AUTOMATION ANYWHERE ENTERPRISE

Control Room - User Guide

Product Version	10.5.10
Document Version	1.0
Date of Publication	7/23/2018
Update(s) to Document Edition	• Day Light Saving and TIme Zone Selection in Schedules • Configuring Client Configuration Settings to Prevent or Allow Login

Copyright © 2018 Automation Anywhere, Inc.

Table of Contents

Introduction to Control Room **5**
Benefits of using the Control Room 5
Control Room Features 5
Viewing Task Relevant Activities in Dashboard **7**
Benefits 7
The Dashboard 7
Dashboard Decoded 7
Manage Roles and Permissions **9**
User Roles in Control Room 9
Create Customized Roles and Assign Permissions 9
Manage User 11
Copy Roles 11
Manage the User 11
Permissions Matrix 12
User Management in Control Room **13**
Creating an User 13
Setting User Password 16
Updating User Details 16
Exporting User Details to CSV File 17
Managing the Repository **18**
Running and Scheduling Tasks 20
Viewing Task Dependencies 20
Unlocking Files when Version Control is enabled 21
Running Tasks in Control Room **23**
Scheduling Tasks in the Control Room **25**
Creating Schedules 27
Viewing Upcoming Task Schedules 30
Editing a Schedule 30
Deleting a Schedule 32
Exporting Schedule Details to CSV 32
Day Light Saving and Time Zone Selection in Schedules 32
Viewing and Managing Task Dependencies **34**
Managing File Dependencies 35
Adding Dependencies 35

Copyright © 2018 Automation Anywhere, Inc.

Removing Password Dependencies 37
Assigning BotRunners To Run/Scheduling Role 38
Assigning BotRunners 38
Scheduling Tasks in Control Room (Version Control Enabled) 40
Production Version 43
Managing the Operation Room 45
Viewing Tasks in Progress 45
Tracking an 'Unknown' Task Status 46
Viewing Task History 46
Operational Analytics Dashboard 47
Monitoring the Audit Trail 48
Adding Filters 48
Managing Clients 50
Viewing and Updating Client Information 50
Exporting Client Details to CSV 51
Defining Credential Keys in Credential Manager 52
Benefits of Defining Credentials 52
Defining the Credential Keys and Attributes 52
Control Room Settings 56
Configuring Control Room Components 57
Configuring Version Control 60
Configuring Outgoing Mail Server 61
Enabling or Disabling Email Notifications 62
Customizing email notifications 64
Configuring the Credential Vault 65
Client Configuration 65
Configuring Client Configurations Settings 70
Version Control Integration 71
Version Control Pre-requisites 71
Enabling 'Version Control' 71
Uploading the Base Version 72
Disabling Version Control 73
Allocation and Management of Licenses 75
Installing a New License before Expiry 76
Viewing License Usage 76
Monitoring App Usage Status 77

Installing a Downgraded License 77
License Allocation 79
Enabling or Disabling Auto Login 81
Purchasing and Installing Control Room License 82
RDP Based Approach To Bot Deployment - Guidelines 83
Overview 83
Prerequisites for RDP Based Bot Deployment 84
Changing screen resolution for Bot Runner session on Control Room 86
FAQs 86
Control Room Authentication API 89
Testing Authentication API using Jmeter 90
Bot Deployment API 92
Overview 92
Control Room APIs 92
Key Features and Business Benefits of Control Room APIs 93
Authentication API 93
Deployment API 94
API Audit Trail in Control Room 95
Testing APIs with JMeter 96
Sample Code 99
APITest Java Class 99
APIClient Java Class 99
RestHelper Java Class 102
Sample Bot CSV (Applicable to above Java Scripts) 103
VB Script to Deploy APIs 103
Contents of Input Files (Applicable to the above VB Script) 104
Control Room API to Get a List of Registered Clients 105
Get Client API Response Codes 105
Sample for getting list of registered clients using Jmeter 106

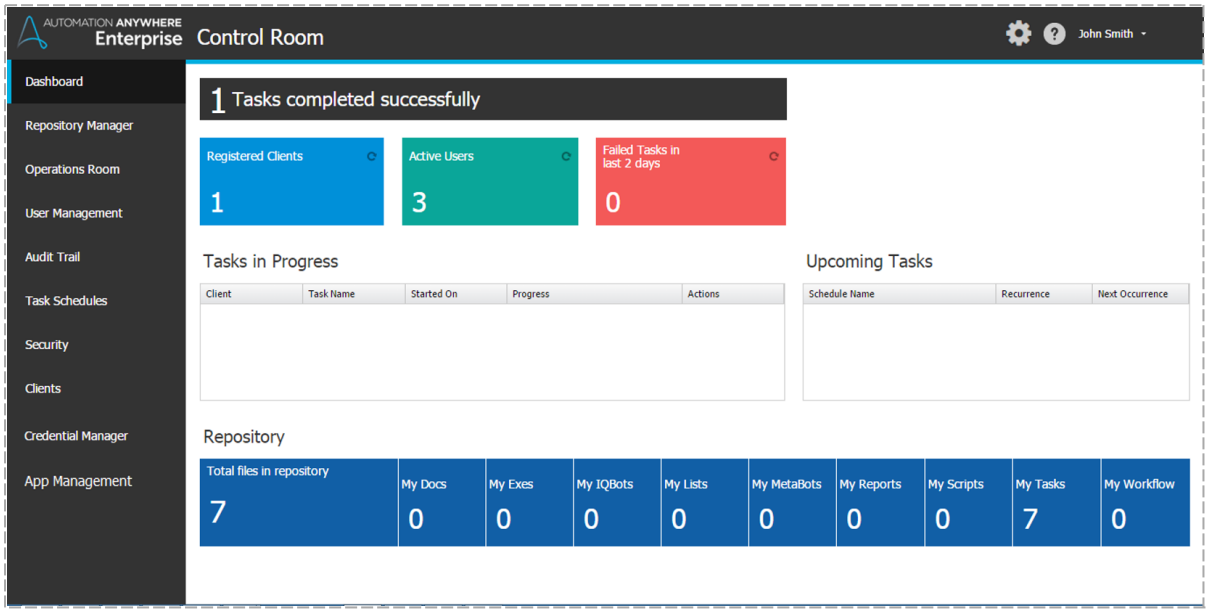
Section 1: Control Room - Access

Introduction to Control Room

Automation Anywhere's web-based Control Room allows you to access the Control Room from anywhere, anytime.

It has the capability to process growing number of Users and Clients.

A role based accessibility model ensures each User views information or data that is relevant to the role assigned to the User by the Control Room Administrator.



Benefits of using the Control Room

- Simplified and improved monitoring and administration of large multi-site complex automation infrastructure using the web based control room.
- Accessing and managing tasks and Clients/Users from anywhere anytime.
- Monitoring task progress and status to enforce internal compliance regulations, as well as to 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.

Control Room Features

- **Dashboard -** View task relevant activities. Learn More
- **Repository Manager -** Manage automation files repository. Schedule, Deploy and/or Run tasks. Learn More
- **Operation Room -** View the control room history and tasks in progress. Learn More
- **User Management -** Configure users (Clients and Administrators), maintain rights/permissions and delete. (Define Roles). Learn More
- **Audit Trail -** Displays recent activities of Users and Administrators. Learn More
- **Task Schedules -** View schedule details. Learn More
- **Security -** Manage Roles - create new and manage existing. Learn More
- **Clients -** Manage Clients - add and update.Learn More

- **Credential Manager -** securely manage i.e.create/update and store sensitive information in the form of Credentials to be used for automation tasks. Learn More

Viewing Task Relevant Activities in Dashboard

A Control Room 'Dashboard' provides a bird's eye view of task relevant activities to the Control Room Administrator.

Note that it is available for management to Admin - the Control Room Administrator only.

