are also migrated.

Tip:

- It is recommended that you migrate data using **Roles** as on migrating roles all users associated with that role are migrated along with related data such as its bots, folder access permissions, schedules, and information regarding the user who created the bot.
- If you migrate data using **Users**, the Roles that are NOT associated with any User might not be migrated. Similarly, the Schedules that are associated with the Users that were NOT selected for migration shall not be migrated.

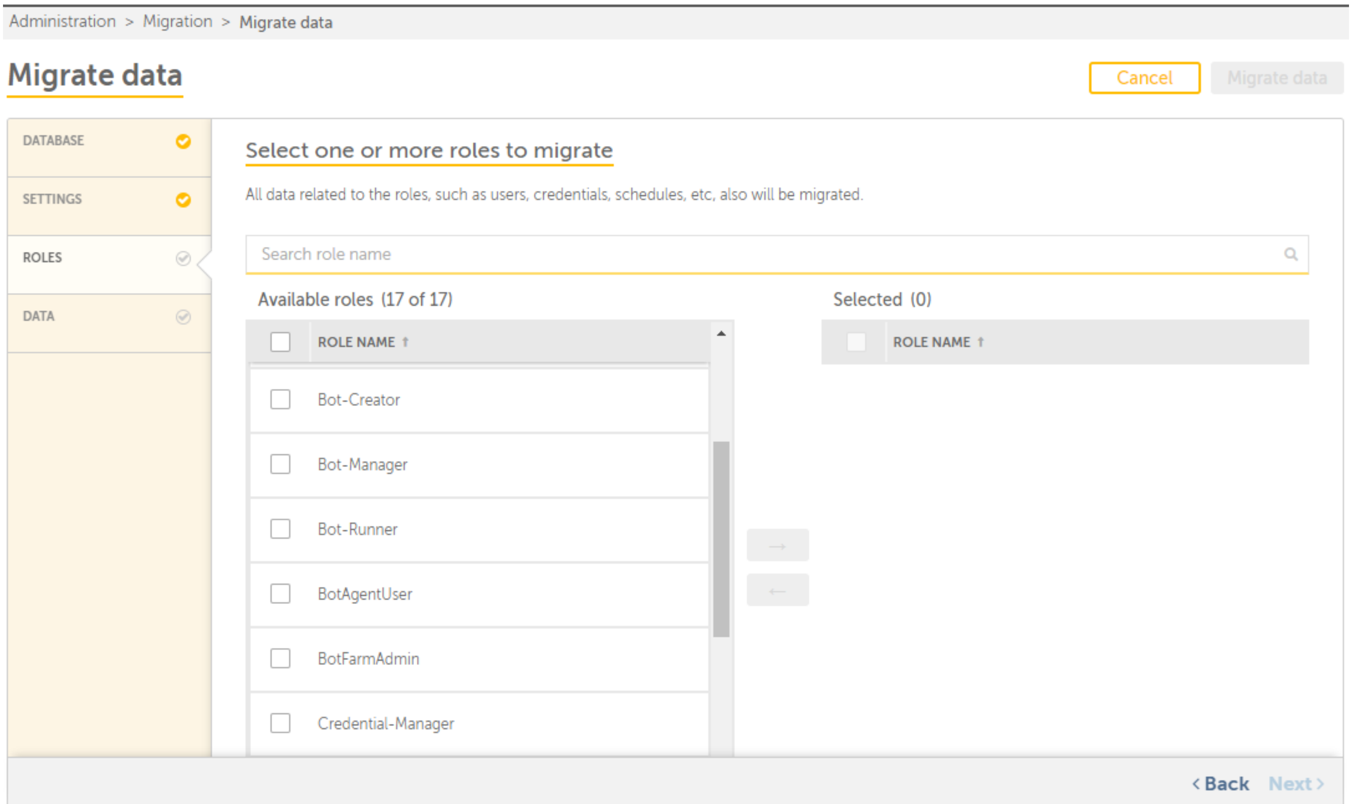
Click Next > once you select an option.

- When you select **Roles and associated data** and click Next >, the **Roles** page is displayed. This option is selected by default.
- When you select **Users and associated data** and click Next >, the **Users** page is displayed
- You can switch between the two options. Use Cancel if you have not made any updates or click < Back to return to the previous page.

Roles

The Roles page allows you to migrate all or only selected roles from source to destination Control Room. When you select roles, other related data such as license, users, credentials, and schedules are also migrated. This tab is shown only if you select **Roles and associated data** in **Settings** tab.

Tip: For ease of access, you can search for role names to migrate.

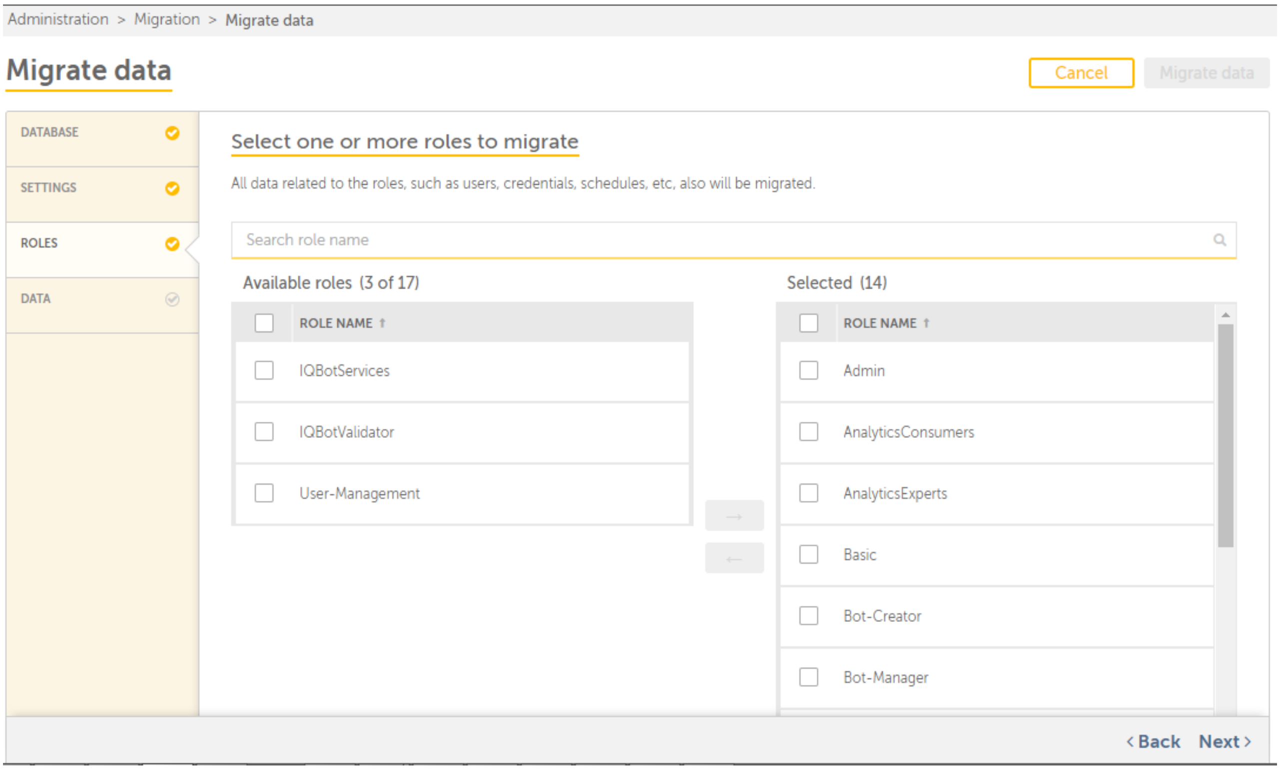


Select Roles

1. In the **Available roles** list, select the check-box beside **Role Name** if you want to select all roles. Alternatively, select each role from the list of roles.

    > `Note: The **Available roles** display all roles - both system and user defined that exist in 10.x CR database.`

2. Click →
3. The roles are added to the **Selected** list.



4. Click Next > to go to **Data** page

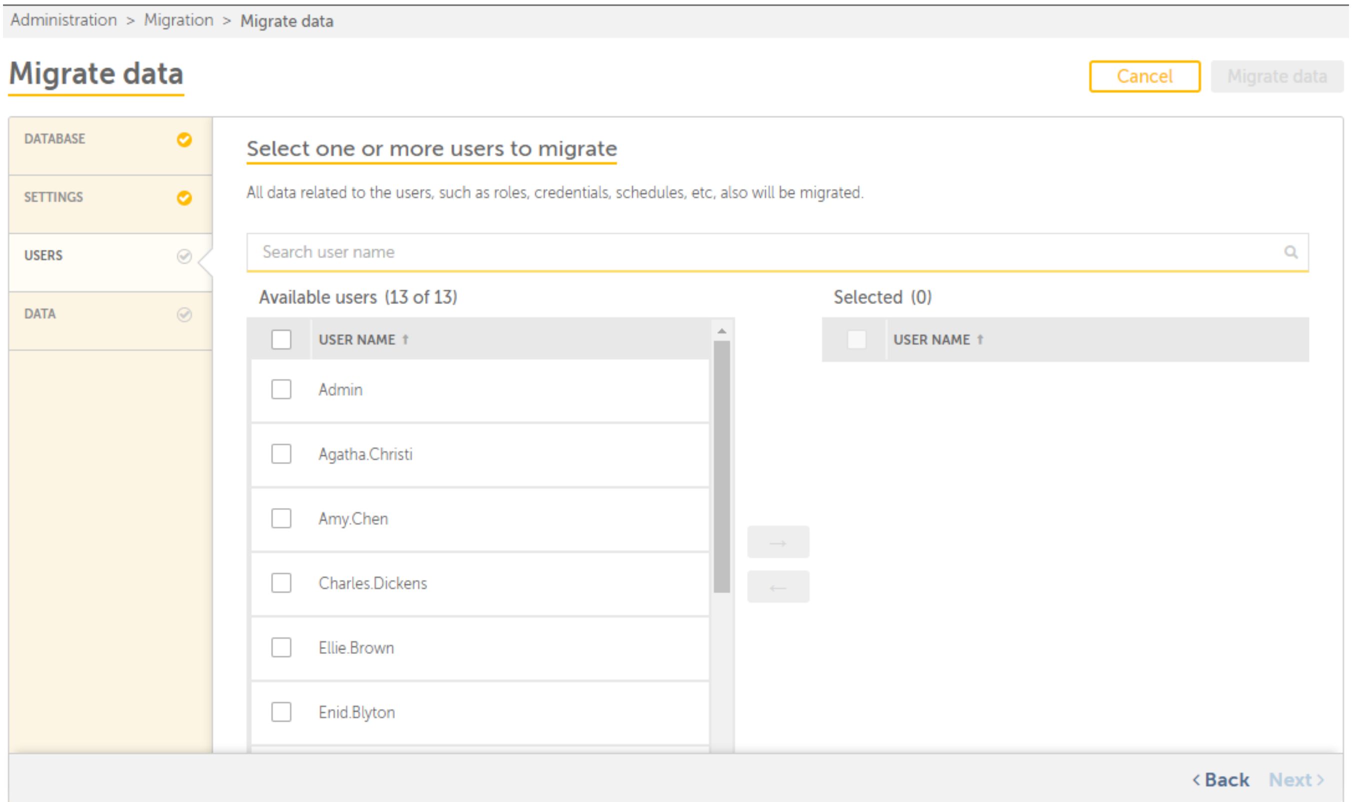
Migration behavior - roles

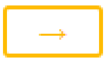
- The system defined roles from source 10.x Control Room are mapped to the destination 11 LTS Control Room
- Similarly, user permissions from source 10.x Control Room are mapped to the destination 11 LTS Control Room
- Roles that have any of the Upload, Download or Delete permissions, are granted Run/Schedule permission by default on migration
- User defined roles with same name will have **_1** suffixed to its name. For example, If a role **Bot_Manager** is available in both versions of the Control Room, the 10.x Control Room role will be created as a new role with the name **Bot_Manager_1**
- For next migration run, the **Available roles** list will display all roles irrespective whether they are migrated or not

Users

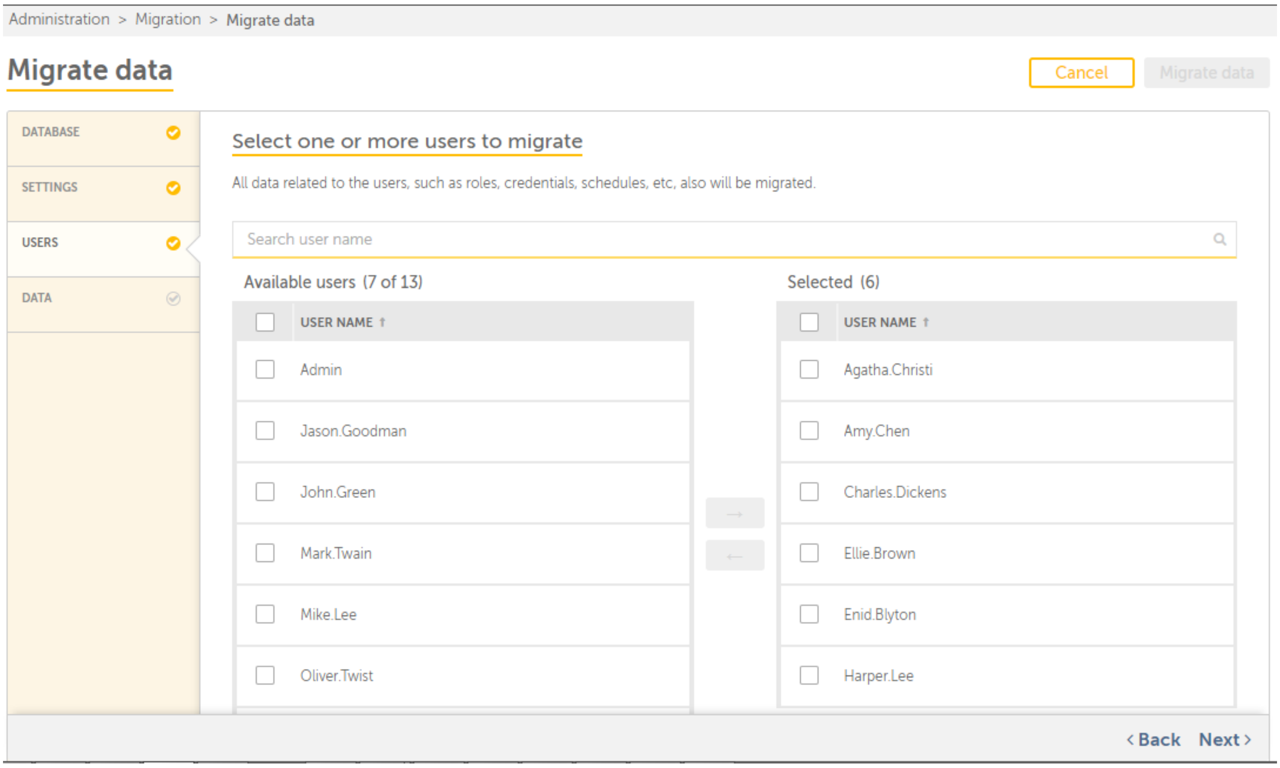
The Users page allows you to migrate all or only selected users from source to destination Control Room. When you select users, other related data such as license, roles, credentials, bots, and schedules are also migrated. This tab is shown only if you select **Users and associated data** in **Settings** tab.

> **Tip:** For ease of access, you can search on user names for migration.



1. In the **Available users** list, select the check-box beside **User Name** if you want to select all users. Alternatively, select each user from the list of users.
2. Click 

3. The users are added to the **Selected** list.



4. Click **Next >** to go to **Data** page

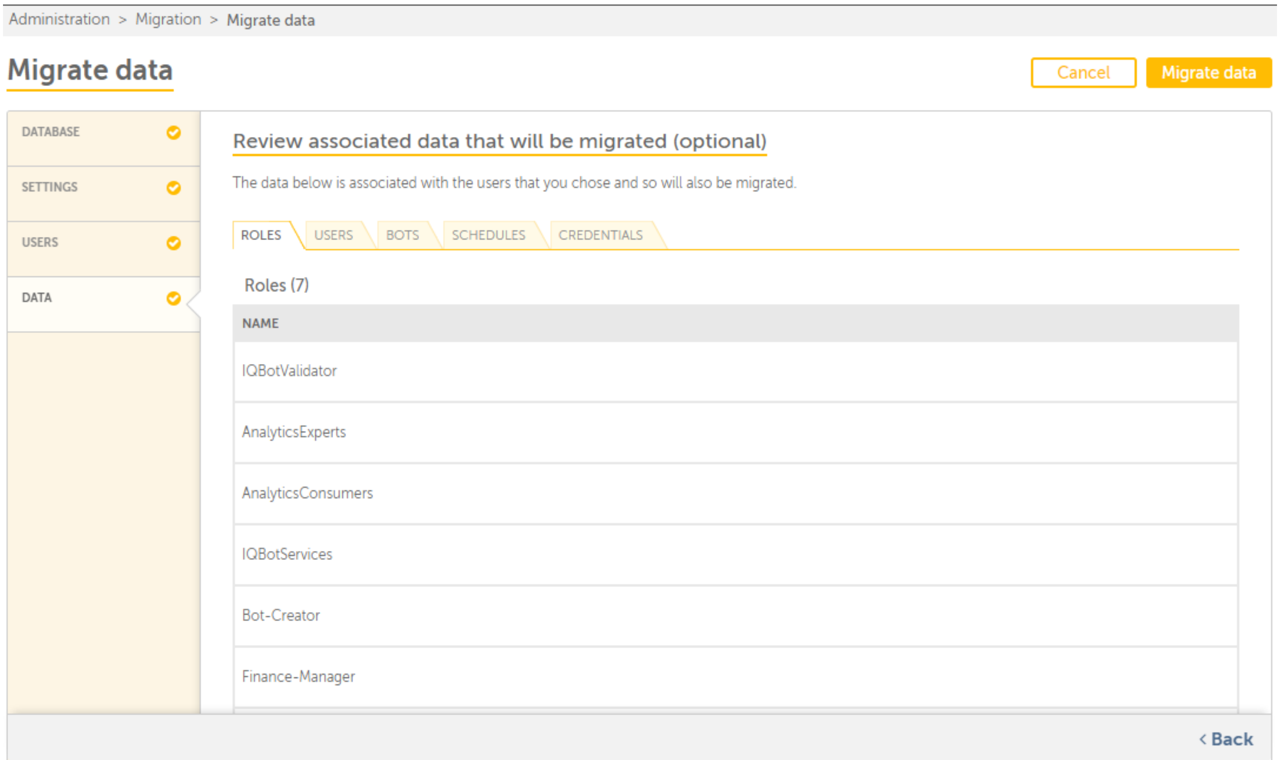
Migration behavior - users

- Users with same name will have **_1** suffixed to its name. For example, If a user **Mike_Lee** is available in both versions of the Control Room, the 10.x Control Room role will be created as a new user with the name **Mike_Lee_1.** However for Active Directory users, if the domain user with same name already exists in the destination Control Room, then such users and their dependencies are skipped during migration.
- For next migration run, the **Available users** list will display all users irrespective whether they are migrated or not
- Deleted users shall not be migrated

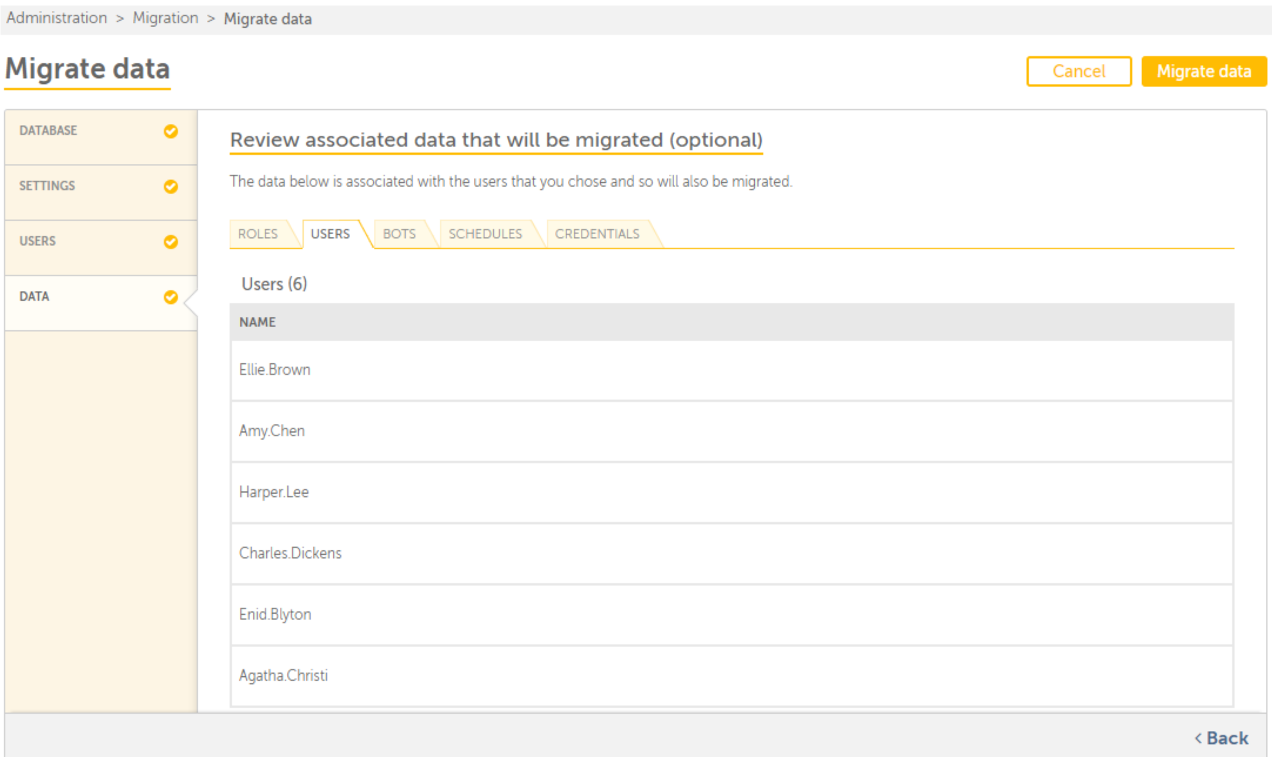
Migration - View Data

You should now verify whether the data that you selected is ready for migration. The data not only includes the Roles and/or Users that were selected, but also dependent or associated data such as Bots, Schedules, and Credentials if any.

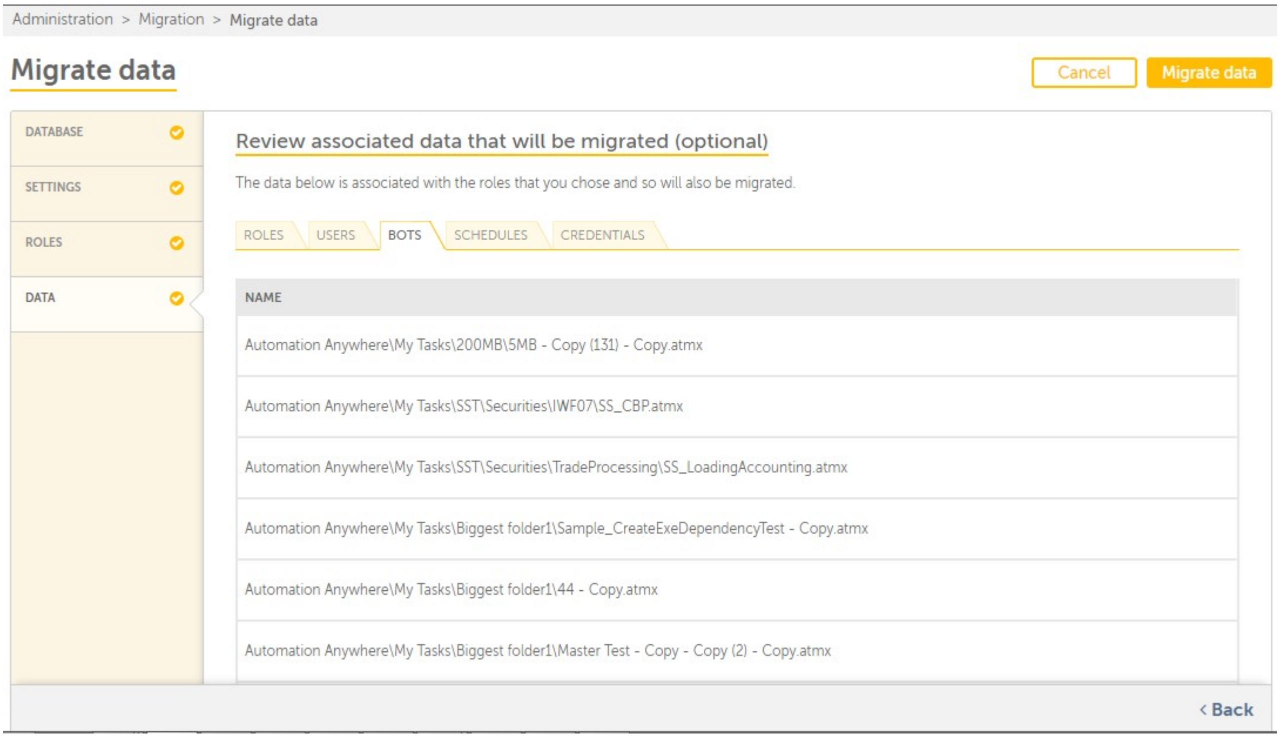
1. The **Roles** tab is displayed first wherein you can verify the roles that you selected are available for migration:



2. Verify the **Users** are available for migration. These could either be the ones that you selected or the ones that were included based on roles that you selected:

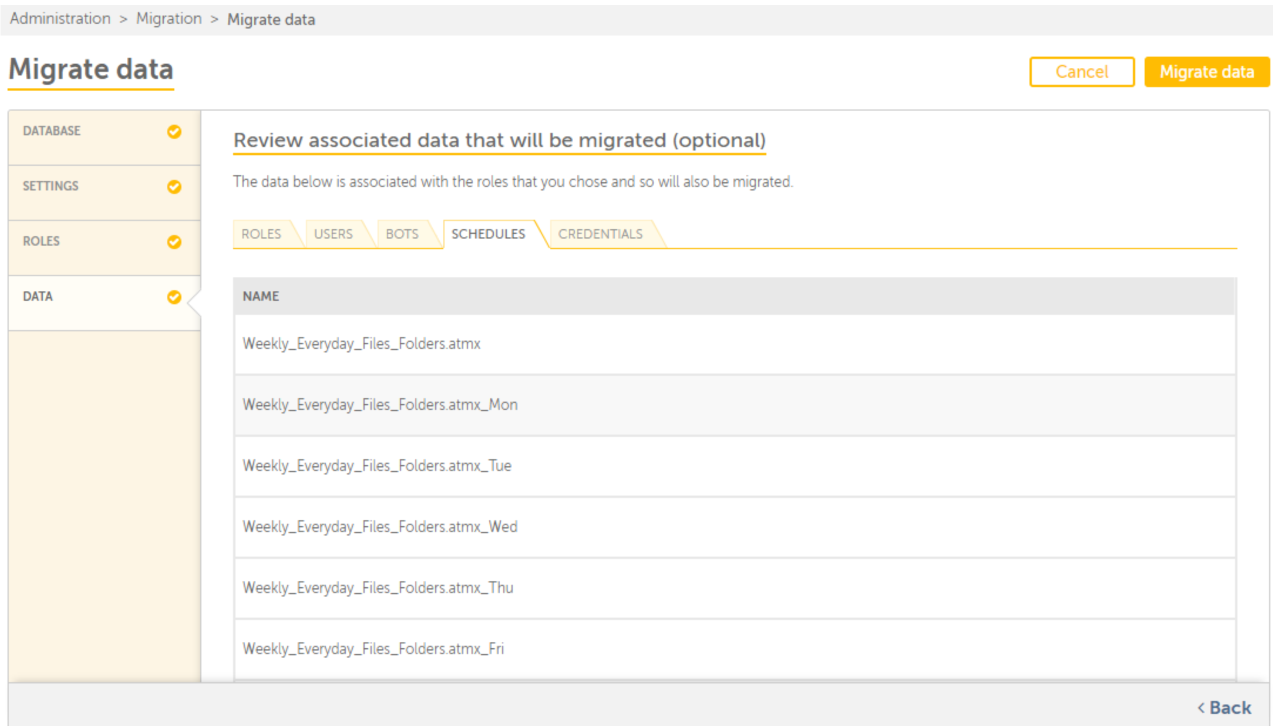


3. Verify the **Bots** are available for migration.

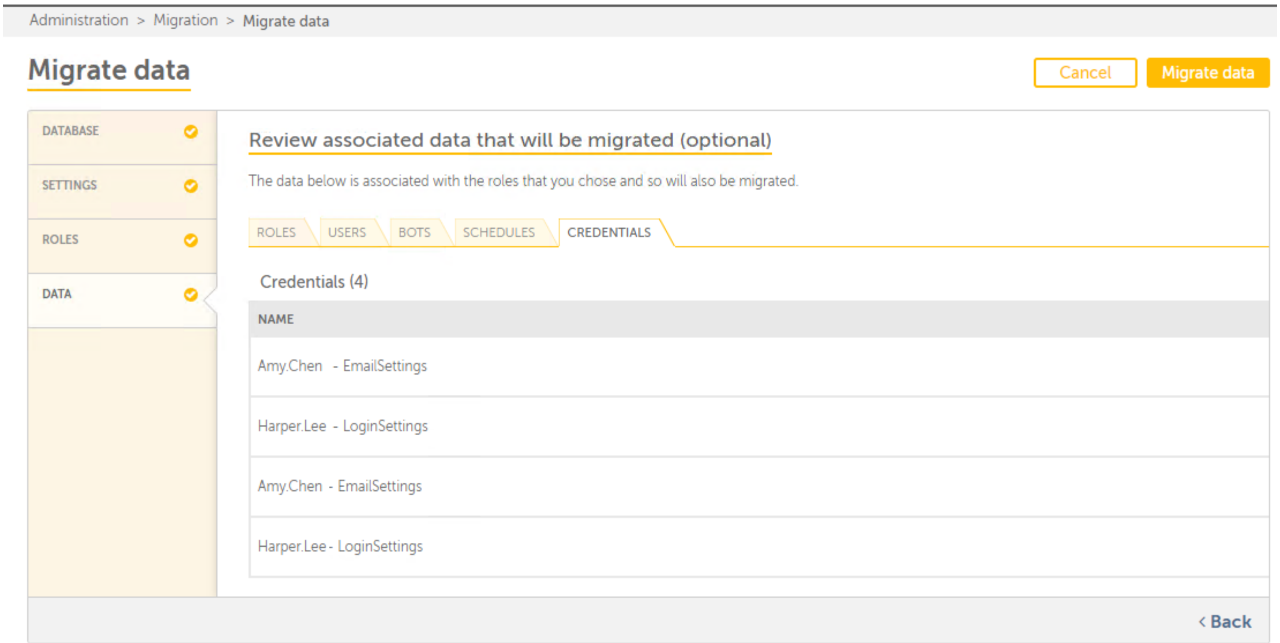


Note: Migration of Bots is based on the User role as well as the folder permission granted to that user. Hence Bots that correspond to that folder are displayed.

4. Verify the **Schedules** associated with the Bots are available for migration:

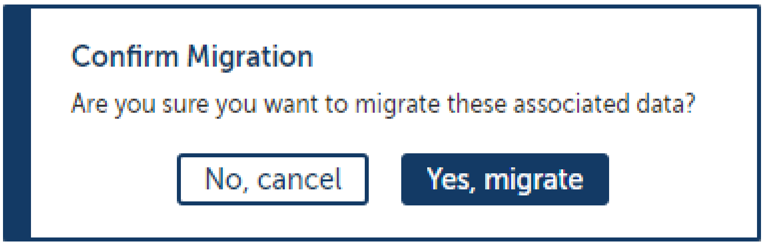


5. Verify the system **Credentials** associated with the Users are available for migration:

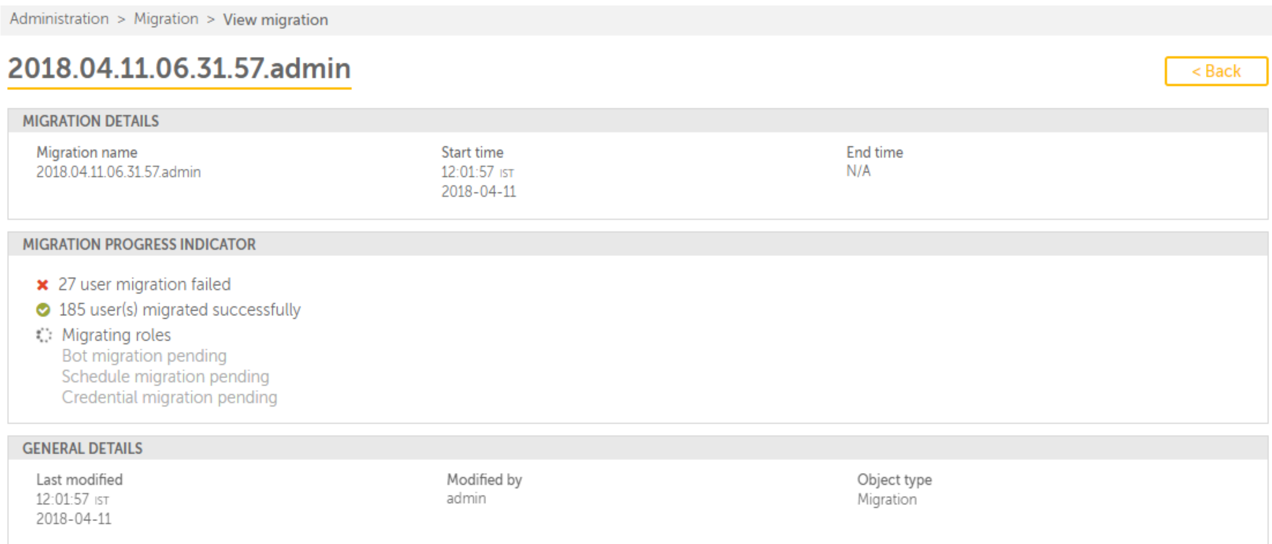


6. Click

7. Confirm:

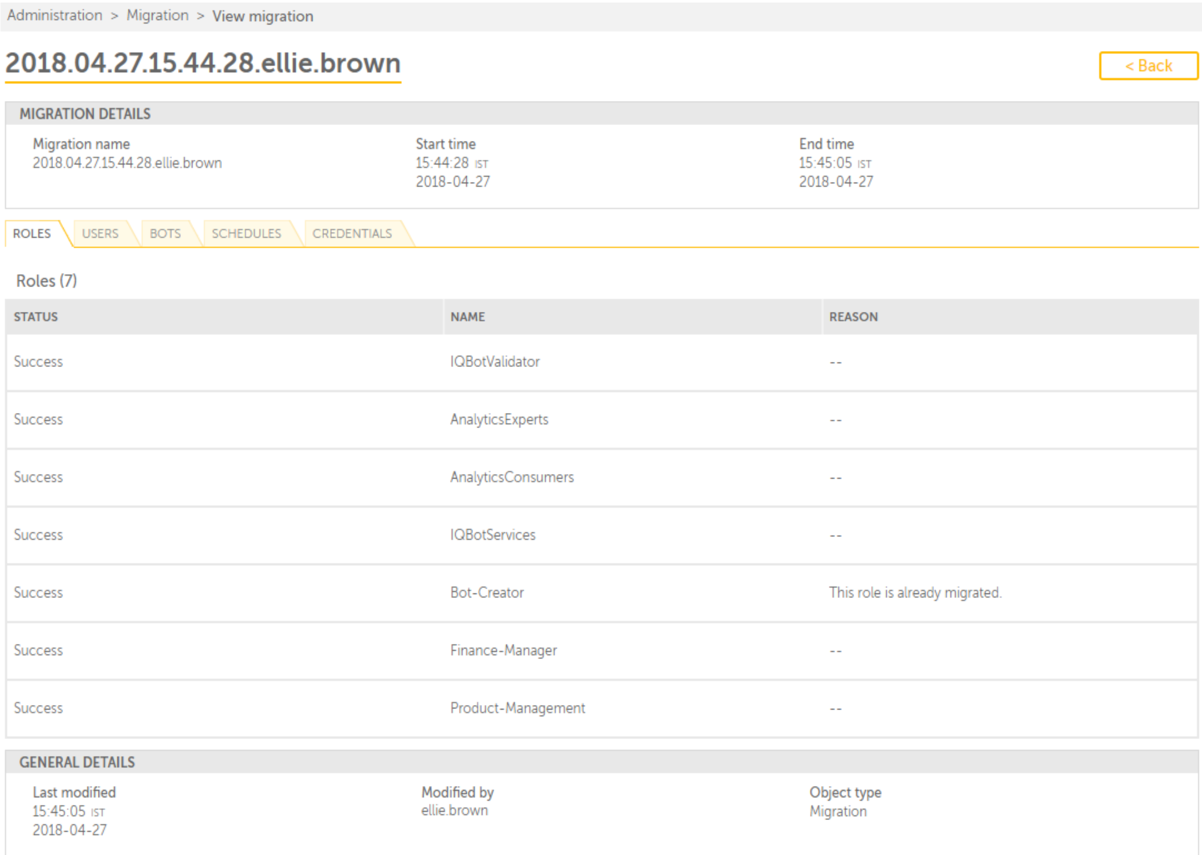


8. You can view the progress as shown:

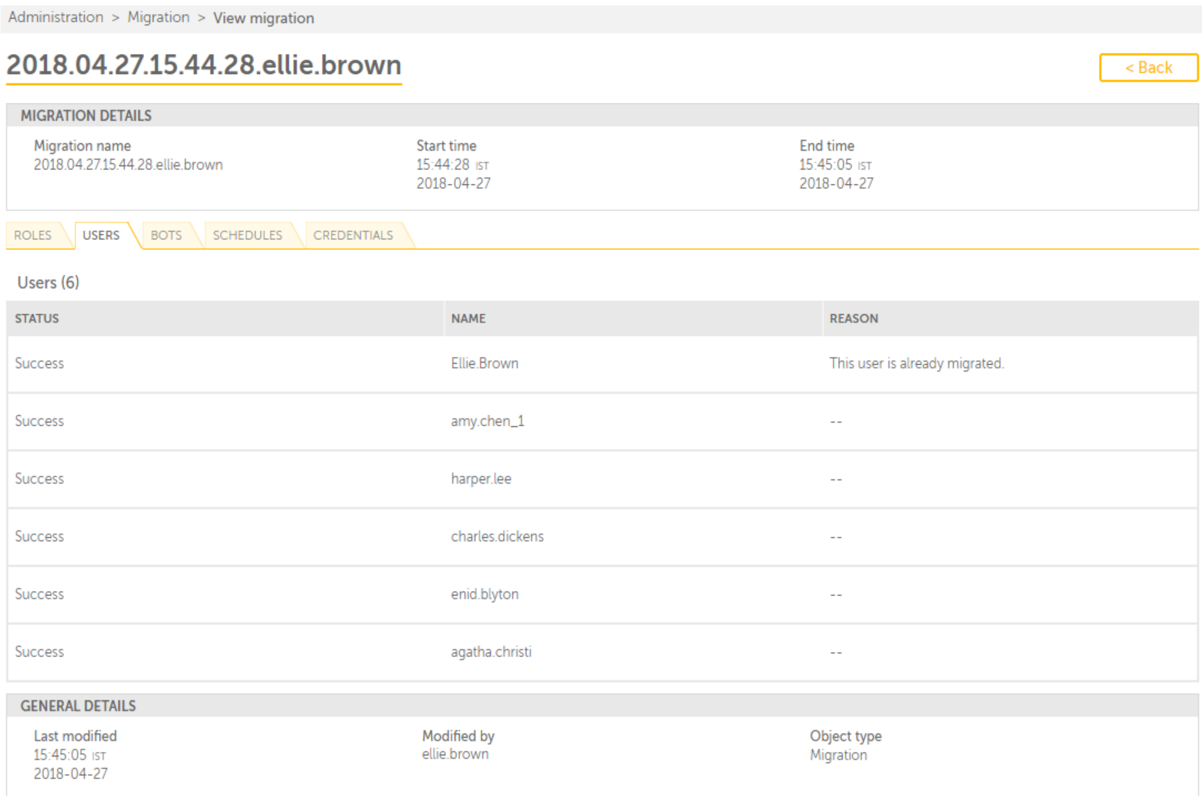


9. Once the migration process finishes, the status of data is shown in separate tabs:

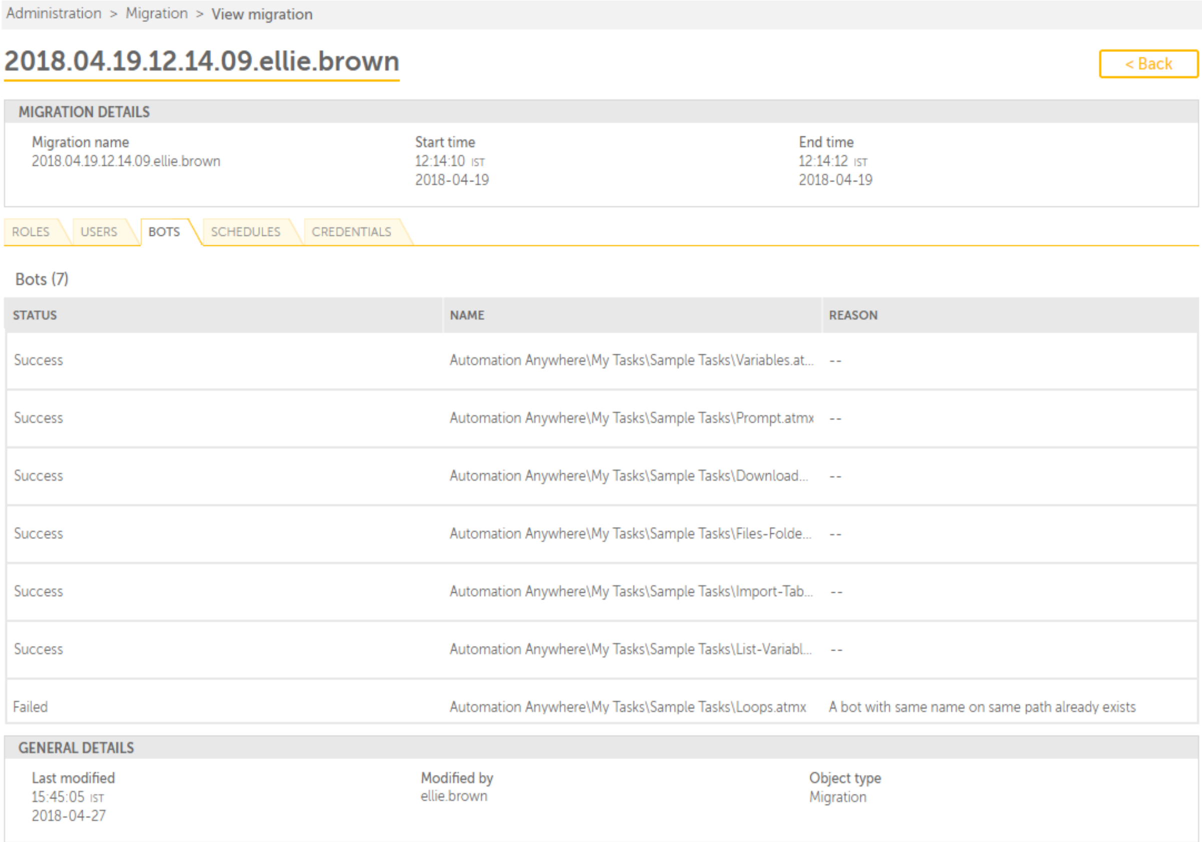
a. The following illustrates a **Roles** tab with the Status, Name, and Reason for each data:



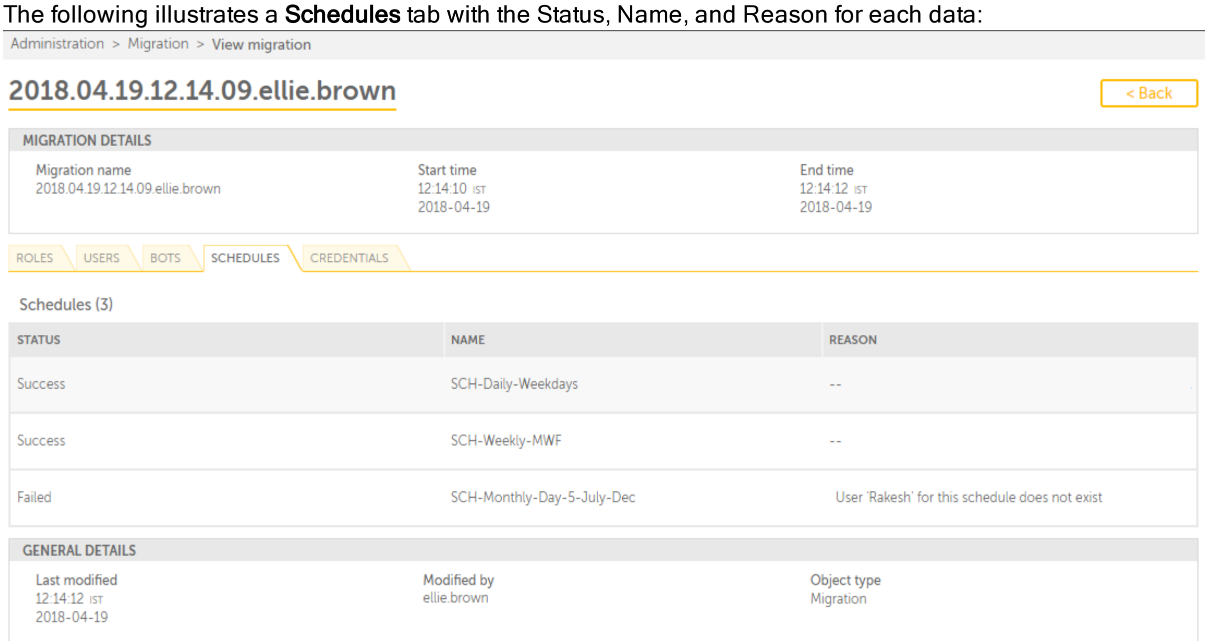
b. The following illustrates a **Users** tab with the Status, Name, and Reason for each data:



c. The following illustrates a **Bots** tab with the Status, Name, and Reason for each data:

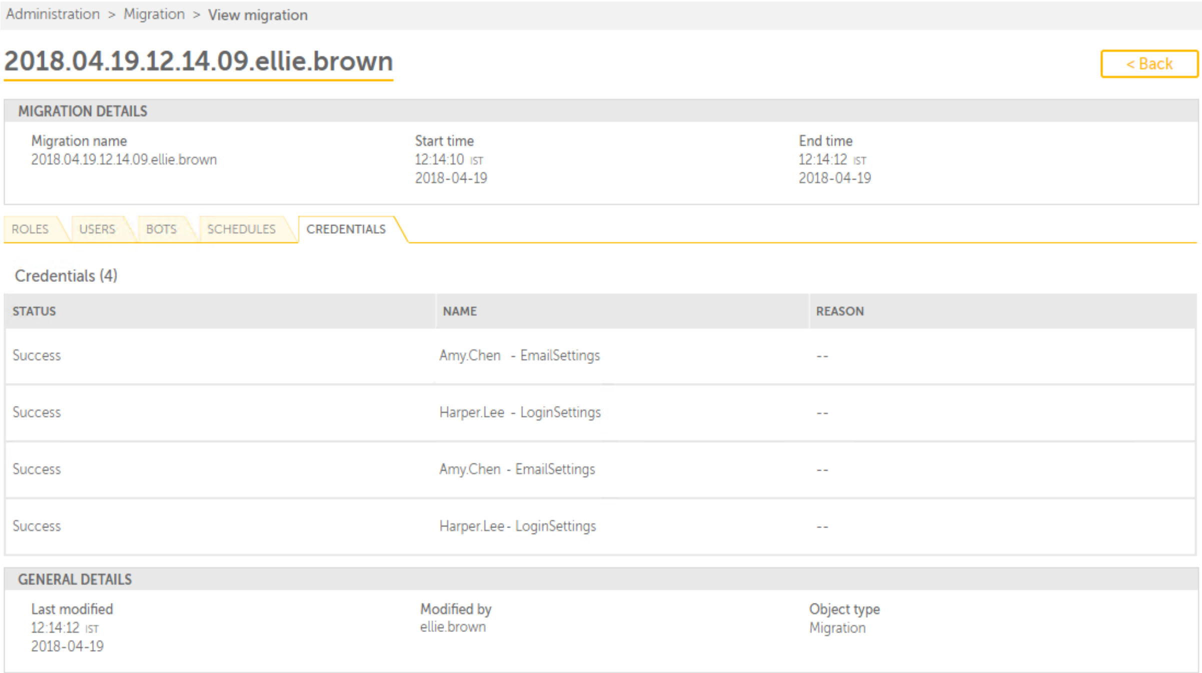


d. The following illustrates a **Schedules** tab with the Status, Name, and Reason for each data:



Note: By default, all schedules are migrated as disabled. These should be activated once the migration process is finished.

e. The following illustrates a **Credentials** tab with the Status, Name, and Reason for each data:



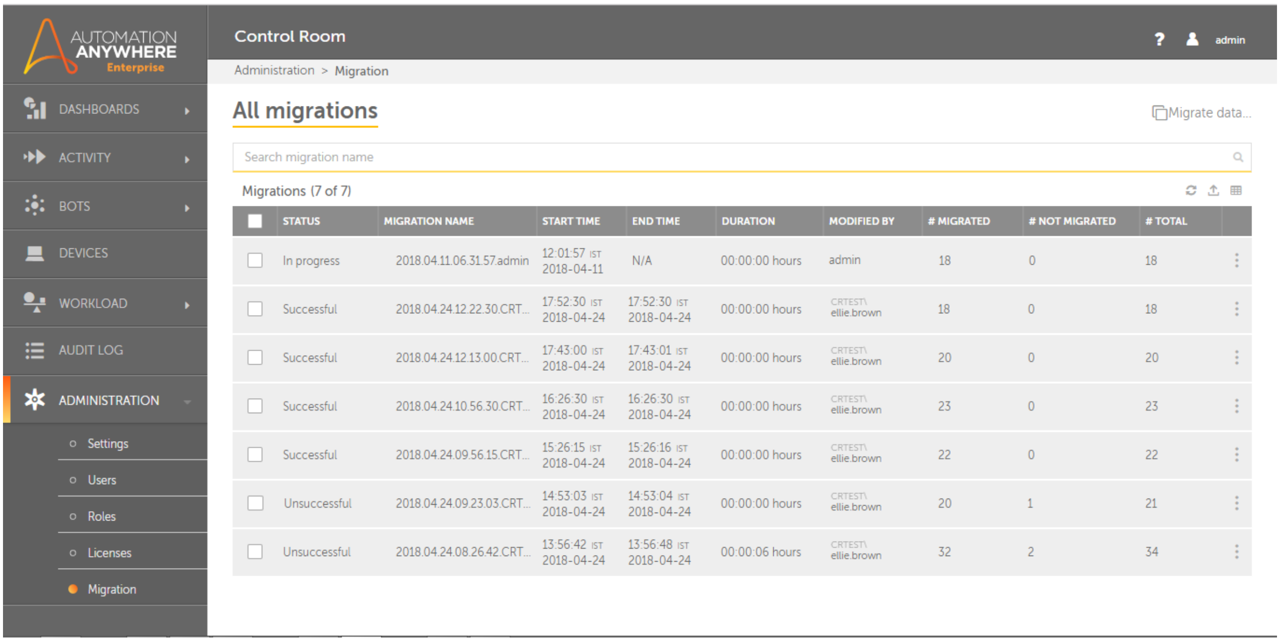
- The status of an entity can either be success or failed. Status is successful if the **Not Migrated** column shows 0 (zero) and unsuccessful if it shows > **0** (more than zero).
- When the data fails to migrate, you can verify why it was not migrated in the **Reason** column. The commonly seen messages are:
  - Role <RoleName> has been renamed
  - User <UserName> has been renamed
  - This <EntityName> is already migrated.

  ```
  Note: The <EntityName> is for Role, User, Bot, Schedule or Credential
  ```

- **General Details** pertaining to the process are displayed such as **Last modified** for the data and time, **Modified by** for user who initiated the migration and **Object type** for the type of action performed.

10. Once you have analyzed the migrated data, click 

to return to the Migration page wherein the migration activity is listed with status and other details:



11. On successful migration, you should perform the post migration steps as summarized in the next section.

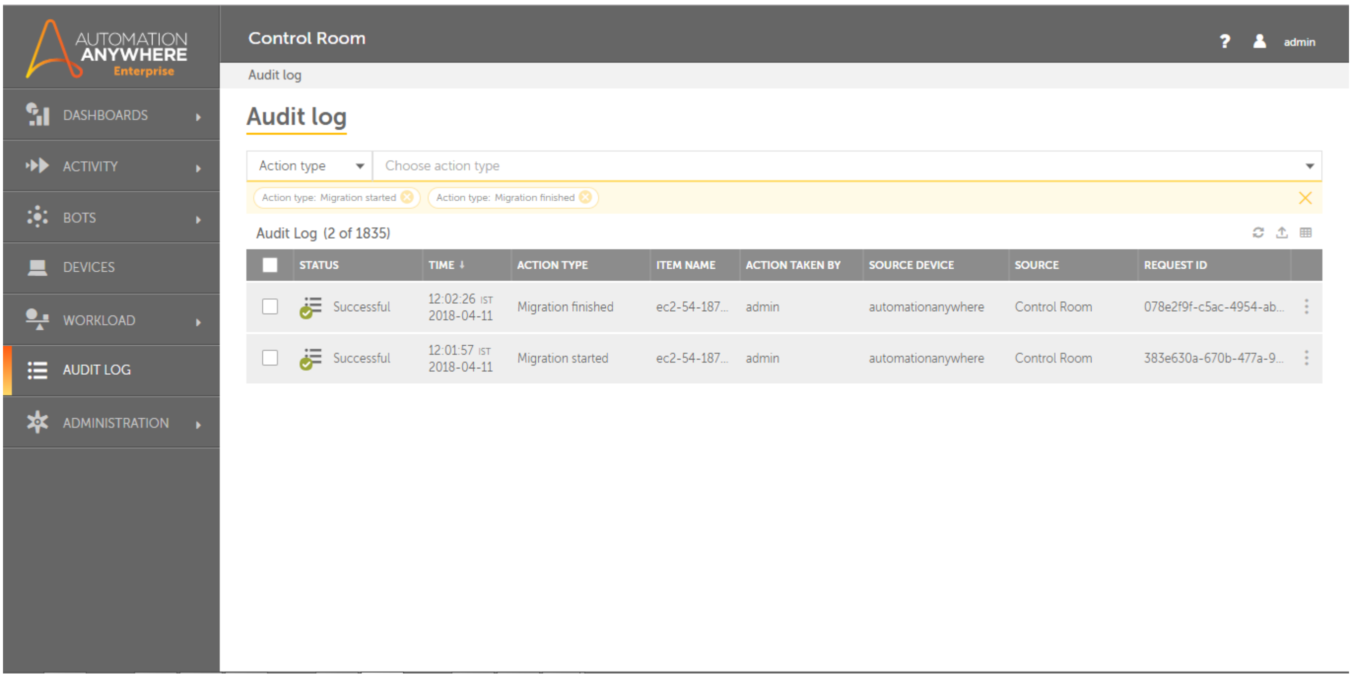
Post Migration Steps

Since all schedules are migrated as disabled by default, you should manually add the devices to the migrated schedules to activate them. You can perform the following to on-board the migrated schedules,

1. Install AAE 11 LTS Client. Refer AAE Client Installation Guide for details.
2. Register the Client devices with the migrated user. Refer Bot creators and bot runners - an overview for details.
3. Edit the schedules to add relevant devices
4. Enable the schedule.
   Refer Schedule a bot for step 3 and 4.

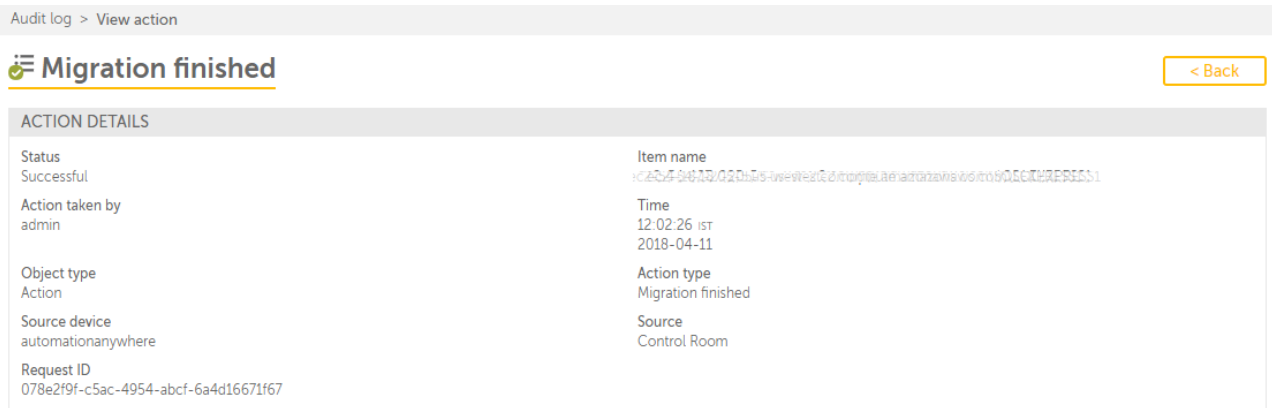
Audit Log

The **Audit Log** displays individual entry for each entity that is migrated.



When the migration process is initiated, a **Migration started** entry is logged in Audit log. Similarly when the migration process is completed, a **Migration finished** entry is logged. Between these two entries, migration entries are logged for each entity that is migrated such as **Create** or **Update** operation.

- Click to view details of the process. For example, the following illustrates details of a successful migration:



Known behavior of data migration

1. Bots and Files are migrated based on user having at least one folder permission viz Upload, Download or Delete. Similarly MetaBots are migrated based on user having at least one folder permission viz Upload, Download Delete or Execute.
   - Note that 'My MetaBots' folder permissions are not propagated when a new folder is migrated in the destination Control Room.
   - If a 10.x bot to be migrated already exists in 11.x then the same will not be migrated
2. If the source Control Room has Version Control enabled then
   - The version history of both the bots and its dependencies is migrated
   - The production version which is last set will be migrated
   - Locked bots and files are unlocked and then migrated to 11.x
   - Client Last Modified and Modified by fields for each version of the migrated bot will be set to name of the current Control Room user running the migration process or else the Modified by field of the migrated bot is set to SYSTEM if the user referencing this field is not migrated in 11.x
3. In case of failure to migrate the Modified by field for bot(s), the field shows the name as SYSTEM in the My bots and Edit page.
4. You can migrate only those bots and files for which you have at least one permission for a Folder - Upload, Download or Delete. Similarly, you can migrate individual Metabots for which you have at least one permission - Upload, Download, Delete or Execute.
5. All user licenses are migrated automatically when you migrate the users. Note that license migration is not visible on the Control Room user interface.
   - If the number of licensed in destination 11 LTS Control Room are less than the ones available in source 10.x Control Room, and all are consumed in the destination Control Room, then a user might not be assigned a license.
6. During the first migration run, the entities related to CR Settings viz. Mail Server Configuration, Email Notification, and Client Configuration are migrated automatically.
7. All dependencies for a user or role are migrated based on the folder permissions the user has for the assigned role.
8. On migrating a 10.x role having any of the Upload, Download or Delete permission on a folder, the role is granted Run/Schedule permission by default in 11.1.
   - All system created roles in 10.x are mapped to the corresponding 11.x roles and hence are not migrated.
   - All default permissions available in 11.x are granted to all the 10.x roles that are migrated.
9. Password protect tasks and its schedules are not supported in 11.x and hence they cannot be migrated. These entities will be shown as Failed in the migration history details page
10. When migrating users, the following entities are automatically migrated,
    - License assigned to the user
    - System-defined Credentials related to Auto-login and Email Settings that are set in AAE 10.x Client by the user

    A license migration for the user may fail if the destination Control Room does not have sufficient user licenses If a user or role already exists in 11.x then on migrating such user or role, they will be renamed with suffix _1 added to their name. The existing entity will not be modified in 11.x. Deleted users in 10.x will not be migrated to 11.x.
11. If a schedule has some manual dependencies added in 10.x then they will not be migrated. Post migration the user will have to edit the TaskBot and add these manual dependencies as references and upload it to Control Room
12. When migrating a bot and its schedule, if the user who created the schedule is not migrated in 11.x then such schedules will not be migrated. If an entity viz. role, user, bot or schedule is migrated once then it will be available for next migration run however they will not be migrated again and the migration history detail page will show their status as Success and Reason as already migrated.
13. If you select a bot from 10.x that has the same name in 11.x, the bot and its' schedules are not migrated.
14. Schedules that are password protected are also not migrated.
15. Dashboard bookmarks are also not migrated. You will have to recreate those.

Migration - FAQs

1. What is the recommended migration strategy?
    - You can migrate data from source Control Room (version 10.x) to destination Control Room (version 11 LTS) in phases using the web based Migration wizard available in the Control Room for a user with Manage migration permission.
    - You can choose to either migrate Roles or Users from source to destination based on which all associated entities shall also be migrated automatically.
    - It is recommended that you migrate data using **Roles** as on migrating roles all users associated with that role are migrated along with related data such as its bots, folder access permissions, schedules, and information regarding the user who created the bot.
2. Are the AAE 10.x Bots compatible with 11 LTS Control Room? Can those be migrated?
    - To ensure the AAE 10.x Bots are compatible, you need to migrate them to 11 LTS Control Room. If you are using AAE 10.2, you should first migrate to either AAE 10 LTS or AAE 10 SP2 using the AAE Migration utility.
3. Are MetaBots created in AAE 10.2 or less compatible? Can those be migrated?
    - If you are using AAE 10.2 or a lower version, you should first migrate to either AAE 10 LTS or AAE 10 SP2 using the AAE Migration Utility to ensure your MetaBots are compatible.
4. Is Database migration required during platform upgrade?
    - Database migration can be done post the platform upgrade.
5. Is version history available once the data is migrated?
    - Yes, the version history is available. However note that you need to configure Version Control in destination Control Room manually as the source 10.x Version Control settings are not migrated. Also, the SVN repository should be different in both - source and destination Control Rooms.
6. Are credential variables and audit log entries migrated?
    - Only system credentials are migrated. The audit logs although migrated, are not available on the destination Control Room user interface.
7. If existing AAE 10.2 database or backup of AAE 10.2 database is used for AAE 11 LTS during setup, would there be challenges for AD mode setup specially when SSO with SAML 2.0 needs to be integrated?
    - You should create a new unused database for AAE 11 LTS. You cannot use the AAE 10.2 database for AAE 11 LTS. To ensure the data from this version is available, you should first migrate to either AAE 10 LTS or AAE 10 SP2 using the desktop migration utility. Thereon you can migrate your data to AAE 11 LTS.
8. Can schedules from the source Control Room that has version control enabled be migrated to the destination Control Room that does not have version control enabled? or the other way round?
    - The status of version control should be same in both Control Rooms. If it is enabled in source Control Room, you should manually configure version control in destination Control Room using an SVN repository that is independent/separate from the AAE 10.x version.
9. Is it possible to migrate schedules from different time zones?
    - This is not supported.
10. Do the migrated schedules retain their status and work as before?
    - The schedules do not retain their status and fire on their own - they are deactivated by default. To activate such schedules, you should perform certain steps - open it in edit mode, add devices, update time/date, etc.
11. What happens to schedules that have manual dependencies created in source Control Room that has version control configured?
    - To retain the manual dependencies after migration, you should,
        a. Download the required file(s) i.e. perform a rollback from Version History
        b. Manually add the reference dependencies
        c. Save the task
        d. Set the production version to run the task.
12. Is it possible to migrate schedules from source Control Room that are already present in the destination Control Room?

    Yes. Such schedules are migrated with the same name unlike Roles/Users which have suffix **_1**.

13. If a role or user is already migrated, will it be available for migration?
Yes such roles and users are available for migration. However, the reason would be shown as "This <entity name> is already migrated."
14. Can I migrate all the entities that were completely migrated?
Yes such entities are available for selection. However, the reason would be shown as "This <entity name>is already migrated."
15. Can I switch to User option of migration, once i have already migrated using Roles?
Yes you can.
16. Can I connect to multiple 10.x Control Room database for migration?
No. You cannot once the migration run is initiated.
17. If during migration, if my machine restarts, will I be able to continue the migration?
If your machine restarts when the migration is in progress, you can initiate the migration process despite the status being In progress. Also the entities that were already migrated will be shown as migrated.
18. Would the schedules created by a user who already exists in destination Control Room or is deleted from source Control Room be migrated?
Such schedules are not migrated. Refer examples given below for both Active Directory User and Non Active Directory user
    - **Active Directory user -** If the user Mike.Lee who has created a schedule say SCH1 in source Control Room also exists in destination Control Room, then the first run of the migration shows the following status for **Schedules**:

Status	Name	Reason
Failed	MyDomain.com\Mike.Lee	Unable to proceed as the user with same name already exists

    - **Non-Active Directory user -** If the user Mike.Lee who has created a schedule say SCH1 in source Control Room does not exist or is deleted in destination Control Room, then the first run of the migration shows the following status for **Schedules**:

Status	Name	Reason
Failed	Mike.Lee	User ‘Mike.Lee’ for this schedule does not exist

19. Since IQBots and My Lists are deprecated from 11 LTS, what happens to the bots that have IQBots as dependent files or the files that are there in My Lists?
IQBot dependency and My Lists are filtered out in the pre-scan as it is deprecated in 11 LTS. These are not listed in the preview.

Bots - Overview

As a Control Room user with administrator or My Bots privileges, you can use the Bots module of Control Room to:

- Run and schedule uploaded bots
- Run bot with queue
- Export bot files for Business Life-cycle Management
- Import bot files for Business Life-cycle Management
- Work with secure and centralized credentials

Note: To perform these actions, you must be an administrator or have the following roles and privileges.

- View my bots
- Run my bots
- Export bots
- Import bots

Credentials - Overview

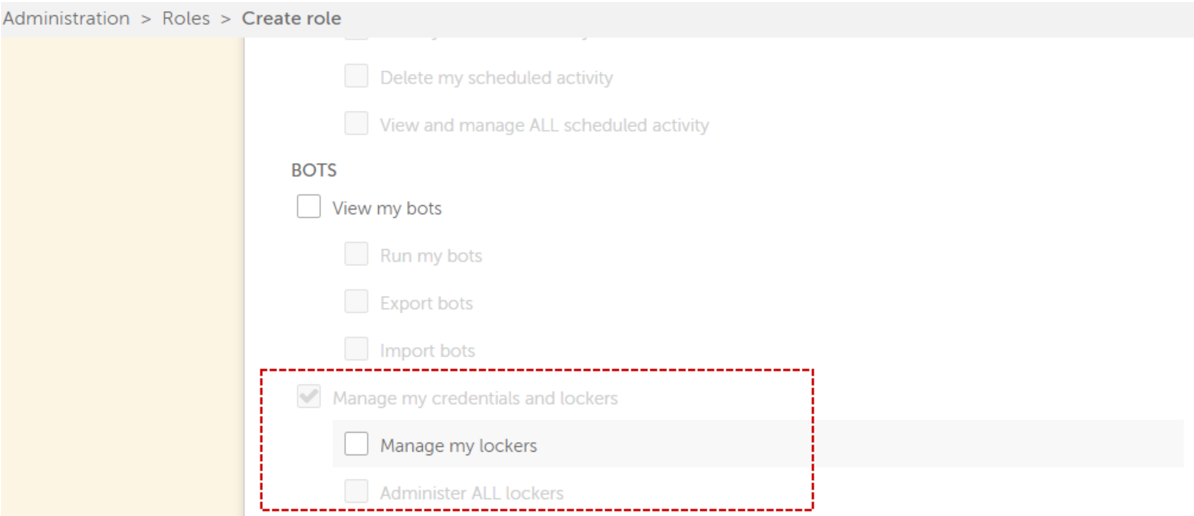
This page provides a centralized location for securely creating and storing sensitive information that is included in automation tasks in the form of credentials. All Control Room users can create credentials. Users with **Manage my lockers** permission can create lockers and users with Administer all lockers can manage all the lockers in the vault..

Benefits of creating credentials and lockers

Apart from providing a secure and centralized location for storing credentials, it:

- Minimizes the possibility of credential fraud.
- Provides an environment to enable improved security.
- Enables businesses to adhere to processes and credential management compliance.
- Offers increased Automation opportunities with secure data/ applications.

Roles permission for credential and locker management



- **Manage my credentials and lockers**: By default, you (all users) can see the Credentials tab and manage your own credentials. In addition, you can interact with locker of other users, if they provide locker access permission.
- **Manage my lockers**: This permission allows you to create and manage your own locker.
- **Administer ALL lockers**: This permission allows you to view all the lockers and perform limited actions on them.

> **Note:** This permission is available for AAE_Locker Admin role only

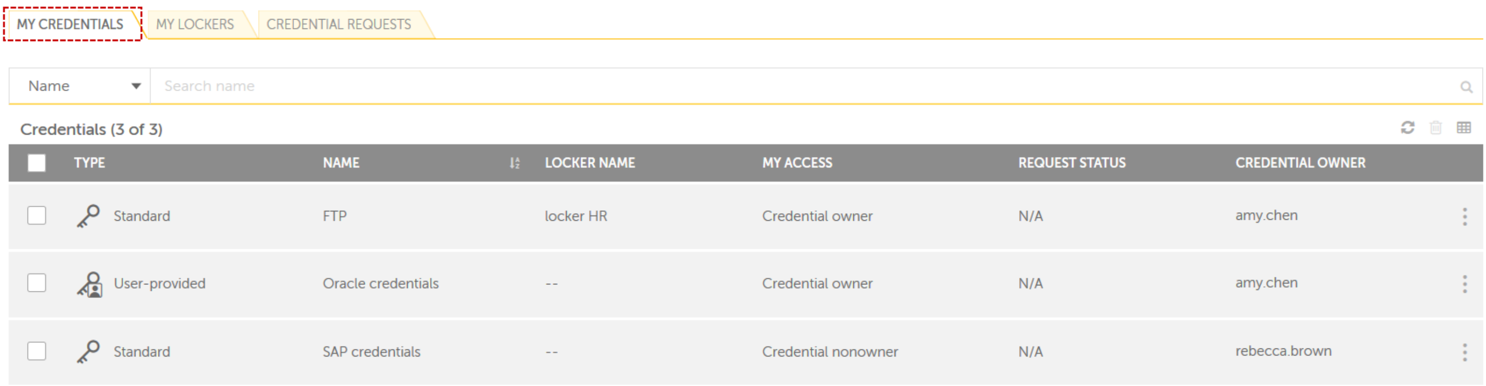
This page covers:

- My Credentials
- My Lockers
- Credential Requests

My Credentials

This tab consists the list of credentials created by a user. All users have permission to see their credentials.

Note: In case you have "AAE_Locker Admin" permission, then you are able to view credentials of all the users.



In the search pane you can filter credentials according to the following:

Search Item	Description
Type	**User- provided**: Credential owner and Locker consumers can input the value with usage access. **Standard**: User must input the value.
Name	Based on credential name
My Access	**Credential owner**: Credential has been created by you. **Credential non-owner**: Credential has been created by other user.
Request Status	All values provided or requests sent.

Note: When you specify search parameters for the same column, the system searches using **OR** operator. When you specify search parameters for different columns, the system searches using **AND** operator.

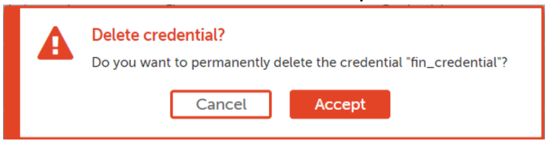
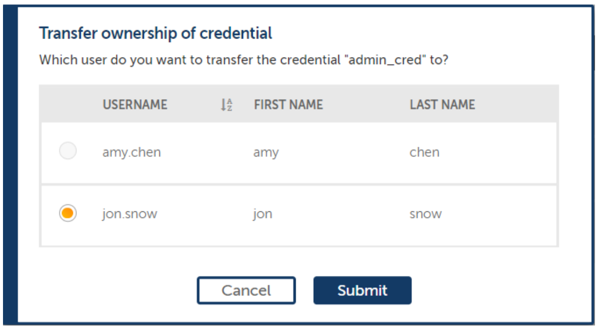
Tip: You can perform the following actions on a column to help you work efficiently.

- Click a column to sort it in ascending and descending order. You can sort up to three columns by holding the Shift key when you click on two more columns. This gives you the option of sorting two additional columns. This way the sorting is done on the entire table and not just the data that is currently visible to you. The last sorting is stored in memory applied by a user per session..
- Use a drag-and-drop operation to move the column left or right.
- Move your mouse cursor at the end of the column and drag to re-size.

The following describes the list of items that can be viewed in the table:

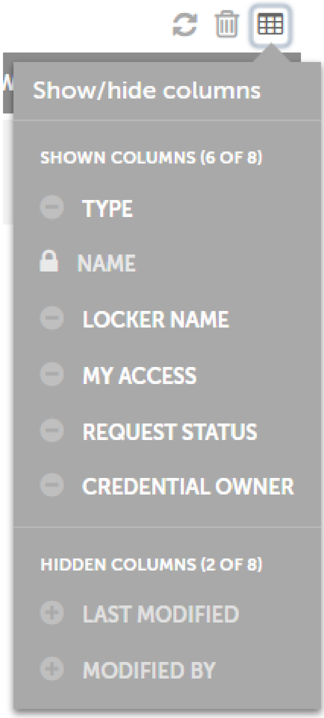
Table Item	Description
Type	Shows the type of credential as user-provided or standard.
Name	Name of the credential.
Locker Name	Name of the assigned locker for the credential .
My Access	**Credential owner**: Credential has been created by you. **Credential non-owner**: Credential has been created by other user.
Request Status	**All values provided**: Value has been given . **Requests sent**: Request has been sent to users to input credential value.

Credential Owner	Name of the user who has created the credential.

Actions	Description
View	Allows you to view credential details .Learn more
Edit	Allows you to edit a credential. Learn more
Delete	Allows you to delete a credential. Learn more **Note:** To delete a credential, user must be a credential owner To delete a credential, click Accept. 
Transfer Credential Ownership	Allows you to transfer the ownership of the credential. If locker is assigned to your credential then the ownership can be transferred to any member of the locker. Else it can be transferred to any user in the system. **Note:** Once the ownership is transferred to another user, the previous owner can no longer access the credentials. Also, only a Locker Admin has permission to transfer credential ownership. Select the user and click Submit. 

Alternatively, you can select all credentials and perform the following table-level actions:

Table Item	Description
Refresh	Allows you to refresh the list of credentials.
Delete	Allows you to delete multiple credentials.
Show/ hide columns	Allows you to show or hide specific columns. By default, all the columns are displayed.

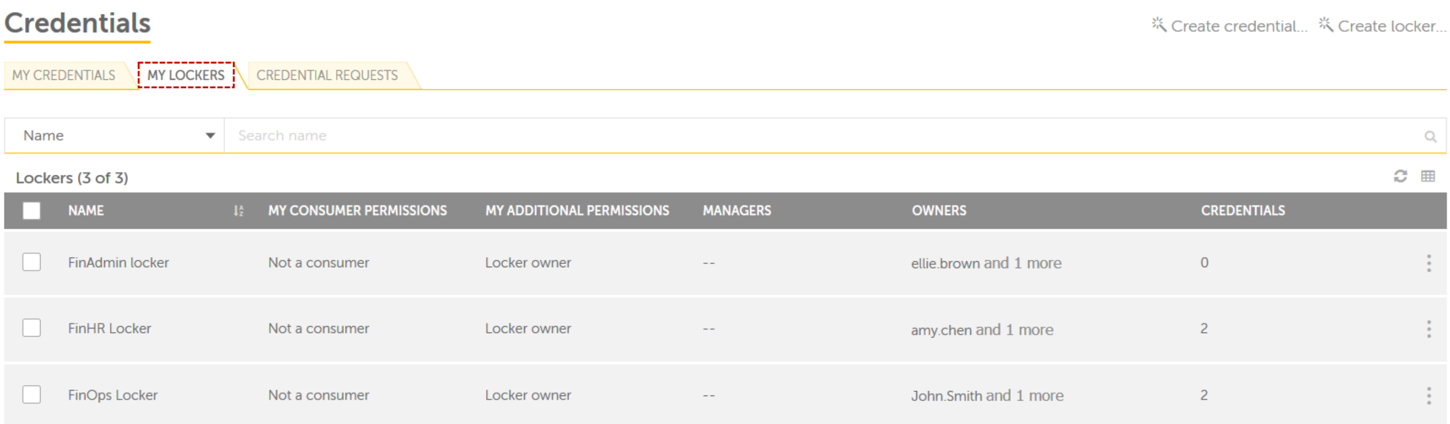


Tip: To **show/ hide** a column, click the column name.

My Lockers

This tab shows the list of lockers that has been created by a user. A locker can only be created by an authorized user with Locker_ Admin permission or a user having 'Manage my locker' permission.

Note: Users can see lockers only if they have created them or if they are a member of that locker.



In the search pane you can filter lockers according to the following:

Search Item	Description
Type	**User- provided**: Credential owner and Locker consumers can input the value with usage access. **Standard**: User must input the value.
Name	Based on locker name.

My consumer permission	Consumer or not a consumer.
My additional permission	Locker participant, manager, owner.

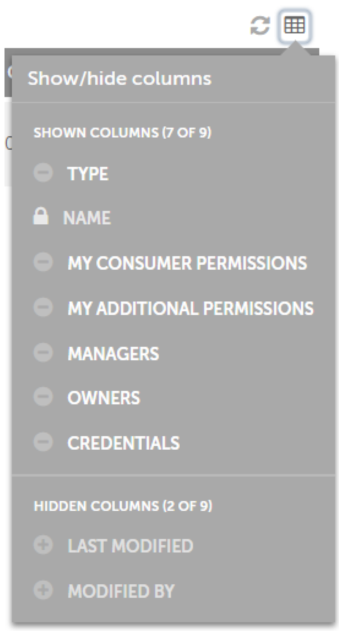
The following describes the list of items that can be viewed in the table:

Table Item	**Description**
Name	Name of the locker.
My consumer permission	Consumer or not a consumer.
My additional permission	Locker participant, Locker manager, Locker owner.
Managers	Users having locker manager permission.
Credentials	No. of credentials assigned to a locker.
Owners	Name of user who created the locker.

Actions	**Description**
View	Allows you to view locker. Learn more
Edit	Allows you to edit a locker. Learn more
Delete	Allows you to delete a locker. Learn more

Alternatively, you can select all lockers and perform the following actions:

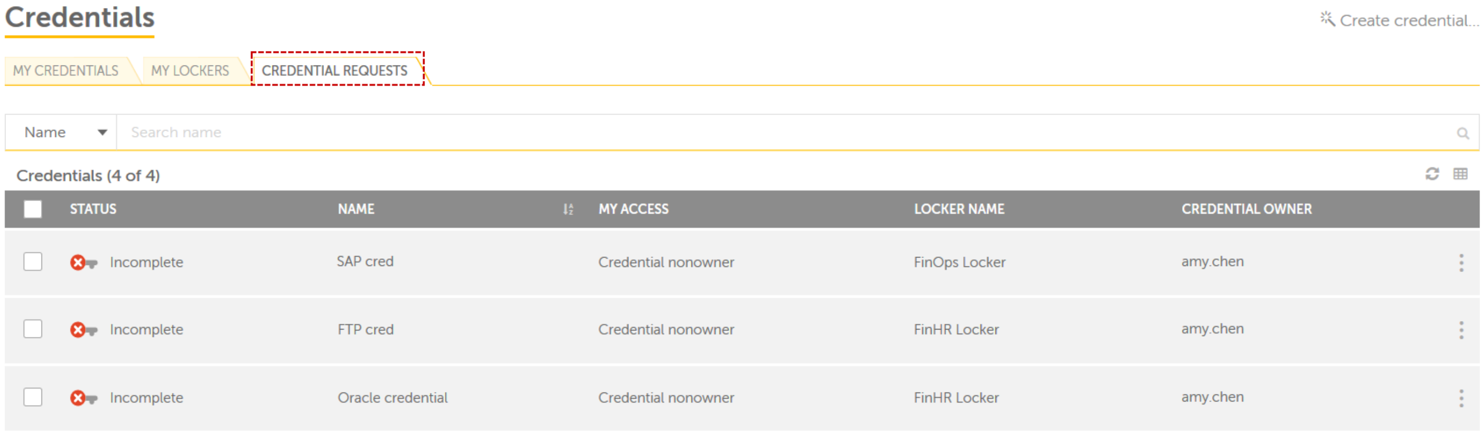
<table>
<tr><th>Table Item</th><th>Description</th></tr>
<tr><td>Refresh</td><td>Allows you to refresh the list of lockers.</td></tr>
<tr><td>Delete</td><td>Allows you to delete multiple lockers. Learn more</td></tr>
<tr><td>Show/ hide columns</td><td>Allows you to show or hide specific columns. By default, all the columns are displayed.



Tip: To **show/ hide** a column, click the column name.</td></tr>
</table>

Credential Requests

This tab shows the list of user-provided credential requests sent to a Locker Admin and Locker owner i.e. when a credential is created with attribute as user-provided, all the consumers in the locker receive a request to fill in the credential value.



In the search pane you can **filter lockers** according to the following:

Table Item	Description
Status	Status of credential is complete or incomplete.
Name	Based on locker name.
My access	**Credential owner**: Credential has been created by you. **Credential non-owner**: Credential has been created by other user.

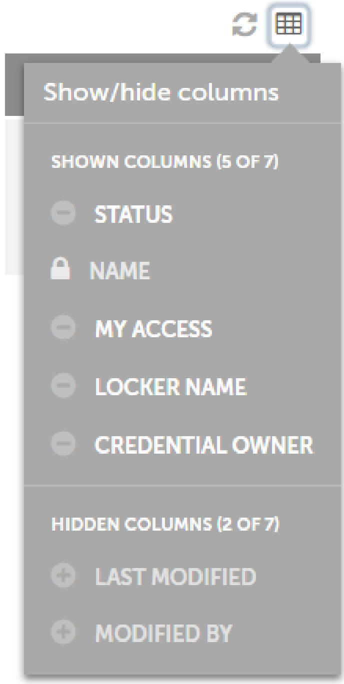
The following describes the list of items that can be viewed in the table:

Table Item	Description
Status	Shows the current status of your credential request.
Name	Name of the credential.
My access	Shows the current access status as credential owner or credential non-owner.
Locker Name	Name of locker assigned to the credential.
Credential Owner	Name of the credential owner.

Table Item	Description
View	Allows you to view credential requests. Learn more
Edit	Allows you to edit credential requests. Learn more

Alternatively, you can perform the following actions:

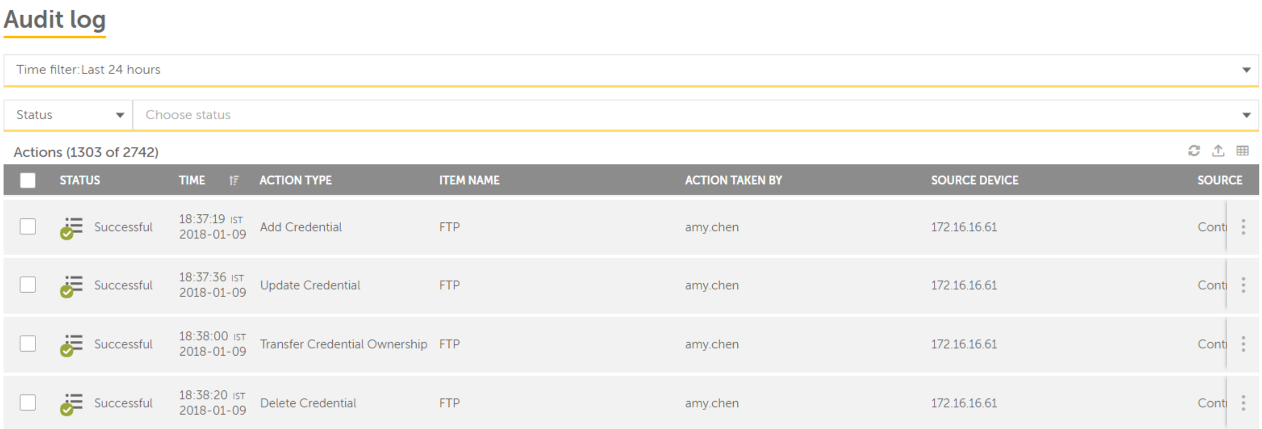
Table Item	Description
Refresh	Allows you to refresh the list of user- provided credential request.
Show/ hide columns	Allows you to show or hide specific columns. By default, all the columns are displayed.



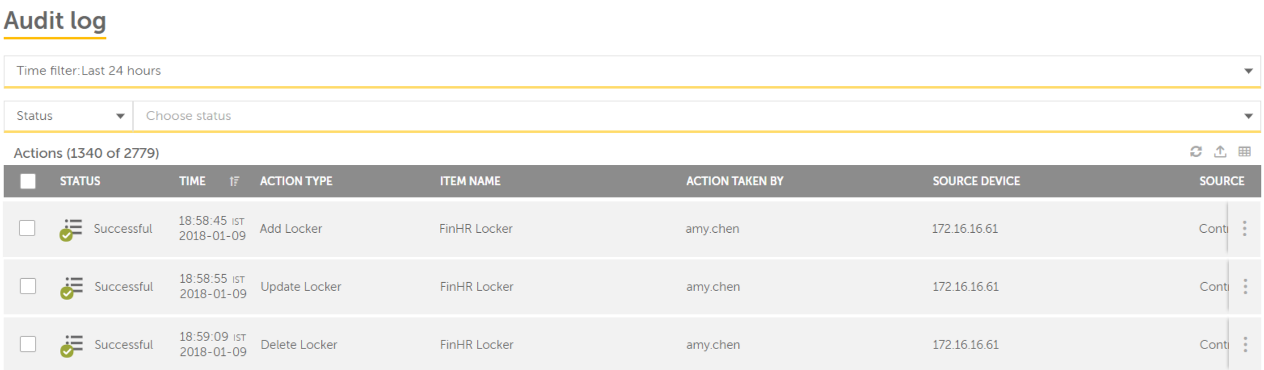
Tip: To **show/ hide** a column, click the column name.

Audit Logs

- **Credentials**: All the **Create, Update, Delete, Transfer Credential Ownership** actions are tracked in audit log for record keeping and future use. You can refer those entries in the Audit Log page:



- **Lockers**: All the **Create, Update, Delete** actions are tracked in audit log for record keeping and future use. You can refer those entries in the Audit Log page:



Create a credential

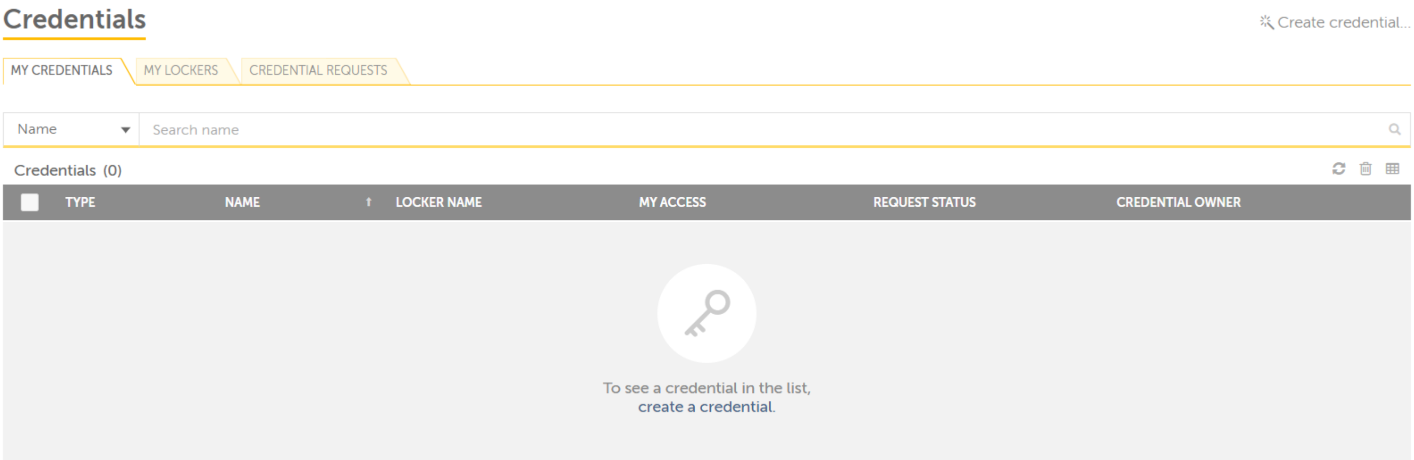
As an Automation Expert, Credential Vault provisions you to securely create and store your credentials. Therefore, it ensures that your credentials can be used in Bots without compromising security with safe deployment of tasks. Any authorized user can create credentials.

To create credential, follow the steps mentioned below:

1. Login to Control Room, click Bots → Credentials.
2. Click **Create credential** button 

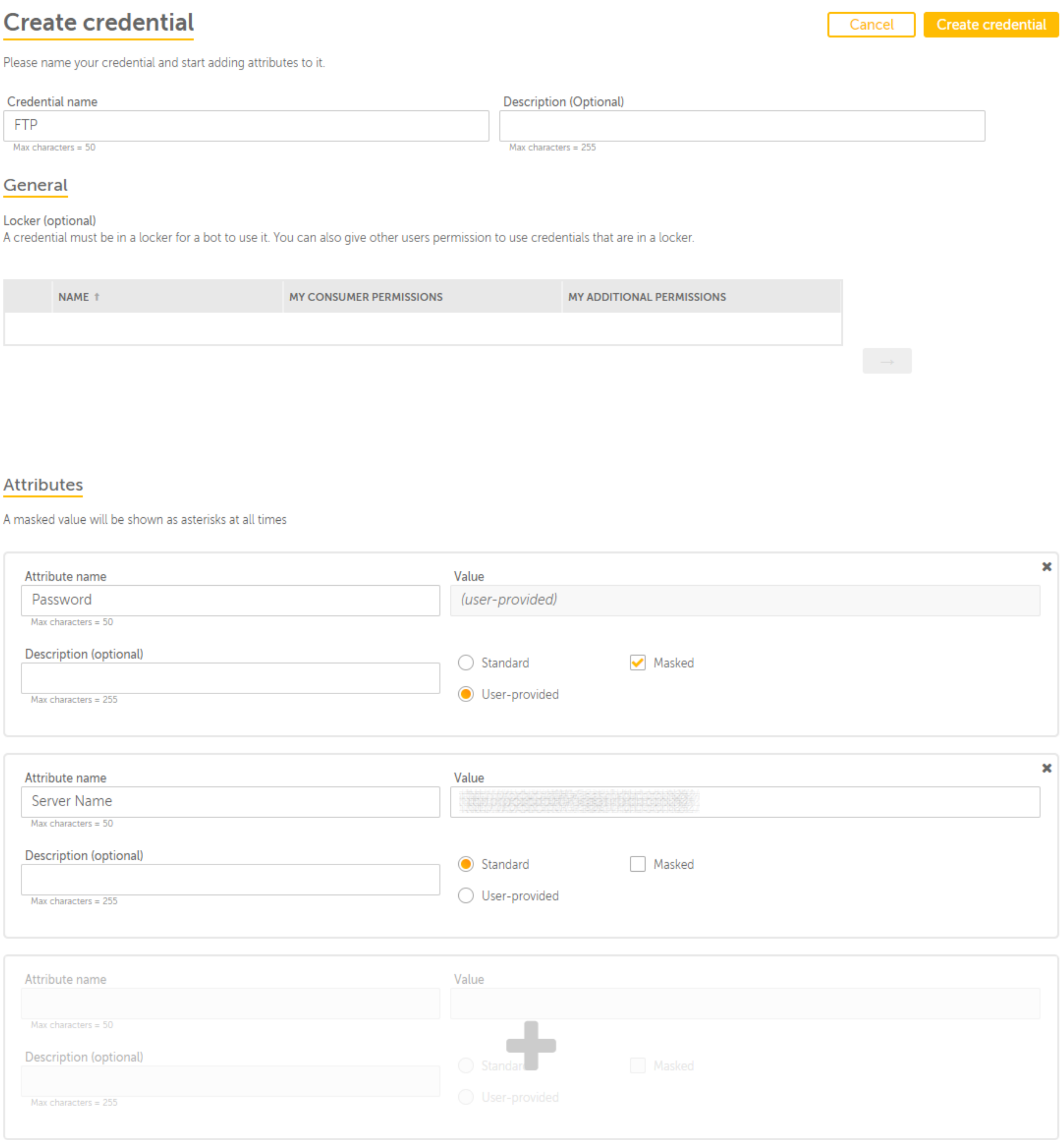
or click **create a credential** under the credentials tab.

> **Note:** The following option is displayed only when you are creating your first credential.



3. This opens the Create credentials page in which you can add attributes to your credentials. Provide Credential details such as Credential name and Description (optional) and Attribute details such as Attribute Name, Description (optional), Value (masked and

unmasked), and also you can check or clear whether you want your credential attributes to be **User-specific** or **Standard**.



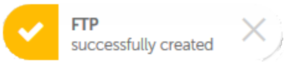
- **Standard**: In case of standard attribute, user must input the value.
- **User specific**: In case of user-specific attribute, the value field is greyed- out.

> **Note:** Only consumers of the locker containing this credential can provide the value

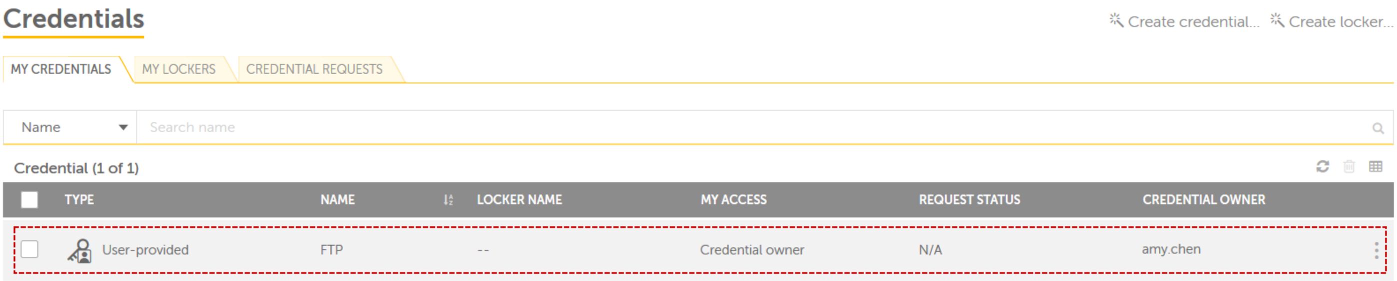
4. Click on Create credential.

Note: If you already have an existing locker, then you can assign your credential to the respective one while adding Credential details. If no locker has been created then you must create a locker and then assign your credential.

5. The following notification indicates that your credential has been successfully created:



6. Once your credential is successfully created, it is visible in the list of credentials tab.



Note: If email notification setting is enabled and credentials are added to a locker, then all the locker consumers shall receive an email. Learn more

Next...

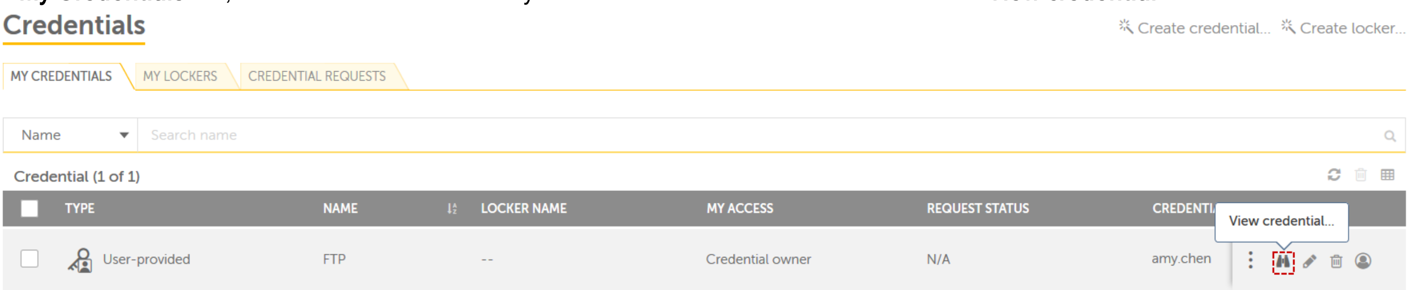
The next step is to add your credentials to a secure locker. Learn More

View a credential

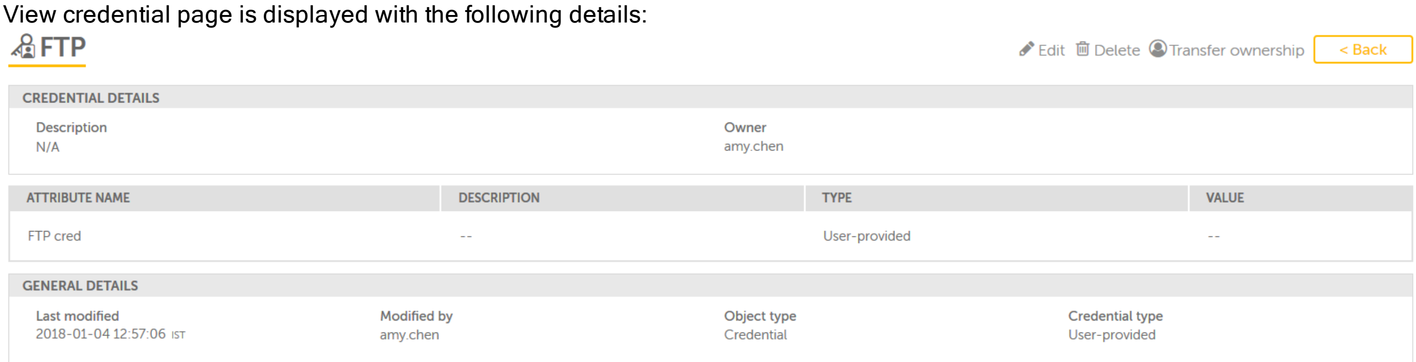
As an authorized user, this page allows user to view details of any credential. When you click the **View** icon for an individual credential. It provides information, such as the Credential details, Attribute name, Description, Credential Type and Value, and General details such as Last modified, Modified by, Object type, and Credential type.