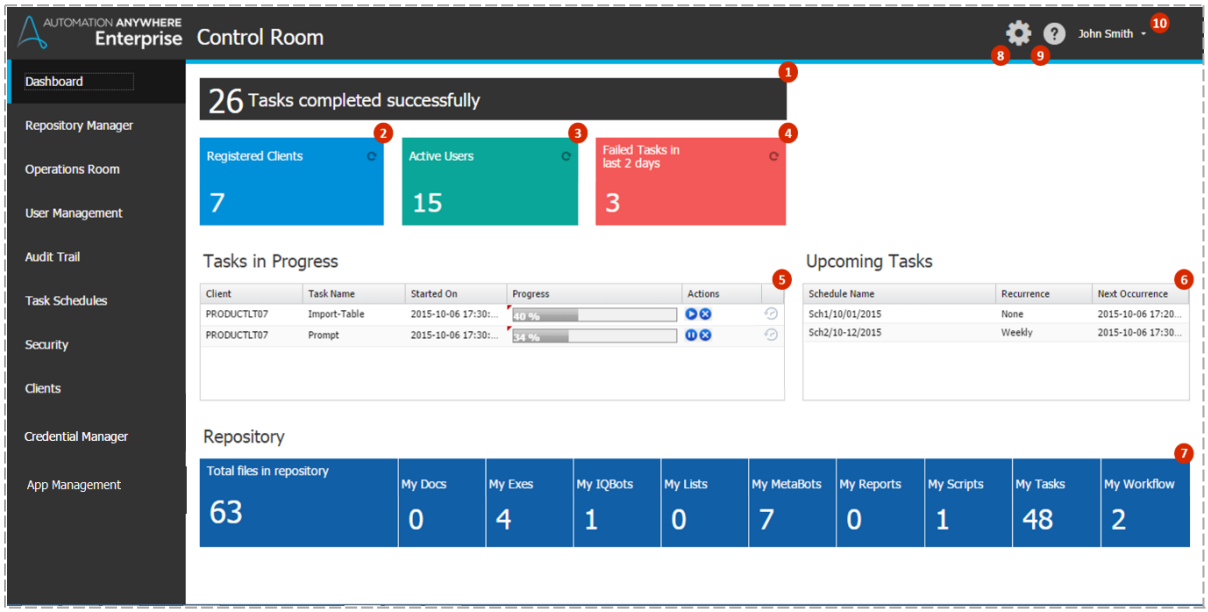
Benefits

- **Accessible -** Access Control Room Anywhere Anytime.
- **Scalable -** Multiple Admin support.
- **Role based management -** Create and manage users and clients based on roles defined.

The Dashboard

You can view task relevant activities such as tasks completed successfully, upcoming tasks, tasks in progress, repository details and tasks that have failed on the Control Room Dashboard.

It also provides details about Clients that are registered to the Control Room and Users (Client and non-Client) who are active.



Tip: To access other Control Room features, navigate to each tab in the left panel.

Dashboard Decoded

A user with access to Dashboard can view the summary of:

1. Number of 'Tasks completed successfully'.
2. Number of Client users that have registered to the Control Room
3. Number of Active Users; includes Client and non-Client users.
4. Number of Failed Tasks in last 2 days.
5. Tasks in Progress with details -Client Connection Status Icon, Client Name, IP Address, the name of the task, started on, the command, progress status and current action in progress.
6. Upcoming Tasks with details - name of the schedule, whether it is to run once, daily, weekly or monthly and the next occurrence if applicable.
7. Number of files in the Repository with demarcation for the file type - doc, exe, IQBots, list, MetaBots, report, script, task and workflow.
8. To access Control Room Settings and License Management console, click on the 'Settings' icon.

9. To access the 'Support' site, click on the link provided beside the user name.
10. If the Control Room is configured for Normal Users (Non-Active Directory Users):
    - Users can 'Logout' of the Control Room by clicking on the drop down arrow near the Username.
    - The session will expire if they are inactive for a certain time period and will have to re-login.

Next…

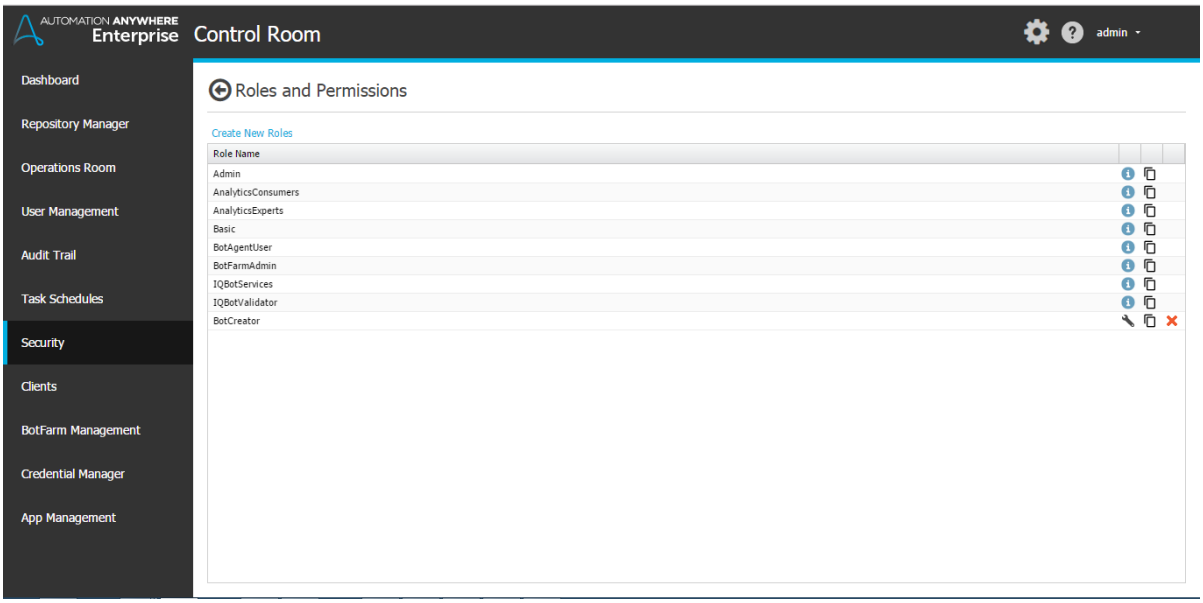
You can now start using the Control Room by defining user roles and permissions. Learn More

Manage Roles and Permissions

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 console-access, to view information or data that is relevant to the role assigned by the Control Room Administrator.

User Roles and relevant privileges are assigned from the Security console.

Tip: It is recommended an administrator create and assign User Roles and Permissions upon creation of the Control Room 'Admin' who has all administrative privileges.



User Roles in Control Room

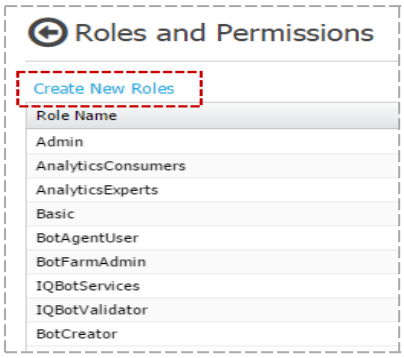
Note: 'Admin' Role is defined by default on creation of administrator while configuring the Control Room. Other roles - AnalyticsConsumer, AnalyticsExperts, Basic, and Validator preexist in the Control Room.

Role	Description
Admin	This role in Control Room is for the Control Room Admin by default. This Admin can, however, create other Admin users.
AnalyticsConsumer	This role is assigned to Business users who would need to consume/analyse the data via dashboard created by AutomationExperts.
AnalyticsExperts	This role is assigned to Automation Experts. These users have the ability to create, save as, publish dashboards.
Basic	This role is for Users that have been imported from earlier versions (8.x.x and 9.x.x) of Control Room to the web-based Control Room, using the migration utility. Such users have access rights to the 'My Tasks' folder only.
Validator	This role is for Client users that are allotted the IQBot license. This role has 'IQBot > Validator' permission only and are not allowed folder access rights.
IQBotServices	This role is available from version 10.5.0.
IQBotValidator	This role is available from version 10.5.0.

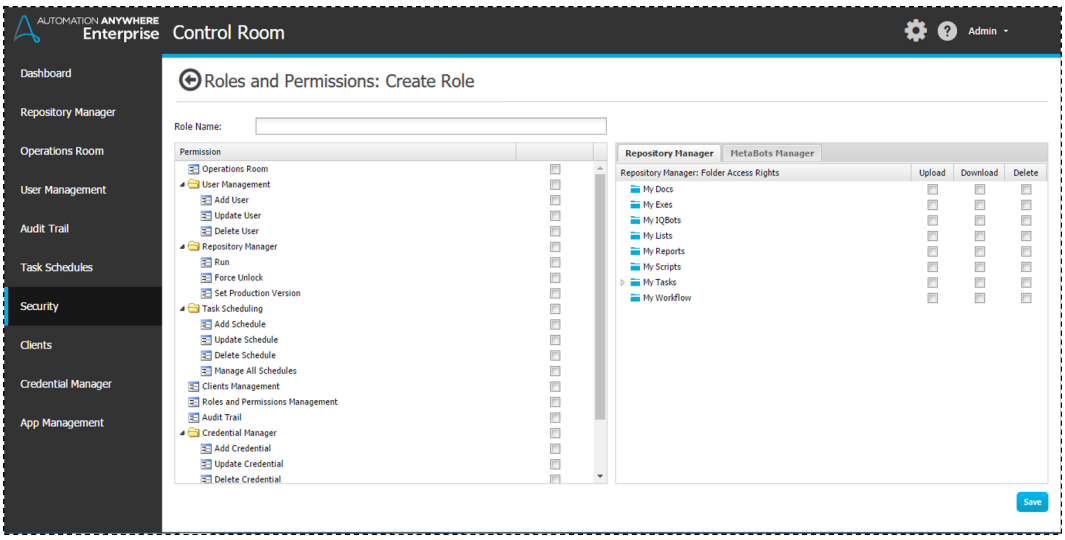
There are certain roles in the Control Room that define a Client type. The BotCreator role can be defined for Client users with development or task creation privileges and BotRunner role can be defined for Client users with task run time privileges.