To view a credential, follow the steps mentioned below:

1. Go to *Bots → Credentials.*
2. In **My Credentials** tab, choose the credential that you wish to view. Go to action list and click **View credential**.



3. View credential page is displayed with the following details:



- 

Edit credential- Allows you to modify the your credential.
- 

Delete credential- Allows you to delete your credential.
- **Credential details**- Description and credential owner.
- **Attribute name, credential description, type, value.**
- **General details**- last modified (date and time), modified by, object type, credential type.

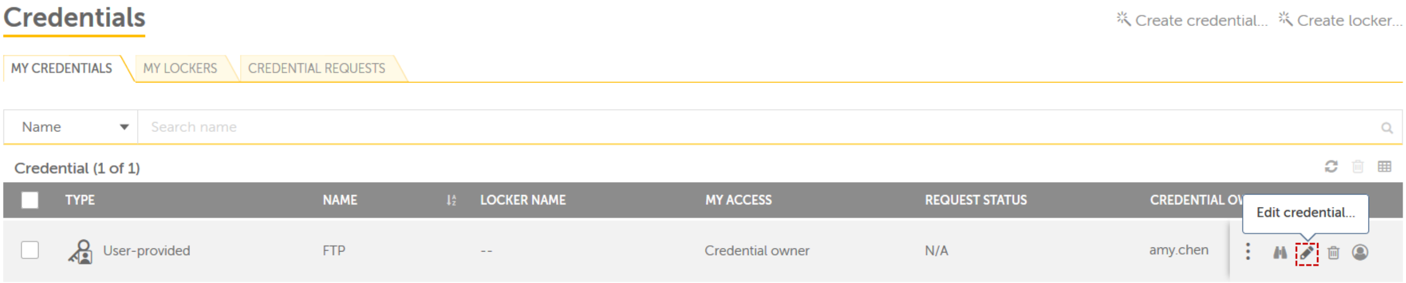
Edit a credential

As an Control Room user, edit credential allows you to edit details of any credential. This is useful in scenarios where you may want to make changes to your credential definition and value.

> **Note:** `If a credential type is user-provided, then locker consumers have permission to edit the credential and their credential value.`

1. Go to *Bots → Credentials*
2. Choose the credential that you wish to edit on the **actions list** click on **edit credential**.

   > **Note:** `If your credential is assigned to a locker, then you can only edit the value of common attribute. And if the attribute is user-specific then the locker consumers can edit the value.`

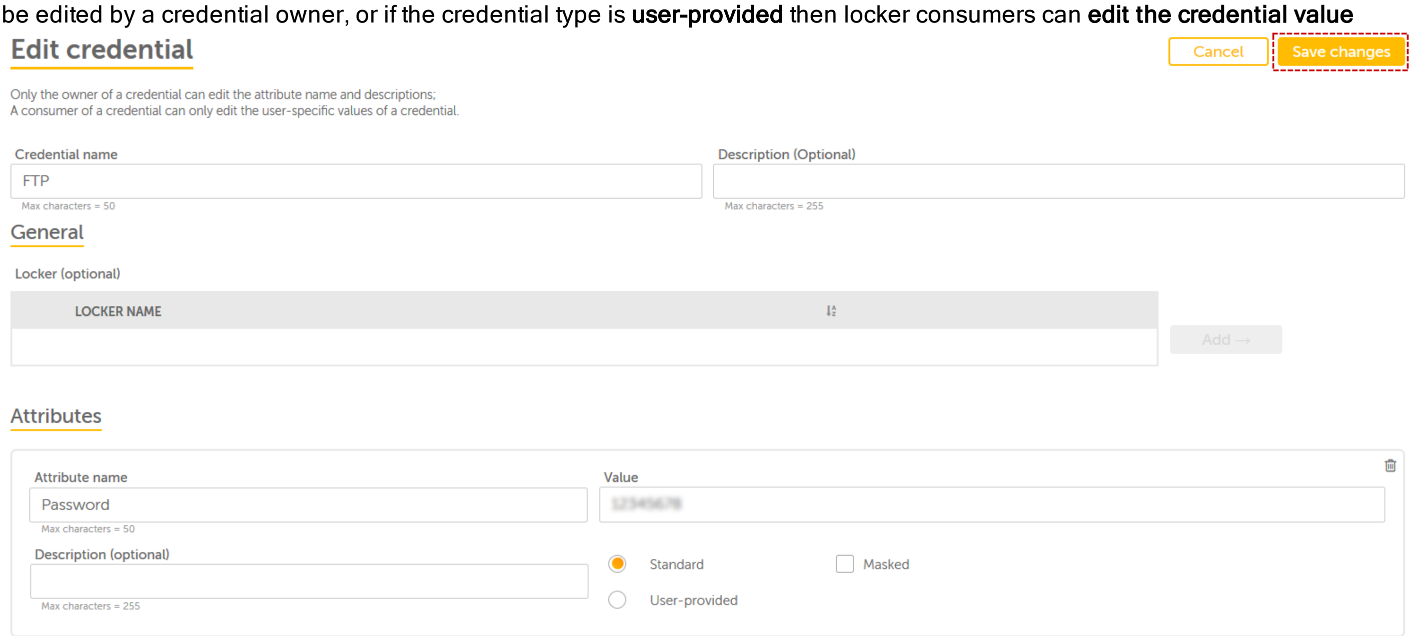
3. In the edit credentials page, make the required changes.

   > `If email notification setting is enabled and credentials are added to a locker, then all the locker consumers shall receive an email.` Learn more

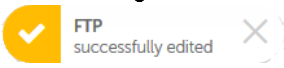
   - In case of **user-provided credential**, you can only edit **General** information such as adding or removing a locker.
   - In case of standard credential, you can edit **General** information such as adding or removing a locker and **Attribute** detail such as credential value

   > **Note:** `You can choose to` **`Close`** `or` **`Cancel`** `your updates.` **`Close`** `option is available when you do not make any updates. It changes to` **`Cancel`** `when you make any change to the page.`

4. Once you complete editing the credential, click on save changes or you may click on cancel to undo the changes. A credential can be edited by a credential owner, or if the credential type is **user-provided** then locker consumers can **edit the credential value**

5. The following notification indicates that your credential has been successfully edited.



Delete a credential

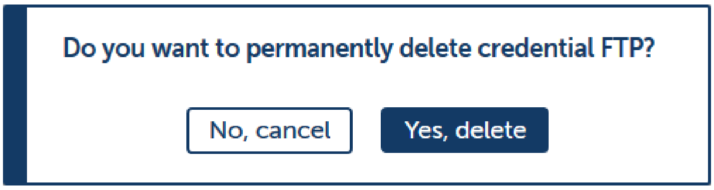
A credential owner can select the **delete** option to remove redundant credentials from the system.

To delete a credential, follow the steps mentioned below:

1. Go to Bots → Credentials
2. In **My credentials** tab, choose the credential that you wish to delete. Mouse over to actions list and click **delete** .

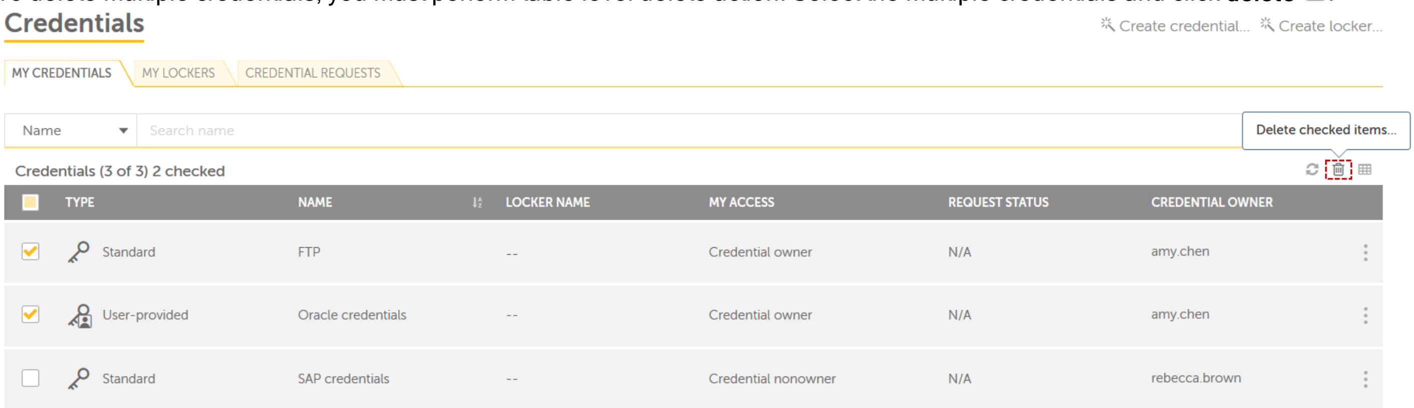
    Note: `If a locker is assigned to a credential, then it cannot be deleted.`

    The following message is displayed, click **Yes, delete** to delete your credential and **No, cancel** to cancel deletion:

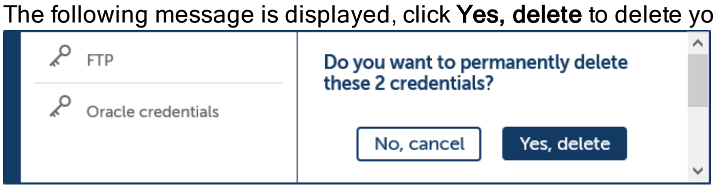
    

    Note: `If you are a credential non-owner, then you cannot delete a credential.`

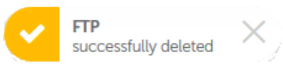
3. To delete multiple credentials, you must perform table level delete action. Select the multiple credentials and click **delete** .

    The following message is displayed, click **Yes, delete** to delete your credential and **No, cancel** to cancel deletion:

4. Once the credentials is deleted, the following notification is displayed:

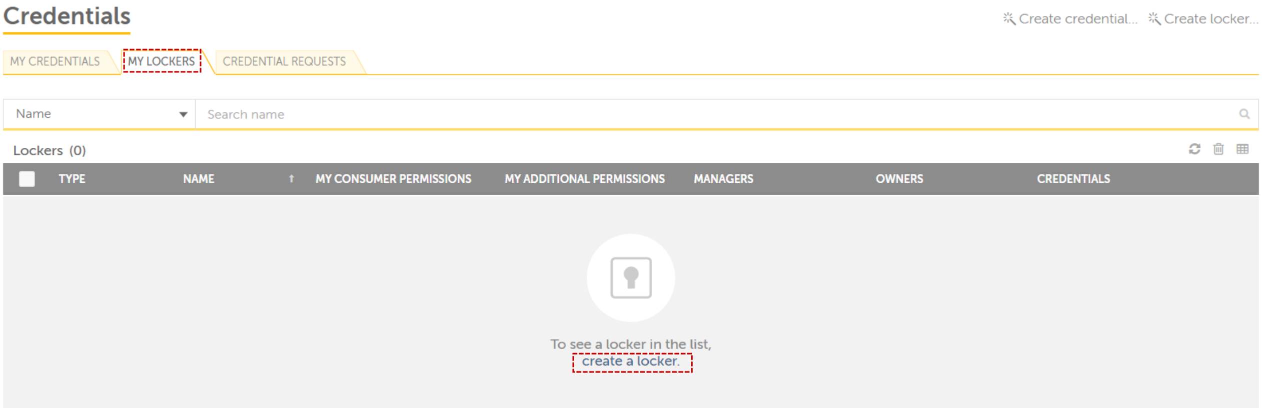
    

Create a locker

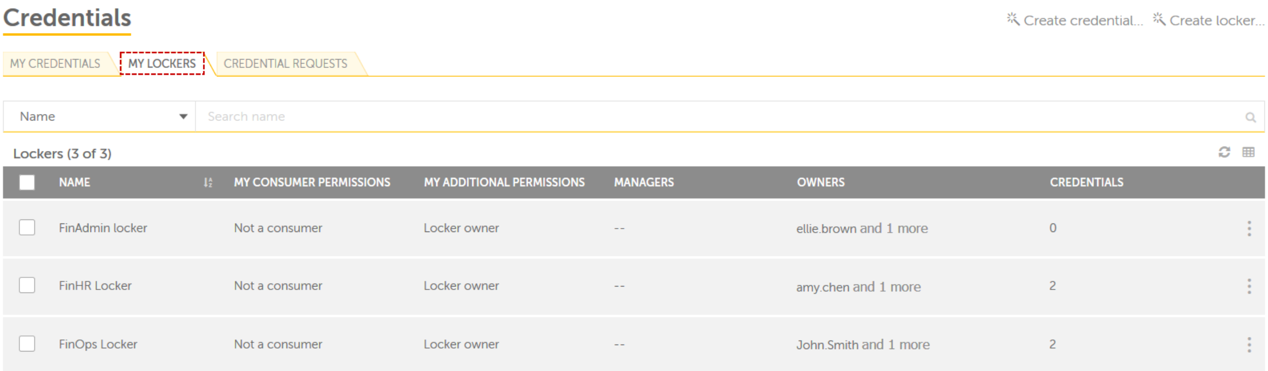
A user with locker admin or manage my locker permission is authorized to create a locker. A locker can be used to group similar credentials and share it with other users.

To create a locker, follow the steps mentioned below:

1. Go to Bots → Credentials
2. In **My Lockers** tab, click **Create locker**. If you are creating locker for the **first time**, then the following screen is displayed:

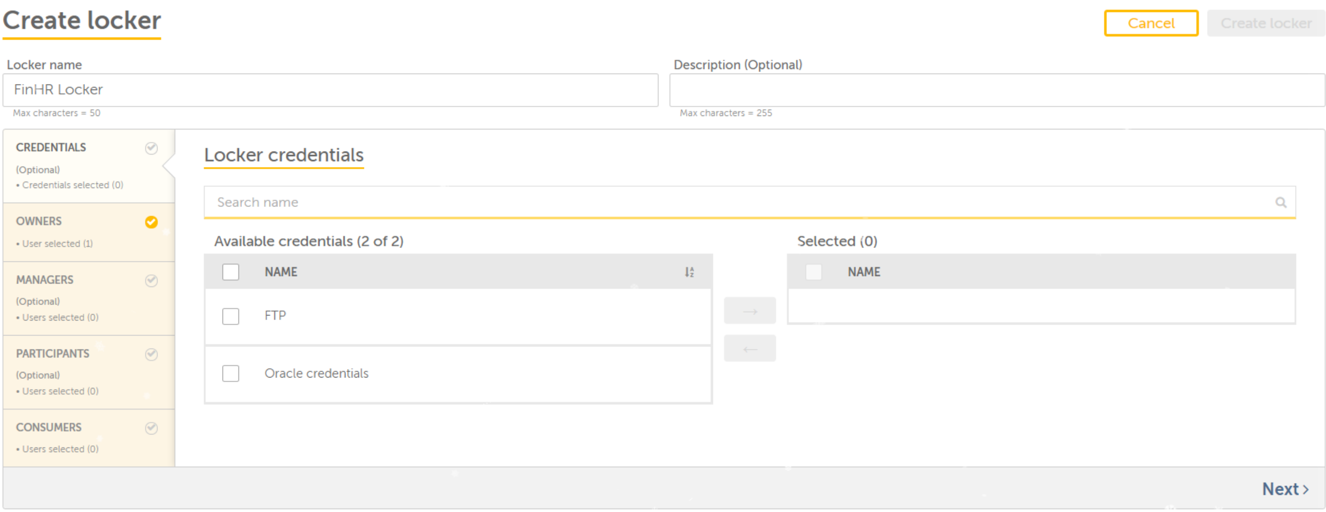


If lockers already exist, then the following screen is displayed:

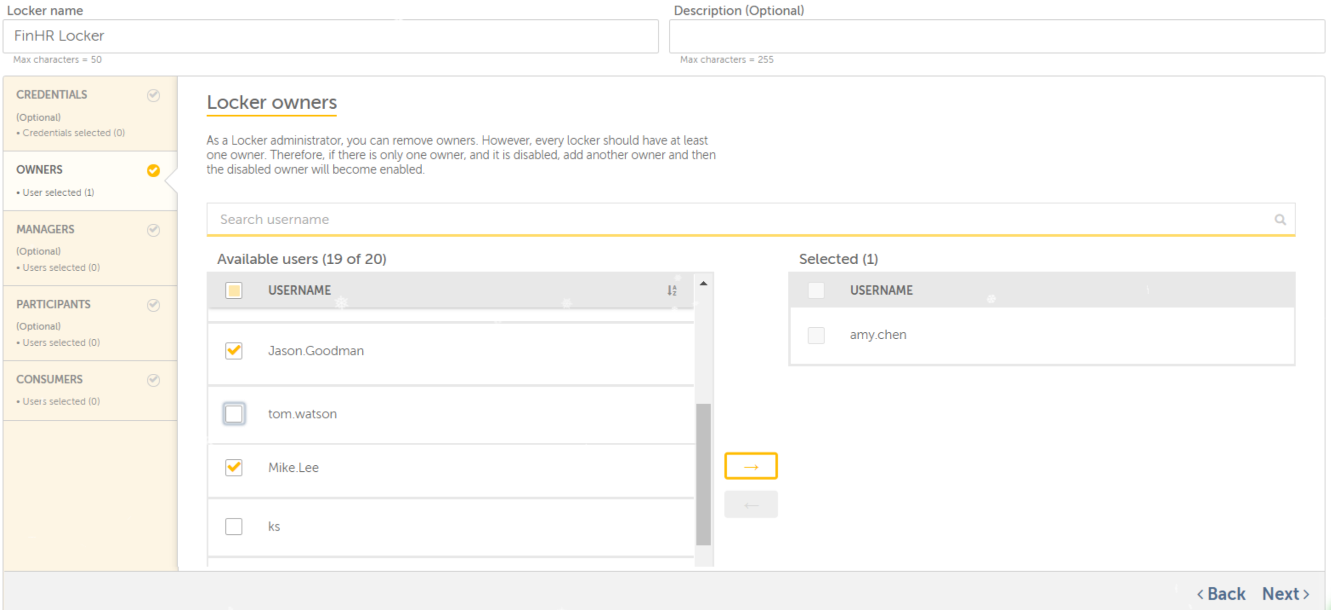


3. The create locker page is displayed. You can add locker details such as:
   - Name and Description
   - Add credentials, owners, managers, participants, consumers.
   - **Credentials**: Shows the available credentials owned by the user. You can select one or multiple credentials from the list and add it to the locker.

> **Note:** If email notification setting is enabled and credentials are added to a locker, then all the locker consumers shall receive an email. Learn more

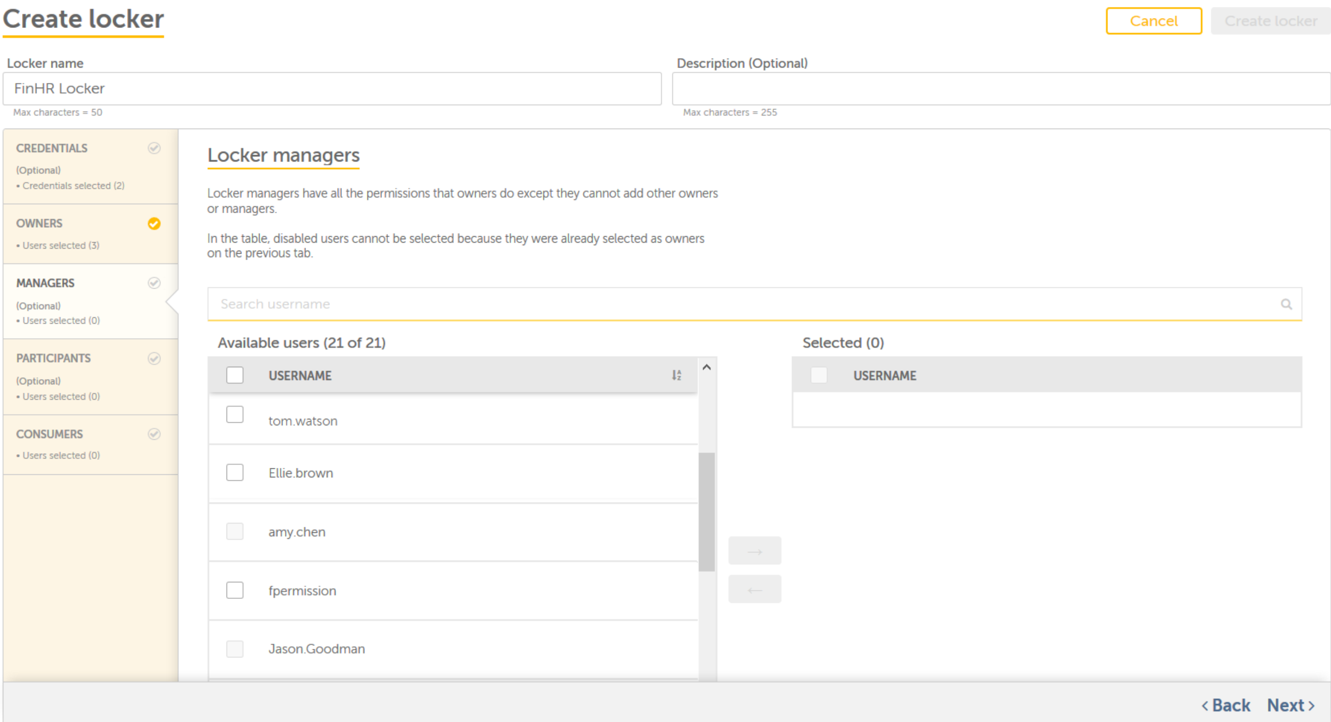


- **Owners**: A locker owner can edit, view, delete a locker and can add or remove other owners. Also, an owner can be a locker consumer but **cannot be a manager or participant** within the same locker.



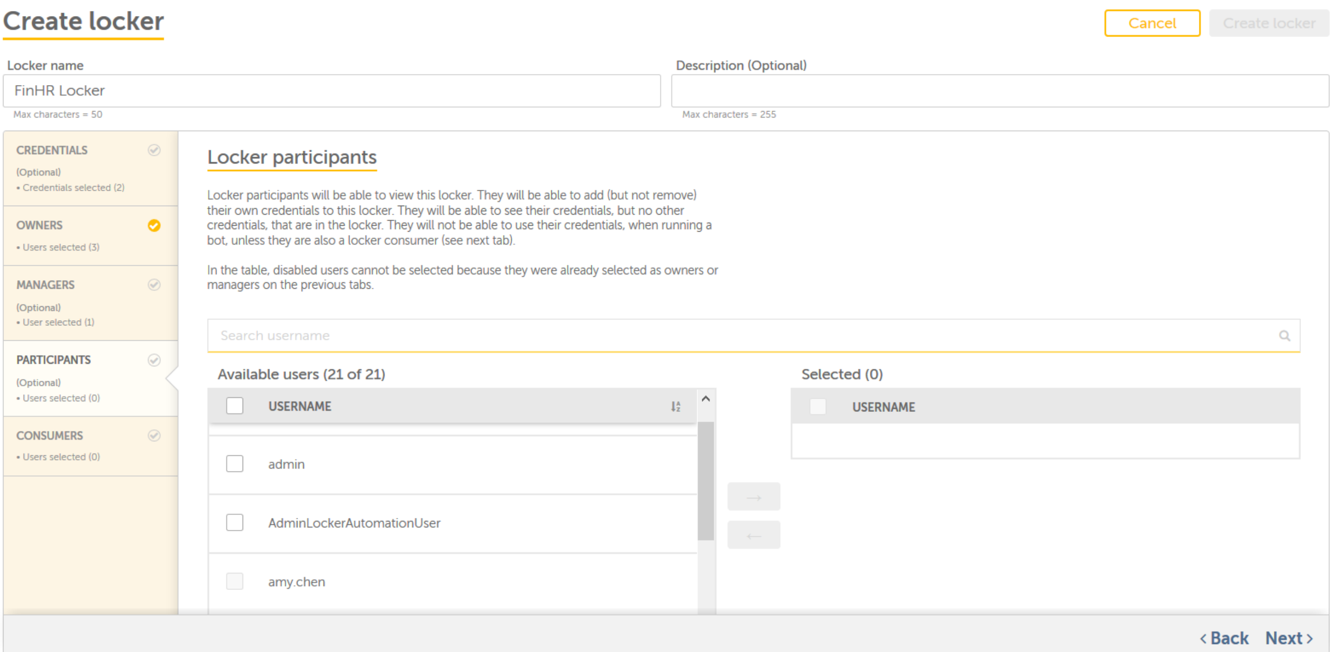
- **Managers**: A locker manager has access to all the functionality like a locker owner, but they do not have permission to add owners, managers, or participants to the locker.

Note: Disabled users cannot be selected as locker managers if they were already selected as owners in the previous tab.



- **Participants**: A locker participant has access to view a locker and participants can also add their own credentials to a locker.

> **Note:** A **locker participant** does not have access or visibility of credentials created by other users.



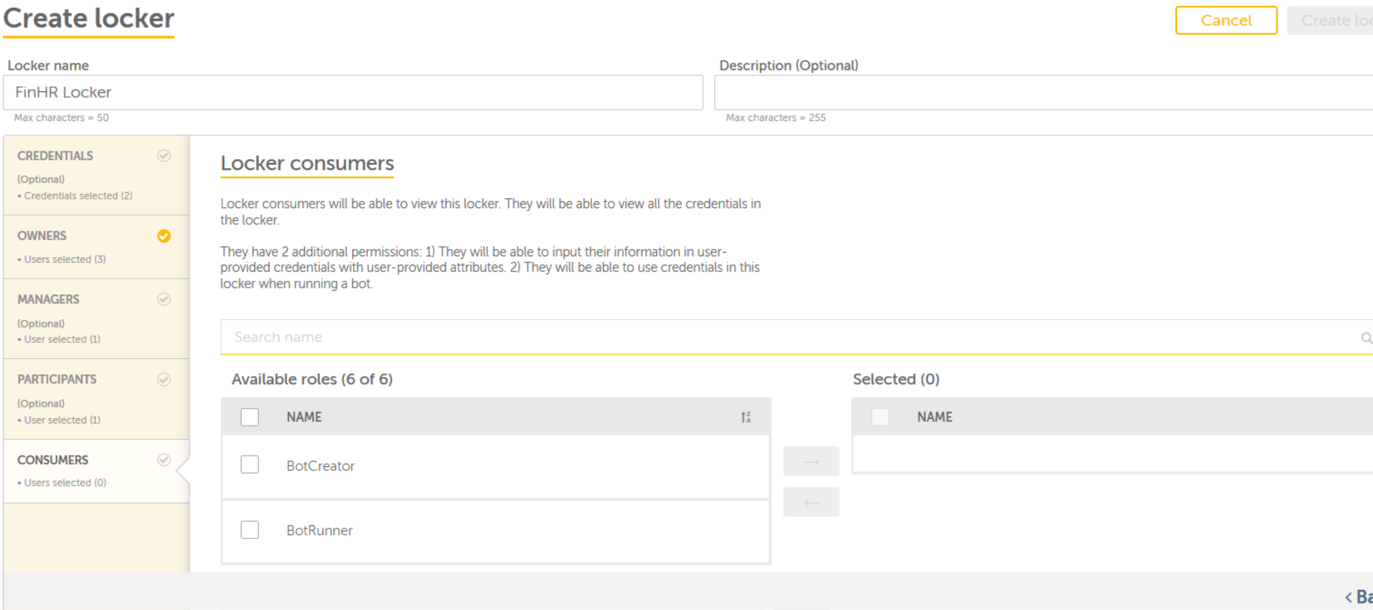
- **Consumers**: You must select one or more roles. The users belonging to these selected roles are the consumers of the lockers. These users have access to view a locker and input credential value.

  If the credential type is:

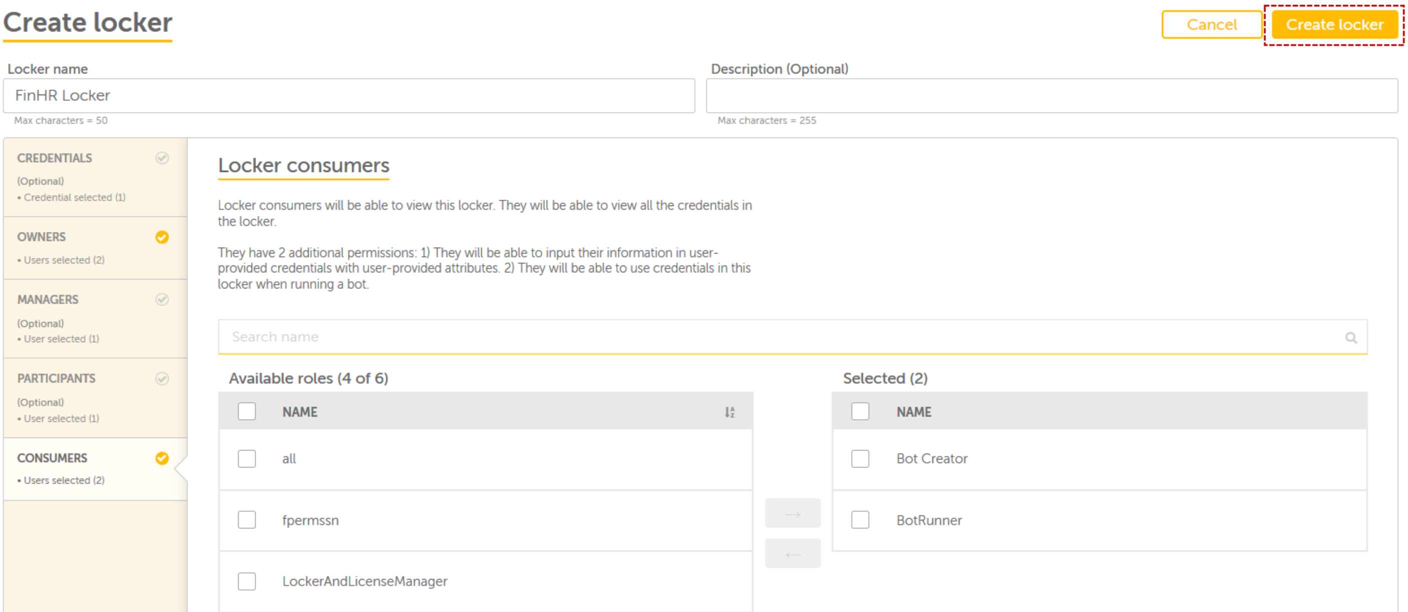
  Standard: Locker consumers can view the locker and all the credentials inside the locker. They are able to utilize credentials in the locker when running a bot. All consumers are able to see the same value of the credential that is set by the owner of the credential.

  User-provided: Consist of same usability as Standard credential; locker consumers are able to input their information in user-provided credentials with user-provided attributes (i.e. credential value).

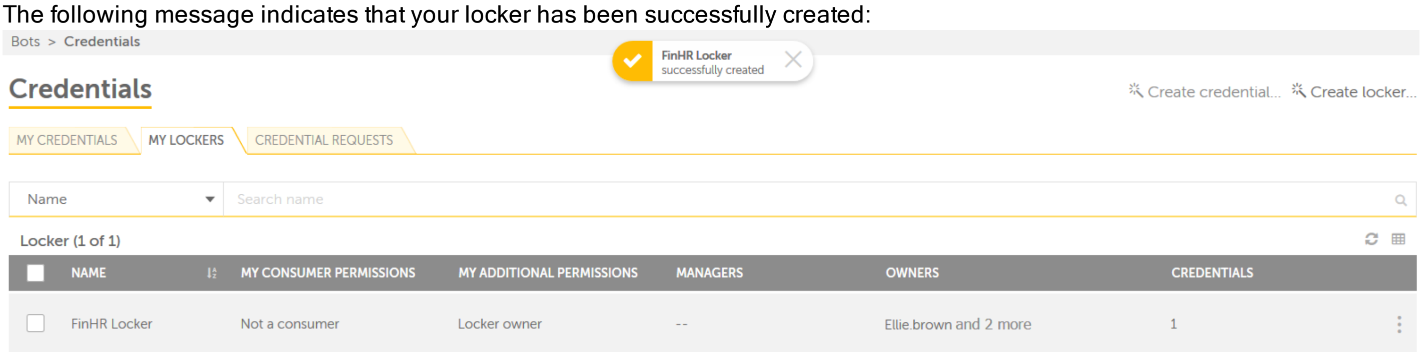
Note: System-created roles are not displayed in the consumer list.



4. Click on **Create locker.**



5. The following message indicates that your locker has been successfully created:



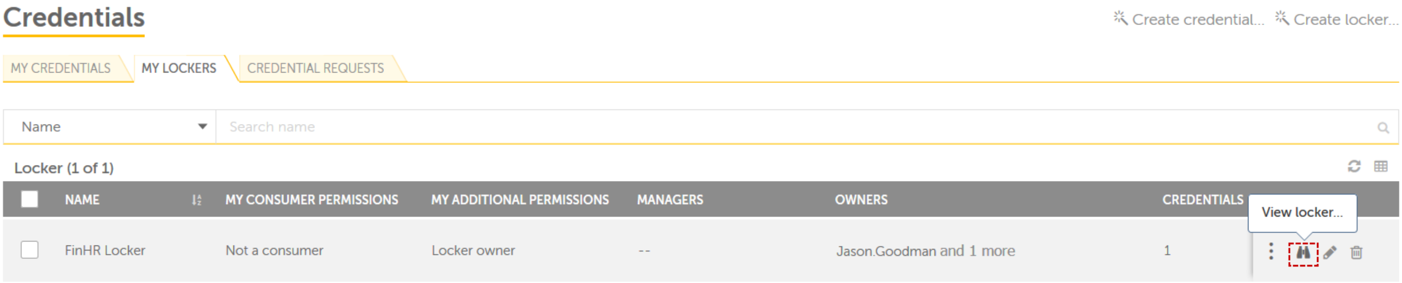
Note: In case of email notification setting enabled, all the locker consumers will receive an email to edit the credential value if credential type is user-provided. Learn more

View a locker

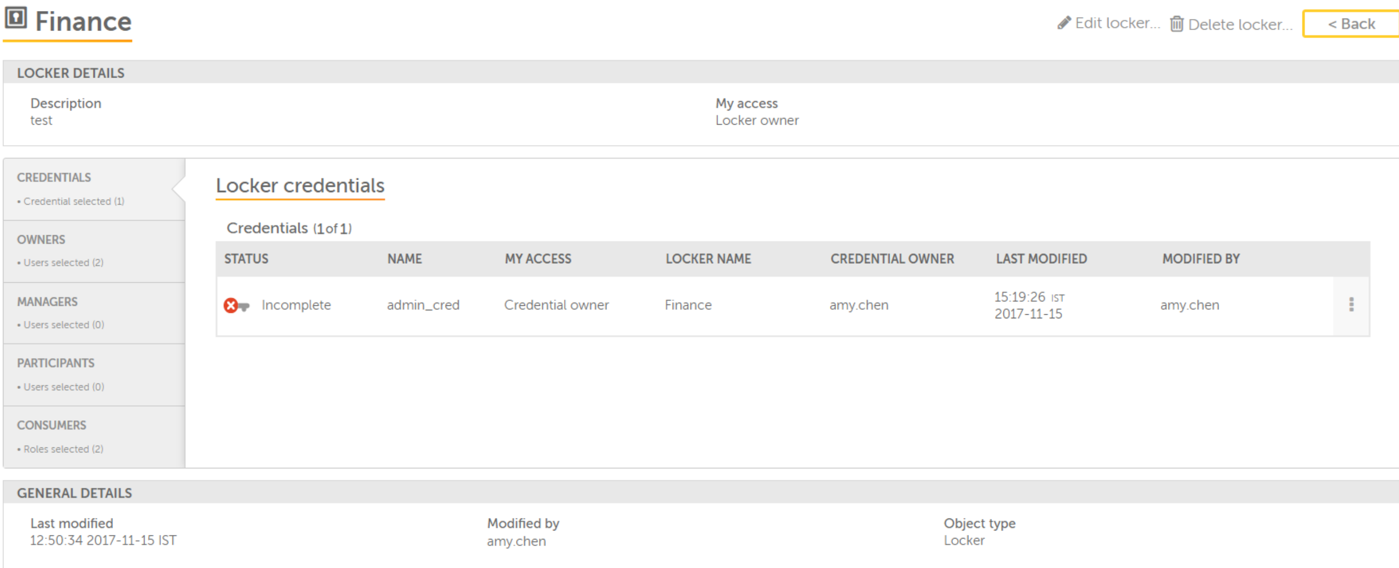
Any user with "Manage my locker" permission can view their own lockers. This provides information such as credentials assigned to the locker, locker owners, locker managers, locker consumers, and locker participants.

To view a locker, follow the steps mentioned below:

1. Go to Bots → Credentials
2. In **My Lockers** tab, choose the locker that you wish to view. Go to action list and click **View locker**.



3. View locker page displays the following details:



- 

Edit locker- Allows you to modify your locker. Learn more
- 

Delete locker- Allows you to delete your locker.
- **Credentials**- Shows list of credentials added to the locker.
- **Owners**- Shows list of locker owners.
- **Managers**- Shows list of locker managers.
- **Participants**- Shows the list of locker participants. **Locker participants** are able to view this locker. They can add their own credentials to a locker. They will be able to see their credentials, but no other credentials, that are in the locker.
- **Consumers**- Shows the list of locker consumers. **Locker consumers** are able to view this locker and all the credentials inside the locker. A locker consumer with user-provided credential type have two additional permissions:
 1) They will be able to input their information in user-provided credentials with user-provided attributes. 2) They will be able to use credentials in this locker when running a bot.

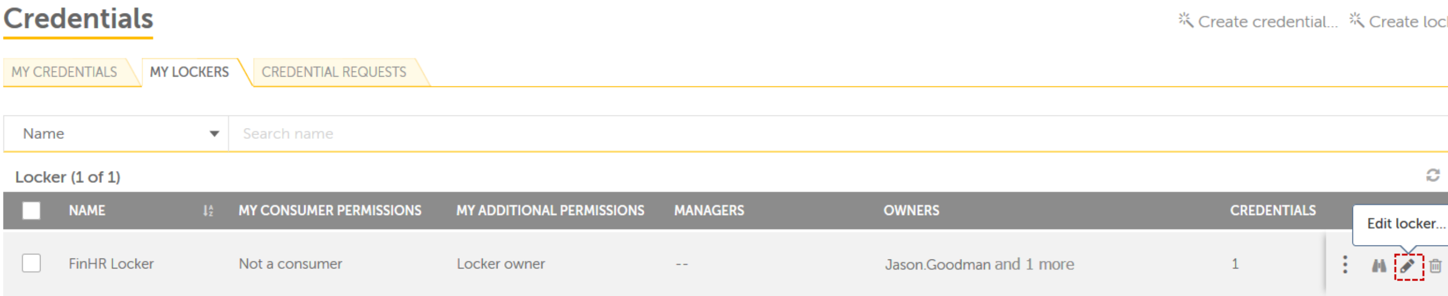
Edit a locker

Control Room users with Locker Admin permission or any user having edit permission can edit their own lockers and access this feature.

To edit a locker, follow the steps mentioned below:

1. Go to Bots → Credentials.
2. In **My Lockers** tab, choose the locker that you wish to edit. Then on the action list, click **edit locker**.

   Note: Only a locker owner or locker admin has permission to edit a locker.

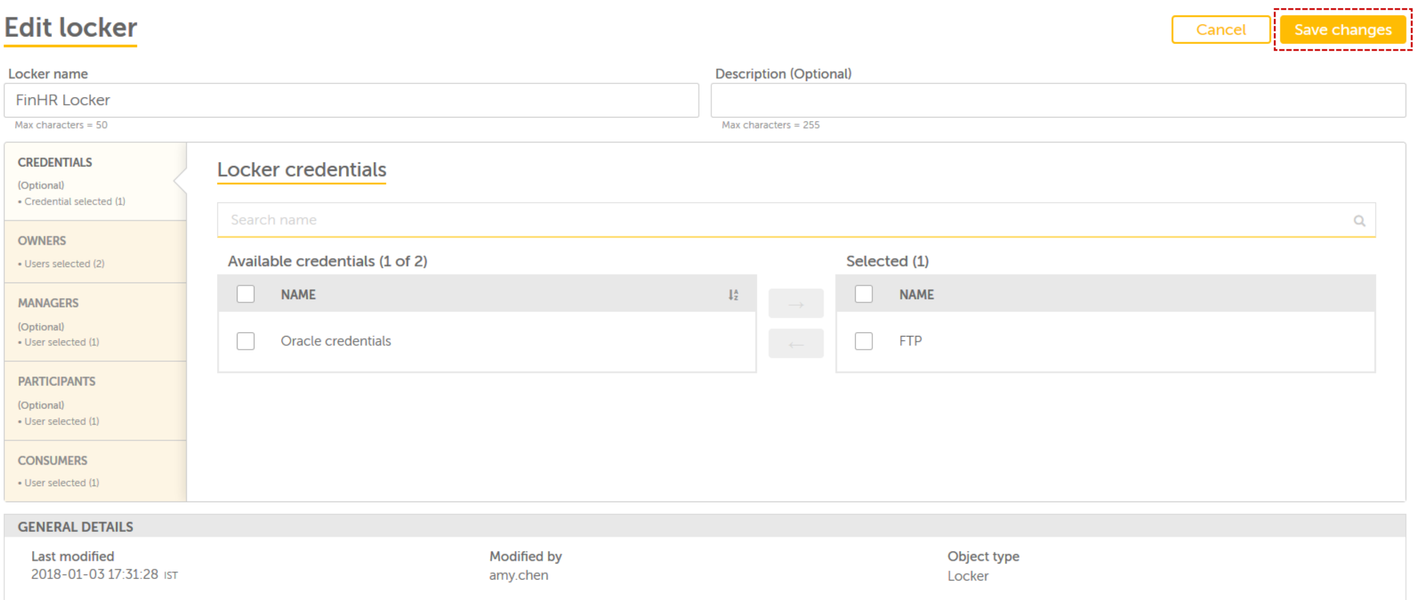


3. You can make changes to the following:

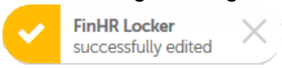
   If email notification setting is enabled and credentials are added to a locker, then all the locker consumers shall receive an email. Learn more

   - **Credentials**- Add or remove credentials that are assigned to a locker.
   - **Owners**- Add or remove locker owners.
   - **Managers**- Add or remove locker managers.
   - **Participants**- Add or remove locker participants.
   - **Consumers**- Add or remove locker consumers.
4. Once you finish editing the locker. Click **Save changes**.

   Note: You can choose to **Close** or **Cancel** your updates. **Close** option is available when you do not make any updates. It changes to **Cancel** when you make any change to the page.



5. The following message indicates that your locker has been **successfully edited**:

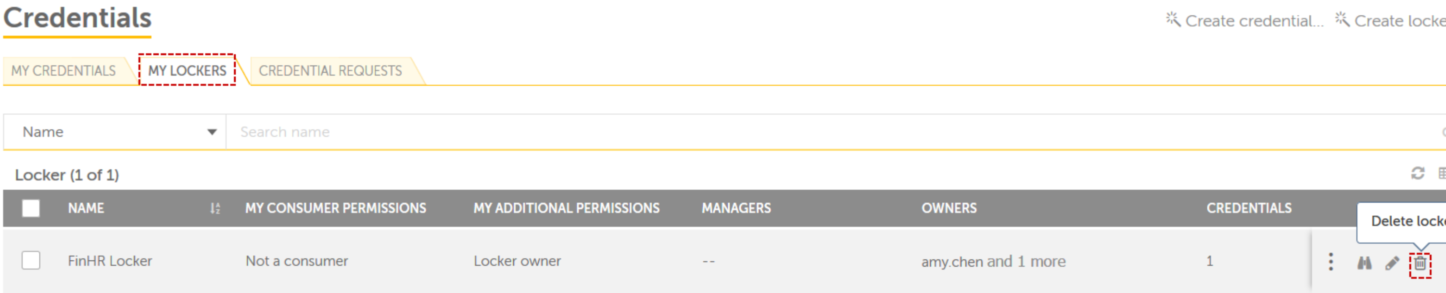


Delete a locker

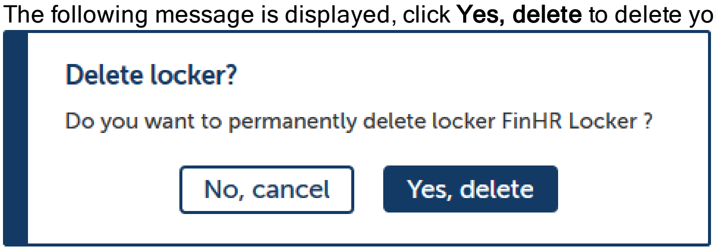
To eliminate redundant lockers from the system, a locker owner can perform the delete action.

To delete a locker, follow the steps mentioned below:

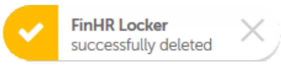
1. Go to Bots →Credentials
2. In My Lockers tab, choose the locker that you wish to delete. Mouse over to actions list and click delete .



3. The following message is displayed, click **Yes, delete** to delete your locker and **No, cancel** to cancel deletion:



4. Once the locker is successfully deleted, the following notification is displayed:



Credential requests

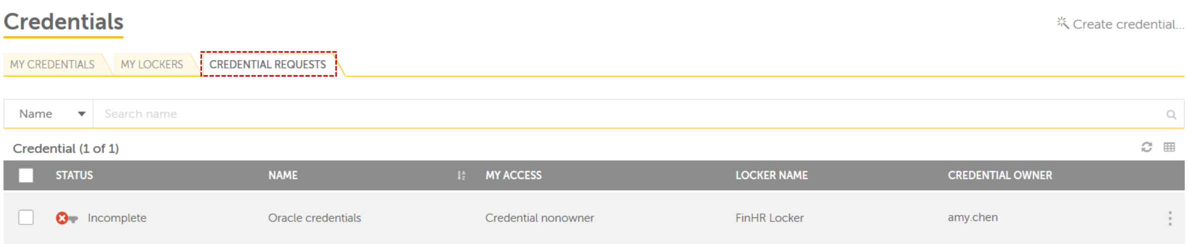
This page allows a Control Room user to send credential requests to locker consumers i.e. when a user-provided credential is added to a locker, all the consumers of the locker receive a credential request in their name to fill in their credential values.

Example: Amy.chen is a user with **manage my locker** permission. Amy.chen creates a credential with credential type as **user-provided** and assigns it to a locker. Therefore, a credential request is sent to all the locker consumers. All the locker consumers will receive a request to complete the credential status by adding the credential value.

To generate credential request, follow the steps mentioned below:

1. Go to Bots → Credentials
2. Create a credential (Learn more) with credential type as **user-provided**.
3. Assign your credential to a locker.
4. All the present locker consumers will receive a credential request. You can see that the following user receives a **credential request:**

   > Note: If locker consumers provide the credential value then the status of this credential is set to complete. However, the overall status of the credential remains incomplete until all consumers add their credential values.

5. Once all the consumers input the credential value, the status of the credential changes to complete.

   > **Note:** If email notification setting is enabled and credentials are added to a locker, then all the locker consumers shall receive an email to input the credential value. Learn more

Next...

After completing the credential request you can use these credentials in automation tasks. Refer the topic **Assigning Credential Variables** in Client User Guide 11.0 to use credentials within a task.

Credential Vault Email-Notifications

In Control Room, if Email notification setting is enabled it ensures that users are notified via email if any important changes regarding credentials and lockers are made.

Email notifications are sent via email for the below mentioned scenarios:

1. When credential is added to a locker. Learn more
2. When a member is added to or removed from the locker. Learn more
3. When there is change in permissions for locker members. Learn more
4. When a consumer gets added or removed from a role assigned to locker, and consumer roles get added to or removed from the locker. Learn more

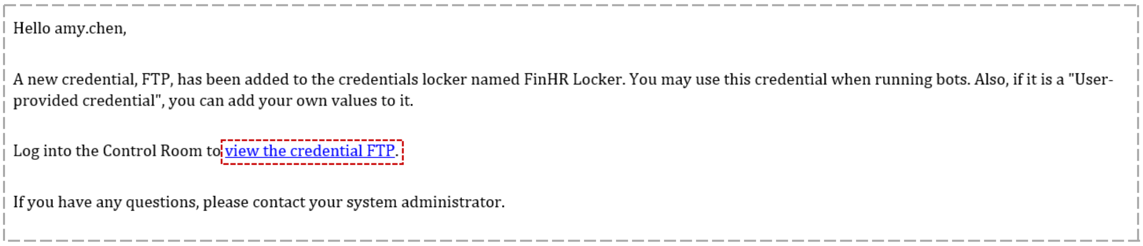
Detailed information on Credential Vault-email notifications

- **Credential is added to a locker**

  When a new credential is added to a locker an email notification is sent to all consumers of the locker at their registered email address in Control Room. The email consists of a link to the Credential that is added to the locker. The consumers are redirected to Edit credential page wherein they must input the credential value.

  For example: Credential FTP is added to a locker Fin HR Locker. All the locker consumers will receive an email notification to add the credential value. The below screen-shot illustrates that consumer amy.chen has received an email with a link to Edit Credential page:

  Click on **view the credential FTP** link. This navigates user "amy.chen" to Edit Credential page.



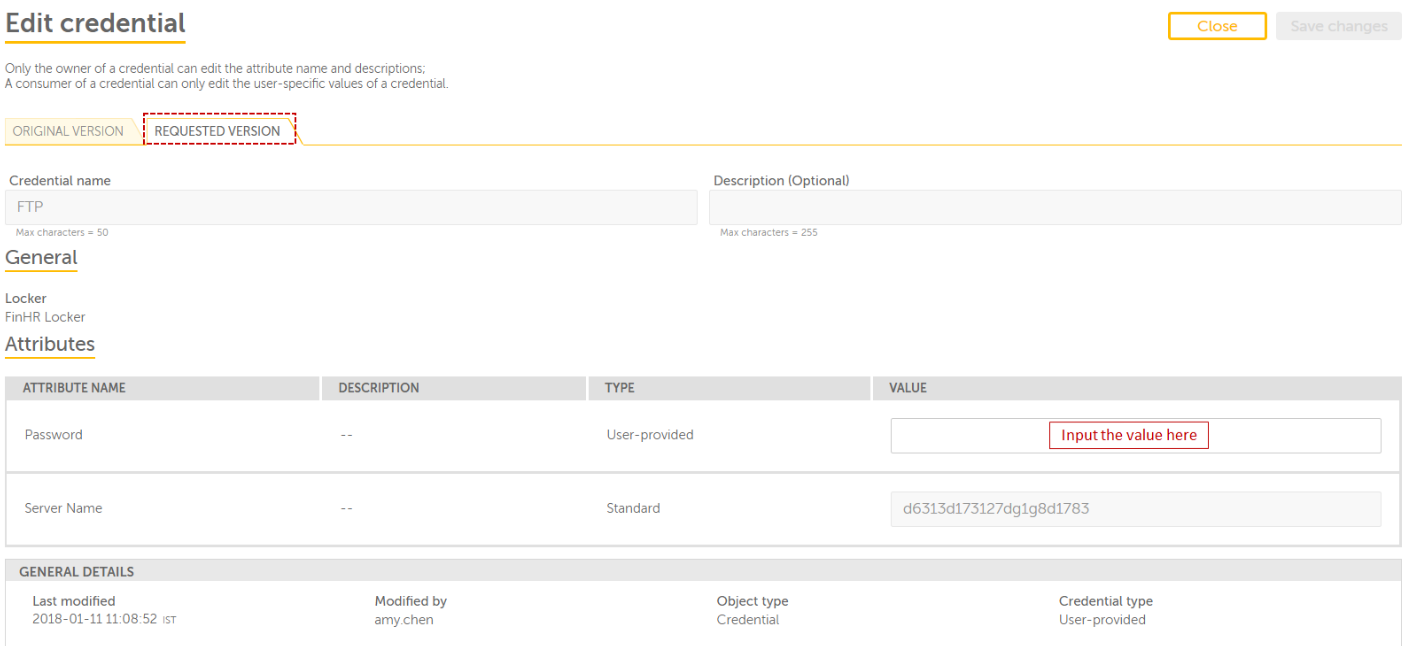
Hello amy.chen,

A new credential, FTP, has been added to the credentials locker named FinHR Locker. You may use this credential when running bots. Also, if it is a "User-provided credential", you can add your own values to it.

Log into the Control Room to view the credential FTP.

If you have any questions, please contact your system administrator.

In Edit Credential page, user must click on **Requested version**and input the value. And click on **Save changes**.



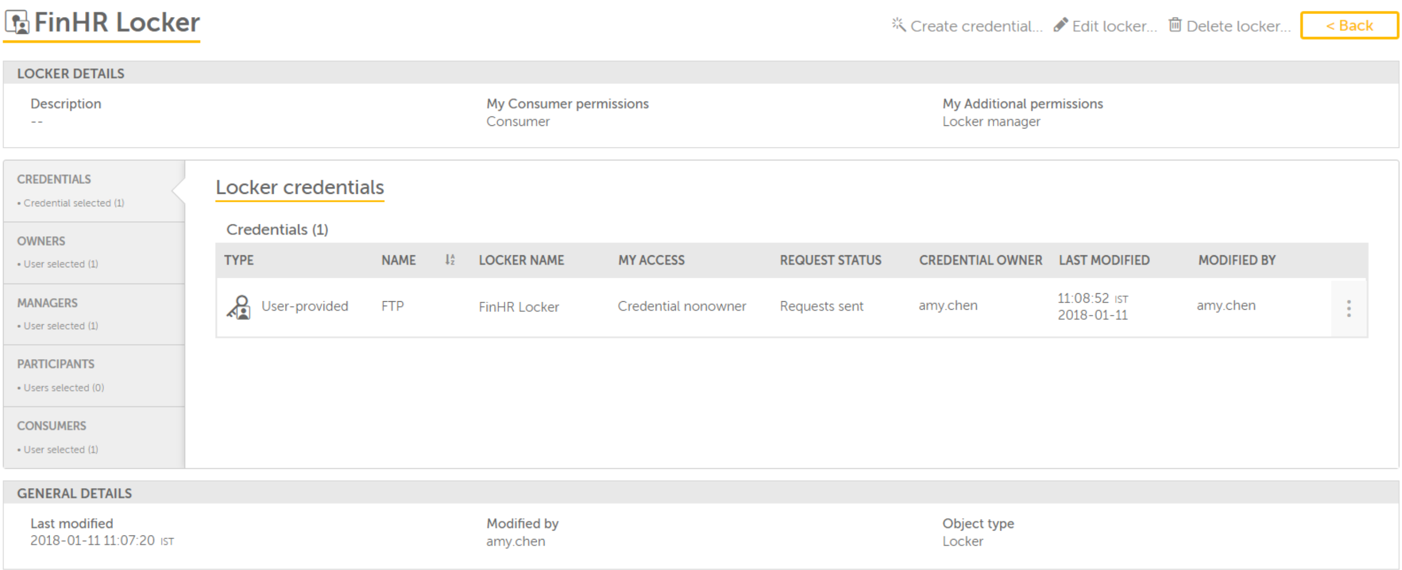
- **Member is added or removed from a locker**

  An email notification is sent when a new member (co-owner or participant) is added to a locker. The email consists link to the Locker of which they are added as member.

  For example: User Ellie.brown is added as a locker participant for FinHR Locker. The following email is sent to the user wherein user must link on the link:

  > Hello ellie.brown,
  >
  > You have been added to a credentials locker. Go to the Control Room now to view the locker FinHR Locker.
  >
  > If you have any questions, please contact your system administrator.

  The link redirects user to View locker- FinHR Locker page as illustrated in the following screenshot:



  The following email is sent to the user when user is removed from the locker as a member of participant:

  > Hello ellie.brown,
  >
  > You have been removed from a credentials locker named FinHR Locker. If you have any questions, please contact your system administrator.

- **Change in permission for locker members**

  When a locker owner/ admin, grants or removes locker membership permissions from a locker, an email notification is sent to the locker members at their email address. This ensures that members are notified of their membership changes within the locker.

- **Locker consumer gets added or removed from a role assigned to a locker, and consumer role gets added or removed from a locker**

  When a role assigned to a locker is modified by addition or removal of users, an email notification is sent to the new or existing user at their email address so that the consumers are notified that credentials are pending for their input in the locker.

  Also when a new role added to a locker or an existing role is revoked from the locker, an email notification is sent to the new or existing consumers at their email address so that the consumers are made aware of the changes.

  For Example: User amy.chen is assigned consumer role "Creator" in FinHR Locker. The role has been **revoked** from the locker, the user receives the following email:

  > Hello amy.chen,
  >
  > Your "Consumer" permissions to the credentials locker named FinHR Locker have been revoked. If you have any questions, please contact your system administrator.

If the role is assigned to the locker, then locker consumer amy.chen receives the following email:

> Hello amy.chen,
>
> You have been given "Consumer" permissions to the credentials locker named FinHR Locker. These permissions allow you to use the credentials inside the locker when running bots. Also, you can provide your own values in any user-provided credentials inside the locker.
>
> Log into the Control Room to [view the locker FinHR Locker](#).
>
> If you have any questions, please contact your system administrator.

S

My bots - Overview

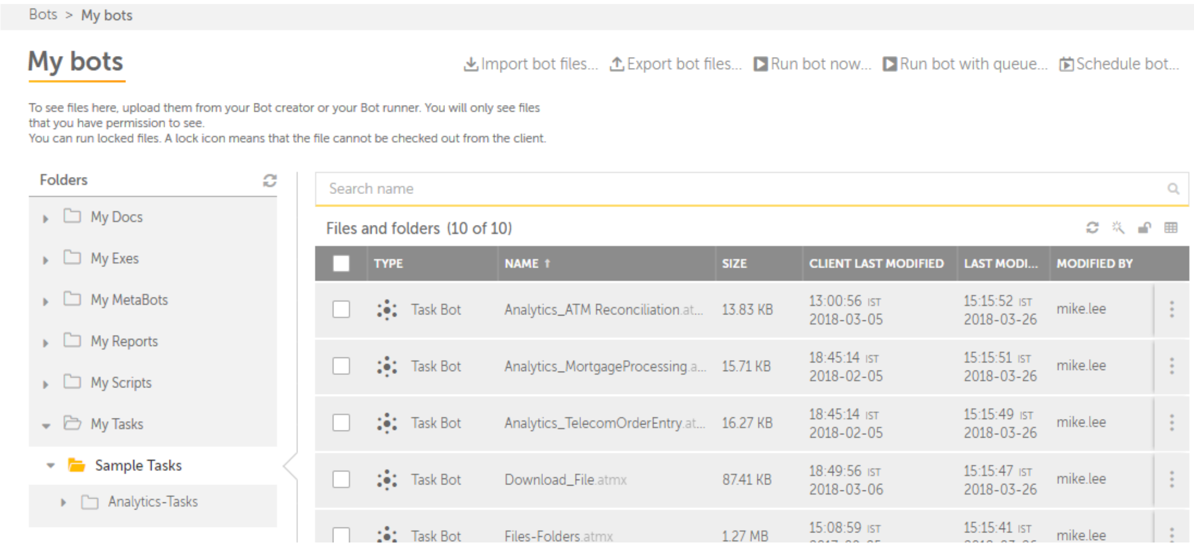
As a Bot Creator, when you upload files from Automation Anywhere Enterprise Client, the files are displayed on the **My bots** page. This page is divided into the following areas.

- Folders
- Files and folders

Note: As a Control Room user, you must have the right privileges to access this page. Folders for which you do not have access to will not be visible to you.

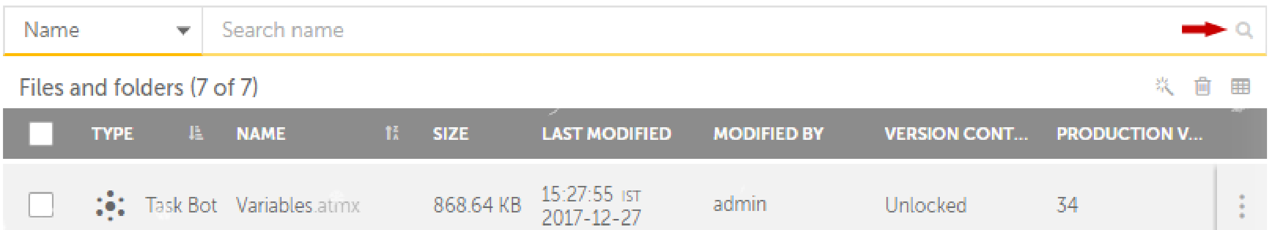
The **My bots** page also allows you to perform tasks, such as exploring your documents, executable files, metabots, reports, scripts, tasks, and workflows from the Folders area. It also allows you to:

- Import bot files
- Export bot files
- Run a Bot
- Schedule a bot
- Run bot with queue



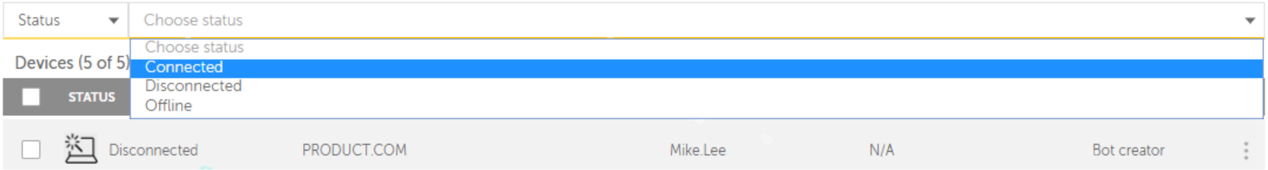
For ease of access, you can apply search parameters to Type, Name and Version Control columns.

- You can specify the search parameters in the search bar for Name:



Note: When you specify search parameters for the same column, the system searches using **OR** operator. When you specify search parameters for different columns, the system searches using **AND** operator.

- You can choose the search parameters from a list in the search bar for Type and Version Control:



My bots - Overview

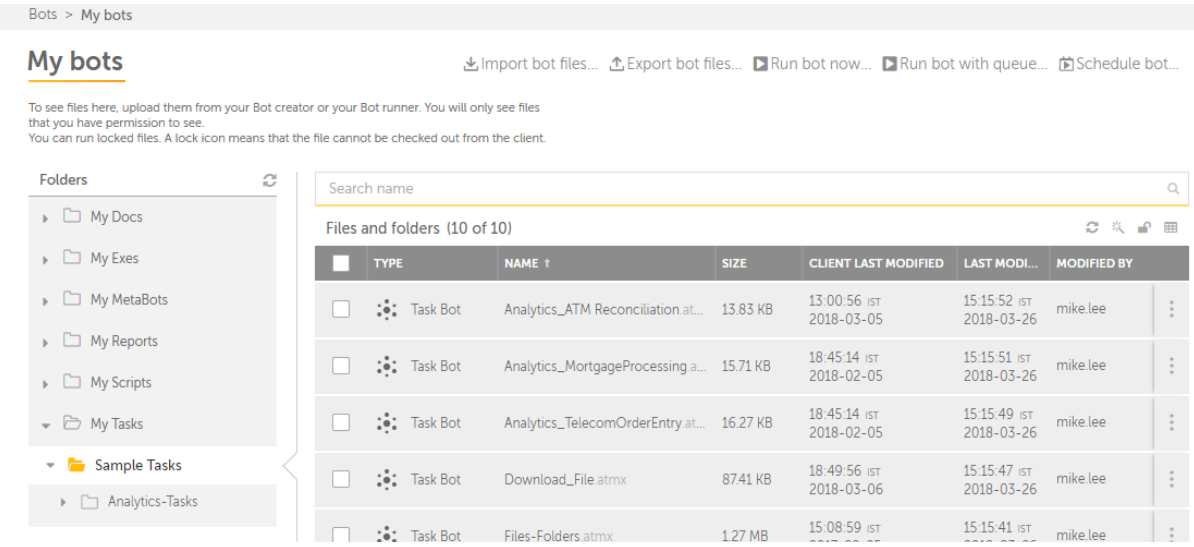
As a Bot Creator, when you upload files from Automation Anywhere Enterprise Client, the files are displayed on the **My bots** page. This page is divided into the following areas.

- Folders
- Files and folders

Note: As a Control Room user, you must have the right privileges to access this page. Folders for which you do not have access to will not be visible to you.

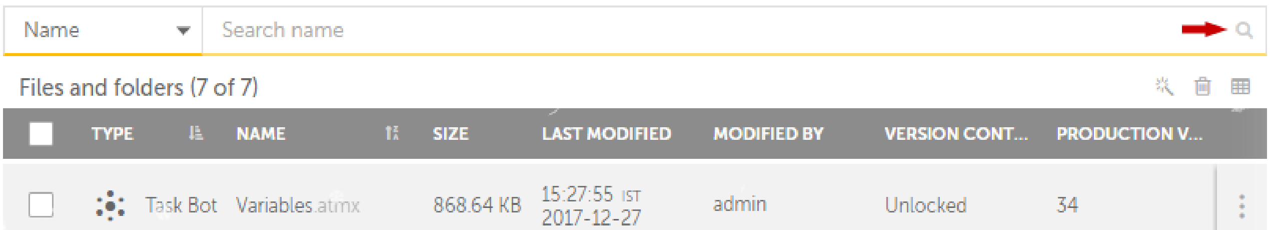
The **My bots** page also allows you to perform tasks, such as exploring your documents, executable files, metabots, reports, scripts, tasks, and workflows from the Folders area. It also allows you to:

- Import bot files
- Export bot files
- Run a Bot
- Schedule a bot
- Run bot with queue



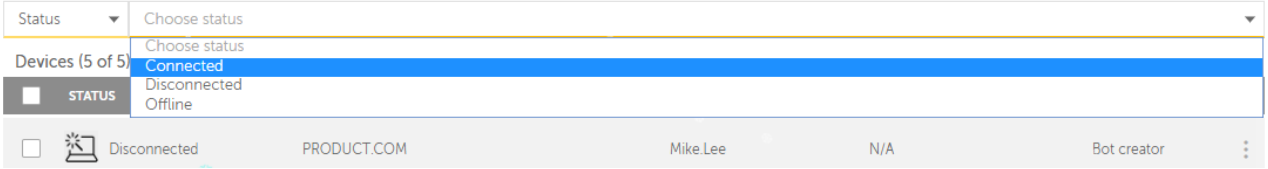
For ease of access, you can apply search parameters to Type, Name and Version Control columns.

- You can specify the search parameters in the search bar for Name:



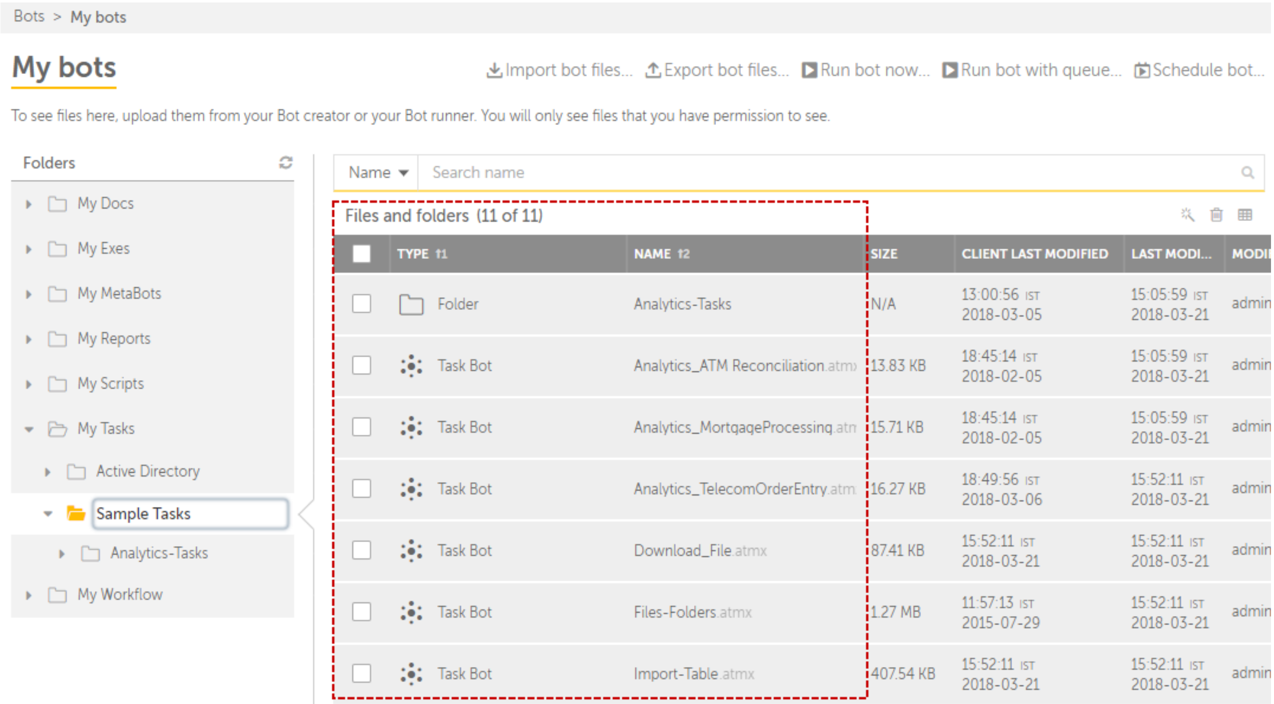
Note: When you specify search parameters for the same column, the system searches using **OR** operator. When you specify search parameters for different columns, the system searches using **AND** operator.

- You can choose the search parameters from a list in the search bar for Type and Version Control:



Files and folder(s)

When you click a folder from the **Folders** area in the **My bots** page, the contents of the folder are displayed in the **Files and Folders** area.



When VCS is enabled, the version related columns are displayed. If production version is set for a file, the information displayed in the rest of the columns, such as size is for that version.

The columns of the **Files and folders** table are described in the following table.

Item	Description
Type	The type of file - Folder or Task Bot. This is based on the type of the file in the folder.
Name	The name of the folder or file.
Size	The size of the file.
Client last modified	• The date on which the file was last modified on the Bot Creator machine before it was uploaded to the Control Room. • If Version Control is enabled and the Production Version is set, the date is the one when that particular production version was last modified before it was uploaded to the Control Room.
Last Modified	The date and time when the file was last updated.
Modified by	Name of the user who last modified the file or folder

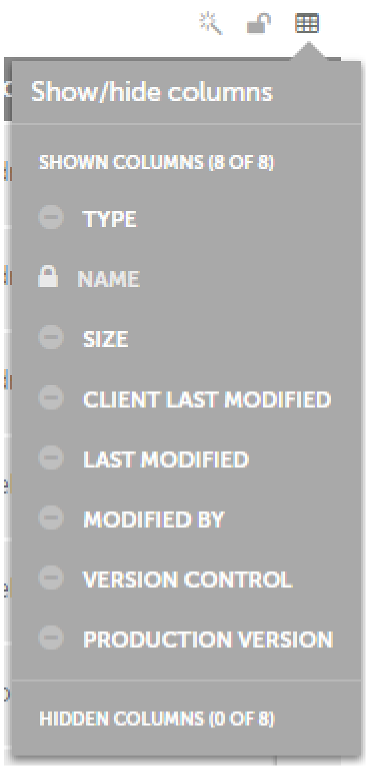
Tip: You can perform the following actions on a column to help you work efficiently.

- Click a column to sort it in ascending and descending order. You can sort up to three columns by holding the Shift key when you click on two more columns. This gives you the option of sorting two additional columns. This way the sorting is done on the entire table and not just the data that is currently visible to you. The last sorting is stored in memory applied by a user per session.
- Use a drag-and-drop operation to move the column left or right.
- Move your mouse cursor at the end of the column and drag to re-size.

You can perform the following tasks on an individual file or folder in the **Files and folders** area.

Action	Description
Run	Allows you to Run the selected Bot.
Unlock bot	Allows you to forcefully unlock the selected Bot if locked for editing by the BotCreator in Enterprise Client.
Schedule	Schedule the Bot to run.
Edit folder	Allows you to rename a folder.
View	Allows you to view details of the file or folder.
Delete Folder / Bot	Allows you to delete a bot, file or folder. Note: This option is **not available** when Version Control is **enabled.**
Note: Only Edit, View and Delete options are **available** for **folders.**	

Alternatively, you can select all Bots or Folders and perform the following actions. Note that these actions can be performed only at a table level and not on individual items.

Table Item	Description
Create folder	Allows you to create a folder from the **Files and folders** section.
Show / Hide columns	Allows you to show or hide specific columns. By default, all columns are displayed:  Tip: To **hide** a column, click on the column name. Note: Columns **Version Control** and **Production Version** are only visible when Version Control is enabled.
Unlock checked items	Allows you to forcefully unlock selected Bots (multiple) if locked for editing by the BotCreator in

	Enterprise Client. Note: This option is **available** only when Version Control is **enabled.**
Delete checked items	Allows you to delete the selected or all Bots or Folders (multiple). Note: This option is **not available** when Version Control is **enabled.**

Create and Edit Folders

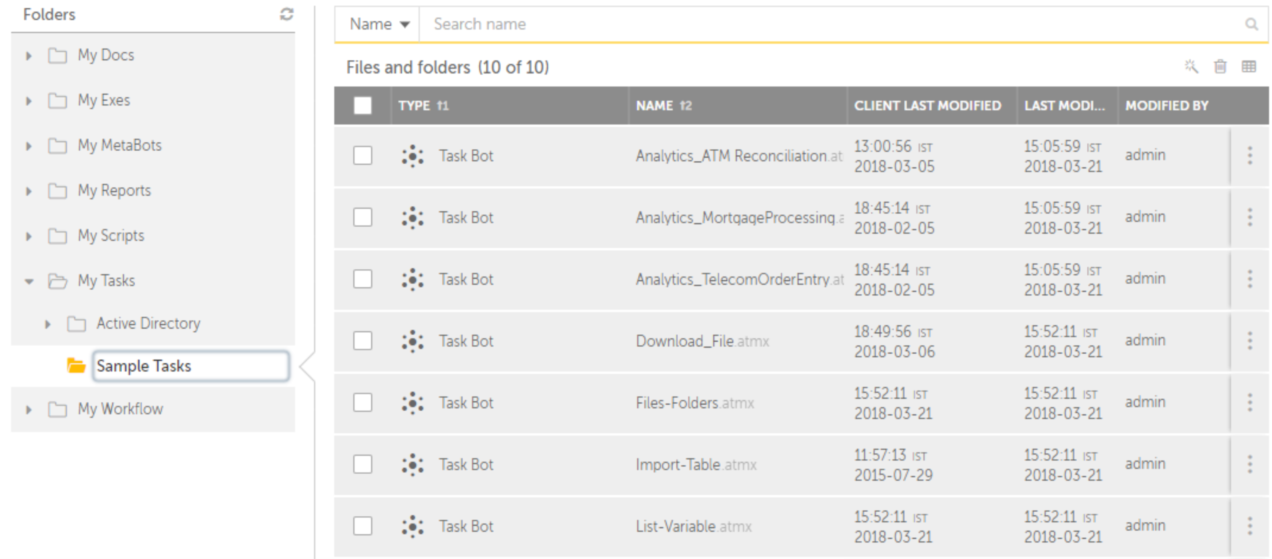
As a Control Room user with **View my bots** and **Create Folder** privileges, you can create folders in the Control Room repository. This enables you to grant access privileges to Bot Creators/Bot Runners to specific folders so that they can upload, download, delete, and/or execute (MetaBots only) their Bots to the Control Room.

If you have **Edit Folder** privileges, you can also rename the folders to which you have access.

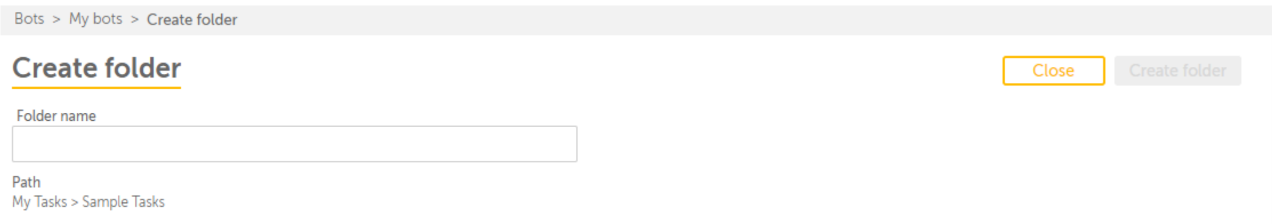
Create a folder

To create a folder,

1. Go to Activity → My Bots →Folders area
2. Click on a folder in the Folders tree view to open it. For example, My Tasks → Sample Tasks:

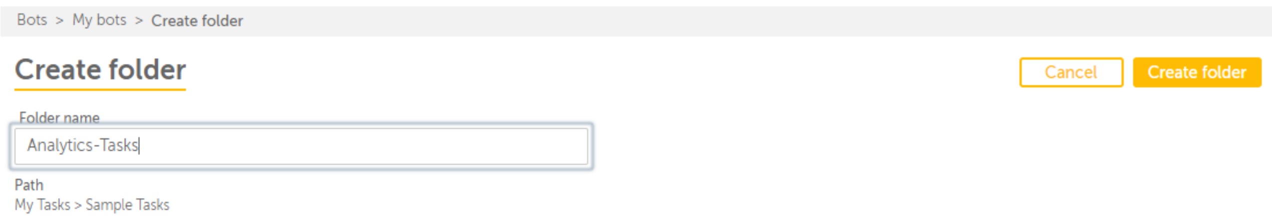


3. Click that is given above the **Files and folders** list
4. The **Create folder** page is launched:



Tip: Click Close if you do not want to continue creating the folder and go back to the **My Bots** page.

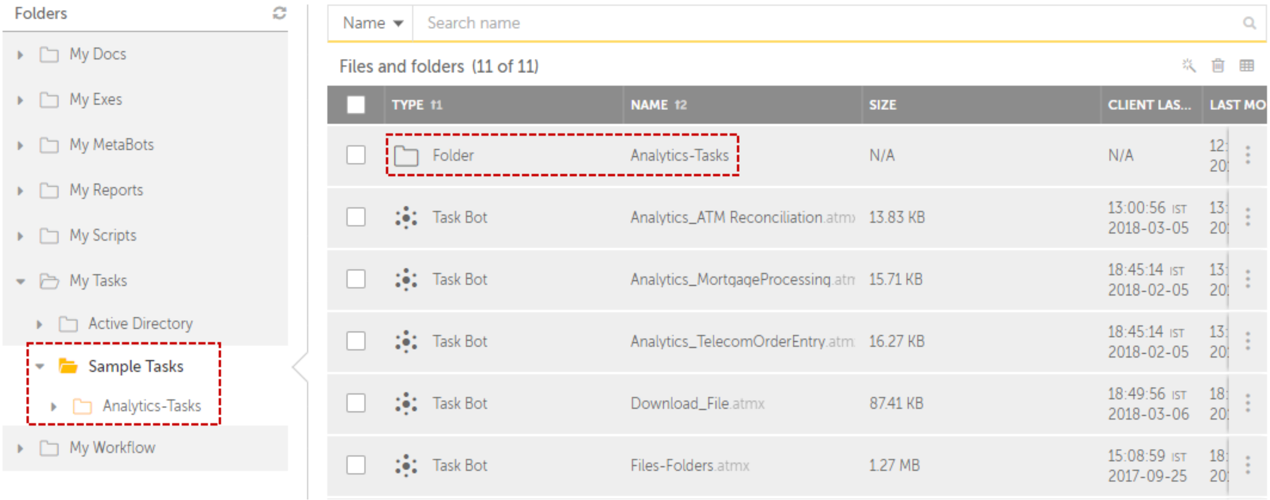
5. Provide an appropriate name. For example, you might want the Bot Creator with Analytics license to store tasks to the **Analytics-Task** folder:



6. Click **Create folder** to save the folder.

   Alternatively, click **Cancel** if you do not want to save changes and go back to the **My Bots** page.

7. The folder is added which can be viewed in the **Folders** tree view and **Files and folders** list:

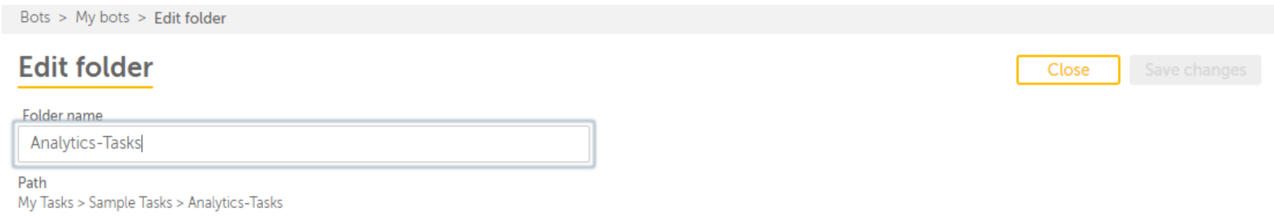


Rename a folder

For some reason, such as a typo or change in naming conventions, you might want to rename a folder. This section describes how to rename the folder.

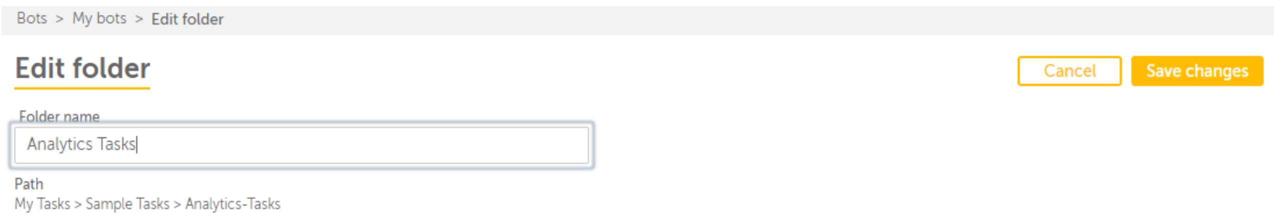
To rename a folder,

1. Go to Activity → My Bots →Folders area
2. Click on a folder in the **Folders** tree view to open it. For example, My Tasks → Sample Tasks.
3. In the **Files and folders** list, hover over the actions icon - ⋮ for the folder that you want to rename. This slides open the actions panel.
4. Click 🖉
5. The **Edit folder** page is launched:



> **Tip:** Click **Close** if you do not want to continue creating the folder and go back to the **My Bots** page.

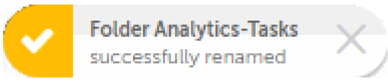
6. Update the folder name as required:



7. Click **Save changes**

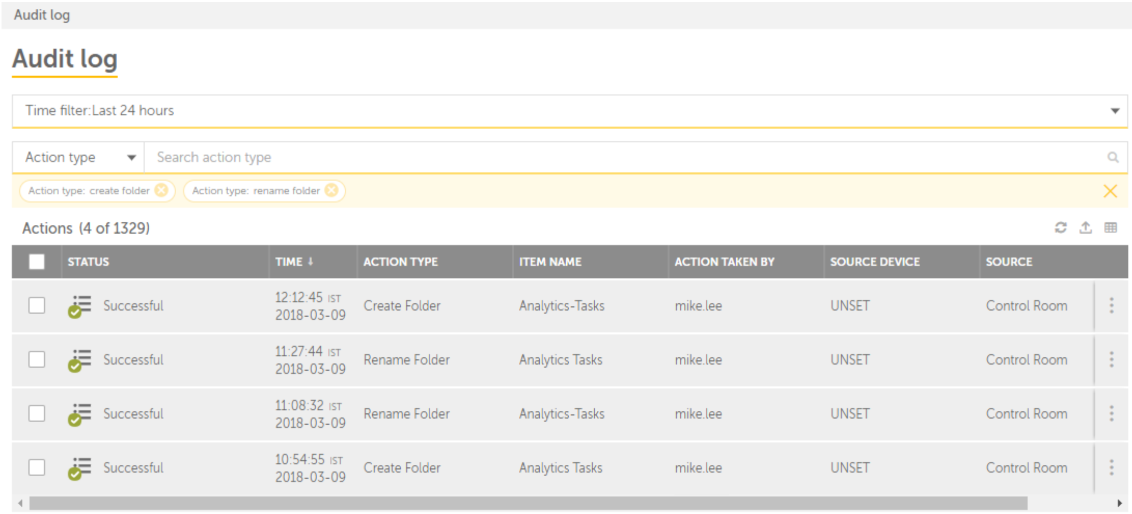
   Alternatively, click **Cancel** if you do not want to save changes and go back to the **My Bots** page.

8. The folder is renamed successfully:

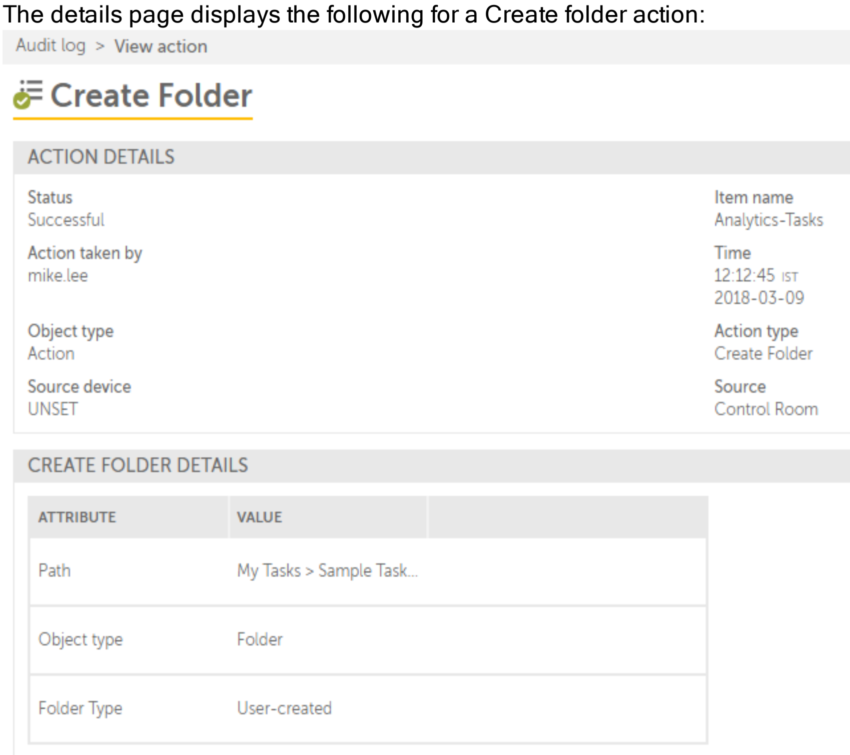


Audit Logs

- When you Create and/or Rename a Folder, the following audit entries are logged:

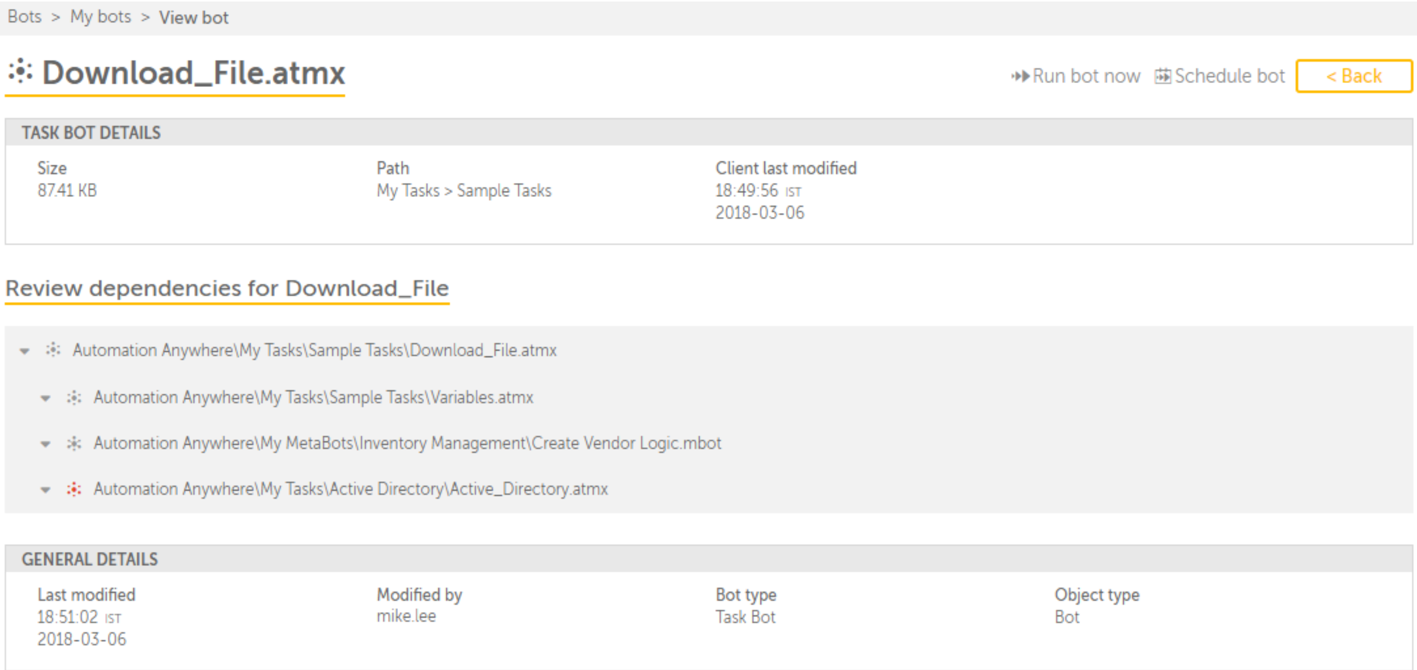


- The details page displays the following for a Create folder action:



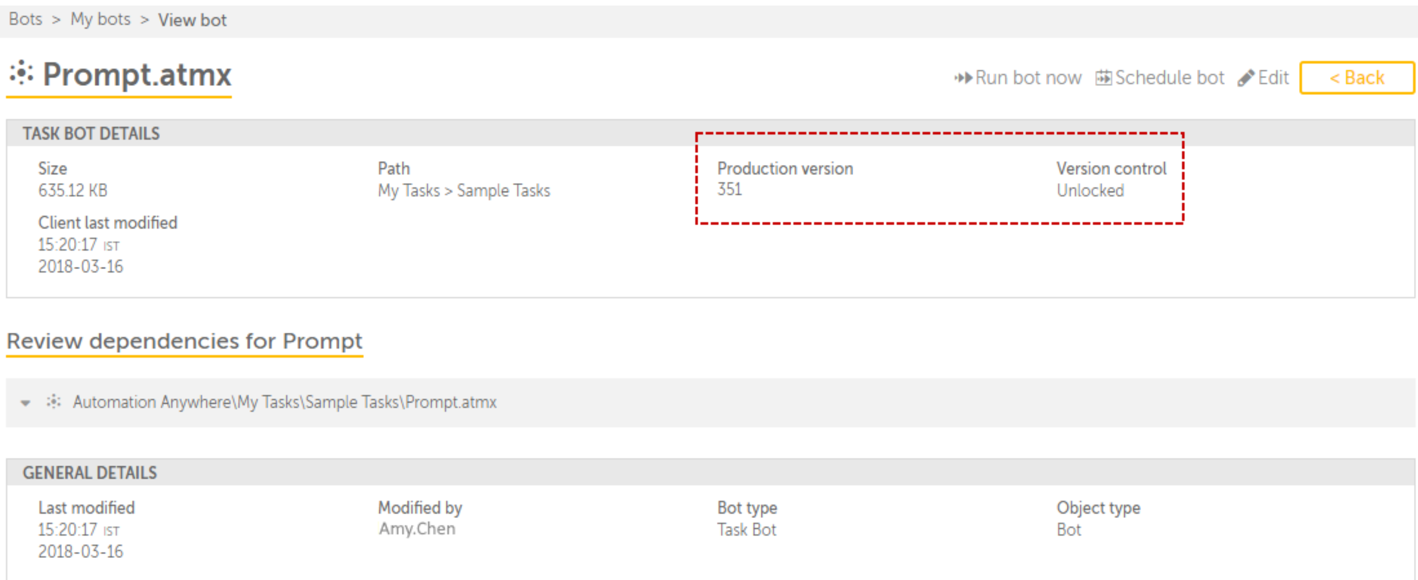
View bot details

When you click the **View** icon for a bot in the **Files and folders** area of the **My bots** page, the **View bot** page is opened. It provides information, such as the name and other details of the bot. Besides this, you can run the bot or schedule when to run the bot. This page is illustrated in the following figure.



When version control is enabled and the production version is set, the **View bot** page also displays the **Production version** and **Version control** fields as shown in the following figure.

Note: If the **Automatically assign the latest version** option is selected in the **Settings → Bots (Version Control)** page, all the production version of the bot is set to the latest version. For more information, refer to Bots - Configure Version Control.



Notes:

- When version control is enabled, the dependencies that are displayed is based on whether the production version is enabled or not.

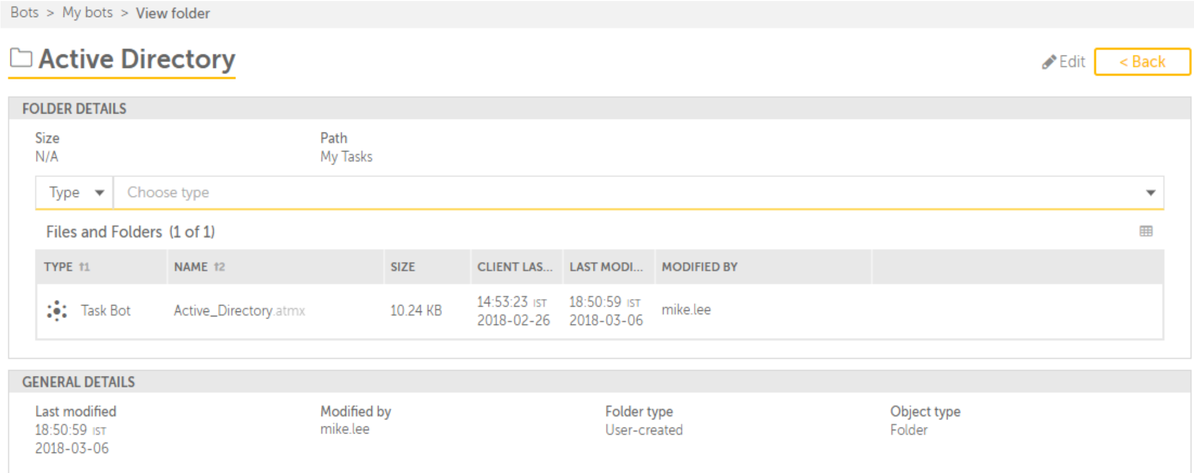
- When production version is enabled, the dependencies for that production version of the bot and its dependents are displayed.
- When production version is not enabled for any dependent file, the dependency information for that bot is not displayed

The different areas of the **View bot** page are described in the following table.

Area	Description
Task bot details	Use this area to view the following details of the folder • **Size:** Displays the size of the bot in KB or MB • **Path:** The location of the bot • **Production version:** The production version that is set either manually or assigned automatically • **Version Control:** The status of the bot - whether locked or un-locked for editing by the Bot Creator • **Client Last Modified:** The date on which the file was last modified on the Bot Creator machine before it was uploaded to the Control Room. ◦ If Version Control is enabled and the Production Version is set, the date is the one when that particular production version was last set by Control Room user. **Note:** Production version and Version control details are visible only when Version Control is enabled.
Review dependencies for <bot name>	Displays the bot and its dependencies. **Tip:** The dependency icon - will display red if you do not have sufficient privileges for the dependent bot or file.
General details	Use this area to view the following details for the folder. • **Last Modified:** Displays the last time changes were made to the folder in date and time. • **Modified by:** Displays the name of the user who last made changes to the folder in date and time. • **Bot type:** Displays the type of the bot, such as Task Bot or Meta Bot. • **Object type:** Displays the object type, such as Bot.

View folder details

When you click the View icon for a folder in the **Files and folders** area, the **View folder** page is opened. Use this page to view the details of the folder and search for items within the folder. This page is illustrated in the following figure.



The **View folder** page is divided into the following areas.

- Folder details
- Items in folder
- General details

These are explained in the following table.

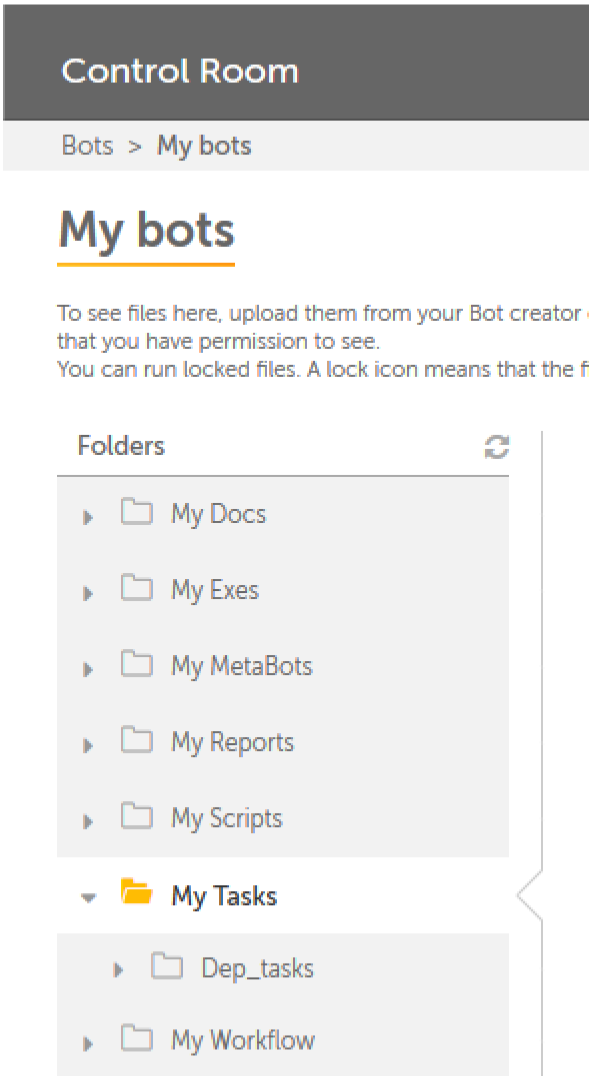
Area	Description
Folder details	Use this area to view the following details of the folder • **Size:** Displays the size of the folder. • **Path:** The path of the folder.
Items in folder	Use this area to search and view the following details for items in the folder. • **Type:** The type of the item, such as Task Bot, Meta Bot, or IQ Bot. • **Name:** The name of the item. • **Size:** The size of the item in KB or MB. • **Client Last Modified:** The date on which the file was last modified on the Bot Creator machine before it was uploaded to the Control Room. ◦ If Version Control is enabled and the Production Version is set, the date is the one when that particular production version was last set by Control Room user. • **Last Modified:** Displays the last time changes were made to the item in time and date. • **Modified:** Displays the name of the user who last made changes to the item
General details	Use this area to view the following details for the folder. • **Last Modified:** Displays the last time changes were made to the folder in date and time. • **Modified by:** Displays the name of the user who last made changes to the folder in date and time. • **Object type:** Displays the type of Object, such as folder or sub-folder.

Folders area

The folders area allows you to explore and browse your documents, executable files, Metabots, Reports, Scripts, tasks, and workflows.

Note: The view may differ from user to user depending on their roles and privileges.

When you click a folder, the contents of the folder are displayed in the Files and Folders area.

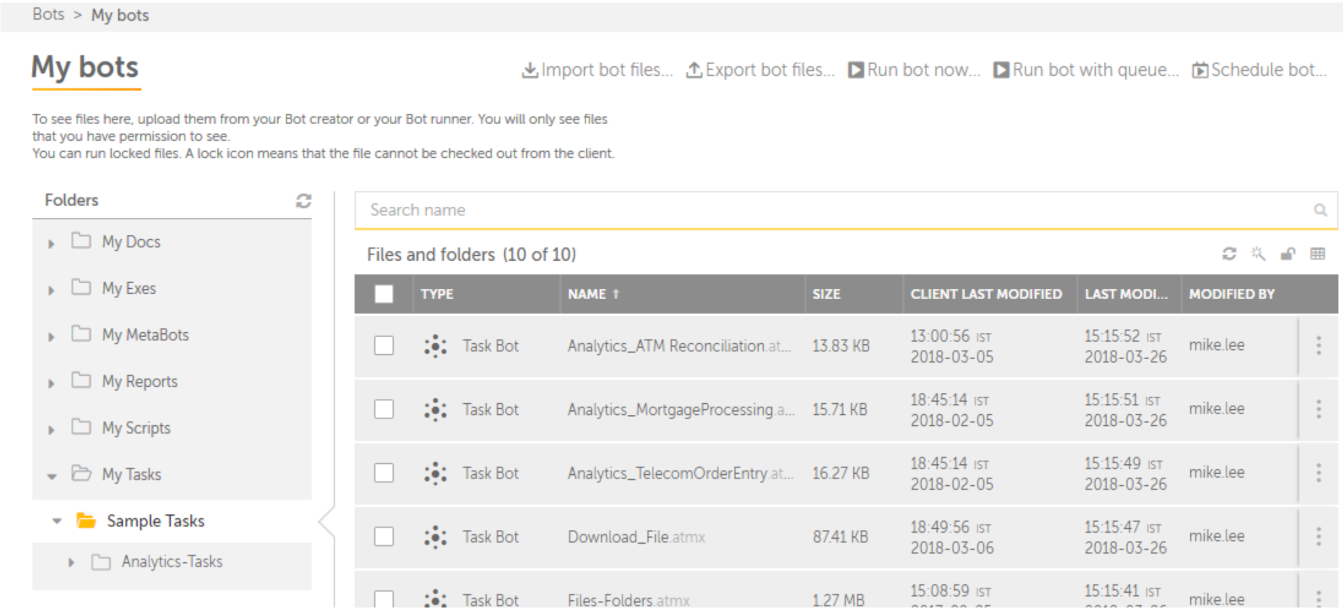


Run a bot

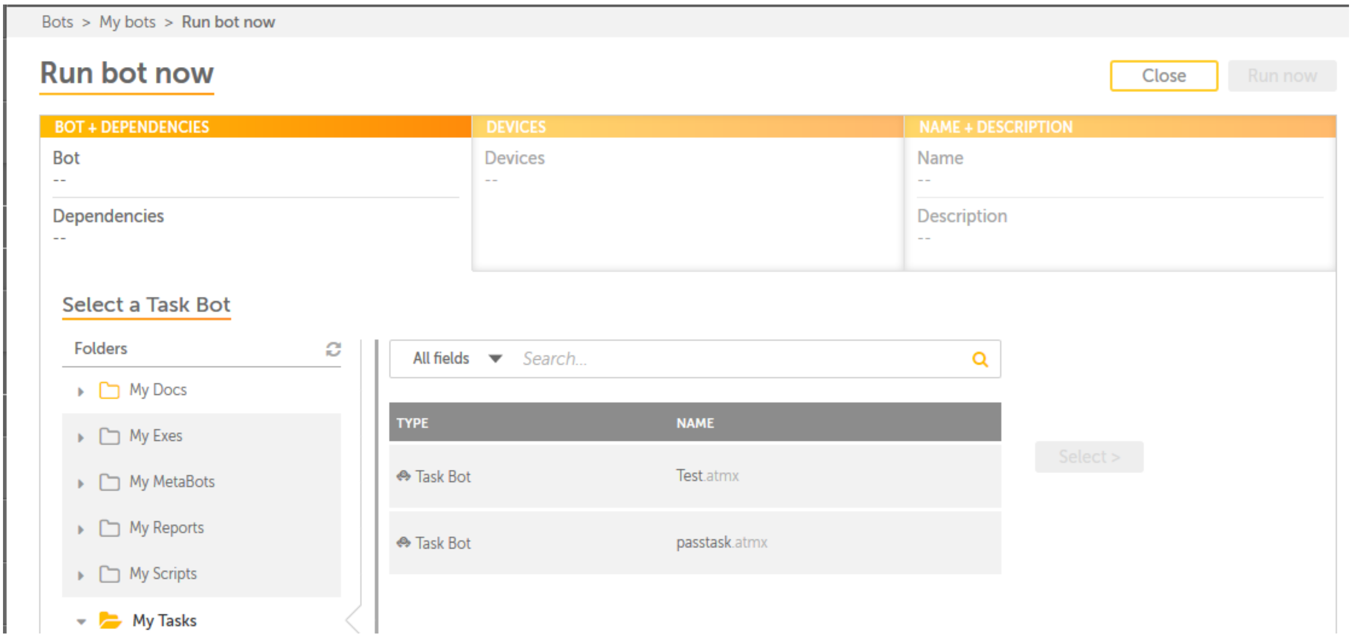
You can run a bot from the **In progress**, **Scheduled**, and also from the **My Bots** page. The procedure for running a bot is the same in all these pages, In the following scenario, we will run a bot from the **My bots** page.

To run a bot, perform the followings tasks.

1. Log on to Control Room with Run bot privileges.
2. Navigate to **Bots** → **My bots**. The **My bots** page is displayed.

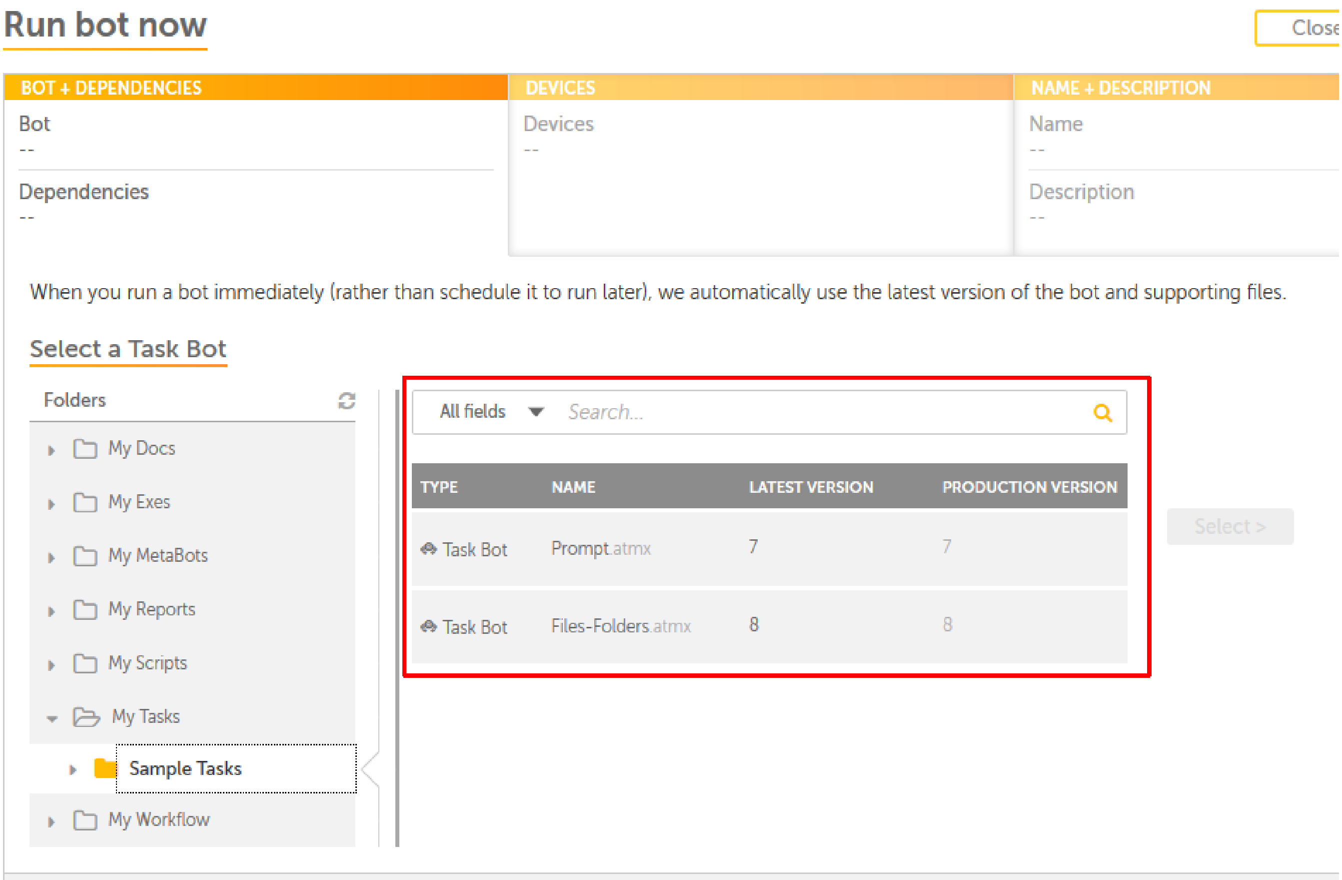


3. Click the ▶ Run bot now... link . The **Run bot now** page is displayed.

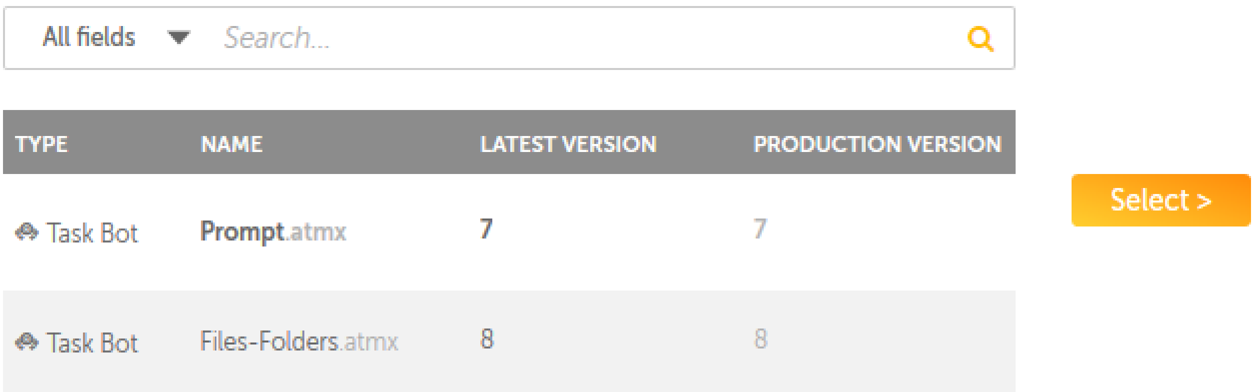


4. From the **Select a Task Bot** area, click one of the folders depending on your requirements. The Type and name of the bot are displayed on the right hand are in a tabular format.

Note: You can access only those folders for which you have **Run+Schedule** permission.



5. Select a task bot depending on your requirements by clicking a bot. The **Select** button is enabled.

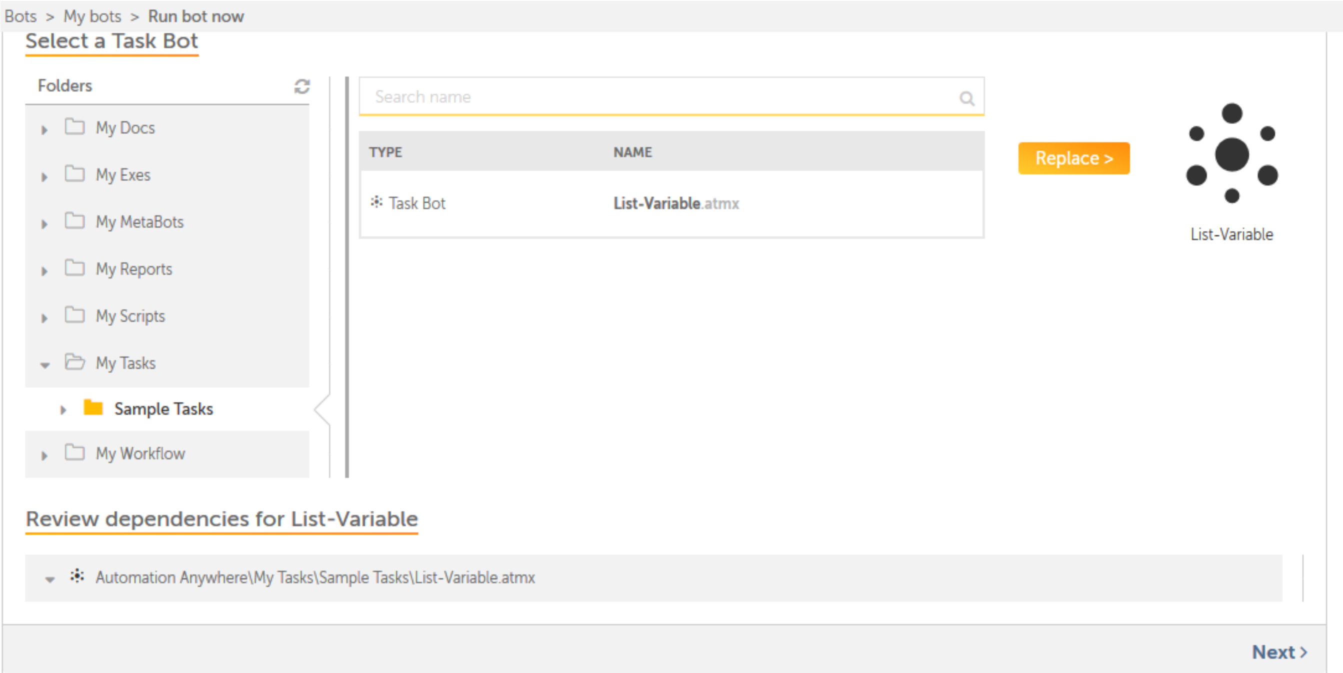


6. Click the **Select** button. The bot is added to the **Review dependencies** area where you can view the dependencies of the selected bot .

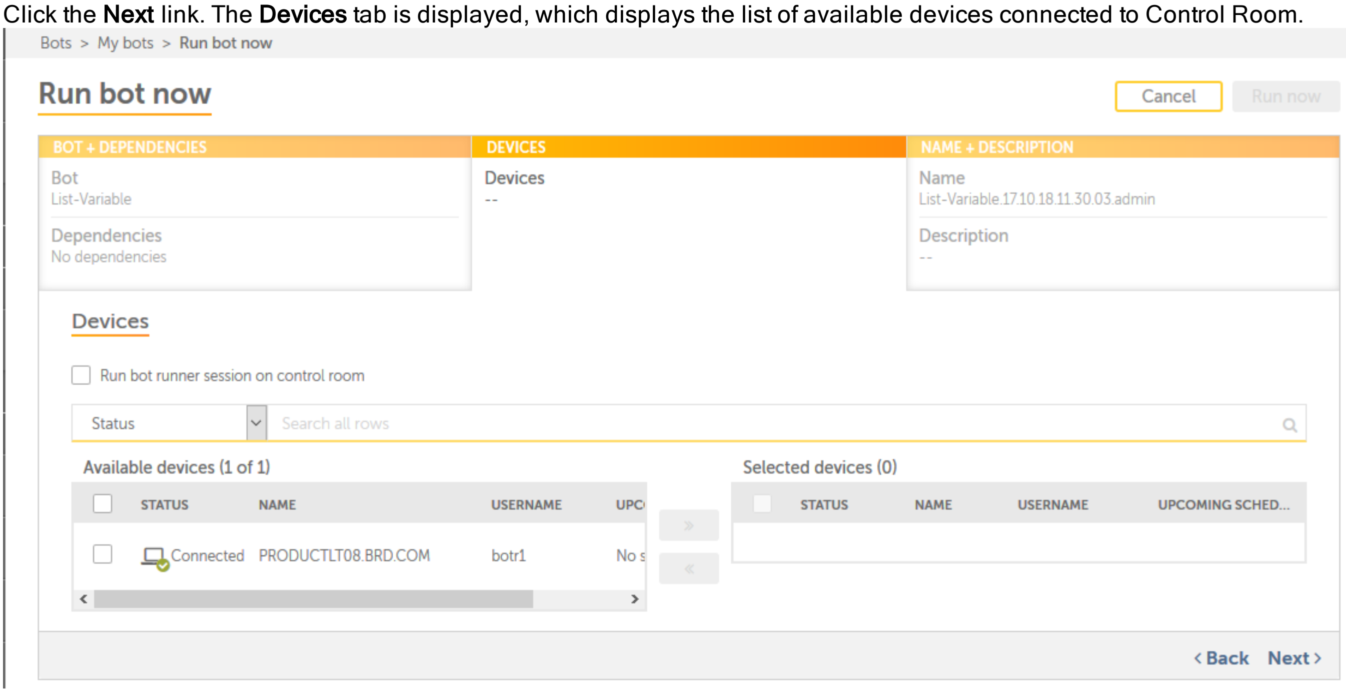
Note: Although you will be able to run a bot, automation will fail in the following cases,

- If any of the bot dependencies are missing
- If you do not have folder privileges on the dependencies
- If you do not have **Run+Schedule** permission (the one that shows a red dependency icon -)

Tip: Once you select a bot, the **Select** button is changed to **Replace**, which gives you to option to replace the selected bot with another one.

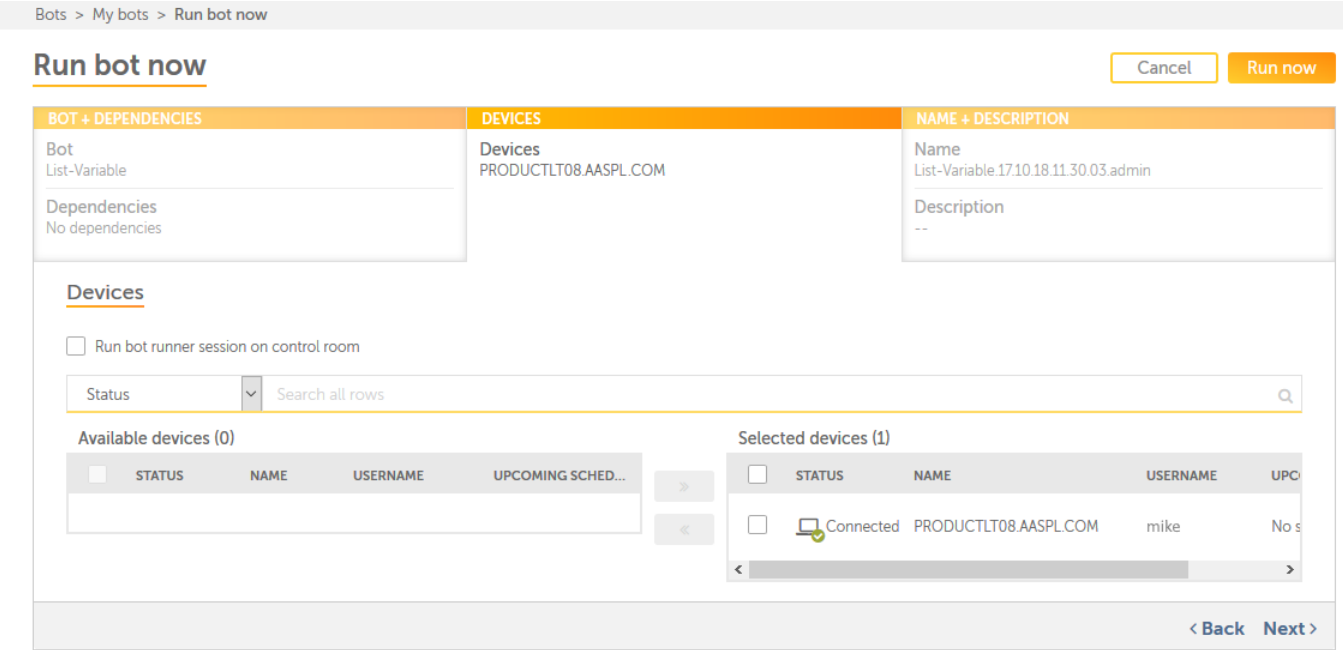


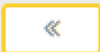
7. Click the **Next** link. The **Devices** tab is displayed, which displays the list of available devices connected to Control Room.



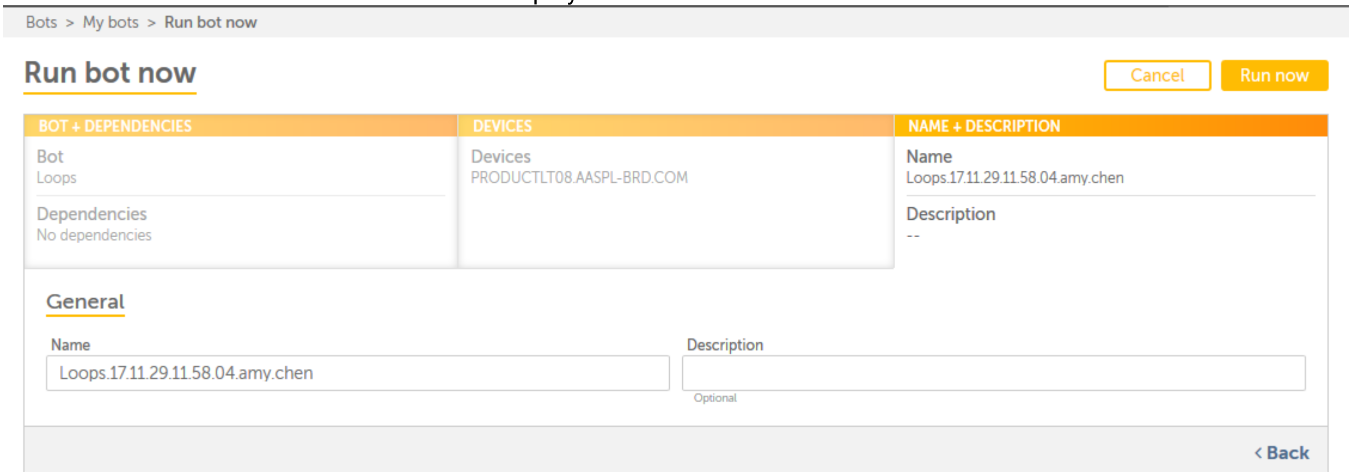
8. Click a device of your choice from the **Available devices** area and click the add **>>** button. The device is added to the **Selected** devices area and the **Run Now** button is enabled.

> **Note:** You can select only bot runner devices that are connected. If a device is not connected, it is not enabled. Also, if the device is not displayed in the list, ensure that an active bot runner session is running on the device.



Tip: To remove the item, click the  icon.

9. Click **Next**. The **NAME+DESCRIPTION** tab is displayed



10. Type a name and description in the General area and click the Run now button. By default, a name is provided by for the automation- this is of the format [bot name].[DD.MM.YY][HH.MM.SS].[USERNAME]. Change this depending on your preferences. For example, Loops.17.11.28.16.44.59.amy.chen.

Note: The **Run now** button is disabled if the device is disconnected or the required fields are not filled.

When you click the **Run now** button the activity is immediately started and its progress can be viewed from the **In Progress activity** page.

Delete bot(s) and folder(s)

As a Control Room admin or user with Delete Bot privileges, you can delete one or more Bots and Folders that are uploaded by a Bot Creator from the Enterprise Client.

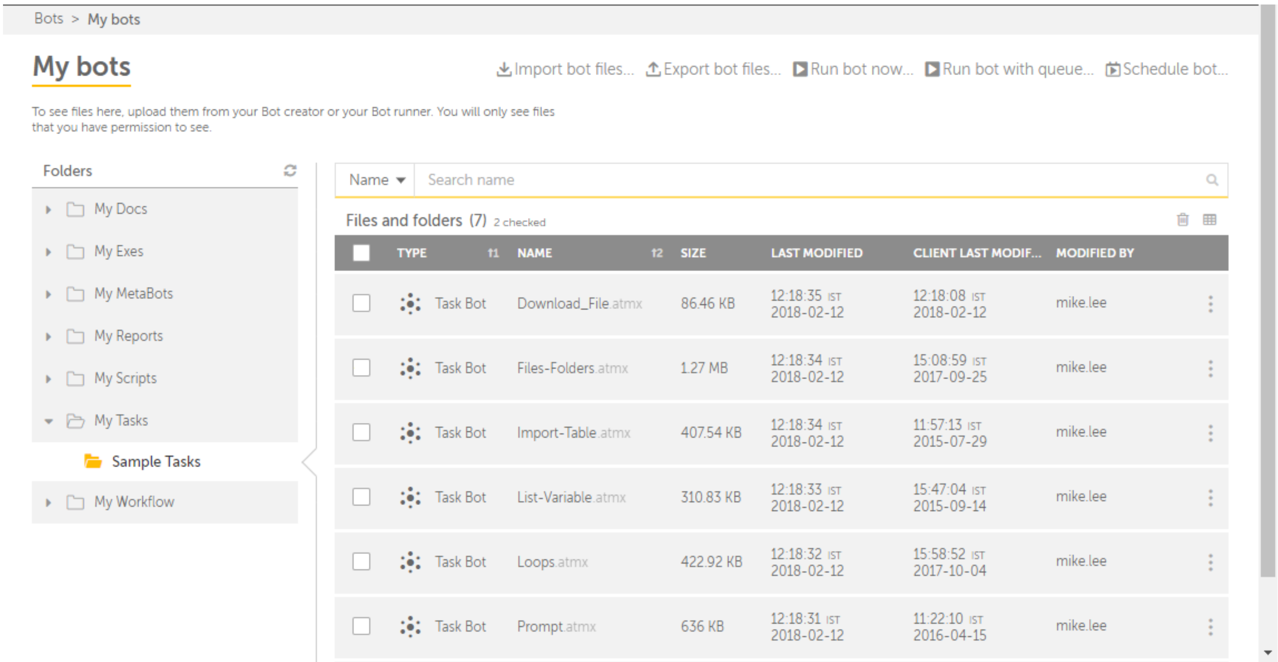
> Note: This option is **not available** when version Control is **enabled.**

Delete a bot

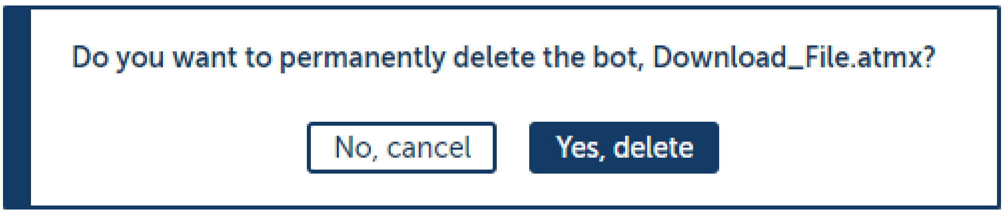
You can delete a Bot (single) that is uploaded by the Bot Creator from Enterprise Client.

To delete a Bot from the Control Room,

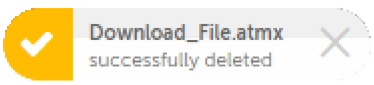
1. Go to **Bots** → **My Bots**
2. The **My Bots** page is launched:



3. In the **Files and folders** list mouse over ⋮ for the Bot that you want to delete. For example, **Sample Tasks** → **Download_File.atmx**
4. Click
5. The following message box is displayed:



6. Select **Yes, delete** to confirm.
7. The Bot is deleted permanently:



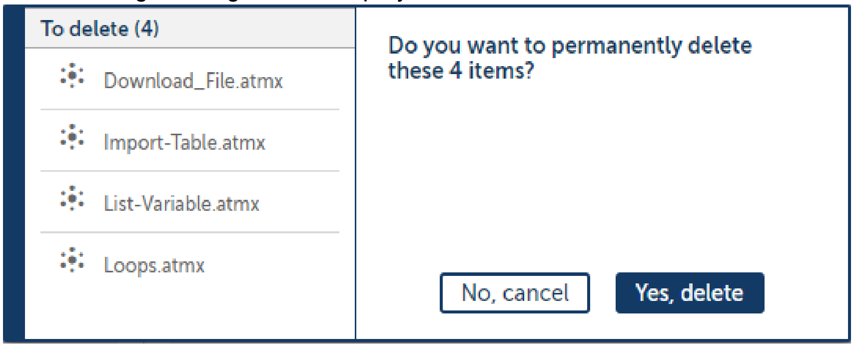
- Select **No, cancel** to go back to the **Files and folders** list without deleting the Bot.

Delete multiple bots

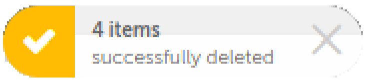
You can delete selected Bots (multiple) that are uploaded by the BotCreator from Enterprise Client.

To delete Bots from the Control Room,

1. Go to **Bots** → **My Bots**
2. The **My Bots** page is launched.
3. In the **Files and folders** list select Bots that you want to delete by clicking required check-boxes. For example, **Sample Tasks** → **Download_File.atmx, Import-Table.atmx, List-Variable.atmx,** and **Loops.atmx**
4. Click given above the table.
5. The following message box is displayed:



6. Select **Yes, delete** to confirm
7. The Bots are unlocked successfully:



- Click **No, cancel** to go back to the **Files and folders** list without deleting the Bots.

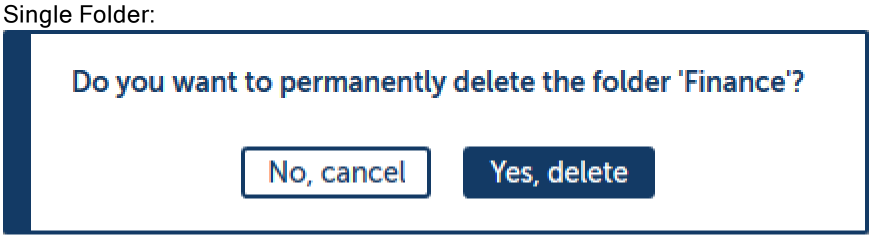
Delete folder(s)

The method to delete Folder(s) is similar to deleting Bot(s). You can choose to delete multiple folders from table level or individually from files and folders list.

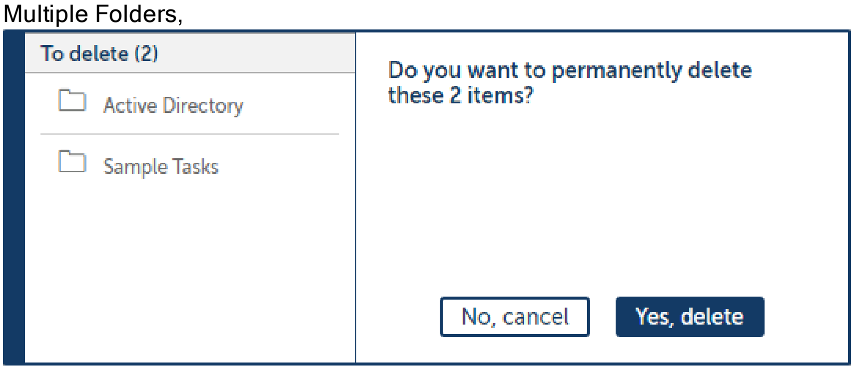
Note: The folder that you want to delete should be empty.

Following messages are displayed when you delete,

- Single Folder:



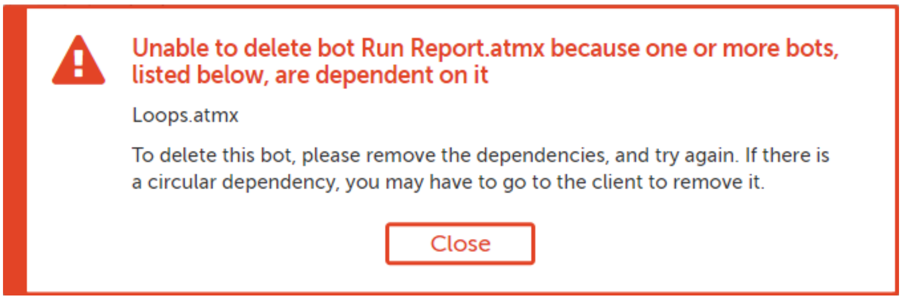
- Multiple Folders,



Delete dependent bots and files

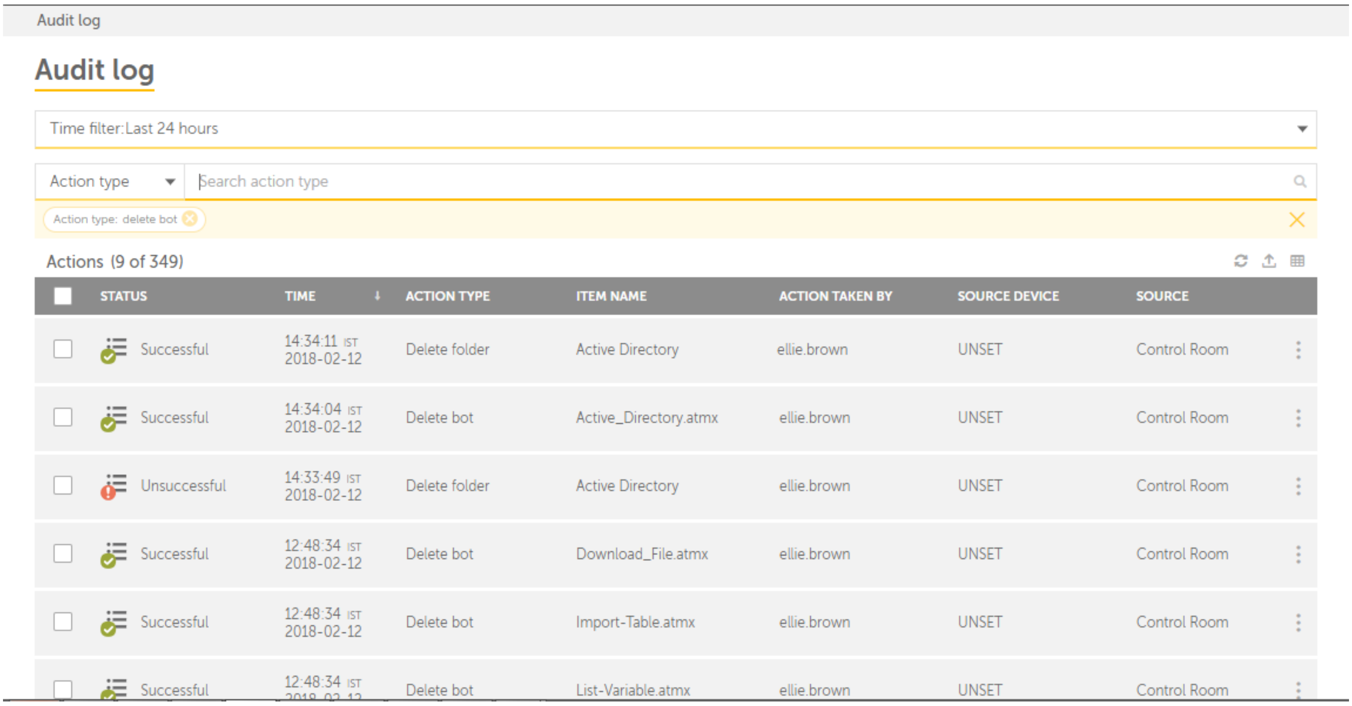
When you delete Bot(s), its dependent Bots and Files are not deleted automatically. If you do not require those, you will have to delete them manually from the folder where they reside.

When you try to delete a bot that is part of another bot as a dependency, you are shown:

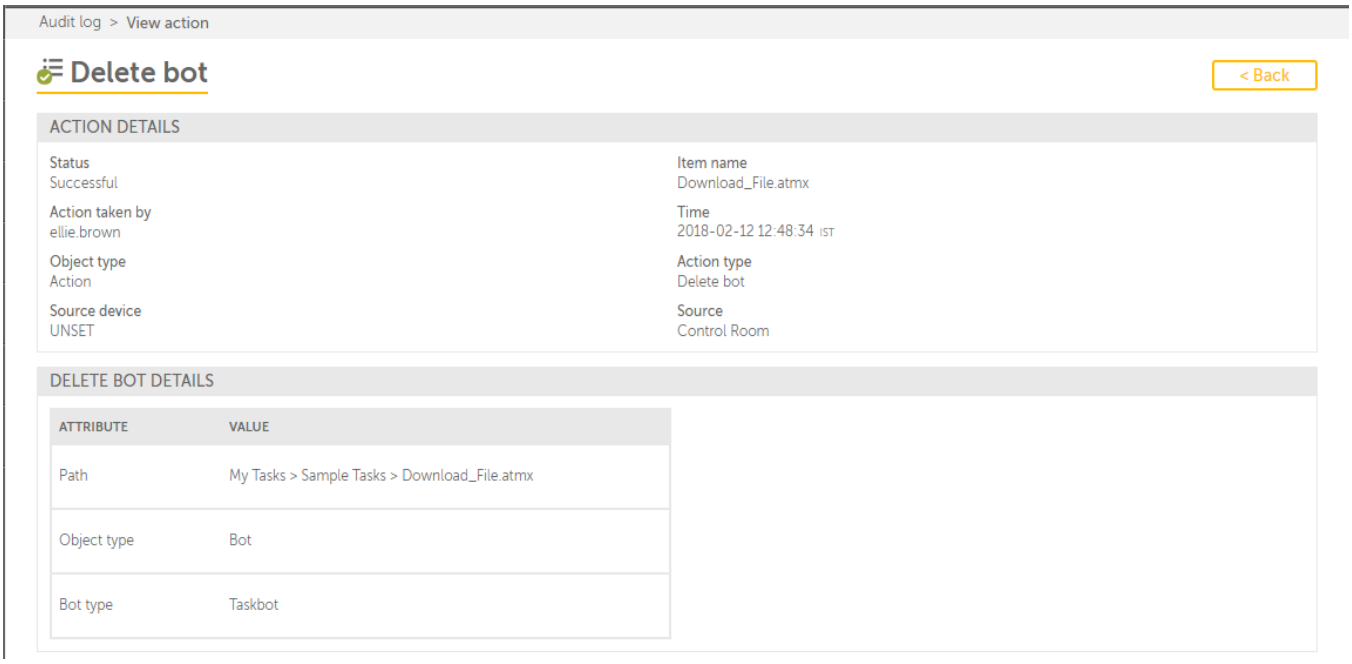


Audit Log

For all the Bot(s) that are deleted, audit entries are logged in the Audit Logs page:



The details page is shown as:



Force unlock Bots

As a Control Room user with Unlock Bot privileges, you can forcefully unlock one or more Bots that are checked out by a Bot Creator in the Enterprise Client.

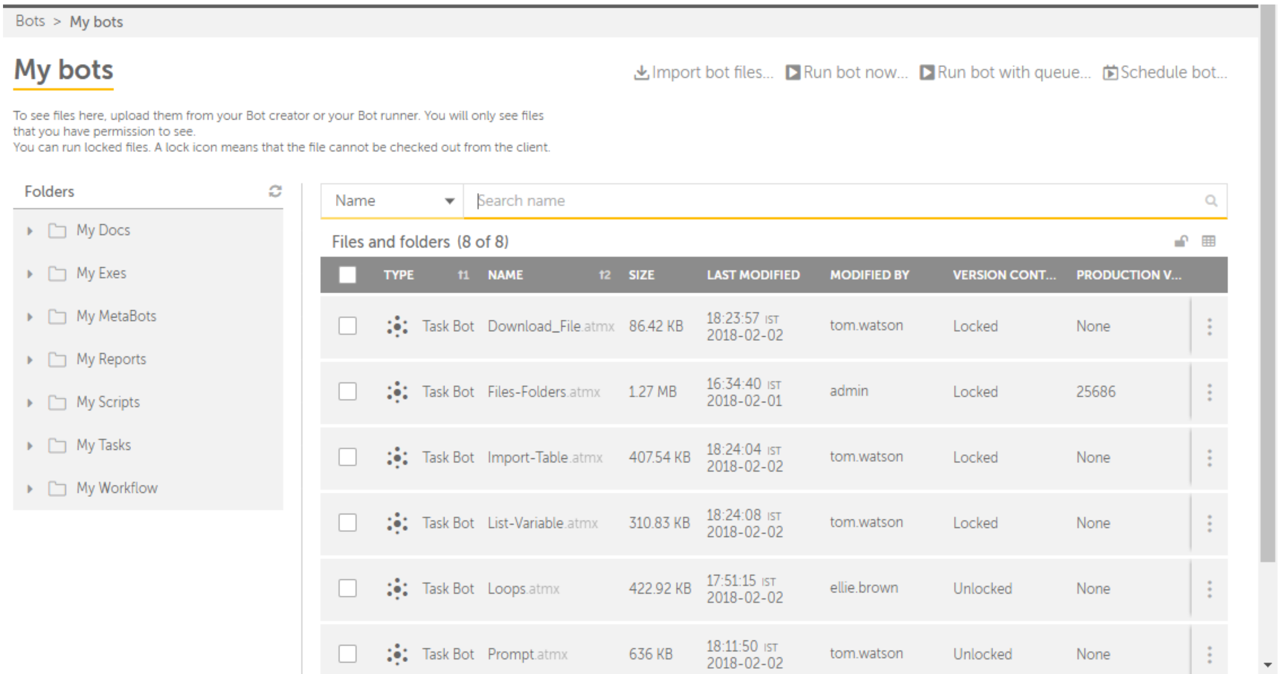
> **Note:** This option is available only when version Control is enabled.

Unlock a Bot

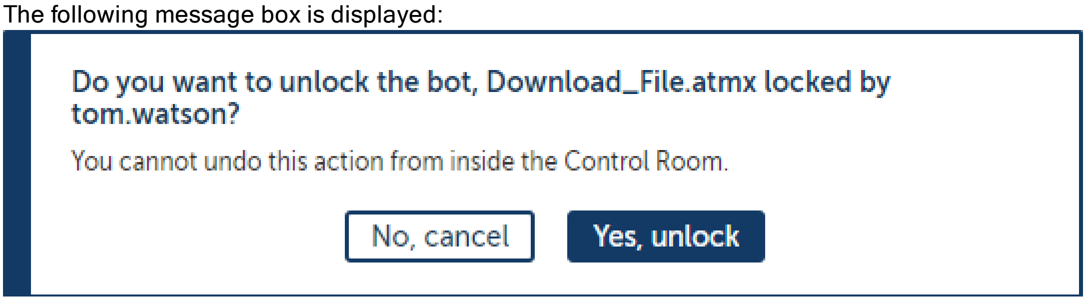
You can forcefully unlock a Bot (single) if locked for editing by the Bot Creator in Enterprise Client.

To unlock a checked out Bot from the Control Room,

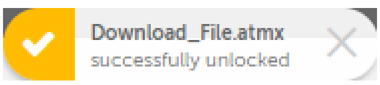
1. Go to **Bots** → **My Bots**
2. The **My Bots** page is launched:



3. In the **Files and folders** list for the Bot that is locked, mouse over ⋮. For example, **Sample Tasks** → **Download_File.atmx**
4. Click
5. The following message box is displayed:



6. Select **Yes, unlock** to confirm.
7. The Bot is unlocked successfully:



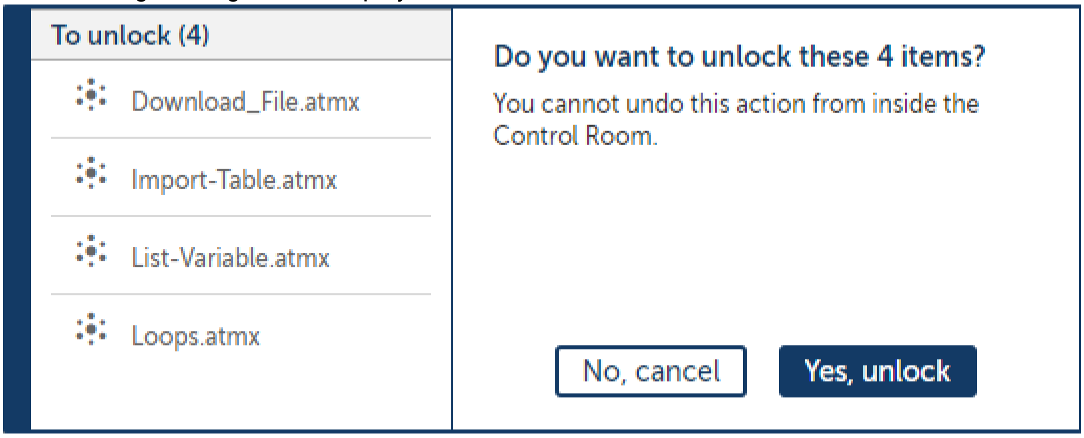
- Select **No, cancel** to go back to the **Files and folders** list without unlocking the Bot.

Unlock multiple Bots

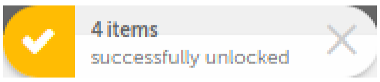
You can forcefully unlock selected Bots (multiple) if locked for editing by the BotCreator in Enterprise Client.

To unlock checked out Bots from the Control Room,

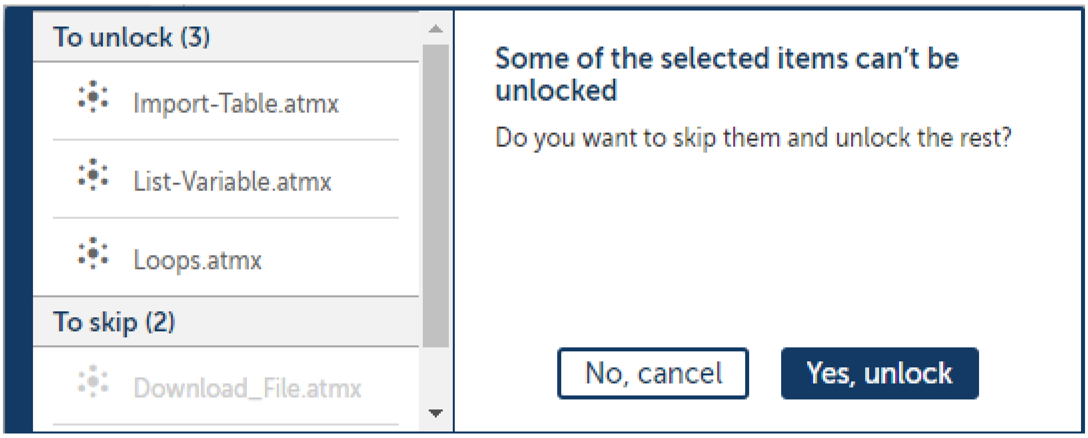
1. Go to **Bots** → **My Bots**
2. The **My Bots** page is launched.
3. In the **Files and folders** list select Bots that are locked by clicking required check-boxes. For example, **Sample Tasks** → **Download_File.atmx, Import-Table.atmx, List-Variable.atmx,** and **Loops.atmx**
4. Click given above the table.
5. The following message box is displayed



6. Select **Yes, unlock** to confirm
7. The Bots are unlocked successfully:

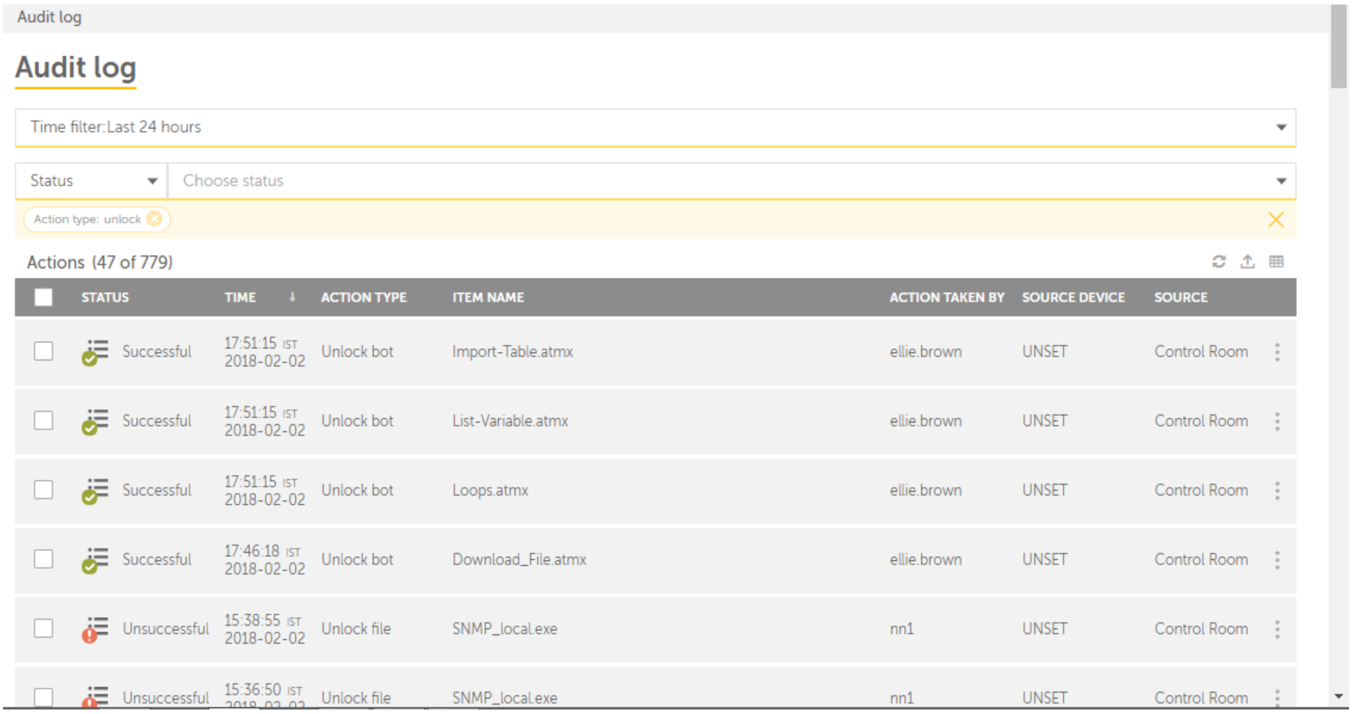


- Click **No, cancel** to go back to the **Files and folders** list without unlocking the Bots.
- If Bots that are already in Unlocked state are selected, the Control Room skips unlocking them:

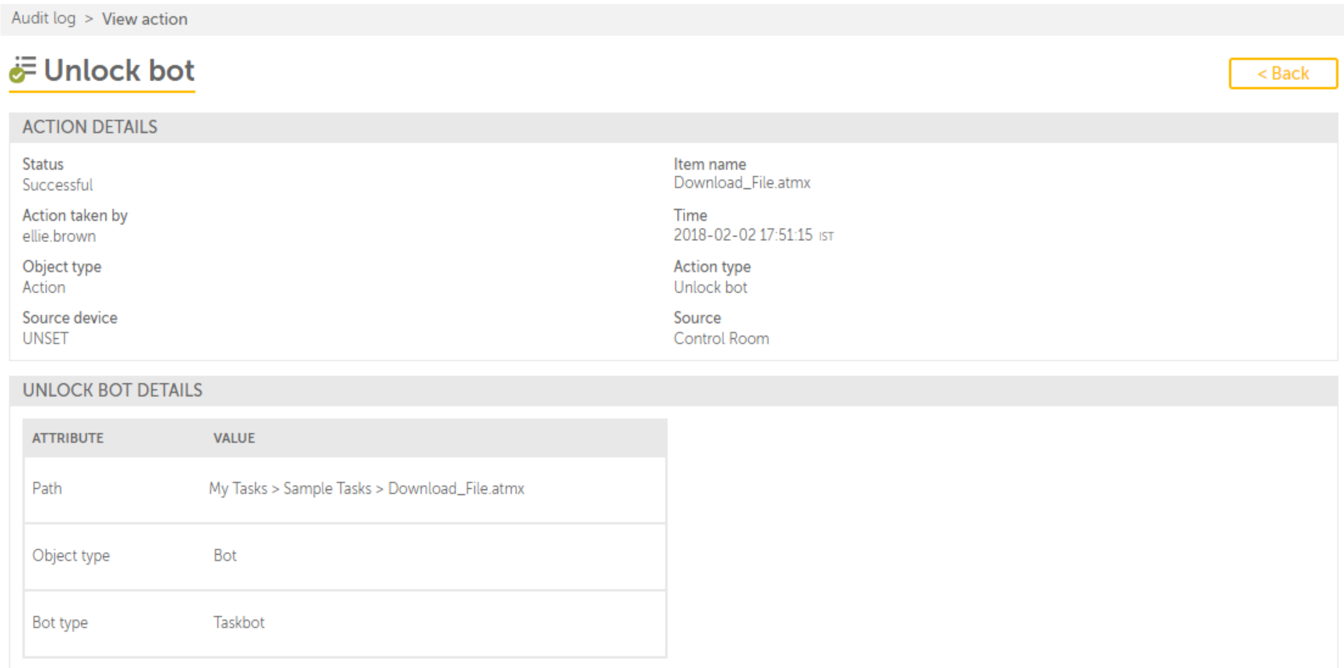


Audit Logs

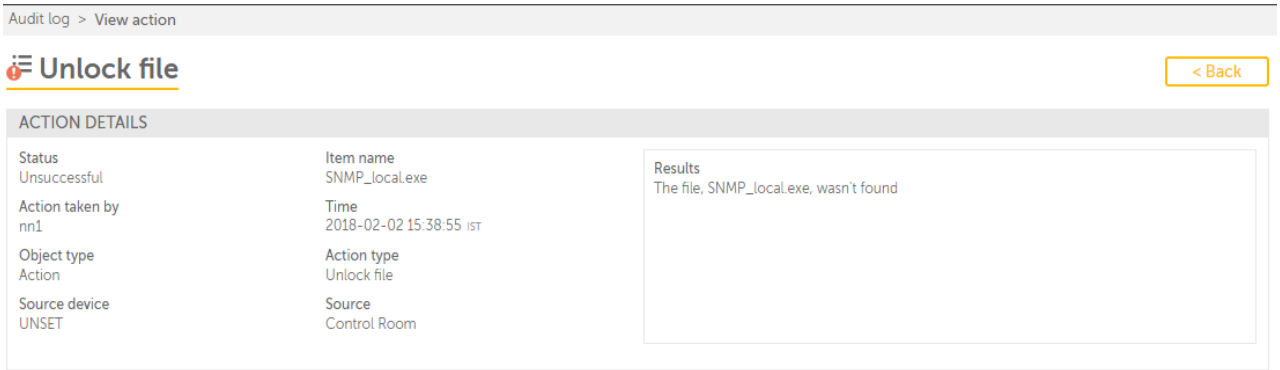
For all the Bot(s) that are forcefully unlocked, audit entries are logged in the Audit Logs page:



The details page is shown as:



- The status of an unsuccessful unlock is shown with its reason in the **Results** column of the details page:



Bot Lifecycle Management (BLM) - an overview

As a Control Room user with Export and/or Import Bots module permission, you can move your bots (new or updated) from one environment to another using Bot Lifecycle Management (BLM) module in Control Room. For example, you can move the Bots that are verified as production ready from staging to production.

The process can be performed in two stages:

1. Export Bots from one environment of a source Control Room
2. Import Bots to another environment of a destination Control Room

You can choose to Export and Import using two methods:

1. Control Room user interface i.e. Export and Import Bots
2. Export and Import API

Export bots

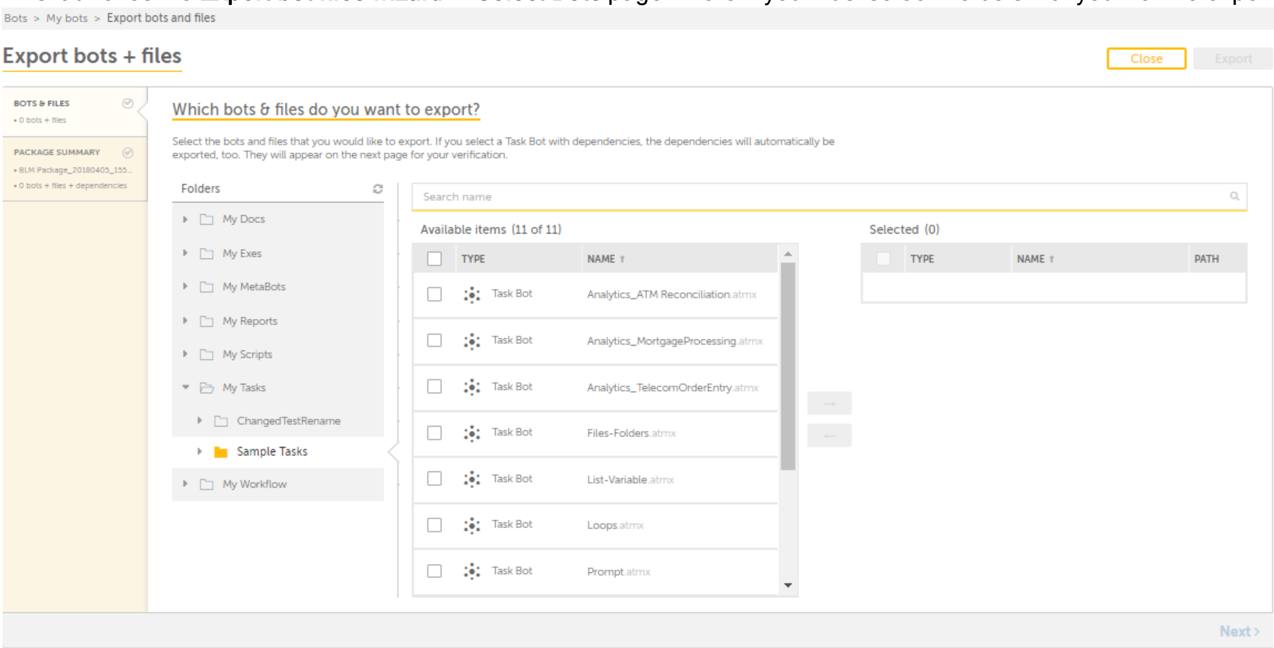
As a Control Room user with BLM Export module permission and download privileges for Tasks, Docs, Workflows, and Reports as well as execute permission for MetaBots, you can export bots and dependent files in different automation environments to help manage your organization's Bot Lifecycle Management (BLM).

The exported package can then be imported in another Control Room environment. Refer Import bots for details on importing a BLM package.

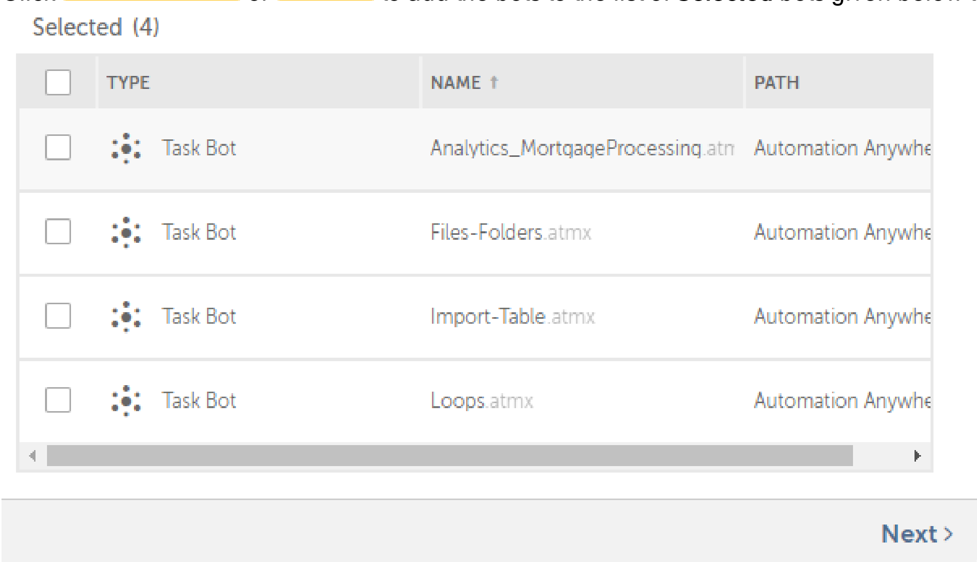
Export bot files - version control disabled

To export bot files,

1. Go to **Bots** → **My Bots** page
2. Click Export bot files...
3. This launches the **Export bot files wizard** →**Select Bots** page wherein you must select the bots that you want to export:



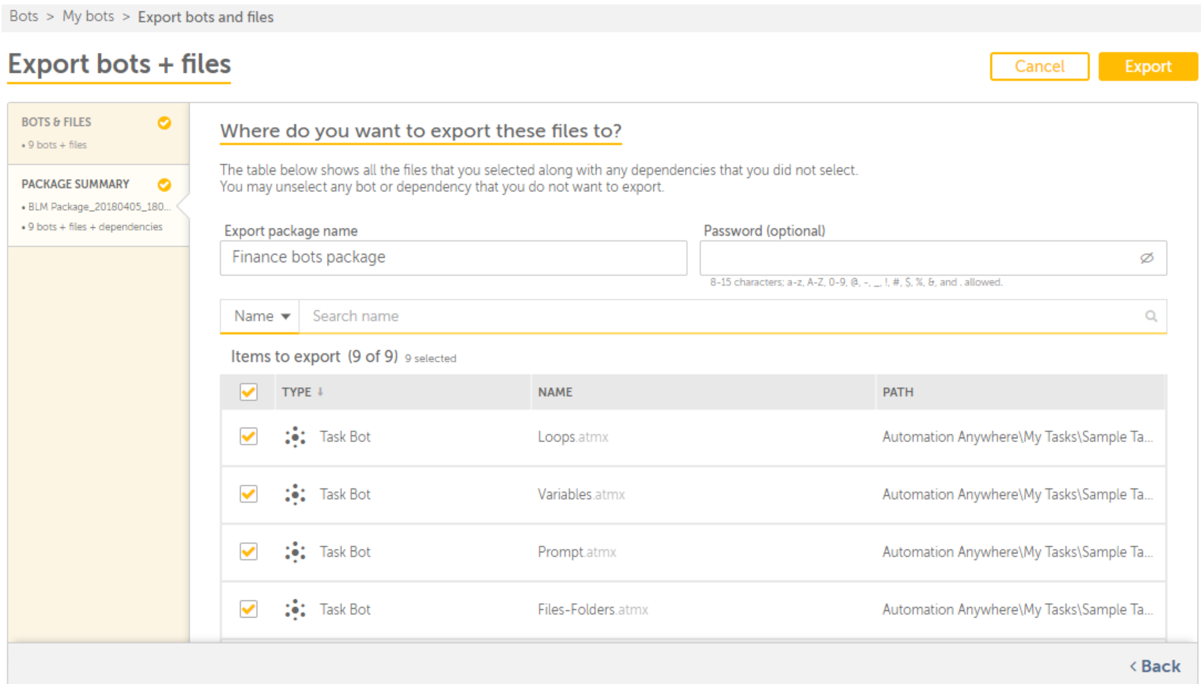
4. Select **TaskBot**(s) from the list of **Available items**. You can choose either all files by selecting the check-box in the header row or certain files by selecting the check-box beside each.
5. Click ↓ or → to add the bots to the list of **Selected** bots given below the **Available items** list:



> **Note:** The **Selected** bots panel will be available either below the **Available items** list or on the right of the list based on your screen's resolution. If it is below, the down arrow will be available and if on the right, the right arrow will be available for bot selection.

6. Click **Next**.
7. This launches the **Export bot files wizard** → **Summary** page wherein you can provide the Export package name and/or choose to exclude a bot or dependency file from the list.
   a. The system assigns a default **Export package name**. However, you can choose to rename the package.
   b. You can also choose to provide a **Password** that will be used to import the package. The password should be set as per the Control Room password policy and one that can be easily remembered.

   > **Note:** The provided password is not stored anywhere in the Control Room. If you provide a password the package is encrypted with AES 256-Bits and cannot be accessed outside of Control Room.



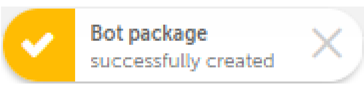
   c. If the Task Bot comprises dependent bots (TaskBots, MetaBots) and/or files, they are also automatically selected for export.

   > **Note:** If any dependent file appears more than once, it is included in the package only once.

8. Click 

   - Click 

 if you do not want to proceed.
   - Click **Back** to go to previous page.
9. The package is successfully exported to the default folder for downloads.



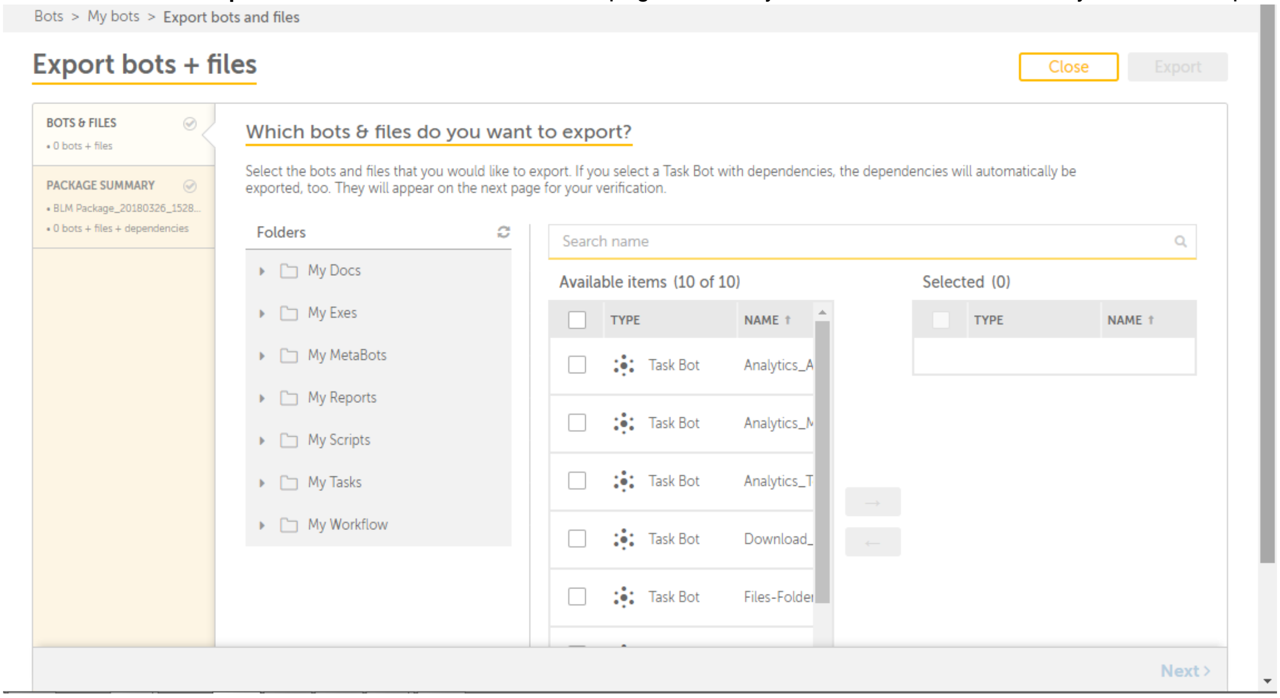
For messages related to export, refer the section Export bot files - Validations

Export bot files - version control enabled

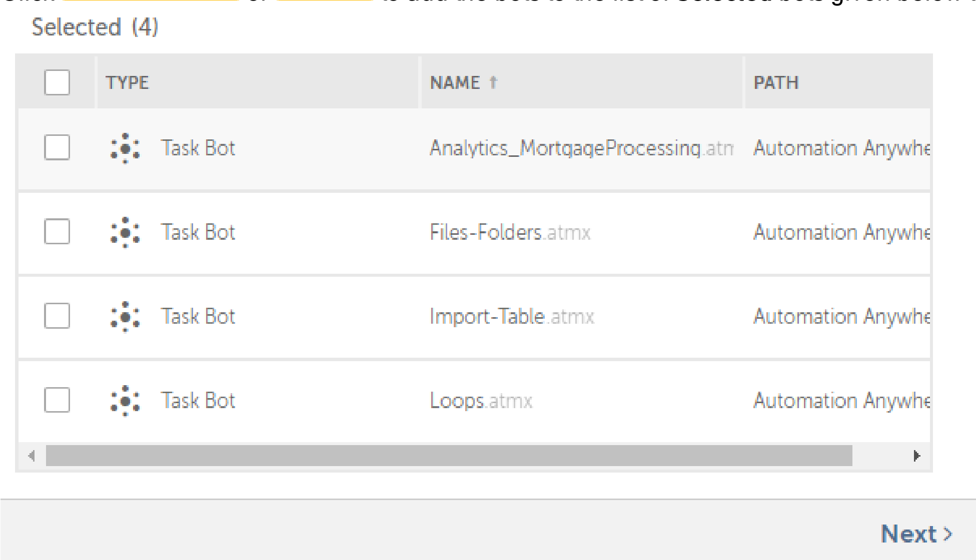
Before you use Export bot files in a Control Room that has version control, ensure that the production version of bots and their dependencies is already set.

To export bot files,

1. Go to **Bots** → **My Bots** page
2. Click Export bot files...
3. This launches the **Export bot files wizard** →**Select Bots** page wherein you must select the bots that you want to export:



4. Select **TaskBot**(s) from the list of **Available items**. You can choose either all files by selecting the check-box in the header row or certain files by selecting the check-box beside each.
5. Click ↓ or → to add the bots to the list of **Selected** bots given below the **Available items** list:

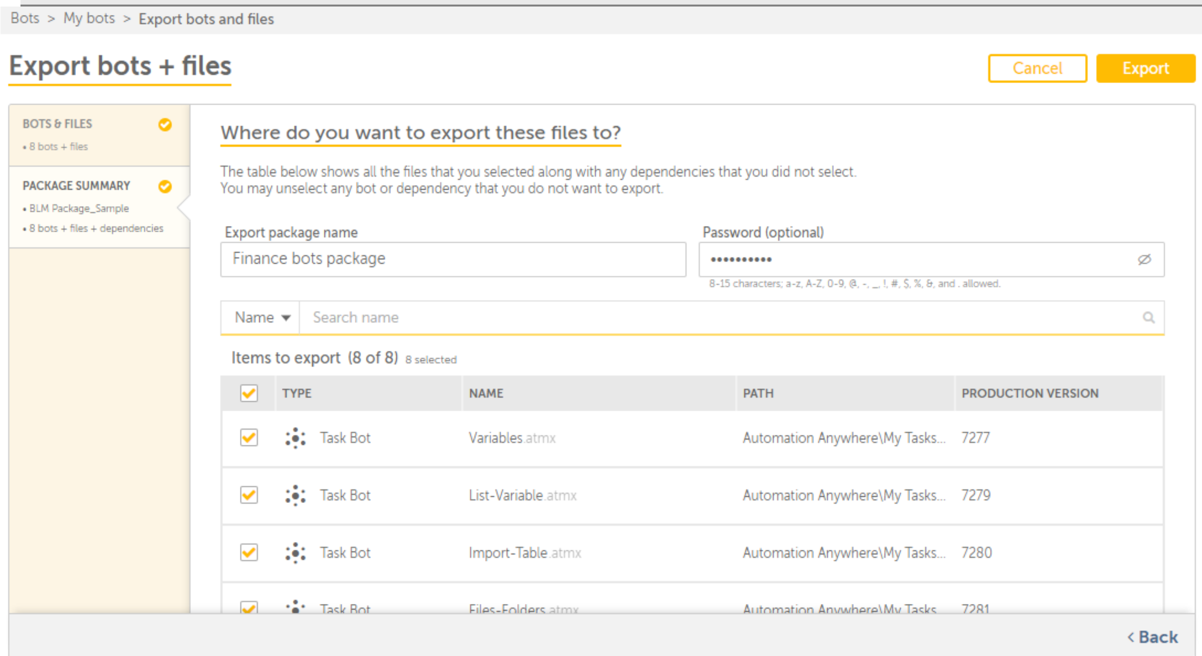


> **Note:** The **Selected** bots panel will be available either below the **Available items** list or on the right of the list based on your screen's resolution. If it is below, the down arrow will be available and if on the right, the right arrow will be available for bot selection.

6. Click **Next**.

7. This launches the **Export bot files wizard** → **Summary** page wherein you can provide the Export package name and/or choose to exclude a bot or dependency file from the list.
   a. The system assigns a default **Export package name**. However, you can choose to rename the package.
   b. You can also choose to provide a **Password** that will be used to import the package. The password should be set as per the Control Room password policy and one that can be easily remembered.

   > **Note:** The provided password is not stored anywhere in the Control Room. If you provide a password the package is encrypted with AES 256-Bits and cannot be accessed outside of Control Room.



- Only those TaskBots and MetaBots are available for selection for which Production Version is set. Hence, if the production version is not set for TaskBots and MetaBots, they cannot be exported. For other types - Docs, Workflows, and Reports, the files with latest version are allowed for export.
- If the Task Bot comprises dependent bots (TaskBots, MetaBots) and/or files, they will also be selected for export.

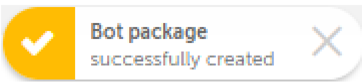
  > **Note:** If any dependent file appears more than once, it is included in the package only once.

8. Click 

   - Click 

 if you do not want to proceed.
   - Click **Back** to go to previous page.

9. The package is successfully exported to the default folder for downloads.



For messages related to export, refer the section Export bot files - Validations

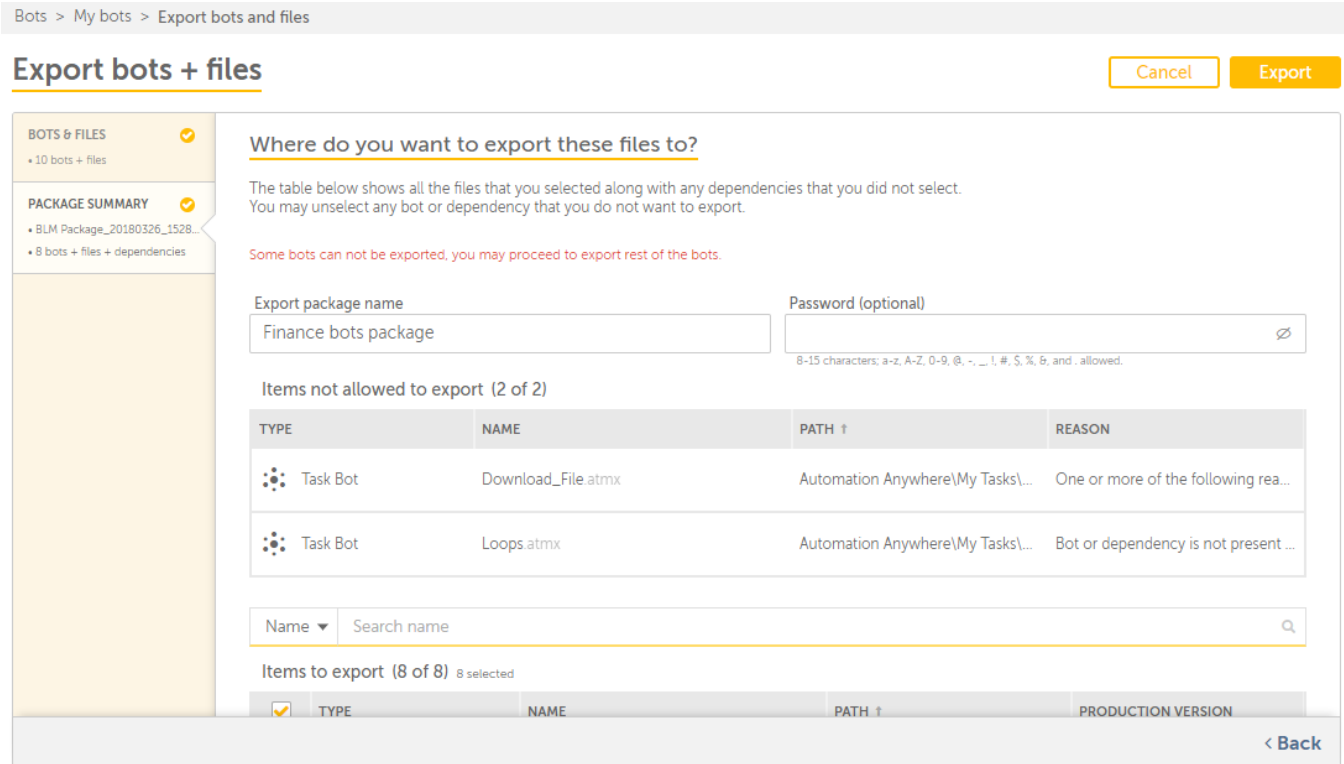
> **Note:** If the **Email settings** are enabled for Export and Import operations of a BLM package, an email notification is sent to the user who performs the export whether the action succeeded or failed.

Export bots - Validations

When you export bot files, the system checks for following validations during export:

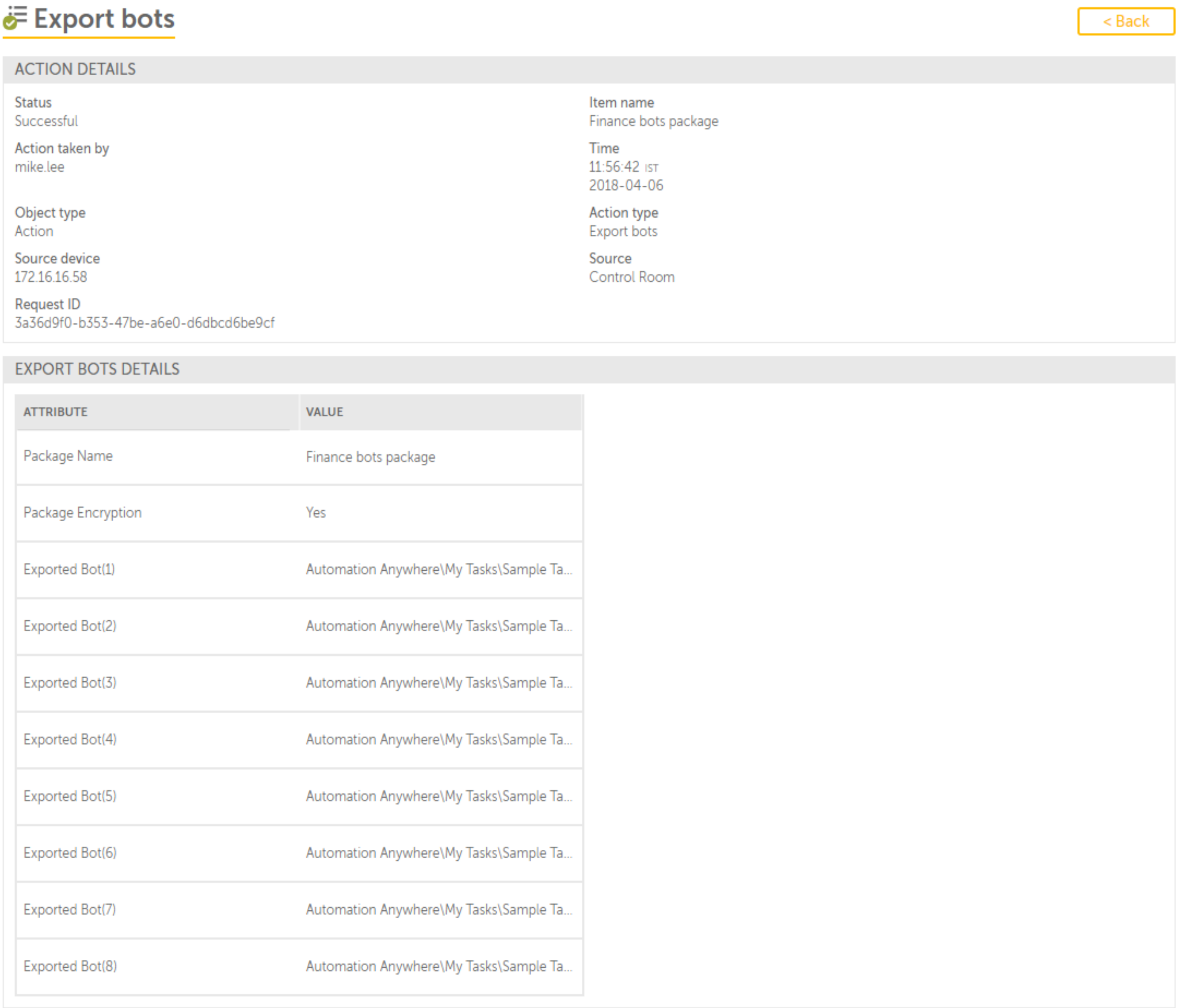
- Whether bot or dependent file is available in Control Room
- Whether you have download permission (Execute permission for MetaBot) on one or more bot or dependent files of selected bot(s)
- Whether the production version is set for all selected bot(s) or dependent file(s)

If any of the validation fails for one or more bots, those are automatically excluded from the package and shown in the **Items not allowed to export** section. You can choose to either fix those error messages and come back to export or you can export rest of the bots as shown in the **Items to export** section.



Audit Logs

An audit entry is logged in the Control Room **Audit Log** page when you export bots. The illustration below shows the detailed audit entries for Export Bots.



The audit details are divided in two parts - **Action Details** and **Export Bot Details,**

- The Export Bot Files Details include the Package Name, Package Encryption if password has been set while exporting the bot, Exported Bot name with filepath, and Exported Dependency name with file path.
- The list number of the Bot and dependency is appended inside a bracket beside each bot. All user selected items are listed, followed by list of dependencies of the bots which are added by the system and exported.

Import bots

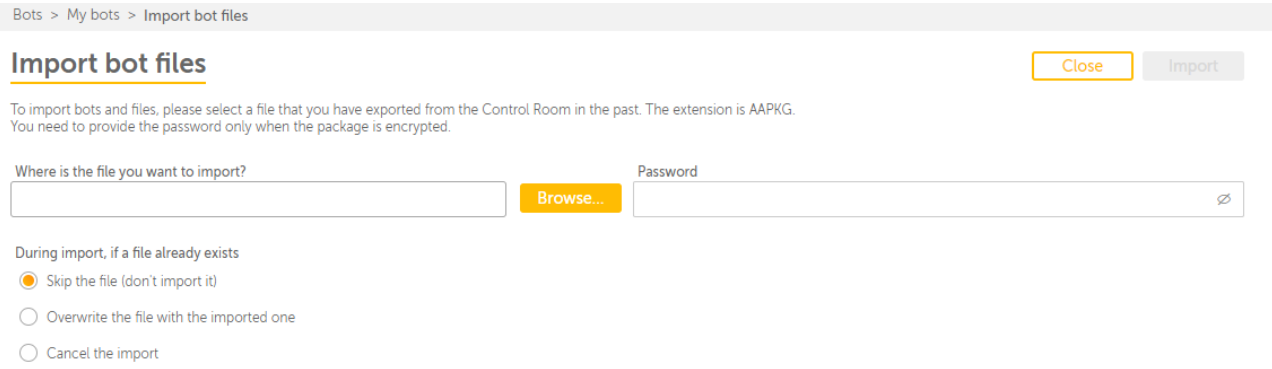
As a Control Room user with BLM Import module permission, and Upload privileges for Tasks, MetaBots, Docs, Workflows, and Reports, you can import bots and dependent files that were exported by another Control Room user in different automation environments to help manage your organization's Bot Lifecycle Management (BLM).

Refer Export bots for details on exporting a BLM package.

Import bot files - version control disabled

To import bot files,

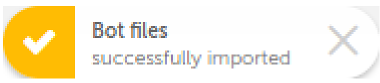
1. Go to **Bots** → **My Bots** page
2. Click Import bot files...
3. This launches the **Import bot wizard** page wherein you must select the package file that was exported by another Control Room user:



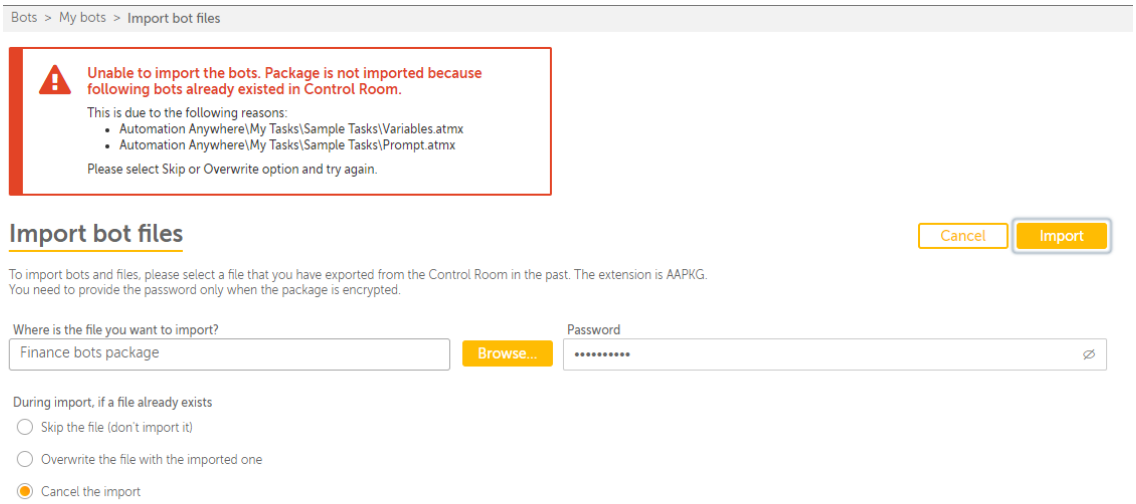
4. To select the file, click Browse...
5. Go to the source folder where the exported package was stored and/or shared by the Control Room user with **Export Bots** privileges.
6. Select the required package - it has an **AAPKG** extension.
7. If encrypted, provide the same password that was used for export from source Control Room.
8. If some of the files that are being imported from the package are already available in the Control Room, you can choose to,
   - **Skip the file(s)** and not import the duplicate files
   - **Overwrite the existing files** with the imported ones
   - **Cancel the import** action.

     ```
     Note: When you use this option, the entire import operation is canceled and if at least one
     file already exists in Control Room. In this case, no bots will be imported into Control
     Room.
     ```

   - When you select **Skip**... or **Overwrite**... options, and click Import the files are successfully imported:

   - However, when you select **Cancel**... and click Import, you are prompted to select either of the above options:

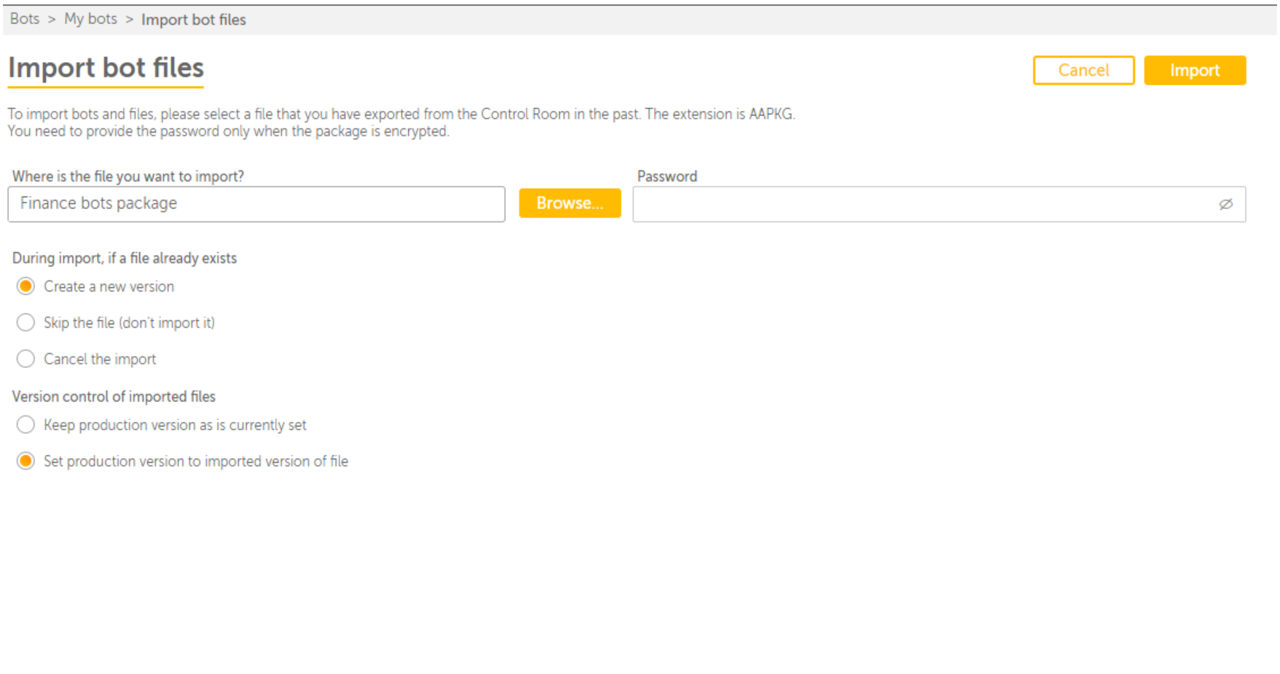


9. Once the bots are imported successfully, you return to the **My Bots** page.

Import bot files - version control enabled

To import bot files,

1. Go to **Bots** → **My Bots** page
2. Click Import bot files...
3. This launches the **Import bot files wizard** page wherein you must select the file that was exported by another Control Room user:



4. To select the file, click Browse...
5. Go to the source folder where the package was exported and/or shared by the Control Room user with **Export Bots** privileges.
6. Select the required package - it has an **AAPKG** extension.
7. If encrypted, provide the same password that was used for export from source Control Room.
8. If some of the files that are being imported from the package are already available in the Control Room, you can choose to,
   - **Create a new version** of files. A new version is created in the destination Control Room irrespective of version control - whether enabled or not in the source Control Room.

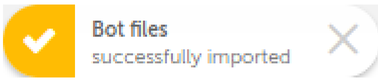
> **Note:** If the bot being imported is already present in the destination Control Room and does not have any updates, a new version of the bot will not be created.

- **Skip the file** and do not import the file. This means that there will be no change in the file of the destination Control Room
- **Cancel the import** action.

> **Note:** When you use this option, the entire import operation is canceled and if at least one file already exists in Control Room. In this case, no bots will be imported into Control Room.

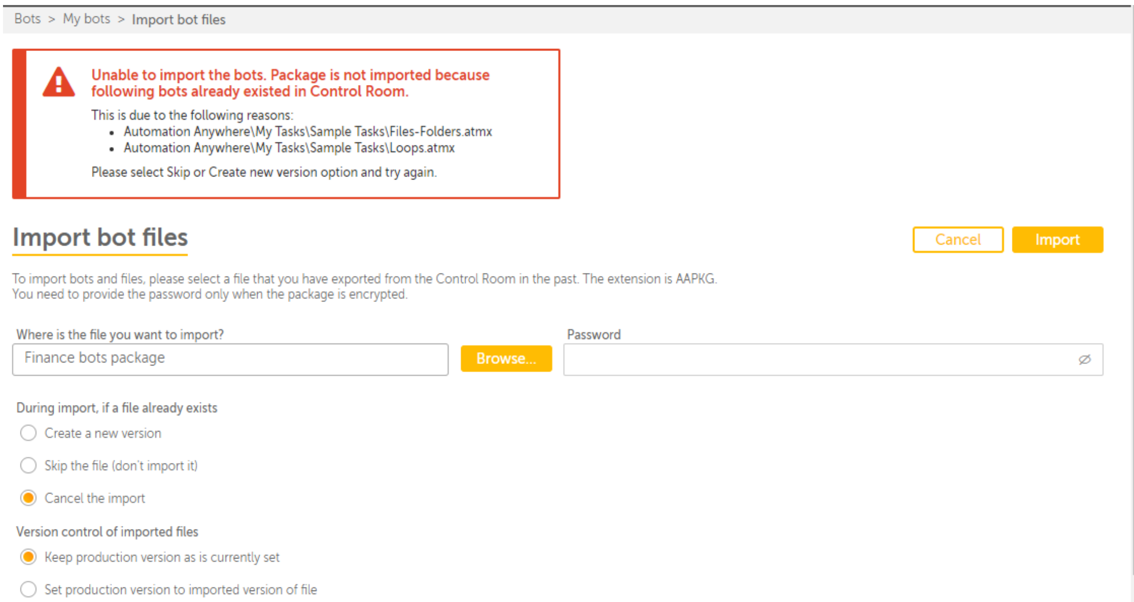
9. You must choose the production version type,
    - Keep production version as is currently set - The system will not make any change in the production versions of the imported bots and dependencies.
    - Set production version to imported version of file - The latest (imported) versions are set as production versions for all the imported bots and dependencies.
        - When you select **Skip**... or **Create**... options, and click 

the files are successfully imported:



        - However, when you select **Cancel**... and click 

, you are prompted to select either of the above options:



10. Once the bots are imported successfully, you return to the **My Bots** page.

> **Tip:** You can also click 

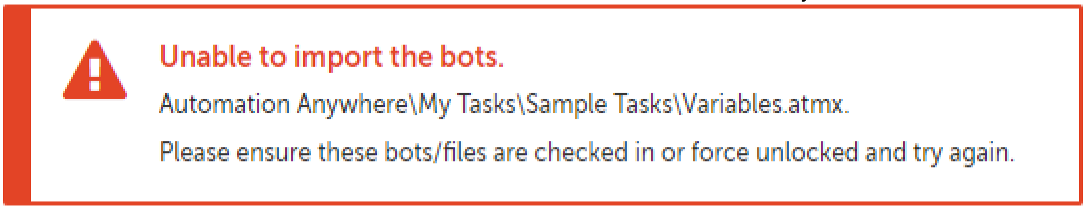
, if you do not wish to continue with the file import at any stage of the import process.

> **Note:** If the **Email settings** are enabled for Export and Import operations of a BLM package, an email notification is sent to the user who performs import whether the action succeded or failed.

Import bots - Validations

When you import bot files, the system checks for following validations during import:

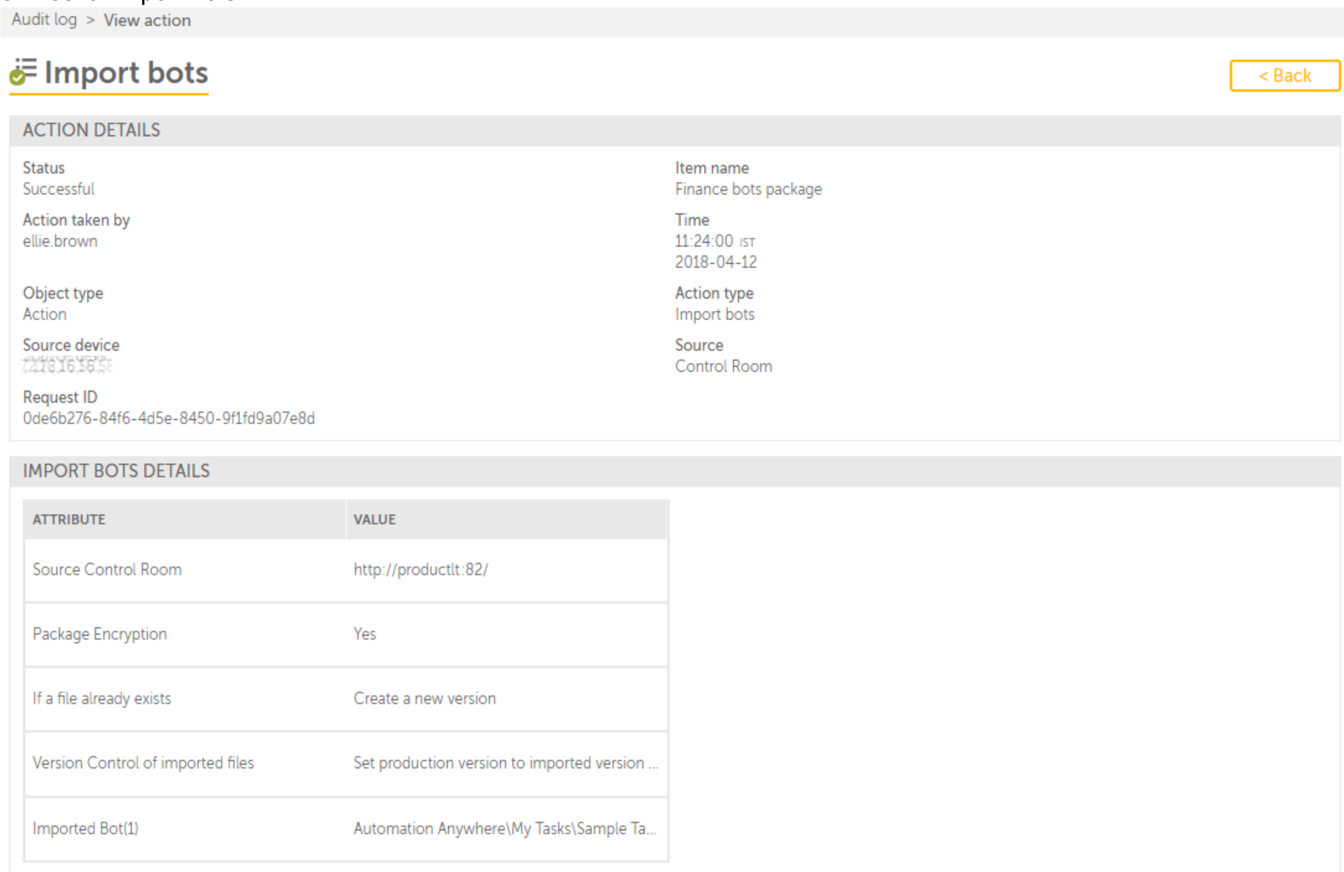
- Whether bot or dependent file already exists in Control Room
- Whether a file is locked if version control is enabled. If this validation fails, you are shown:



You can fix this issue from the Control Room using **Unlock bot** or from the Client using **Checkin** option.