Create Customized Roles and Assign Permissions

To define a new customized user 'Role', click on 'Create New Roles'.



In the 'Create Role' page input the required information:



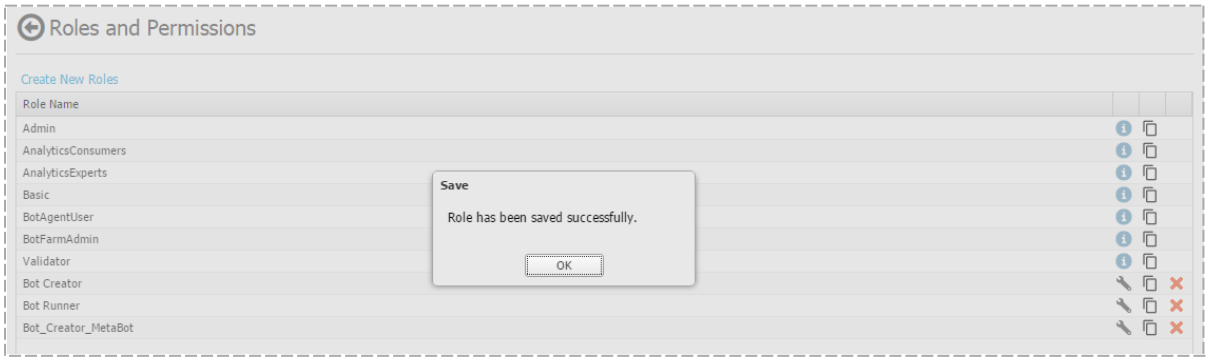
You can choose to assign permissions based on user roles in your organization.

- For instance you can permit the new User to manage a repository only; in which case you can select the Repository Manager folder.

You can then assign the User access rights that could include any or all - Upload, Download and Delete permissions for different folders.

- For instance, you can assign a User 'Upload' and 'Download' permission to the 'My Tasks' folder only.

'Save' the new role.



Verify whether the User has been created in the 'Roles and Permissions' list. The User Roles are listed in the chronology that they are added and updated.

Note: Control Room users with task run and scheduling permissions can run and/or schedule tasks only on those BotRunners that are assigned to their role. Learn More

Manage User

You can reassign or revoke permissions to the user.

- To view permissions and access rights available to an admin user on clicking the information icon. Similarly, you can also view permission and access rights for the 'Basic' role.

  Note: Though in edit mode, you will not be able to update the permissions and access rights of Admin & Basic roles.

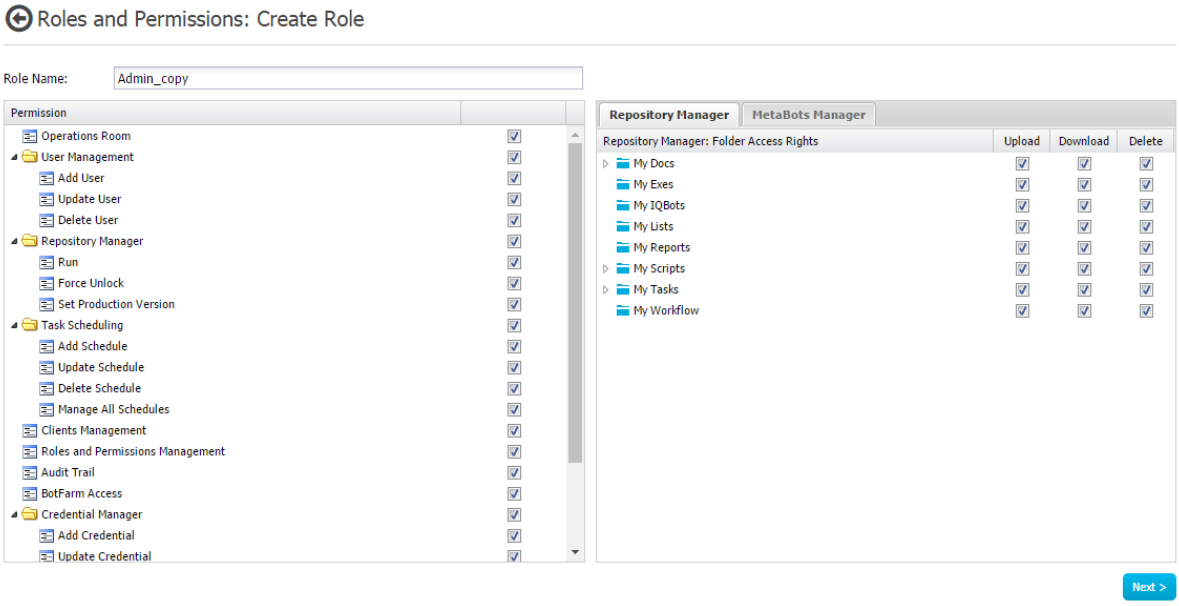
- To edit the User roles and permissions, click on and to delete.

- To return to the Dashboard, click on .

Copy Roles

When you have a number of Roles that have similar permissions, it is easier to make a copy of an existing role and update permissions if required.

To copy a role, simply click . This launches the 'Create Roles' page wherein the role is created with 'copy' appended to the **Role Name** and all the permissions that were selected already pre-filled. (see image).



Here, you can choose to select or clear the permissions and folder access check-boxes. You can also amend the **Role Name**.

Manage the User

You can reassign or revoke permissions to the user.

- To view permissions and access rights available to an admin user on clicking the information icon. Similarly, you can also view permission and access rights for the 'Basic' role.

  Note: Though in edit mode, you will not be able to update the permissions and access rights of 'Admin' and 'Basic' roles.

- To edit the User roles and permissions, click on and to delete.
- To return to the Dashboard, click on .

Permissions Matrix

The permissions matrix published here will enable you to create a combination of roles and permissions that suit your organizational requirements.

Permission	Description
User Management	User can add, update and/or delete Control Room users.
Repository Manager	User can run, force unlock and/or set production versions of tasks available in the Control Room repository.
Task Scheduling	User can add, update, delete and manage all tasks for scheduling to BotRunner machines.
Credential Management	User can view the Clients that are registered to the Control Room and export Client details to a CSV file, if required.
Roles and Permissions Management	User is granted privileges to manage roles and permissions to other Control Room users.
Audit Trail	User can review all Control Room relevant activities.
Credential Manager	User can create, edit, and delete credentials in the Control Room
License Management	User can allocate/deallocate licenses to Client users.

Next…

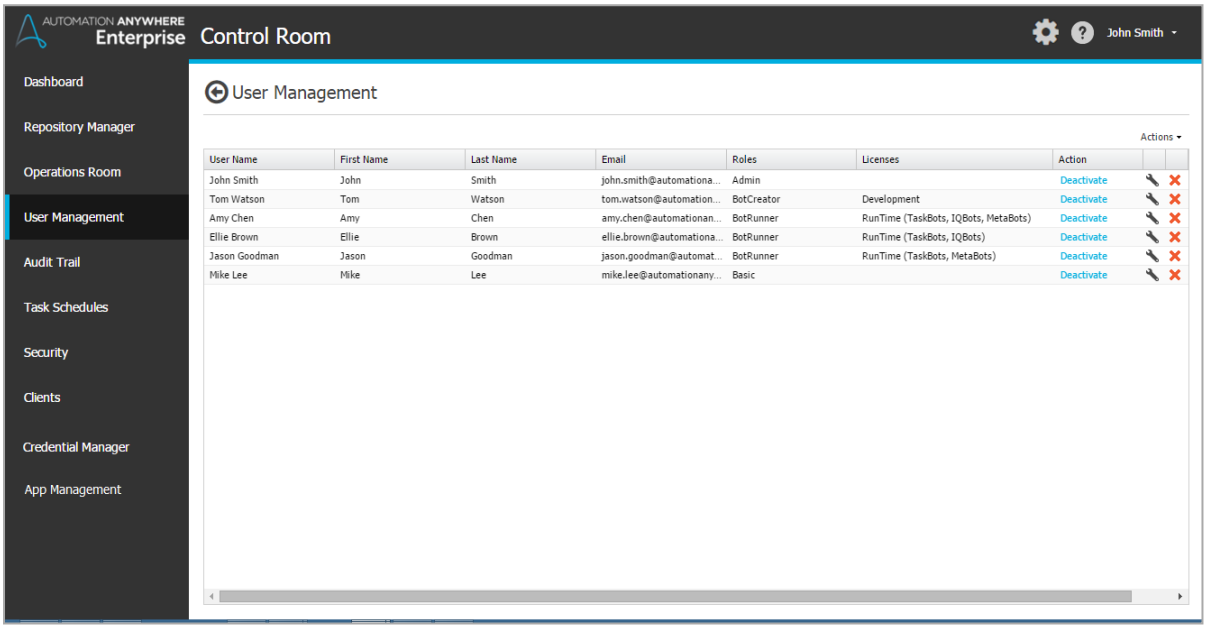
You can now start creating Control Room Users based upon the roles and permissions assigned. Learn More

User Management in Control Room

Client User management involves creating users after defining specific roles as soon as the Control Room is hosted. These users can be either Non-Active Directory Users or Active Directory Users, as configured during installation.