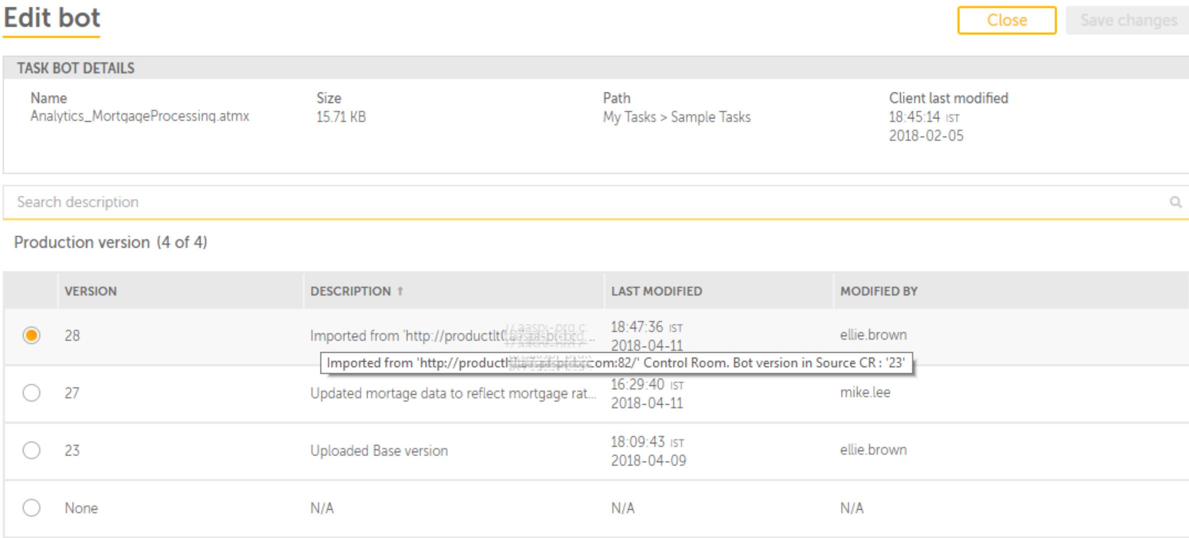
Audit Logs

An audit entry is logged in the Control Room **Audit Log** page when you import bots. The illustration below shows the detailed audit entries for Import Bots.

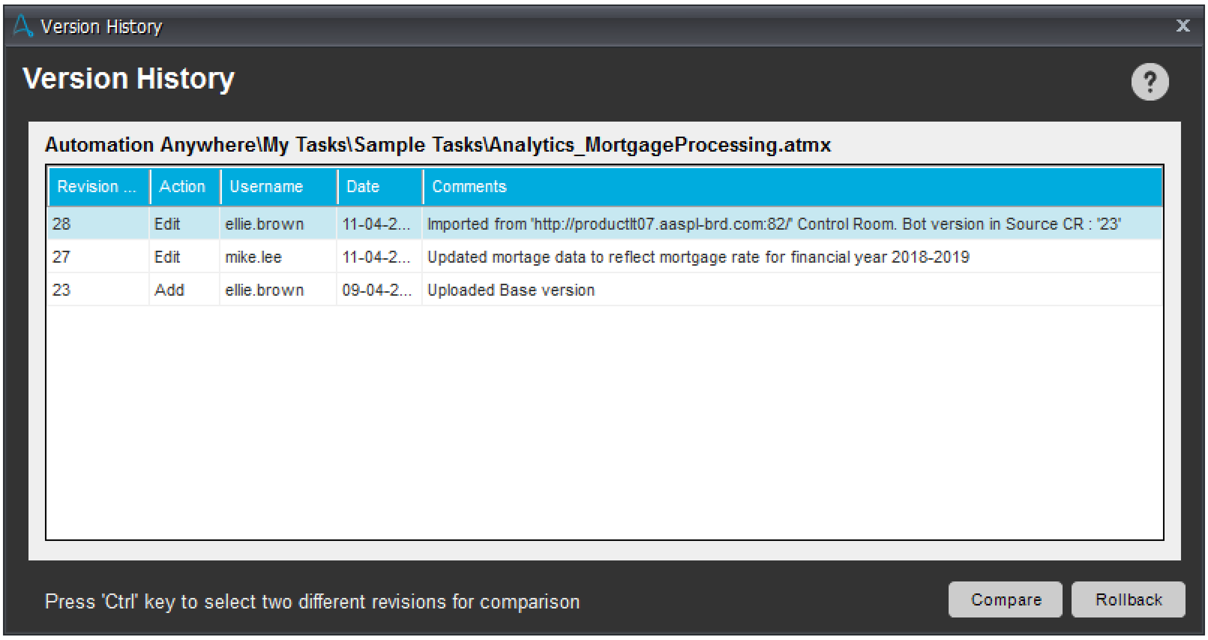


The audit details are divided in two parts - **Action Details** and **Import Bot Details** :

- The Import Bot Details include the Package Name, Package Encryption if password has been set while exporting the bot, Imported Bot name with filepath, and Imported Dependency name with file path.
- The list number of the Bot and dependency is appended inside a bracket beside each bot. All user selected items are listed, followed by list of dependencies of the bots which are added by the system and imported.
- When Version Control is enabled, the source Control Room version of each item in the list are displayed and the version number is appended towards the end of the file.
  - If you want to know from which Control Room a bot was imported with its version number, you can track it through version history in the **Edit bot** page



- Alternatively, if you want to know from which Control Room a bot was imported with its version number, you can also track it through the **Version History** in the Automation Anywhere Enterprise Client:



Activity - Overview

If you have **View everyone's In progress activity, View my scheduled bots, and View my bots** privileges, the Activity page of Control Room allows you to perform tasks, such as viewing activities that are scheduled and are in progress. At the same time, it allows you to view a historical chronology of activities performed on a bot using the Historical Activity page. You can perform the following tasks using this page.

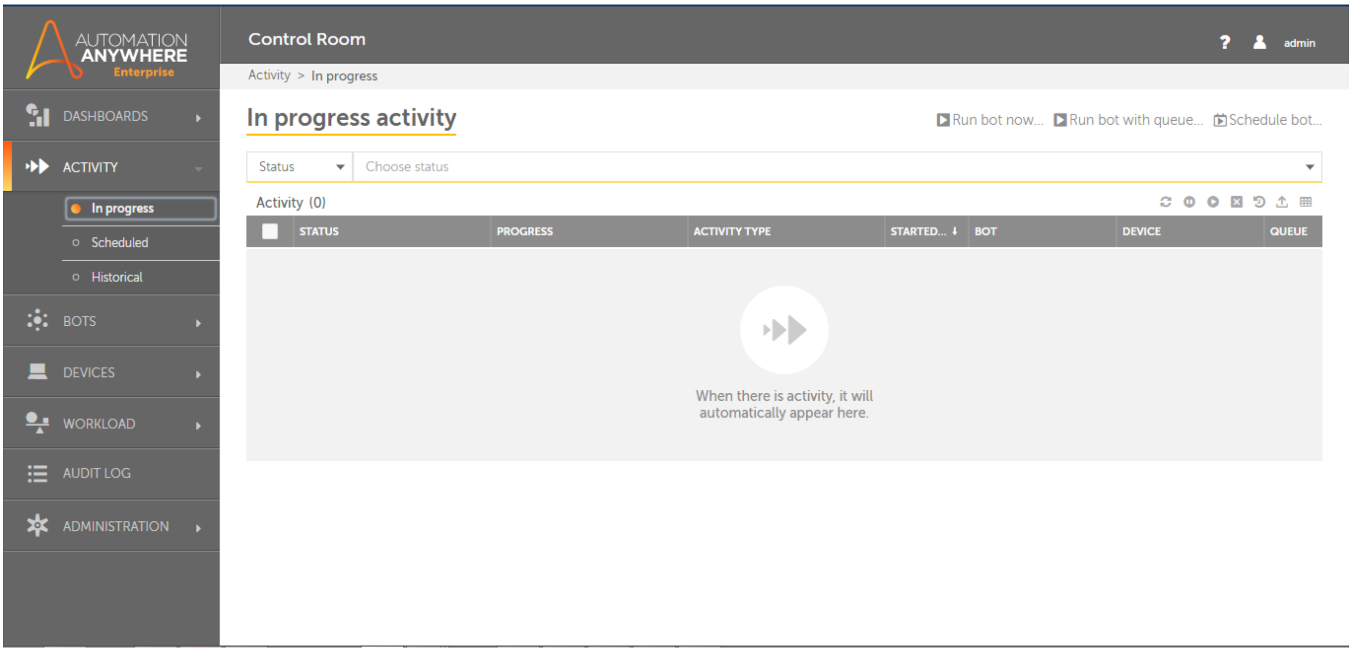
- Run a bot
- Schedule a bot
- Run a bot with queue
- Edit a scheduled bot
- Delete a schedule
- Activate or Deactivate a schedule
- View scheduled activities
- View in-progress activities

In progress activity page

The **In progress activity** page displays a live status of all the on-going activities for Control Room. Depending on your privileges, you can manage one or more automation activities using a pause, stop, or resume operation.

By default, you will be able to monitor and manage all the ongoing automation which has been triggered or scheduled by you. If you have “View my in-progress activity” permission, you can also manage and monitor all the ongoing automations on the bots where you have either of Upload, Download or Delete permission.

The default page is illustrated in the following figure.

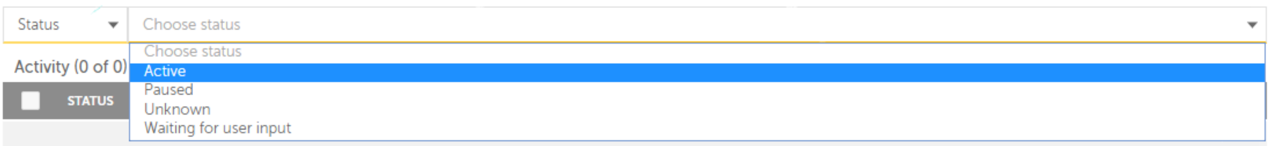


For ease of access, you can apply search parameters to Status, Activity Type, Bot, Queue, Device, and Item Name columns.

- You can use specify the search parameters in the search bar for Bot, Queue, Device, and Item Name:

Note: When you specify search parameters for the same column, the system searches using **OR** operator. When you specify search parameters for different columns, the system searches using **AND** operator.

- You can choose the search parameters from a list in the search bar for Status and Activity Type:



The items of the **Activity** table are described in the following table.

Tip: You can perform the following actions on a column to help you work efficiently.

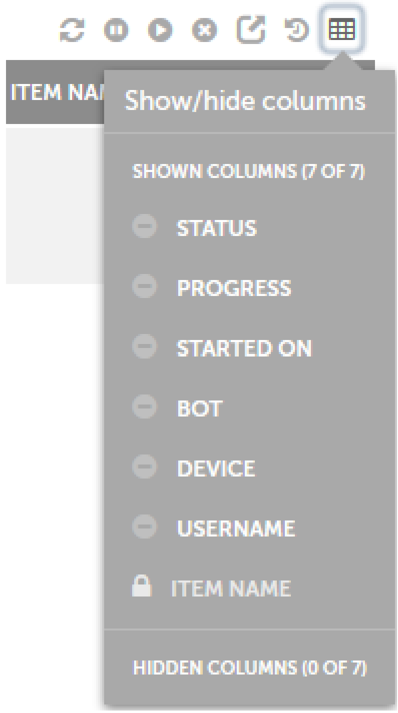
- Click a column to sort it in ascending and descending order. You can sort up to three columns by holding the Shift key when you click two or more columns. This gives you the option of sorting two additional columns. This way the sorting is done on the entire table and not just the data that is currently visible to you. The last sorting is stored in memory applied by a user per session.
- Use a drag-and-drop operation to move the column left or right.
- Move your mouse cursor at the end of the column and drag to re-size.

Table Item	Description
Status	Whether the status of the activity is: • **Active** (In progress) **-** This is shown when the bot is being run on Bot machine • **Paused -** This is shown when the bot is paused either from Control Room or Device. • **Unknown -** This is shown when the bot fails to run reasons that are not known. • **Waiting for user input -** This is shown when the bot is paused and requires an input from the Device user.
Progress	The progress of the activity in percentage.
Started on	The time at which the activity was started. This is of the format HH:MM:SS YYYY-MM-DD.
Bot	The name of the bot.
Device	The device on which the activity is running.
UserName	The Control Room user account used for running the automation on a remote Bot runner.
Item Name	The name of the automation.

You can also perform the following table-level actions for a set of multiple activities.

Note: These actions can be performed only at a table-level and not on individual items.

Table Item	Description
Refresh	Refreshes the activities listed in the table
Pause in progress activities	Pauses any activity being performed on the bot
Resume in progress activities	Resumes any paused activity being performed on the bot
Stop in progress activities	This stops all activities of the bot regardless of the stage it is in.
Export in progress activities	Exports the list of items in the Activity table in CSV format
Move to History	Moves the selected activity to history
Show/hide columns	When you click this icon, the list of available columns is displayed, as shown in the following figure. Select or deselect an item to add or remove a column.



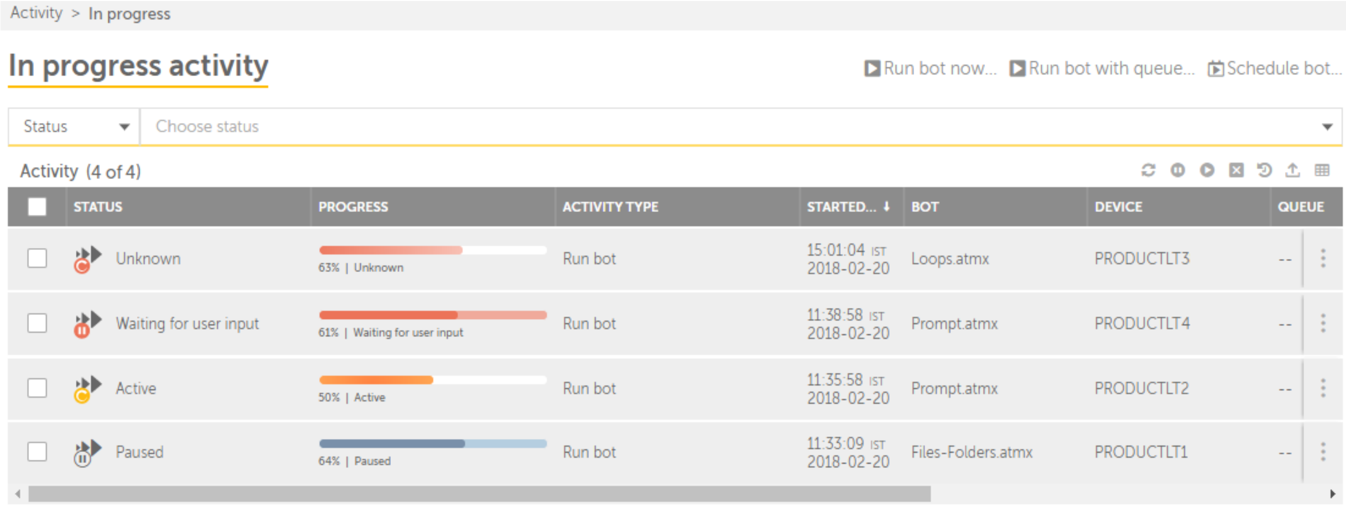
You can perform the following tasks on an individual activity.

Table Item	Description
View in progress activity	Select this to view details of the activity
Pause in progress activity	Select this to pause the activity
Resume in progress activity	Select this to resume the activity that was paused. This is visible only when you pause the activity
Stop in progress activity	Select this to stop the activity
Move in progress activity	Select this to move the activity to Historical Activity page

View in progress activity details

As a Control Room admin or a user with **View everyone's In progress activity** privilege, you can view the progress details of activities that are currently being executed in real time.

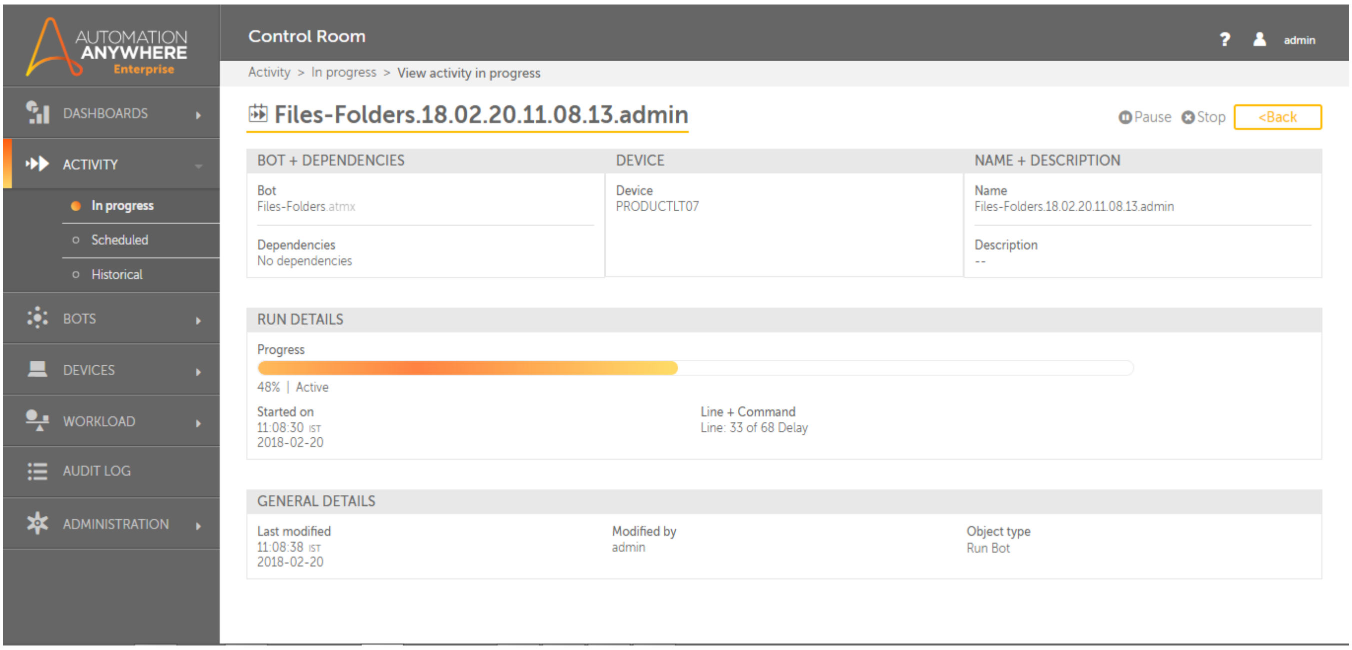
You can access the **In progress activity** page by logging on to Control Room and click **Activity** → **In Progress**. The in progress activities with different status is illustrated in the following figure.



In progress details

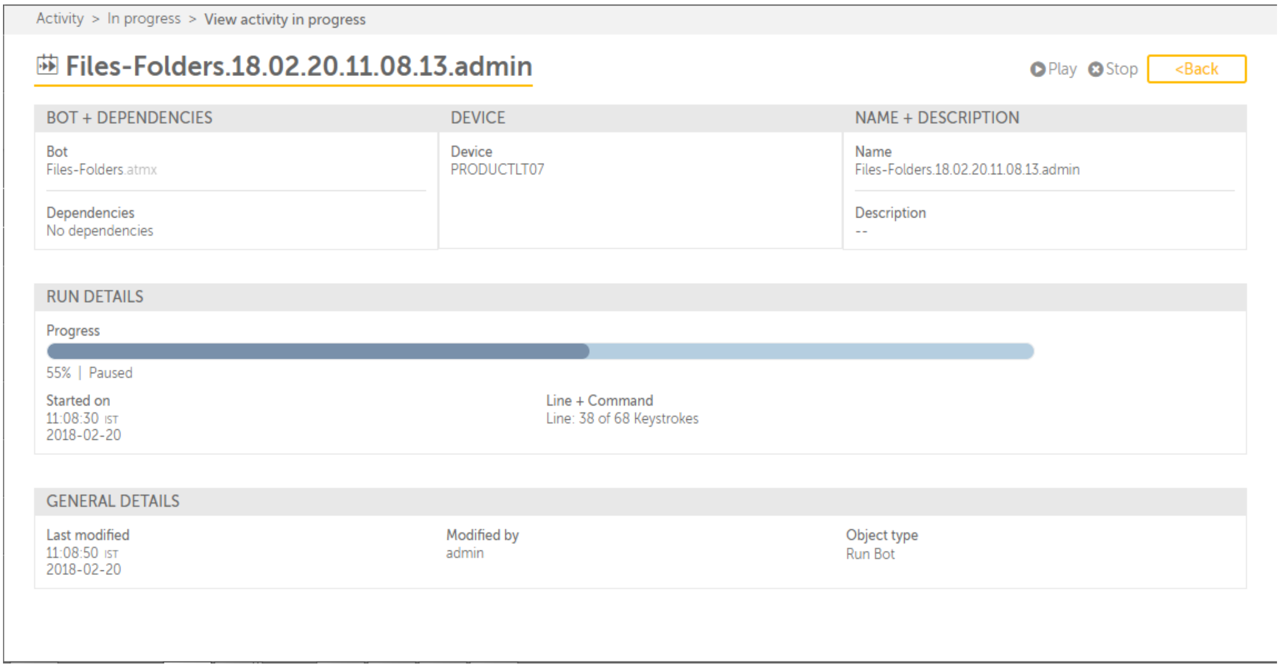
To view in progress activity details,

1. Go to **Activity** → **In Progress**
2. Mouse over an activity
3. Click
4. The following page is launched:

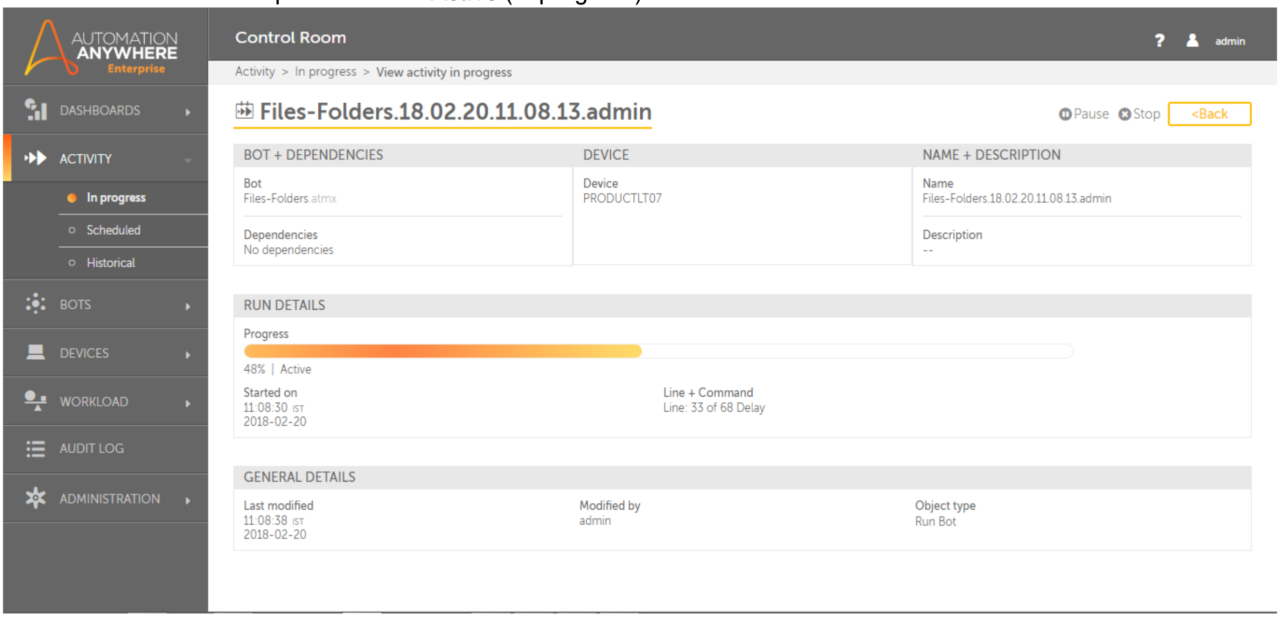


Here, you can choose to Pause, Play, Stop or Move the activity to historical activity page.

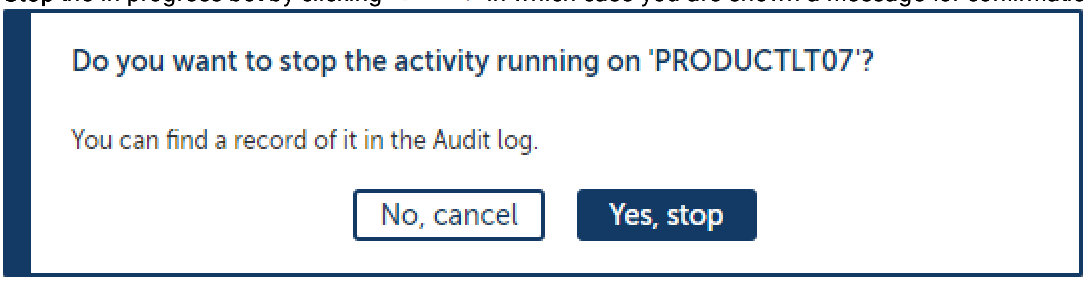
1. Click Play to run a bot that is **Paused**:



2. Click Pause to interrupt a bot that is **Active** (In progress):

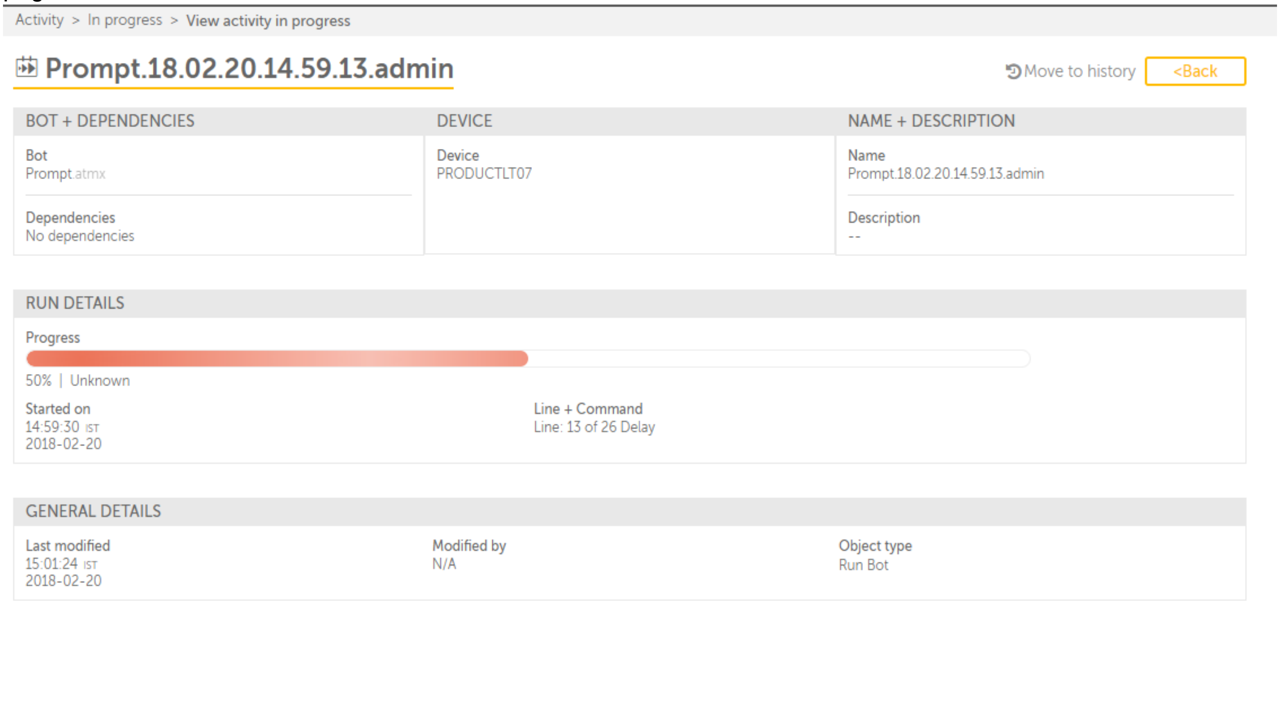


3. **Stop** the in progress bot by clicking Stop in which case you are shown a message for confirmation:



   1. Click Yes, stop to return to the **In progress** page.
   2. Click No, Cancel to return to the **View activity in progress** details page.

4. Click Move to history to remove the activity that is in Unknown status from the **In progress activity** page to **Historical activity** page



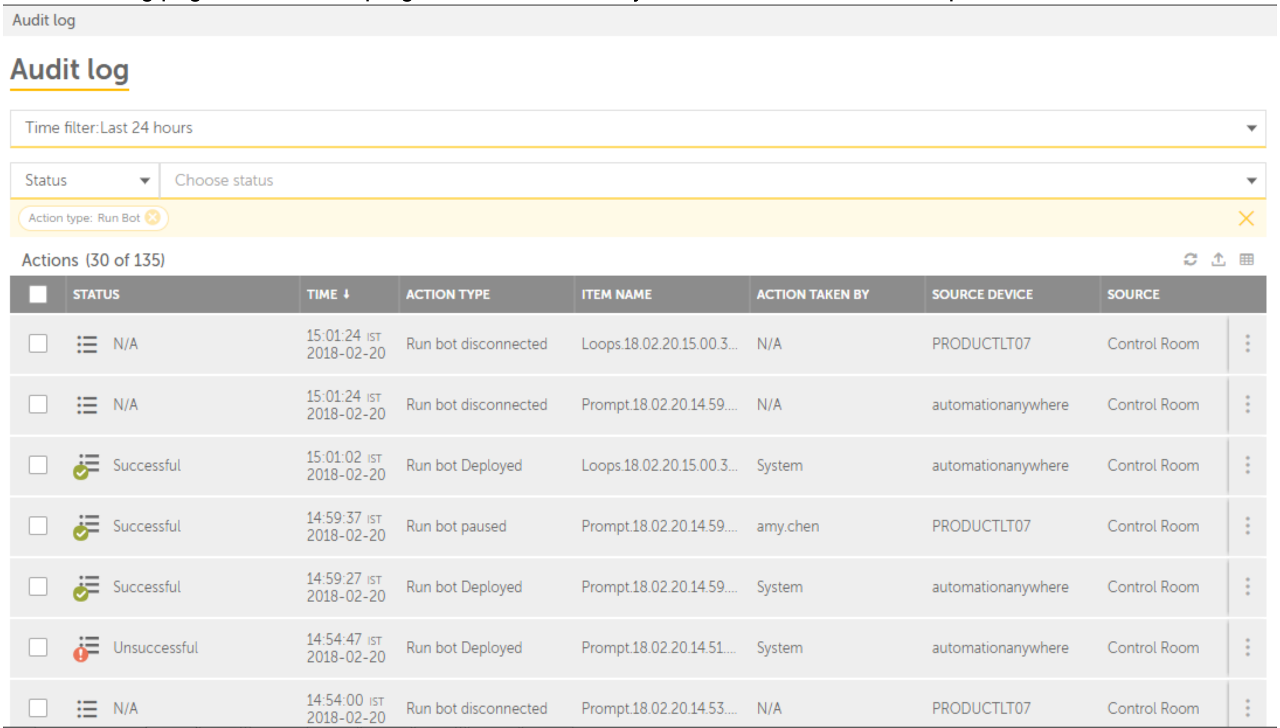
Note: You cannot **Pause**/**Resume** or **Stop** an automation that has queues from the **View activity in progress** page. You can do that from the **Workload** → **Queues** page by using the **View Automation** option. Refer Manage work items for details.

The different areas of the **View in progress activity** page are described in the following table.

Area	Description
BOT + DEPENDENCIES	The name of the bot and dependencies for the scheduled bot.
DEVICES	The name of the device connected to the bot.
NAME + DESCRIPTION	The name and description for the activity. By default, this displays the Bot name, date, time, and name of the person who ran the bot.
RUN DETAILS	The run details for the bot which include: • **Progress -** The bot progress in percentage • **Status -** Active, Paused, Unknown or Waiting for user input • **Started on -** The date and time when the bot was executed • **Line + Command -** The current line number and command name of that line
GENERAL DETAILS	The details for the bot execution which include: • **Last modified -** The last date and time the bot was modified. • **Modified by -** The name of the user who last made changes to the bot. • **Object type -** The type of object of the bot, such as Run Bot.

Audit Details

- The Audit Log page shows the In progress activities when you use the **Run bot now...** option:


Audit log

Audit log

Time filter:Last 24 hours

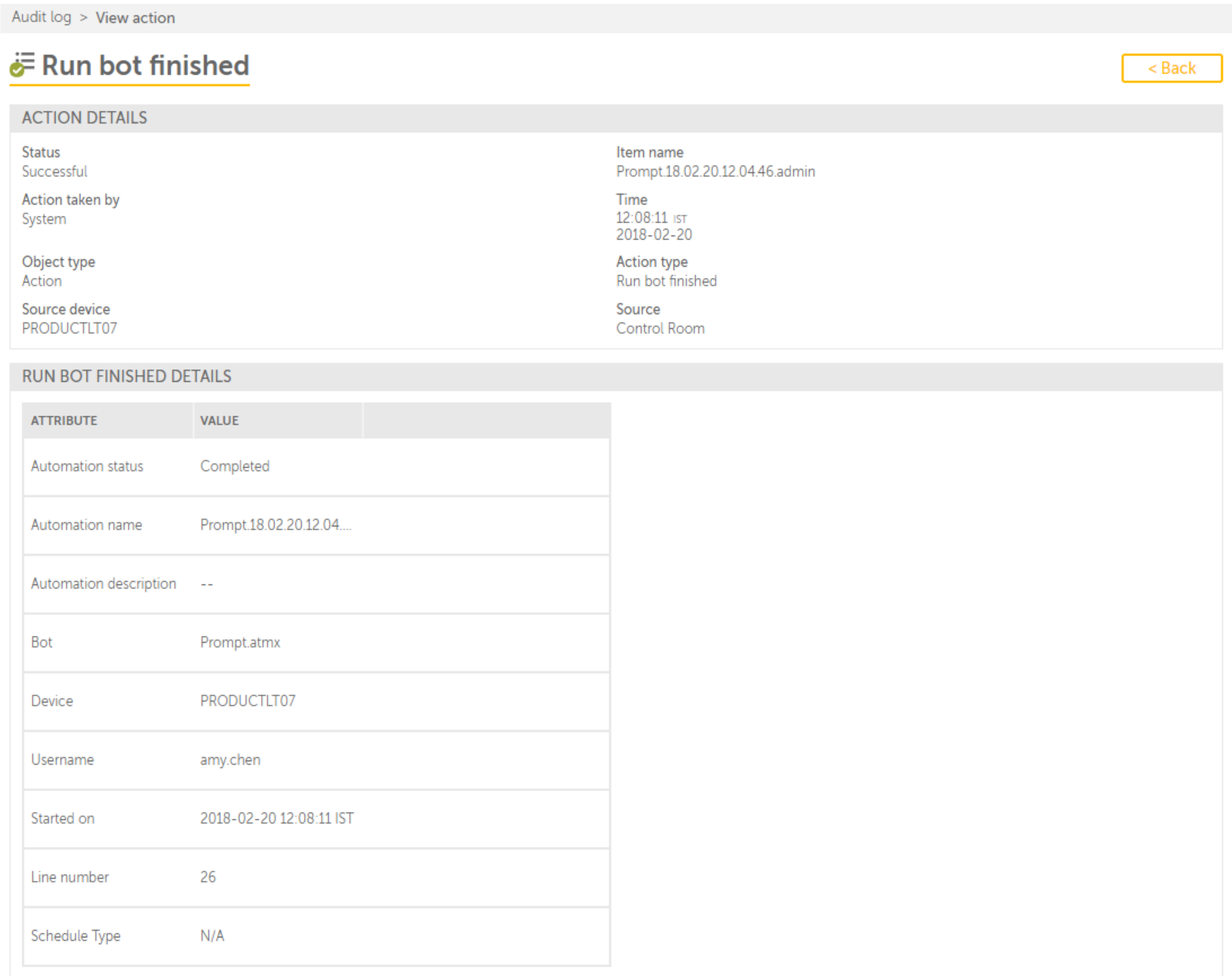
Status | Choose status

Action type: Run Bot

Actions (30 of 135)

STATUS	TIME	ACTION TYPE	ITEM NAME	ACTION TAKEN BY	SOURCE DEVICE	SOURCE
N/A	15:01:24 IST 2018-02-20	Run bot disconnected	Loops.18.02.20.15.00.3...	N/A	PRODUCTLT07	Control Room
N/A	15:01:24 IST 2018-02-20	Run bot disconnected	Prompt.18.02.20.14.59....	N/A	automationanywhere	Control Room
Successful	15:01:02 IST 2018-02-20	Run bot Deployed	Loops.18.02.20.15.00.3...	System	automationanywhere	Control Room
Successful	14:59:37 IST 2018-02-20	Run bot paused	Prompt.18.02.20.14.59....	amy.chen	PRODUCTLT07	Control Room
Successful	14:59:27 IST 2018-02-20	Run bot Deployed	Prompt.18.02.20.14.59....	System	automationanywhere	Control Room
Unsuccessful	14:54:47 IST 2018-02-20	Run bot Deployed	Prompt.18.02.20.14.51....	System	automationanywhere	Control Room
N/A	14:54:00 IST 2018-02-20	Run bot disconnected	Prompt.18.02.20.14.53....	N/A	PRODUCTLT07	Control Room

- The audit details are shown as:


Audit log > View action

Run bot finished

< Back

ACTION DETAILS

Status
Successful

Action taken by
System

Object type
Action

Source device
PRODUCTLT07

Item name
Prompt.18.02.20.12.04.46.admin

Time
12:08:11 IST
2018-02-20

Action type
Run bot finished

Source
Control Room

RUN BOT FINISHED DETAILS

ATTRIBUTE	VALUE
Automation status	Completed
Automation name	Prompt.18.02.20.12.04....
Automation description	--
Bot	Prompt.atmx
Device	PRODUCTLT07
Username	amy.chen
Started on	2018-02-20 12:08:11 IST
Line number	26
Schedule Type	N/A

Historical activity page

The **Historical activity** page chronologically displays a list of all activities that have occurred. This page lists all the activities, which have finished running - successfully or unsuccessfully completed. For example, there may be scenarios where an activity failed to run and you can use this page to come back and check the status of the activity.

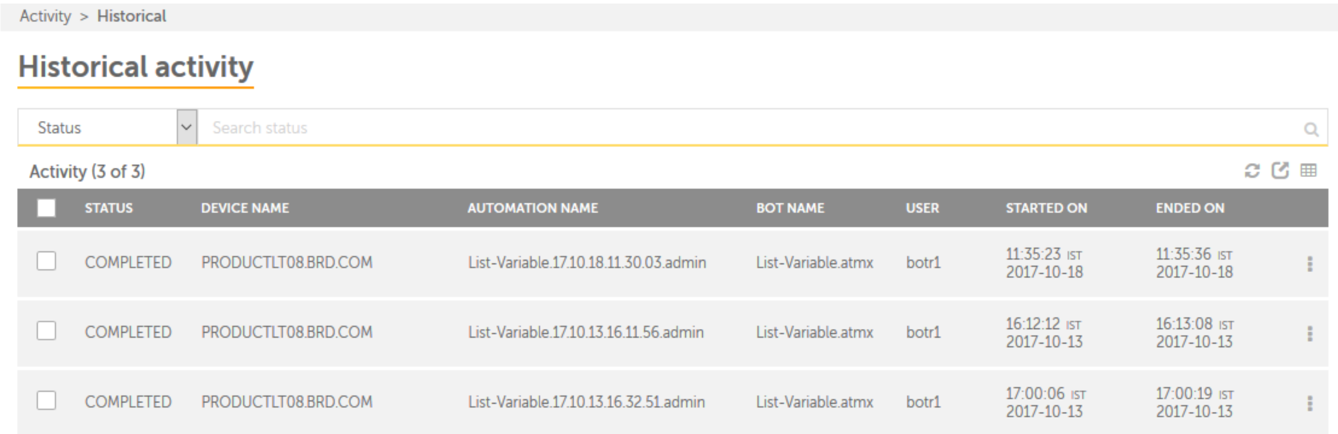
To view this page, you should have **View my in-progress activity** or **View everyone's in-progress activity** permission.

- If you have **View my in-progress activity** permission, you should be able to see all the completed automations that you deployed or scheduled.
- If you have **View everyone's in-progress activity**, you should be able to see all the automations run or scheduled by other users.

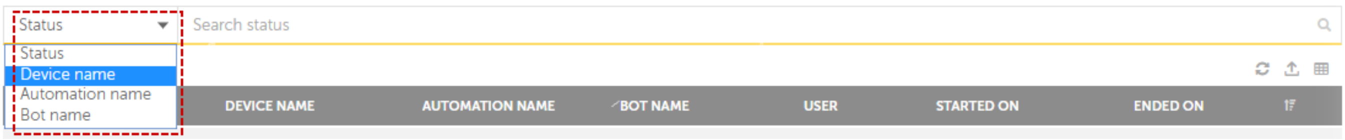
> **Note:** You must have **Run/Schedule** permission on the corresponding bot to be able to see the activity here.

Refer Create a role for details on role description.

You can use this page to run the activity again and perform other tasks, such as export the data in the table in CSV format, show/hide columns, or refresh the list in the table. The page is illustrated in the following figure.



For ease of access, you can apply search parameters to Status, Device Name, Automation Name, and Bot Name columns in the search bar.



> **Note:** When you specify search parameters for the same column, the system searches using **OR** operator. When you specify search parameters for different columns, the system searches using **AND** operator.

The items of the **Activity** table are described in the following table.

> **Tip:** You can perform the following actions on a column to help you work efficiently.
>
> - Click a column to sort it in ascending and descending order. You can sort up to three columns by holding the Shift key when you click on two more columns. This gives you the option of sorting two additional columns. This way the sorting is done on the entire table and not just the data that is currently visible to you. The last sorting is stored in memory applied by a user per session.
> - Use a drag-and-drop operation to move the column left or right.
> - Move your mouse cursor at the end of the column and drag to re-size.

Item	Description
Status	The status of the activity. This may be Unknown, Completed, Failed, Stopped, or Time Out.
Device name	The name of the Bot runner machine on which automation was running.
Automation name	The name of the automation.
Bot name	The name of the bot.
User	The name of the user under whose account that particular activity/automation was running on the device.
Started on	The date and time on which the activity was started.
Ended on	The date and time on which the activity was completed.

You can perform the following tasks on an individual item in the **Historical activity** page.

Action	Description
View	Allows you to view details of the activity.
Run bot	Allows you to Run the selected Bot. **Tip:** Move your mouse over the Actions icon and click the Run icon to run the activity again. Clicking the Run icon opens the **Run bot now** page with all the values of the bot populated. You can then make changes to the bot and run the bot again.

You can also perform the following table-level actions for a set of multiple activities.

Note: These actions can be performed only at a table-level and not on individual items.

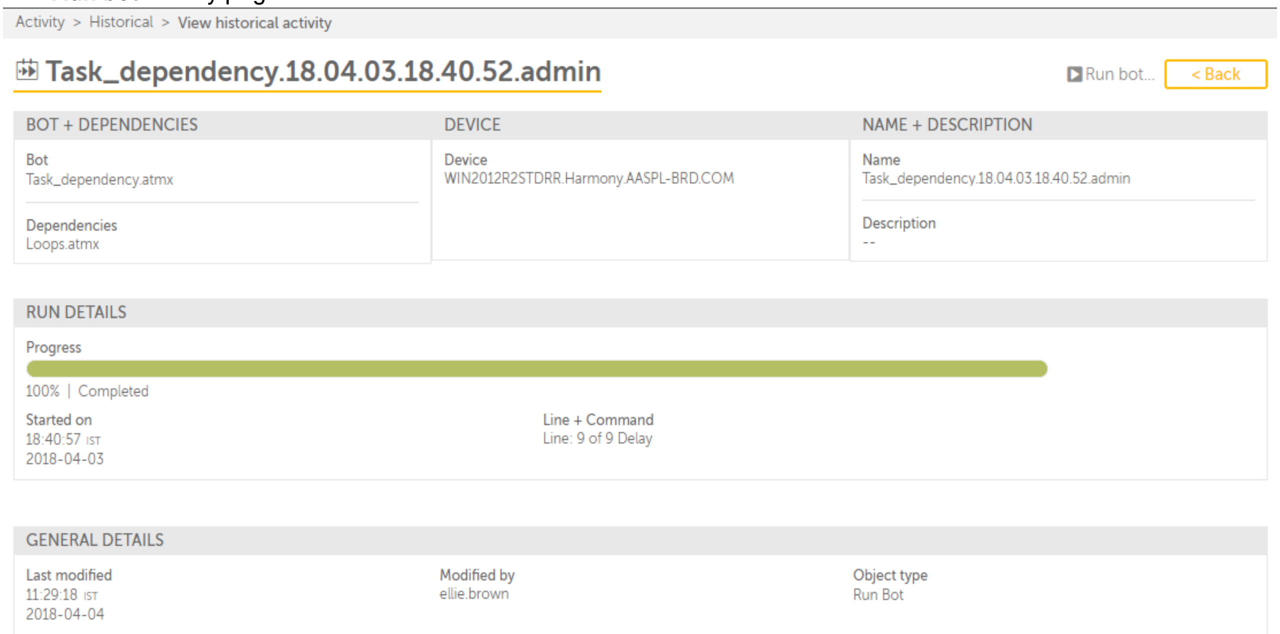
Table Item	Description
Refresh	Refreshes the table
Export to CSV	Export the selected items in the table in CSV format
Show/Hide columns	Select the columns to show in the table.

View details of selected activity from history

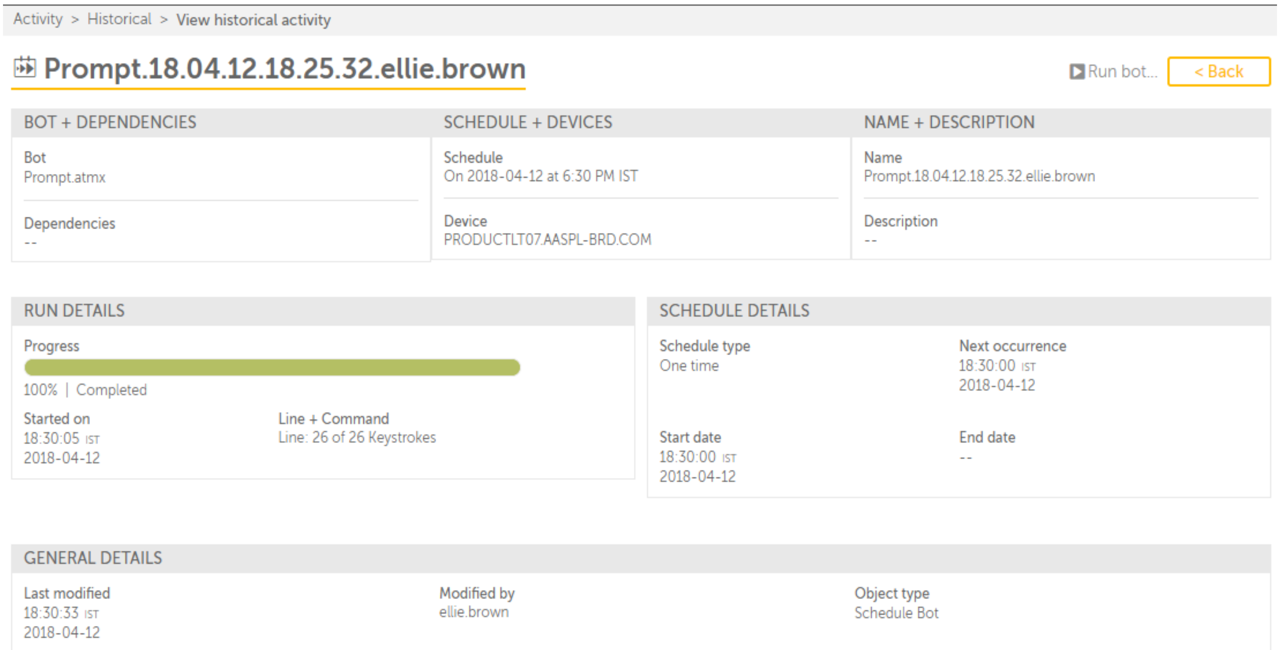
As a user with access privileges to the Historical activity, when you click the **View** icon for an activity, the **View historical activity** page is opened. It provides information in three sections - Details of activity such as Bot + Dependencies, Device, Name + Description of activity, Run details, and General details. Besides this, you can also run the bot again from this page.

The page shows details based on the activity type,

- The **Run bot** activity page is illustrated below:

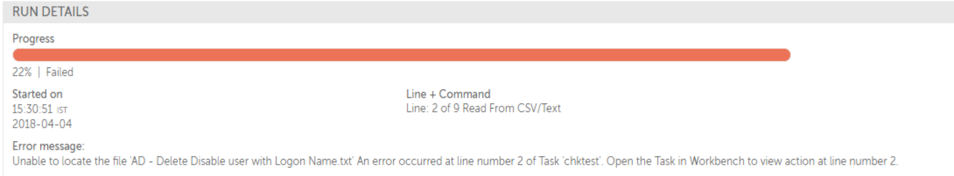
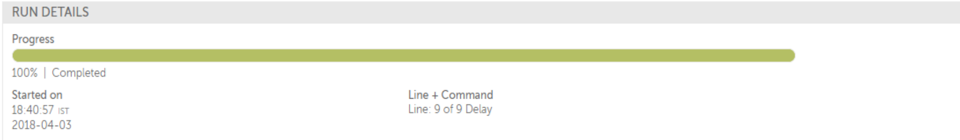


- The **Schedule a bot** activity page is illustrated below:



The different sections of the **Historical activity view details** page are described in the following table.

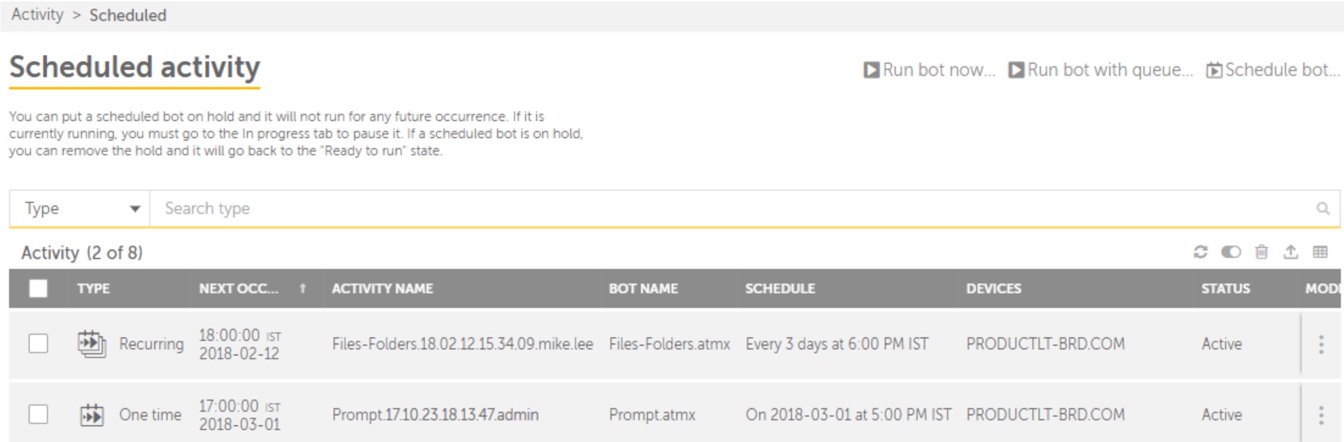
Area	Description
Bot + Dependencies	Displays the Bot name as well as name of its dependent bots or files.
Device	Displays the device name of the source Control Room from which the Bot was deployed
Run Details	• **Progress:** Displays color coded progress in automation,

	• **Red** - when automation fails or is stopped with error message  • **Green** - when automation is completed  • **Percentage** of automation completed, stopped or failed
Schedule Details	This tab is visible only if the bot is deployed using **Schedule a bot** operation. • **Schedule type:** Displays the type of schedule used to deploy the bot. For example, Run once. • **Next occurrence:** Displays the next schedule run date + time • **Start/End date:** Displays the schedule start and end date + time
General details	Displays following details, • **Last Modified:** Displays the last time changes were made to the folder in date and time. • **Modified by:** Displays the name of the user who last made changes to the folder in date and time. • **Object type:** Displays the activity type - Run Bot or Schedule Bot

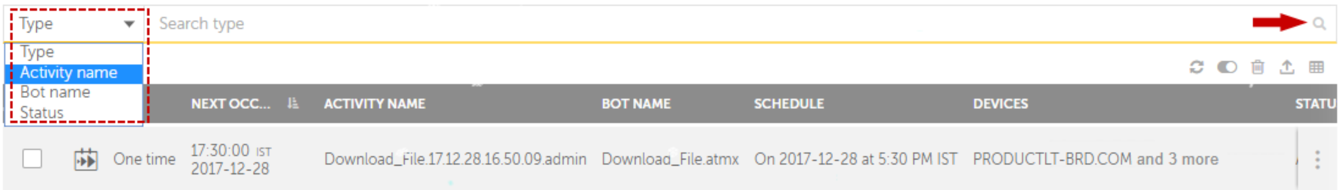
Scheduled activity page

The **Scheduled Activity** page displays a list of activities that have been scheduled for a later time (future) in an **Activity** table. If you have **View my scheduled bots,** and **View my bots** privileges, you can perform tasks, such as edit, view, activate, deactivate, or delete the schedule.

You can access the **Scheduled activity** page by logging on to Control Room and click **Activity** → **Scheduled**. The page is illustrated in the following figure.



For ease of access, you can apply search parameters to Type, Activity Name, Bot Name, and Status columns in the search bar.



Note: When you specify search parameters for the same column, the system searches using **OR** operator. When you specify search parameters for different columns, the system searches using **AND** operator.

The items of the **Activity** table are described in the following table.

Tip: You can perform the following actions on a column to help you work efficiently.

- Click a column to sort it in ascending and descending order. You can sort up to three columns by holding the Shift key when you click on two more columns. This gives you the option of sorting two additional columns. This way the sorting is done on the entire table and not just the data that is currently visible to you. The last sorting is stored in memory applied by a user per session..
- Use a drag-and-drop operation to move the column left or right.
- Move your mouse cursor at the end of the column and drag to resize.

Table Item	Description
Type	The type of schedule. For example, One time or recurring.
Next occurrence	The next time the scheduled bot will run.
Activity name	The name of the activity. For example, List files in a folder, loops.
Bot Name	The name of the bot. For example, monthly-payroll.atmx
Schedule	The description of when the activity will run. For example, every Monday at 3 PM
Devices	The devices on which the bot will run at the scheduled time.
Status	The Status of the scheduled activity. For example, active or inactive.

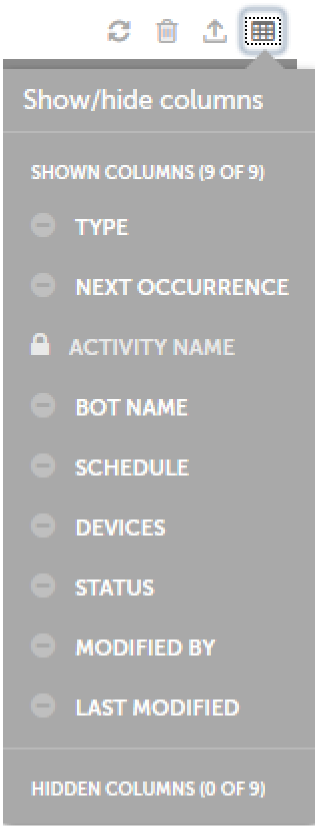
Modified by	The name of the user who last modified the activity.
Last modified	The date and time when the activity was last modified.

You can perform the following tasks on an individual Schedule by moving your mouse over the Actions icon.

Item	Description
Edit	Click this icon to Edit the scheduled bot .
View	Click this icon to View details about the scheduled bot.
Activate / Deactivate	Click this icon toactivate or deactivate the scheduled bot.
Delete	Click this icon to delete the scheduled bot.

You can also perform the following table-level actions for a set of multiple activities.

Note: These actions can be performed only at a table-level and not on individual items.

Table Item	Description
Refresh	Refreshes the schedules page
Activate / Deactivate Activities	Activates or deactivates the schedules.Learn More
Delete	Deletes the schedules.Learn More
Export	Export the selected schedules in CSV format.
Show/Hide column	Select the columns to show or hide in the **Activity** table. **Tip:** Click the or icons to add or remove items in the table. 

Schedule a bot

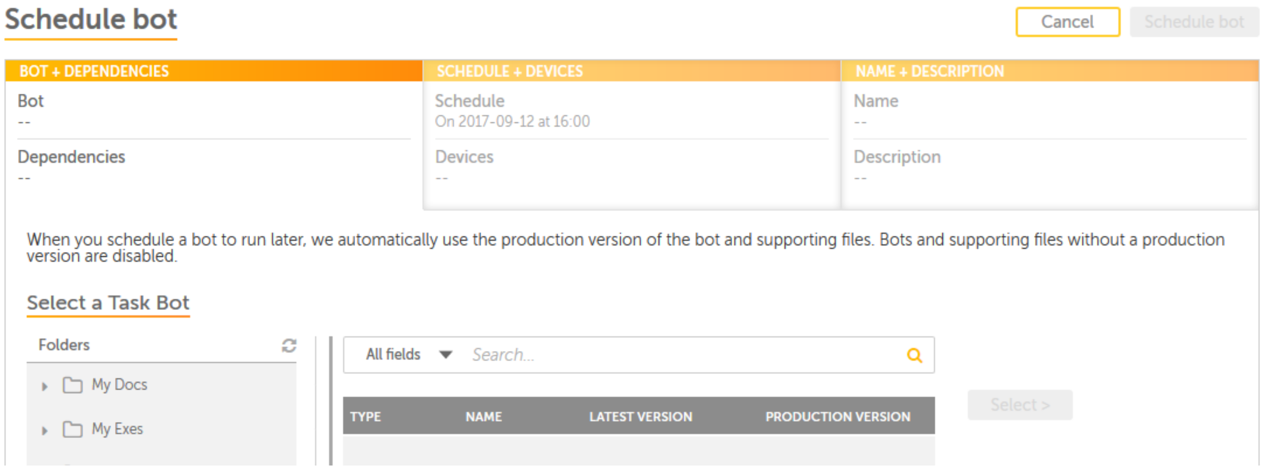
There may be times when you want to run a bot at a later point in time (future) or when you want the bot to run on a periodic basis or at a specific point in time. In such cases, use the **Schedule bot** page to perform such tasks.

Note: You can schedule a bot from any of the following pages of Control Room if you have **View everyone's In progress activity, View my scheduled bots, and View my bots** privileges:

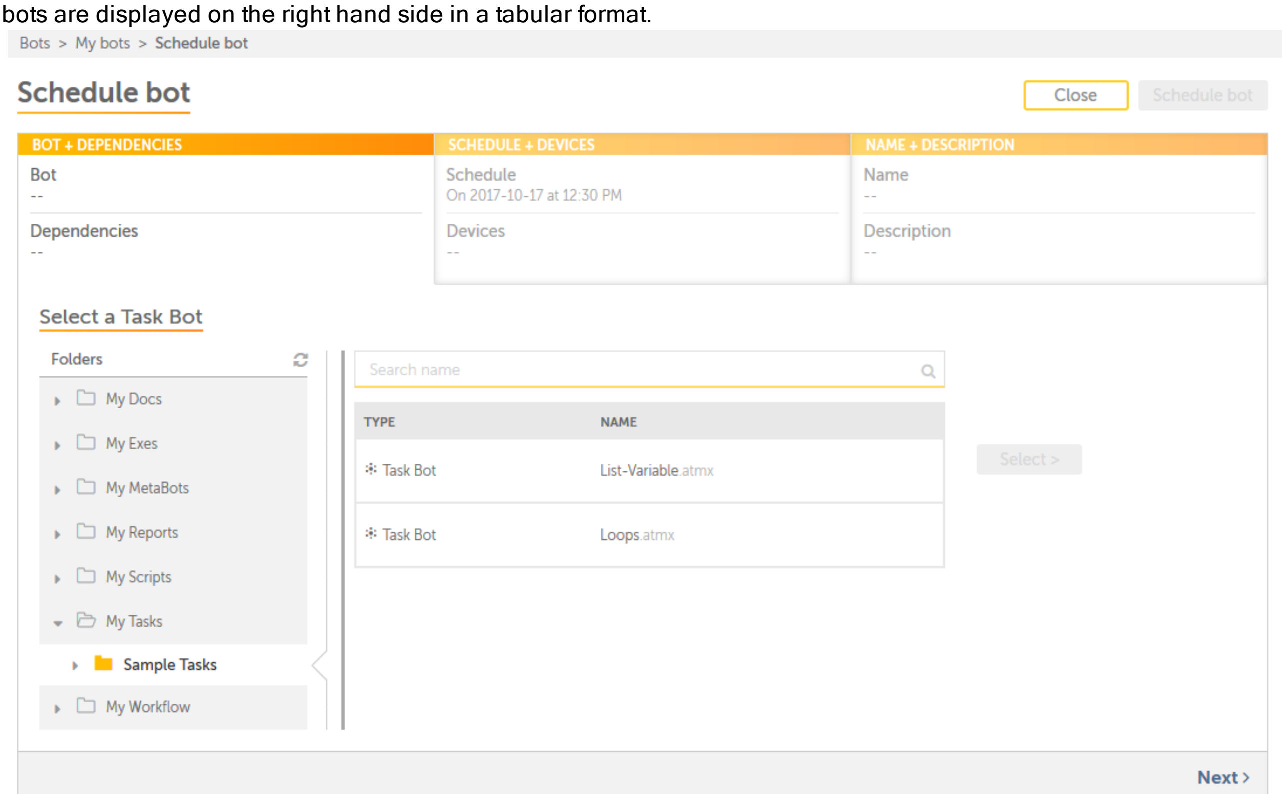
- Activity → In progress
- Activity → Scheduled
- Bots → My bots
- Devices → Bot runners and bot creators

To schedule a bot, perform the following steps.

1. Click the Schedule bot... link on the appropriate page, such as **In progress**, **Scheduled**, **My bots**, or **Bot runners and bot creators** page. The **Schedule bot** page is displayed.

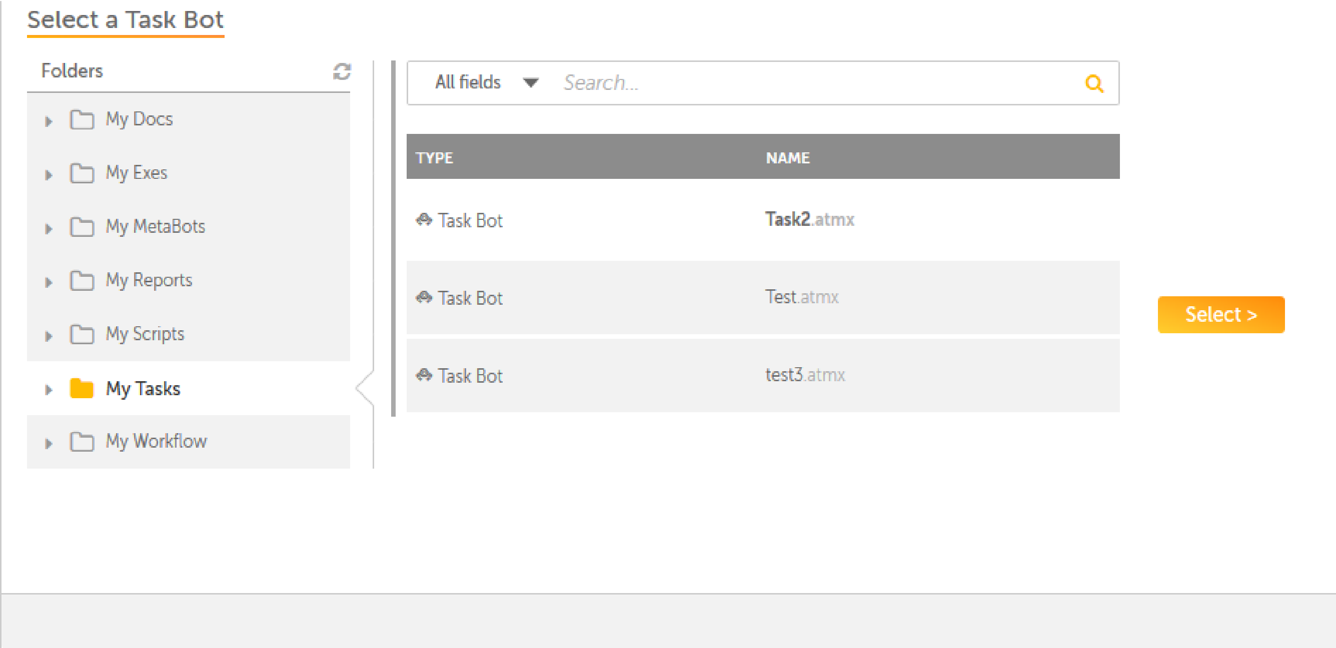


2. From the **Select a Task Bot** area, click one of the folders depending on your requirements. The Type and name of the available bots are displayed on the right hand side in a tabular format.



Note: You can access only those folders for which you have **Run+Schedule** permission.

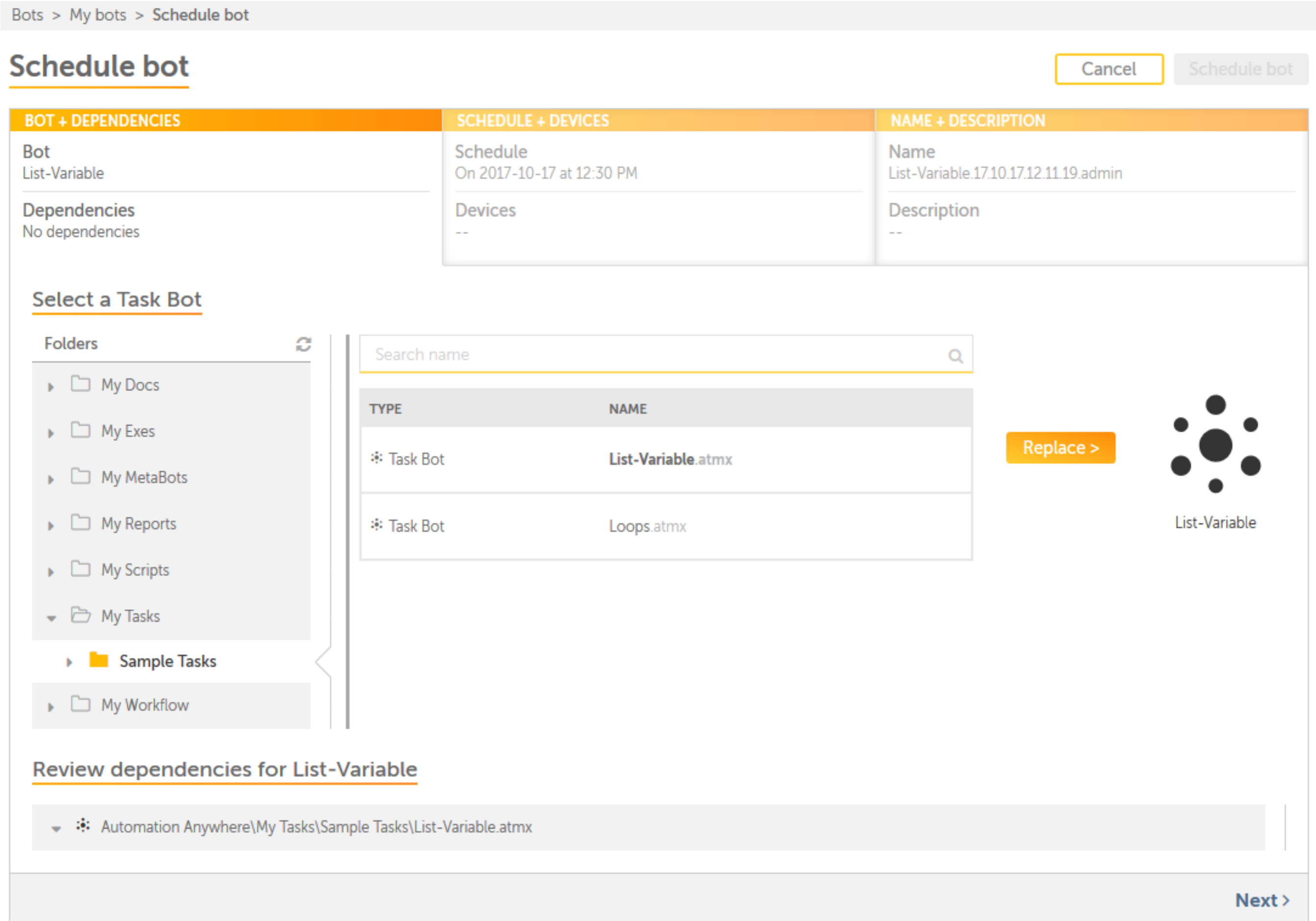
3. Select a task bot depending on your requirements by clicking a bot. The **Select** button is enabled.



When you click the **Select** button the bot is ready to be scheduled and you can view the dependencies of the selected in the **Review dependencies for <bot name>** section.

Note: When you click the **Select** button, the label of the button is changed to **Replace.** This gives you an option of selecting another bot and replace the selected bot.

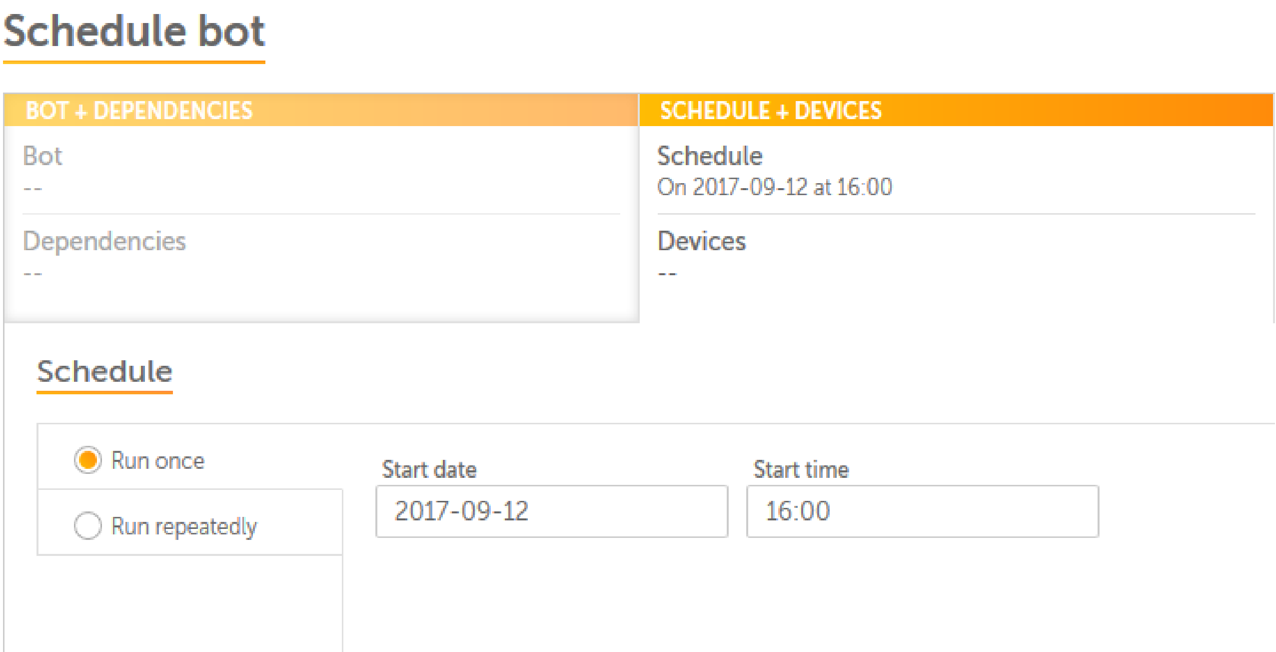
4. Click the **Select** button. The bot and all its dependencies are added to the **Review dependencies for <bot name>** section. In the following figure, the **<bot name>** or name of the bot is **List-Variable**.



Note: Although you will be able to schedule a bot, automation will fail in the following cases,

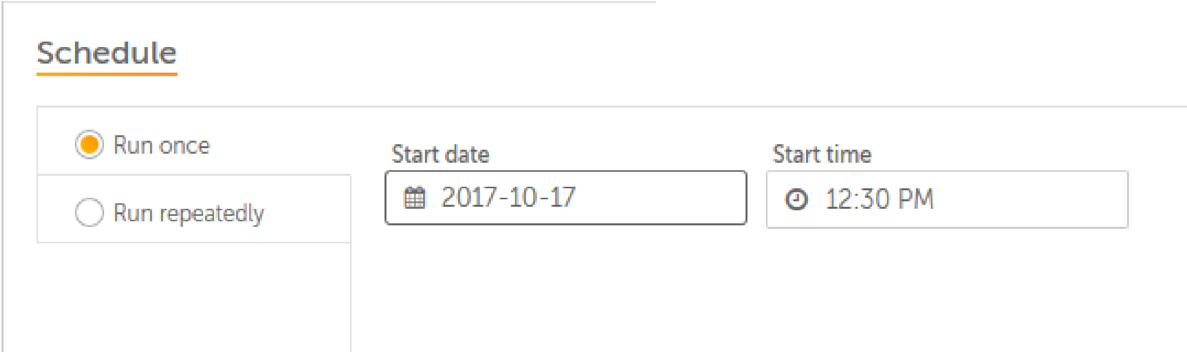
- If any of the bot dependencies are missing
- If you do not have folder privileges on the dependencies
- If you do not have **Run+Schedule** permission (the one that shows a red dependency icon -)

5. Click the **Next** link. The **SCHEDULE + DEVICES** tab is displayed.



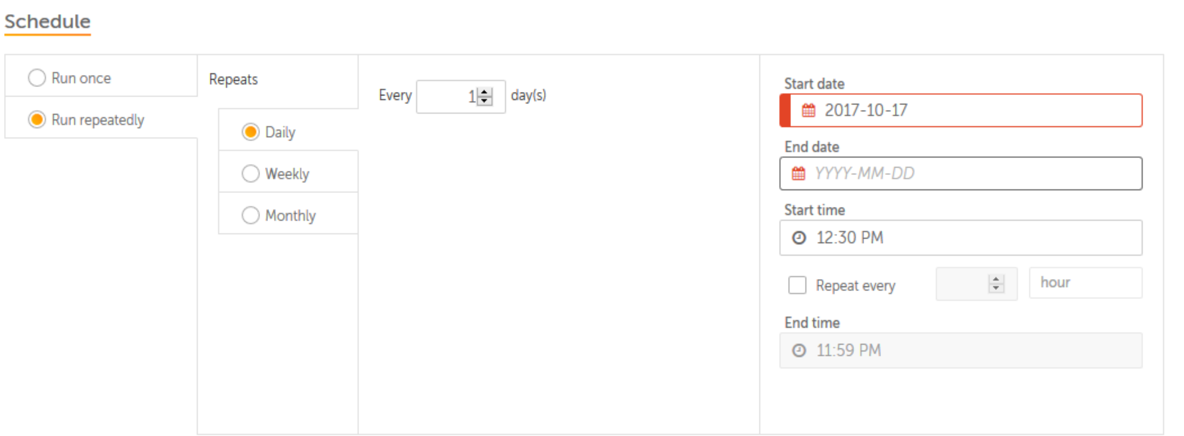
You have two options of scheduling a bot - **Run once** and **Run repeatedly**.

- **Run once:** Use this option to run the bot once on a given day at X hour. When you select this option, you must enter the Start date and Start time. The default value of the **Start date** field is set to the current day while the default value of the **Start Time** field is a roundup of the closest half-hour that is 15 minutes away. As an example, if the current time is 13:43 hours, a value of 14:00 hours is displayed.



> **Note:** The value of the Start date box is always later than or equal to the current date. If the Start date is the current date, the scheduled time cannot be less than the current time.

- **Run repeatedly:** Use this option when you want to schedule your bot to run every X minutes/hours on a given day. When you select this option, you must select the Start date, end date, and Start time. The default value of the **Start date** field is set to the current day while the default of the **Start Time** field is a roundup of the closest half-hour that is 15 minutes away. As an example, if the current time is 13:43 hours, a value of 14:00 hours is displayed. The default value of the **End date** field is blank.

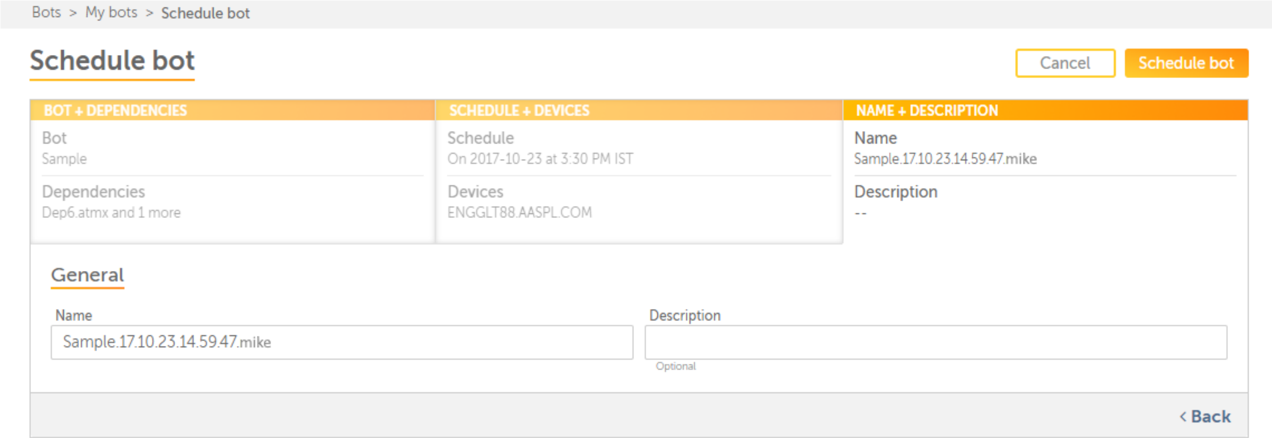


> **Note:** If the value selected in the Start date box is the current day, the scheduled time must be greater than the current time. Also, the value of the End date box must be later than or equal to the value in the **Start date** box.

6. After selecting the **Run once** or **Run repeatedly** options, click a device of your choice from the **Available** devices area and click the **>>** button. The device is added to the **Selected devices** area, which displays the list of connected and disconnected devices to Control Room.

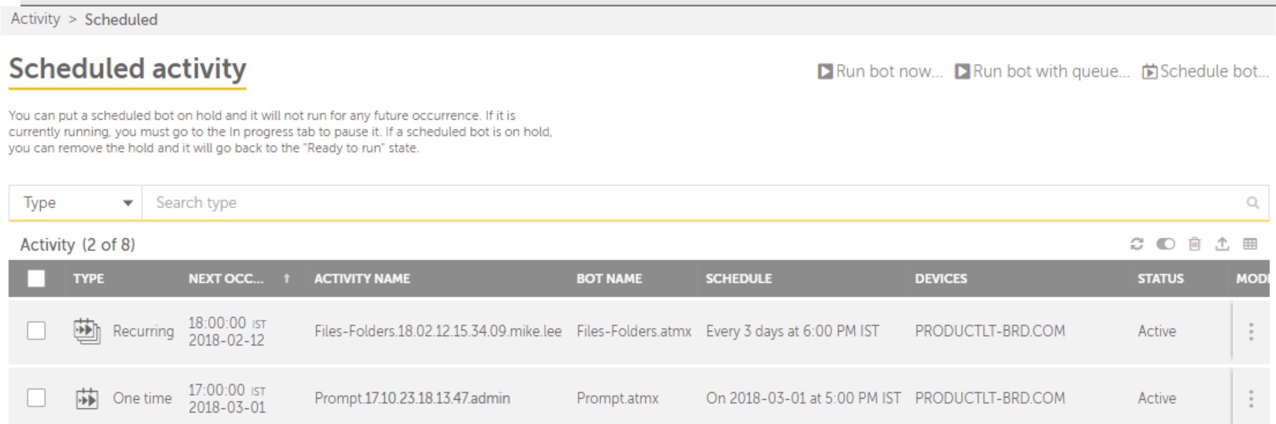
> **Note:** You can select only bot runner devices that are connected. If a device is not connected, it is not enabled. Also, if the device is not displayed in the list, ensure that an active bot runner session is running on the device

7. Click the **Next** link. The **NAME+DESCRIPTION** tab is displayed.



8. Type a name and description in the General area and click the Schedule bot button. The bot is added to the **Activity** table of the **Scheduled activity** page.

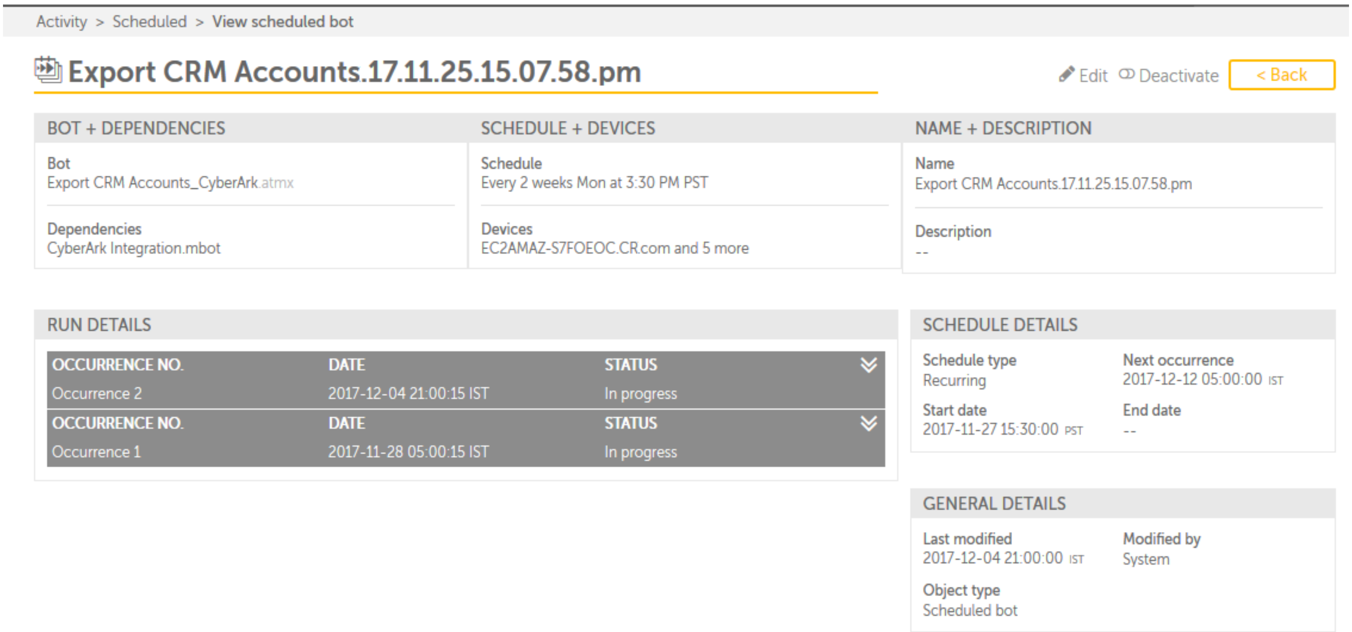
> **Note:** The **Schedule bot** button remains disabled until all the required items, such as bots, schedule details, and devices are not selected.



View scheduled bot details

Once you have scheduled a bot, you can view details for the bot from the **View scheduled bot** page. This page allows you to make changes to the bot using the **Edit** button and activate or deactivate it depending on your requirements by using the activate/deactivate toggle button .

This page illustrated in the following figure.



The different areas of the View scheduled bot page are described in the following table.

Area	Description
BOT + DEPENDENCIES	The name of the bot and dependencies for the scheduled bot.
SCHEDULE + DEVICES	The date and time at which the bot has been scheduled along with the name of the device connected to the bot.
NAME + DESCRIPTION	The name and description for the bot.
RUN DETAILS	The run details for the bot. For example, when did the bot last run?
SCHEDULED DETAILS	The following details for the schedule are displayed here. • **Schedule type:** Whether the schedule will run once or repeatedly? • **Next occurrence:** When the schedule will run again • **Start date:** The date when the schedule will run for the first time. • **End date:** The date when the schedule will stop running.
GENERAL DETAILS	The following details for the schedule are displayed here. • **Last modified:** The last date and time the bot was modified. • **Object type:** The type of object of the bot, such as scheduled bot. • **Modified by:** The name of the user who last made changes to the scheduled bot.

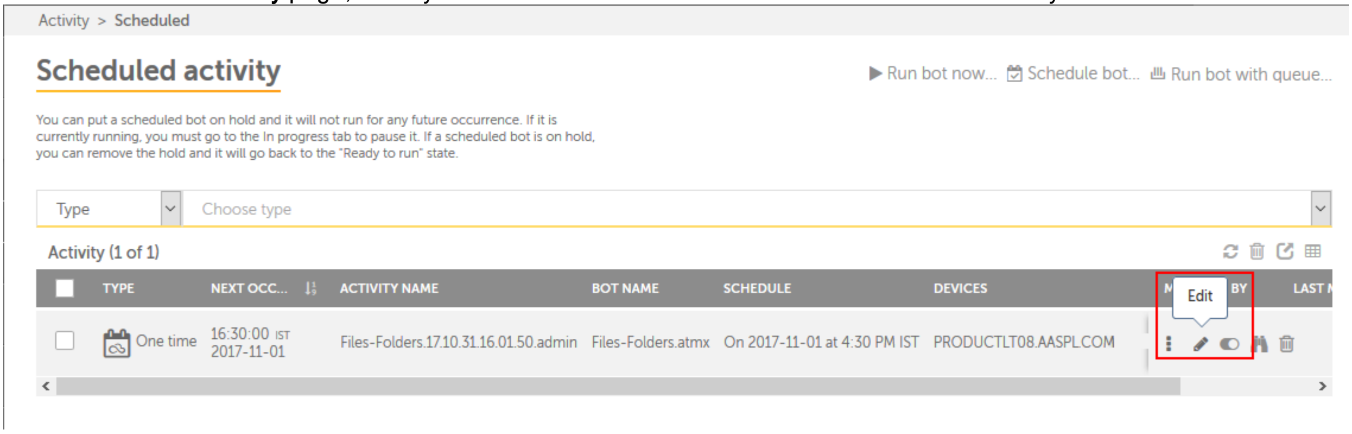
Edit scheduled activity

There may be times when you want to change the number of retries or the retry interval so that the automation is not skipped. Besides this, you may also want to edit the scheduled activity to:

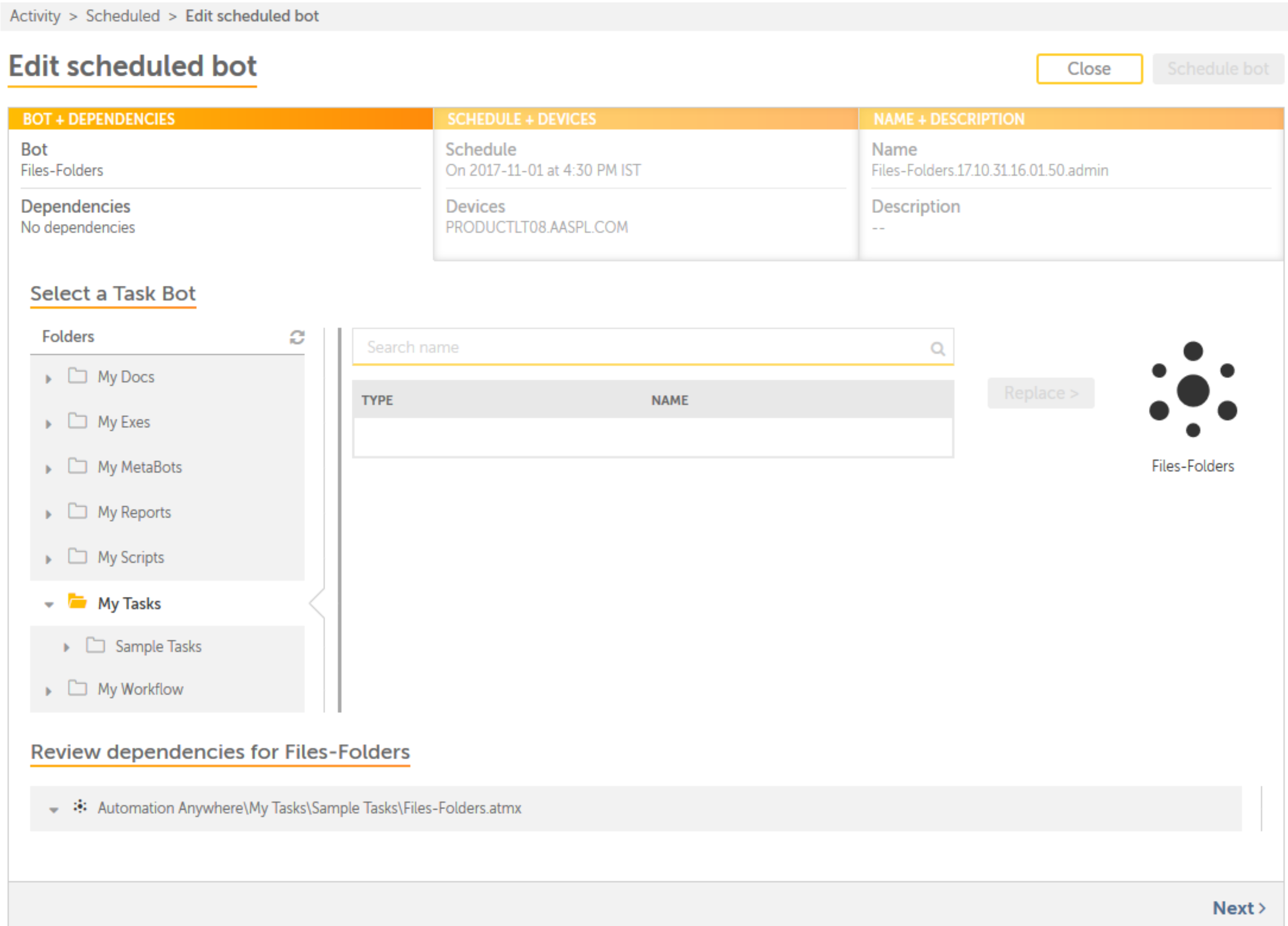
- Change the schedule type, date, or time.
- Add or remove Bot runners from the schedule.
- Change the retry settings.

To edit a scheduled activity, perform the following steps.

1. On the **Scheduled activity** page, move your mouse over the **Actions** icon of an item in the Activity table and click the **Edit** icon.



When you click the **Edit** icon, the **Edit scheduled bot** page is displayed.



2. Make changes to the bot depending on your requirements. Once done, click the **Schedule bot** button.

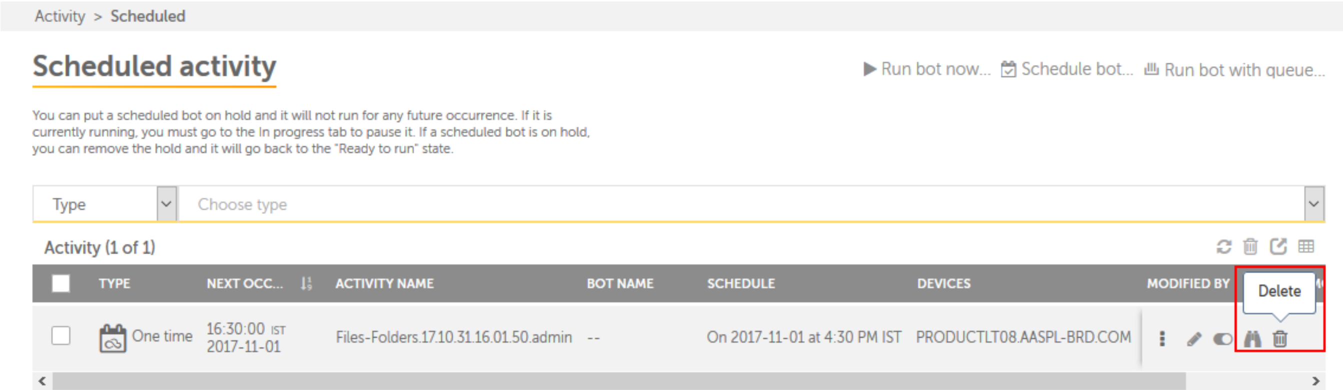
Note: You must select the fields, such as Bots and devices. These are required to save your changes.

Tip: As you start typing and make changes to the fields of the **Edit scheduled bot** page, the text of the **Close** button changes to **Cancel** to visually indicate that you have made changes. Clicking **Cancel** closes the **Edit Schedule bot** form.

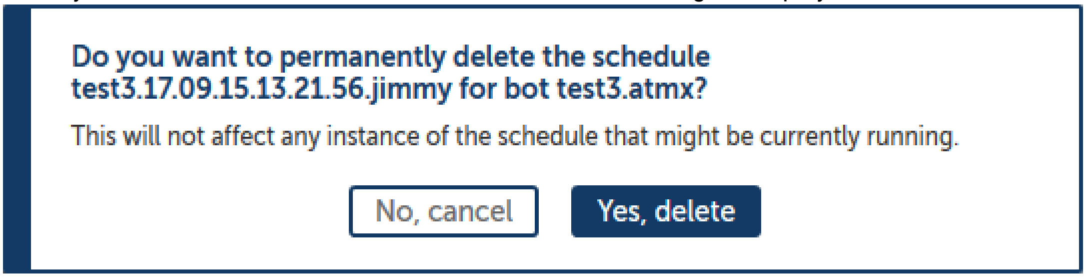
Delete a schedule

If you have Delete my bots privileges, you can delete a scheduled activity. To delete a scheduled activity, perform the following steps.

1. On the **Scheduled activity** page, move your mouse over the **Actions** icon of an item in the Activity table and click the **Delete** icon .



When you click the Delete icon , a delete confirmation message is displayed.



2. Click **Yes, delete** to delete the scheduled activity.

Activate or deactivate a scheduled activity

As a Control Room user with Manage and Update all schedules privileges, you can activate or deactivate scheduled activities individually or in bulk.

For example, you can choose to activate schedules that are inactive when you want to run the automation in bulk. Or you can deactivate multiple schedules during down time.

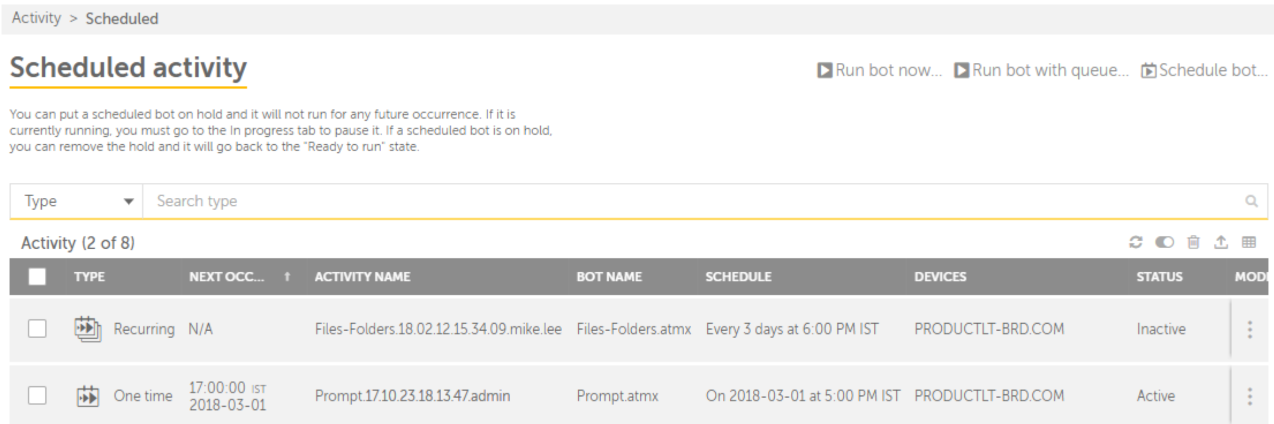
By default, all schedules on this page are in activated state.

Deactivate Schedule(s)

You can deactivate a single or multiple schedules based on your requirement.

To deactivate a schedule,

1. Go to **Activity** → **Scheduled**
2. The **Scheduled activity** page is launched.
3. In the **Activity** area mouse over for the Schedule that you want to deactivate. For example, the **Recurring** type schedule for **Files-Folders.atmx**
4. Click
5. The schedule is deactivated. The status in the **Next Occurrence** column is displayed as **NA** and **Status** changes to **Inactive:**



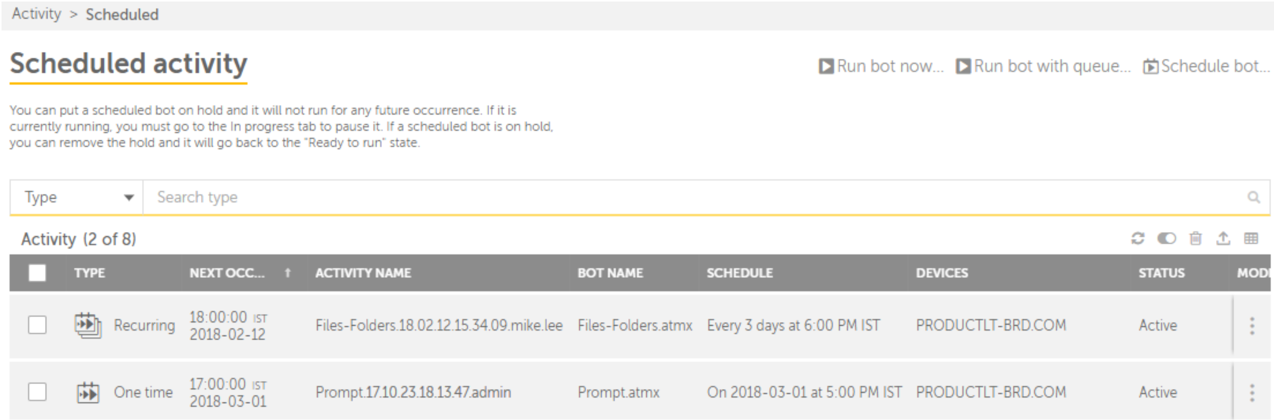
Similarly, you can deactivate multiple schedules by clicking that is given above the **Activity** table.

Activate Schedule(s)

You can activate a single or multiple schedules based on your requirement.