Tip: Active Directory users are authenticated with their Active Directory credentials and Non-Active Directory Users are authenticated with credentials that are stored in the Control Room database.

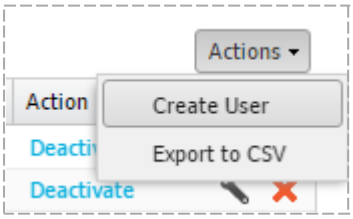
Ideally, an 'Admin' and if required 'Administrators' can create Users/Clients. These are then assigned roles depending upon access privileges.



Creating an User

Users in Control Room are created depending upon the type of user configured during installation. Hence, you can create either Non-Active Directory Users or Active Directory Users - users with Windows credentials.

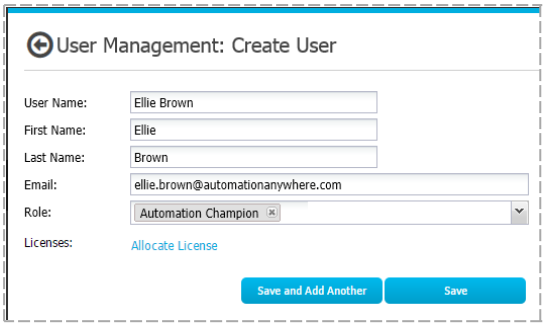
1. To start creating an user, click on Create User under 'Actions'



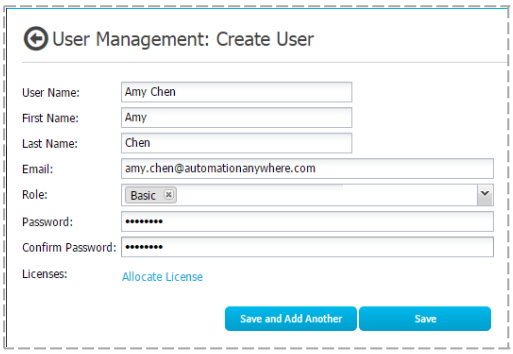
2. Input the required information:

Tip: Firstname and Lastname are optional. If you do opt to have Firstname and Lastname, you are allowed to included Numbers, Spaces ( ), Period (.), Hyphen (-), and Underscore (_).

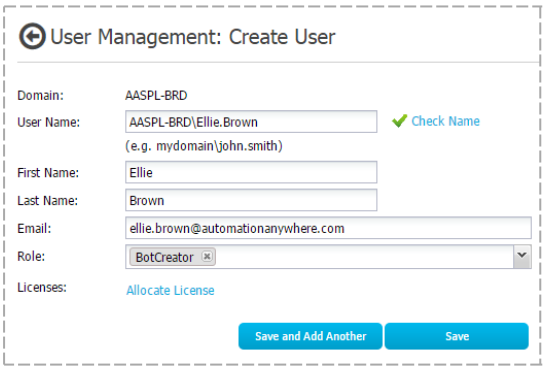
- For a Non-Active Directory User, you will have to provide information in each field:



- In addition, provide the password if you have opted not to configure the Outgoing Mail Server settings:

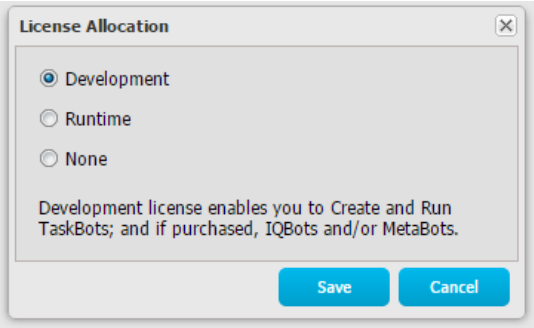


- The information for an User with Windows credentials gets auto-populated when you input the User Name and click 'Check Name':

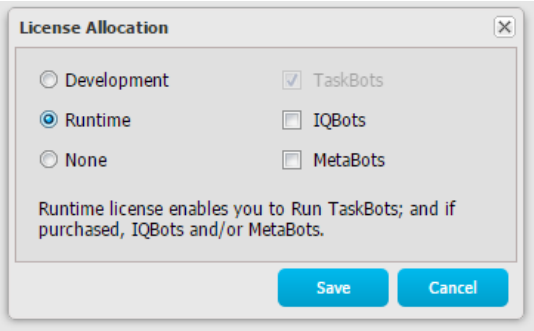


> Note: If the Control Room is configured for a multi-domain environment, the 'Domain' is auto-populated with the domain name that you append for the user.

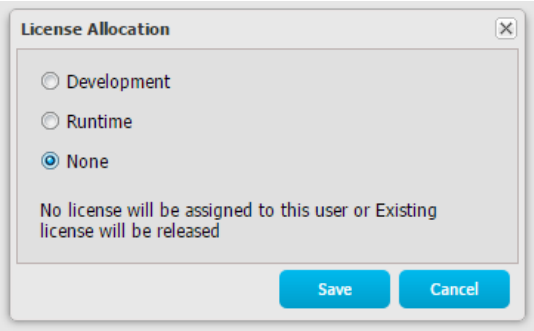
3. An email is sent wherein the user will use the link to:
   - Verify the email id and set the Control Room access password, if the Control Room is configured for 'Non-Active Directory' users.
   - Verify the email id, if the Control Room is configured for 'Active Directory' users.
4. Now allocate licenses based on the role by clicking ‘Allocate License’ link.
   - For instance, a BotCreator role can be allotted a ‘Development’ license:



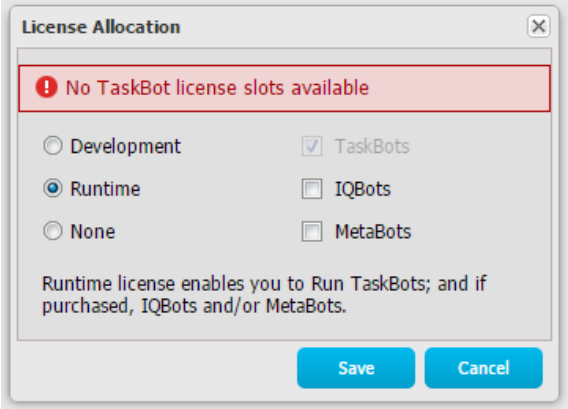
- While a BotRunner role can be allotted a Runtime license:



- Or a Control Room user would not require any Client license:



Note: If no slots are available for license usage, you are displayed:



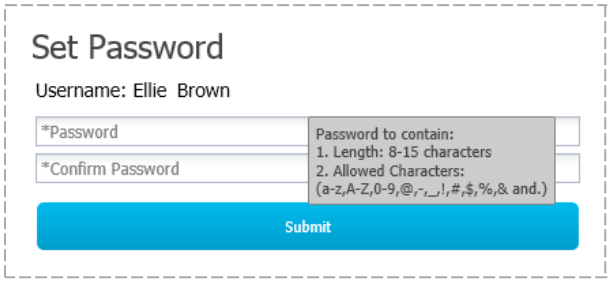
7. Click to 'Save'.

Tip: You can choose to switch a user type i.e. from Development to Runtime or vice versa as per organization's automation requirements by updating the license type from 'License Management'.

Setting User Password

Applicable to Non-Active Directory Users with SMTP Configuration enabled

A Non-Active Directory User clicks the link in the email that she/he receives and sets the password as required:



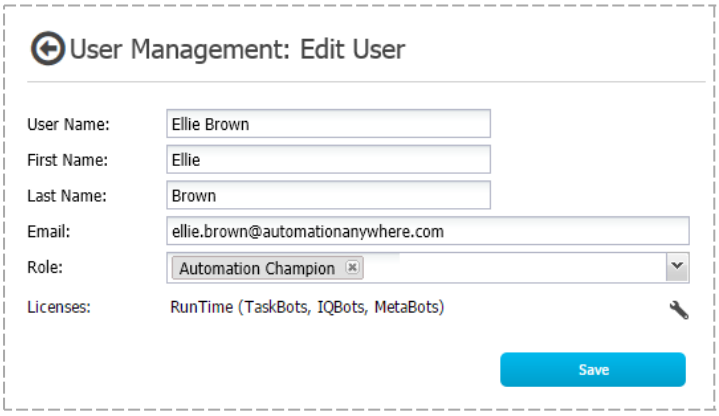
The User can login to the Control Room using these credentials. She/he will be able to view consoles that are relevant to the role assigned.

> Note: An Active Directory user will be able to login directly using Windows credentials after verifying the link sent in an email.

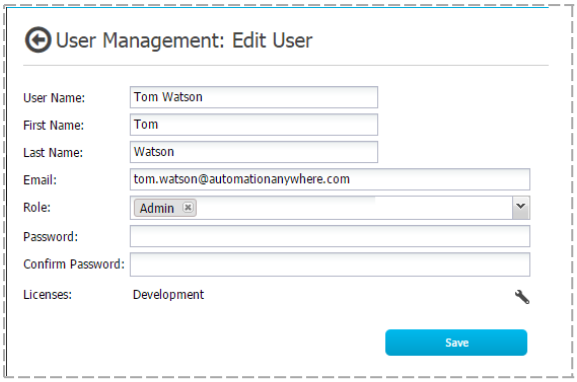
Updating User Details

The Control Room administrator can update user details. User details such as alias names, email and roles can be modified; users can be activated, deactivated or even deleted if necessary.

1. To update user details, click .
2. Update required information and save.



> Note: You can set a password for a User who has forgotten the same when you opt not to configure the Outgoing Mail Server settings. The User can then reset the same during Control Room login.



3. You can also choose to reallocate license to switch users; for instance from Development to Runtime by clicking on 🔧. Refer section on 'License Allocation' for more information.

- To activate a user, click Activate; to deactivate click Deactivate.

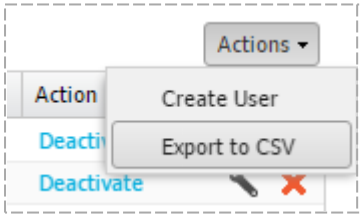
> Note: To enable a Client User to Register to the Control Room, it is important to 'Activate' the user. Use the 'Deactivate' option only if the Client user needs to be made inactive temporarily.

- To delete the user, click ✖.

Exporting User Details to CSV File

The user details can be exported to a CSV file for data sharing by the Control Room administrator or a User with User Creation permission.

To export user details, click on Actions > Export to CSV:



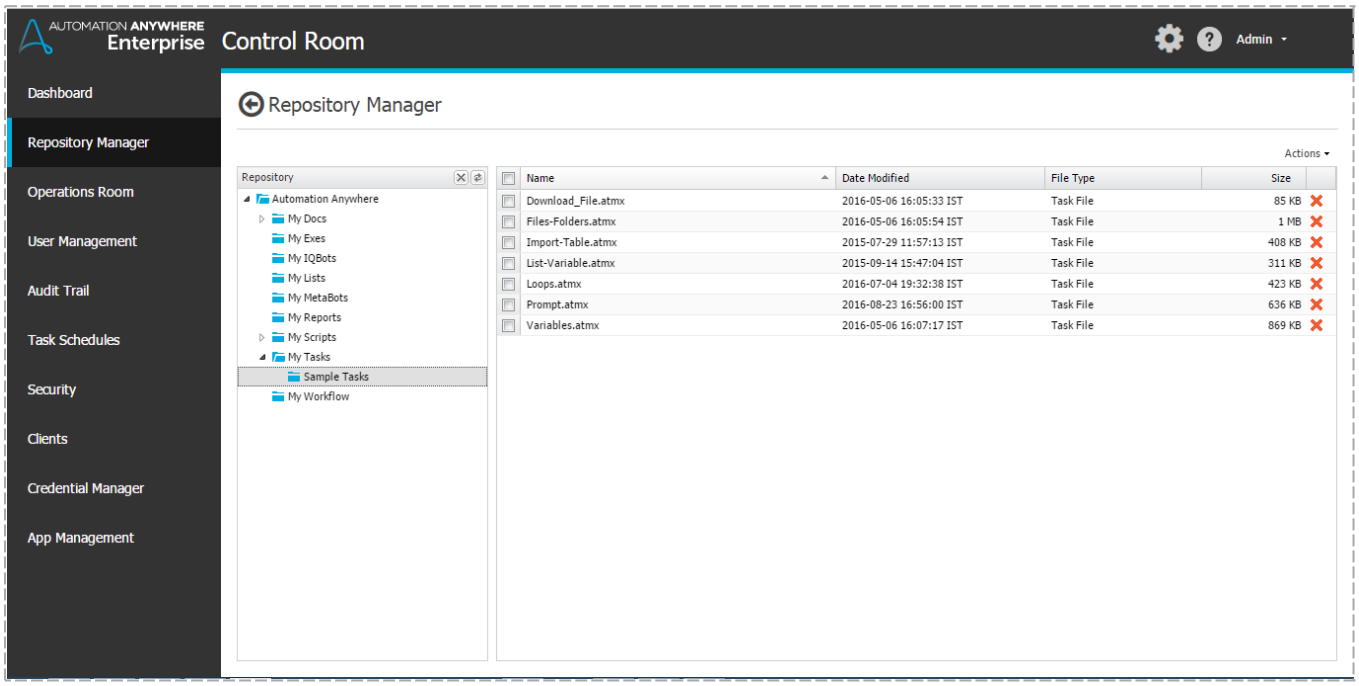
Next...

You can run and schedule tasks from the Repository Manager if you have been assigned the privilege. Learn More

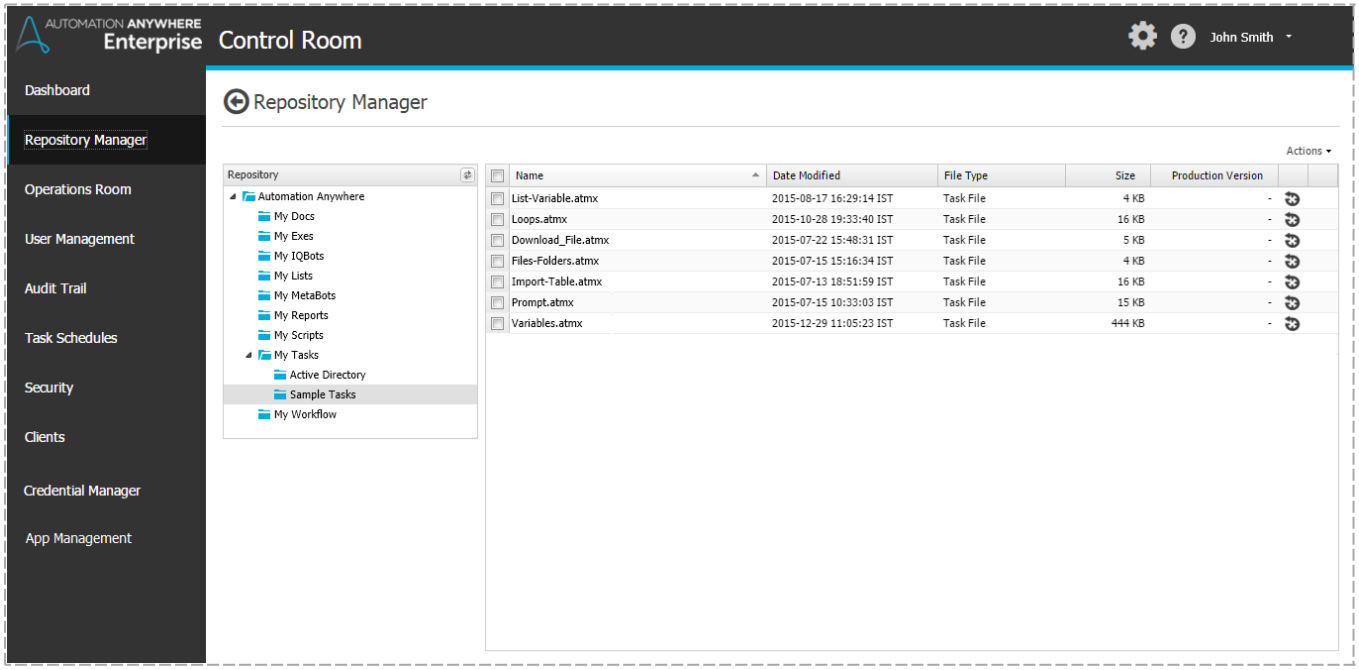
Managing the Repository

One of the most important benefits of using the Enterprise Control Room is the ability to closely manage automated tasks that are uploaded to the server. The number of tasks uploaded over time can grow to be quite large. Organizing and managing these tasks is of great importance to the organization.

Hence, the most powerful capability that the Repository Manager provides is the ability to run and schedule tasks on 'Runtime' i.e. client users with 'TaskBot' privileges. It also offers the capability to delete uploaded files to the Control Room administrator.