To activate a schedule,

1. Go to **Activity** → **Scheduled**
2. The **Scheduled activity** page is launched.
3. In the **Activity** area mouse over for the Schedule that you want to activate. For example, the **Recurring** type schedule for **Files-Folders.atmx**
4. Click
5. The schedule is activated. The status in the **Next Occurrence** column is displayed in **date & time format** and **Status** changes to **Active.**



Similarly, you can activate multiple schedules by clicking that is given above the **Activity** table.

Note: The **Deactivate** - or **Activate** - button above the table appears based on the **greater** number of schedule status.

- When the number of schedules with **Active status are more** than the Inactive ones, is shown.
- When the number of schedules with **Inactive status are more** than the Active ones, is shown.

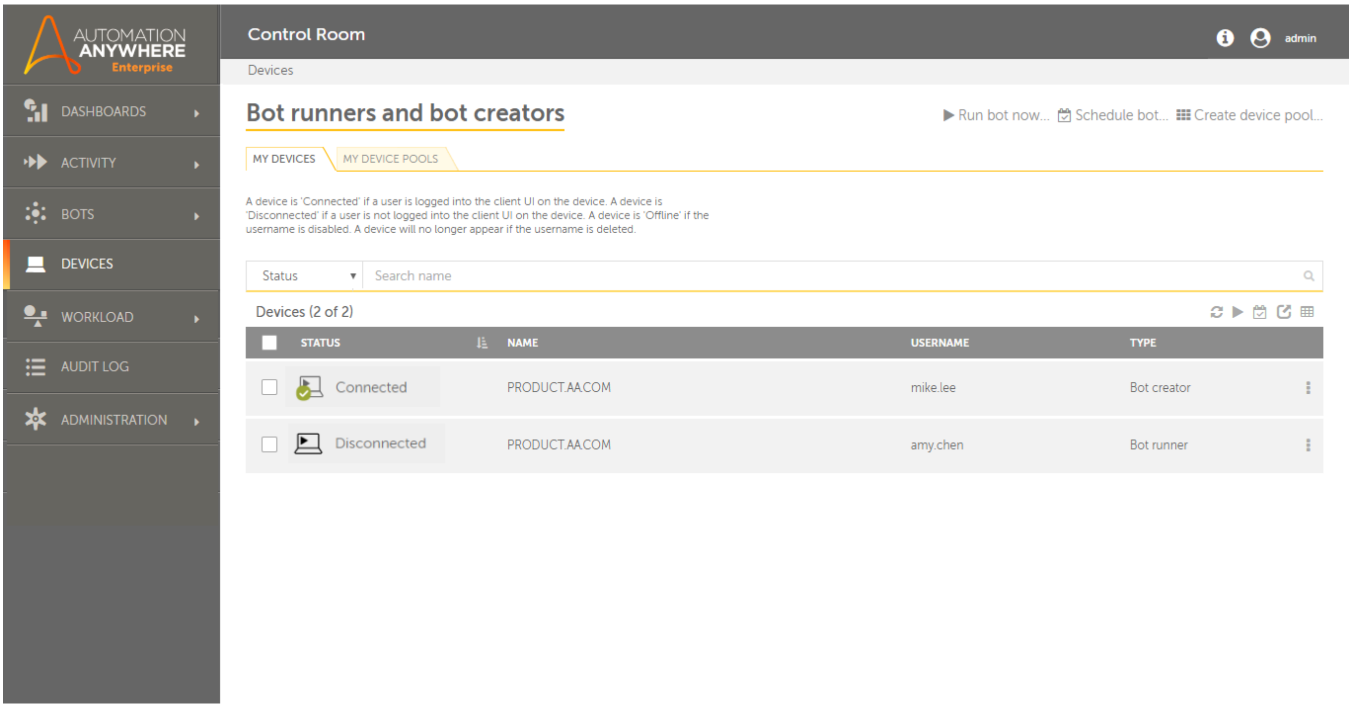
Bot runners and bot creators - overview

As a Control Room user with Bot creator, Bot runner and Device pools privileges, use the Control Room **Bot runners and bot creators**, to:

- View a list of Devices registered and connected to the current instance of the Control Room in My Devices
- Create and view a list of Device pool available from the current instance of the Control Room in My Device Pools
- Run Bots immediately on selected Bot runners using Run bot now
- Schedule Bots to run on selected Bot runners using Schedule bot
- Run Bots on selected Device pools using Run bot with queue

Note: Only an admin user has access to see all the devices in the Control Room. A non- admin user will not have access to view Bot creators.

The **Bot runners and bot creators** page is illustrated in the following figure:



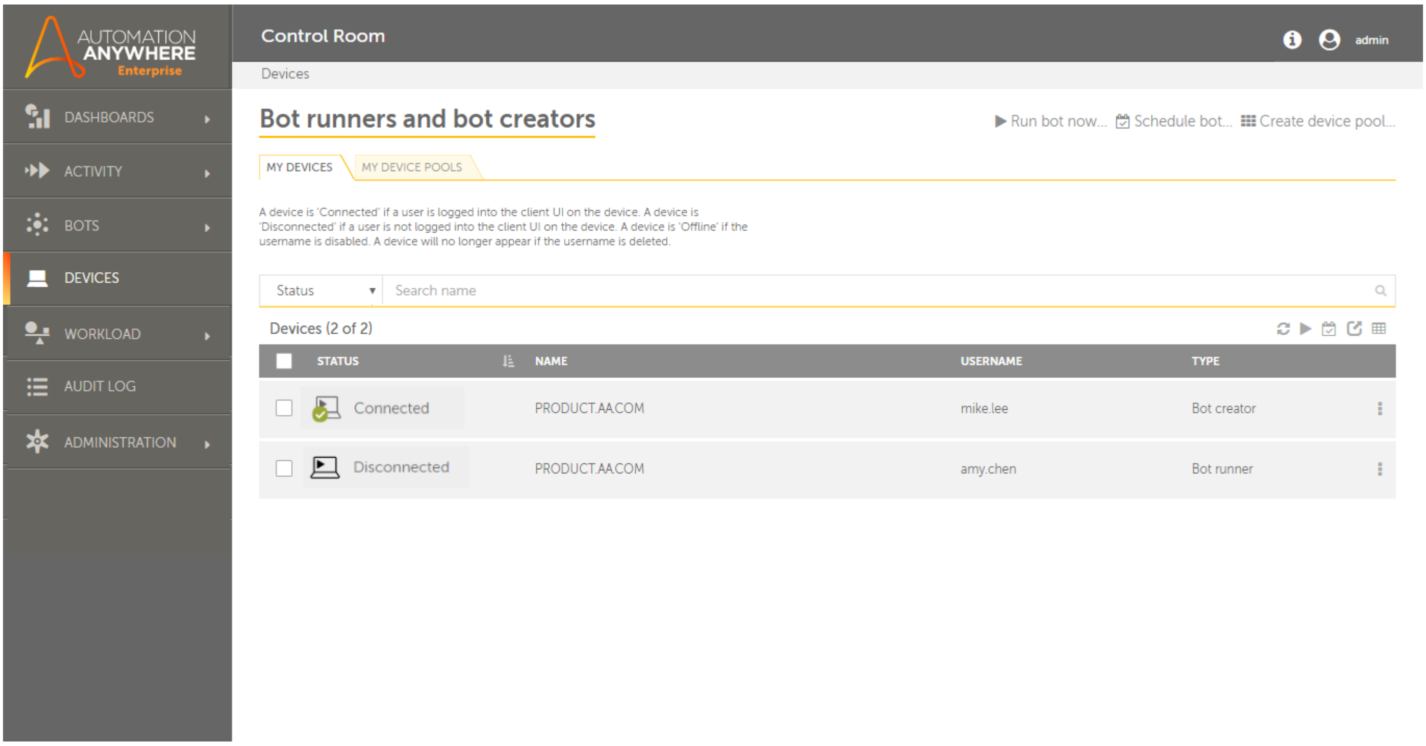
My Devices

As a Control Room admin or a user with manage devices privileges, you can view the devices that are registered to your Control Room instance.

Devices privileges include View and Manage Bot runners, Bot creators, as well as Create and Manage Device Pools. Learn More about privileges in Roles - Overview

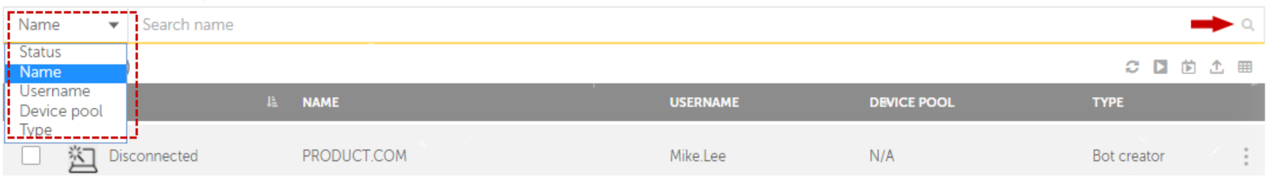
Note: Only an admin user has access to see all the devices(Bot runners and Bot creators) in the Control Room. A non - admin user will not have access to view Bot creators.

The **My Devices** page is illustrated in the following figure:



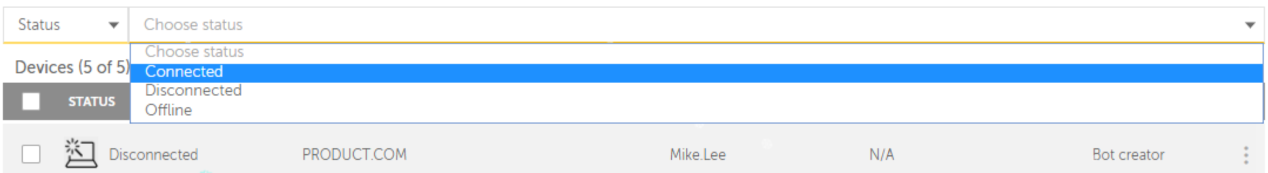
For ease of access, you can apply search parameters to Status, Name, Username, Device pool, and Type columns.

- You can use specify the search parameters in the search bar for Name, Username, and Device Pool:



Note: When you specify search parameters for the same column, the system searches using **OR** operator. When you specify search parameters for different columns, the system searches using **AND** operator.

- You can choose the search parameters from a list in the search bar for Status and Type:



The following describes the list of items that can be viewed in the table:

<table>
<tr><th>Table Item</th><th>Description</th></tr>
<tr><td>Status</td><td>

Shows device's status, which is the combined status of the user and the device used by that user.

For example Mike Lee and Amy Chen might be using the same device 123.456.7.89. However, Mike Lee - a Bot Creator could be shown connected while Amy Chen could be shown disconnected.

Following statuses are visible:

- **Connected** when the Bot is logged on to the Control Room
- **Disconnected** when the Bot is not logged on to the Control Room
- **Offline** when the device user has been unregistered/disabled by the Control Room admin

Note that the icon indicates the user type.

Bot Creator **Bot Runner**

</td></tr>
<tr><td>Name</td><td>Shows the machine's fully qualified server name</td></tr>
<tr><td>Username</td><td>Shows name of the user connected with the device</td></tr>
<tr><td>Device Pool</td><td>Shows the name of the device pool that the device is part of, if any. Note that "--" indicates the device is not part of any device pool and N/A indicates that it cannot be included in any device pools. Learn More</td></tr>
<tr><td>Type</td><td>Shows the type of license that is assigned by the Control Room admin.</td></tr>
</table>

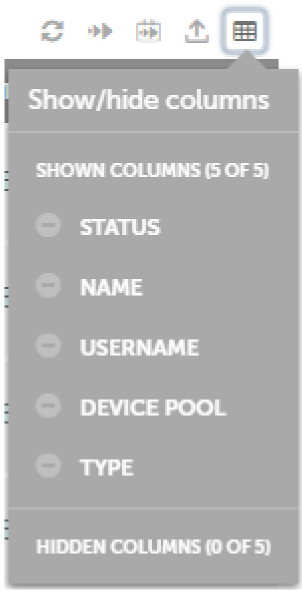
Tip: You can perform the following actions on a table column:

- Click a column to sort it in ascending and descending order. You can sort up to three columns by holding the Shift key when you click on two more columns. This gives you the option of sorting two additional columns. This way the sorting is done on the entire table and not just the data that is currently visible to you. The last sorting is stored in memory applied by a user per session.
- Use a drag-and-drop operation to move the column left or right
- Move your mouse cursor at the end of the column and drag to re-size

The following describes the tasks that you can perform on an individual device:

Table Item	Description
Run	Allows you to run a Bot on the device immediately.
Schedule	Allows you to schedule a Bot to run on the device.

Alternatively, you can select all devices and perform the following actions. Note that these actions can be performed only at a table level and not on individual items.

Table Item	Description
Refresh	Allows you to refresh the table contents so that you can view the latest device status
Run	Allows you to run a Bot on selected devices immediately.
Schedule	Allows you to schedule a Bot to run on selected devices.
Export to CSV	Allows you to export the data to a csv file. You can export data based on: • Filters • Selection
Show / Hide columns	Allows you to show or hide specific columns. By default, all columns are displayed:  Tip: To **hide** a column, click on the column name.

When you want to perform actions such as **Run**, **Schedule** or **Create a device pool** quickly without switching your current location, you can use the following options:

Table Item	Description
Run bot now...	Allows you to run a Bot on the device immediately.
Schedule bot...	Allows you to schedule a Bot to run on the device.
Create device pool...	Allows you to create a device pool for workload management.

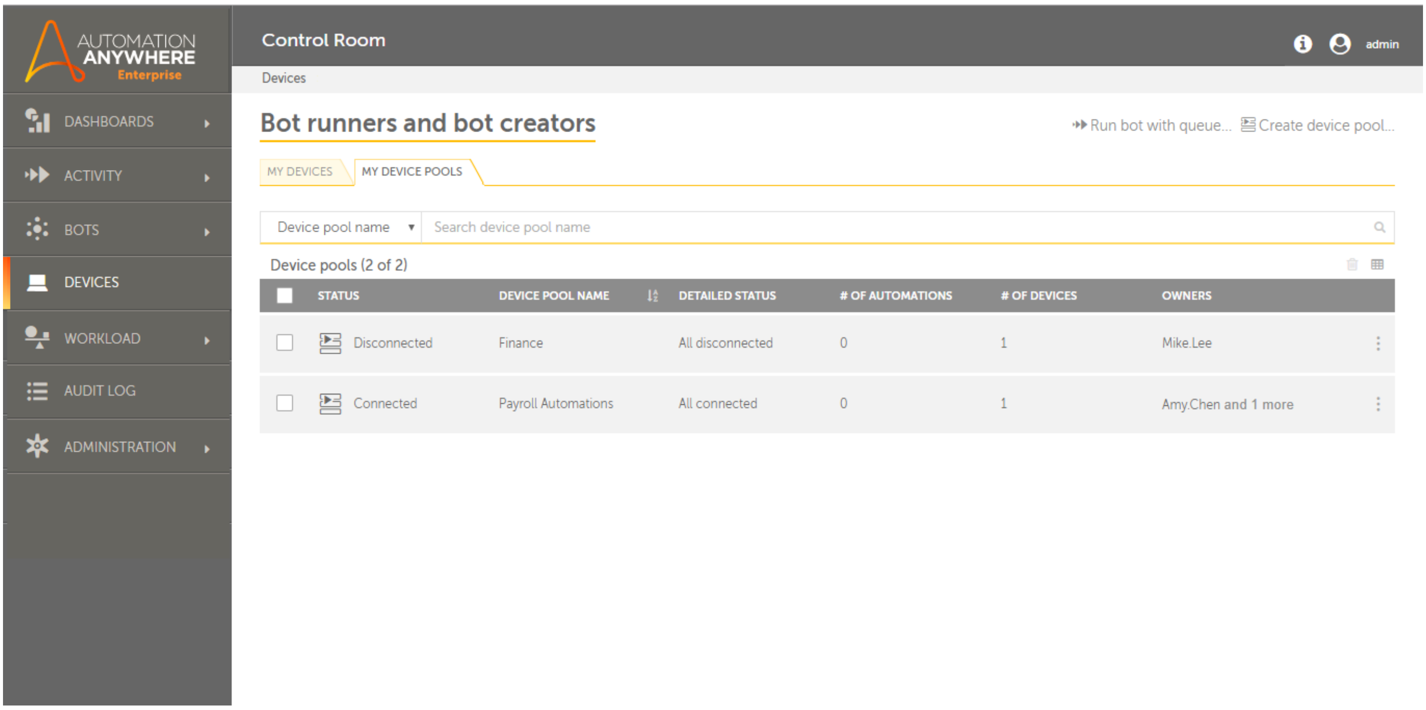
My device pools

As a Device Pool admin you can view all devices pools that can be used for work items in workload management. You can also create device pools comprising Bot Runners.

If you are a Device Pool Owner / Consumer you can view only those Device pools of which you are the owner or consumer.

Device pools provide a logical grouping of similar Bot Runners on which you want to run bot(s) with the work item from a queue. For example, you can group devices of a particular department/unit and create a device pool for it.

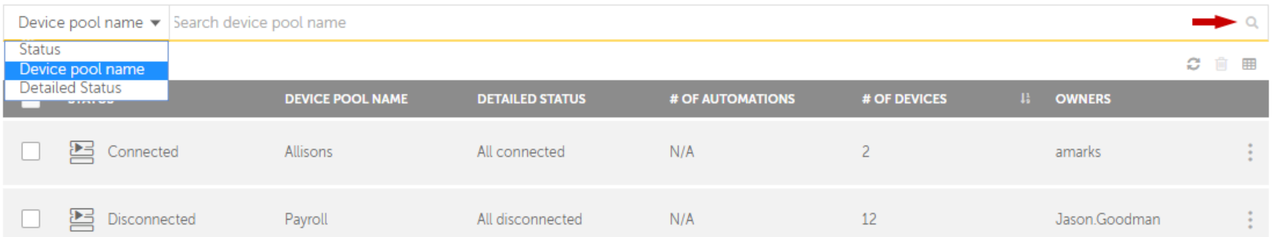
The **My device pools** page is illustrated in the following figure:



> **Note:** You need to create device pools to view those in the list. To get started, click on the **create a device pool here** link.

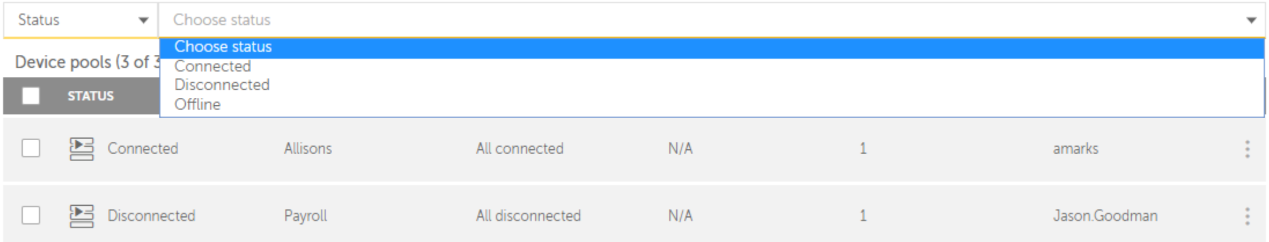
For ease of access, you can apply search parameters to Status, My Access and Queue Name columns.

- You can use specify the search parameters in the search bar for Detailed Status and Device Pool Name:



> **Note:** When you specify search parameters for the same column, the system searches using **OR** operator. When you specify search parameters for different columns, the system searches using **AND** operator.

- You can choose the search parameters from a list in the search bar for Status



The following describes the list of items that can be viewed in the table:

Table Item	Description
Status	Shows device's status. Here, status refers to the status of both User and Device from which the user is connects. • Connected when the user and device are connected to the Control Room from selected Bot Runner • Disconnected when the user and device are not connected to the Control Room from selected Bot Runner • Offline when the user is deactivated by the Control Room admin
Device Pool Name	Shows name of the device pool
Detailed Status	Shows status of the devices that are part of that particular device pool • All Connected when all users and devices are connected to the Control Room • All Disconnected when one or more user and device are disconnected from the Control Room
# of Automations	Shows the number of automation that are currently deployed on that particular device pool
# of Devices	Shows the number of devices that are included in the device pool
Owners	Shows the owner name(s) of the device pool

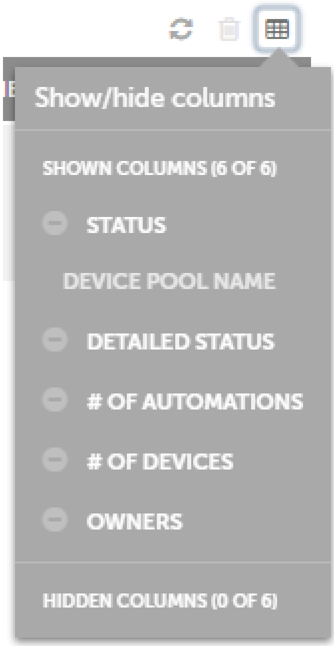
Tip: You can perform the following actions on a table column:

- Click a column to sort it in ascending and descending order. You can sort up to three columns by holding the Shift key when you click on two more columns. This gives you the option of sorting two additional columns. This way the sorting is done on the entire table and not just the data that is currently visible to you. The last sorting is stored in memory applied by a user per session.
- Use a drag-and-drop operation to move the column left or right
- Move your mouse cursor at the end of the column and drag to re-size

The following describes the tasks that you can perform on an individual device pool:

Table Item	Description
Run	Allows you to run a Bot on the device pool immediately
View	Allows you to view device pool details
Edit	Allows you to edit device pool details
Delete	Allows you to delete the device pool

Alternatively, you can select all device pools and perform the following actions. Note that these actions can be performed only at a table level and not on individual items.

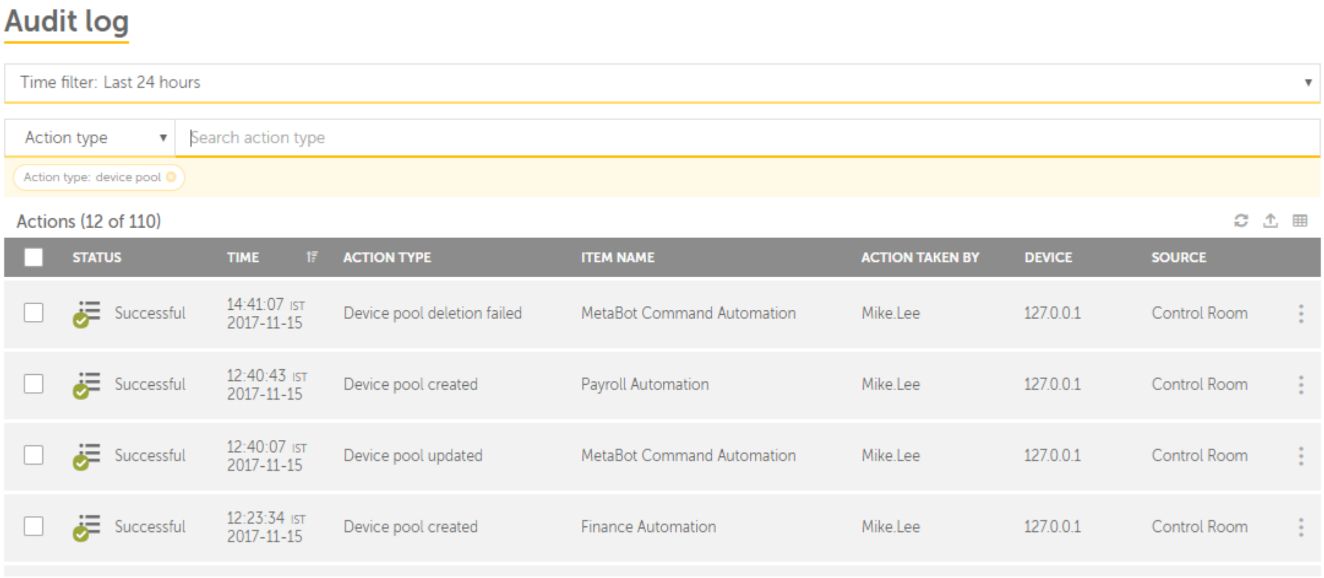
Table Item	Description
Delete	Allows you to delete one or more device pools
Show / Hide column	Allows you to show or hide columns other than **Device Pool Name:**  `Tip: To show or hide a column, click on the column name.`

When you want to perform actions such as **Run bot with queue** or **Create a device pool** quickly without switching your current location, you can use the following options:

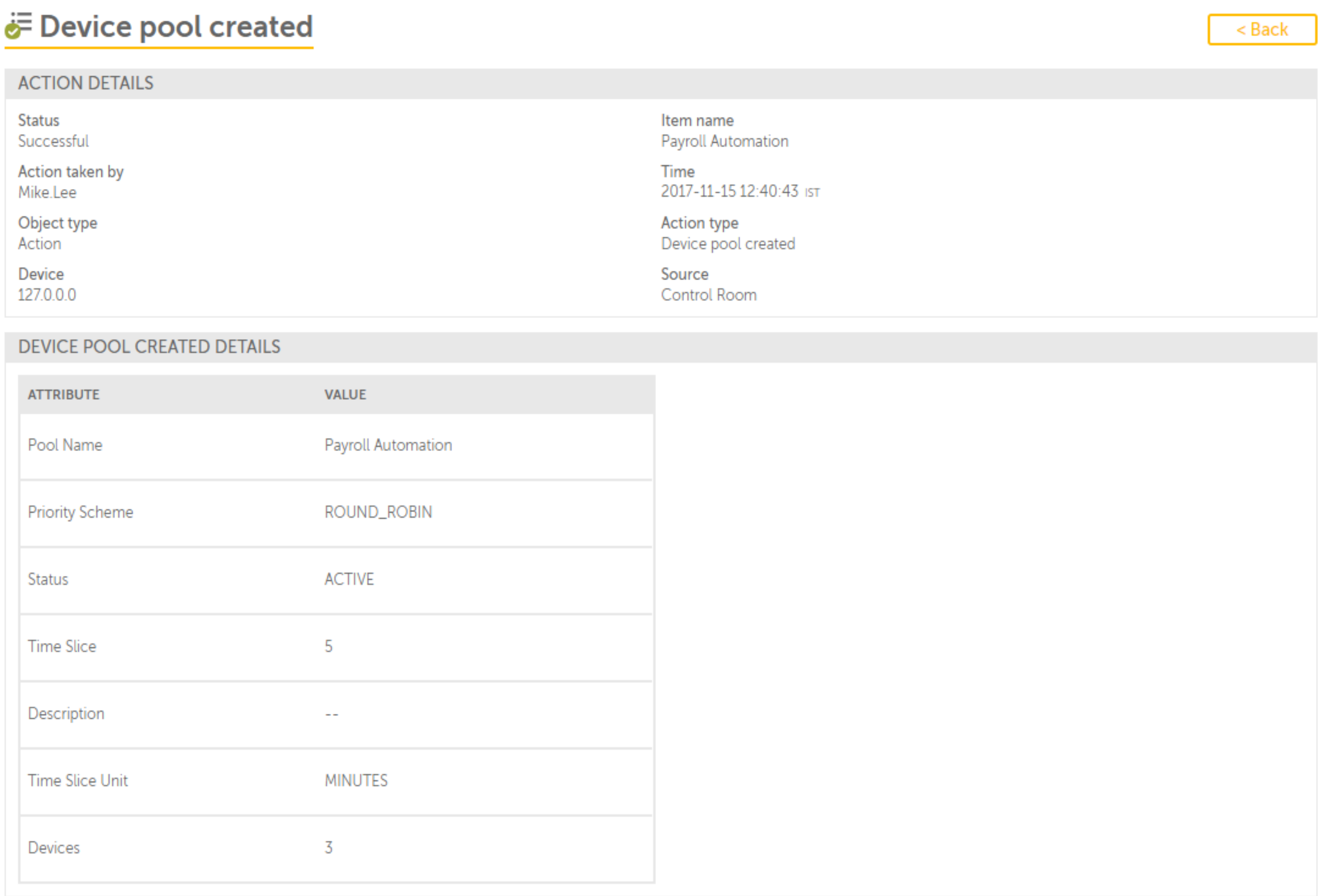
Table Item	Description
Run bot with queue...	Allows you to run bot with a queue for workload management
Create device pool...	Allows you to create a device pool for workload management

Audit Log

All the Create, Update, Delete actions are tracked in audit log for record keeping and future use. You can refer those entries in the Audit Log page:



To view details of the audit entry, click which is visible when you mouse over . For example, the device pool creation details are shown as:



Create and delete device pools

As a Device Pool admin, you can create a Device pool comprising Bot Runners to optimize your automation workload and thereby achieve your entity's SLA.

Create device pool

A Device pool is created to group similar type of devices and run bots on those devices with work items from their respective queues.

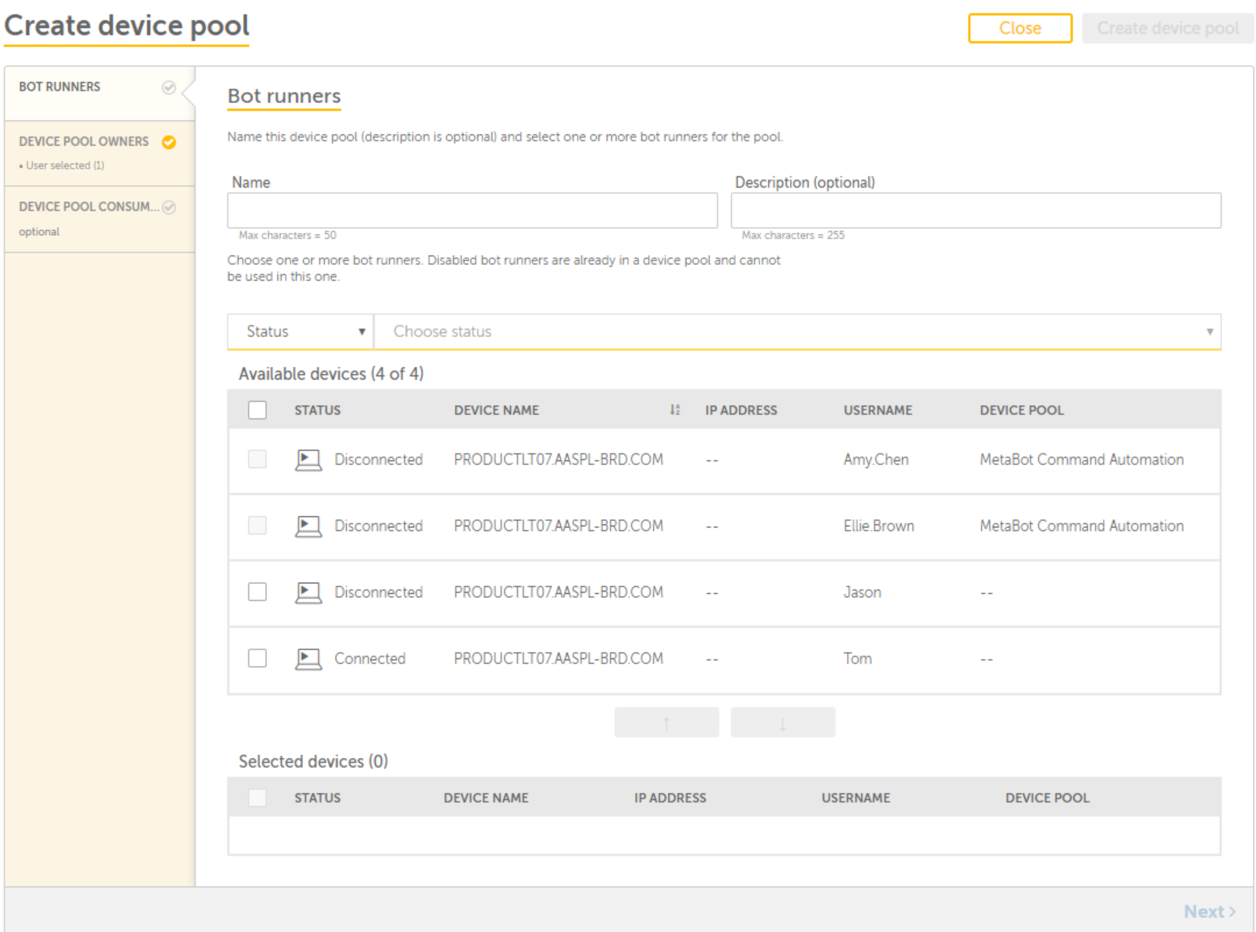
To create a device pool, you must give a unique name to the pool and add Bot Runners to it. You can add only those Bot Runners that are not part of any pool and are not associated with any role. Optionally, you can add other users as owners so that they can manage the pool. You can also add Control Room user roles as consumers. Only users with these roles can use the pool for any automation.

A. Create a device pool and select Bot Runners

1. Go to **Devices** → **My Device Pools**
2. Click Create device pool... at the top right of the Devices page.

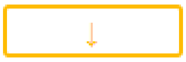
   ```
   Tip: Click the create a device pool here link, which is shown if no device pools are present.
   ```

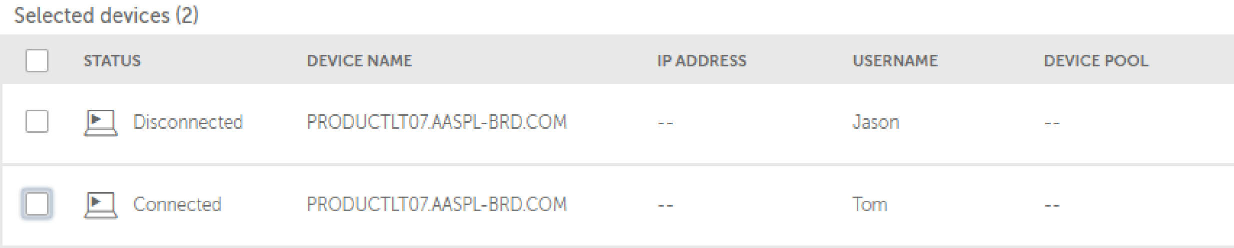
3. The Create device pool page is launched:



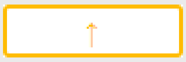
4. Select the Bot Runners for which the automation will be relevant. For example, you can create a Finance Automation pool that can run all finance relevant automations on Bot Runners from the finance department.

   ```
   Note: You can add only those Bot Runners that are not part of another device pool. Such Bot Run-
   ners are disabled for selection.
   ```


5. Click  to add the Bot Runner(s) to the list of **Selected devices**



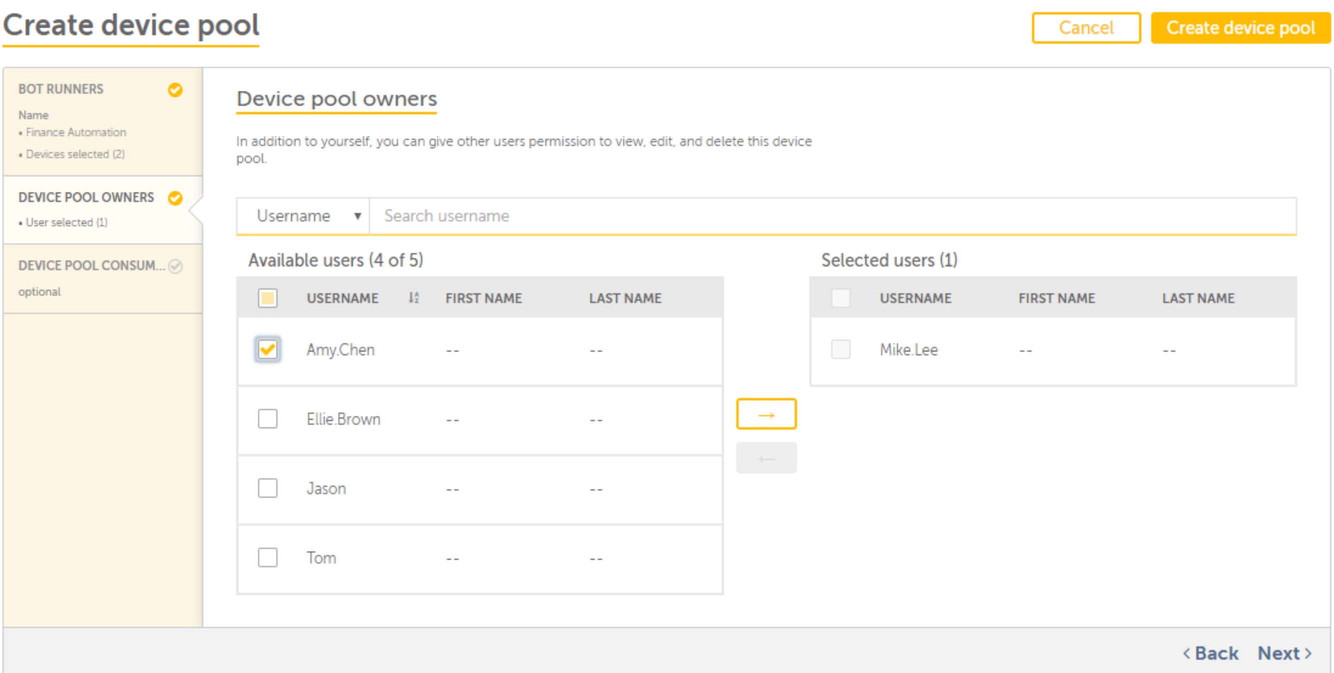

```
Tip: Click [button] to remove the Bot Runner from the list of Selected devices.
```



6. Click **Next** to select **Device Pool Owners**

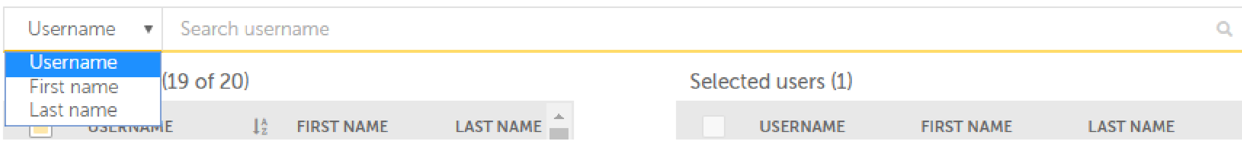
B. Select Device Pool Owners

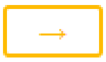
You can choose to grant other Control Room users permissions to view, edit, and delete the device pool.



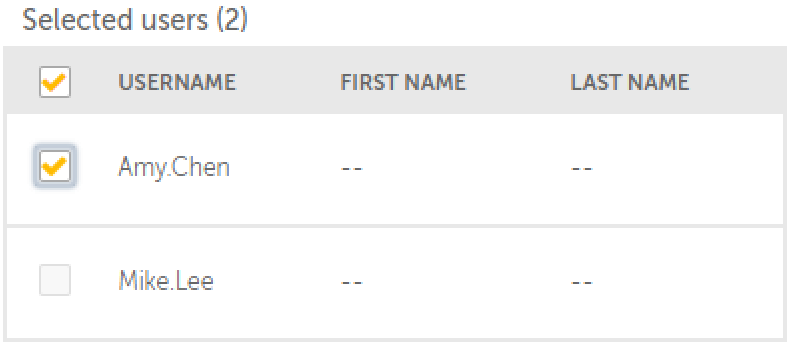
1. Select user(s) from the list of **Available users**

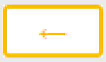
```
Tip: You can search the list of users based on their Username, First name, or Last name.
```



2. Click 
3. The user is shown in the list of **Selected users** .

```
Note: The Device pool creator is listed as the default owner of the pool.
```



Tip: Click  to remove the user from the list of **Selected users.** You cannot remove the user who created the device pool though.

4. You can choose to create the device pool at this instance or select **Device Pool Consumers**.
   - Click 

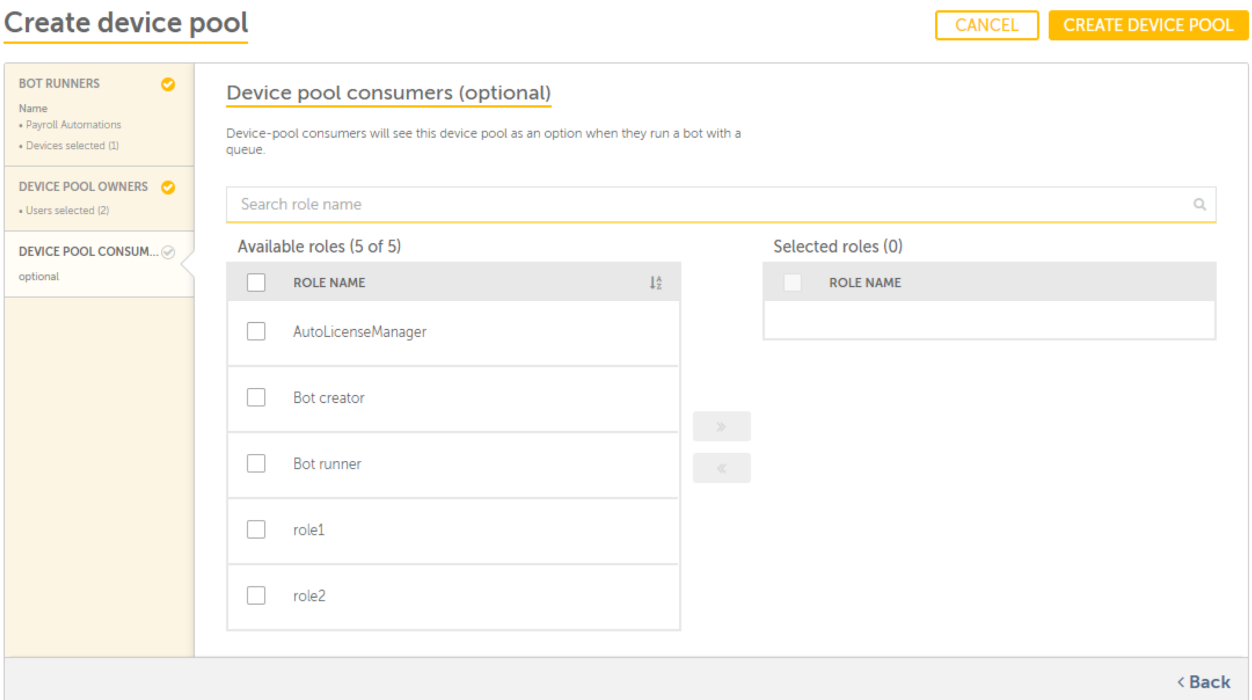
 to complete device pool creation process
   - Click **Next** to select **Device Pool Consumers**

C. Select Device Pool Consumers

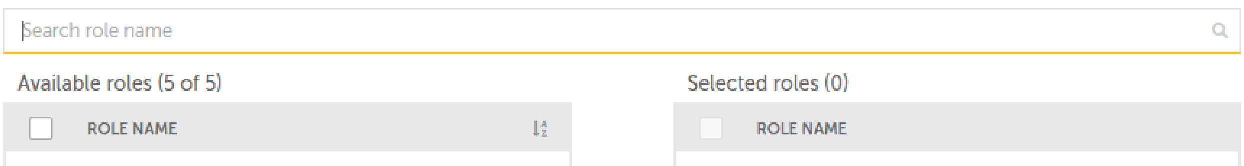
You can select the device pool consumers so that they can view the device pool when they want to run automation/bot with a queue. Refer Run bot with queue for details.

Note: This step is optional.

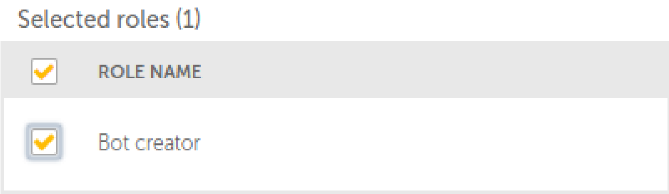
1. Select a Role from the list of **Available roles**.



Tip: You can search for a role name:



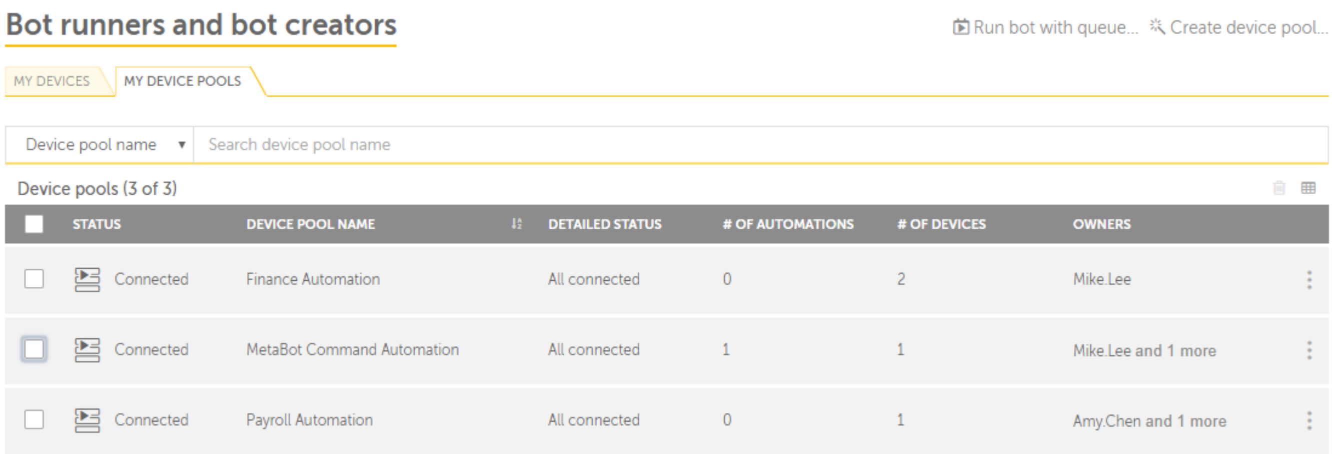
2. Click →
3. The user is shown in the list of **Selected roles**.



> **Tip:** Click ← to remove the user from the list of **Selected roles**.

4. Click CREATE DEVICE POOL

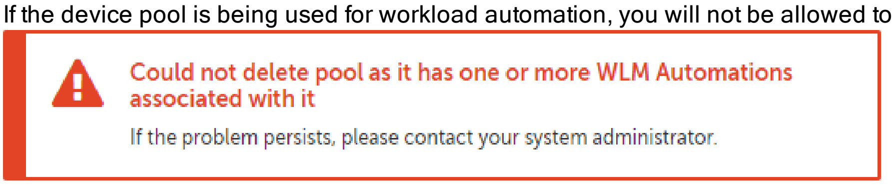
Your device pools for which you have consumer privileges are listed in the **My Device Pools** page:



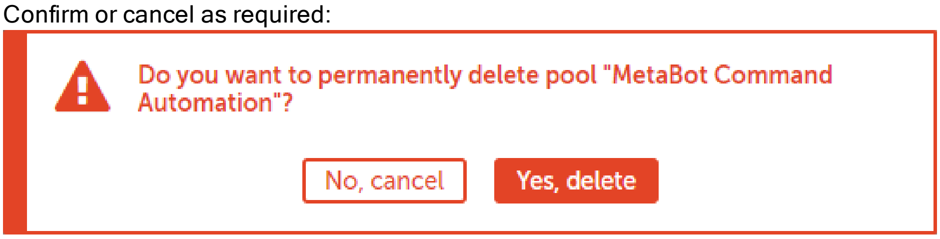
Delete device pool

You can choose to delete your device pools in either of two ways:

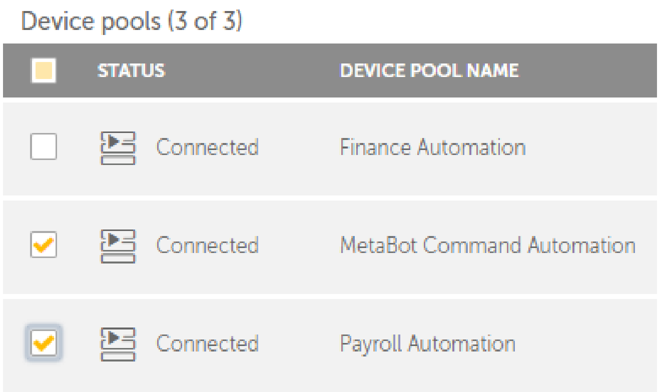
- Delete one device pool -
  1. To delete one device pool, mouse over the actions icon - ⋮
  2. Click 🗑
     - If the device pool is being used for workload automation, you will not be allowed to delete it:



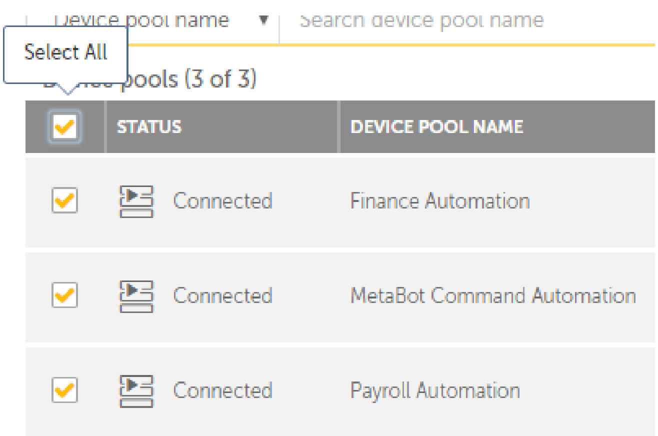
  3. Confirm or cancel as required:



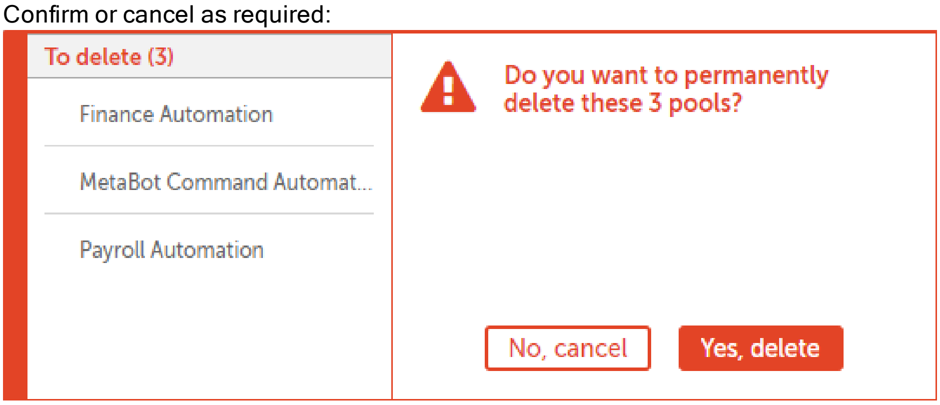
- Delete multiple or all device pools -
  1. Select the device pools that you wish to delete:



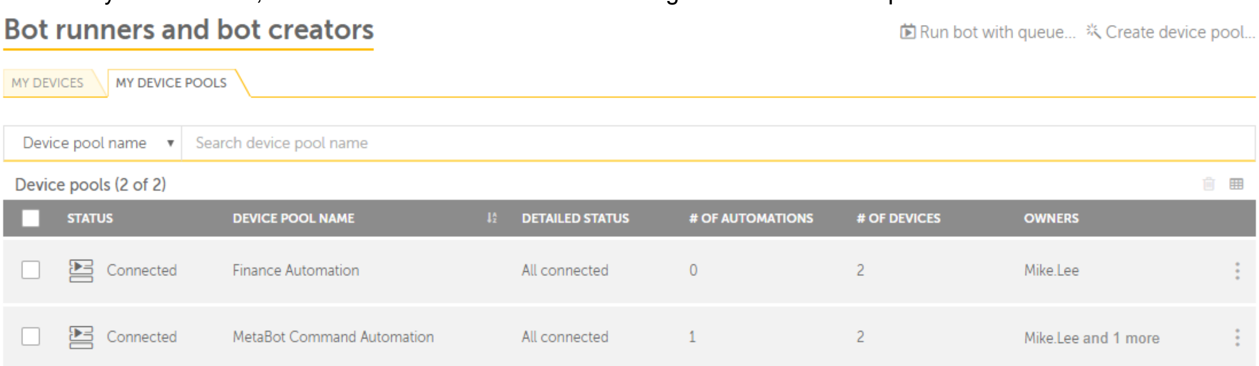
Or select all device pools by selecting the **Select All** check-box in the header:



2. Click given at the top of the device pools table
3. Confirm or cancel as required:



- Based on your selection, the devices are deleted. The following shows one device pool deleted:

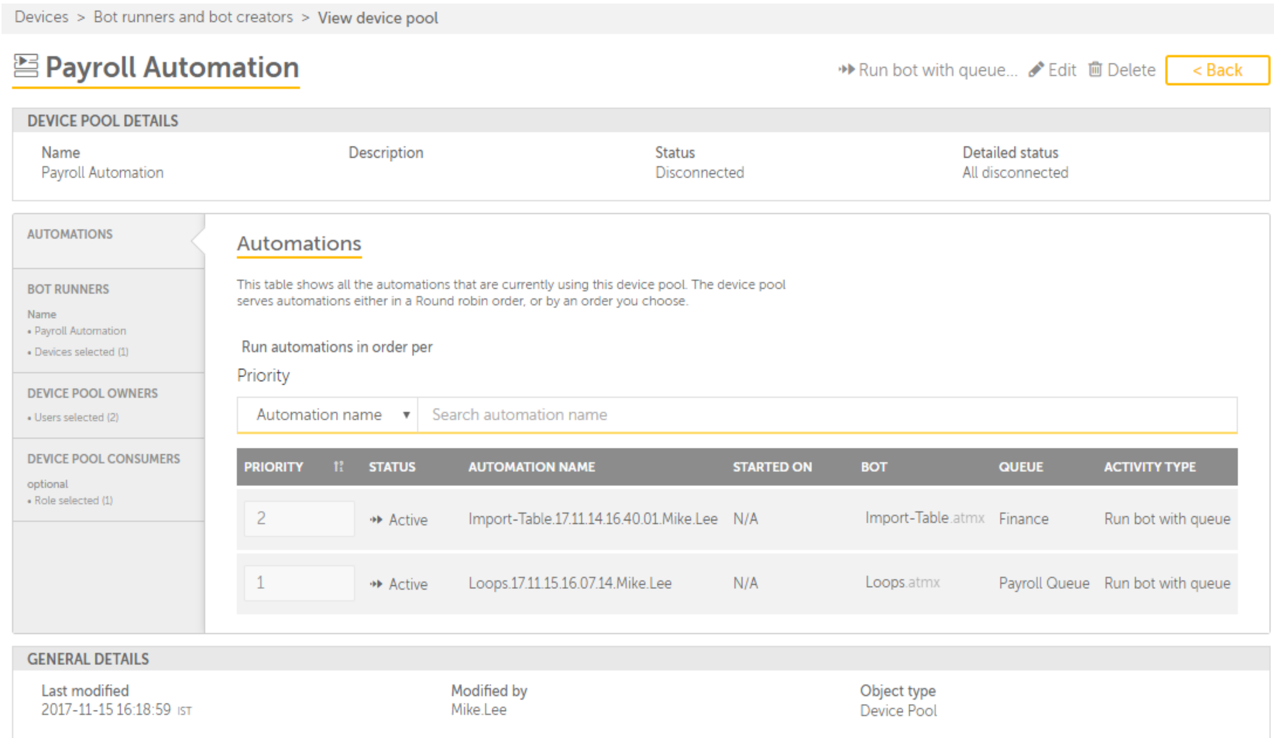


View device pool

As a Control Room user with device pool management privileges or as a device pool owner, you can view device pool details to ensure the information provided is correct and if required customize as per your workload requirement.

To view device pool details,

1. Go to **Devices → My Device Pools**
2. For the device pool that you need to view, mouse over the actions icon -
3. Click
4. The **Device Pool Details** page is launched in view mode



The page provides details of the device pool in two sections:

- Device Pool Details such as the Name, Description, Status, and Detailed Status
- Device Pool contents in tabs such as Automations, Bot Runners, Device Pool Owners, and Device Pool Consumers.

> **Tip:** Select each tab to view its details.

The following provides details for each of the following tabs:

- **Automations -** Shows the automations that are using the device pool and the order that is chosen to run those. This is shown as the default view. To find an automation quickly, use the search option using Status, Automation name, Queue, or Activity type.

  > Tip: You can perform the following actions on a table column:

  - Click a column to sort it in ascending and descending order. You can sort up to three columns by holding the Shift key when you click on two more columns. This gives you the option of sorting two additional columns. This way the sorting is done on the entire table and not just the data that is currently visible to you. The last sorting is stored in memory applied by a user per session.
  - Use a drag-and-drop operation to move the column left or right
  - Move your mouse cursor at the end of the column and drag to re-size
- **Bot Runners -** Shows list of Bot Runners that are part of the device pool.

- **Device Pool Owners -** Shows list of Device Pool Owners that are granted permission to view, edit, and delete the device pool. Refer the article Create and delete device pool for details.
- **Device Pool Consumers -** Shows the list of Device Pool Consumers who are granted permission to view the device pool as an option while running automations. Refer the article Create and delete device pool for details.
- **General Details -** Shows the Last modified date and time, name of the user who modified device pool details, and the Object Type which is the component on which modification was done.

When you view a device pool, apart from updating the Bot Runner, Device Pool Owner, and Consumer details, you can additionally choose to

- Run Bot with queue
- Edit the device pool
- Delete the device pool

Edit device pool

As a Control Room user with device pool management privileges or as a device pool owner, you can edit device pool details to customize as per your workload requirement.

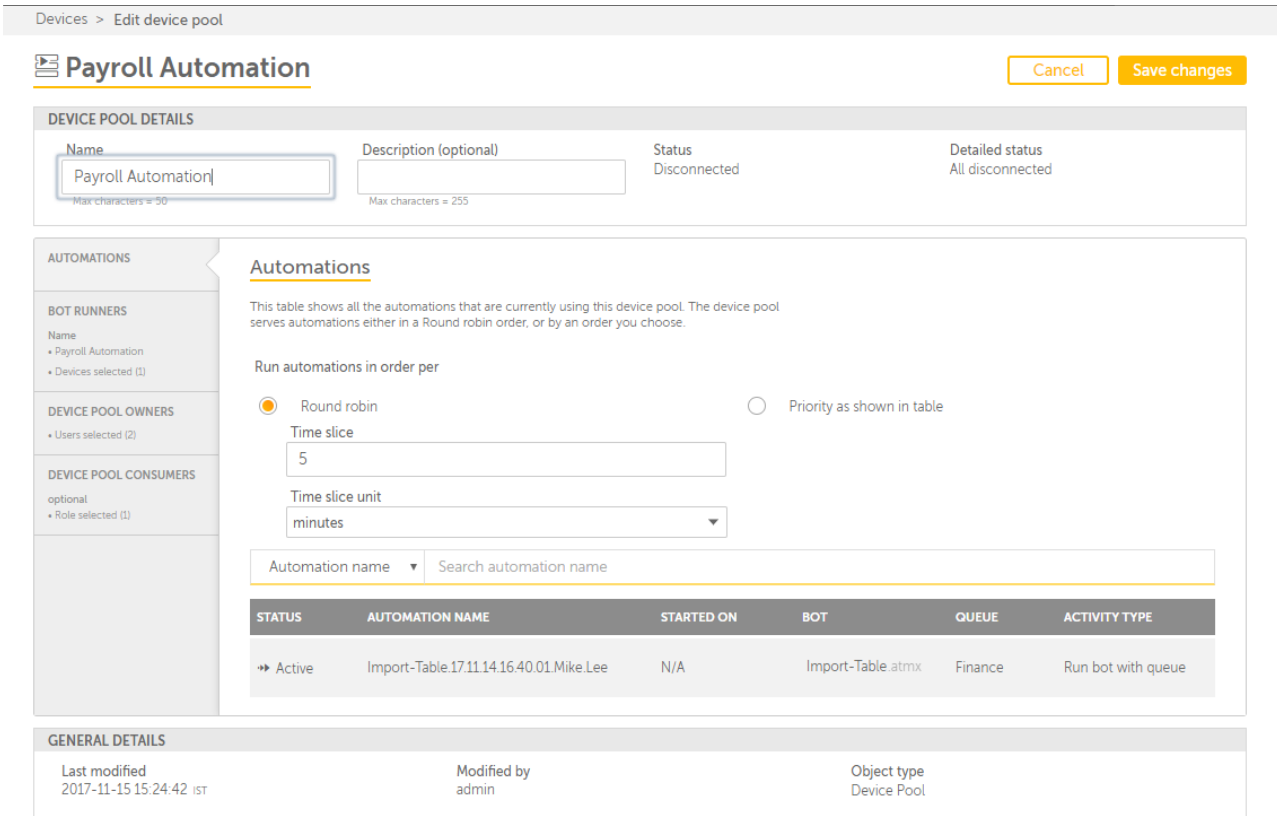
When you open the device pool in edit mode, you have to first define the priority or the order in which the automations will run in the Automations tab. This is visible only when you edit a device pool and is not available when you create a device pool. Apart from this you can update the Bot Runner, Device Pool Owner, and Consumer details.

To edit a device pool,

1. Go to **Devices → My Device Pools**

   > **Tip:** You can also edit device pool details when in view mode. Refer article View device pool to learn more.

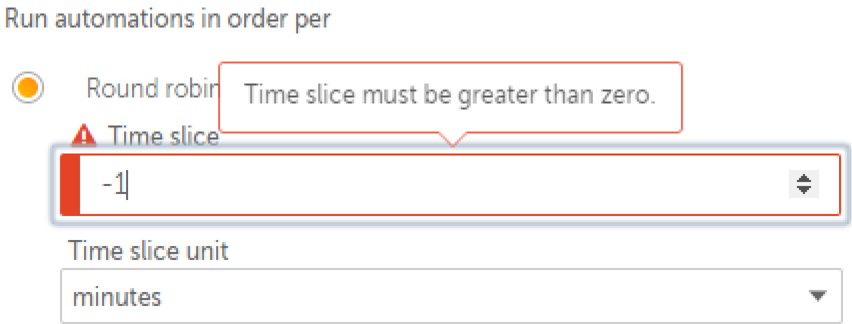
2. For the device pool that needs to be updated, mouse over the actions icon -
3. Click
4. The **Device Pool Details** page is launched in edit mode



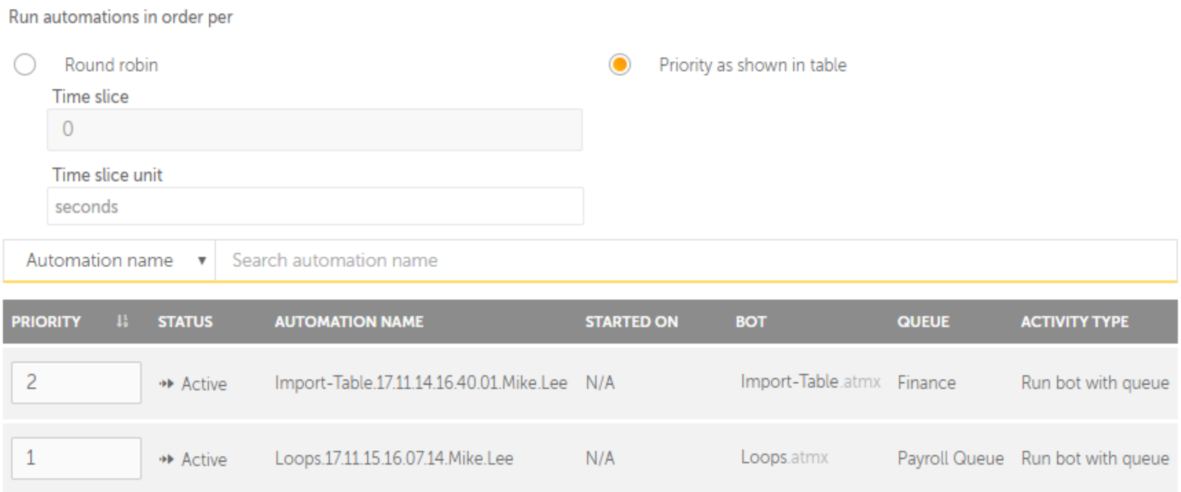
5. You can choose the order in which your automations will run. Select either **Round robin** or **Priority as shown in table.**
   - **Round robin -** Use this when you want to run your automations at equal time intervals termed as **Time slice**. A **Time slice unit** can be defined in seconds, minutes, and hours. You can calculate or estimate the time for each automation and then provide this number.
     This means that the automations are executed for only 5 minutes first, then system checks for other automations in queue for execution, If yes, that automation is paused and next automation is executed. This will continue till all automations in the queue are executed.

     > **Note:** The default Time Slice is set to **5 minutes.**

The Time slice should be more than zero:



- **Priority as shown in table -** Use this when you want to run your automations on priority defined in the Priority table. This method allows you to run automations in order of priority. Automations are processed till all are consumed from the specified automation queue.



The following details are shown in the priority table:

Table Item	Description
Priority	Shows the priority number allotted to that queue
Status	Shows the automation status - Active or Inactive
Automation Name	Shows the automation that is selected to run on the device pool
Started On	Shows the run date and time of the automation
Bot	Shows the Bot name that will run using this device pool
Queue	Shows the Queue name that will be used to run automation using this device pool
Activity Type	Shows the Activity type used to run the automation using this device pool - Run bot

	with queue.

Tip: You can perform the following actions on a table column:

- Click a column to sort it in ascending and descending order. You can sort up to three columns by holding the Shift key when you click on two more columns. This gives you the option of sorting two additional columns. This way the sorting is done on the entire table and not just the data that is currently visible to you. The last sorting is stored in memory applied by a user per session.
- Use a drag-and-drop operation to move the column left or right
- Move your mouse cursor at the end of the column and drag to resize
- Search on Status, Automation Name, Queue, and Activity Type headers in the table if the data available is large.

- The **Priority** column is editable. You can set/re-set automation implementation priority. Ensure that you provide unique priority value to two different work items as same values will not be allowed:

- You can also view the Priority list in ascending or descending order by clicking the ordering arrows in the **Priority** header

6. You can update the list of Bot Runners that will be included in the device pool. Refer the article Create and delete device pool for details.
7. You can update the list of Device Pool Owners who are granted permission to view, edit, and delete the device pool. Refer the article Create and delete device pool for details.
8. You can update the list of Device Pool Consumers who are granted permission to view the device pool as an option while running automations. Refer the article Create and delete device pool for details.
9. Click 

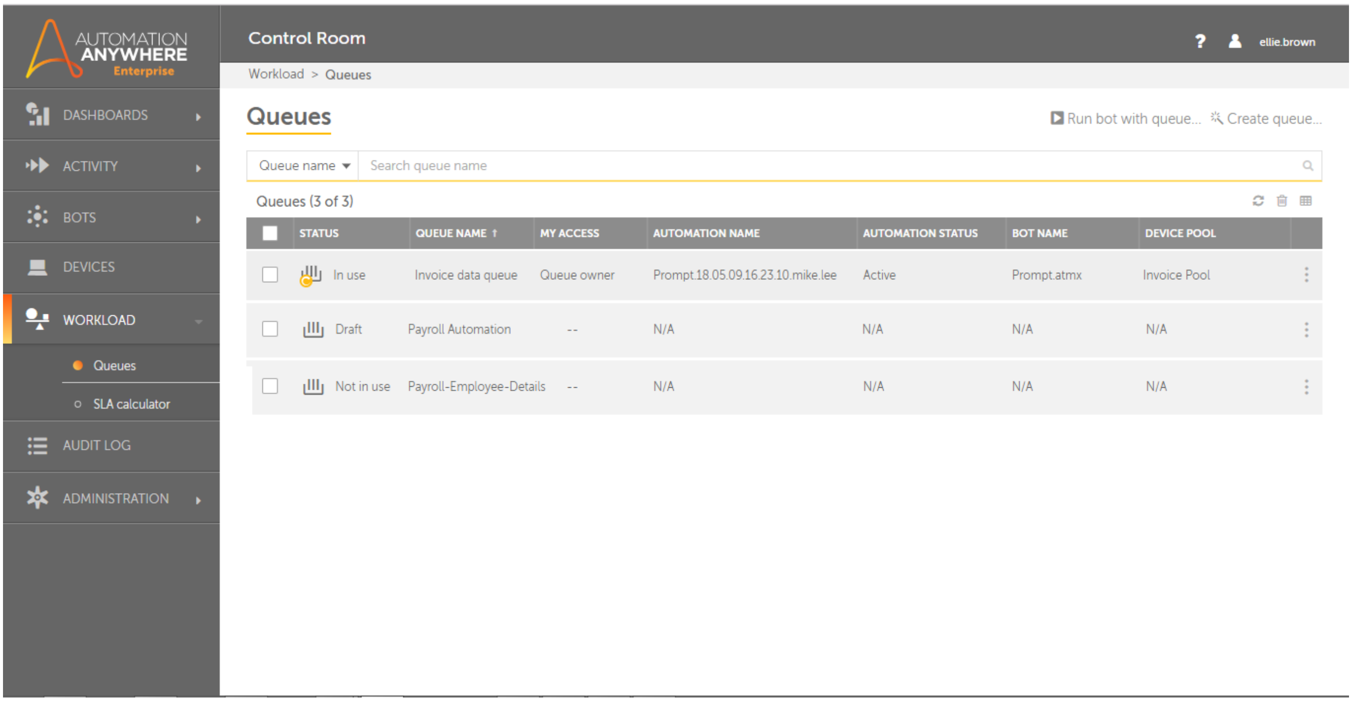
Note: If at any point you do not want to save the changes, click Cancel.

Workload - an overview

Workload Management allows you to manage your work items by dividing them into small yet logical modules and processing those simultaneously to ensure your time based SLAs are met and resource utilization is optimized.

As a Control Room admin user, you can manage the work items in your Control Room instance with help of **Queues**. You can create, update and control the way work items are included in Queues and distributed to Bot Runners that are part of Device Pools.

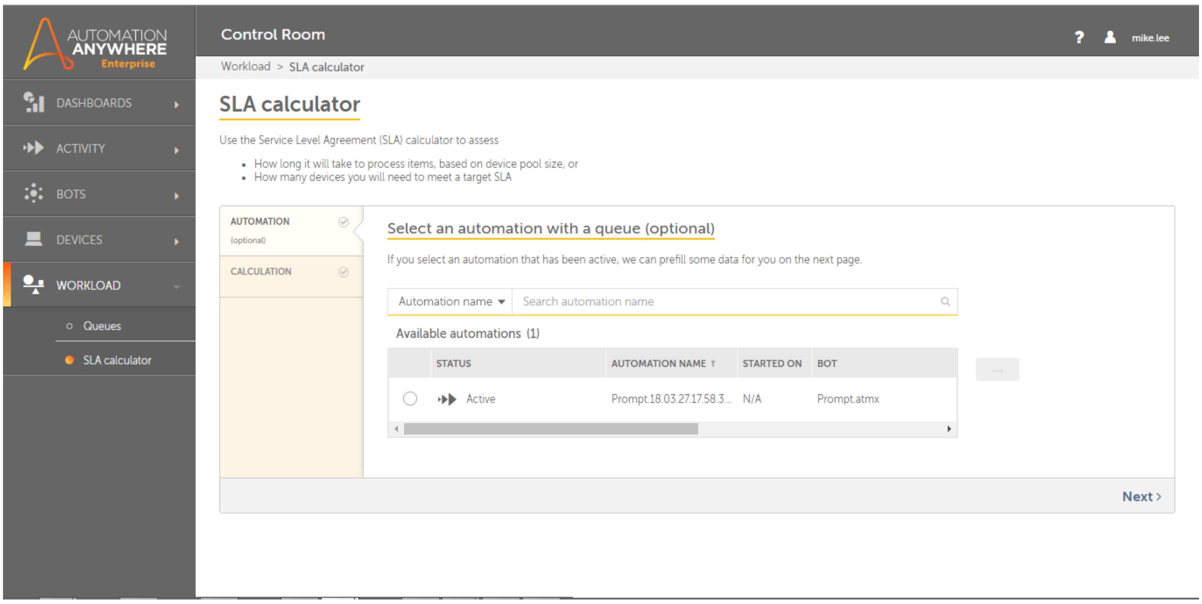
The **Workload - Queues** page is illustrated below:



Refer Workload - Queues for details

As a Control Room admin user or a user with SLA Calculator privilege, you can access the **Service Level Agreement (SLA) calculator** page. It allows you to assess how long would it take to process items based on device pool size or how many devices are required to meet your target SLA.

The **Workload - SLA calculator** page is illustrated below:



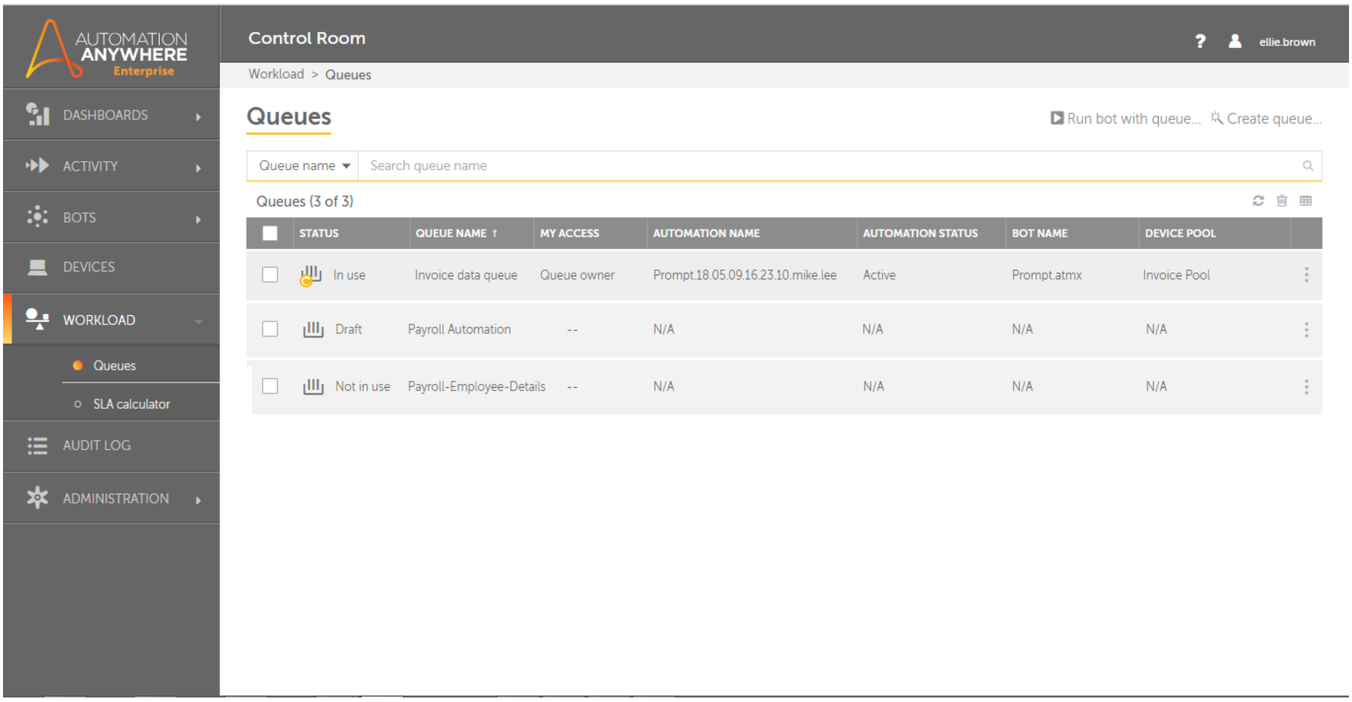
Refer Workload - SLA calculator for details.

Workload - Queues

As a Control Room admin user, you can manage the work items in your Control Room instance with help of **Queues**. You can create, update and control the way work items are included in Queues and distributed to Bot Runners that are part of Device Pools.

Workload Management allows you to manage your work items by dividing them into small yet logical modules and processing those simultaneously to ensure your time based SLAs are met and resource utilization is optimized.

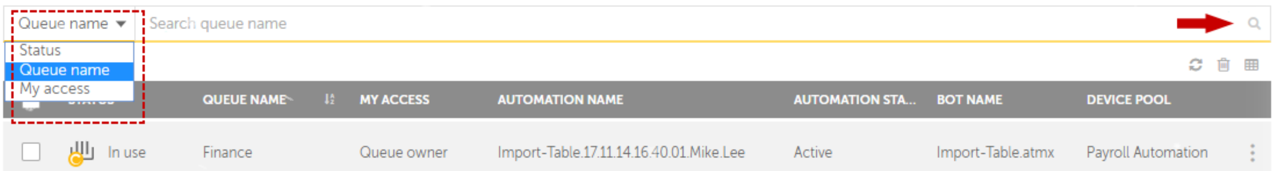
The **Workload - Queues** page is illustrated below:



Note: You can see only those queues for which you are either the owner /participant /consumer. However, the **Queue Admin** can see all the queues in the system.

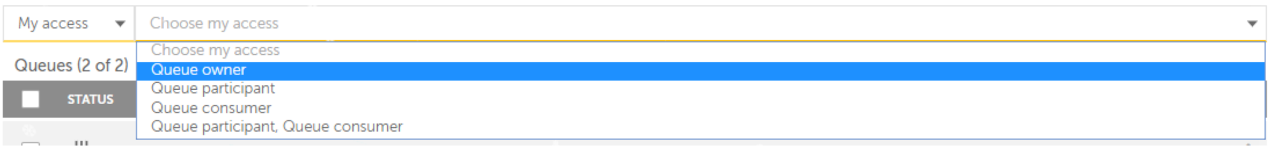
For ease of access, you can apply search parameters to Status, My Access and Queue Name columns.

- You can use specify the search parameters in the search bar for Queue Name:



  When you specify search parameters for the same column, the system searches using **OR** operator. When you specify search parameters for different columns, the system searches using **AND** operator.

- You can choose the search parameters from a list in the search bar for Status and My Access



The following describes the list of items that can be viewed in the table:

Table Item	Description
Status	Shows Queue's status: • **Draft** when the Queue is created but saved as a draft. This option is generally selected by the Queue admin when some information needs to be updated or when the queue is not meant for running automations yet. • **In use** when the Queue is created, saved and used to Run a bot with queue. This shows that an existing automation is using this queue. • **Not in use** when the Queue is created and saved but not used to Run a bot with queue.
Queue Name	Shows the name of the Queue
My Access	Shows the currently logged on user's access status to the queue. • **Queue Owner -** is the user who can create, edit and view the queue. • **Queue Participant -** is the user who can add new work items and view the queue • **Queue Consumer -** is the user who can view the queue and all the work items in the queue.
Automation Name	Shows the name of the Automation. If the queue is not being used or is in draft state, this will show **N/A** and the automation name if in use.
Automation Status	Shows the status of the Automation created for this queue. If the queue is not being used or is in draft state, this will show **N/A** and **Active** if in use.
Bot Name	Shows the name of the Task Bot selected for this queue's automation.
Device Pool	Shows the name of the Device Pool that is used for the automation of this queue.

Tip: You can perform the following actions on a table column:

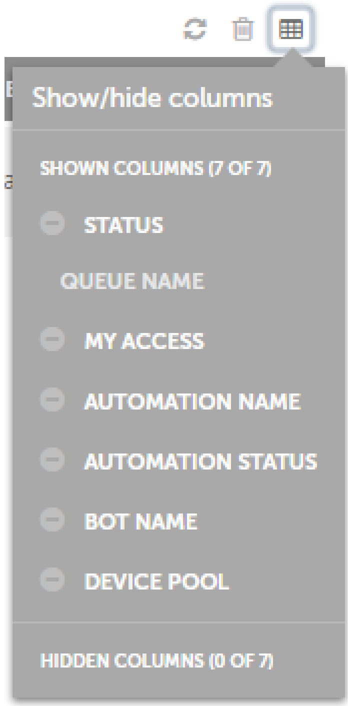
- Click a column to sort it in ascending and descending order. You can sort up to three columns by holding the Shift key when you click on two more columns. This gives you the option of sorting two additional columns. This way the sorting is done on the entire table and not just the data that is currently visible to you. The last sorting is stored in memory applied by a user per session.
- Use a drag-and-drop operation to move the column left or right
- Move your mouse cursor at the end of the column and drag to re-size

The following describes the tasks that you can perform on an individual queue:

Table Item	Description
View	Allows you to view details of selected queue
Edit	Allows you to edit details of selected queue. You can see this icon only if you are the **Queue Owner** or **Participant.**
Delete	Allows you to delete the selected queues. Note that if a queue is in use, you are not allowed to delete the queue.
View automation	Allows you to view the automation in progress. When you click this option, you are navigated to the **Activity → In progress** page for the selected automation.
SLA Calculator	Allows you to estimate device pool size or time required to process a given queue size for the selected automation.

Alternatively, you can select all devices and perform the following action. Note that these actions can be performed only at a table level and not on individual items.

Table Item	Description
Refresh	Allows you to refresh the table contents so that you can view the latest queue status
Delete	Allows you to delete all or multiple queues.
Show / Hide columns	Allows you to show or hide specific columns. By default, all columns are displayed:

	 Tip: To **show** or **hide** a column, click on the column name.

When you want to perform actions such as **Run bot with queue** or **Create queue** quickly without switching your current location, you can use the following options:

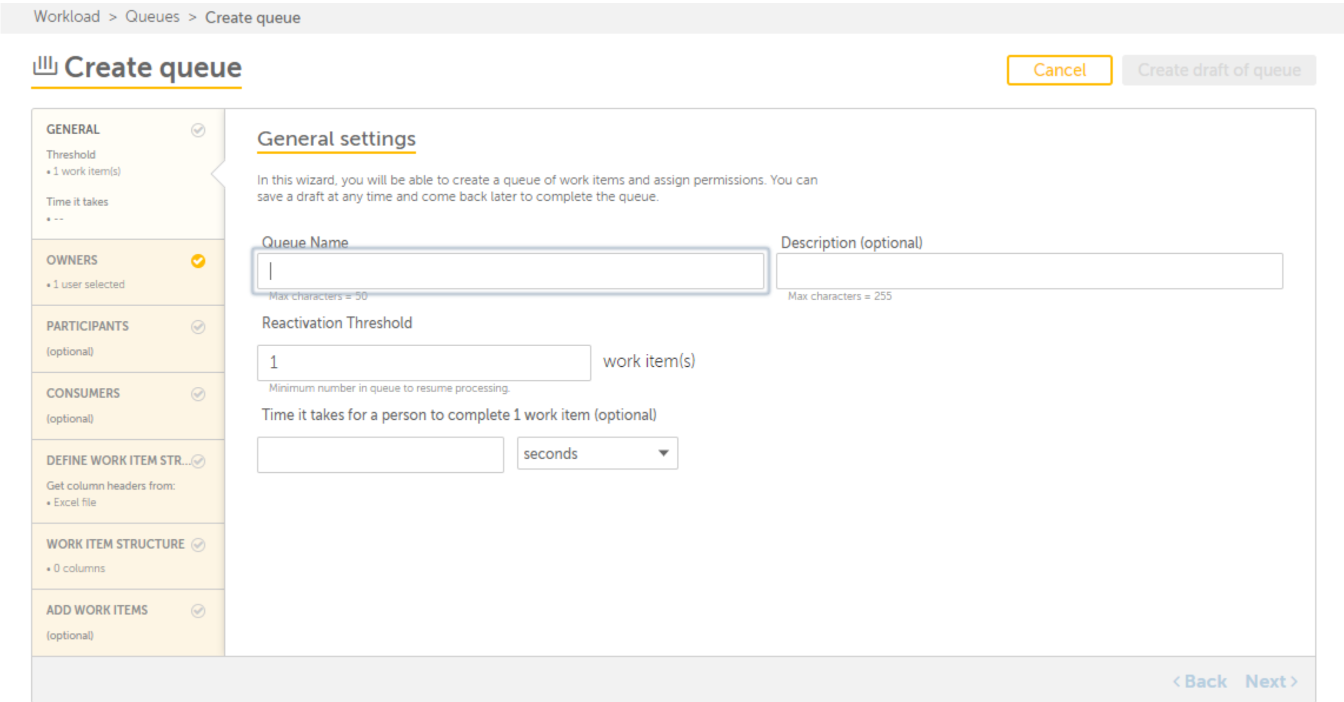
Table Item	Description
Run bot with queue...	Allows you to run bot with a queue
Create queue...	Allows you to create queues

Create queues

As a Control Room user with create queue privilege, you can create queues. Queue is one of main building blocks for Work Load Management. Queue holds data (Work Items) that will be processed. System distributes these work items to individual Bot Runners in a Device pool for processing.

You can define a queue to hold a specific set of data that your bot is expecting. For example, you can create Payroll Data Queue with payroll related information for a Payroll Processing bot. Work items can be added to the queue by uploading a CVS/Excel file or from an API.

The following illustration shows the **Create queue** page when it is launched:



Create queues

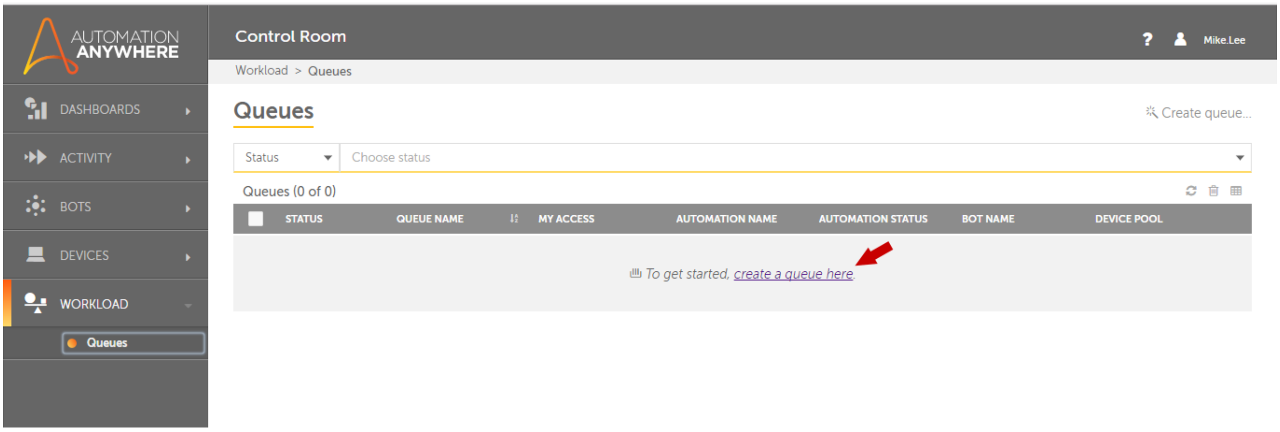
You can **Create queue** by providing details such as Queue name, Queue owners, participants, consumers and work item structure.

These details are summarized in the tab on the left side. You can refer this summary while editing the queue and open the tab that you want to update. Refer the article Edit Queue.

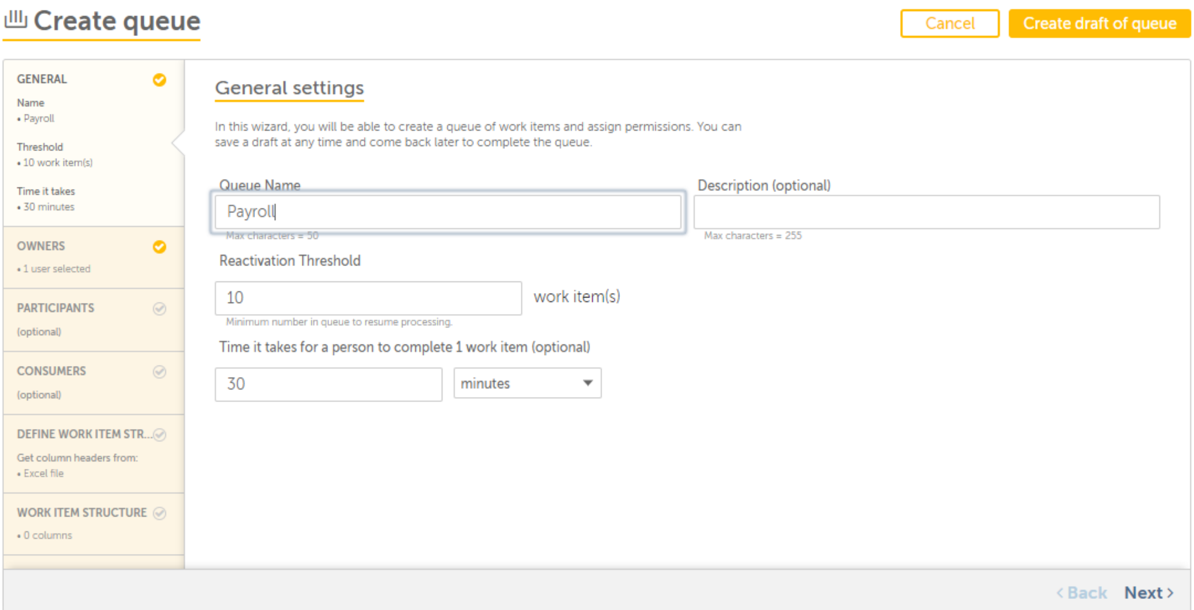
To Create a queue:

1. Go to **Workload** → **Queues**
2. Click 

   or if you are creating a queue for the first time, click on the Create a queue here link, which is available when you launch the Queues page as shown:

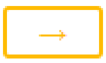


3. The Create queue page is launched wherein you can first configure **General Settings**
   a. **General settings -** Here, you can specify general settings for the queue such as Queue Name, Description, Reactivation Threshold, and Time required for a person to complete one work item.

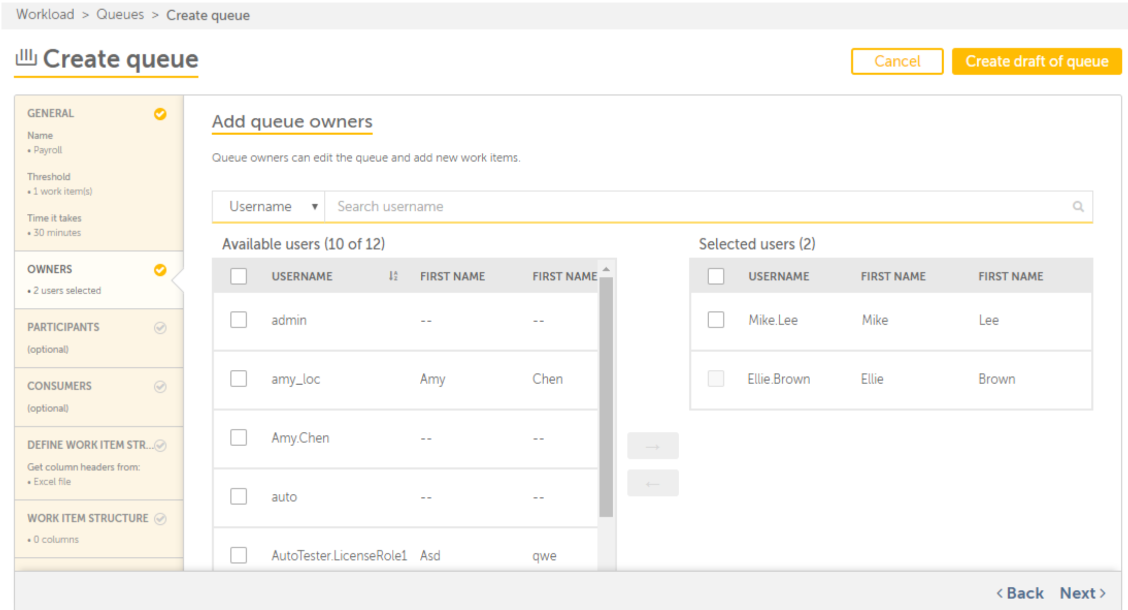


      i. Type a name for the queue that reflects its purpose in **Queue Name**. For example, you can specify Payroll Queue for work items that are designed to manage the payroll system.
      ii. Optionally type in the **Description** that reflects what the queue will achieve. For example, the Payroll Queue will process those automations that are designed to manage the payroll system.
      iii. Specify the minimum number of new work items (i.e. in 'Ready to Run' status) that should be present in the queue in order to resume the queue processing after all the work items in the queue are processed in **Reactivation Threshold.** By default this is set to 1.
      iv. Optionally, specify the average time that a person would need to complete one work item in **seconds**, **minutes**, **hours** or **days**.
      v. Click **Next** to assign queue owners.

```
Tip: You can choose to save a draft of the queue by clicking Create draft of queue and
add rest of the information later.
```

   b. **Owners -** Add name(s) of Queue Owner(s) to **Selected Users** from the list of **Available Users**. Queue owners can edit the queue and also add new work items to the queue. The Queue creator is the default **Queue Owner**. You can choose to add other users as Queue Owners only if required.
      i. To add Queue Owners, select user(s) from list of **Available Users**
      ii. Click 

iii. The users are added as **Queue Owners** in the list of **Selected Users**:



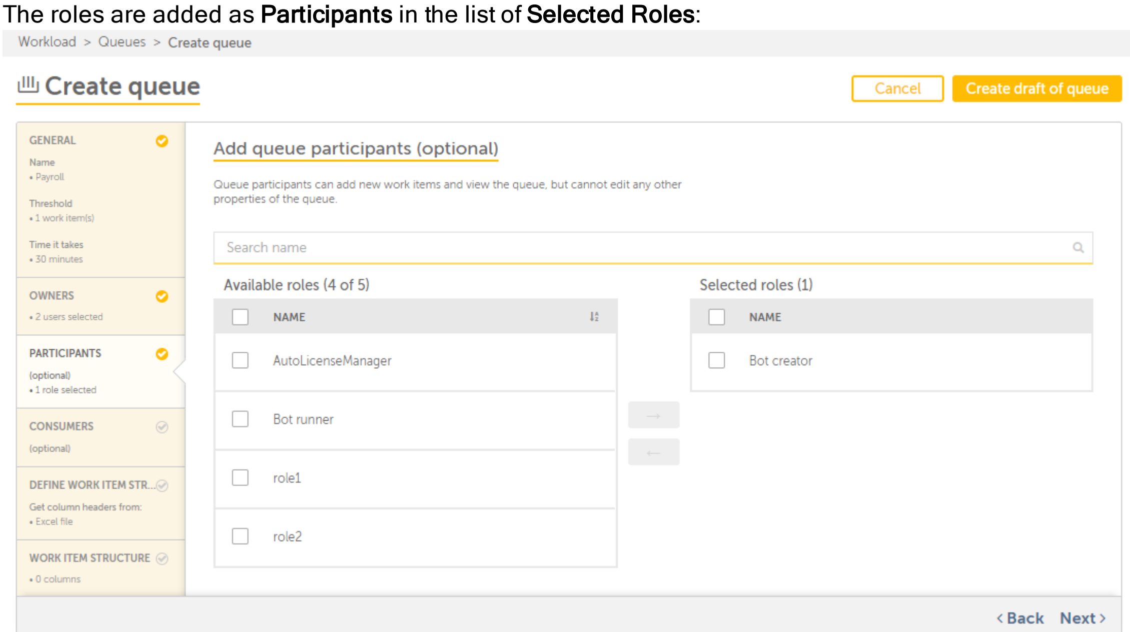
iv. Click **Next** to add roles as queue participants

c. **Participants -** Optionally add Roles as Participants from the list **Available Roles**. Participant roles can add new work items and view the queue. however, they are not allowed to edit other queue properties.

i. To add **Participants**, select role(s) from list of **Available Roles**

ii. Click →

iii. The roles are added as **Participants** in the list of **Selected Roles**:



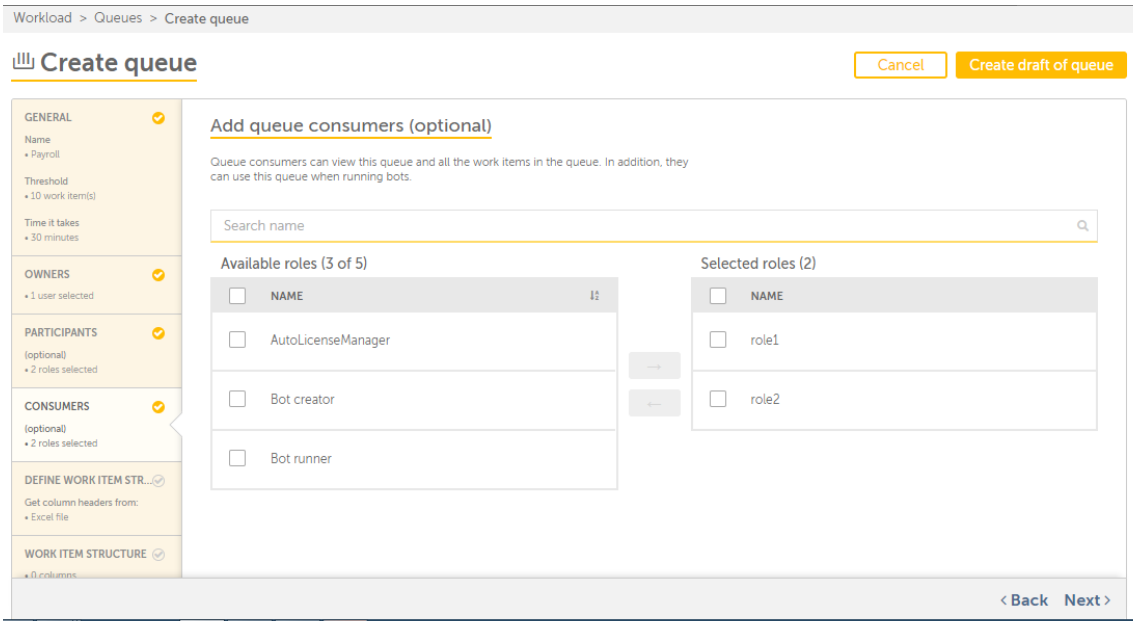
iv. Click **Next** to add queue consumers

d. **Consumers -** Optionally add Queue **Consumers** from the list of **Available Roles**. Queue consumers can view the queue and all the work items in the queue. In addition, they can use this queue when running bots.

i. To add **Consumers**, select role(s) from list of **Available Roles**

ii. Click →

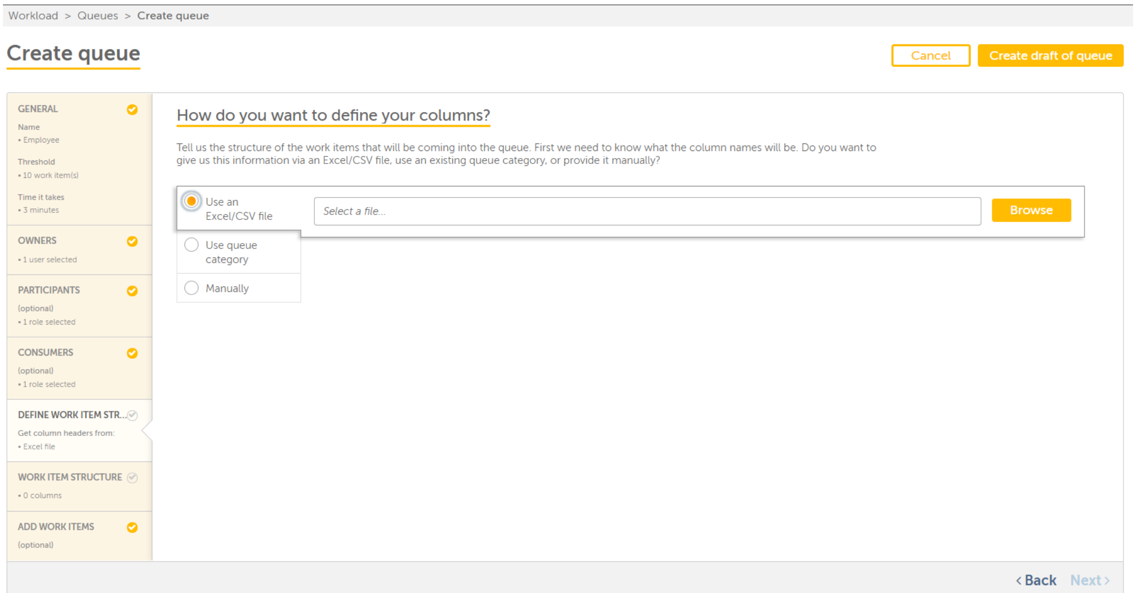
iii. The roles are added as **Consumers** in the list of **Selected Roles**:



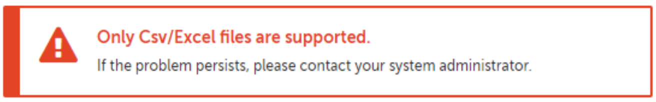
iv. Click **Next** to define the work item structure.

e. **Define Work Item Structure -** You can define the work item structure when you do not have the ready data in a file and directly want to load the work items manually from the system. Define the structure of the work items that will be processed in the queue. For this you must add column names to the structure. This can be done in either of **three** ways:

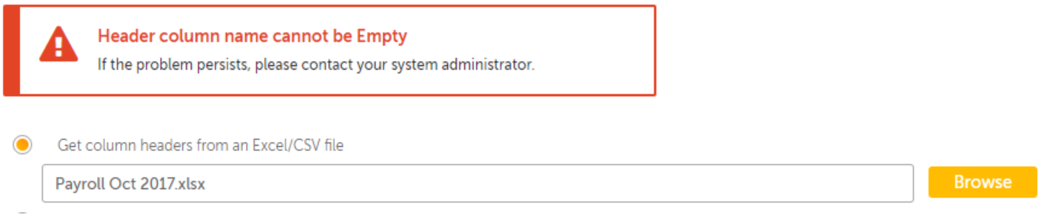
i. Selecting a csv or excel file that automatically populates the headers to the structure by clicking **Browse...**:



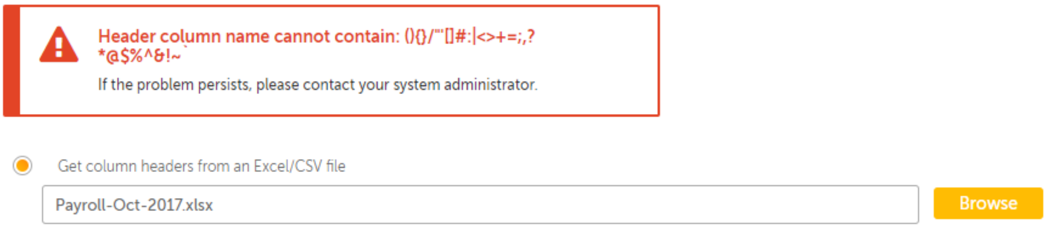
- Only excel or csv files are allowed. For any other file, the following error is shown:



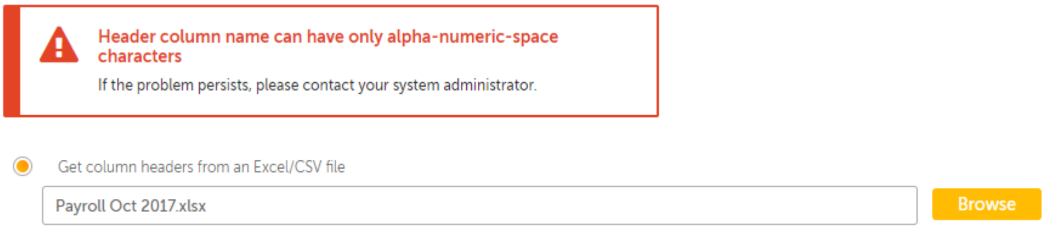
- If the header column name is empty in the excel/csv file, the following error is shown:



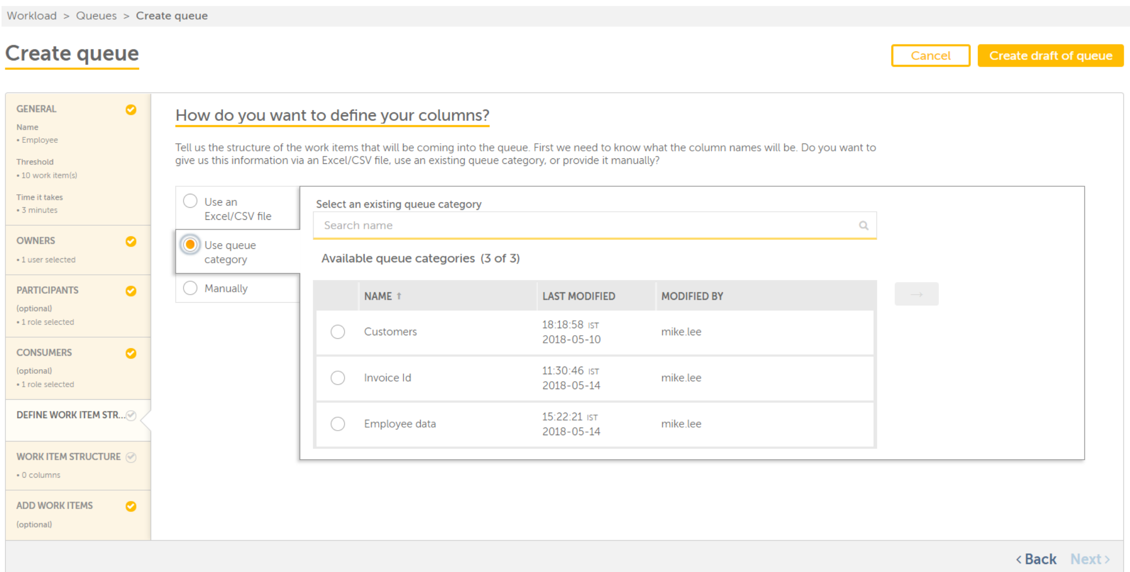
- If the header column name has special characters, following error is shown:



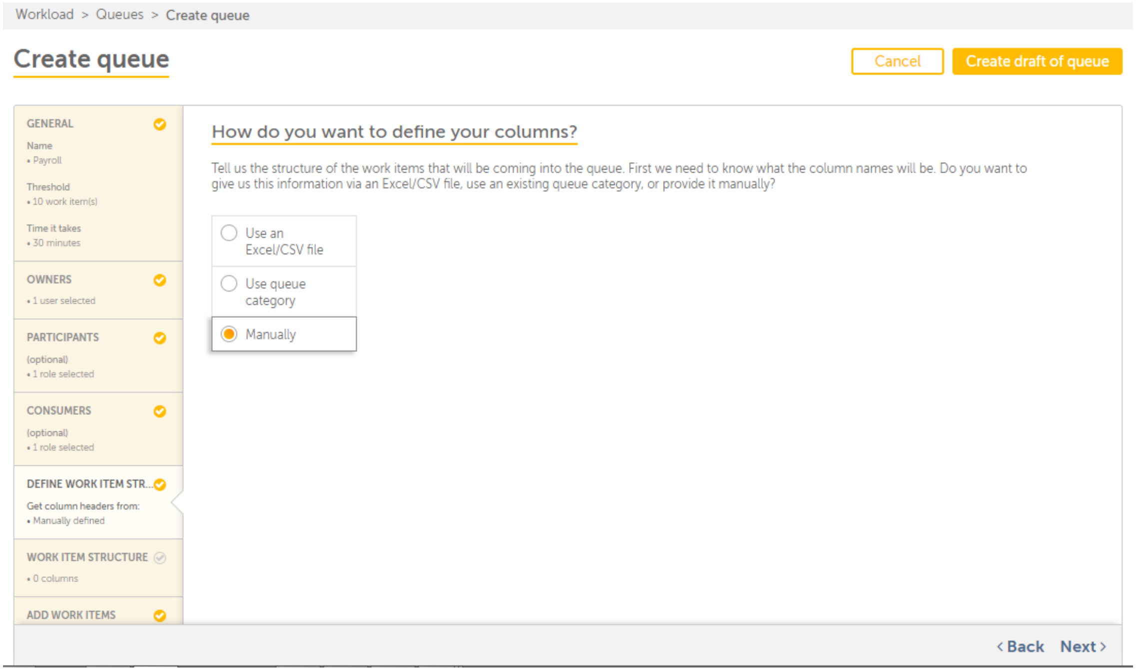
- If the header column name contains characters other than alpha numeric spaces, the following error is shown:



ii. Selecting from an existing **Queue Category**:



iii. Adding column headers **manually** to the structure.



iv. Click **Next** to select the data category and column headers that will be processed.

f. **Work Item Structure -** Based on the option that you choose in **Define Work Item Structure** panel, your workflow to process work items in this queue differs.

a. Adding header columns using an **Excel/CSV file** - When you select this option, you can define the work structure in steps:

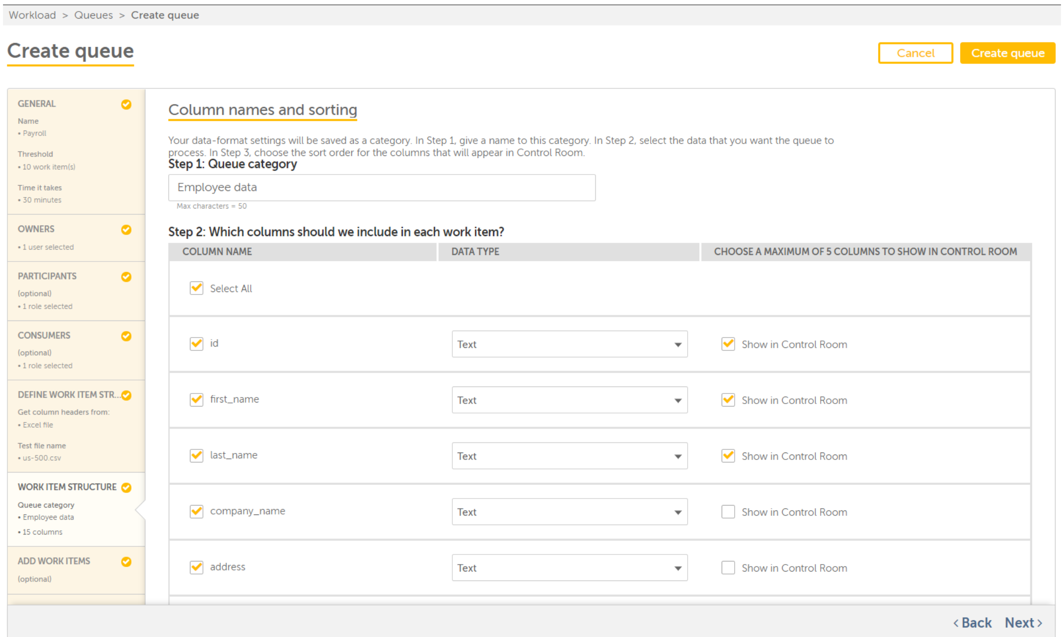
i. In **Step 1**, you must provide a name to the work item structure in Queue Category. For example, if the queue contains employee information, you can specify Queue Category as 'Employee Data'. Queue category should be unique.

ii. In **Step 2**, you are shown all the column names from the header row. You can choose only those columns that you want to include in the work item structure.
You can select up to five columns to view in the Control Room. While viewing work item data in Control Room, system allows you to filter/sort work items only on these selected five columns.

For example, you can select column headers **Employee Name**, **Employee ID** and **Designation**. You can then select the **Data Type** for that column. In our example selected columns belong to the **Text** data type.You can also choose to view those columns being processed in the Control Room Activity page.

iii. In **Step 3**, you can choose to sort the selected column data in **Ascending** or **Descending** order. Out of the five "Show in control room" selected columns, you can select up to three columns to specify the sort criteria. When the system is processing work items from this queue, it will use the sort criteria specified to fetch the work items in that order.

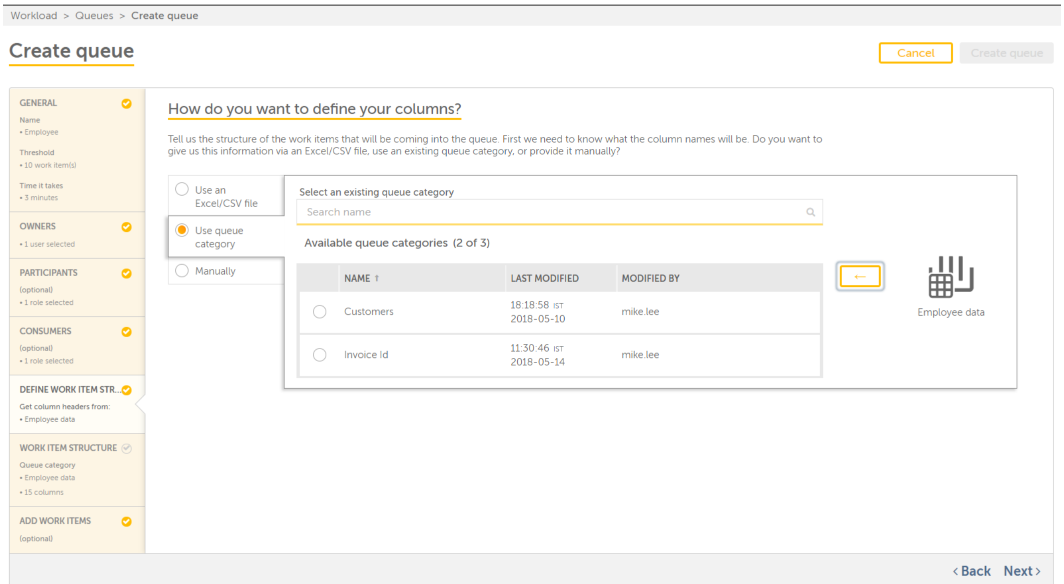
For example, if you want to process payslips with first Employee Id followed by Employee Name from **1 to n** and **A to Z**, you can specify Employee Id and Employee Name in **Ascending** order.



iv. Click **Next** to add the data to work items.

b. Adding header columns using **existing queue category** - When you select this option, you can select from a list of Available queue categories:

i. Either search for an existing queue category when there are a large number of categories available for selection or select one from the list:



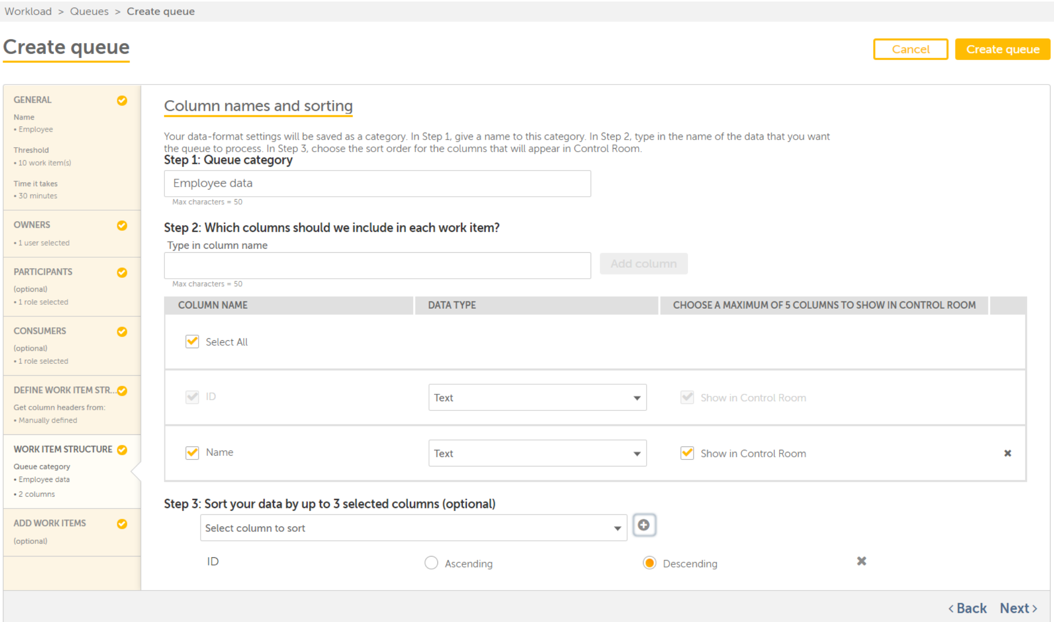
ii. Click **Next** to add the data to work items.

c. Adding header columns **Manually** - When you select this option, you can define the work item structure manually. You do not have to select from an existing structure.

a. In **Step 1**, provide a name to the work item structure in **Queue Category** field. For example, if the queue contains employee information, you can specify Queue Category as 'Employee Data'. Queue category should be unique.

b. In **Step 2**, add column header names that should be included in the work item. Also define the data type for each column - Text, Number, or Date.

c. In **Step 3**, optionally provide the order in which the columns should be displayed and sorted in the Control Room.

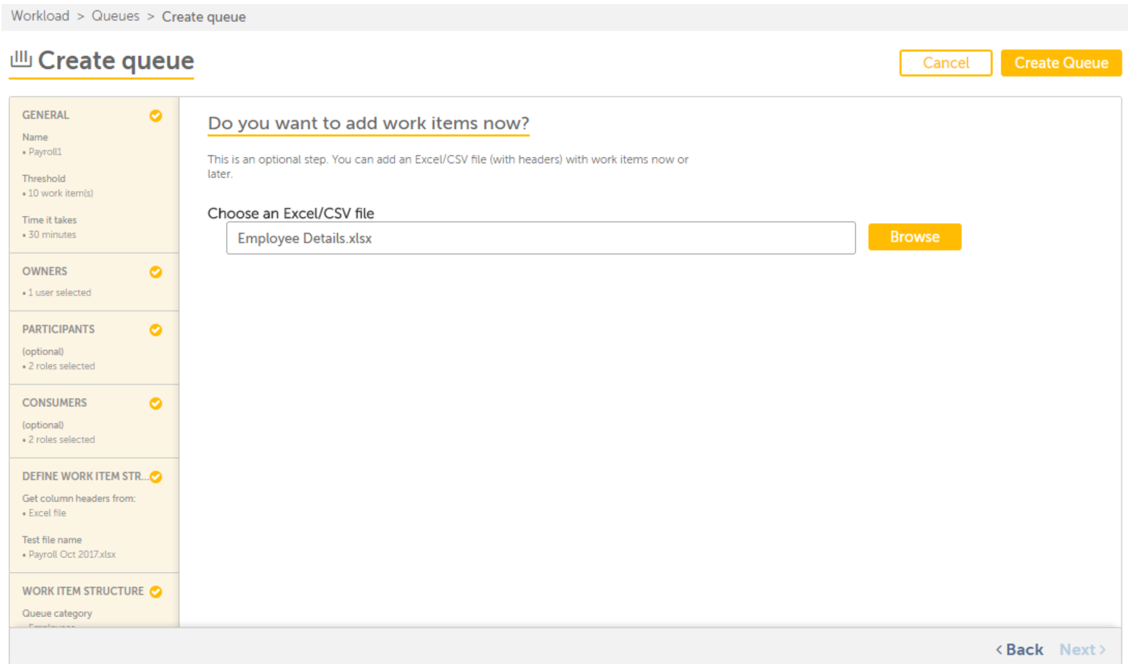


d. Click **Next** to add data to the work items.

g. **Add Work Items -** Optionally choose an excel or csv file if you want to add work items to this queue. You can add work items later by editing the queue.

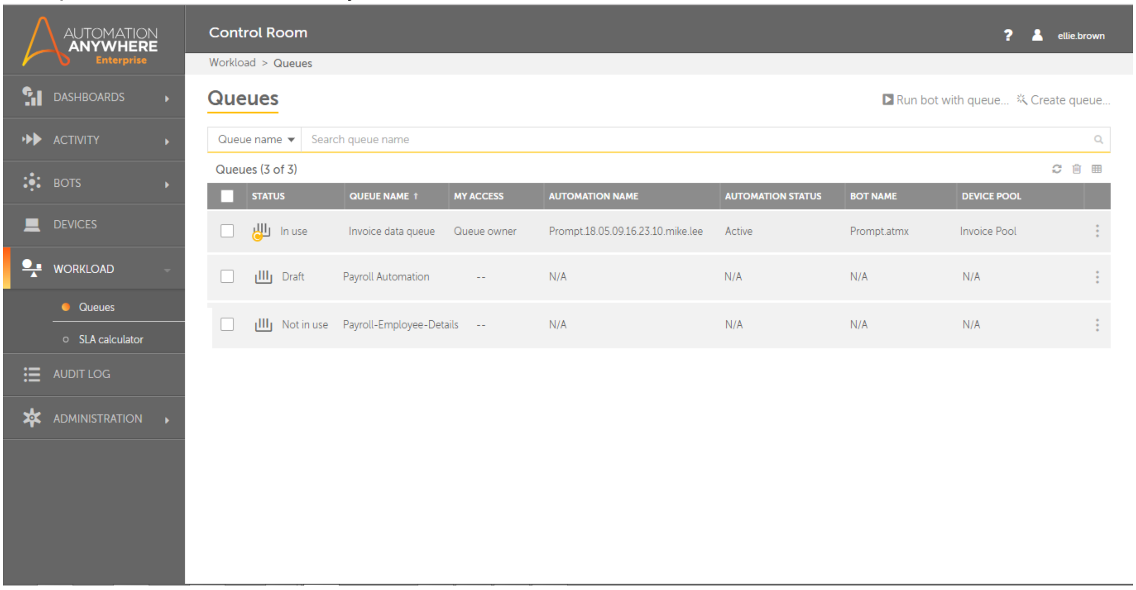
i. To add an excel or csv file, click Browse...

ii. The file is added as a work item.



iii. Click Create Queue

iv. The queue is added successfully added to the list :



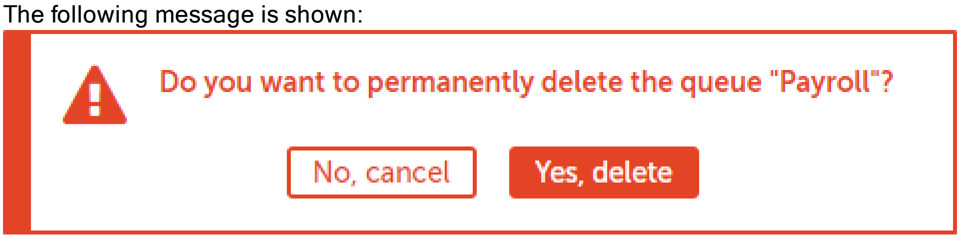

```
Tip: The new queue is added at the top of the list. You can choose to apply column
sorting to view as required.
```

Delete Queues

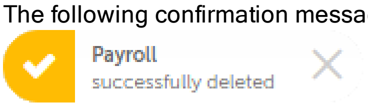
You can delete the queues if you have **Queue Admin or Owner** access rights. You can delete an individual queue, selected or all queues.

To delete an individual queue,

1. Go to **Workload → Queues**
2. For the queue that needs to be deleted, mouse-over the actions icon -
3. Click
4. The following message is shown:

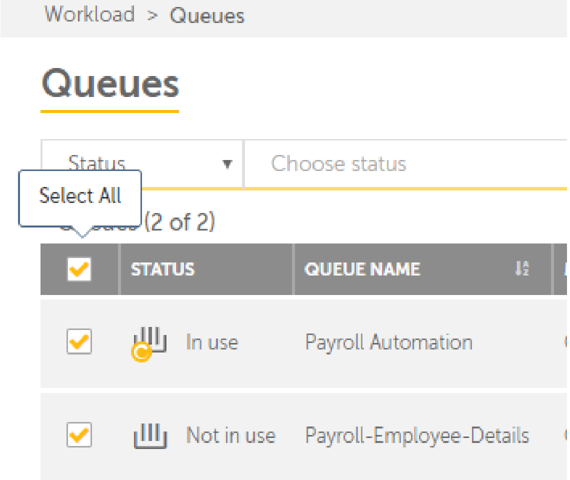


5. Click **Yes, delete** to confirm or **No, cancel** to discard the action.
6. The following confirmation message appears once you delete the queue:

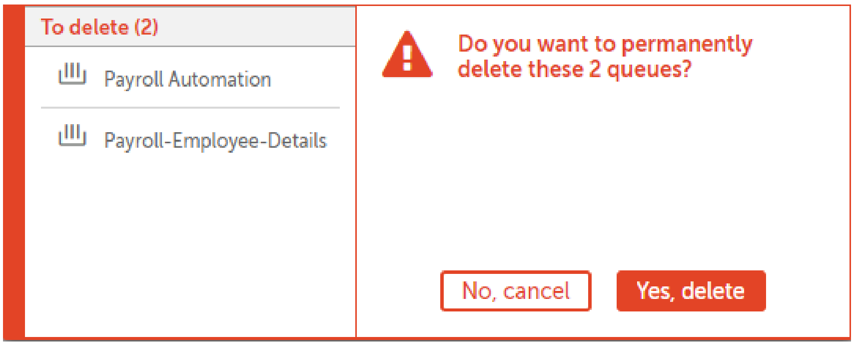


To delete selected or all queues:

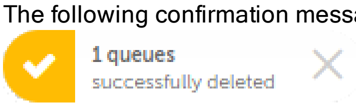
1. Go to **Workload → Queues**
2. Select the check-box of required queues or select the check-box given in the header to select all queues:



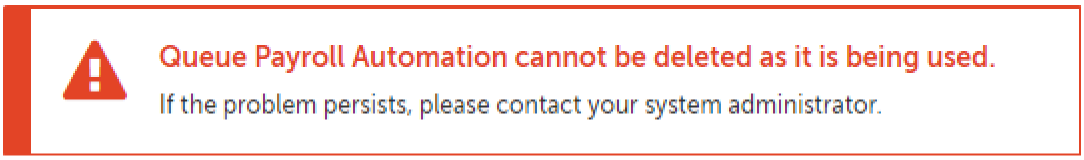
3. Click above the table header.
4. The following message is shown:



5. Click **Yes, delete** to confirm or **No, cancel** to discard the action.
6. The following confirmation message appears once you delete the queues:



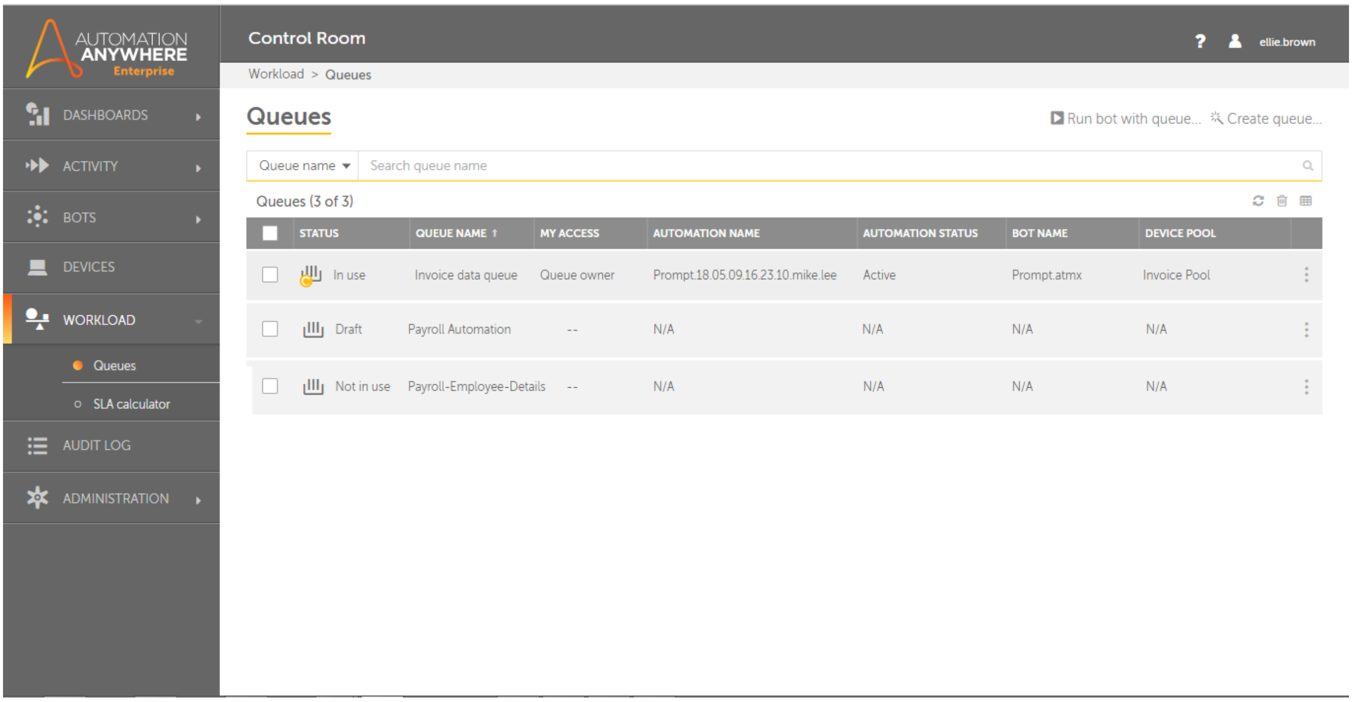
Note: Only one queue is deleted instead of two because the second queue is being used for processing work items. For that particular queue you are shown the following error:



Edit queues

As a Control Room user with owner privileges you can edit the queues that you created and as a user with participant privileges you can edit queues that are created by other queue owners.

Refer Queue Owners section in Create Queues article.



You can edit a queue using two methods - from **Queues** list and from **View queue** page

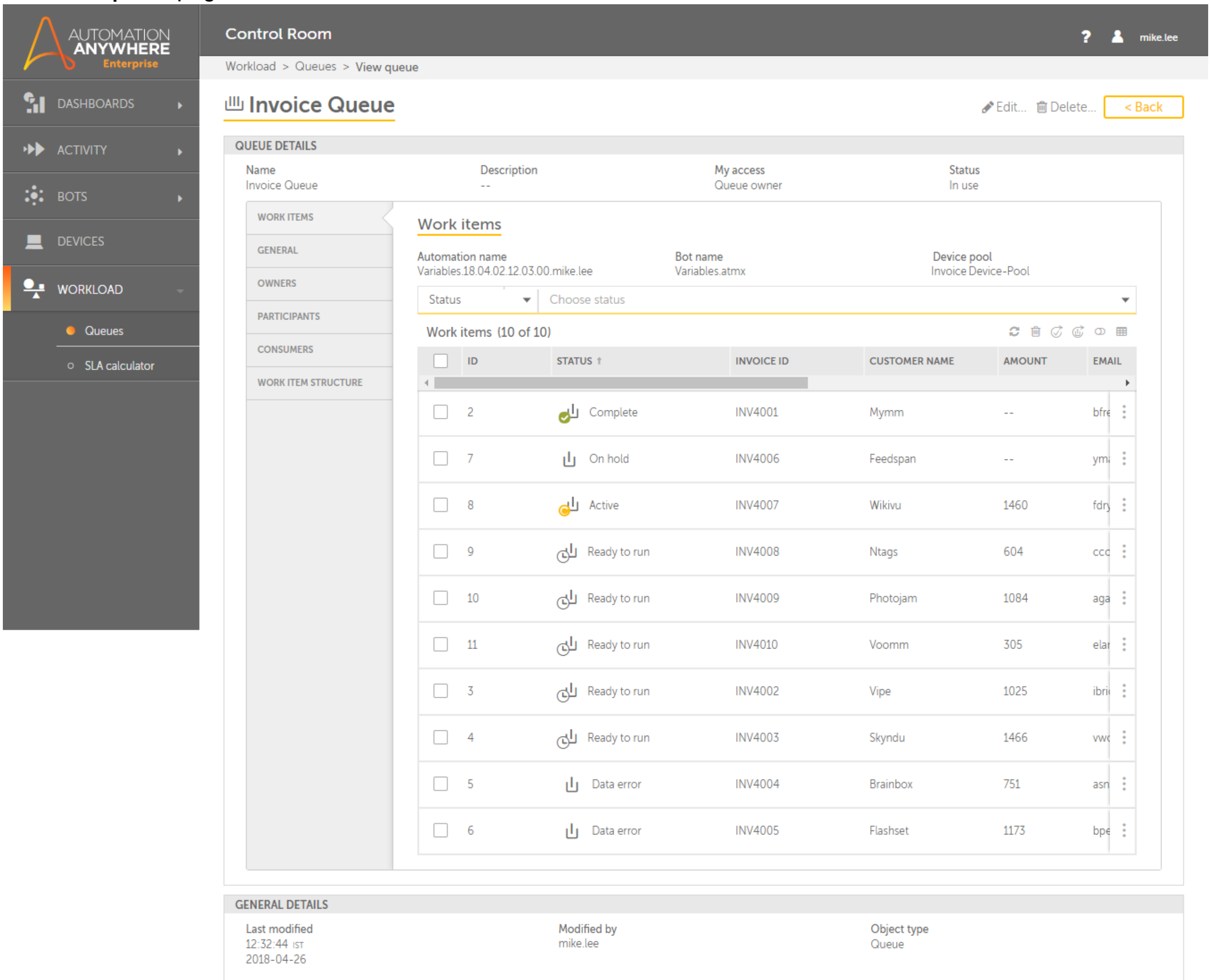
- To **Edit** a queue from **Queues** list,

1. Go to **Workload** → **Queues**
2. For the queue that needs to be updated, mouse over the actions icon -
3. Click

- To Edit a queue from View queue page,

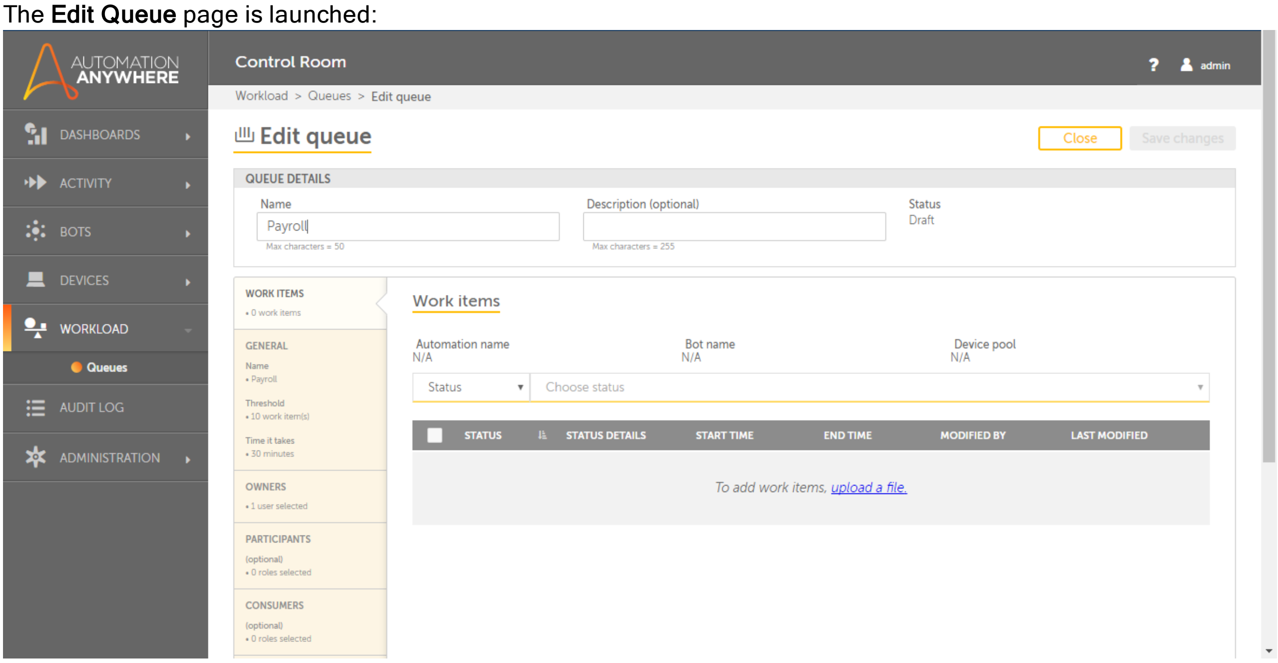
1. Go to **Workload** → **Queues**
2. For the queue that needs to be updated, mouse over the actions icon -
3. Click

4. The **View queue** page is launched:



5. Either click on **edit this queue** link or Edit...

6. The **Edit Queue** page is launched:

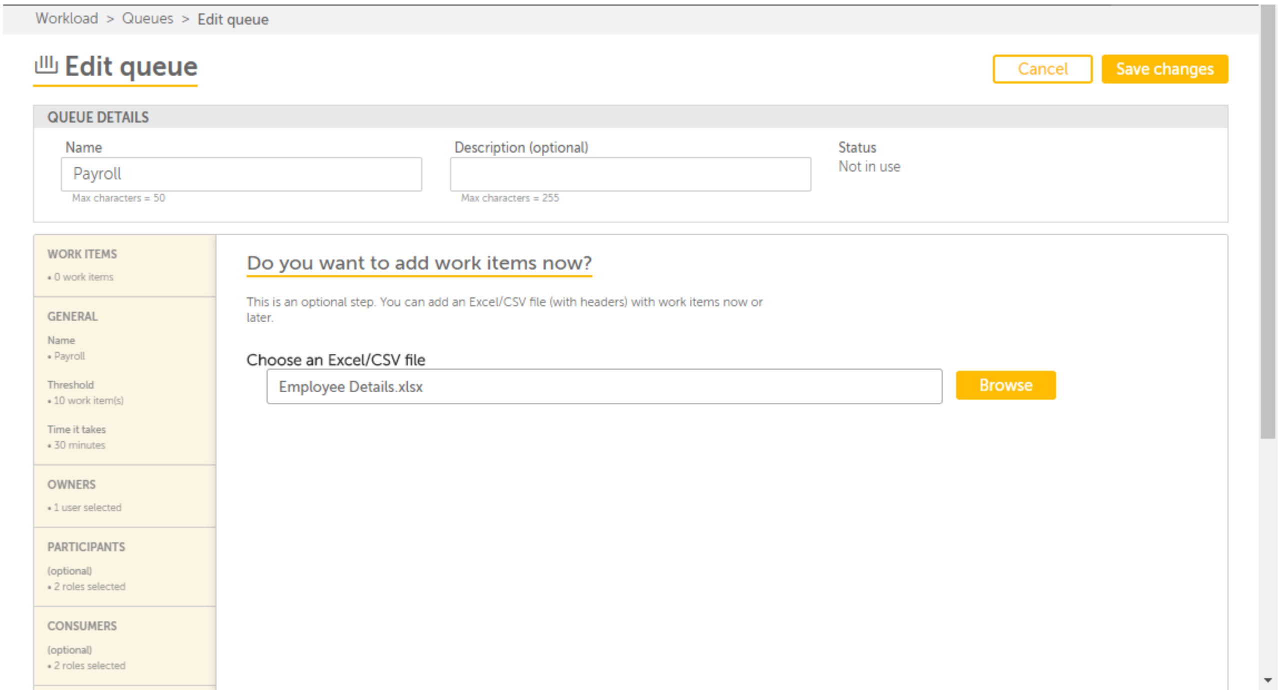


Note: You can choose to **Close** or **Cancel** your updates. The **Close** option is available when you do not make any updates. It changes to **Cancel** when you update the page.

7. You can choose to edit the entire queue details such as the queue name (applicable only if in draft), description, work items, threshold and time values, owners, participants, and consumers. The Work Item structure cannot be edited once it is defined. Refer article Create Queues to know more about adding details in each tab.
8. By default, you are shown the **Work Items** tab wherein you must first upload a file for the work item that will be used for processing in this queue.

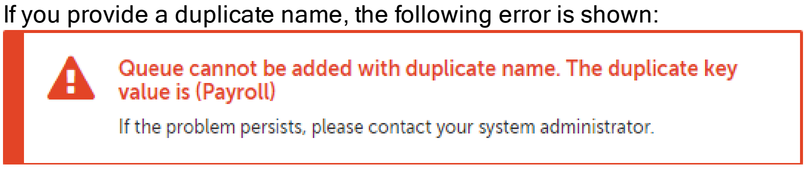
> **Tip:** You can search for a work item quickly based either on **Status** or **Status details** using the search option.

9. Click **Browse...** and select the file that you want to upload.

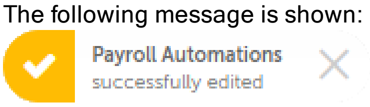


> **Tip:** You can upload only an excel or csv file.

10. Click **Save changes** when you finish updating details as required.
    - If you provide a duplicate name, the following error is shown:



    - Edit the name and save the changes made to the queue.
11. The following message is shown:

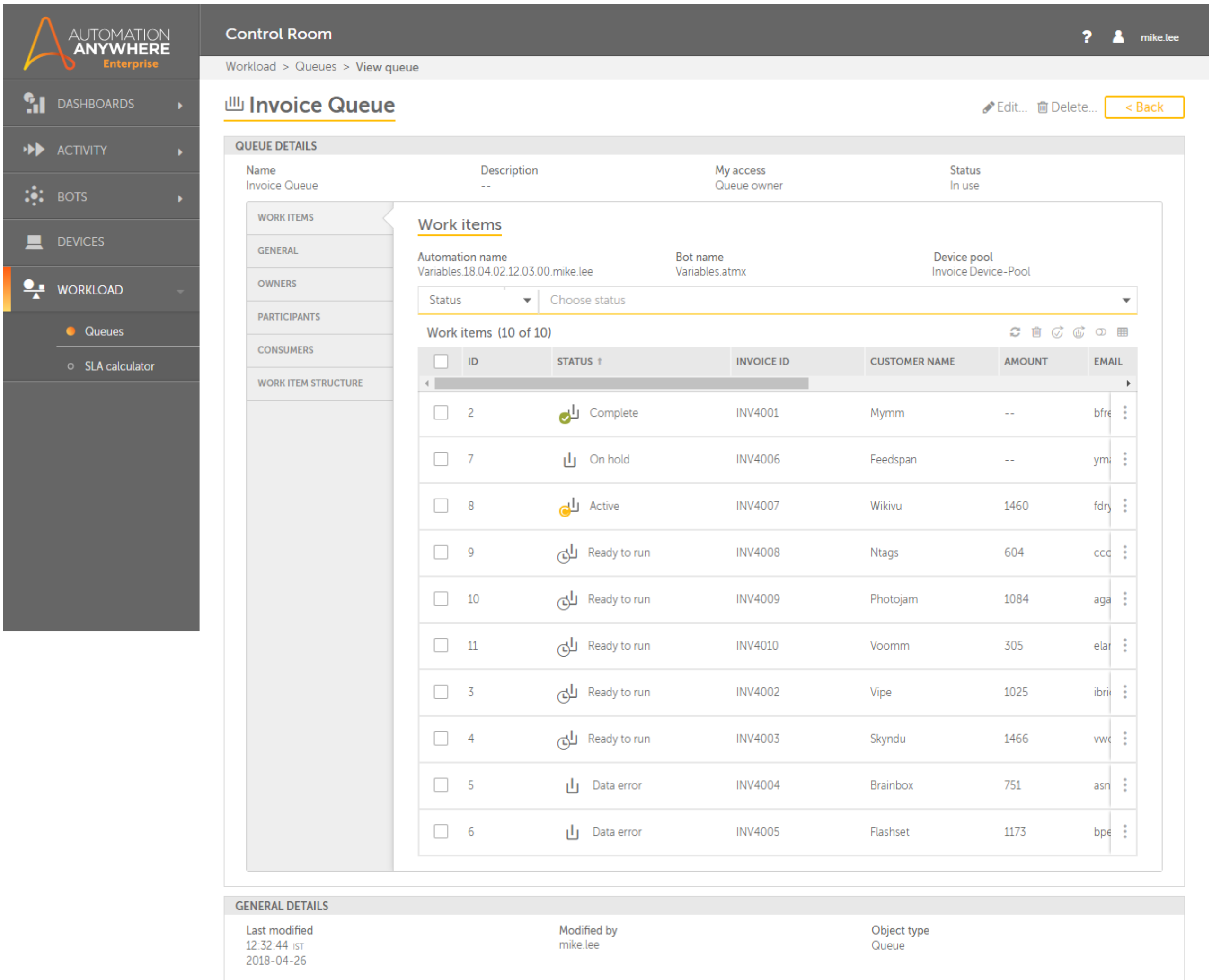


View queue details

As a Control Room user with queue management privileges you might want to view the details of a Queue that either you created or are granted participant rights.

To view details of a particular queue,

1. Go to **Workload → Queues**
2. Mouse over the queue that you want to view and click
3. Click
4. The **View queues** page is launched:



5. The page provides details of the queue in two sections:
   a. Queue Details such as the **Name**, **Description**, **My access** status, and queue **Status**
   b. Queue contents in different tabs such as,
      i. **Work Items -** This is the default view. This allows you to view all work items in a list form. You can perform actions such as edit and delete as well as modify the column view, and change the status of all or selected work items.
      ii. **General -** This displays the **Reactivation Threshold** and **Time** required to complete one work item,
      iii. **Owners -** This displays Queue owners who can edit the queue and add new work items.
      iv. **Participants -** This displays Queue Participants who can add new work items and view the queue.
      v. **Consumers -** This displays Consumers who can view the queue and all the work items in the queue. In addition,

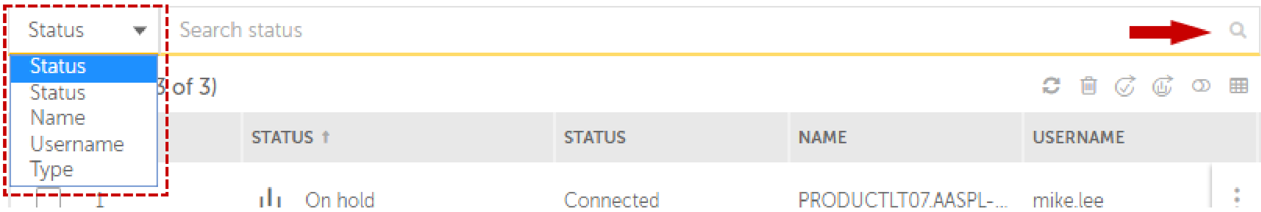
they can use this queue when running bots.

vi. **Work Item Structure -** This displays the work item structure that you defined when creating the queue.

> **Tip:** You can choose to edit any of these details by either clicking the **edit this queue** link or Edit... . You can also delete the queue by clicking Delete... . Refer the articles Edit queues and Create and delete queues for details.

For ease of access, you can apply search parameters to Status, My Access and Queue Name columns.

- You can use specify the search parameters in the search bar for Queue Name:



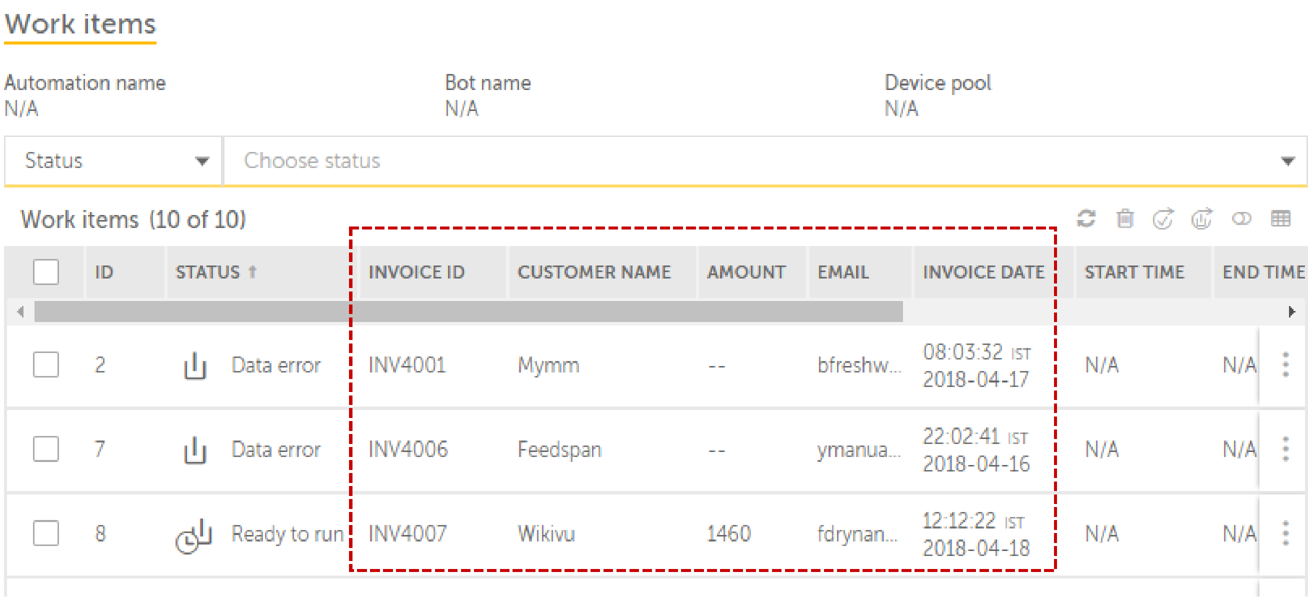
When you specify search parameters for the same column, the system searches using **OR** operator. When you specify search parameters for different columns, the system searches using **AND** operator.

- You can choose the search parameters from a list in the search bar for Work item Status

The following describes the list of items that can be viewed in the table:

Table Item	Description
ID	Shows the system generated id for a work item. When a work item is added to a queue, system generates an id for that work item.
Status	Shows Work item status: • **Active** when work item is currently being processed or staged for processing • **Complete** when work item successfully processed by a Bot Runner or marked Complete • **Unsuccessful** when work item processing failed on Bot Runner • **Ready to run** when work item is successfully processed for execution does not have any data errors and can be staged for processing • **On hold** when work item is deferred from processing by a Bot Runner • **Data error** when there is an error in loading data from the file
Start Time and End Time	Shows the work items processing start/end time and date
Modified by	Shows the name of the user who had modified the work item last
Last Modified	Shows the time and date when the work item was modified last

> **Note:** Apart from the above system generated columns, the fields that you define in your work item are also displayed as columns:



Tip: You can perform the following actions on a table column:

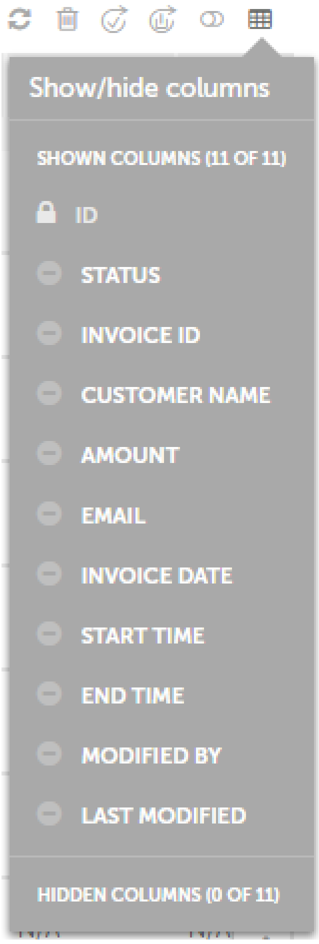
- Click a column to sort it in ascending and descending order. You can sort up to three columns by holding the Shift key when you click on two more columns. This gives you the option of sorting two additional columns. This way the sorting is done on the entire table and not just the data that is currently visible to you. The last sorting is stored in memory applied by a user per session.
- Use a drag-and-drop operation to move the column left or right
- Move your mouse cursor at the end of the column and drag to re-size

The following describes the tasks that you can perform on an individual work item:

Table Item	Description
View	Allows you to view details of selected work item
Edit	Allows you to edit details of selected work item. You can see this icon only if you are the **Queue Owner** or **Participant** or **Consumer** and the status of the work item is **Unsuccessful**, **On hold**, or **Data error**
Delete	Allows you to delete the selected work item. Note that if a work item is in **Active** state, you are not allowed to delete it.

Alternatively, you can select all devices and perform the following action. Note that these actions can be performed only at a table level and not on individual items.

Table Item	Description
Refresh	Allows you to refresh the table contents so that you can view the latest work item status
Delete	Allows you to delete one or multiple work items.
Mark complete	Allows you to mark one or more work items as **Complete** whose status is **On hold**, **Data Error**, or **Ready to run**.
Ready to run	Allows you to mark one or more work items as **Ready to run** whose status is **On hold**, or **Data Error**
On hold	Allows you to mark one or more work items as **On hold** whose status is **Ready to run**
Show / Hide columns	Allows you to show or hide specific columns. By default, all columns are displayed including the ones defined in the work item:



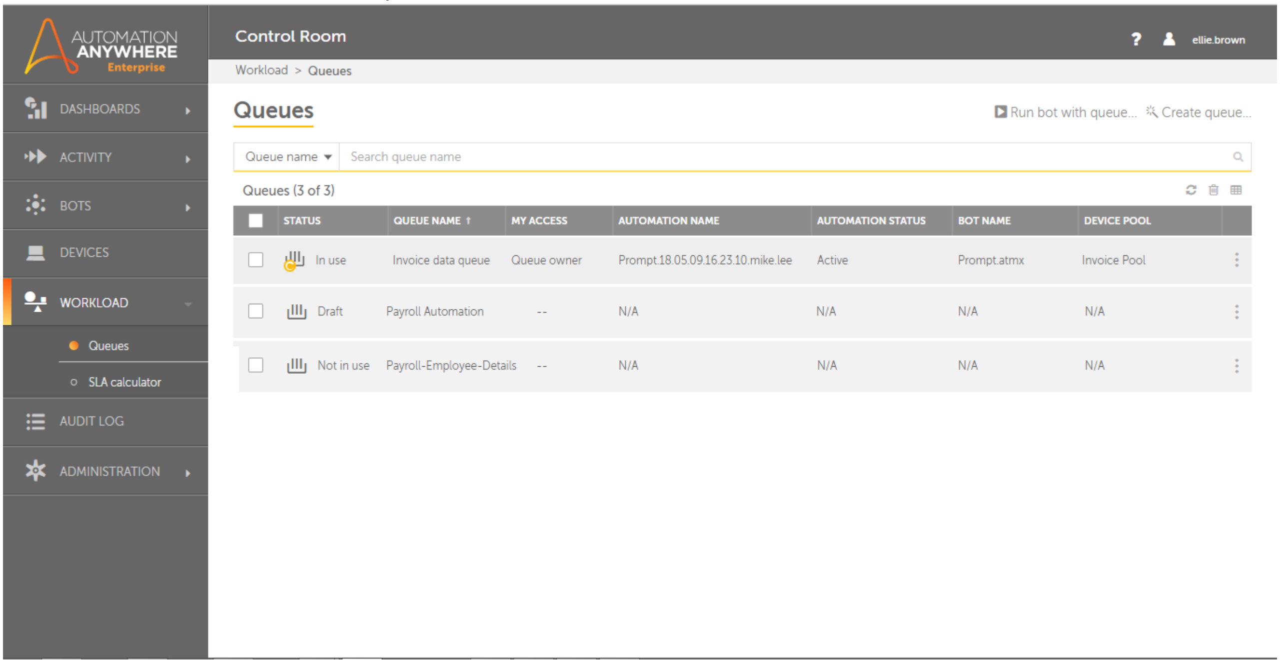
Tip: To **show** or **hide** a column, click on the column name.

View automation of a queue

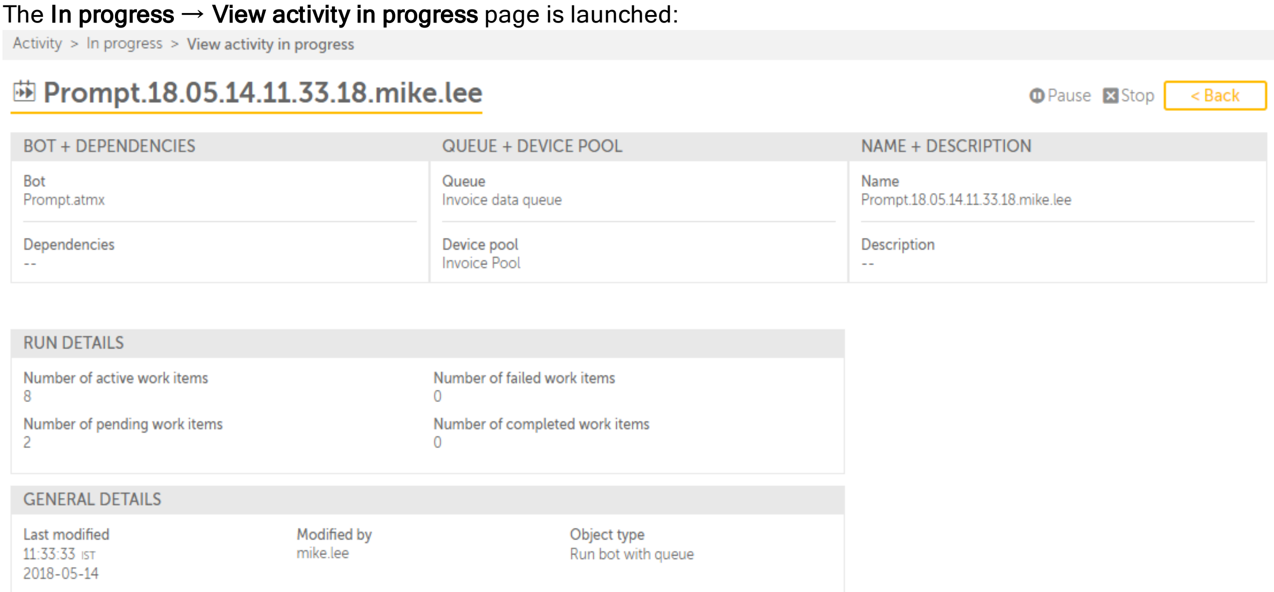
You can choose to **Pause**/**Resume** or **Stop** an in progress automation when you have the **Manage my in progress activity** permission.

To view in progress activity details of an active automation,

1. Go to **Workload** → **Queues**
2. Mouse over the action icon - of a queue with status **In use**:



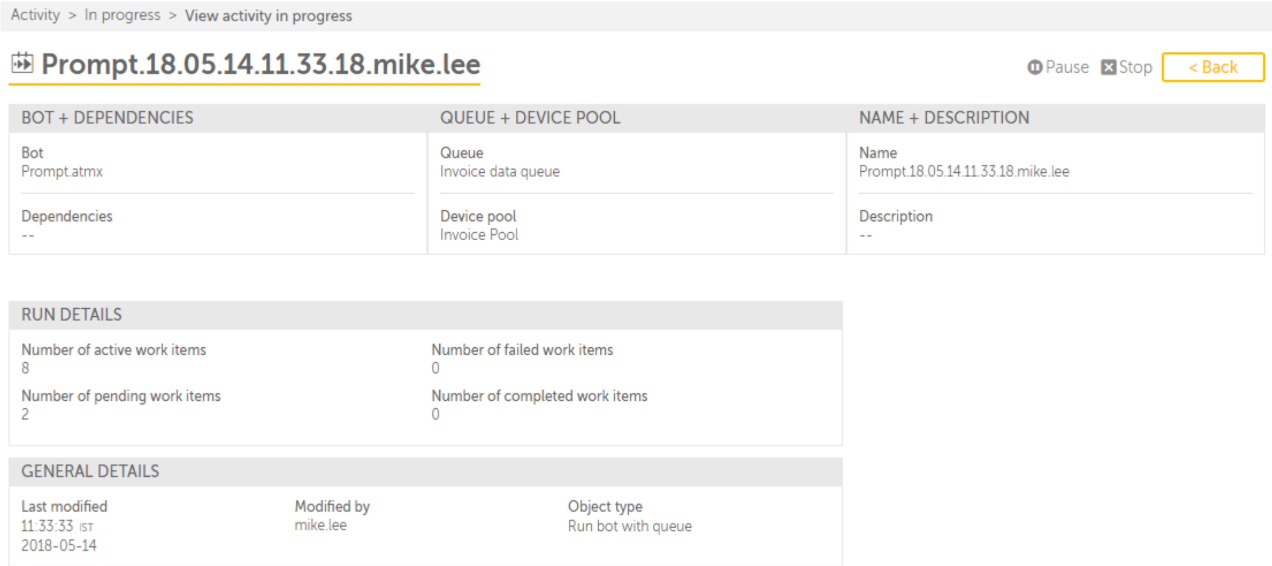
3. Click
4. The **In progress** → **View activity in progress** page is launched:



Here, you can choose to **Pause**/**Resume** or **Stop** the automation.

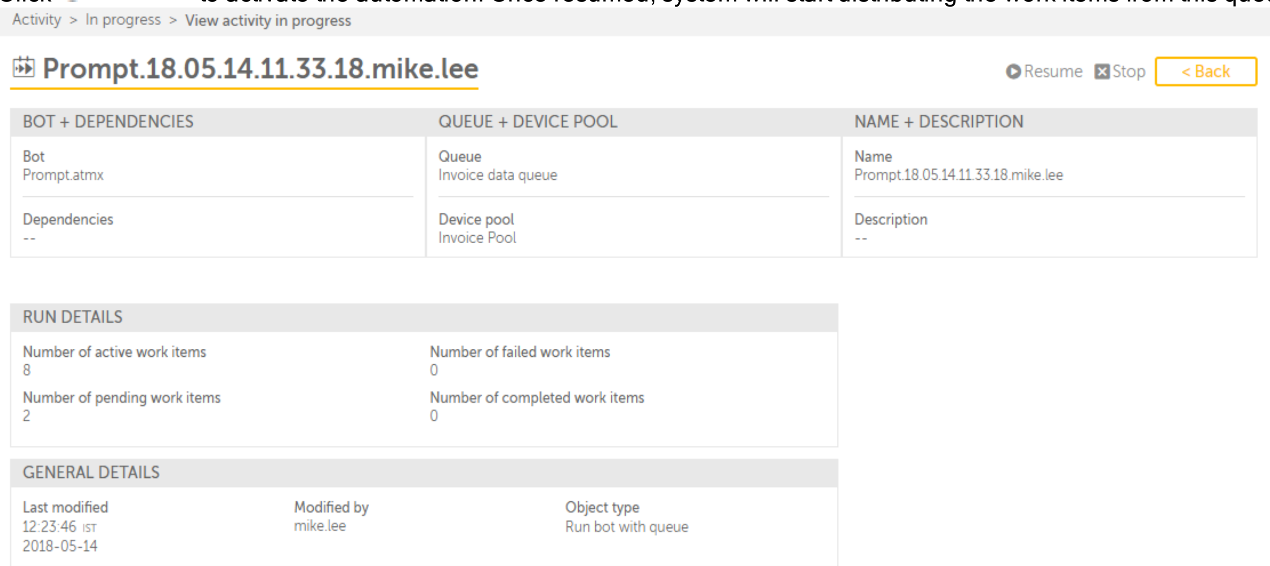
Note: Although this page is accessible from the **Workload** module, the page is launched from **Activity** module. However, you cannot perform the **Pause**/**Resume** or **Stop** actions directly from the **Activity** → **In progress** page. For these actions, the **Workload** → **Queues** → **View automation** ( ) action is used.

1. Click Pause to pause an active automation. System will pause distributing work items from this queue to available bot runners in the device pool.

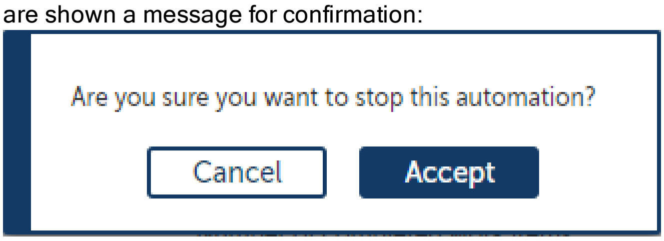


Note: Until you resume this automation, any work items with **Ready to Run** status from this queue are not sent for processing.

2. Click Resume to activate the automation. Once resumed, system will start distributing the work items from this queue:



3. Click Stop to stop the automation. System stops distributing the work items from the queue associated with this automation. You are shown a message for confirmation:



   1. Click **Accept**, to return to the **Queues** page.
   2. Click **Cancel**, to return to the **In progress** page.

Manage Work Items

As a Control Room user with queue management privileges, based on the work item status you can View, Edit, and Delete one or more work items in a Queue of which you are an owner, consumer, and/or participant. For actions allowed on work item based on its status, refer section on Work item - status and actions allowed given in this article.

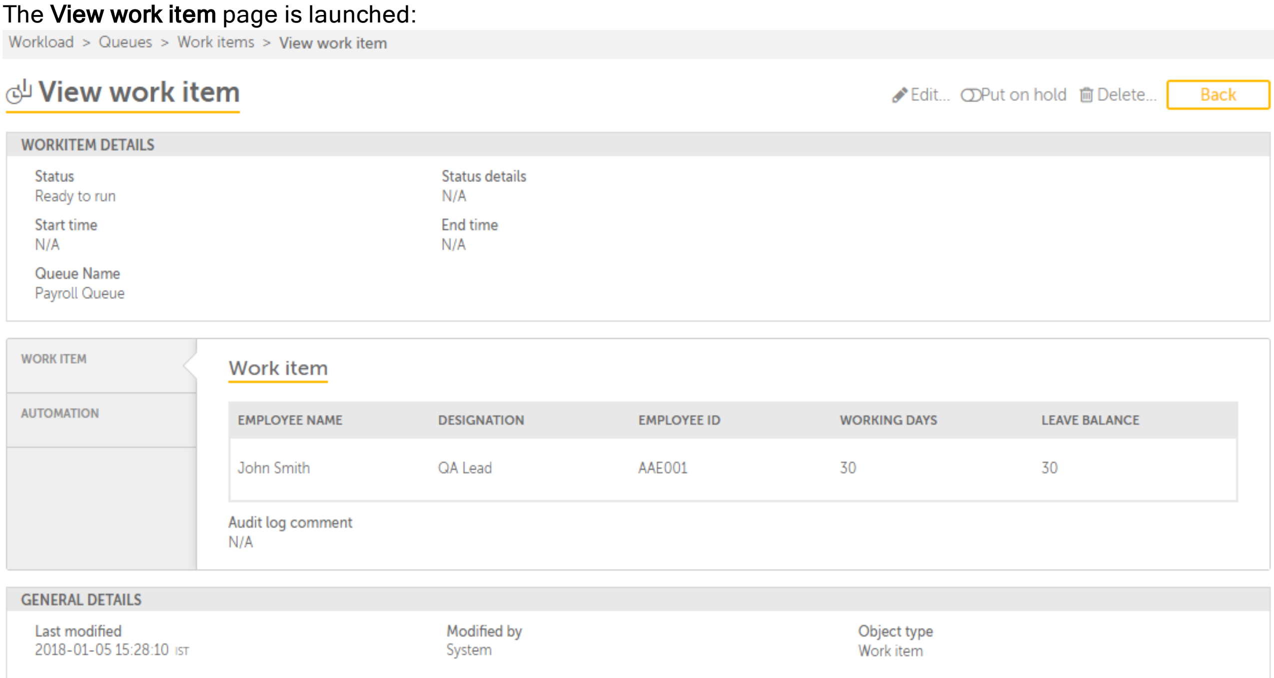
This allows you to fix discrepancies prior to queue processing and reduce your automation related errors and failures.

View work item

You can view a work item when its status is **Successful**, **Unsuccessful**, **On hold, Active**, or **Data Error**.

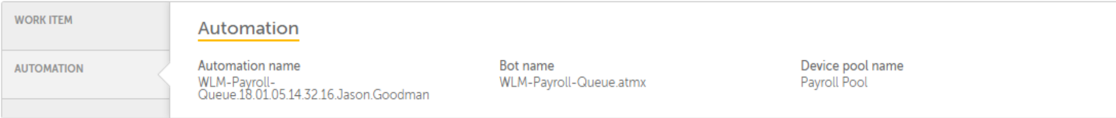
To view a work item,

1. Go to **Workload** → **Queues**
2. Select and open the Queue in view or edit mode whose work items you want to view
3. Mouse over the work item that you want to view and click
4. Click
5. The **View work item** page is launched:



6. The page provides details of the work item in three sections:
   a. **Work Item Details** such as the **Status**, **Status Details**, **Start Time**, **End Time**, and **Queue Name**
      - **Status -** Whether **Successful** or **Unsuccessful** for work items that have Failed, are in Unknown state or Stopped, **Pending** for work items that are Deferred, New or Paused, **Active** for work items that are processed in queue, **Data error** for work items that are being uploaded from the file.
      - **Status Details** - **Successful** for work item with status NA, **Unsuccessful** for work items with one or more errors, has **Unknown** status or is Stopped, **Active** for work item with status NA and **Pending** for a work item that is New, Deferred, or Paused, and **Data Error** for work item with one or more errors.
      - **Start time** and **End time** - This is shown when the work item is being processed.
      - **Queue Name** - This displays the name of the queue of this work item.

   b. Tabs for **Work Item** and **Automation**
      - **Work Item -** Displays the attributes of the selected work item and Audit log comments that were added while editing the work item, if any.
      - **Automation -** Displays the name of the automation, Bot name, and the Device pool under which this work item was processed.



c. **General Details** such as the Last modified date and time, Modified by and Object type.

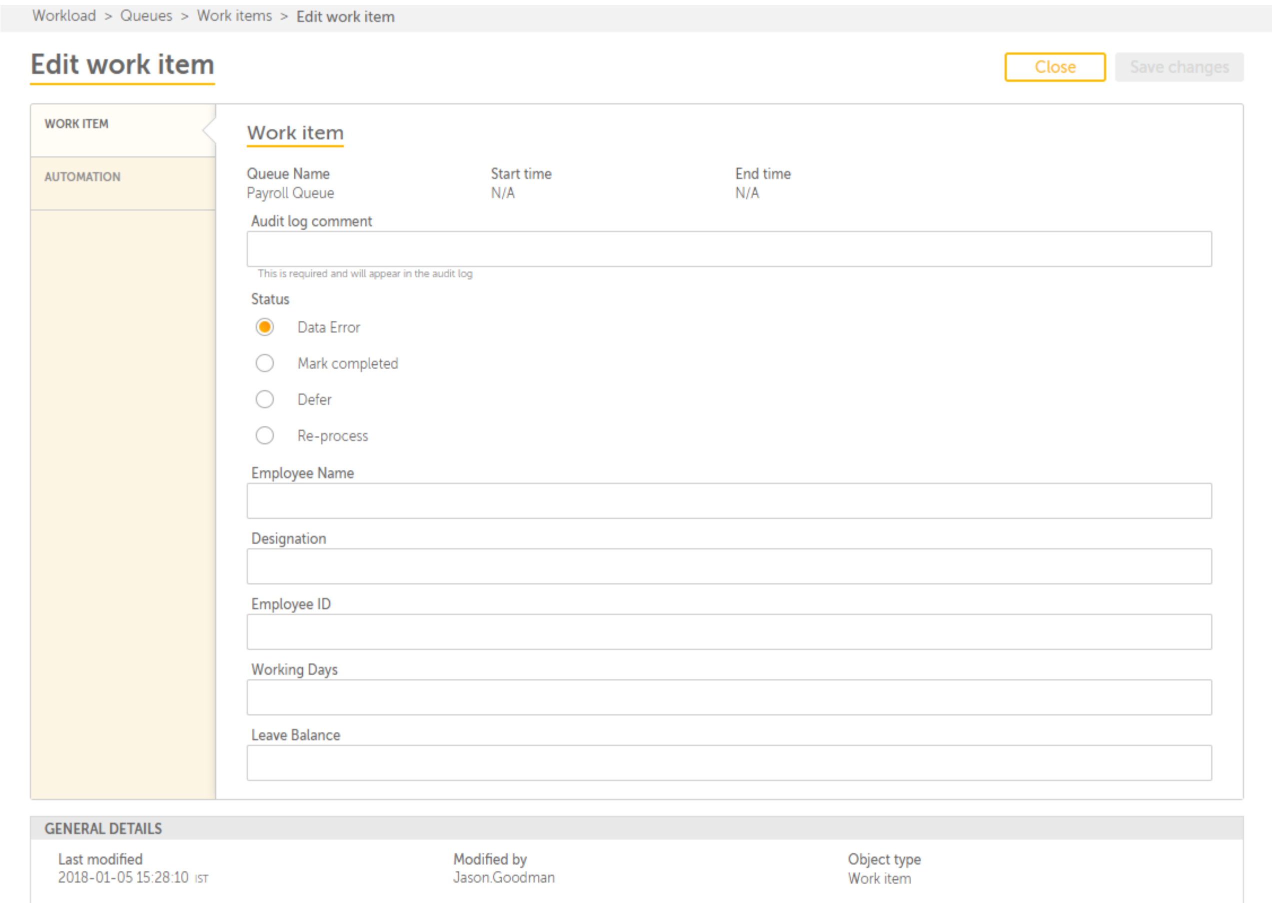
> **Tip:** You can choose to edit any of these details by clicking Edit... . You can also delete the work item by clicking Delete... provided its status is other than **Active**.

Edit work item

You can edit a work item only if its status is **Unsuccessful**, **on hold**, or **Data error**.

You can edit a work item in one of two ways depending upon where you are in the Workload page:

- If you are on the **Queues** page,
  a. Mouse over a work item from the list of work items
  b. Click
- If you are on the **Work Item** page, click Edit...
- The work item page is launched in edit mode:



- The page provides details of the work item in two sections:
  a. Tabs for Work item attributes and automation details
     - **Work Item -** Displays the Name of the Queue, Start and End time if it is processed, text box for adding comments that will appear in the Audit log, Option to change the work item status to Mark complete, Defer or Re-process, and work item attributes.
       Note that the system will set the status to **Data Error** during the data load if there is any issue with the data. For example, if user gives a text value for a number field or invalid date string for an attribute of date type, the status will

be displayed Data Error.

- **Automation -** Displays the name of the automation that is deployed by the pool admin, Bot name, and the Device pool on which the Bot will execute if processed or is being processed.

b. **General Details** such as the Last modified date and time, Modified by and Object type.

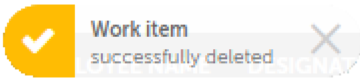
- Click Save changes

Delete work item

You can delete a work item when only if its status is not **Active.**

To delete a work item,

1. Go to **Workload** → **Queues**
2. Select and open the Queue in view or edit mode whose work items you want to delete
3. Mouse over the work item that you want to view and click
4. Click
5. The selected work item is deleted and you are shown:



> **Note:** You can also delete a work item one at a time or **in bulk** by using the delete option above the table. Refer View queue for details.

Work item - status and actions allowed

The following table provides description of each status and action allowed for that status:

Work Item Status	Description	Actions Allowed
Active	Work item is currently being processed	View
Successful	Work item successfully processed by a Bot Runner	View and Delete
Unsuccessful	Work item processing failed on Bot Runner	View, Edit, and Delete
Ready to run	Work item is successfully processed for execution	View, Edit, and Delete
On hold	Work item is deferred for use by the Queue admin	View, Edit, and Delete
Data Error	Error in loading data from the file	View, Edit, and Delete
Paused	Work item processing was paused by the Queue admin	View, Edit, and Delete

Run bot with queue

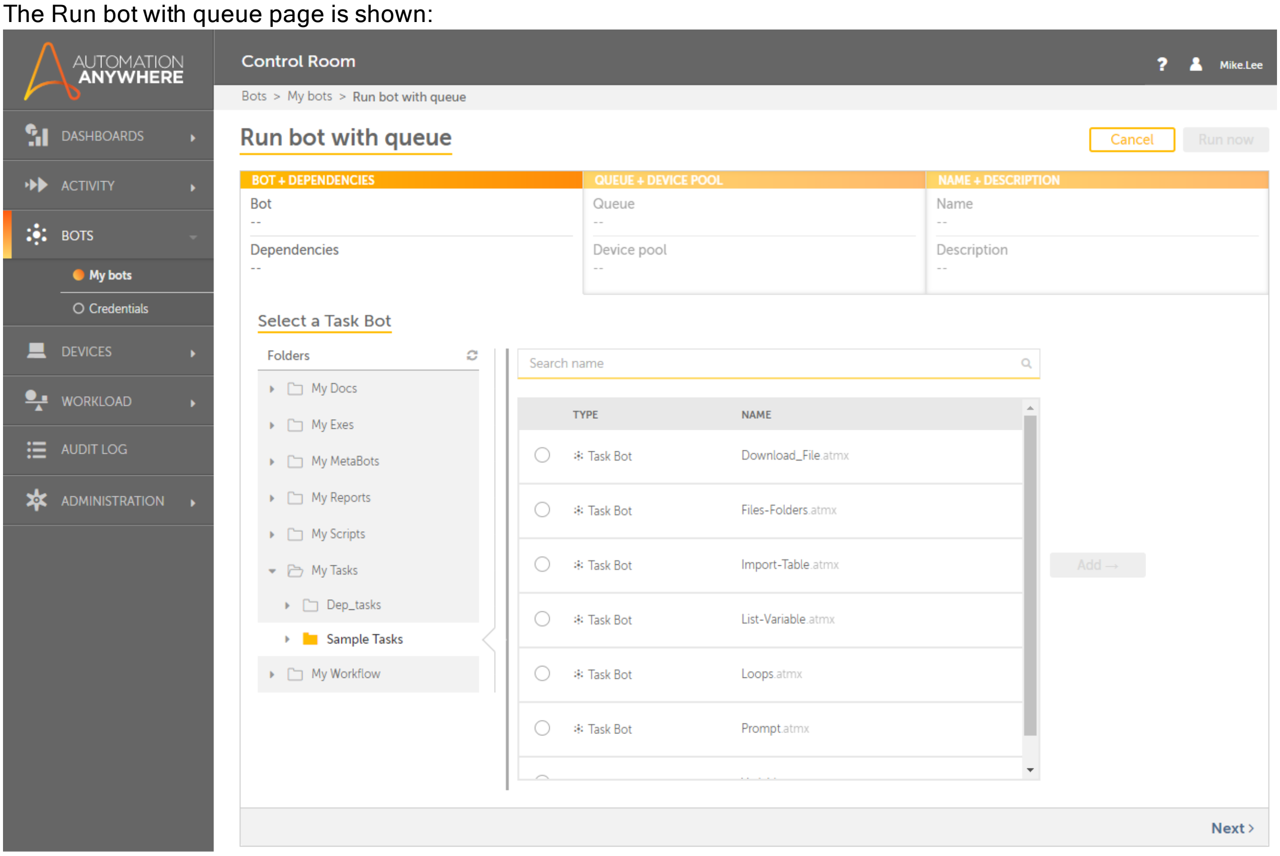
As a Control Room user with **Run my bots** or **Schedule my bots to run** privilege, you can choose to run a TaskBot with the work items present in queues. These work items will be collectively processed across all the Bot Runners present in one or more device pools.

You can **Run a bot with queue** from the **Activity** → **Scheduled**, **Bots** → **My Bots,** and **Workload** → **Queues** page. The procedure for running a bot with queue is the same in all these pages,

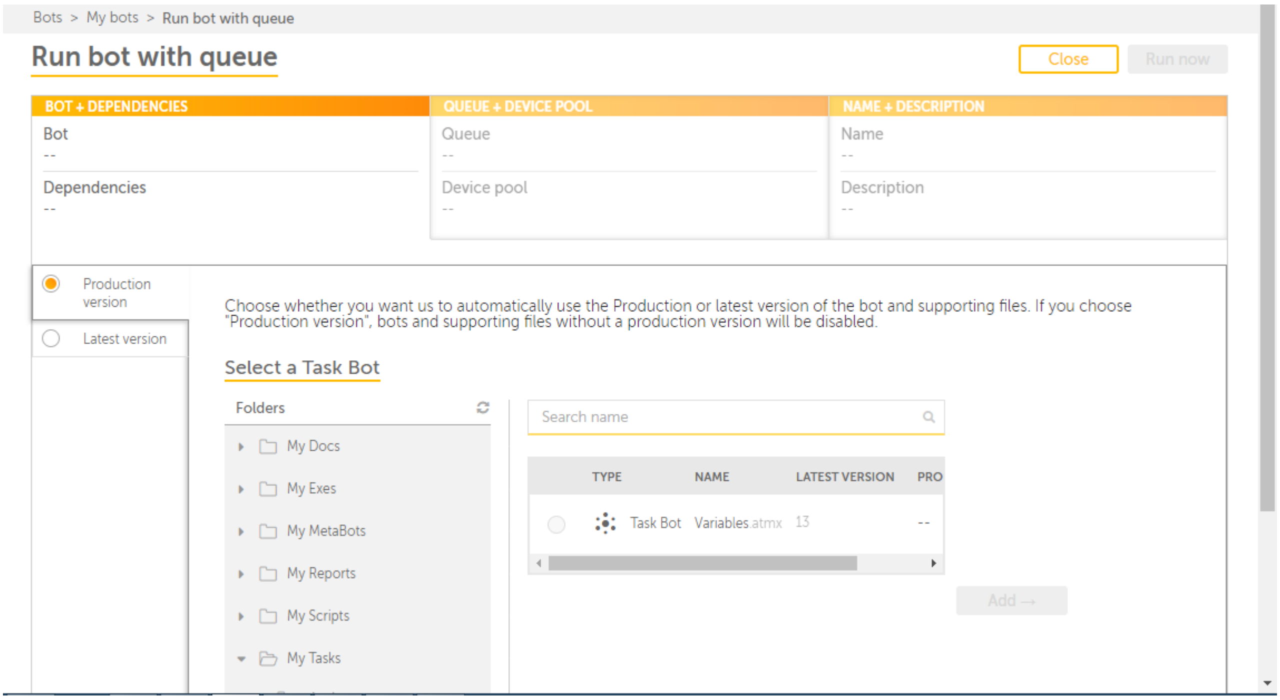
Here, you will choose the bot, queue and device pool(s).

To run a bot with queue:

1. Go to **Activity** → **Scheduled**or **Bots** → **My Bots**or **Workload** → **Queues** page
2. Click Run bot with queue...
3. The Run bot with queue page is shown:



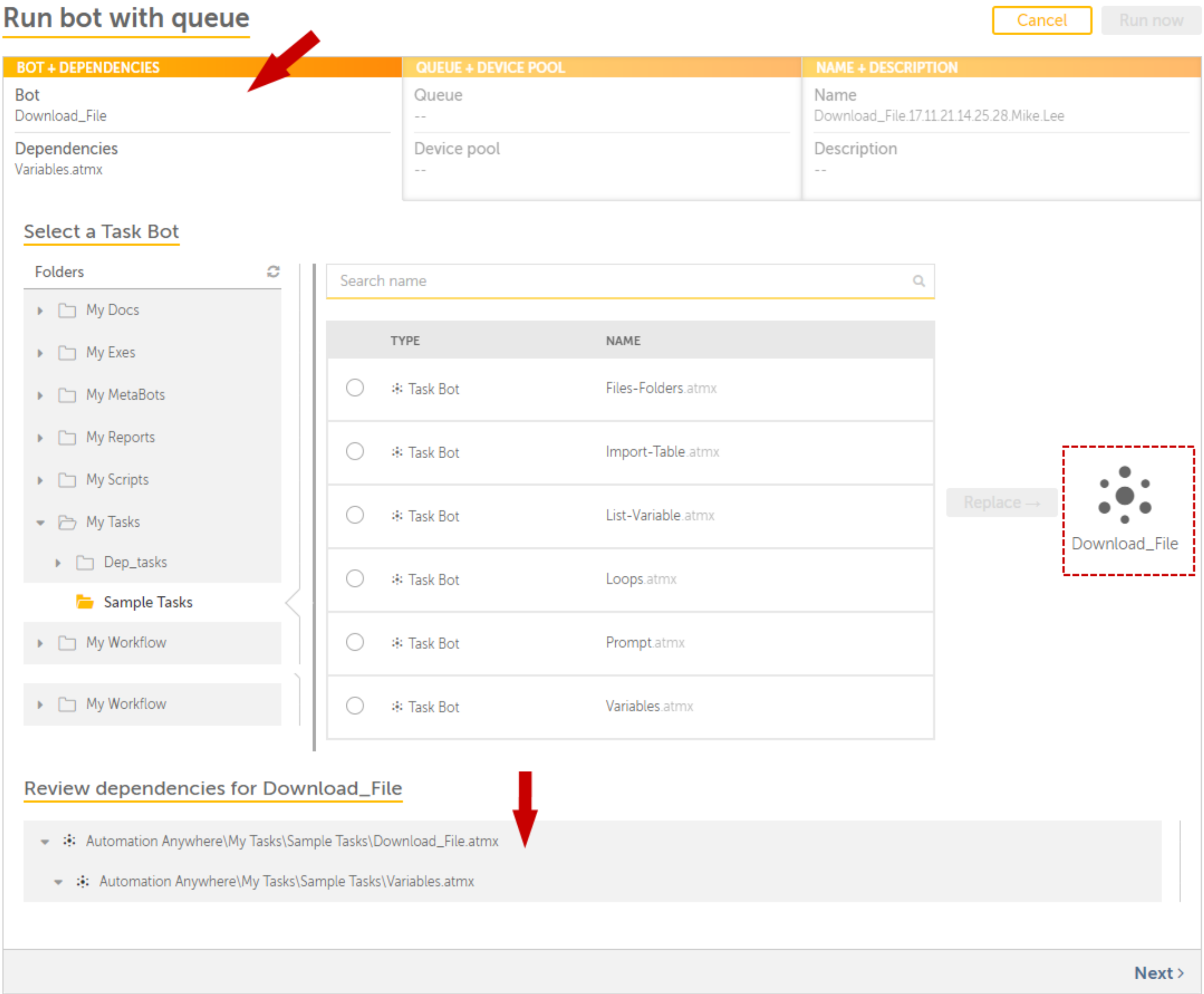
> **Note:** Even if you select the run bot with queue option from **Activity** → **Scheduled** or **Workload** → **Queues** page, you are navigated to **Bots** → **My bots** page. If version control is enabled, you can choose either the latest version or the production version of the Bots as shown:



4. You must select a Task Bot to process in the queue. By default, the **My Tasks** folder is selected. Navigate to the folder which contains the required Tasks.

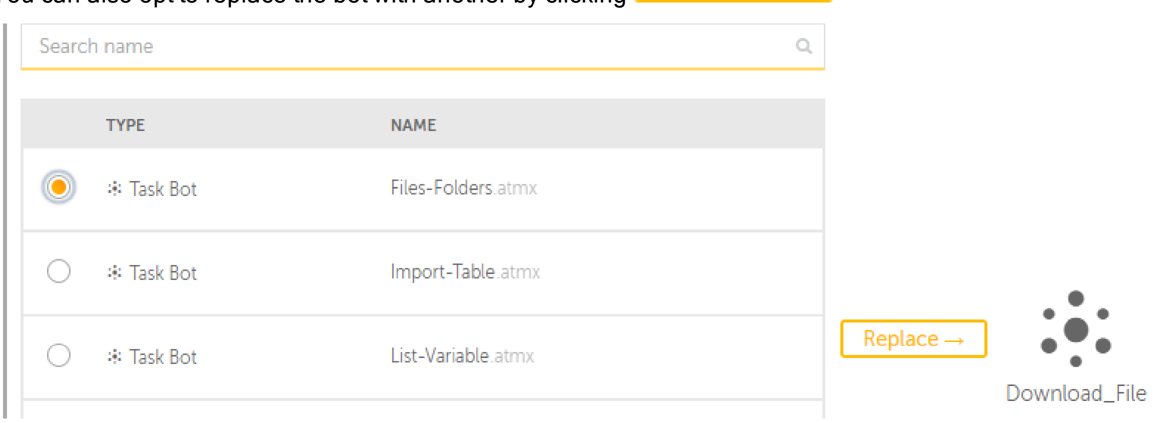
5. Select the Task Bot and click 

6. The following illustration shows **Download_File.atmx** selected from **Sample Tasks** folder.

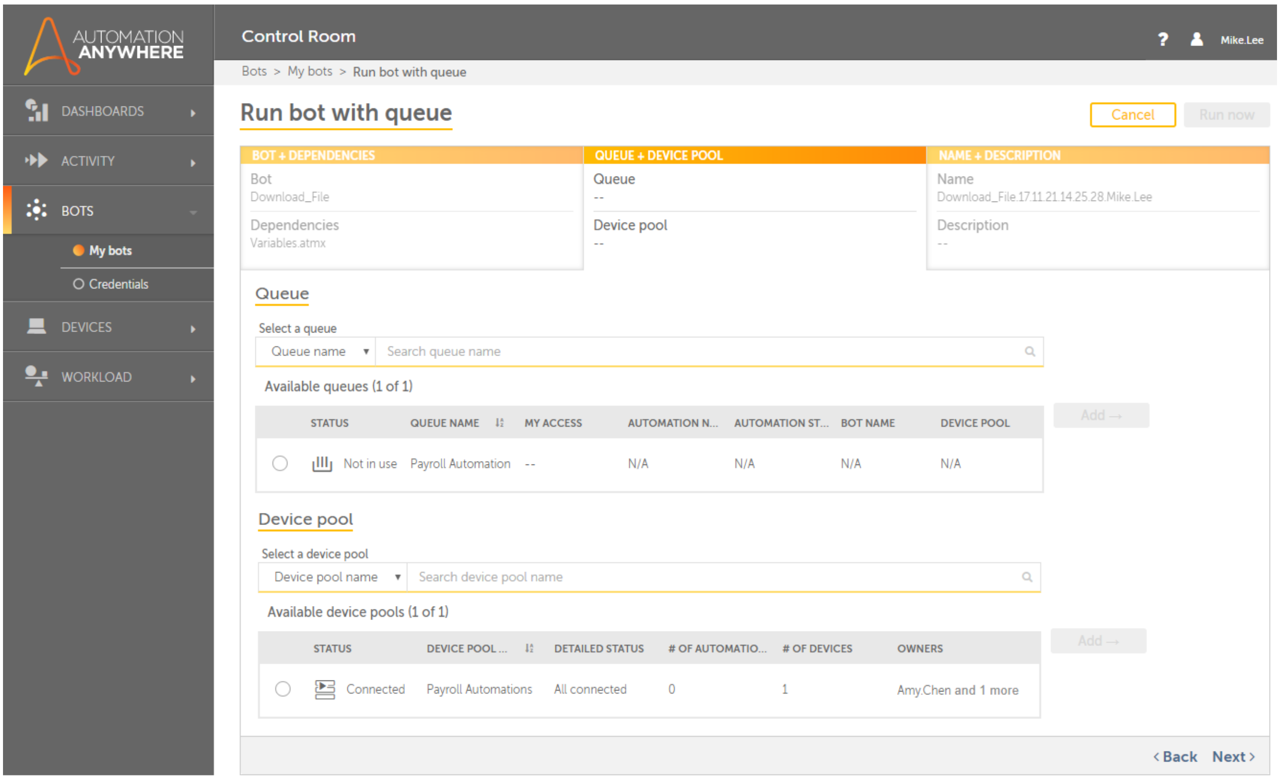



```
Tip: Use Search to find the required file quickly.
```

- If the task has any dependent files, they are shown in the **Bot + Dependencies** tab above the file selection.
- You can review the list of dependent files at the bottom of the page, if available.
- You can also opt to replace the bot with another by clicking 



7. Click **Next** to select appropriate queue and device pool.
8. You must select a queue and device pool that will be used to run the selected bot. Only the queues that are not in use are available for selection and for which you have consumer access privileges. The In use queues are shown disabled.

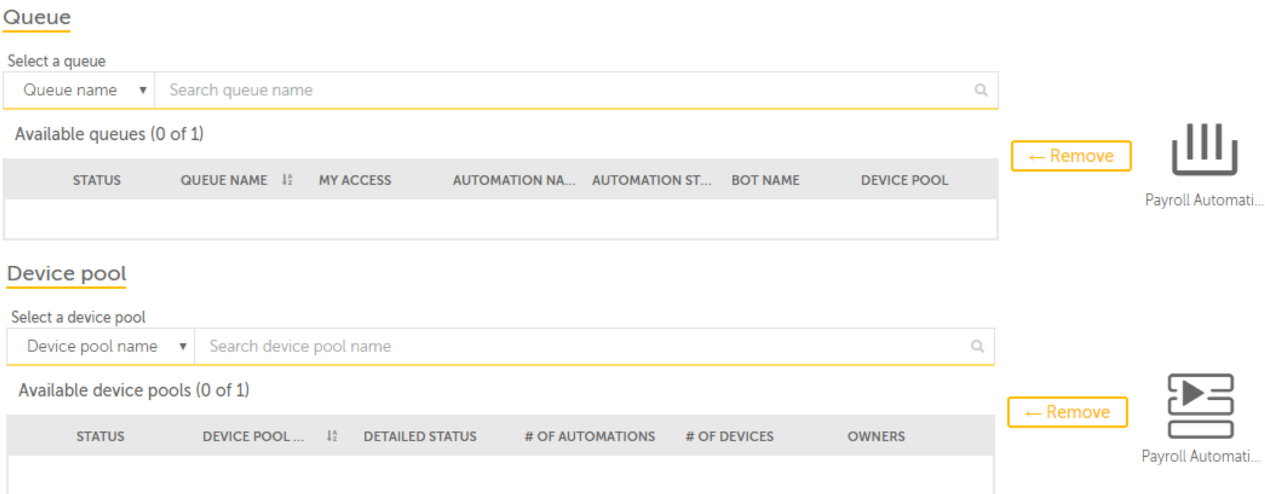


Tip: Use **Search** to quickly find the required queue and device pool.

9. To select a **Queue** from the list of **Available queues** , click Add →

Note: If the Queue is In use,it will not be available for selection.

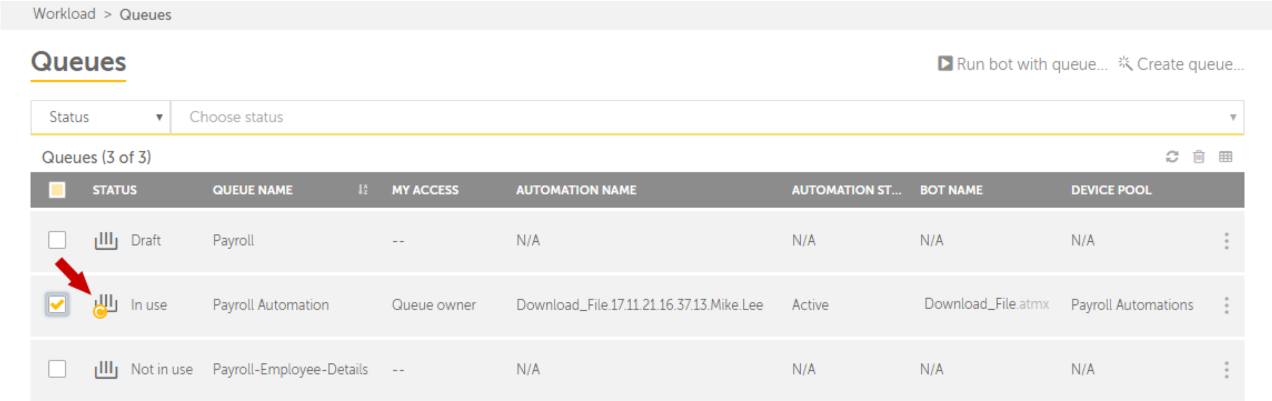
10. To select a **Device Pool** from the list of **Available device pools**, click Add →.
11. The queue and device pool are added to the run bot with queue list.



Tip: You can click ← Remove if you want to replace the queue and/or device.

12. Click Next to provide Name and Description.
13. In the Name + Description tab, the **Name** field shows the **filename+date+time+username** as the default name. This is automatically generated and can be changed per requirement.
14. Optionally add the description.This could describe the purpose of running the bot with a queue.

15. Click **Run now** to run the bot with queue. The status of the queue changes to **In use** in the list of **Queues**:

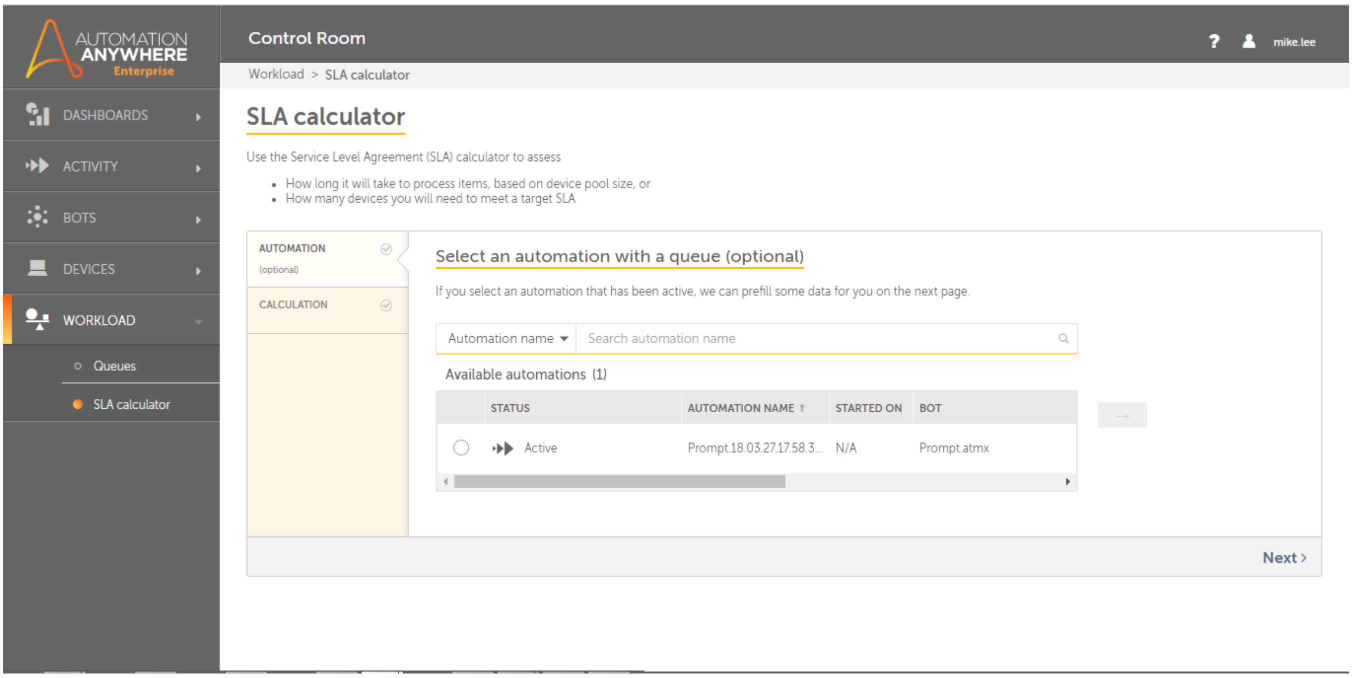


Note: This queue will not be available for any other automation. This means that only one queue can be used by one bot.