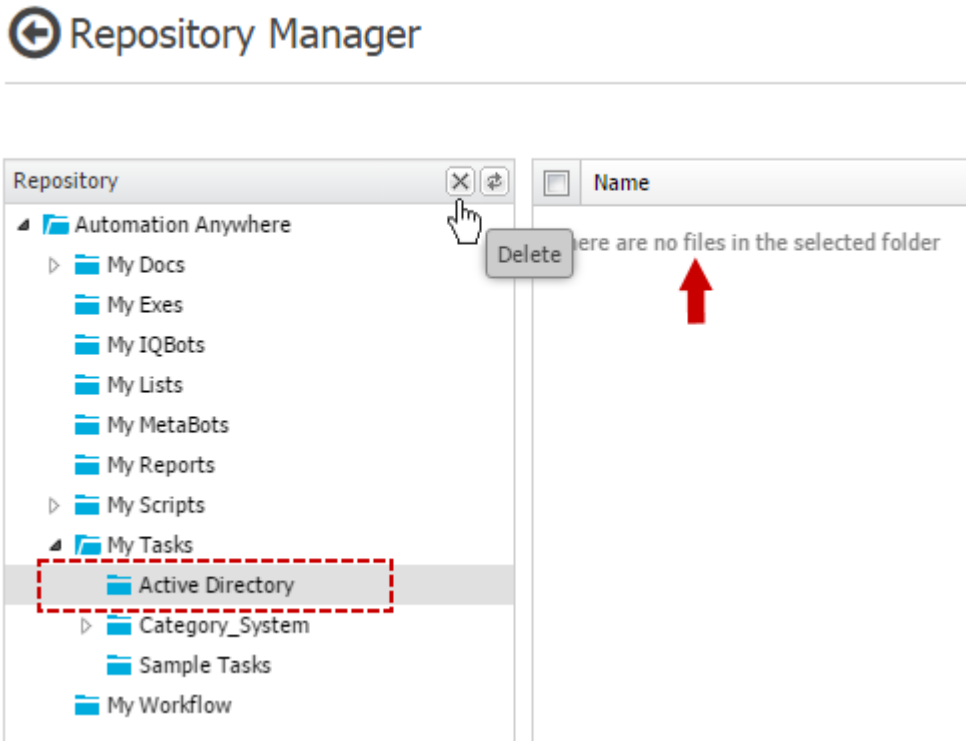
When Version Control is enabled, the default screen of Repository Manager is seen as below:



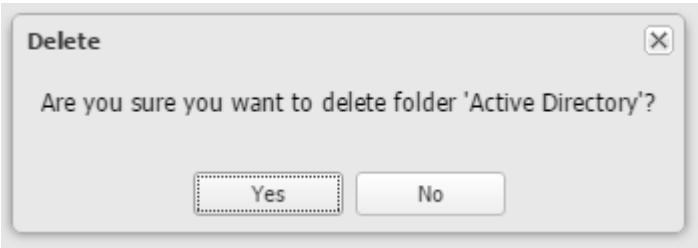
Note: Available to users with appropriate privileges.

Additionally, the Repository Manager allows only the Control Room administrator to delete redundant files and sub-folders.

- **Deleting a File -** To delete a file, go to the required folder and mark the TaskBot(s), MetaBot(s), and IQBot(s) that you want to delete. Click on ✖.
- **Deleting a Folder -** To delete a folder, select the folder and click on delete icon (beside the Refresh icon) in the Repository title panel as shown:

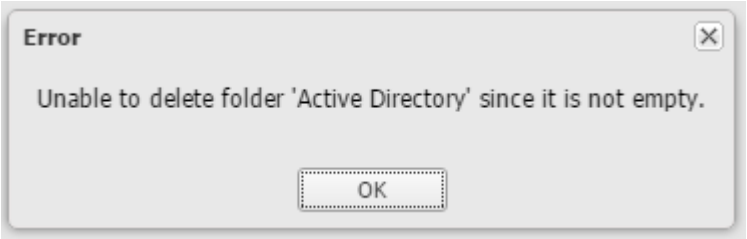


Confirm whether to delete folder:



- When deleting a folder, *remember:*

  1. The folder to be deleted *must* be empty; it should not comprise any files and/or sub-folders. If you try to delete such folders, you are given an error:

  2. Only user created folders and/or sub-folders are allowed to be deleted.

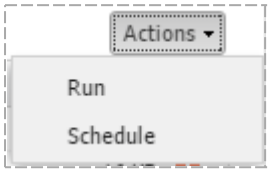
     The *default folders* of Automation Anywhere such as My Docs, My Exes, My IQBots, My Lists, My MetaBots, My Reports, My Scripts, My Tasks, and My Workflows *cannot be deleted*.

Note: When Version Control is enabled, a Control Room admin can also delete files and folders.

Running and Scheduling Tasks

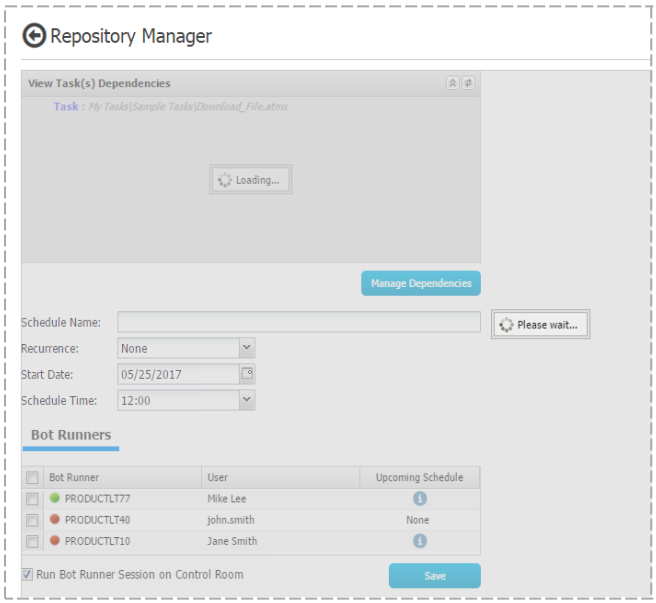
The Control Room admin can run and schedule tasks on selected Client users.

To perform any of the two actions, simply click on Actions button on the top left.



- **Run -** Use this option to deploy and run the task on any of the Client(s) machine. Learn More.
- **Schedule** - Use this option to schedule a task to run on any of the Client(s) machine. Learn More.

Note: Control Room searches for task dependencies as soon as you perform any of the above operations.



Learn More.

To return to the previous page, click .

Viewing Task Dependencies

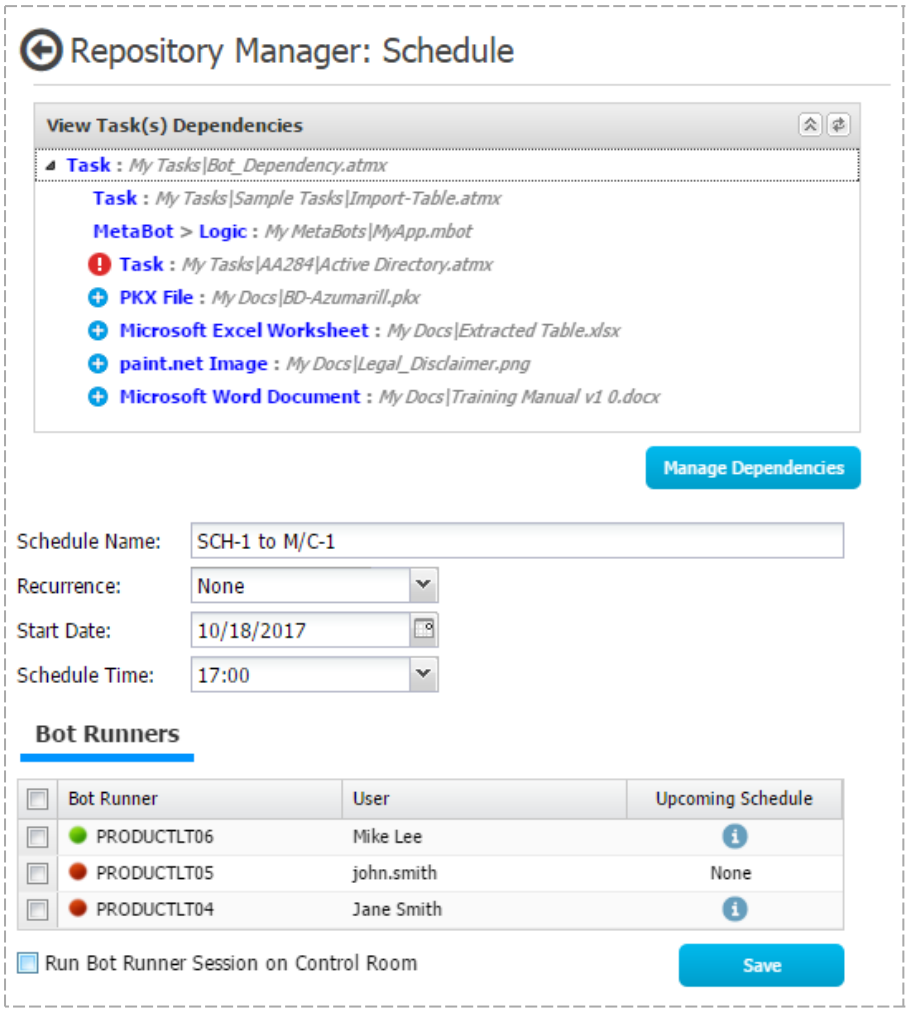
As processes become complex, there's a need to manage multiple tasks. This can be achieved by either queuing one task after another or playing a task that includes sub-tasks.