Workload - SLA calculator

As a Control Room admin or a user with SLA Calculator privilege, you can access the **Service Level Agreement (SLA) calculator** page. It allows you to estimate device pool size or time required to process a given queue size. You can use this information while orchestrating work load management to meet your organizations' target SLA.

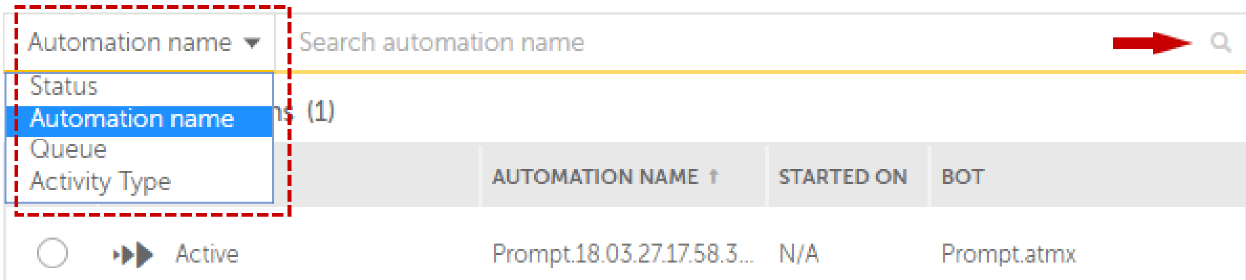
The **Workload - SLA calculator** page is illustrated below:



Note: You can see only those automations with queues for which you are either the owner /participant /consumer. However, the **Queue Admin** can see all the queues in the system.

For ease of access, you can apply search parameters to Status, Automation, Queue, and Activity Type columns.

- You can use specify the search parameters in the search bar for Automation:



When you specify search parameters for the same column, the system searches using **OR** operator. When you specify search parameters for different columns, the system searches using **AND** operator.

The following describes the list of items that can be viewed in the table:

Table Item	Description
Status	Shows automation status: • **Active** when work item is currently being processed • **Paused** when work item processing was paused by the Queue admin • Active with error when work item is currently being processed. However, there are some errors while processing.

Automation Name	Shows name of the Automation
Started On	Shows the time and date when the automation was started
Bot	Shows name of the Bot that is selected for automation
Queue	Shows name of the Queue selected for this automation.
Device Pool	Shows name of the Device Pool that is used for the automation of this queue.
Activity Type	Shows type of activity performed on this automation - Run bot with queue

Tip: You can perform the following actions on a table column:

- Click a column to sort it in ascending and descending order. You can sort up to three columns by holding the Shift key when you click on two more columns. This gives you the option of sorting two additional columns. This way the sorting is done on the entire table and not just the data that is currently visible to you. The last sorting is stored in memory applied by a user per session.
- Use a drag-and-drop operation to move the column left or right
- Move your mouse cursor at the end of the column and drag to re-size

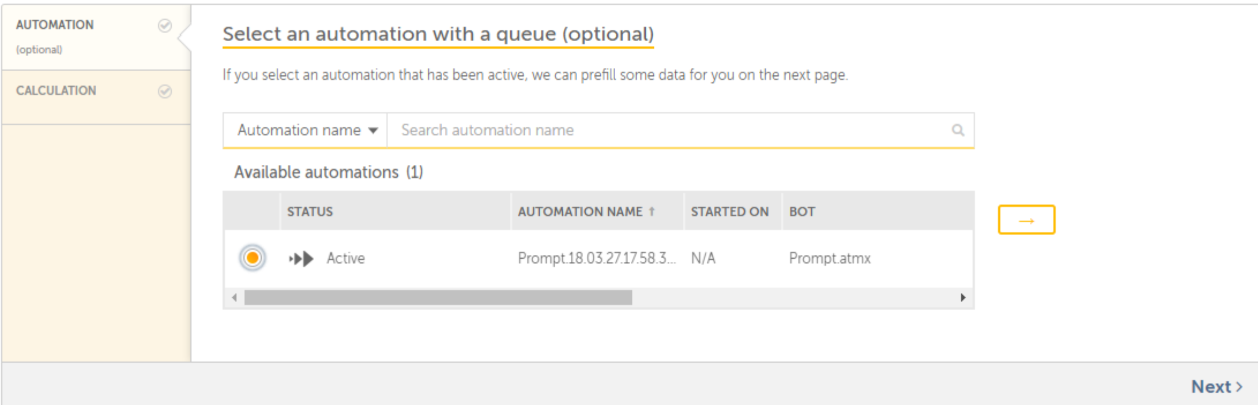
Select Automation

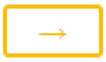
To arrive at the targeted SLA, you can choose to select an automation that is active. You can also directly fill in the parameters for calculation if you do not have an existing automation.

If specified the data from this is used to calculate the SLA in next tab - **Calculation**.

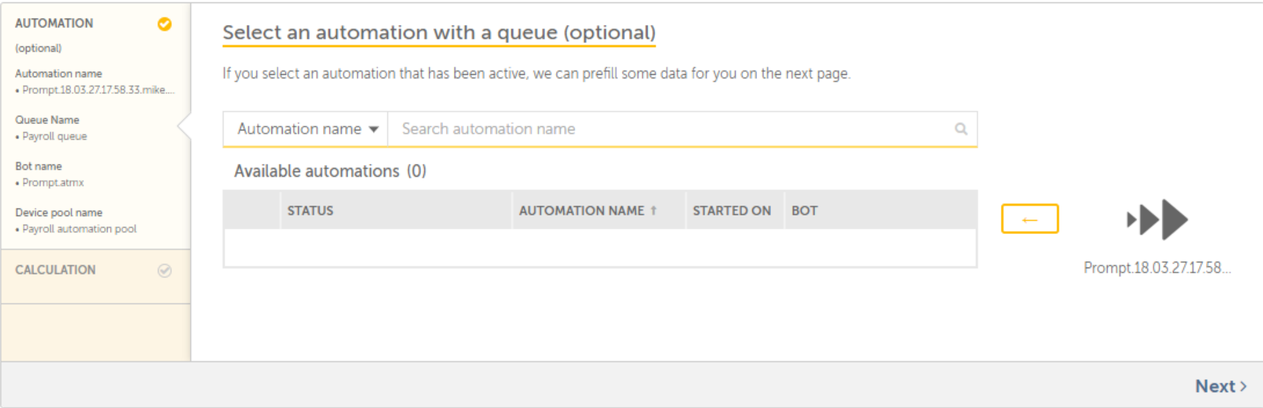
To add automation data,

1. Select an automation from the list:



2. Click 

3. The automation is selected for SLA calculation

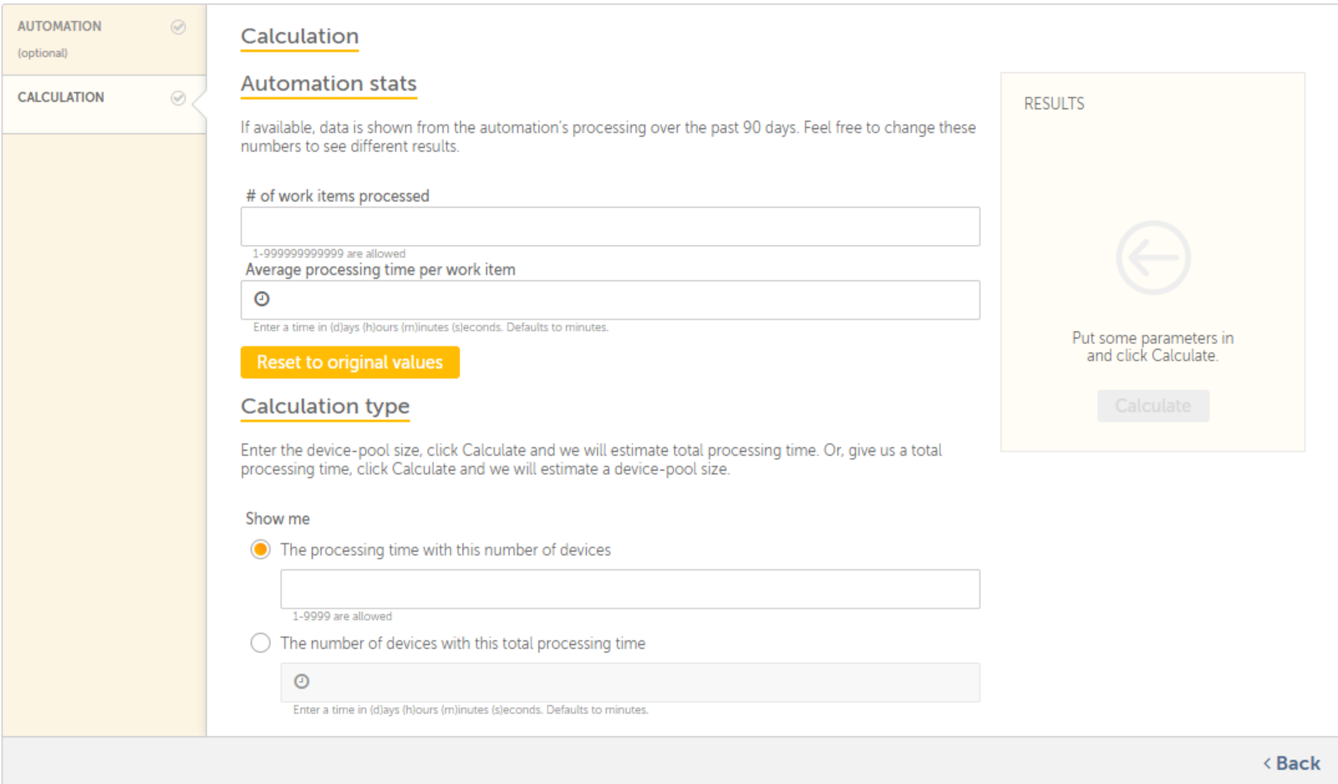


4. Click **Next >**

5. The **Calculation** tab is launched

Calculation

If you have selected an existing automation, system populates the the number of work items processed and average processing time of a work item for that automation.



Specify,

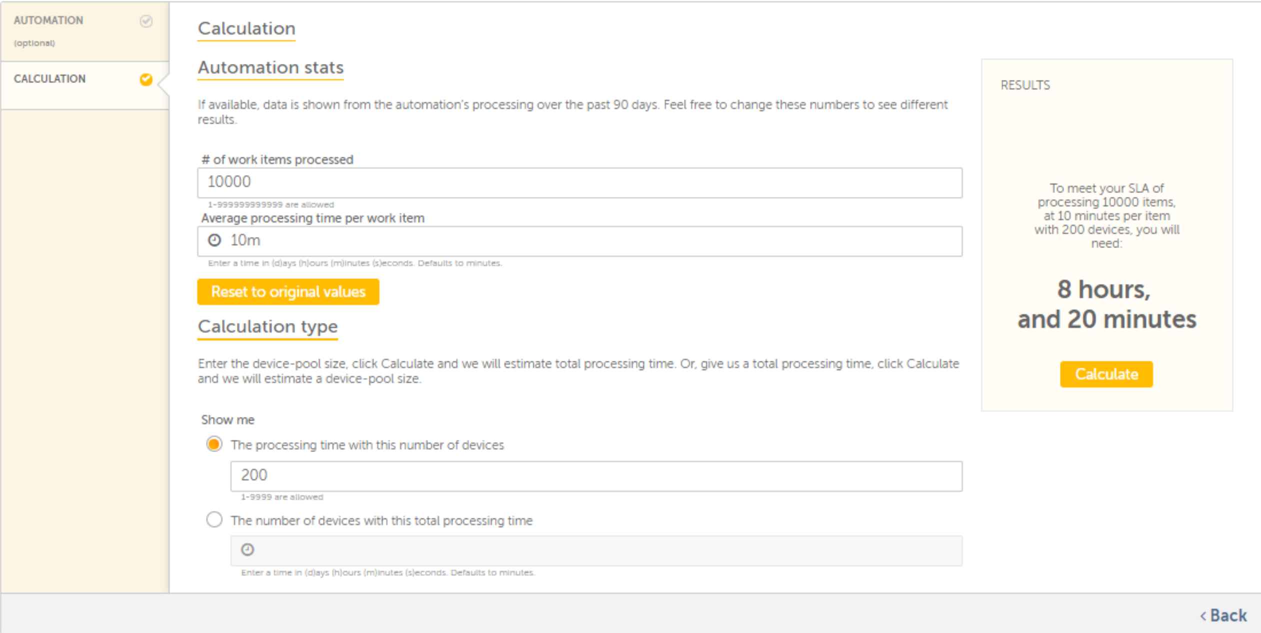
1. Number of work items processed. You can add up to 999999999999 (ninety-nine billion, nine hundred ninety-nine million, nine hundred ninety-nine thousand, nine hundred ninety-nine) work items. For example, 67890

2. Average processing time per work item. You can add the time in days, hours, minutes, and seconds. For example, 2000s or 33 minutes and 20 seconds

3. If you want to calculate the time it takes to process the number of work items specified with the given average processing time of each work item, enter the number of devices in your device pool in **The processing time with this number of devices** text box. For example, the number of devices for processing time is 120.

4. Click Calculate

5. The system shows the result based on specified parameters:



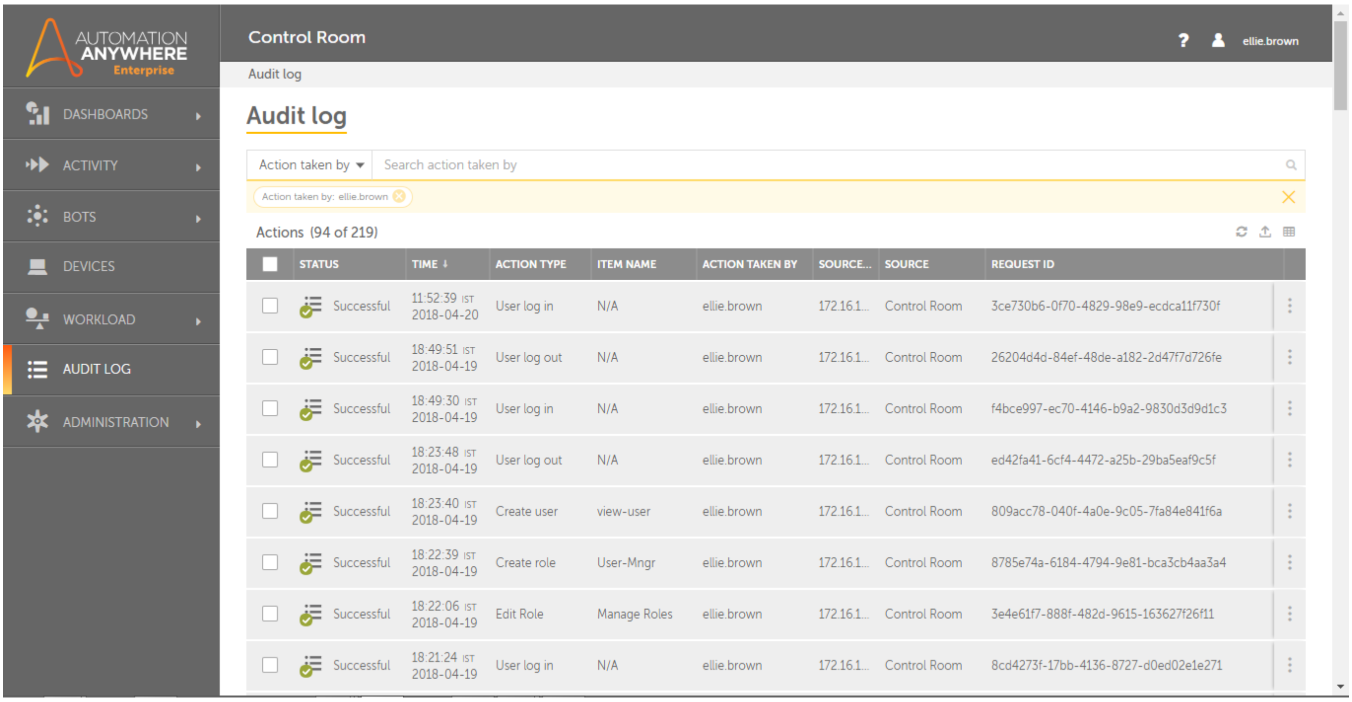
Based on the parameters provided in the example, your SLA will be 8 hours and 20 minutes.

- If you want to calculate the device pool size to meet your business SLA, specify your SLA in **The number of devices with this total processing time** text box
- Click **< Back** to return to the previous tab if required.

Audit log - overview

Audit Log captures and provides read-only records of all the important actions performed by users for Control Room and Client.

As a Control Room admin or a user with Audit Log privileges, you can view logs and details of various activities performed by Control Room users in **Audit Log** as shown in the following illustration:

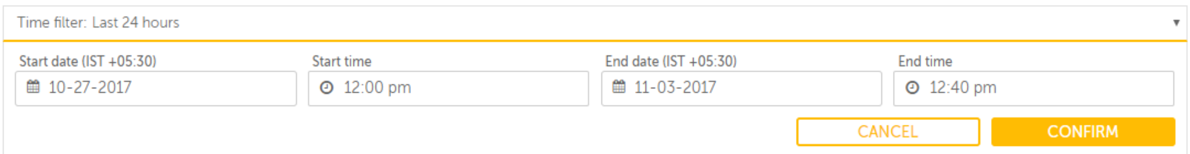


In Audit Log, you can:

- Apply **Time filters** to view activities for specific time period :

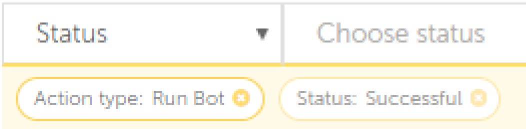
Note: By default the time filter **Last 24 hours** is selected.

- Also apply **Custom** filters wherein you can specify **Start date** and **time** as well as **End date** and **time**.



- Apply search filters based on the header types in the table that lists the audit logs.

  - Your search parameter(s) are displayed below the search bar. For example, the illustration below shows search filters applied on **Action Type** = **Run Bot** and **Status** = **Successful**



Note: When you specify search parameters for the same column, the system searches using **OR** operator. When you specify search parameters for different columns, the system searches using **AND** operator.

Known Behavior: When you use special keys "-" or "_", the system lists all **Item Names**, **Source Devices**, and **Request ID** instead of these columns having these parameters.

- Combine **Time** and **Search** filters to refine your search parameters. For example, you can filter the audit log to search for **Status** = **Successful** for **Last 7 days**.
- View the following audit details in the table:

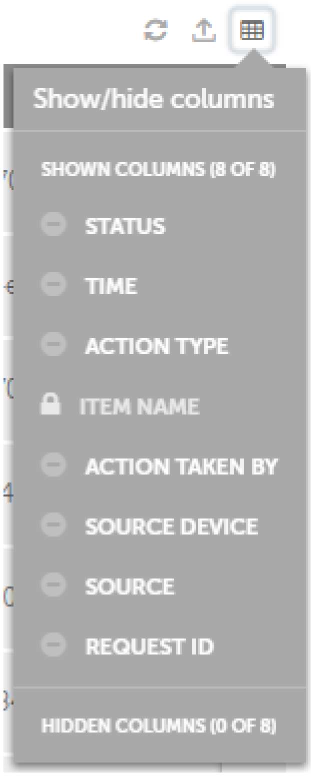
Table Item	Description
Status	Shows action status - whether Successful or Unsuccessful
Time	Shows the date and time of the action performed. You can sort this data in ascending or descending order
Action Type	Shows the type of action performed. Some action types captured in Audit logs are: • Connect Credential Vault • Create / Edit / Delete Role / User • User / Client Login / Logout • Allocate License • Create / Activate / Deactivate Automation • Run / Schedule Bot Stopped / Resumed / Paused / Ended • Unlock bot
Item Name	Shows the entity on which action was performed. For example, user name, automation name, role name etc.
Action Taken By	Shows the user that performed the action
Device	Shows the device or machine name / IP that was used to perform the action
Source	Shows the component - Control Room, Client or API, from where the action was originated or performed
Request ID	Shows the unique identity number assigned to a specific set of user actions.

Tip: You can perform the following actions on a column to help you work efficiently:

- Click a column to sort it in ascending and descending order. You can sort up to three columns by holding the Shift key when you click on two more columns. This gives you the option of sorting two additional columns. This way the sorting is done on the entire table and not just the data that is currently visible to you. The last sorting is stored in memory applied by a user per session.
- Use a drag-and-drop operation to move the column left or right
- Move your mouse cursor at the end of the column and drag to re-size

- View details of selected audit log using which is seen once you mouse over the actions icon -
- Alternatively, select all audit logs and perform the following actions:

<table>
<tr><th>Table Item</th><th>Description</th></tr>
<tr><td>Refresh</td><td>Allows you to refresh the table contents so that you can view the latest audit logs</td></tr>
<tr><td>Export to checked item to.csv</td><td>Allows you to export the data to a csv file. You can export data based on:
Month
Filters
Selection</td></tr>
<tr><td>Show / Hide columns</td><td>Allows you to show or hide specific columns. By default, all columns are displayed:



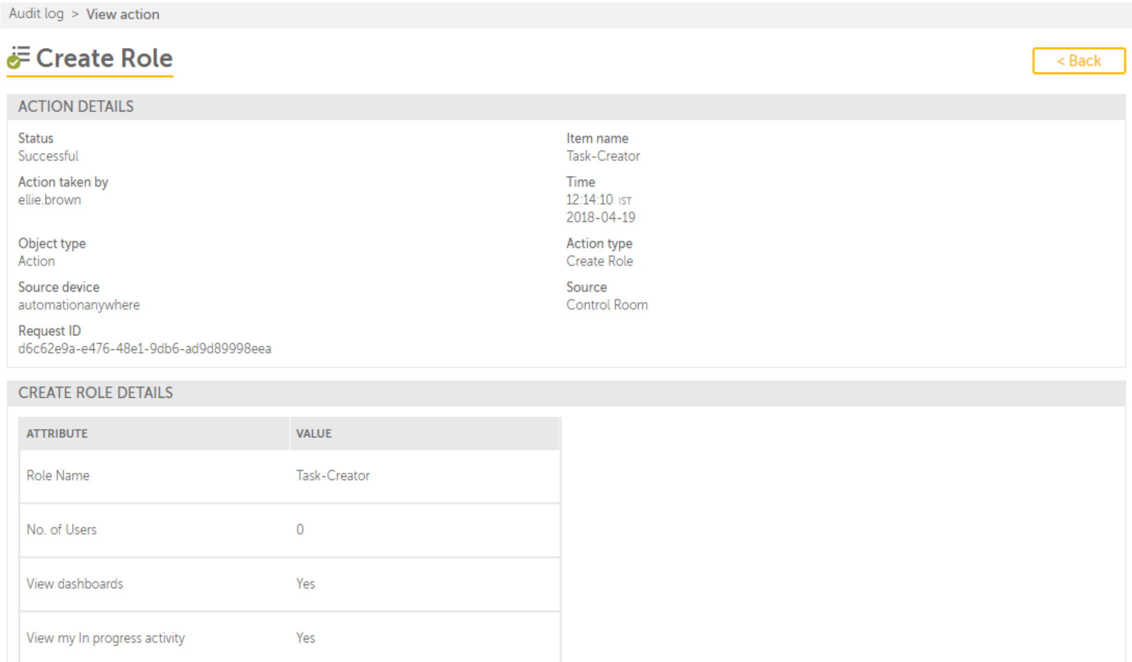
Tip: To **hide** a column, click on the column name.</td></tr>
</table>

View audit details

As a Control Room admin or a user with Audit Log privileges, you can select an activity from the Audit Logs to view its details. Viewing details of an action ensures that you can track all the changes that are being made in Control Room as well as Client.

To view Audit details,

1. Go to **Audit Log** page
2. Mouse over actions icon - in the audit entry for which you want to view details
3. Click
4. The Audit Log details page is launched. The following illustration shows the details of successful modification of User details:

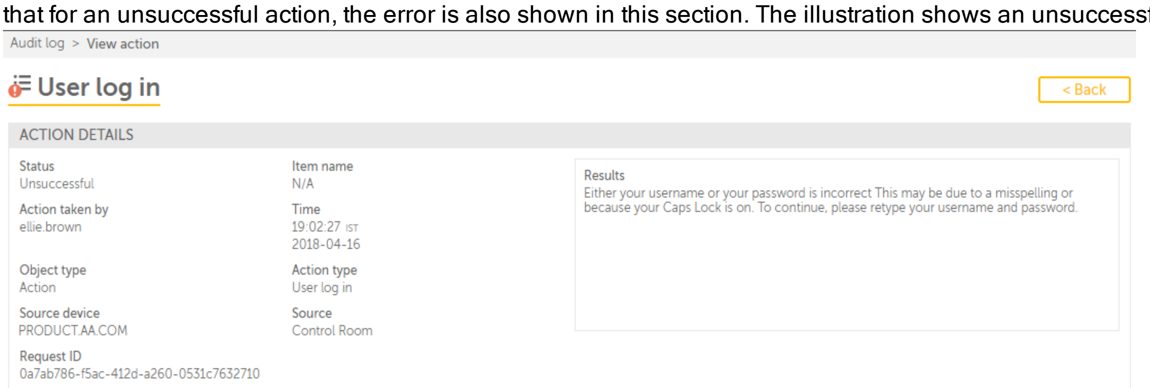


- An audit details page is divided in two sections:

  Details of the action performed

  Details of action type that comprises **Attribute** and **Values** of the action performed.

1. **Action details -** This forms the upper half of the Audit details page and shows all details that are shown on the landing page. Note that for an unsuccessful action, the error is also shown in this section. The illustration shows an unsuccessful attempt at login:



2. **Action type details -** This section, which forms the bottom half will show the details of the **Action** performed. You can view details of the type of action performed. You can see **What Changed?** in the **New Value** from the **Old Value**. You can see only those fields that were updated. Also, the information that is stored in the Credential Vault is shown (Encrypted). Based on our illustration of **Edit User** details, you compare the old and new values and understand what changes were made.

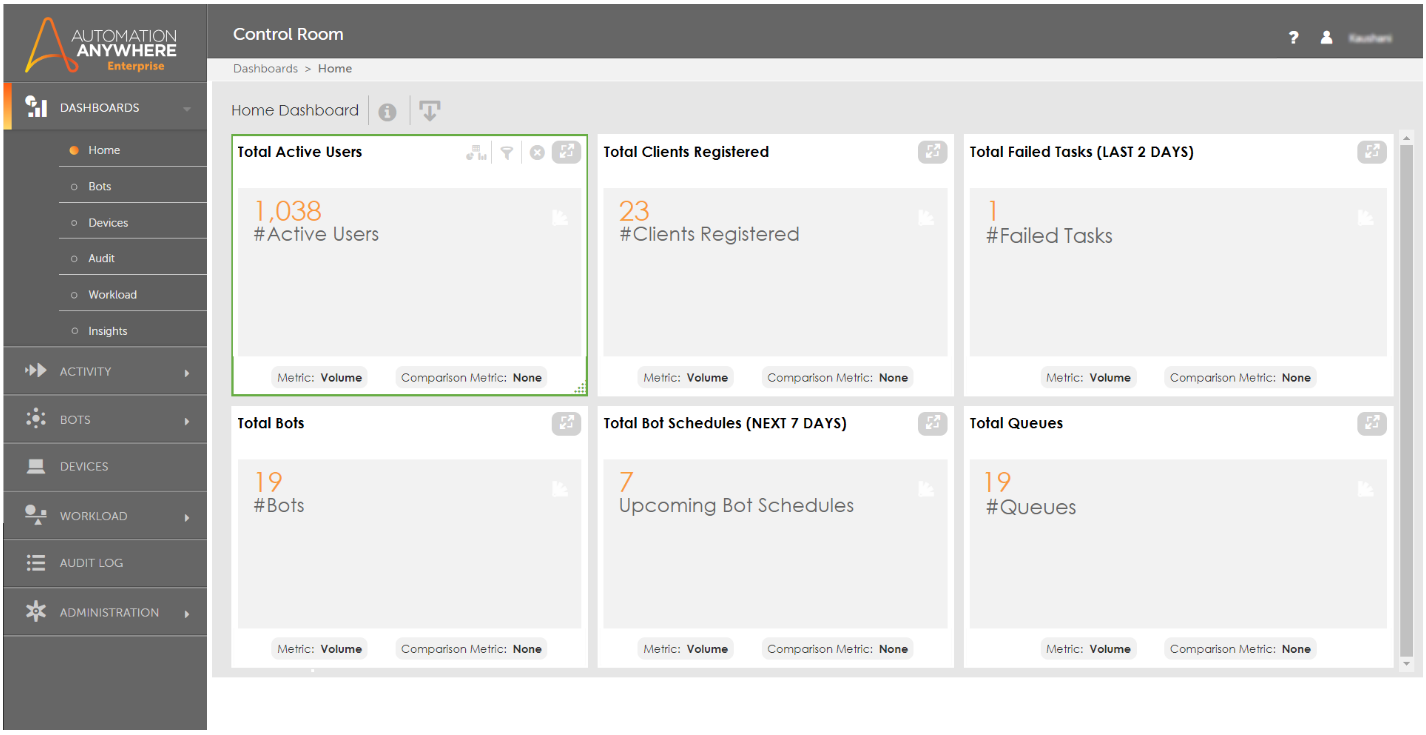
Dashboards overview

Control Room Dashboard provides exclusive graphical insight so that you can make informed decisions for your Bots. It represents your RPA infrastructure in the form of meaningful visuals and charts so that you can analyze it, interpret it, and take action on updates important to you. It dynamically updates information related to active users, registered clients, failed tasks, apps, bots, bot schedules, workflows, queues, and the overall status of devices - their memory, CPU, and HDD utilization.

The primary purpose is to help you take business decisions, and take corrective actions to fix any errors instead of going to each module and page of Control Room. For example, using the information provided to you about the disk usage, CPU status or the total number of active users, you can determine at what hour and day is Control Room the most busy or what caused a problem at 1:00 PM on Thursday.

It also has rich features that let you work with your data by using features like filtering, sorting, applying visually appealing colors to charts, and setting the time bar for each widget on the dashboard.

The following figure illustrates the **Dashboards Home** page.



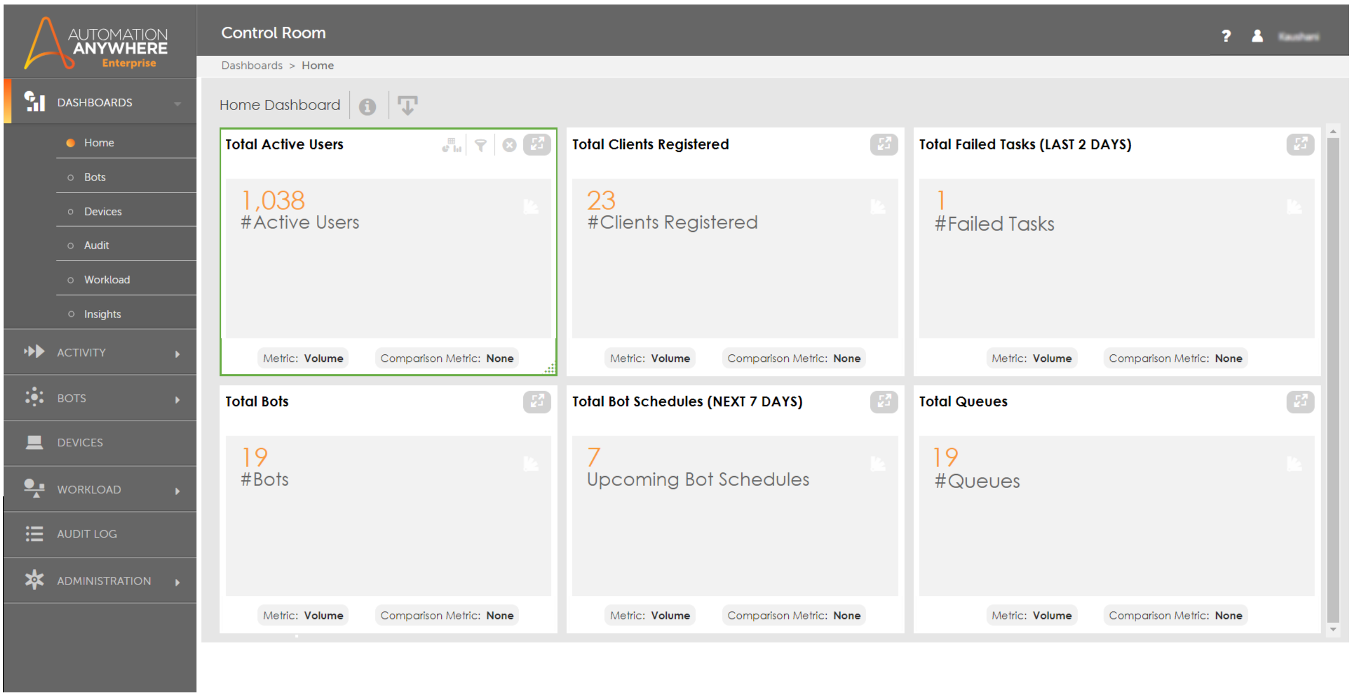
Refer to the following sections to learn more about the different pages of the Dashboards module.

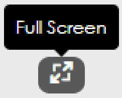
- Dashboards Home
- Dashboards Bots
- Dashboards Devices

Dashboards-home

As a Control Room user with Dashboard view privileges, you can view data presented in the form of widgets which provide information about the following:

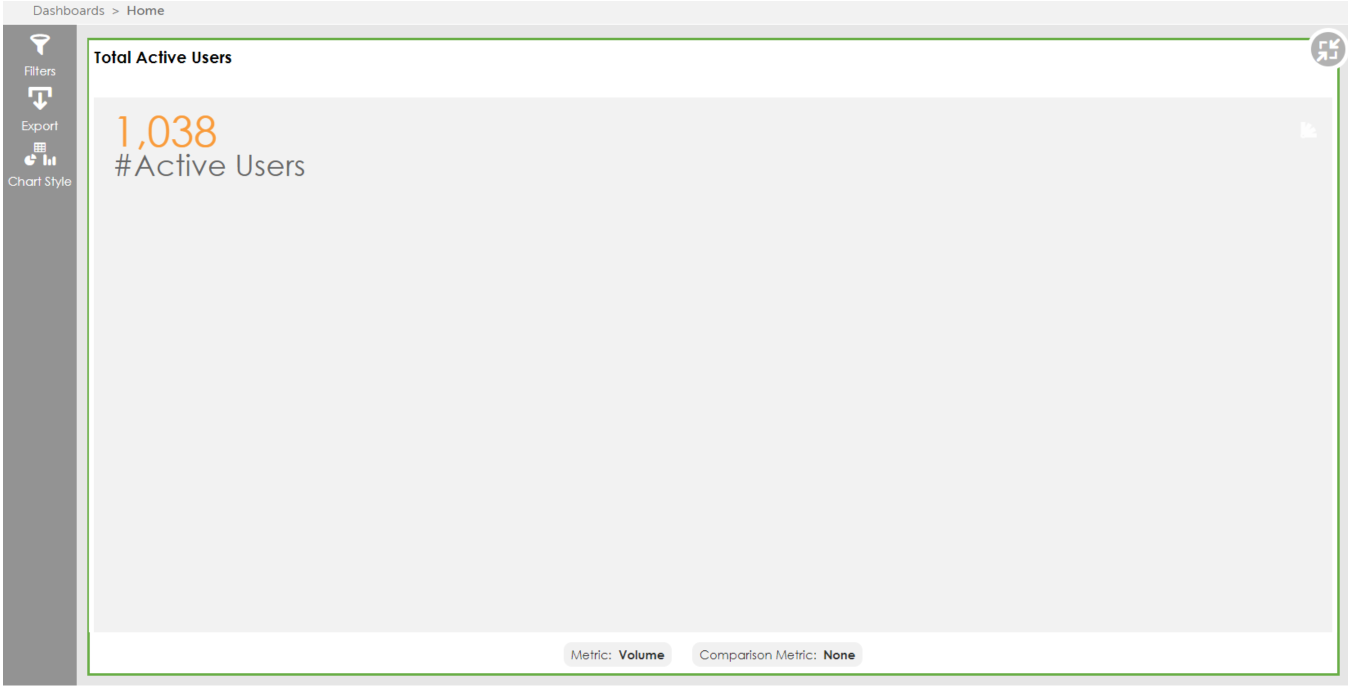
- Number of active users
- Number of registered clients
- Number of failed tasks
- Number of existing Bots
- Number of upcoming Bots that have been scheduled
- Number of queues available



Tip: To expand to a detailed view, click the Full Screen icon for a given widget: 

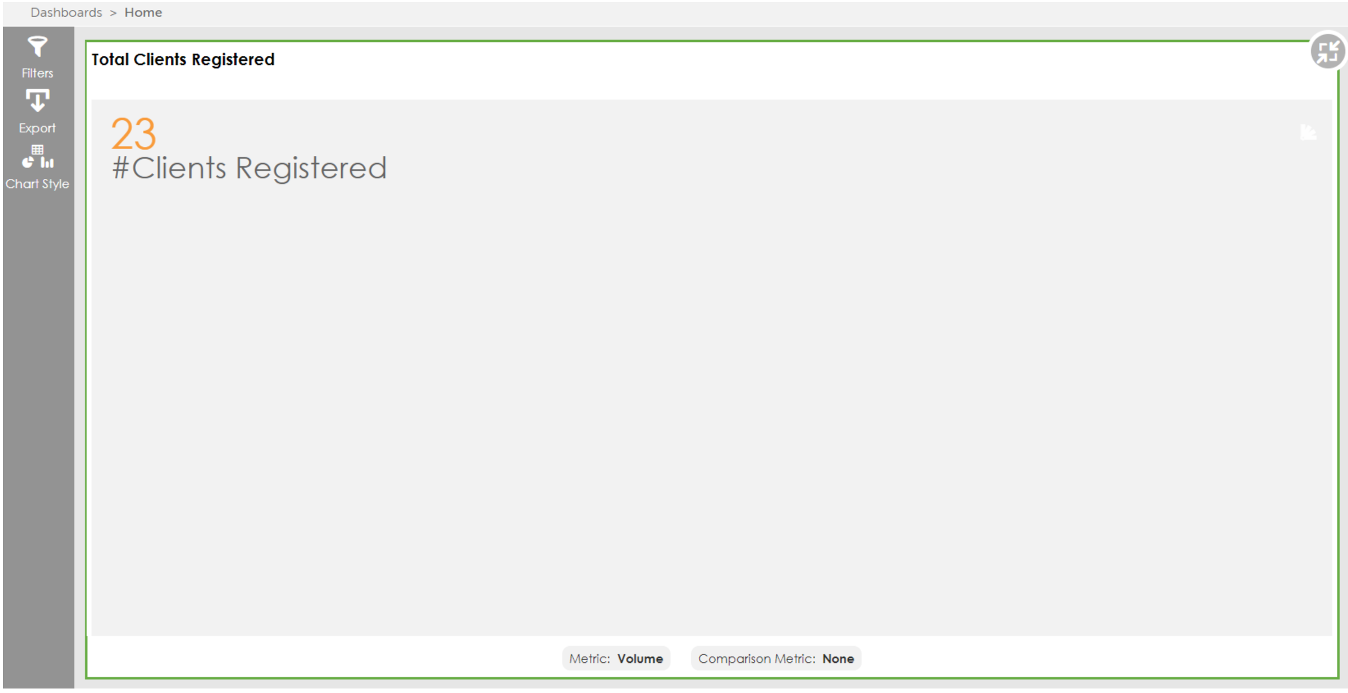
Total active users widget

This widget displays the total number of active users in Control Room



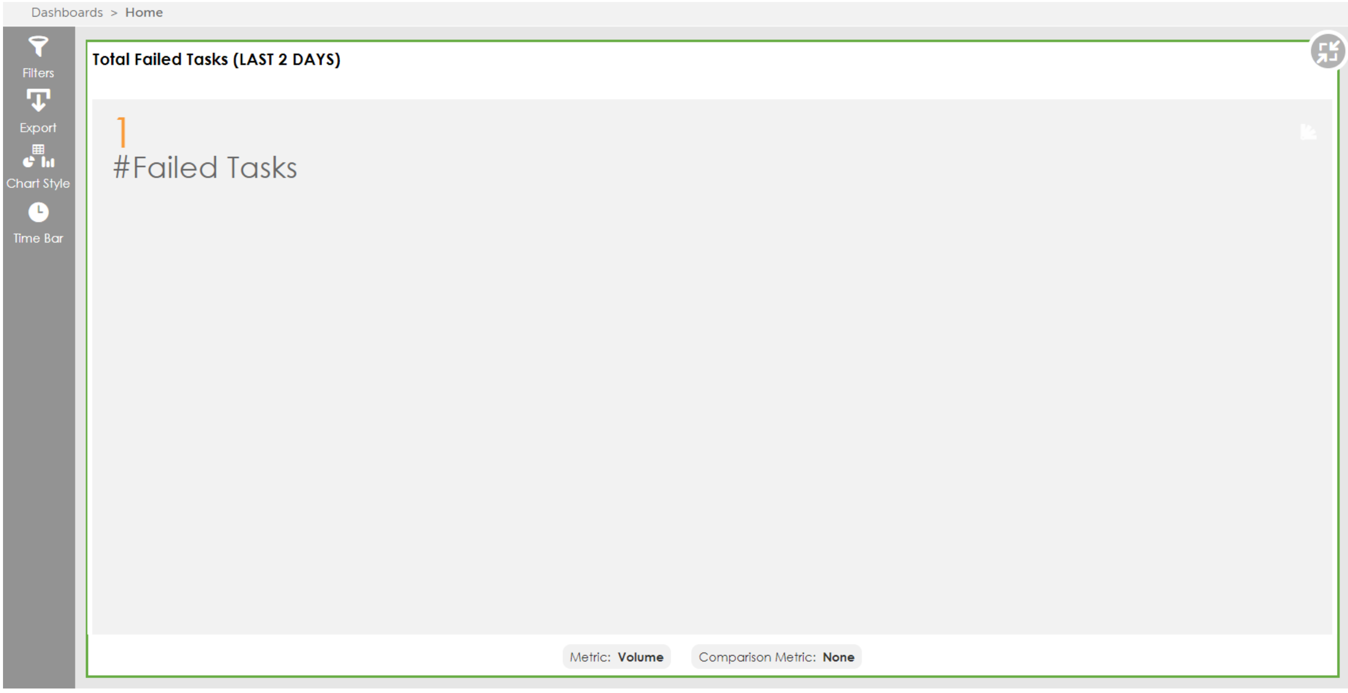
Total clients registered widget

This widget displays the total number of registered clients connected to Control Room



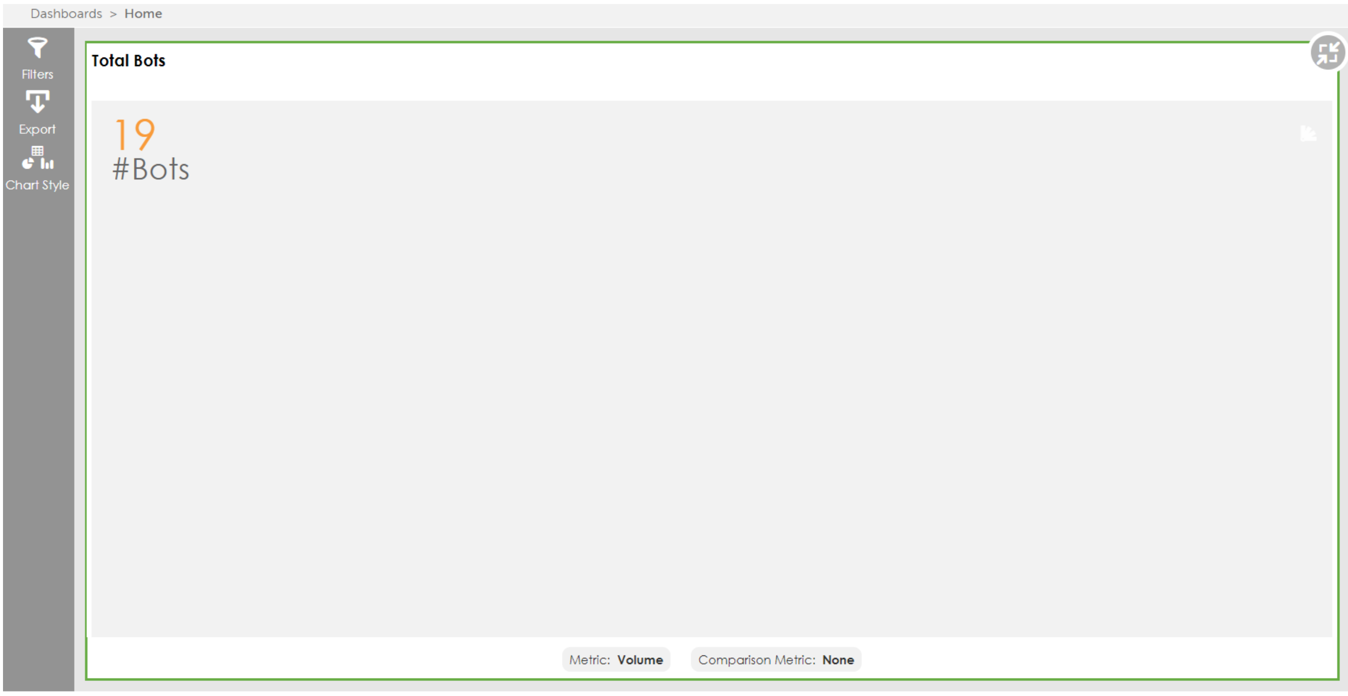
Total failed tasks widget

This widget displays the total number of task execution failure. **Last 2 days**



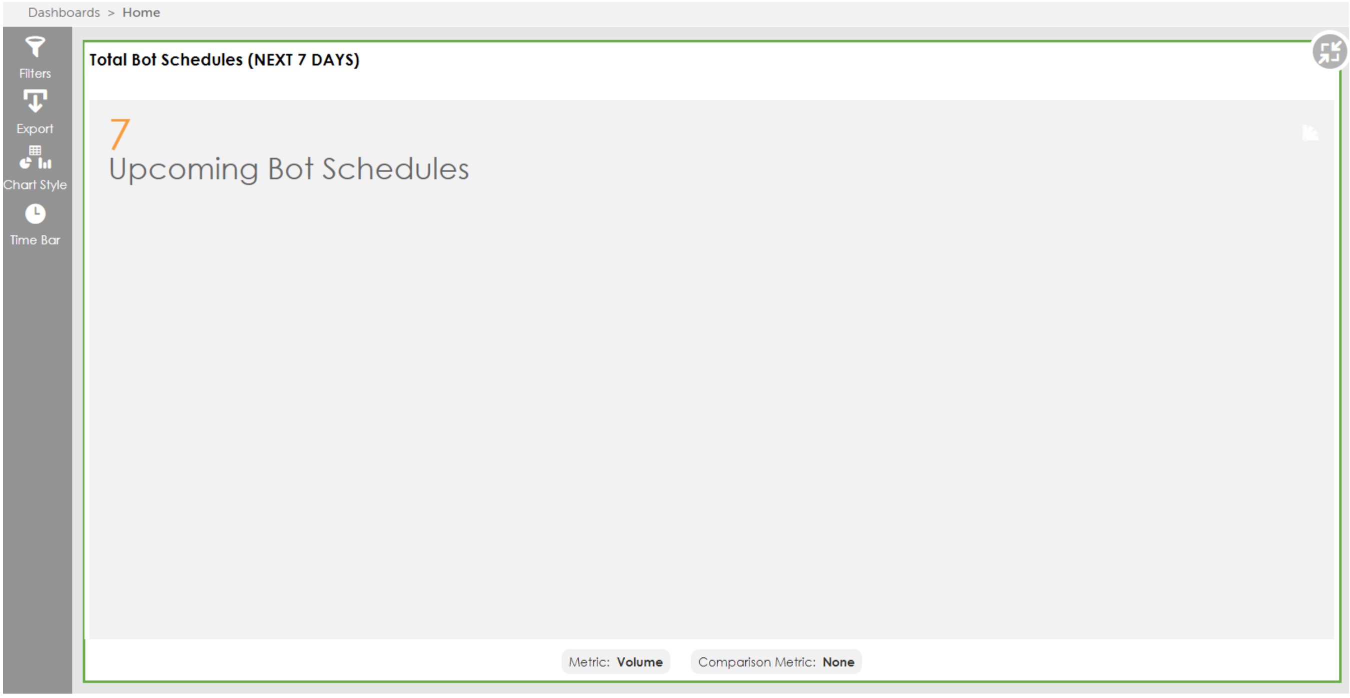
Total Bots widget

This widget displays the total number of Bots



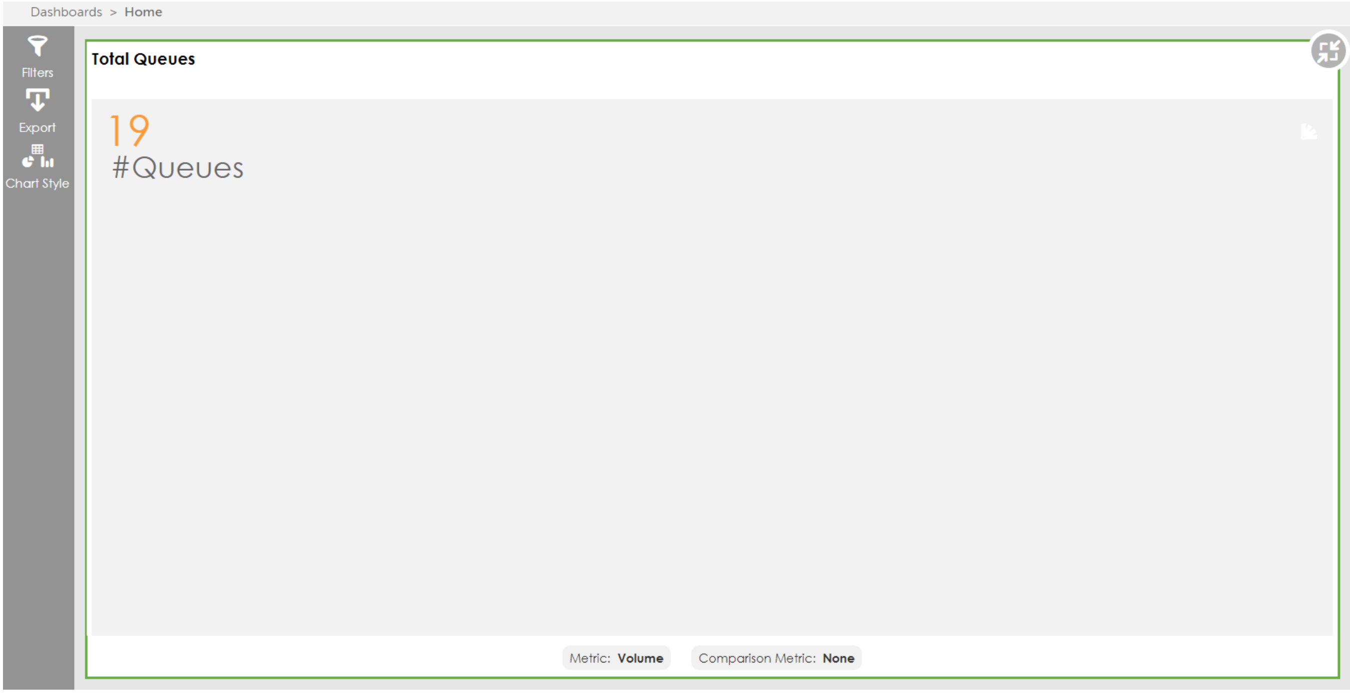
Total Bot Scheduled widget

This widgets displays the total number of Bots that have been scheduled in Control Room. **Next 7 days**



Total queues

This widget displays the total number of active queues



Dashboards - Bots

As a user with appropriate permissions, the **Bots** page of the **Dashboards** module provides you with a graphically summarized view of all the deployed bots in Control Room. This dashboard gives you answers to the following questions.

- Which of my bots use the most system resources?
- Which bots are scheduled to run? Which of these bots failed to run?
- What percentage of bots are in progress, paused, unknown, failed, and completed?

Bot Heartbeat Widget

The Heartbeat widget provides a statistical representation of the relationship between the failure score of a bot and the respective bot. A failure score is a calculation of the resources utilized by the CPU, memory, and hard disk (HDD) when you run a bot. By default, the formula for calculating the failure score is:

- Failure Score = 0.5*M + 0.3*C + 0.2*H

  where,
  - M =Memory usage
  - C = CPU usage
  - H = HDD usage

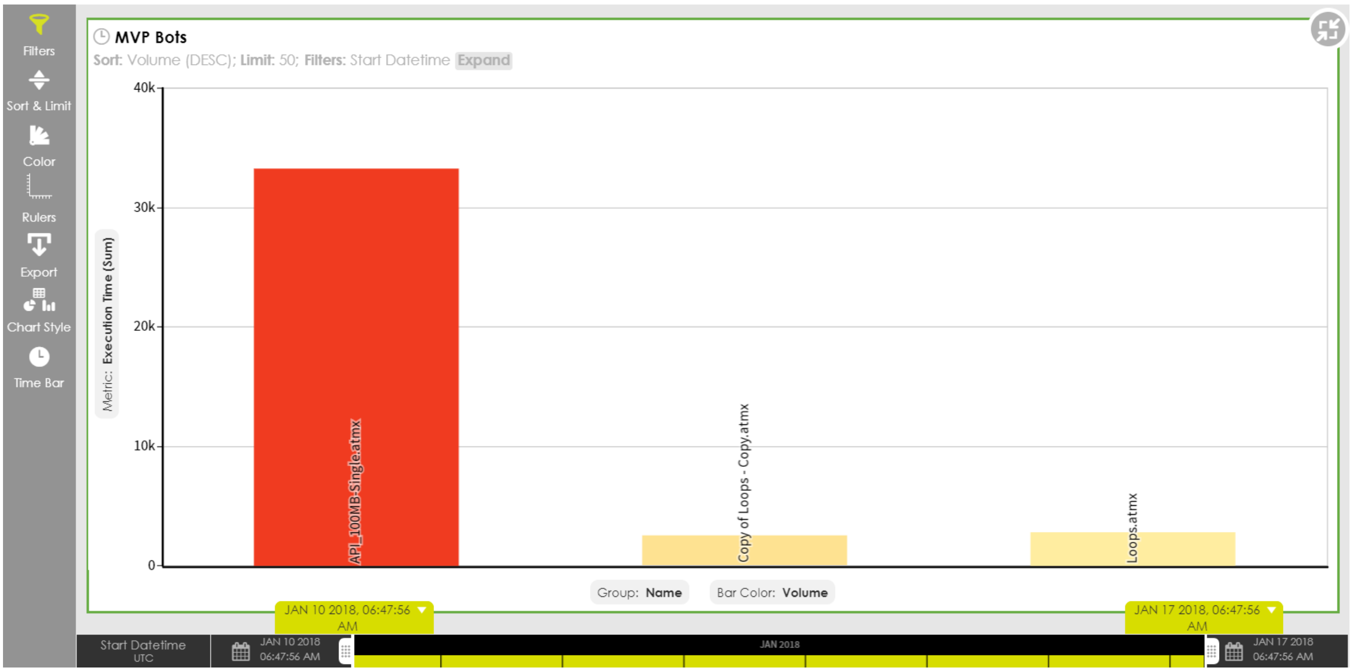
Once the failure score is calculated, it is plotted against the respective bot and is displayed in the heartbeat widget. While the failure score is plotted in the Y-axis, the respective bot is plotted in the X-axis.

```
Tip: The heartbeat widget also displays the most busy bot (MVP) and is represented with a different color.
```

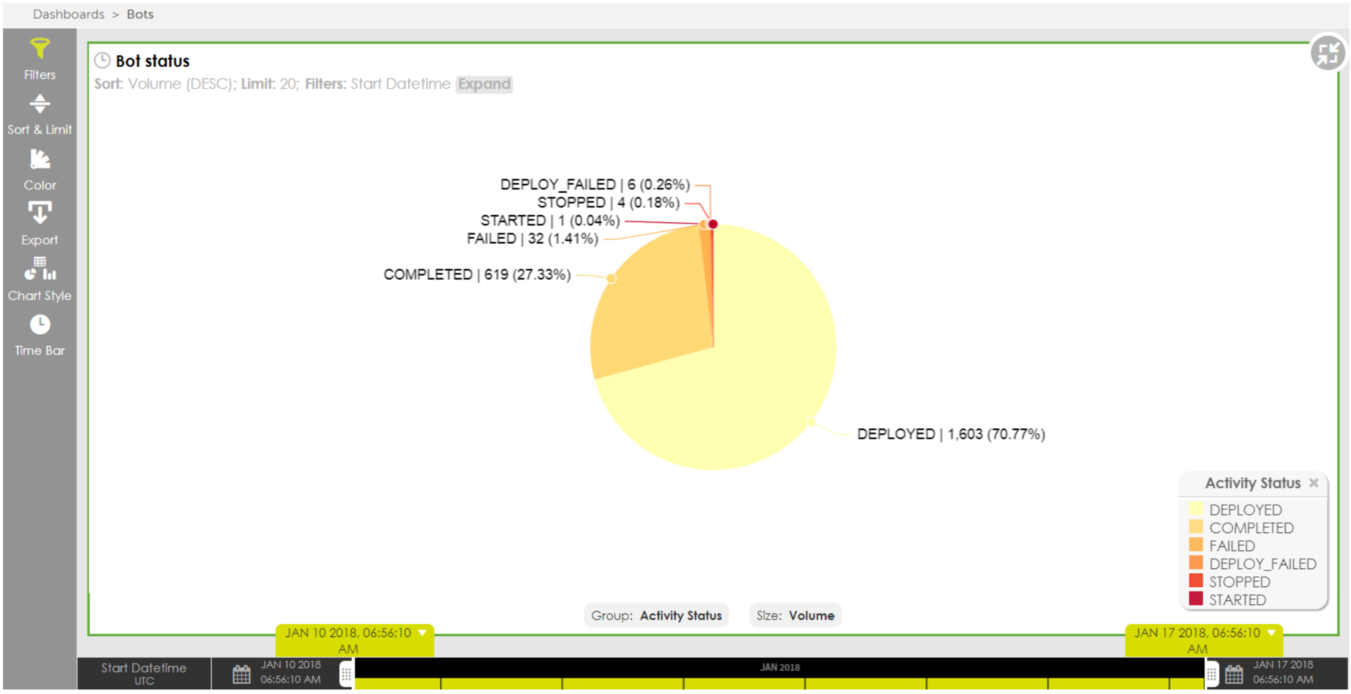
Use this widget to identify, which bot is using the most resources and take decisions on whether you need to upgrade your system configuration. A sample figure of the heartbeat widget is displayed in the following figure.

MVP Bots Widget

This widget displays bots based on their maximum processing time and the number of times they are run.

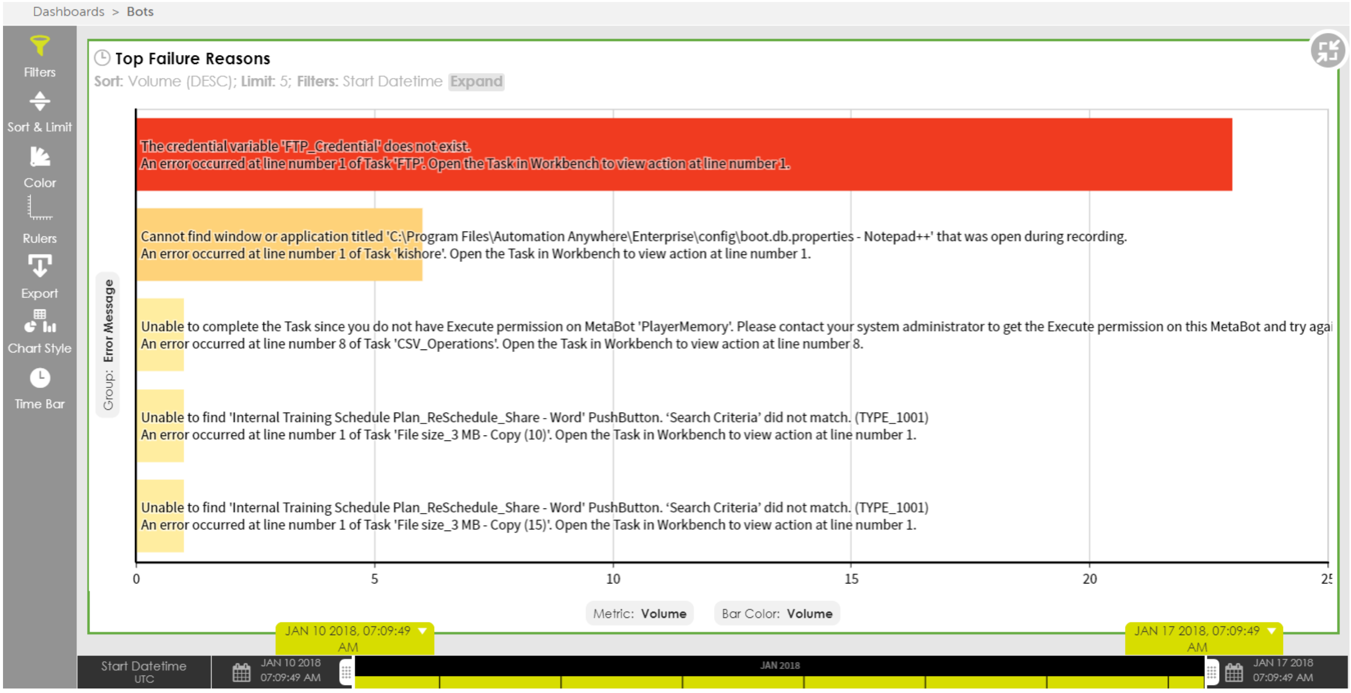


Bot status Widget



Top Failure Reasons Widget

This widget categorizes the errors that your bots may encounter into various groups and shows the count of each group



Upcoming Schedules Widget

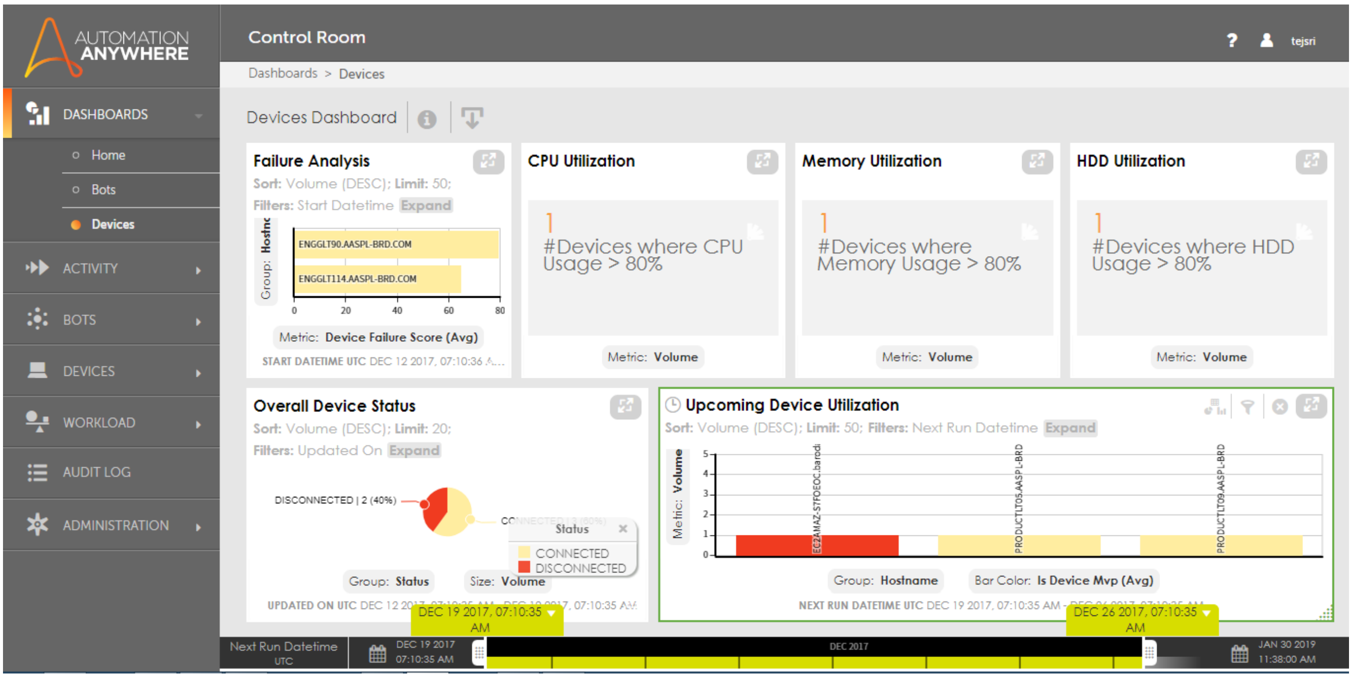
This widget shows all bots that are scheduled to run, which are sorted by the number with which they are run.

Mark the bots that failed a lot before (e.g. failed more than 50% etc.)

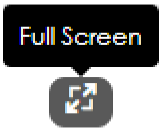
Dashboards - Devices page

As a Control Room user with Dashboard view privileges, you can view and analyze Devices (Bot Runner machine) relevant data when Bots are deployed on those Devices. This data is presented in the form of widgets which provide information about:

1. The number of bots that failed to execute on devices for a given time
2. The number of devices that either crossed, did not achieve or are equal to the threshold for CPU, Memory, and HDD utilization for a given time frame
3. The overall device status for given time frame
4. The number of devices on which automations are scheduled for given time frame



Tip: To expand to a detailed view, click the Full Screen icon for a given widget:

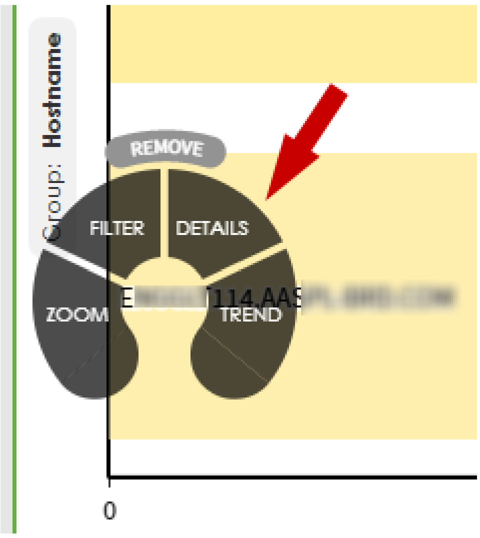


Failure Analysis Widget

This widget displays the top **n** number of devices with most failures for a given time period. You can expand the widget to see a detailed view of the devices that failed:

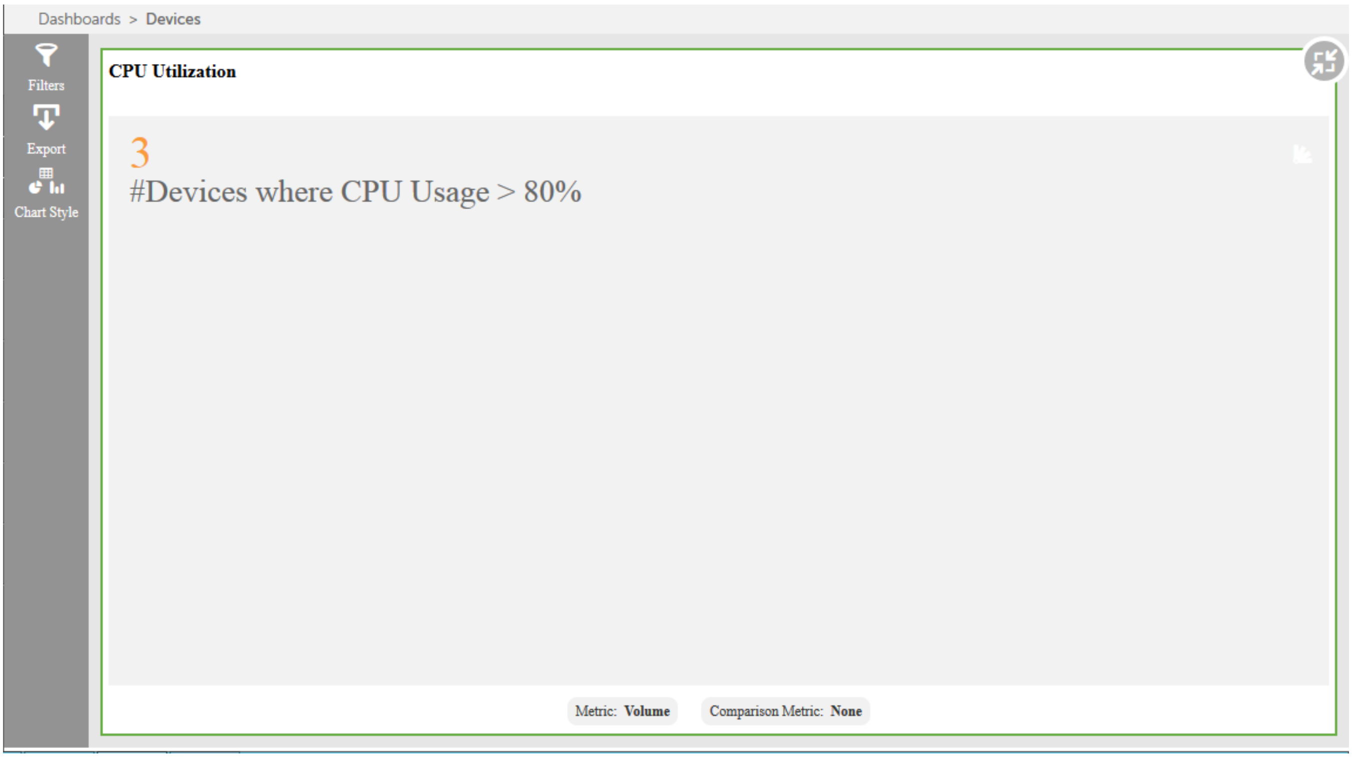
In expanded mode, the widget shows the list of bots that failed ordered by the number of times it failed on that device during that time.

You can also click on the graph to perform tasks such as Zoom, Filter, Details and Trends.



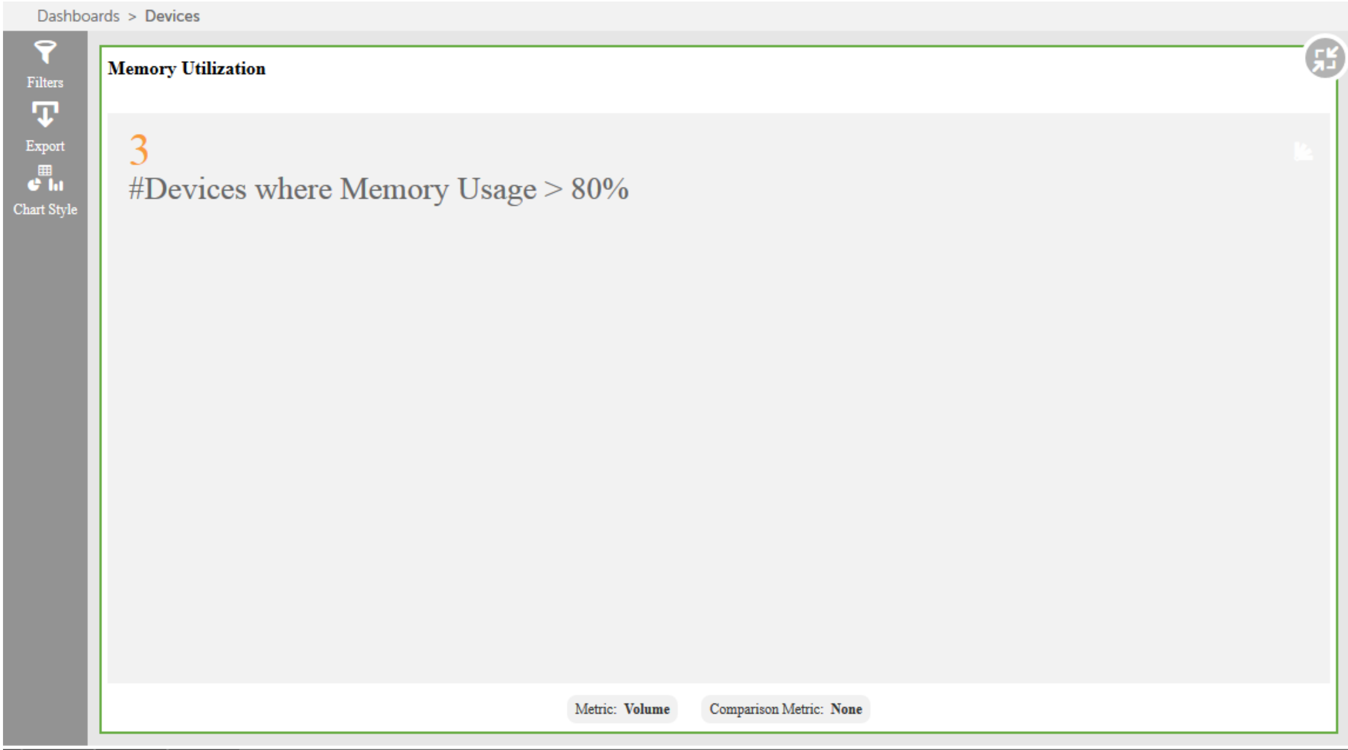
CPU Utilization Widget

This widget displays the number of devices that crossed the threshold for CPU usage for a given time period. You can expand the widget to see detailed view of the CPU usage of devices:



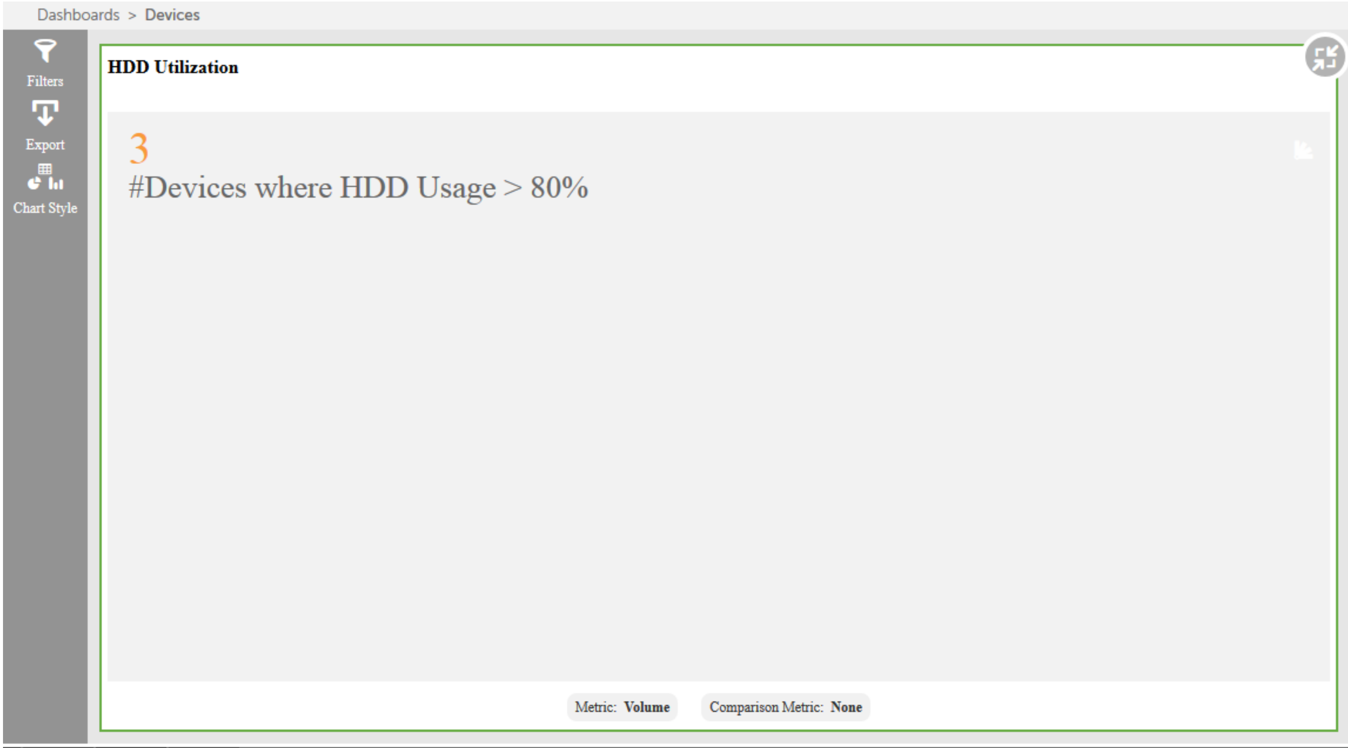
Memory Utilization Widget

This widget displays the number of devices that crossed the threshold for Memory usage for a given time range. You can expand the widget to see detailed view of the Memory usage of devices:



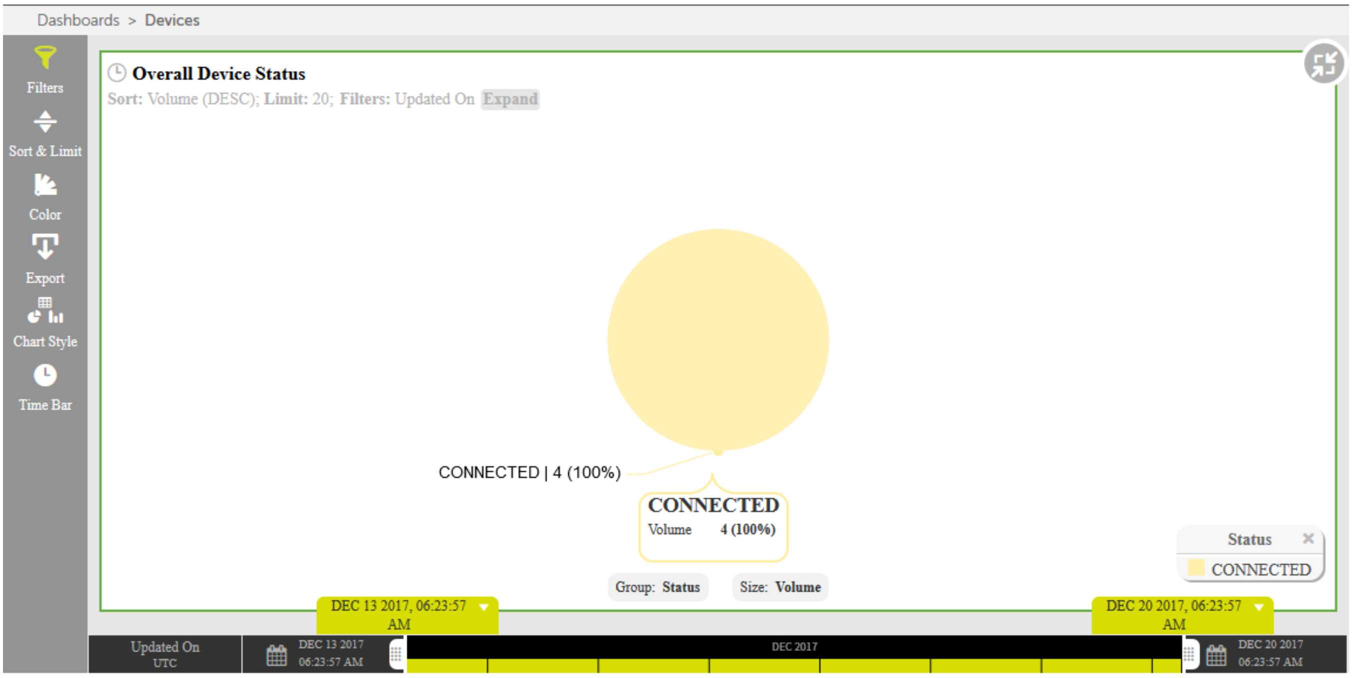
HDD Utilization Widget

This widget displays the number of devices that crossed the threshold for HDD usage for a given time range. You can expand the widget to see detailed view of the HDD usage of devices:

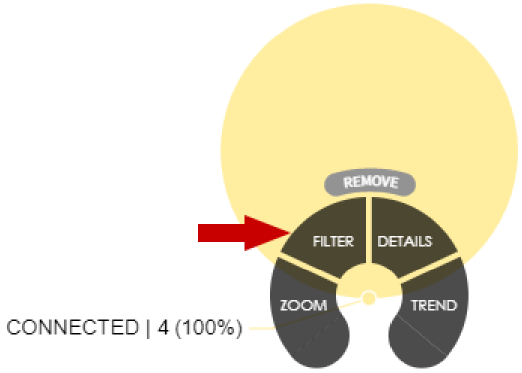


Overall Device Status Widget

This widget displays the number of Devices that are Connecte or Disconnected for a given time range. You can expand the widget to see a detailed view of the device statuses.



You can also click on the graph to perform tasks such as Zoom, Filter, Details and Trends.



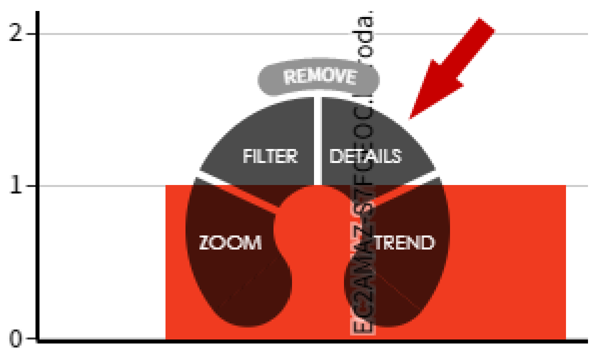
Upcoming Device Utilization Widget

This widget displays the number of devices on which automations are scheduled to run, offline devices and MvP (most used) devices for a given time range. You can expand the widget to see a detailed view of the device utilization status:

In expanded mode, it shows the number of devices that are filtered on **Limit** for a specific time period and sorted either on Device failure score, Hostname, Device MvP, and Volume.

The default time period is set to next 7 days i.e. the data is shown from January 7 - 13 when viewed on January 6.

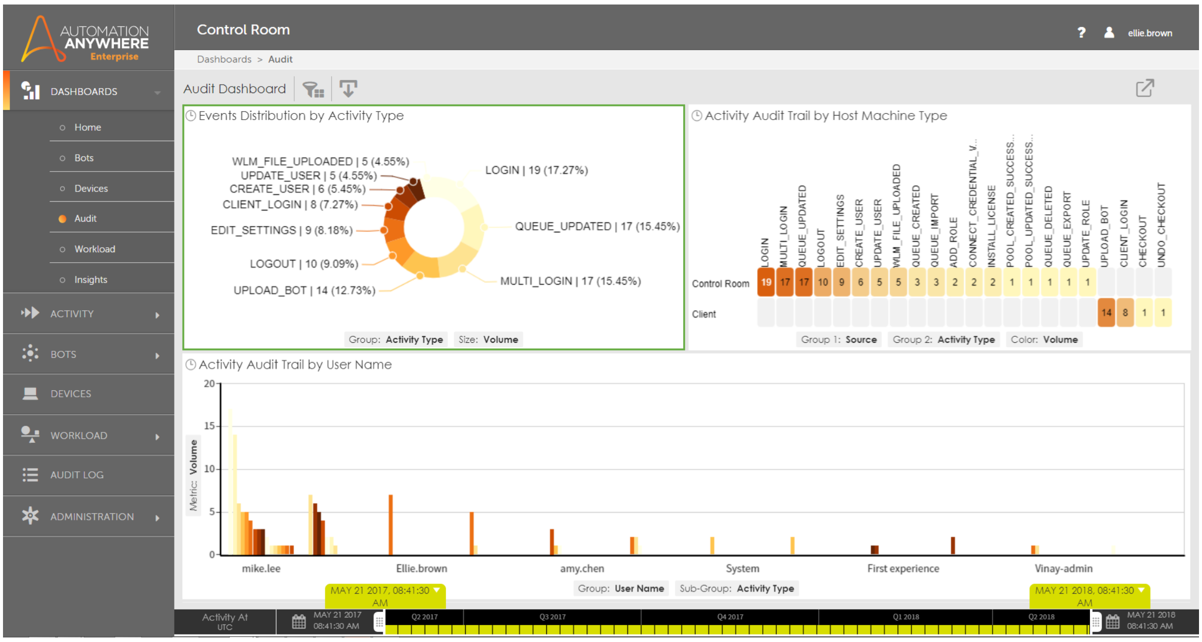
You can also click on the graph to perform tasks such as Zoom, Filter, Details and Trends.



Note: CPU, Memory, and HDD utilization data collectively provide the inputs for Heartbeat widget in Dashboards → Home.

Dashboards - Audit page

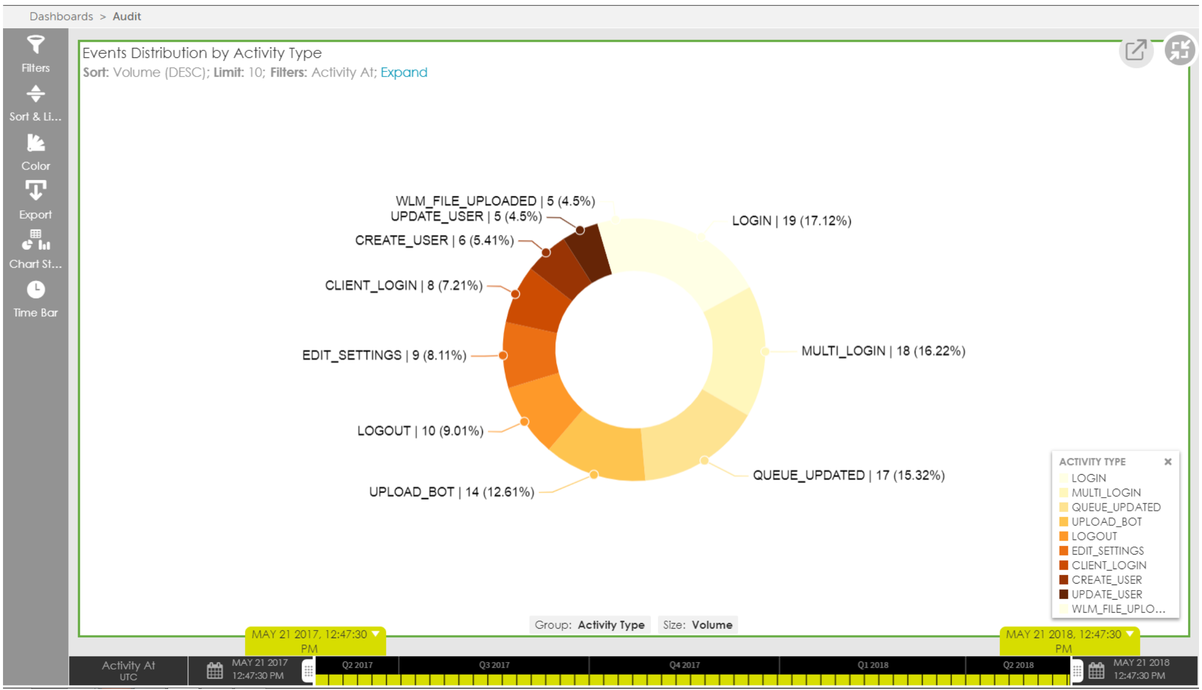
As a Control Room user with **View Dashboards** permission, you can view a snapshot of audit information as processed in the Control Room. It allows you to monitor various events such as the highest percentage of a particular activity being performed based on either user name or host machine type, and a visual representation of the failure log.



Tip: You can opt to customize the chart settings and parameters. The illustrations used in this article are for reference.

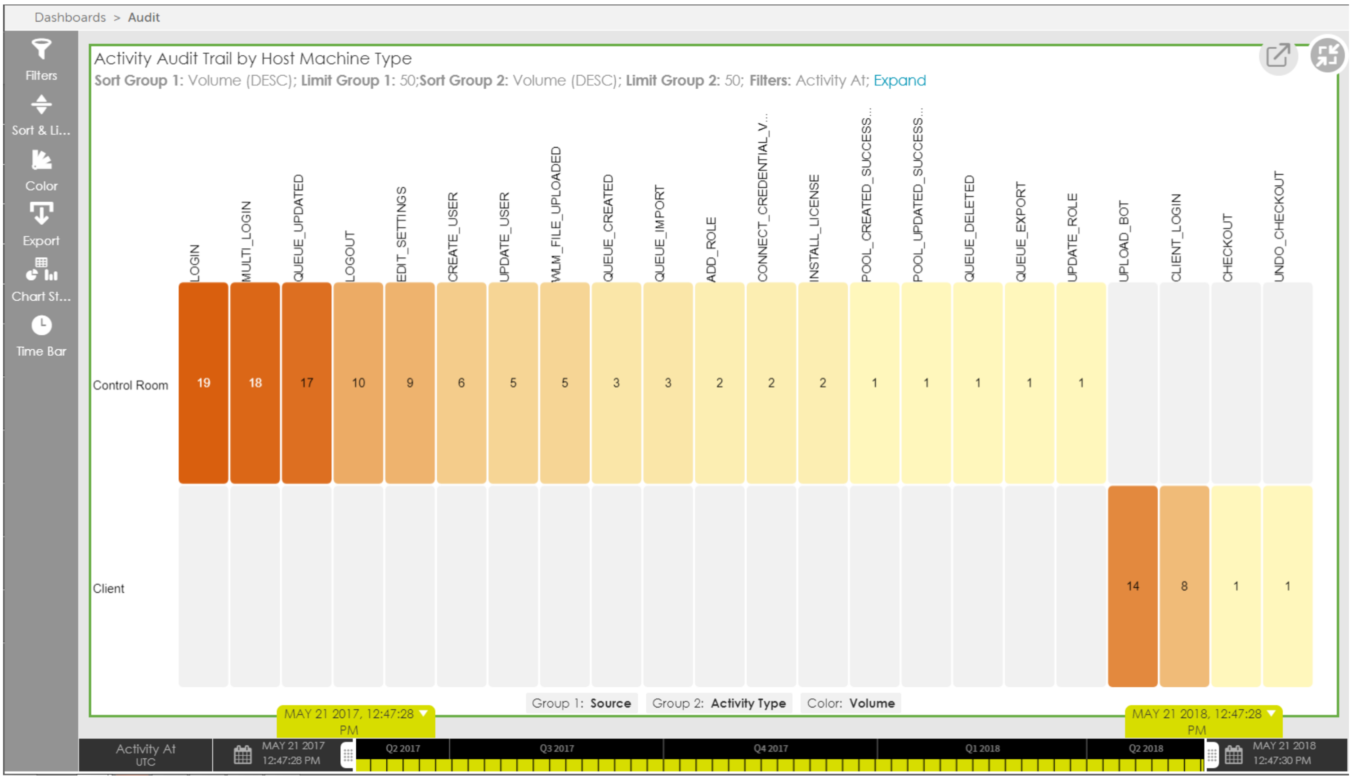
Events Distribution by Activity Type

This widget provides a chart based view of activities filtered on the **Action Type** column in the Audit Log page for as specific time period.



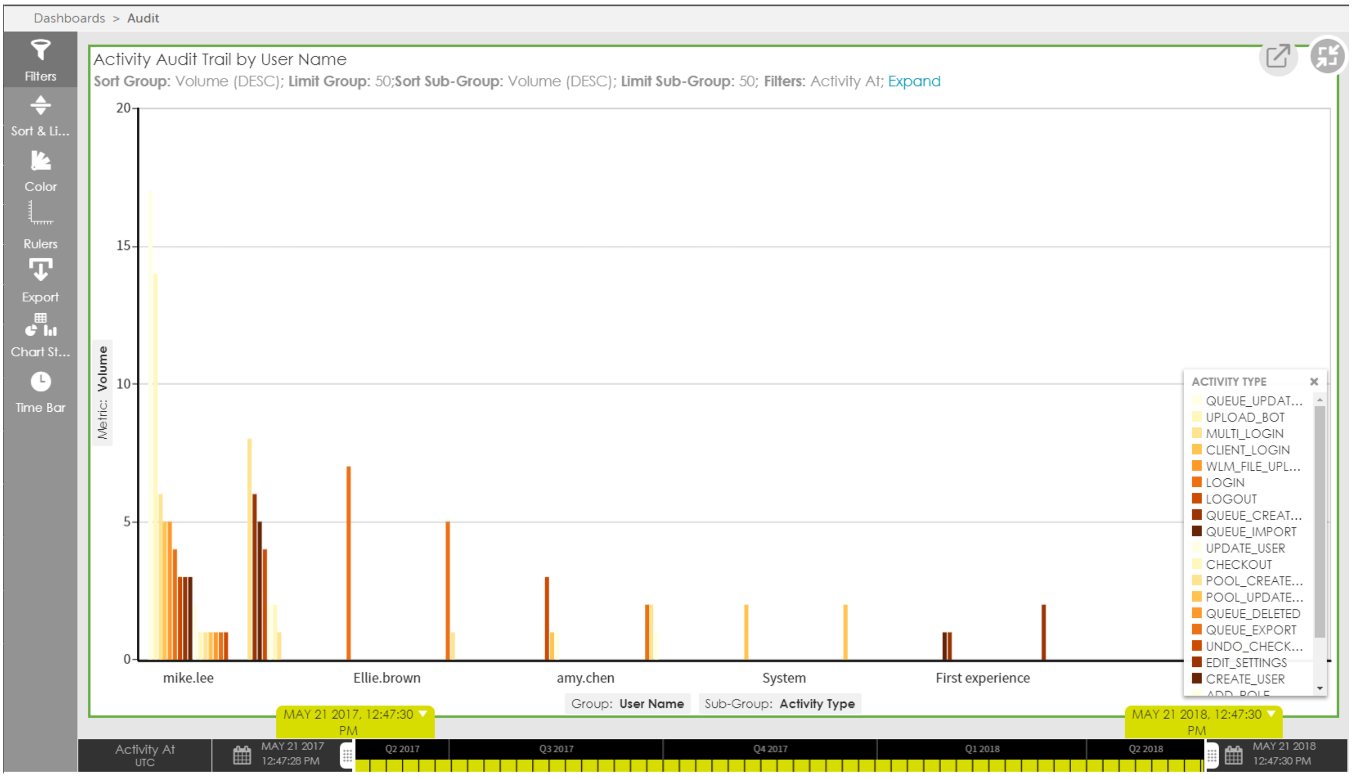
Activity Audit Trail by Host Machine Type

This widget provides a chart based view of activities filtered on the **Source** column in the Audit Log page for as specific time period.



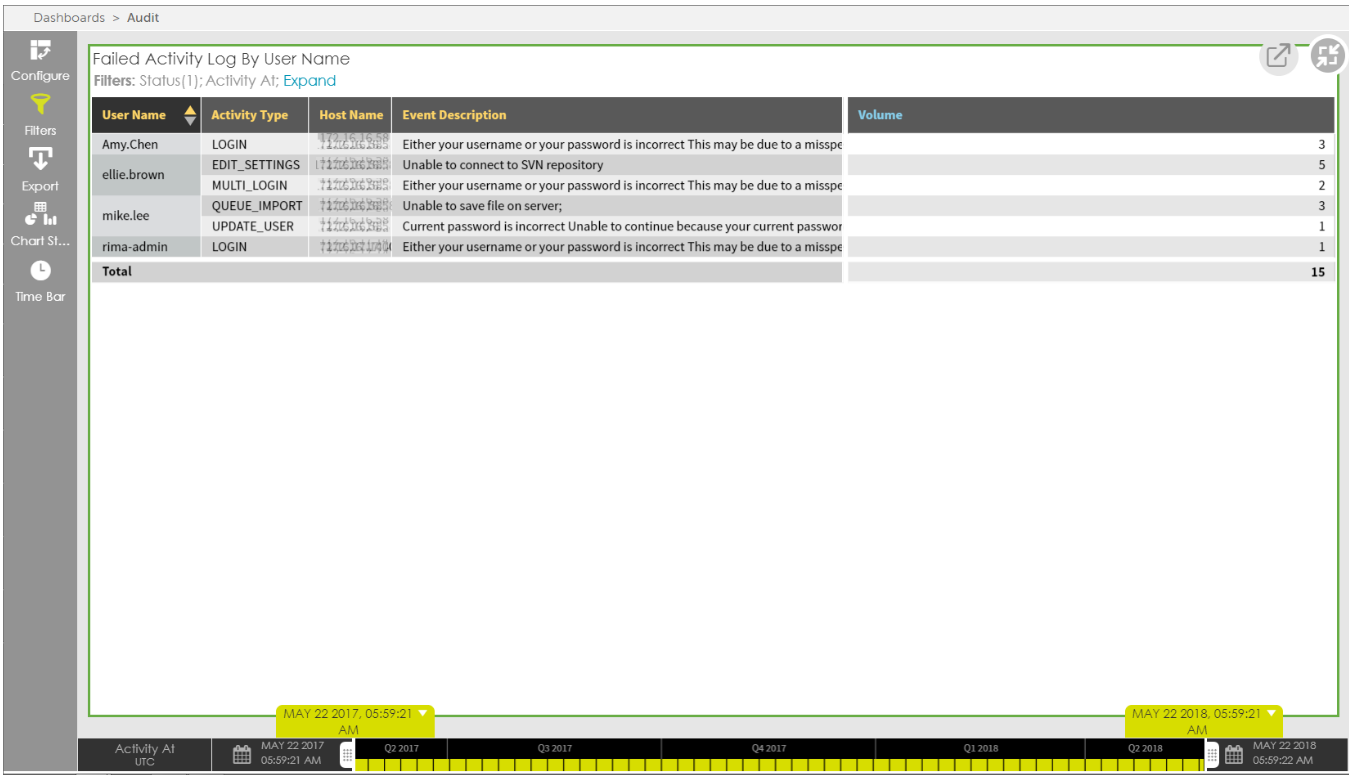
Activity Audit Trail by User Name

This widget provides a chart based view of activities filtered on the **Action Taken By** column in the Audit Log page for as specific time period.



Failed activity log by user name

This widget provides a chart based view of activities filtered on the **Action taken by**, **Action type**, and **Source** columns in the Audit Log page for as specific time period.



For more information on audit details, refer View audit details.