If a task includes sub tasks and files, it is termed to have 'Dependencies'. In Control Room for such tasks to play successfully, a user needs to upload the sub-tasks and files as well.

Similarly, if a task is password protected, you will be required to input the password during deployment. This is also termed as a 'Dependency'.

While deploying a task, the Control Room scans for the task dependencies and displays those in the 'View Task(s) Dependencies' window:

Note: View Task(s) Dependencies only displays dependency of IQBot, MetaBot, sub task or a task called using Run Task command, and files such as documents, certificate, exe & script.



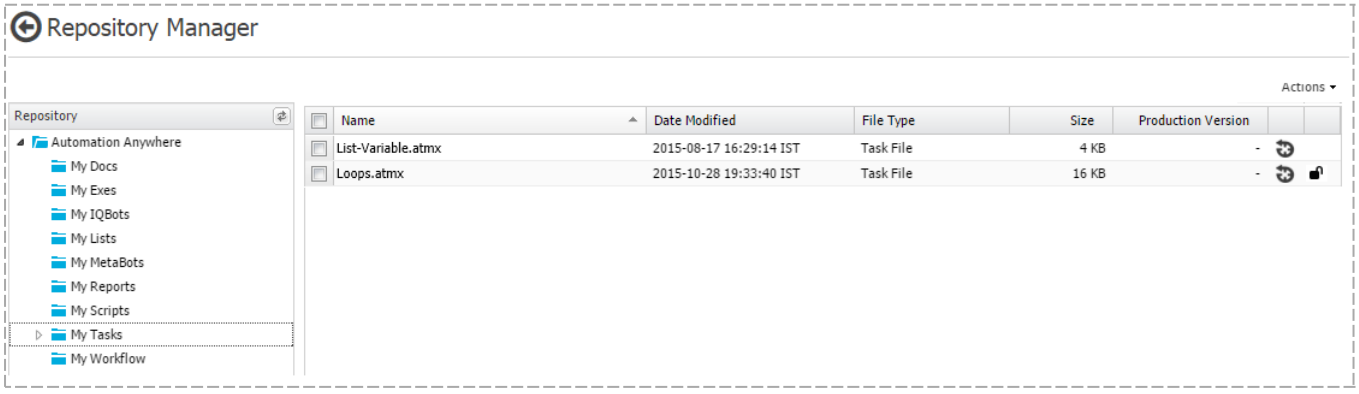
Learn More

Unlocking Files when Version Control is enabled

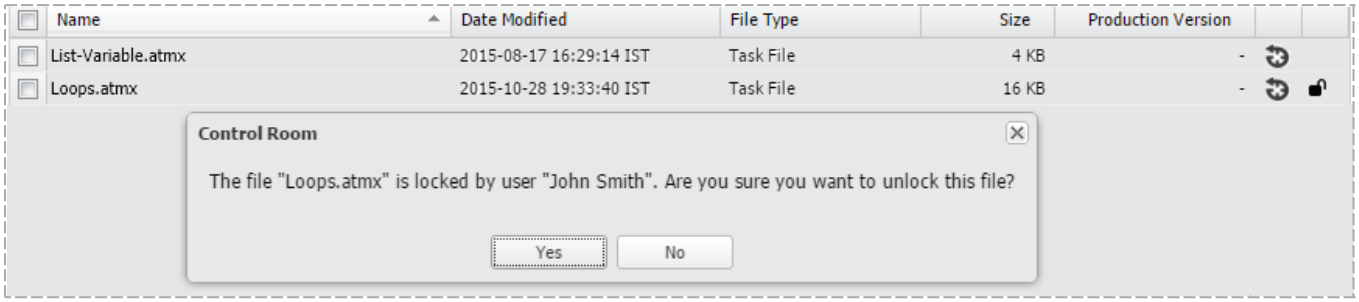
If your Control Room is enabled for 'Version Control', as an administrator you have the privilege of unlocking files that have been checked out by a Client, for editing by other users. You cannot, however, delete the files.

For instance, Client A checks out a file for editing. Meanwhile Client B also wants to edit the file. However, since it is in 'Check Out' state for Client A, Client B will have to either wait for the client to check in the updates or request the Control Room Admin to unlock the file. In the latter case, the client sends the file-name (including the path) to be unlocked.

The locked files are indicated by 🔓 as shown:



To 'Force Unlock' a file, click on . Choose to unlock the file in:



On clicking 'Yes' the file is unlocked for editing by other users.

Next…

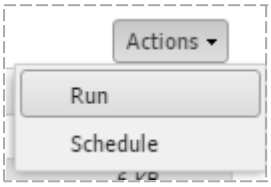
You can view all schedules in the Task Schedule console. Learn More

Running Tasks in Control Room

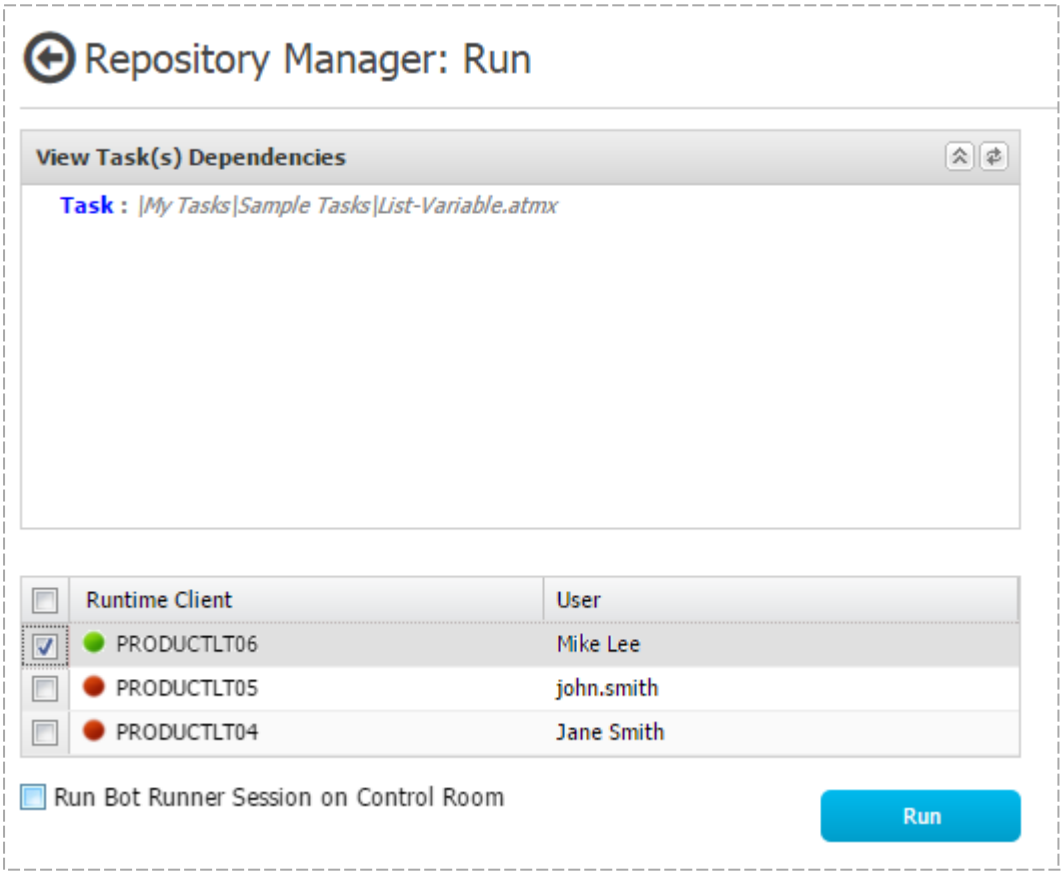
In Control Room, users with required privileges can run a selected task on selected Runtime Client(s).

To Run a task on Client(s) machines, follow the steps mentioned below:

1. In Repository Manager select the task that you wish to Run on Client(s) machines.
2. Click on 'Run' from the Actions menu on top right.