Dashboards - Workload page

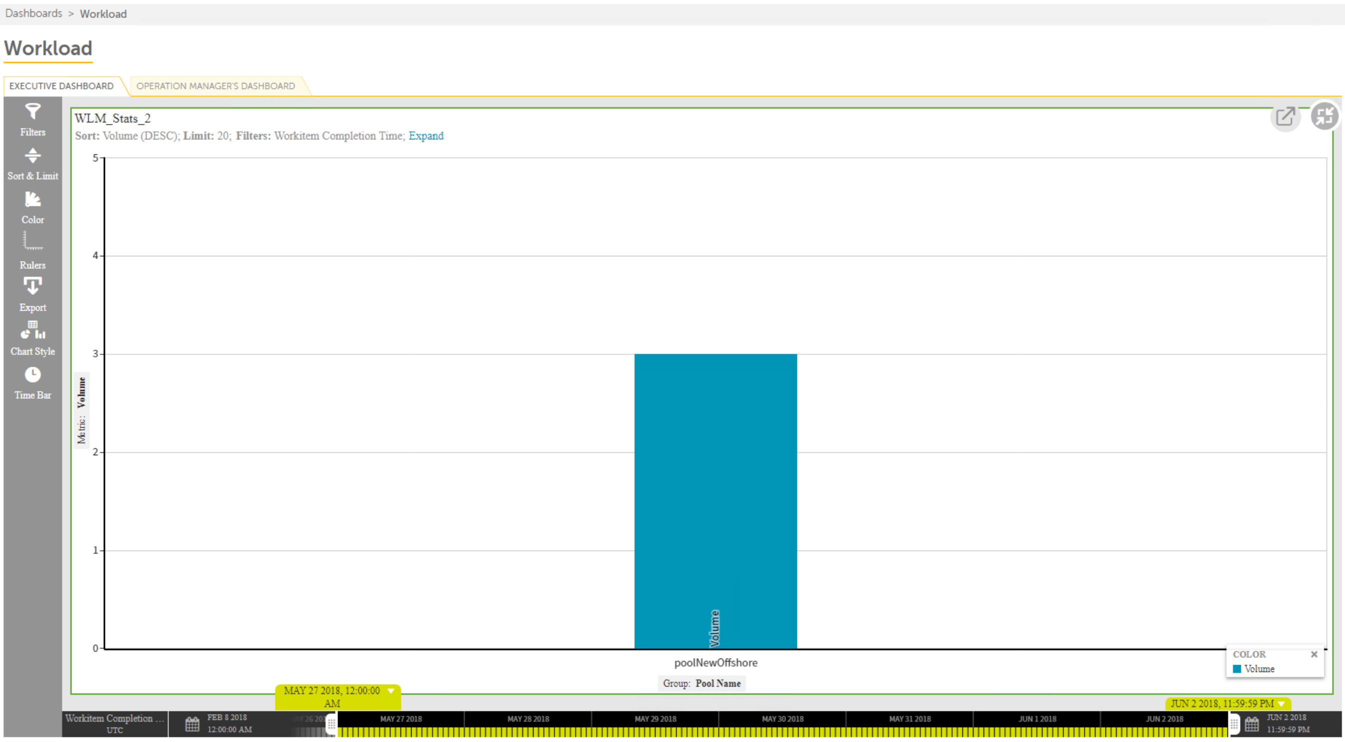
As a user with View Dashboard permissions, you can view Workload status of device pools, queues and work items in the Workload Executive and/or Operation Manager's Dashboard.

Executive dashboard

In the Executive dashboard, you can monitor the progress of the queues for which you are owner and/or consumer:

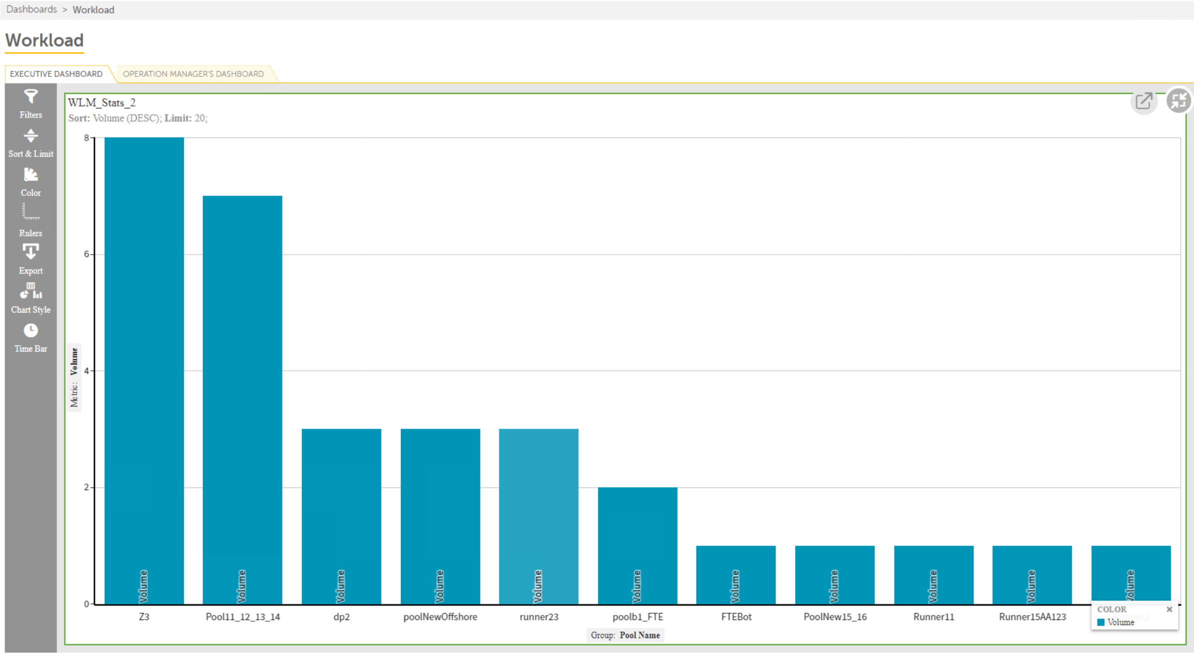
1. Device pools by backlog

In this widget, you can view the device pools by backlog. This allows you to adjust the device pool size or reorder the automations if required. The device pool backlog is measured in the number of hours it takes to complete the existing work items from all automations in that pool. Refer SLA - Calculator for details.



2. Queues by time to complete

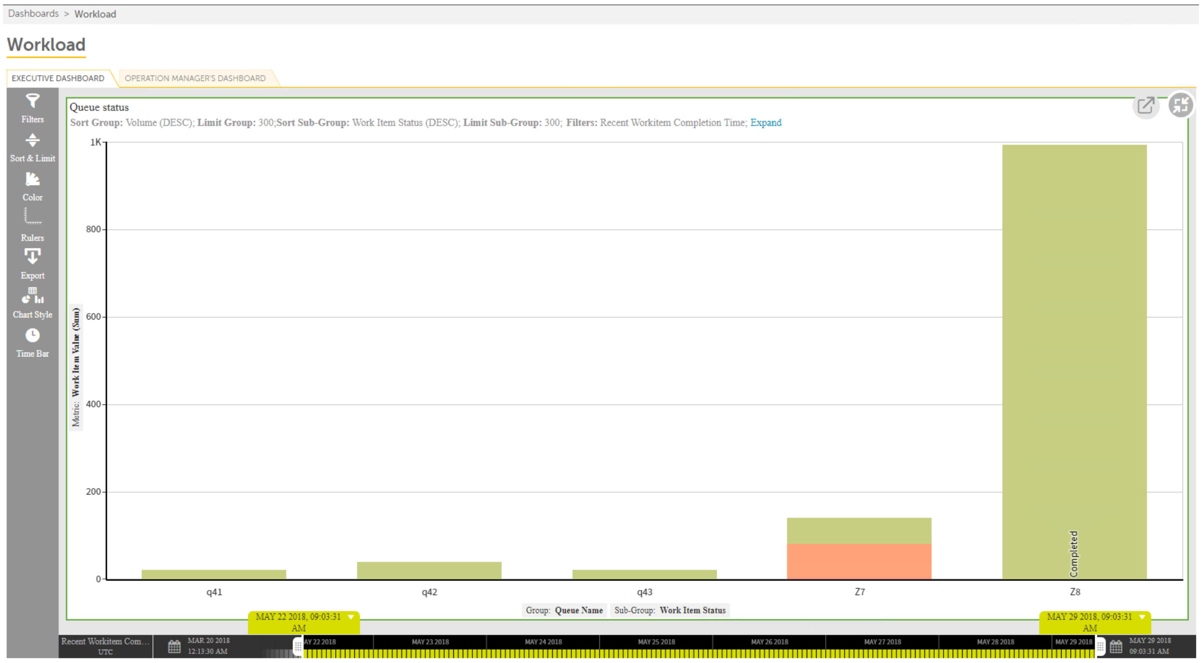
In this widget, you can view the list of queues ordered by time to complete. This allows you to pause or change the priority of the automations if required. Time to complete is measured in the number of hours it takes to complete the existing work items. Refer SLA - Calculator for details.




```
Tip: Click on individual queue to view its details such as queue name, number of open items, average processing time, and expected time to complete.
```

3. Queue status

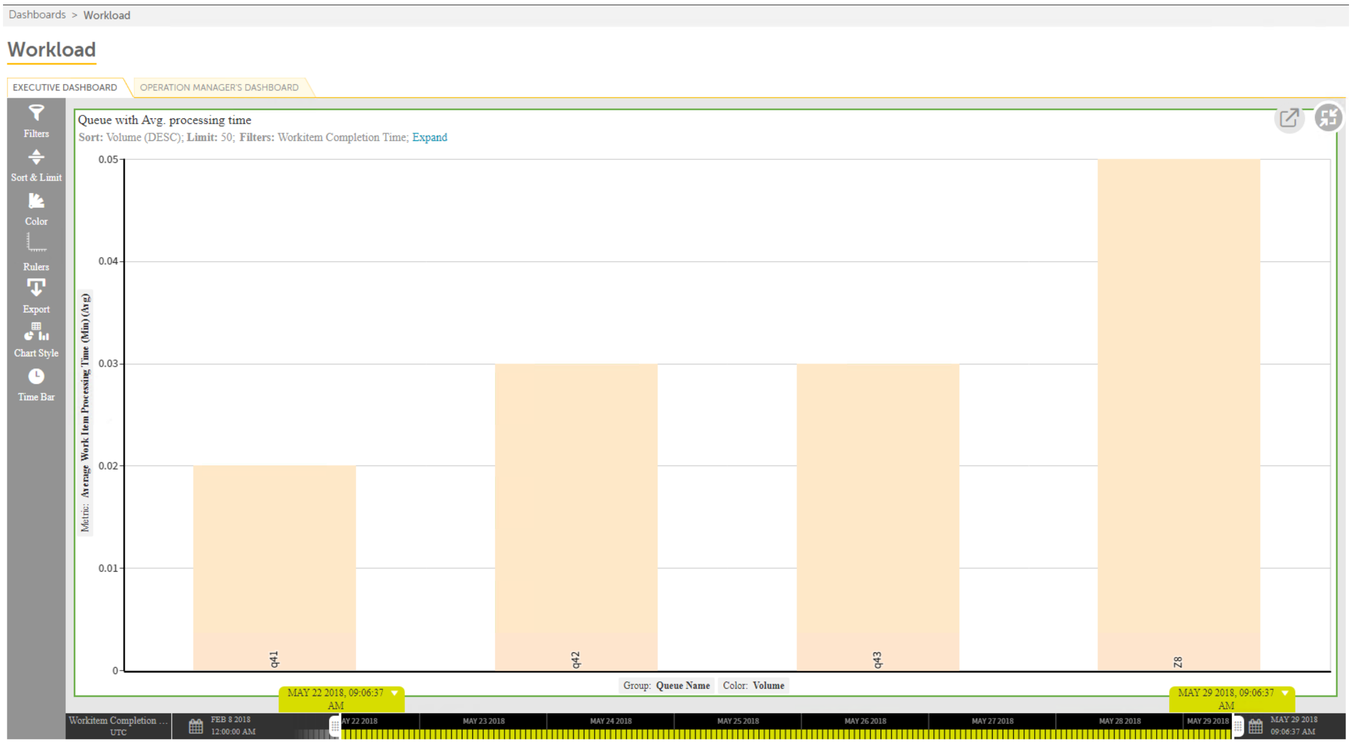
In this widget, you can view the list of queues that were processed in the last **n** days. This allows you to monitor the progress (status) of your workload items. The statuses displayed for the work items of each queue are Active, Successful, Unsuccessful, Ready to run, On hold, and Data error.




```
Tip: By default the queues that were processed in the last 7 days are shown. You can opt to provide a custom date range for last 6 months.
```

4. Queue with average processing time

In this widget, you can view the list of queues that were processed in the last **n** days with average processing time. This allows you to understand if there is any issue with the processing of these work items. The list of queues are shown on the basis of the average processing time for a work item with a daily average.



Tip:

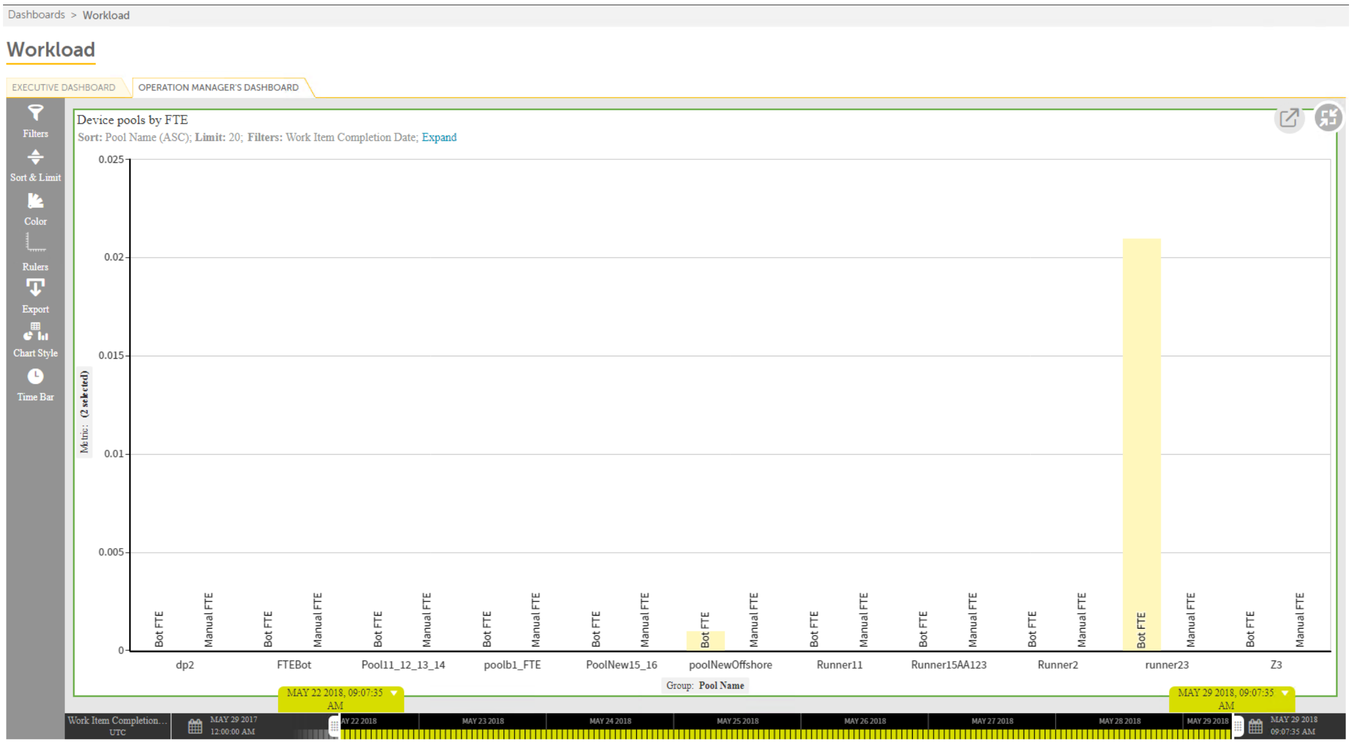
- Click on individual queue to view its details such as queue name, automation name, date, and average processing time.
- By default the queues that were processed in the last 7 days are shown. You can opt to provide a custom date range for last 6 months.

Operation Manager's dashboard

In the Operation Manager's dashboard, you can monitor the queues for which you are owner, consumer, and/or participant.

1. Device pools by FTE (Full Time Equivalent)

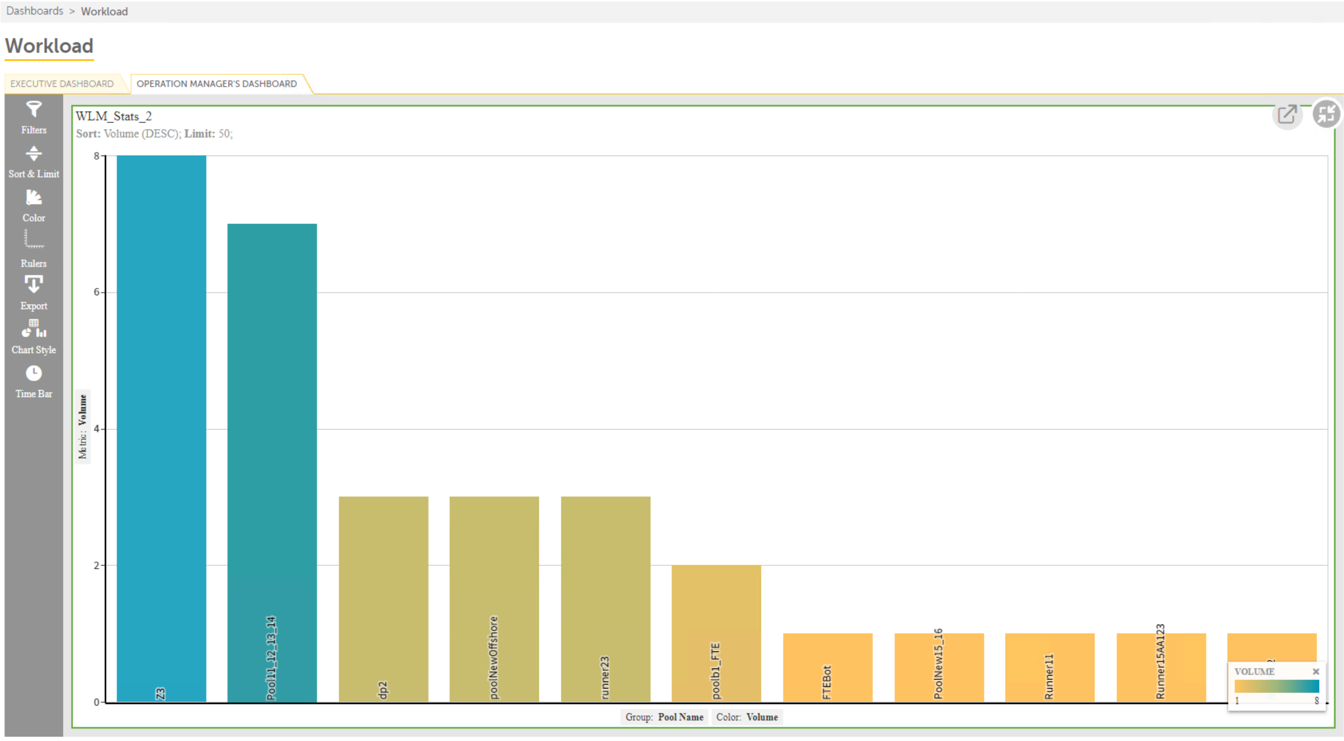
In this widget, you can view pools in descending order of FTE (Full Time Equivalent). This allows you to measure the value of each pool in terms of the equivalent manual effort required to process the same work item.



> **Tip:** By default the queues that were processed in the last 7 days are shown. You can opt to provide a custom date range for last 6 months.

2. Pools by decreasing error rate

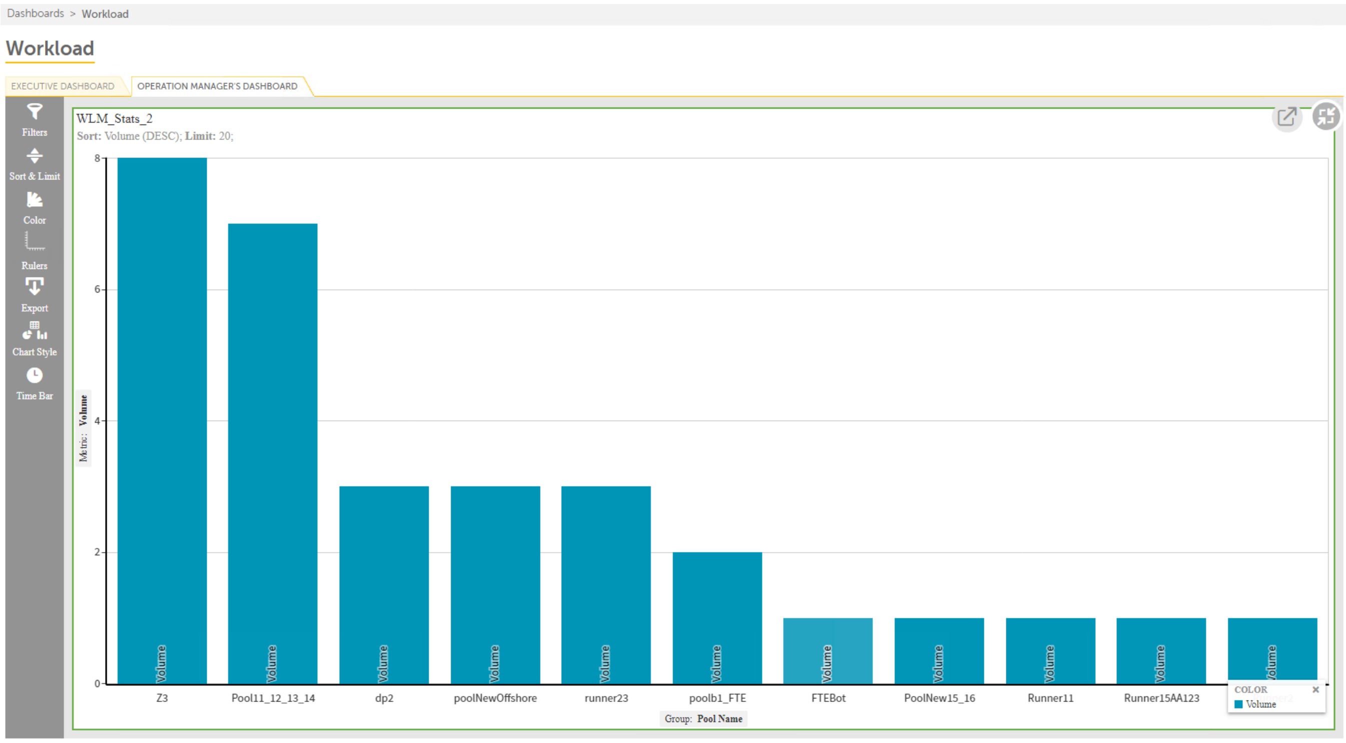
In this widget, you can view the list of pools ordered by decreasing error rate. It thus gives you a quick view of pools that require attention. This error rate is measured by the number of work items failed divided by the number of work items processed from that pool.



Tip: `Click on the individual pool to view details such as pool name, automation name, queue name, number of items processed, and number of failed items.`

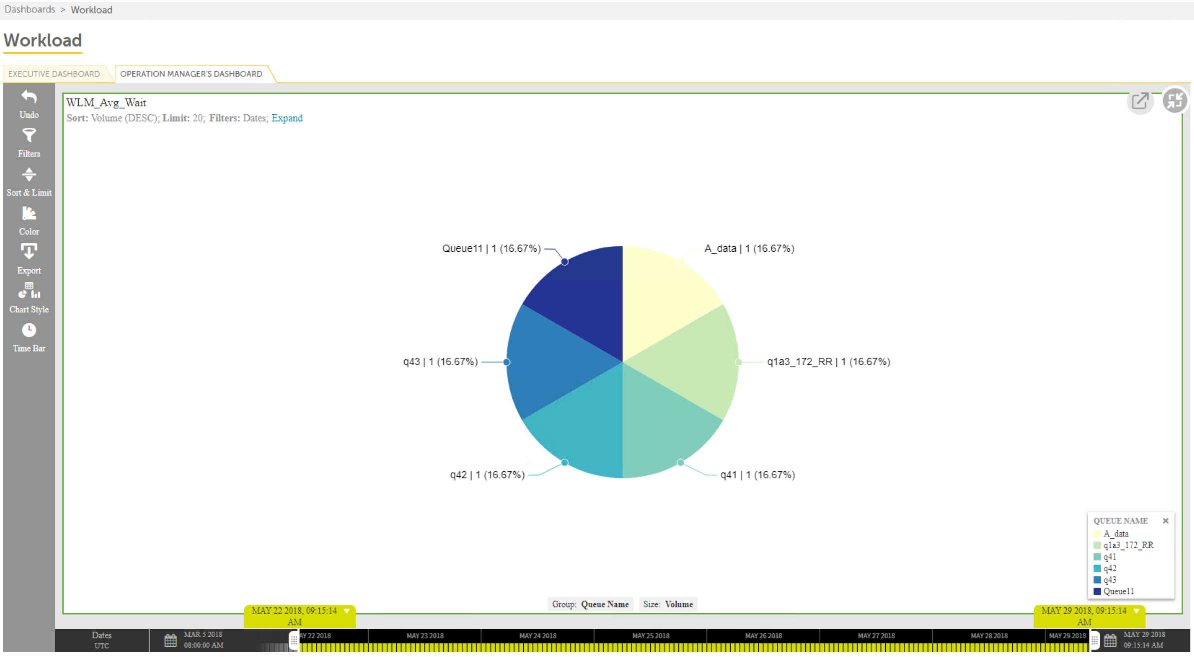
3. Device pools by backlog

In this widget, you can view the device pools by backlog. This allows you to adjust the device pool size or reorder the automations if required. The device pool backlog is measured in the number of hours it takes to complete the existing work items from all automations in that pool. Refer SLA - Calculator for details.



4. Queues with average wait time

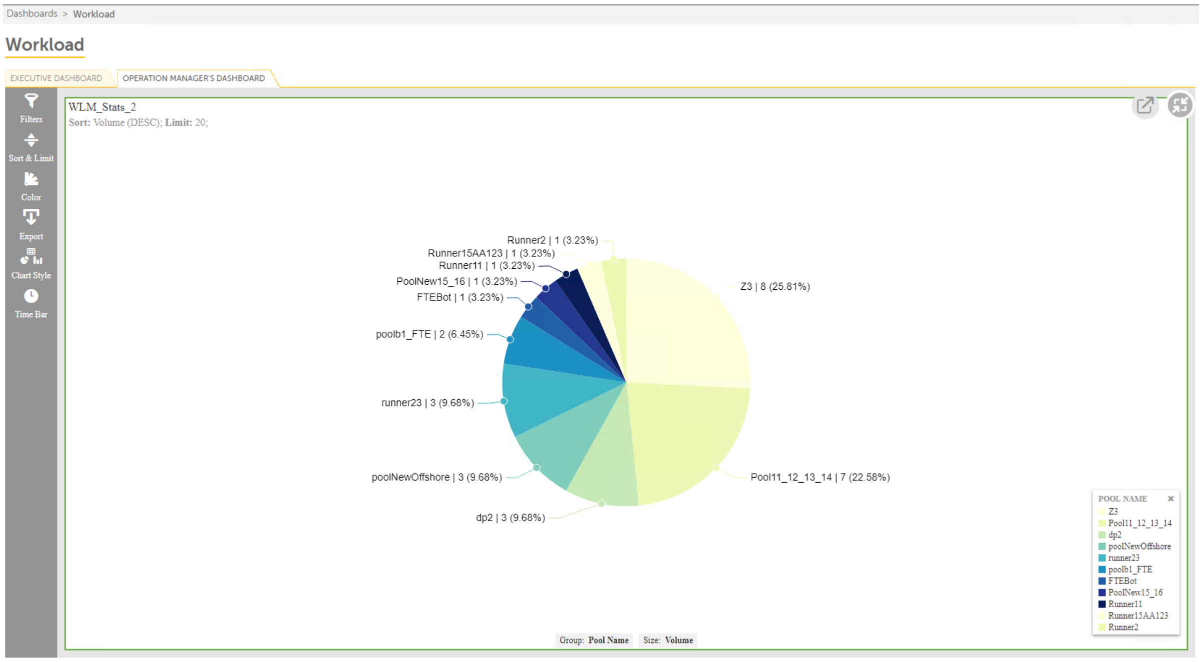
In this widget you can view the list of queues that were processed in the last **n** days with average wait time. This allows you to decide whether to increase priority or pool size to meet the business needs as required. For each queude, the average wait time for a work item in that queue with a daily average is shown. The wait time is calculated by subtracting processing start time from the automation start/resume time.



Tip: `By default the queues that were processed in the last 7 days are shown. You can opt to provide a custom date range for last 6 months.`

5. Queues by decreasing error rate

In this widget, you can view the list of queues ordered by decreasing error rate. It thus gives you a quick view of queues that require attention. This error rate is measured by the number of work items failed divided by the number of work items processed from that pool.



Tip: `Click on individual pool to view details such as pool name, automation name, queue name, number of items processed, and number of failed items.`

Refer articles in the Workload module for details on queues, work items, and queue processing.

Dashboards - Insights page

Bot Insights helps automation experts to access real-time business insights and digital workforce performance measurement by leveraging massive amounts of content-level and productivity data that the deployed bots generate, touch, interact with, and process. It helps the automation experts and consumers to interactively analyze task data and enhance widgets.

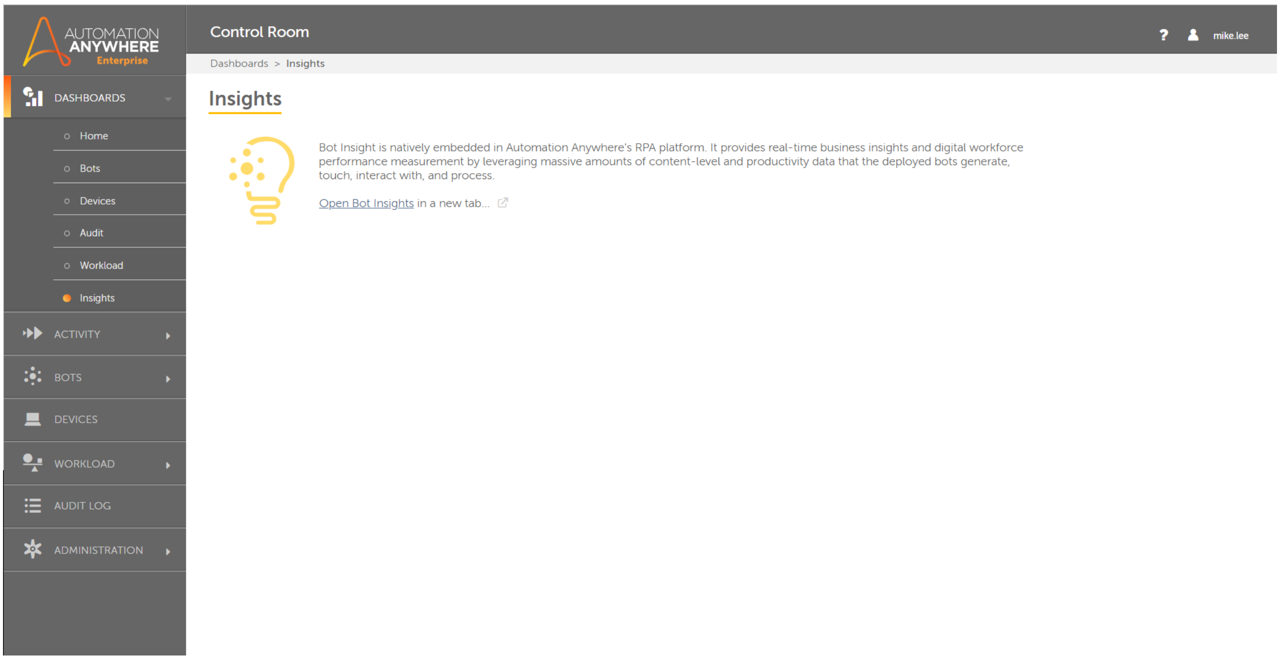
Accessing Bot Insights

You can access the Bot Insights application from the Control Room Insights dashboard if you are a **Bot Creator** and/or a Control Room user with **AAE_Bot Insight Admin**, **AAE_Bot Insight Consumer**, or **AAE_Bot Insight Expert** role privileges. Refer Create a role for description on system defined roles.

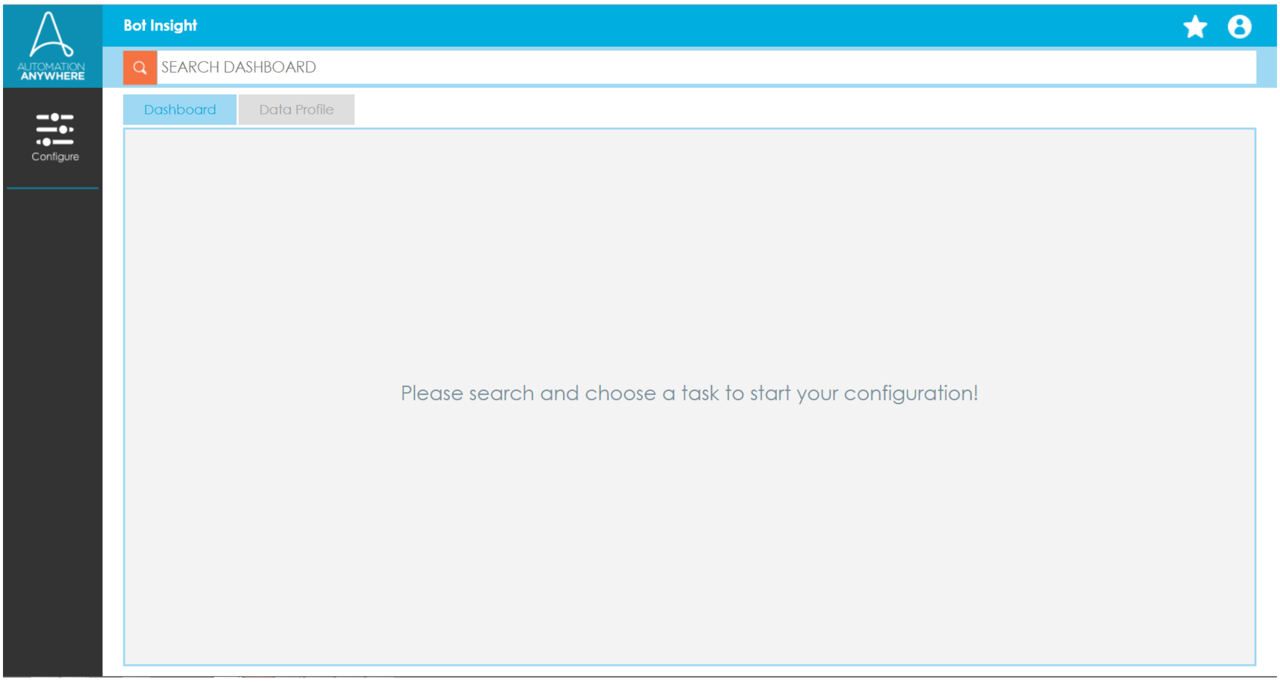
Additionally, the **Bot Insights - Business Analytics** license also needs to be turned on. Refer Licenses - an overview for details.

To access Bot Insight application,

1. Go to **Control Room** → **DASHBOARDS** → **Insights**.

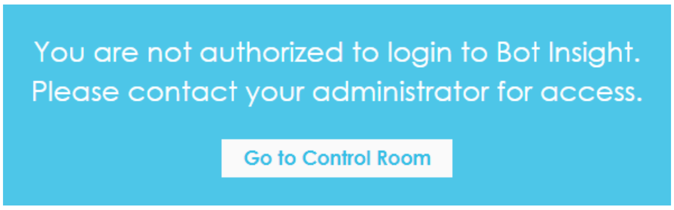


2. Click on the **Open Bot Insights** link.
3. The system opens the Dashboard of Bot Insights application in a separate tab:

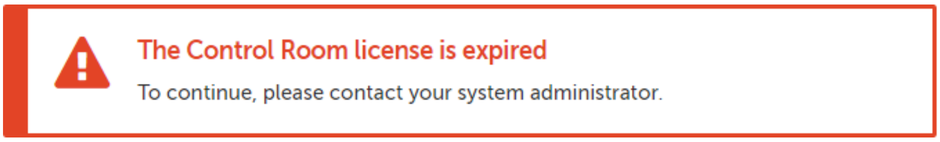


When you are already logged into the Control Room, you do not need to login again into Bot Insights. For more information about the Single Sign-on feature into applications, see Log onto Bot Insights.

- If you do not have the Bot Insight permission, you are shown:



- Click on **Go to Control Room**.
- If the license has expired, you are shown:



For more information on Bot Insights, refer the Bot Insights user guide.

Control Room APIs

The Automation Anywhere Enterprise Control Room provides various public APIs which allow you to customize your business automation for third party applications. It enables the third party applications to consume RPA, orchestrate bots and manage the RPA data based on events.

Control Room offers the following APIs:

1. Authentication
2. Bot Login Credentials
3. Bot Deployment
4. Export Import Workload Management Configuration
5. Get list of all queues
6. Get list of all work items in a given queue
7. Insert work item data to a given queue

API for authentication

All the APIs are preceded by an Authentication API, wherein the user invoking third party application has to authenticate so as to use the downstream APIs. Click here for details.

API to manage bot login credentials

In enterprise organizations where the password rotation policy is applied, the Client user has to remember to update the password from Tools → Options → Login Settings during each password rotation. To automate this process, Control Room enables you to use an API to create, update or delete the Login Credentials stored in the credential vault. Click here for details.

API for bot deployment

To deploy Bots onto the Automation Environment the user has to login into Control Room, select the Bot and the Bot Runners and then 'Run/Schedule' the task. However, as the Automation scenarios scale up, there is an increasing need to deploy/trigger Bots from an external third party application. To meet this business requirement, you can use the Bot Deployment API which enables you to trigger a Bot from an External System. Click here for details.

API for export import of bots for Business Lifecycle Management

Usually, the Control Room user has to depend on means other than Control Room (for example email) to deploy TaskBots from one environment to another. Using the Export-Import APIs, you can easily introduce a customized BLM solution thus removing all external factors that could possibly disrupt your automation life cycle. Click here for details.

API to export and import Workload Management (WLM) configuration

Automation Anywhere has provided the Workload Management configuration API which can be used to export and import Workload configuration to move validated configurations from one environment to another. Click here for details.

API to get list of all queues

Automation Anywhere has provided a REST API that allows you to fetch the list and queue details available in the Control Room. Click here for details.

API to get all work items in a given queue

Automation Anywhere has provided a REST API that allows you to fetch the list of work items in a given queue and its details available in the Control Room. Click here for details.

API to add/insert work item data to a given queue

Automation Anywhere has provided a REST API that allows you to insert work item data in a given queue available in the Control Room. Click here for details.

Control Room API for Authentication

Control Room v.11 exposes public APIs so as to manipulate the Control Room data and to deploy bots from an external system. This enables third party applications to consume RPA, orchestrate bots and to manage the RPA data based on events - for example, create an AAE user as soon as a user is created in SAP system; update the login credentials in AAE as soon as password is rotated in domain controller.

All the APIs are preceded by an Authentication API, wherein the invoking third party application user has to authenticate so as to use the downstream APIs.

Authentication API

API: v1/authentication

If the Control Room URL is https://ultron.com:81, then the API will be https://ultron.com:81/v1/authentication

The API takes two parameters as input in JSON format:

1. The username of the AAE user
2. The password of the AAE user

> **Note:** All parameters are mandatory.

For example:

1. The AAE username is **mike_williams**.
2. The AAE password is **abc123**, then the JSON will be :

```
 {
"Username":"mike_williams",
”Password":"abc123"
 }
```

If the authentication is successful, the Control Room will issue an authentication token which needs to be passed on to the Deployment API as header information.

> **Note:** The authentication token will ONLY be valid for 15 minutes from the time it is issued.

Authentication API Response Codes

Http Status code	Response	Description
200	{ "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9. eyJ1c2VyIjoiMSIsImlzcyI6Imh0dHA6Ly9sb2NhbGhvc3Qvd2ViY3 JzdmMvliwiYXVkIjoiaHR0cDovL2xvY2FsaG9zdC93ZWJjcnN2Yy8iLCJle HAiOjE0OTUwOTAwOTksIm5iZiI6MTQ5NTA4OTE5OX0.qPPhpti0j7 LGAmWkj3XFymFfJXzA1P4zPehIjVYfulc" }	Authentication is successful
401	{ "message": "Invalid credentials." }	◦ The password is invalid ◦ User does not exist ◦ AD Authentication - Credentials are Invalid
401	{ "message": "Please verify your email by clicking on the email verification link. This is mandatory as you will be able to login post verification only."	Email notification is enabled - user has not verified email

	}	

402	{
	
	"message": "License expired."
	
	}
		License has expired

403	{
	
	"message": "Your account is not activated. Please contact the admin."
	
	}
		User is deactivated

Control Room API for Bot Deployment

To deploy Bots onto the Automation Environment, currently, the user has to login into Control Room, select the Bot and the Bot Runners and then 'Run/Schedule' the task.

However, as the Automation scenarios scale up, there is an increasing need to deploy/trigger Bots from an external third party application.

To meet this business requirement, Automation Anywhere Enterprise has published Application Programming Interfaces (APIs) using which a Bot can be triggered from an External System.

A Control Room user can use these APIs to deploy Bots (Tasks) to BotRunners on commencement of events specified by a third party/external application.

Key Features and Business Benefits of Control Room APIs

- Bots can be deployed from an external third party systems using AAE APIs.
- The input and output of APIs is JSON based (industry standard data-interchange format).
- Bot Deployment can be orchestrated from an External Application / Workflow using a combination of scripts and AAE APIs.

Note: The Bot deployment API can ONLY be invoked once the system/user has authenticated using the Authentication API

Also, the user will need to have the 'Run my bots' privileges and the privileges of the bot runners on which the bot is to be deployed.

Deployment API

The Deployment API is used to deploy Bots to BotRunners.

API: <Control Room URL>/v1/schedule/automations/deploy

For example, if the Control Room URL is https://www.ultron.com:81 ; then the bot deployment API will be https://www.ultron.com:81/v1/schedule/automations/deploy

The user can pass three parameters as JSON string.

1. Bot name with relative path - This is mandatory.
2. List of Bot-Runners and users in JSON format - This is mandatory.
3. Use RDP based approach - This is optional and set to **false** by default.

Deployment Scenario and corresponding JSON string:

1. For example, the name of the Bot is AccountsBot.atmx and the Bot is under 'My Tasks'
2. The Bot is to be deployed on 3 machines
   - First machine hostname BR-1 with user U-1
   - Second machine hostname BR-2 with user U-2
   - Third machine hostname BR-3 with user U3.
3. The JSON string in the above scenario will be:

```
{
"taskRelativePath":"My Tasks\\AccountsBot.atmx", "botRunners":
[
{
"client":"BR-1", "user":"U-1"
},
{
"client":"BR-2", "user":"U-2"
},
{
"client":"BR-3", "user":"U-3"
}
]
}
```

Bot Deployment API Response Codes

Http(s) Status code	Response - Description
200	Succesful creation of automaton.
400	Bad Request
401	Authentication Required
403	Unauthorized access
409	Conflict
500	Internal Server error

Control Room API to manage bots login credentials

When the Bot is deployed from Control Room to the Bot Runner, the Bot will auto-login into the Bot Runner (if the machine is locked / logged off). The Bot will use the credentials stored in the Credential Vault for auto-login. These credentials are set by the user using the Tools → Options → Login Settings of AAE Client.

However, there could be cases when the user's Windows password is modified; especially in Enterprises where there is a password rotation policy. In such cases, the user has to remember to update the new password from Tools →Options → Login Settings.

In order to automate the above process, Control Room 11.1 provides a direct API to create, update or delete the Login Credentials stored in the credential vault.

There are 2 steps to use this API:

1. Invoke the Authentication API
2. Invoke the Login Credentials API

Authentication API

The details for the Authentication API are provided in the article Control Room API for Authentication.

Login Credentials API

Note that only the Control Room Administrators (users having AAE_Admin Role) can use the Login Credentials API; this means that if the user invoking the Authentication API has an AAE_Admin role, only that user can use the Login Credentials API.

Also, this API will make use of the authentication token that is obtained using the Authenication API. The authentication token has to be passed on as one of the header inputs to the Login Credentials API.

API: v1/credentialvault/external/credentials/loginsetting

If the Control Room URL is https://ultron.com:81, then the API will be: https://ultron.com:81/v1/credentialvault/external/credentials/loginsetting

The API takes three parameters as input in JSON format:

1. The username of the AAE user.
2. The Login (Windows) username for the user which is to be updated in the Credential Vault against that user.
3. The Login (Windows) password for the user which is to be updated in the Credential Vault against that user.

```
Note: All parameters are mandatory.
```

For example:

If we take a 'Database Authentication' scenario (where users are stored and authenticated by the Control Room) and

1. The AAE username is **mike_williams**
2. The fully qualified Login username is **ultron.com\mike.williams**
3. The Login password is **abc123**, then the JSON will be
{ "Username": "mike_williams", "Windows_Username": "ultron.com\\mike.williams", "Windows_Password": "abc123" }

Using the Login Credentials API, the Control Room Admins can:

1. Create a user's Login Credentials in the Control Room - by using the 'POST' method
2. Update a user's Login Credentials in the Control Room - by using the 'PUT' method
3. Delete a user's Login Credentials from Control Room - by using the 'DELETE' method.

VB Script to Create User's Login Credentials

```
'AUTHENTICATION API - START
Set objStream = CreateObject("ADODB.Stream")
objStream.CharSet = "utf-8"
objStream.Open
objStream.LoadFromFile("D:\Deven.Deshpande\Office\Products\API for CV\auth-input.txt")

restRequest = objStream.ReadText()

objStream.Close
Set objStream = Nothing

contentType = "application/json"

Set oWinHttp = CreateObject("WinHttp.WinHttpRequest.5.1")

oWinHttp.Open "POST", "http://productslt12.aaspl-brd.com:81/v1/authentication", False

oWinHttp.setRequestHeader "Content-Type", contentType

oWinHttp.Send restRequest

response = oWinHttp.StatusText

MsgBox response

Dim AuthToken

'Set oJson = new aspJSON

AuthToken = oWinHttp.ResponseText

'oJson.loadJSON(AuthToken)

'MsgBox oJson.data("token")

MsgBox AuthToken

'AUTHENTICATION API - ENDS

'---------------------------------------------------

'RESPONSE HEADER PARSING - START
Dim sToken
Dim posUser

sToken = Right(AuthToken, Len(AuthToken) - 10)

MsgBox(sToken)

'sToken = Left(sToken, Len(sToken) - 4)

posUser = InStr(sToken, "user")

MsgBox posUser

sToken = Left(sToken, posUser - 4)

MsgBox(sToken)

'RESPONSE HEADER PARSING - END

'DEPLOYMENT API - START

Set objStream_dep = CreateObject("ADODB.Stream")
objStream_dep.CharSet = "utf-8"
objStream_dep.Open
objStream_dep.LoadFromFile("D:\Deven.Deshpande\Office\Products\API for CV\cred-input.txt")

restRequest = objStream_dep.ReadText()
```

```
objStream_dep.Close
Set objStream = Nothing

contentType = "application/json"

Set oWinHttp = CreateObject("WinHttp.WinHttpRequest.5.1")

oWinHttp.Open "POST", "http://productslt12.aaspl-brd.-
com:81/v1/credentialvault/external/credentials/loginsetting", False

oWinHttp.setRequestHeader "Content-Type", contentType

oWinHttp.setRequestHeader "X-Authorization", sToken

oWinHttp.Send restRequest

response = oWinHttp.StatusText

MsgBox response

Dim DeployResponse

DeployResponse = oWinHttp.ResponseText

'MsgBox DeployResponse

'DEPLOYMENT API - ENDS
```

Contents of Input Files

Applicable to the above VB Script

The text Of auth-input.txt will have the input JSON String For authentication **{"UserName":"admin","Password":"12345678"}**

The text For deploy-input.txt will have the input JSON String For deployment
{ "Username": "mike_williams", "Windows_Username": "ultron.com\\mike.williams", "Windows_Password": "abc123" }

API - Export and Import Bots for Bot Lifecycle Management

Usually, the Control Room user has to depend on means other than Control Room (for example email) to deploy TaskBots from one environment to another. Using the Export-Import APIs, you can easily introduce a customized Bot Lifecycle Management (BLM) solution thus removing all external factors that could possibly disrupt your automation life cycle.

As a Control Room user with **Export bots** and **Download** bots permission, you can export a bot and its dependent files. Similarly, as a user with **Import bots** and **Upload** bots permission, you can import that bot and its dependent files.

For example, you can move the Bots that are verified as production ready from staging to production.

You can use the Control Room Export Import REST API to manage your automation TaskBots including dependent files in different environments such as Development, Testing, Acceptance, and Production based on your organization's automation needs.

Refer Export bot files and Import bot files to use the functionality from your Control Room user interface.

Features and benefits

- Role based access control on Bot Lifecycle Management
- Automatic export of dependencies (files and bots)
- Audit and traceability on source and target environment for compliance
- Email notification on successful execution or failure of export and import.

Prerequisites

Export

- The Control Room user whose credentials are used for authentication must have **Export bots** permission
- The Control Room user whose credentials are used for authentication must have **Download** permission on the Bots, minimum **Execute** permission on MetaBot, and dependencies that are being exported.
- If Version Control is enabled in the source Control Room, the production version of all bots and dependencies which you want to export must be set.
- User account that is used to run the Control Room services must have access to the location where package is getting exported, e.g. network location(shared drive) or on Control Room server machine

Import

- The Control Room user whose credentials are used for authentication must have **Import bots** permission
- The Control Room user whose credentials are used for authentication must have **Upload** permission on the Bots and dependencies that are being imported.
- The Control Room user who will use the APIs to import multiple bots must have access to the exported package file provided by Automation Anywhere.

API Endpoints

a. **Export -** <Control Room URL>/v1/alm/export
For example, `https://crdevenv.com:81/v1/alm/export`

b. **Import -** <Control Room URL>/v1/alm/import
For example, `https://crtestenv.com:82/v1/alm/import`

Using the above end points of the BLM Export Import API you can export and import a single bot and all of its dependencies.

Export Bot

Export a single bot with its dependent files using the Export API provided by Automation Anywhere:

1. Use the Post method to generate a token using the end point **http(s)://<hostname:port>/v1/authentication**. For this provide the Control Room instance as **Server Name** /**Hostname** /**IP** and the **Port** number.
For example, `https://crdevenv.com:81/v1/authentication`

2. Use the Post method and state the parameters for credentials in Body Data. Refer sample:
```
{
"username":"cradmin",
```

```
"password":"cr@admin"
}
```

3. Click Play/Start
4. BLM Export API will make use of the authentication token that is obtained using the Authenication API. The authentication token has to be passed on as one of the header inputs to the BLM Export API.
5. Provide parameters such as **filename**, **destination path** and **package name** in Body Data to export a bot. Following list provides parameter description:
   - **filename** - use this to specify the filepath ending with the name of the bot that you want to export
   - **destination path** - use this to specify the destination path where the exported package is to be stored
   - **package name** - use this to specify the package name that you want to assign to the exported package

     Refer sample,
     ```
     {
      "filePath":"Automation Anywhere\\My Tasks\\Finance\\Account Reconciliation.atmx",
      "destinationPath":"tempshare\\datashare\\Finance Department",
      "packageName":"Finance package"
      }
     ```
6. Click Play/Start
7. You can use multiple sources to view the export results in,
   - Reponse Data that comprise **package path** and **checksum**.
   - Audit Log page (landing page as well as details page)
   - Email when you receive notification on success or failure, if configured

Import Bot

Once the bot is successfully exported to a network drive or Control Room machine path, another authorized user can import that package to a different Control Room using the Import API:

1. Use the Post method to generate a token using the end point **http(s)://<hostname:port>/v1/authentication**. Provide the Control Room instance as **Server Name** /**Hostname** /**IP** and the **Port** number.
   For example, **`https://crtestenv.com:82/v1/authentication`**
2. Use the Post method and state the parameters for credentials in Body Data.

   Refer sample:
   ```
   {
   "username":"cradmin2",
   "password":"cr@admin"
   }
   ```
3. Click Play/Start
4. BLM Import API will make use of the authentication token that is obtained using the Authenication API. The authentication token has to be passed on as one of the header inputs to the BLM Import API.
5. Once your credentials are authenticated, provide parameters such as **package path** and the **checksum** that was generated as a token during export in Body Data.

   Refer sample:
   ```
   {
   "packagePath":"tempshare\\datashare\\Finance Department\\Finance Package_20171221-154403.aapkg",
   "checksum":"ZLyQ+Lbu2N+beEuXf6qd2Qi9uwi3BZxApn57C7mYjKQ="
   }
   ```

Tip: You can copy the response of the **BLM Export API** and directly pass that as an input to the **BLM Import API**, if the package path is same and is accessible to the **BLM Import API** user.

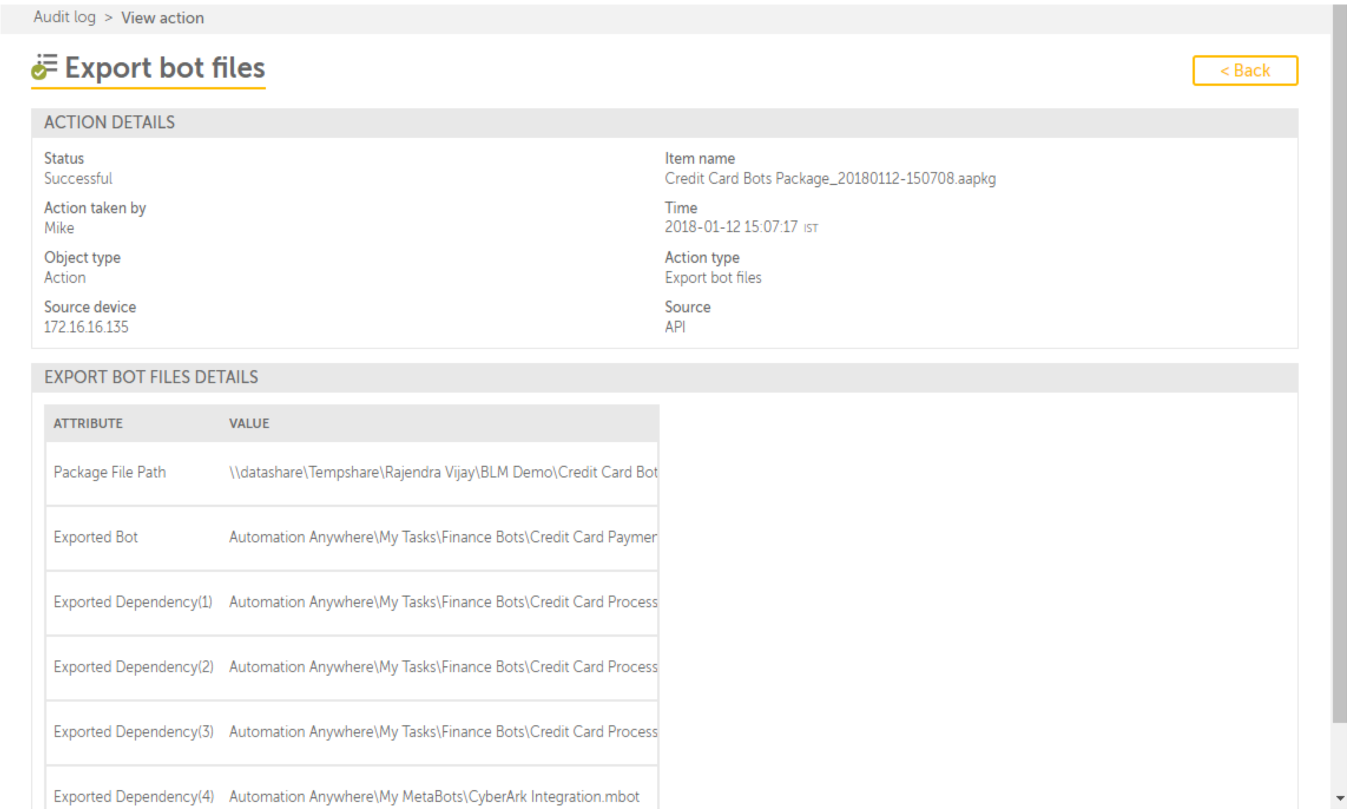
API Response Codes

Http(s) Status code	Response - Description	Corrective Action
200	Package created successfully	NA
400	Bad request parameter	Retry with valid parameters
404	File not found	Ensure that the file/bot is present in Control Room
501	Permission error	Ensure that you have the **Export/Import bots** or **Upoad/Download** permission

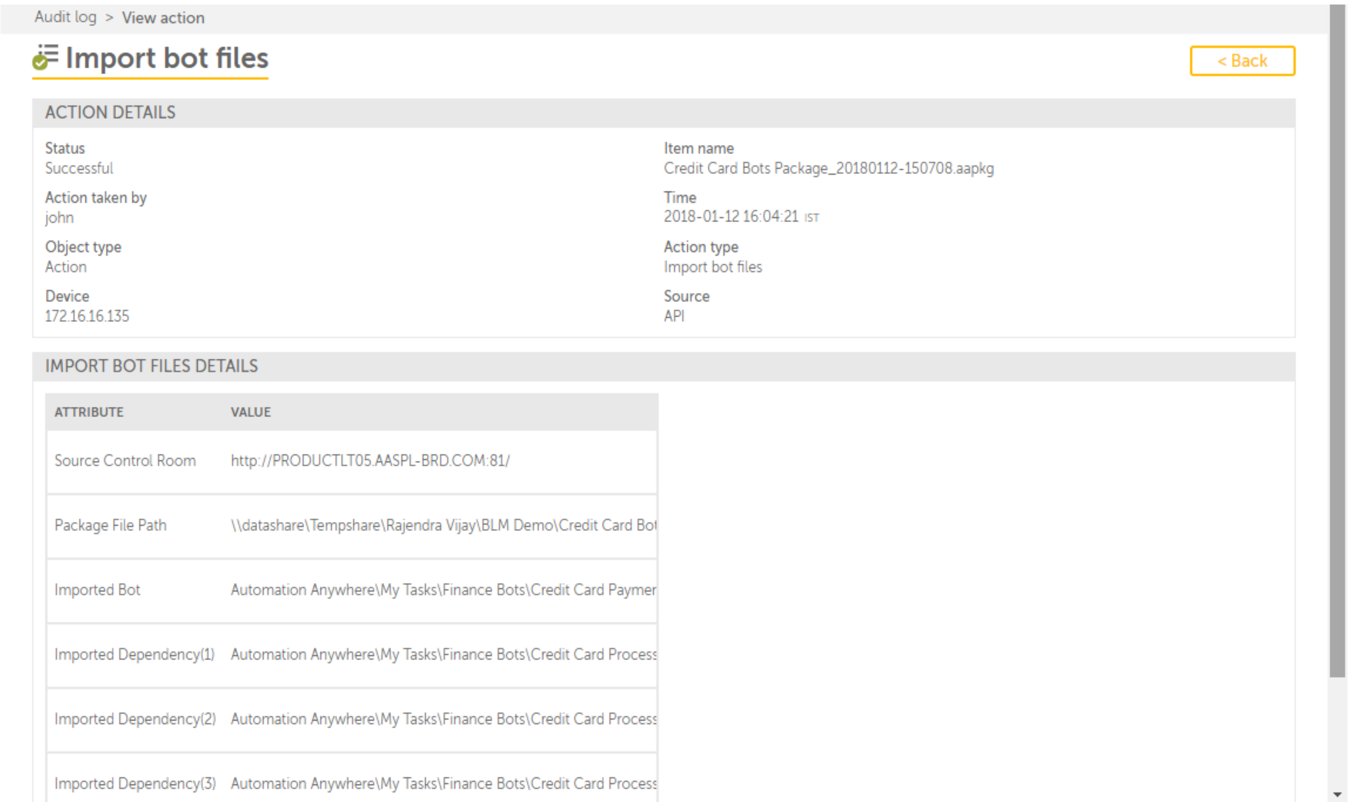
Audit Logs

An audit entry is logged in the Control Room **Audit Log** page when you export or import bots. The illustration below shows the detailed audit entries for Export Bots and Import Bots

Export bots audit details



Import bots audit details



API - export and import workload management configuration

As a Control Room administrator or a user with Export and Import bots permissions, you can export and import Workload configuration to move validated configurations from one environment to another.

For example, you can move the queues that are verified as production ready from staging to production.

You can use the Control Room Export Import REST API to manage your automation in different environments such as Development, Testing, Acceptance, and Production based on your organization's automation needs.

Features and benefits

- Role based access control on Workload Management module
- Audit and traceability on source and target environment for compliance

Prerequisites

Export

- The Control Room user whose credentials are used for authentication must be either ADMIN or should have **Export bots** permission
- The Control Rom user must be either **Queue Admin** or should be **Owner** of the queue to export a particular queue
- Since details of queue Owners, Consumers, Participants are not part of the export, you need to manually add those as required after import.
- User account that is used to run the Control Room services must have read/write access permission to the folder where package is getting exported, i.e. the application path which could be either a network location (shared drive) or local machine.

  For example,
  C:\Users\Public\Documents\Server Files\wlm-files\export
- Maximum 200 queues can be exported in a package
- Queues in draft state cannot be exported
- Entire export operation will fail, if any of the queue export fails.

Import

- The Control Room user whose credentials are used for authentication must have **Import bots** permission
- The Control Room Queue Admin can import **all** queues.
- The Control Room user who will use the APIs to import multiple bots must have **read /write** access permission to the folder where the exported package file shall be provided by Automation Anywhere. i.e. the application path which could be either a network location (shared drive) or local machine.

  For example,
  C:\Users\Public\Documents\Server Files\wlm-files\import
- The user who imports the package becomes the Owner of the imported queue by default. Add **Participants**, **Consumers** or additional **Owners** manually on the imported queues as required.
- If a queue category is already created by any previous import, subsequent imports will just use that queue category as long as all column names and types match.

API Endpoints

a. **Export -** <Control Room URL>/v1/wlm/queues

   For example,
   `https://crdevenv.com:81/v1/wlm/queues`
b. **Import -** <Control Room URL>/v1/wlm/queues

   For example,
   `https://crtestenv.com:82/v1/wlm/queues`

Using the above end points of the WLM Export Import API you can export and import queues.

Export Queues

To export queues using the Export API provided by Automation Anywhere:

1. Use the POST method to generate a token using the end point **http(s)://<hostname:port>/v1/authentication**. For this provide the Control Room instance as **Server Name** /**Hostname** /**IP** and the **Port** number.

   For example, **`https://crdevenv.com:81/v1/authentication`**
2. Use the POST method and state the parameters for credentials in Body Data.
   For example,
   ```
   {
   "username":"Mike.Lee",
   "password":"1234567890"
   }
   ```
3. Click Play/Start/Send
4. The Workload Export API will make use of the authentication token that is obtained using the Authenication API. The authentication token has to be passed on as one of the header inputs to the Workload Export API.
5. Provide Request parameters **X-Authorization**, **Accept** and **queue-ids** as Headers.
   For example,
   ```
   {
    "X-Authorization":"authorization token issued by Control Room after login",
    "Accept":"application/json/file",
    "queue-ids":"1,2,3,4,5"
    }
   ```
6. Click Play/Start/Send
7. The action is successful when the response status is `200 OK`.
8. Copy the package name from the response frame. You can use this to import the queue package.

   > **Tip:** Ensure the import package has the correct extension - **.wlmpkg**

   For example, copy the **filename** given in **content-disposition**:

   ```
   cache-control → no-cache, no-store, max-age=0, must-revalidate
   content-disposition → attachment; filename=WorkloadPackage_20180524_180900.wlmpkg
   content-length → 887
   content-type → application/aapkg
   date → Thu, 24 May 2018 12:39:00 GMT
   expires → 0
   pragma → no-cache
   x-frame-options → SAMEORIGIN
   ```

Import Queues

Once the queue package is successfully exported to a network drive or Control Room machine path, another authorized user can import that package to a different Control Room using the Import API:

1. Use the Post method to generate a token using the end point **http(s)://<hostname:port>/v1/authentication**. Provide the Control Room instance as **Server Name** /**Hostname** /**IP** and the **Port** number.
   For example, **`https://crtestenv.com:82/v1/authentication`**
2. Use the POST method and state the parameters for credentials in the request body.

   Refer sample:
   ```
   {
   "username":"Tom.Watson",
   "password":"1234567890"
   }
   ```
3. Click Play/Start/Send
4. Workload Import API will make use of the authentication token that is obtained using the Authenication API. The authentication token has to be passed on as one of the header inputs to the Workload Import API.

5. Provide Request parameters **X-Authorization**, and **Content-Type** as Headers.

   For example,
   `"X-Authorization":"authorization token issued by Control Room after login",`
   `"Content-Type":"multipart/form-data"`

6. Now provide the parameters **Content-Disposition: form-data; name="upload"; filename="{file name}"** to import the queue package in the request body.

   For example,
   `Content-Disposition: form-data;`
   `name="upload"; filename="{WorkloadPackage_20180524_180900.wlmpkg}"`

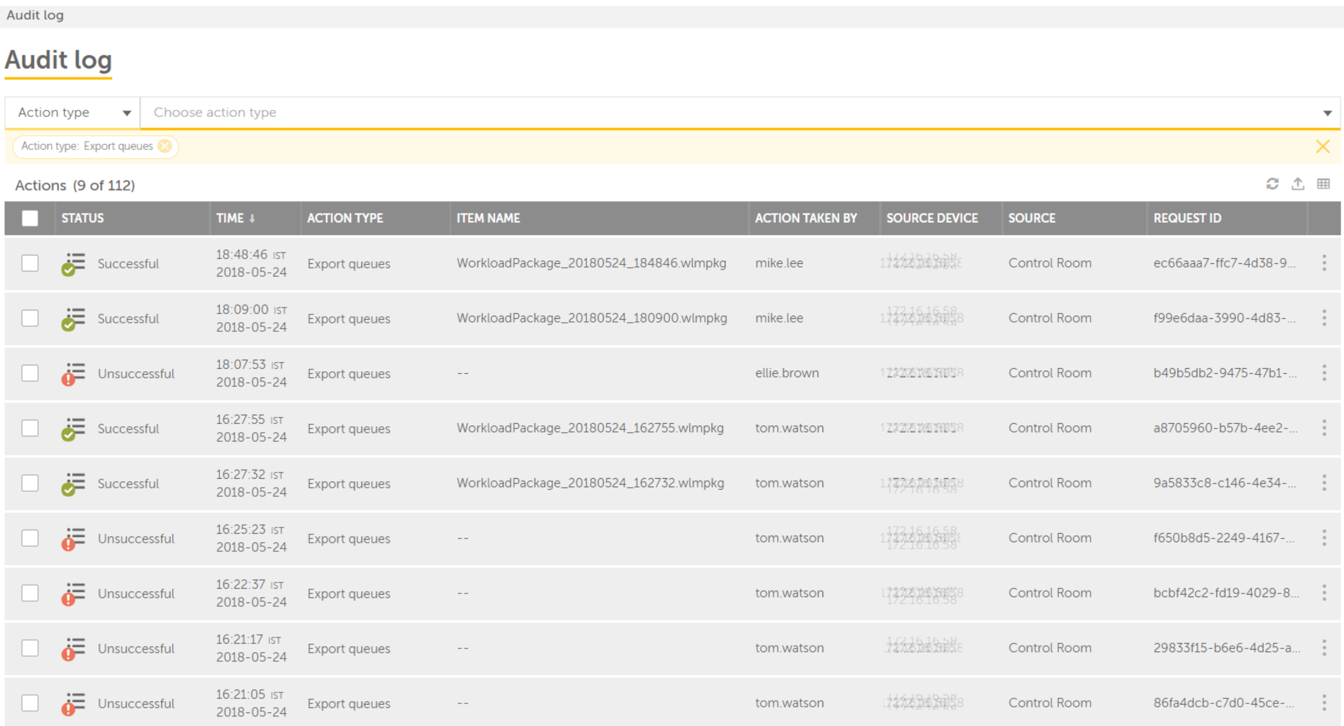
7. Click Play/Start/Send
8. The action is successful when the response status is `200 OK`.

API Response Codes

Http(s) Status code	Response - Description	Corrective Action
200	Package created successfully	NA
400	Bad request parameter	Retry with valid parameters
404	File not found	Ensure that the queue is present in Control Room
501	Permission error	Ensure that you have the required permission

Audit Logs

An audit entry is logged in the Control Room **Audit Log** page when you export or import queues. The illustration below shows the audit entries (successful as well as unsuccessful) for Export queues:



API - get all queues

As a Control Room user with Export and Import Bots and Queue Admin role permissions, you can use the Get all queues API fetch the list of work items of **all queues** and its details available in the Control Room.

Similarly as Control Room **user** with **Export** and **Import Bots** permissions as well as **Queue Owner**, **Participant**, and/or **Consumer** privileges, you can use the Get all queues API to fetch the list of work items **in a given queue** and its details available in the Control Room.

API End Point

Use the following end point to access the API:

<Control Room URL>/v1/wlm/queues

For example,

`https://crdevenv.com:81/v1/wlm/queues`

Get all queues

1. Use the Post method to generate a token using the end point **http(s)://<hostname:port>/v1/authentication**. For this provide the Control Room instance as **Server Name** /**Hostname** /**IP** and the **Port** number.

   For example,
   `https://crdevenv.com:81/v1/authentication`

2. Use the GET method to access the Workload APIs

   For example,
   `GET https://crdevenv.com:81/v1/wlm/queues`
3. Provide the following Request parameters in Headers

   ```
   "X-Authorization" : "Authorization token"
   "Content-Type" : "application/json"
   ```
4. Click **Send**
5. The action is successful when the response status is **`200 OK`**.
6. You can view the result in the Body data.

   For example,


```
[
{
 "id": 1, "createdBy": 2, "createdOn": "2018-05-23T16:53:46+05:30", "updatedBy": 2, "updatedOn":
"2018-05-24T16:26:02+05:30", "tenantId": 1, "version": 2, "name": "Invoice Queue", "description": "",
 "reactivationThreshold": 1, "status": "IN_USE", "expiry": null, "manualProcessingTime": null, "manu-
alProcessingTimeUnit": "SECONDS", "workItemProcessingOrders": [ { "id": 3, "priority": 1, "columnId":
2, "sortDirection": "asc" } ], "displayColumnIds": null, "workItemModelId": 1
},

{
 "id": 2, "createdBy": 2, "createdOn": "2018-05-25T12:28:36+05:30", "updatedBy": 2, "updatedOn":
"2018-05-25T12:28:36+05:30", "tenantId": 1, "version": 0, "name": "Devices for deployment queue",
"description": "", "reactivationThreshold": 1, "status": "NOT_IN_USE", "expiry": null, "manu-
alProcessingTime": null, "manualProcessingTimeUnit": "SECONDS", "workItemProcessingOrders": [ { "id":
4, "priority": 1, "columnId": 6, "sortDirection": "asc" } ], "displayColumnIds": null,
"workItemModelId": 2
 }
]
```

API Response Codes

Http(s) Status code	Response - Description	Corrective Action
200	Queue details listed successfully	NA
400	Bad request parameter	Retry with valid parameters
404	File not found	Ensure that the queue is present in Control Room
501	Permission error	Ensure that you have the required permission

API - add/insert work item data to queue

As a Control Room administrator or a user with **Export** and **Import Bots** and **Queue Admin** role permissions as well as **Queue Owner**, **Participant**, and/or **Consumer** privileges, you can use the REST API provided by Automation Anywhere to add work item data to queues created in the Control Room.

API End Point

Use the following end point to access the API:

<Control Room URL>/v1/wlm/queues/<queue-id>/workitems

For example,

`https://crdevenv.com:81/v1/wlm/queues/1/workitems`

Steps to add work item data to a queue

1. Login to Control Room. Refer Log on to Control Room for more information.
2. Create a queue. Refer Create a queue for more information
3. For the next step, you need to note down the Queue Id from the database that you configured for your Control Room. Refer AAE Control Room Installation Guide for more information.

   For example,
   a. Go to Control Room Database
   b. Right click dbo.QUEUES in the Tables node
   c. Click Select Top 1000 Rows to run the SQL query for Queues.
   d. Identify the queue **id** that is displayed beside the queue **name** column - in this case **1**
4. Use POST method to the insert work item data to queue API to upload work items.

   For example, if the Queue Id is '**1**', use the following parameters,
   https://crdevenv.com:81/v1/wlm/queues/1/workitems
5. Provide the following Request parameters in Headers

   ```
   “X-Authorization” : “Authorization token”
   “Content-Type” : “application/json”
   ```
6. In the Request Body provide required parameters i.e. the work item column names with its data to insert it in a queue. Ensure the parameters for columns in the body data match that of the queue structure.

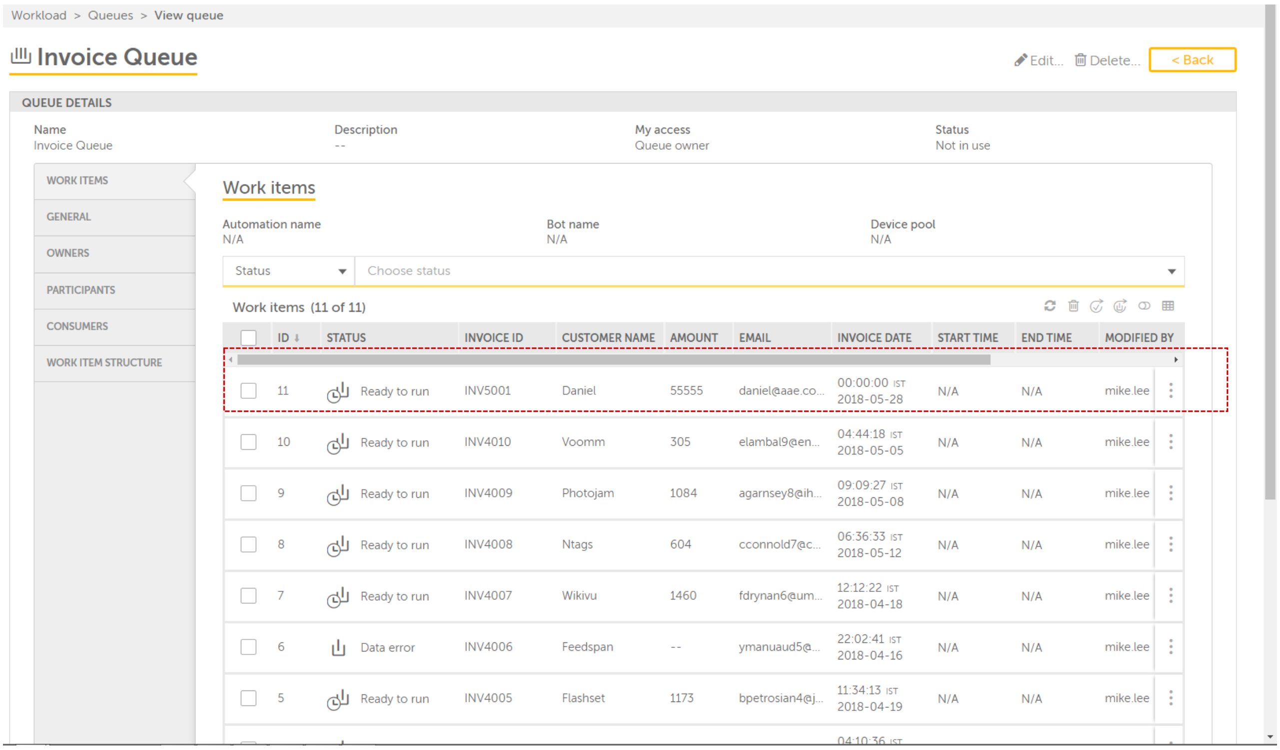
   For example,
   ```
   [{"Invoice Id":"INV5001","Customer Name":"Daniel","Amount":"55555","email":"daniel@aae.com","Invoice Date":"2018-05-28"}]
   ```
7. Click **Send**
8. The action is successful when the response status is `200 OK`.
9. You can view the result in the Body data.

   For example,

   ```
   [
   {
   "id": 11, "createdBy": 2, "createdOn": "2018-05-28T12:29:22+05:30", "updatedBy": 2, "updatedOn": "2018-05-28T12:29:22+05:30", "tenantId": 1, "version": 0, "json": "q+j74omkZEMS0Ta2obN0Pvm-b1se/xK+MDc3k0/V4TOXfm1ICoG2jNEsT/yPlW5Xc64opOqAuozVoSf8Hg/us3HqIOtKRun-IJB4is/rCG9xK7g9LN+e3Cg4DTlgfoxD9UeB0oU+bXKKq1b3p6EI9f07gvvrymM45pIsoktSkM3+U=", "deviceId": null, "status": "NEW", "startTime": null, "endTime": null, "col1": "INV5001", "col2": "Daniel", "col3": "55555", "col4": "daniel@aae.com", "col5": "2018-05-28", "brUserId": null, "queueId": null, "com-ment": null, "botId": null, "poolId": null, "automationId": null, "lastPausedTime": null, "totalPausedTime": 0
   ```

```
    }
]
```

10. Go to Control Room → Workload → Queues → View page to verify that the data is added:



API Response Codes

Http(s) Status code	Response - Description	Corrective Action
200	Work item data inserted successfully	NA
400	Bad request parameter	Retry with valid parameters
404	File not found	Ensure that the queue is present in Control Room
501	Permission error	Ensure that you have the required permission

API - get all work items of a queue

As a Control Room user with Queue Admin role or **Queue Owner**, **Participant**, and/or **Consumer** privileges, you can use the Get all queues API to access all work items of a particular queue.

API End Point

Use the following end point to access the API:

<Control Room URL>/v1/wlm/queues/<queue-id>/workitems

For example,

`https://crdevenv.com:81/v1/wlm/queues/1/workitems`

Get all queues

1. Use the Post method to generate a token using the end point **http(s)://<hostname:port>/v1/authentication**. For this provide the Control Room instance as **Server Name** /**Hostname** /**IP** and the **Port** number.

   For example,
   `https://crdevenv.com:81/v1/authentication`
2. Use the GET method to access the Workload API and the work items within a specific queue

   For example,
   `GET https://crdevenv.com:81/v1/wlm/queues/1/workitems`
3. Provide the following Request parameters in Headers
   ```
   "X-Authorization" : "Authorization Token"
   "Content-Type": "application/json"
   ```
4. Click **Send**
5. The action is successful when the response status is `200 OK`.
6. You can view the result in the Body data.

   For example,

```
[
 { "id": 1, "createdBy": 2, "createdOn": "2018-05-23T16:54:15+05:30", "updatedBy": 2, "updatedOn":
"2018-05-23T16:54:15+05:30", "tenantId": 1, "version": 0, "deviceId": null, "status": "ERROR",
"startTime": null, "endTime": null, "brUserId": null, "queueId": 1, "comment": null, "botId": null,
"poolId": null, "automationId": null, "data": { "Invoice Id": "INV4001", "Customer Name": "Mymm",
"Amount": "", "email": "bfreshwater0@nps.gov", "Invoice Date": "2018-04-17T02:33:32Z" },
"lastPausedTime": null, "totalPausedTime": 0
 },

 { "id": 2, "createdBy": 2, "createdOn": "2018-05-23T16:54:15+05:30", "updatedBy": 2, "updatedOn":
"2018-05-23T16:54:15+05:30", "tenantId": 1, "version": 1, "deviceId": null, "status": "NEW",
"startTime": null, "endTime": null, "brUserId": null, "queueId": 1, "comment": null, "botId": null,
"poolId": null, "automationId": null, "data": { "Invoice Id": "INV4002", "Customer Name": "Vipe",
"Amount": 1025, "email": "ibricksey1@godaddy.com", "Invoice Date": "2018-04-14T08:52:35Z" },
"lastPausedTime": null, "totalPausedTime": 0
 },
{ "id": 3, "createdBy": 2, "createdOn": "2018-05-23T16:54:15+05:30", "updatedBy": 2, "updatedOn":
"2018-05-23T16:54:15+05:30", "tenantId": 1, "version": 1, "deviceId": null, "status": "NEW",
"startTime": null, "endTime": null, "brUserId": null, "queueId": 1, "comment": null, "botId": null,
"poolId": null, "automationId": null, "data": { "Invoice Id": "INV4003", "Customer Name": "Skyndu",
"Amount": 1466, "email": "vwooster2@nymag.com", "Invoice Date": "2018-04-25T14:02:29Z" },
"lastPausedTime": null, "totalPausedTime": 0
 },
....]
```


API Response Codes

Http(s) Status code	Response - Descrip-	Corrective Action

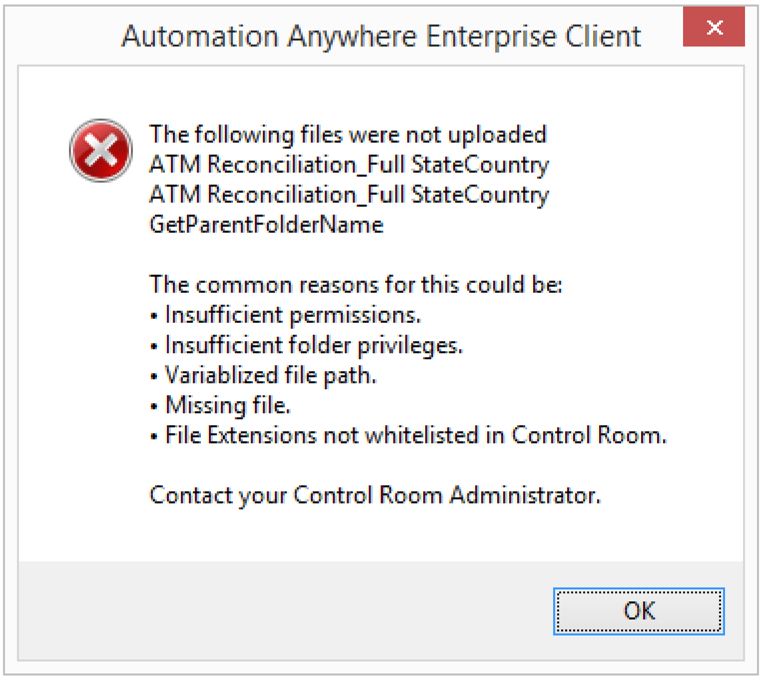
	tion	
200	Work items listed successfully	NA
400	Bad request parameter	Retry with valid parameters
404	File not found	Ensure that the queue is present in Control Room
501	Permission error	Ensure that you have the required permission

Restrict upload of malicious files

As a Control Room Administrator you can add file extensions to the configuration file that restricts the Bot user from uploading files that have extensions other than the ones whitelisted in it. This will help restrict uploading of malicious files to the Control Room repository.

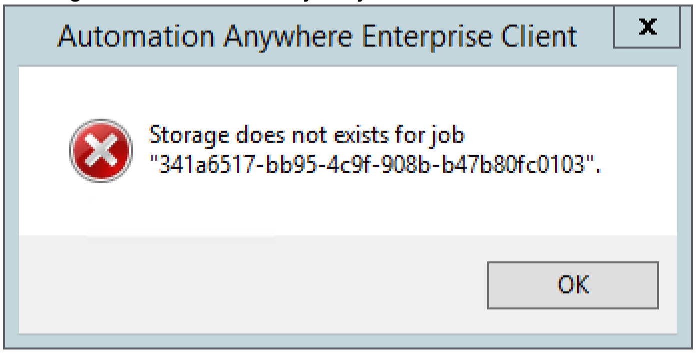
To whitelist files,

1. Open the config folder from Control Room installation path.
   For example, `C:\Program Files\Automation Anywhere\Enterprise\config`
2. Open the **repository.properties** file in edit mode; preferably in **Run as administrator** mode
3. Update **"repository.whitelisted.file.extensions="** to include the files that you wish to white list. Add the extensions separated by a comma (,)
   For example, `repository.whitelisted.file.extensions=atmx,mbot,csv`
   a. To allow files with all extensions, use asterisk (*)
   b. DO NOT add space between the extension names
   c. If using load balancer, update the config file in all nodes
4. Using **POST** method execute the Authentication API. Refer article on Authentication API for details.
   - The token passed through this API has to be used for the next step.
5. Using the **PUT** method execute the API **http(s)://{{hostname}}:{{port}}/v1/repository/fileExtensions/update**
   For example, `https://ultron.com:81/v1/repository/fileExtensions/update`
6. On successful implementation, when a Bot user attempts to upload files that are not part of the whitelist from the AAE Client, the following message is shown in AAE Client,



Troubleshooting Control Room

1. When I try to upload an automation file from AAE Client in a distributed environment, the following error message is displayed. “Storage does not exists for job <job number>”



This is due to one of the following reasons.

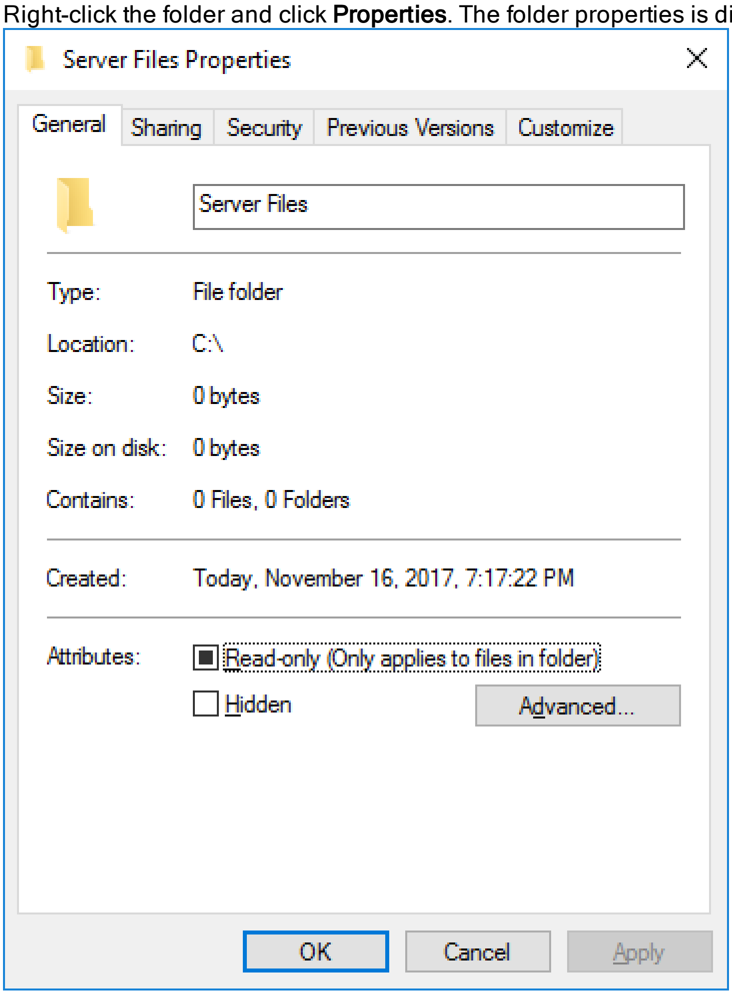
- The Control Room installation wizard did not create the folder where automation files will be uploaded
- The folder where automation files are to be uploaded does not have the required shared permission

To troubleshoot this, perform the following steps.

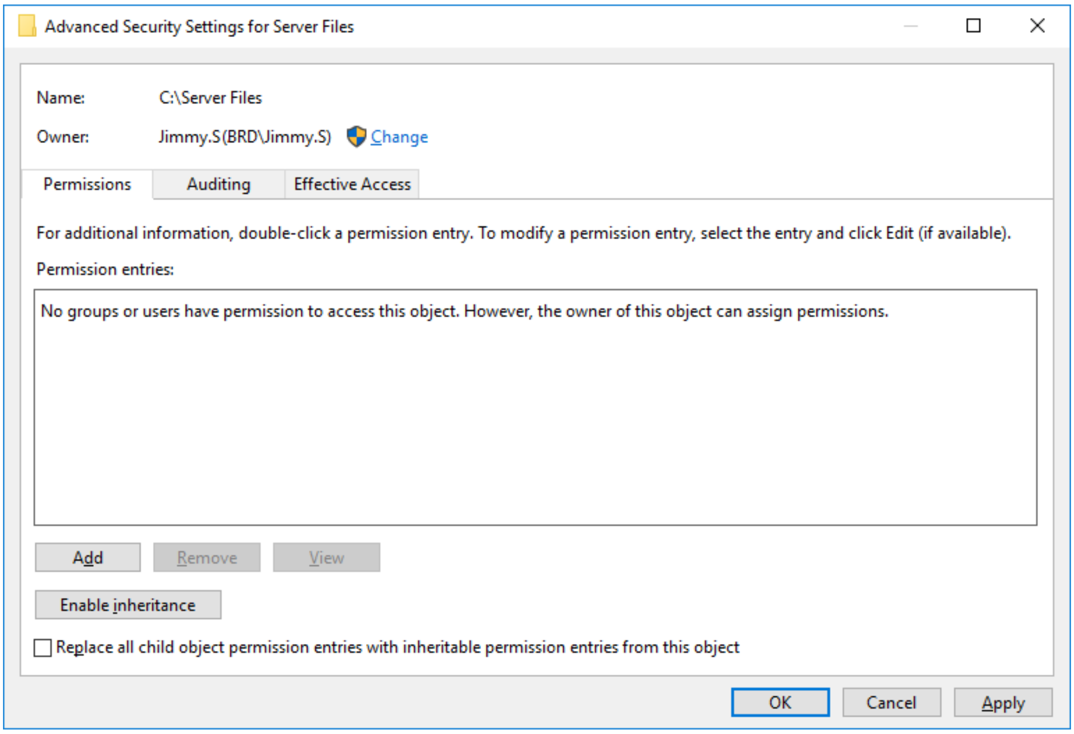
A. Ensure that the folder where automation files are to uploaded has been created.

B. If the folder has been created, ensure that the folder has the **Enable inheritance** and **shared** permissions. To do this perform the following steps.

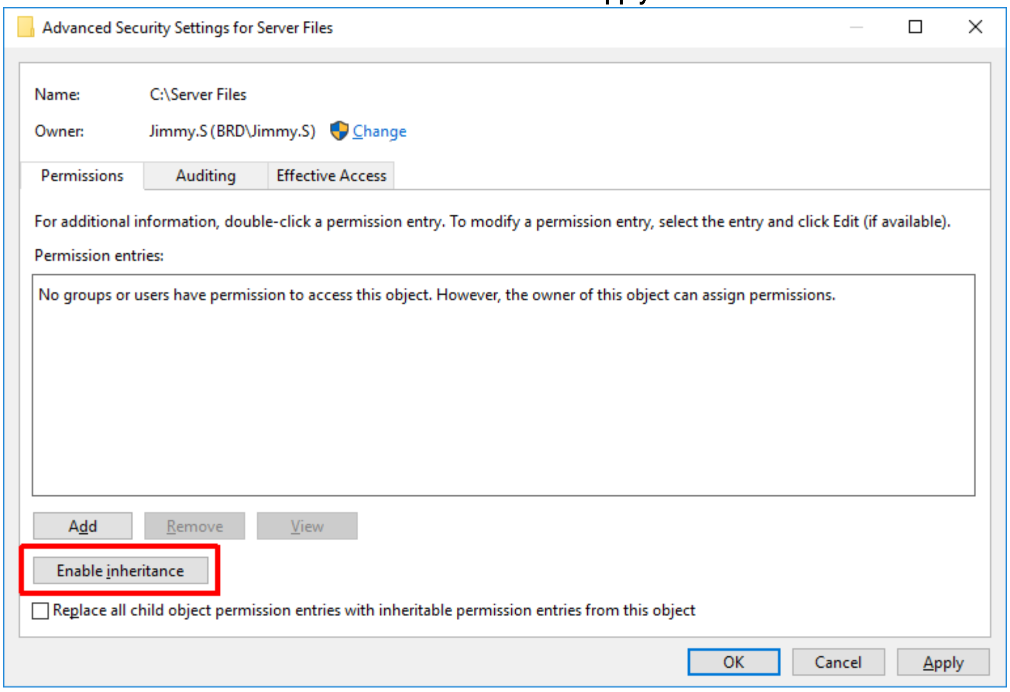
  i. Right-click the folder and click **Properties**. The folder properties is displayed.



  ii. Click the **Security** tab and then click the **Advanced** button. The **Advanced Security Setting** dialog box is displayed.



iii. Click the **Enable Inheritance** button and then click the **Apply** button.



Appendix - Guidelines for General Data Protection Regulation

The General Data Protection Regulation (GDPR) is one of the strictest compliance frameworks with respect to maintaining privacy of personal data. The GDPR defines personal data as any data that can be used to identify a natural person. That natural person is defined as the Data Subject. Business entities that define and determine the purpose and means of the processing of personal data (business process) are defined as Data Controllers. Business entities that perform the processing of personal data are defined as Data Processors. Data controllers and processors must be ready to demonstrate that their data processing activities and security processes adhere to the GDPR if the personal data they process refers to any Data Subject that is a citizen of any European Union (EU) member country or territory, even when that processing is performed outside of the EU. The purpose of the GDPR is to make sure that the rights of Data Subjects with respect to their personal information are maintained. These rights are concerned with privacy, processing for legitimate business purposes only, the right to control, access, and remove their personal information from the Data Processors systems.

Automation Anywhere customers, which utilize Automation Anywhere Enterprise (AAE) are typically Data Controllers and/or Data Processors in the context of GDPR. As software that is purchased, deployed and managed by the customer, compliance with GDPR depends upon the policies and procedures of the deploying customer entity. GDPR compels the deploying entity to implement appropriate technical and organizational measures to assure data is processed for stated purposes and that data is protected by design and by default. The guidelines in described below must be followed to assure that AAE is being utilized in a way that is compliant with the GDPR.

Data Protection

Automation anywhere has a full set of security features that either automatically provide or are configurable by design to provide data protection. As with any enterprise application the consistent and proper utilization of security controls depends upon the organization. Several aspects of security within a customer environment are outside the scope of AAE, for example the security posture of the operating system upon which AAE is deployed, or the network security of the environment.

AAE utilizes encryption technologies for data at rest, data in motion, and data in memory. Encryption technologies are documented in the AAE Security Architecture Guides (for versions 10 and 11).

All users accessing AAE may be authenticated utilizing standard centralized authentication methods such as Active Directory. Additionally credential access by AAE may be done either with the built-in bank grade secure Credential Vault or with external credential storage systems such as CyberArk.

Authorization of AAE users is outside the scope of AAE software, the deploying entity must assure that only authorized personnel with a business need can access AAE. Corporate users with access to AAE can be granted fine grained permissions via roles within the product supporting role based access controls (RBAC). The permissions and roles support sophisticated RBAC models assuring dual-controls and separation of duties within the operations of AAE. Permissions can be implemented on all aspects of AAE operation including: credentials, bots, bot runners, bot creators, bot schedules, audit log access, workload management queues, and pools. Because AAE allows for the automation of any type of business process, it is the responsibility of the deploying entity to assure that only those personnel that are permitted to access applications involved with any automation are authorized to do so. Within this consideration, AAE provides all permissions necessary to separate different bots, bot runners, and operating personnel along any line of business or processing, assuring separate processing domains within the product.

All user actions are audited within AAE providing records of all access and actions taken by operations personnel. AAE audit logging supports all major compliance frameworks.

AAE supports a redundant and load balanced architecture that scales with business needs assuring availability of processing resources. AAE support state synchronization across geographically distinct deployments supporting disaster recovery and resiliency in processing.

Bots are software programs developed by customer business experts, and as with any enterprise application development, state of the art requires Secure Software Development Life Cycle (SDLC) processes be implemented. AAE supports separation of Development, Testing, and Production environments through a combination of separate deployments and RBAC as described above. See Security Architecture documents for more details (for versions 10 and 11).

Pseudonymization

GDPR specifically calls out pseudonymization as an appropriate technical measure to protect data. An in-depth discussion of pseudonymization is outside the scope of AAE. Pseudonymization transforms data to artificial identifiers. This gives the Controller and Processor a way to process data such that it is no longer possible to use the data to identify a natural person. Tokenization is another approach that transforms data such that it can be referenced later but in terms of the tokenized data such that it cannot be used to identify a natural person. Automation Anywhere recommends adherence with GDPR Article 25 in the use of pseudonymization and tokenization, in all cases where personal information is being processed by bot. The use of pseudonymization for personal data removes any risk involved with data remanence within the AAE platform.

Data Remanence In Control Room

There are instances where data is retained within the databases which support the AAE Control Room. Specifically when using Workload Management, Bot Insight, and IQ Bot. In all cases regarding data remanence in Control Room, pseudonymization and tokenization reduce Controller and Processor entity effort to comply with GDPR. Also, when enabling logs for debugging information such as username (users of the platform) will be retained in the logs.

Workload Management and Queues

When utilizing workload management to deploy multiple bots to the same automation, the work items that are placed into the queues are stored in the database. Through the Control Room UI any work item may be queried, reviewed, and deleted. When processing personal data in work items, queues should be periodically deleted.

Bot Insight

When using Bot Insight, any field that is tagged for analytics inside the automation task built in the AAE developer tool will be logged and stored in the Analytics database. In version 11 Bot Insight, all variables are automatically tagged for capturing data and therefore would be stored in the database. For version 11 Bot Insight, this default action of tagging all data variables should be unchecked for fields that contain personal data.

IQ Bot

IQ Bot stores images uploaded by users or RPA tasks and extracts structured data from those images. These images and the extracted data are temporarily stored in the database while IQ Bot is running or when it is halted with an exception. After all exceptions in an IQ Bot run are either validated or invalidated, the data is removed from the database. Training images for IQ Bot are stored in the database and should not contain personal data that can identify a natural person. For IQ Bot version 5.2.1 or earlier the system will automatically move production images to the training environment. The training environment should be reviewed periodically to identify production images and remove them. In version 5.3, scheduled for release in June 2018, there will be a feature to disable this automatic movement of production images to the training environment.

User Credentials

User credentials in AAE versions 10 and 11 can be added and deleted by any administrator with the appropriate privileges, set by a role. The Control Room supports the querying, reviewing, and deleting of any credential at any time.

AAE Databases and Data Removal

If processing has been done and pseudonymization has not been applied, it may be necessary to remove data from AAE databases. AAE uses a standard SQL database either co-resident on the Control Room server or a corporate database server or cluster identified during installation and configuration of the Control Room. Consult your database admins to find, report, extract data from the AAE database. A Bot is available from the Automation Anywhere Bot Store that can be used and adapted for this purpose.