3. Now select Client(s) to play the task on deployment.



Before clicking Run, the user can view:

- Task dependencies to ensure if any dependency is missing.
- Connection status of Runtime Client(s)
- Clients with domain name, if the Control Room is setup for Active Directory users in a multi-domain environment.

```
Note: You can run a task on Runtime Client(s) that are currently connected to Control Room. The
connection status of a Runtime Client can be identified by (connected), (disconnected) or
(deactivated) icons.
```

4. Select Run Bot Runner Session on Control Room* to allow the Control Room machine to take RDP of the Bot Runner machine

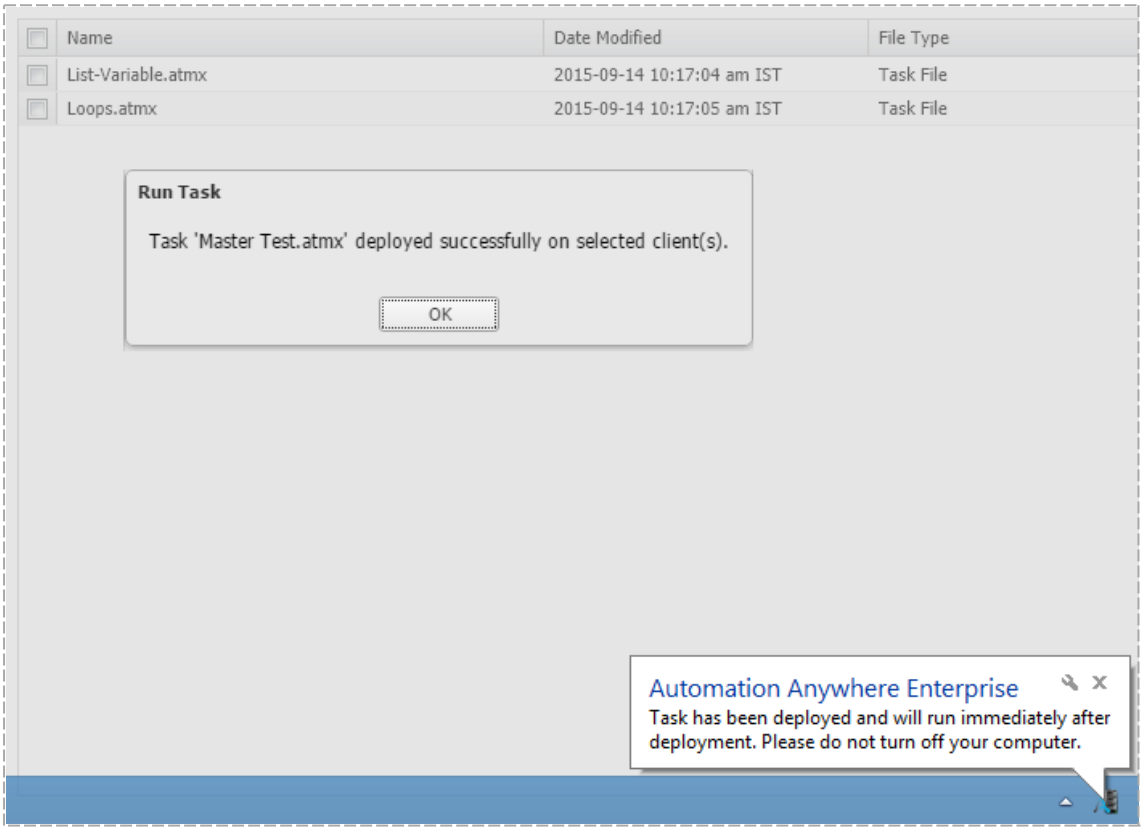
if it is in locked or logged off state to run the scheduled task. This method is recommended when Bots are deployed on virtual machines.

**Available from AAE 10 SP2 with product version 10.5.0*

Refer RDP Based Bot Deployment - Guidelines for details.

> Note: The RDP session ends once the task is executed. However, if an RDP session is not possible, the Control Room machine uses the normal auto-login route.

5. Click Run A notification indicates successful task deployment and run:



If you are unable to deploy a task on client machine, refer Troubleshooting Client and Server Communication.

Next…

You can create and organize the task schedules. Learn More

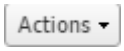
Scheduling Tasks in the Control Room

In Control Room, users with required privileges can schedule a selected task on selected Runtime Clients and also export the upcoming task schedule details to a CSV file.

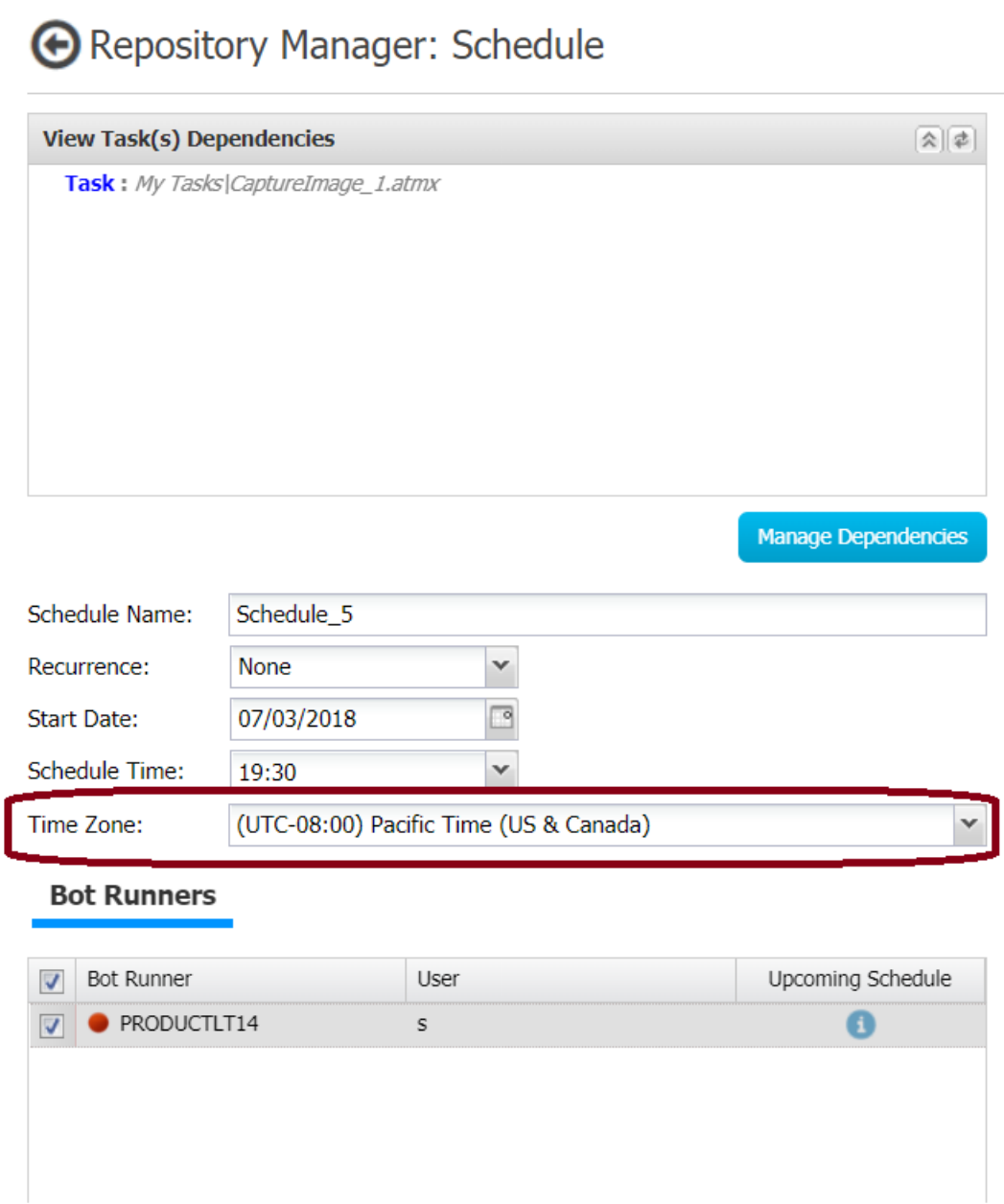
Follow the steps mentioned below if Version Control is disabled:

Note: The Control Room Administrator can also create schedules when Version Control is enabled in the Control Room. Refer Scheduling Tasks (Version Control Enabled) for details on how.

1. In Repository Manager select the task that you wish to Schedule on Clients machines. Alternatively you can also create a schedule from Task Schedules.
2. Click on '**Schedule**' from the **Actions** menu on top right.

3. Enter the schedule details such as name of schedule, date, time, and time zone of schedule.
4. Select Clients to schedule the task.



Before clicking Schedule, the user can view:

- **Task dependencies** to ensure if any dependency is missing.
- **Connection status** of Bot Runners (previously termed as Runtime Clients)
- **Upcoming Client schedule** to avoid creating schedule conflicts.
- **Clients with domain name**, if the Control Room is setup for Active Directory users in a multi-domain environment.

Note: You can schedule a task on Bot Runners that are currently connected or disconnected to Control Room. The connection status of a Bot Runner can be identified by (connected), (disconnected) or (deactivated) icons.

5. Select Run Bot Runner Session on Control Room* to allow the Control Room machine to take RDP of the Bot Runner machine if it is in locked or logged off state to run the scheduled task. This method is recommended when Bots are deployed on virtual machines.

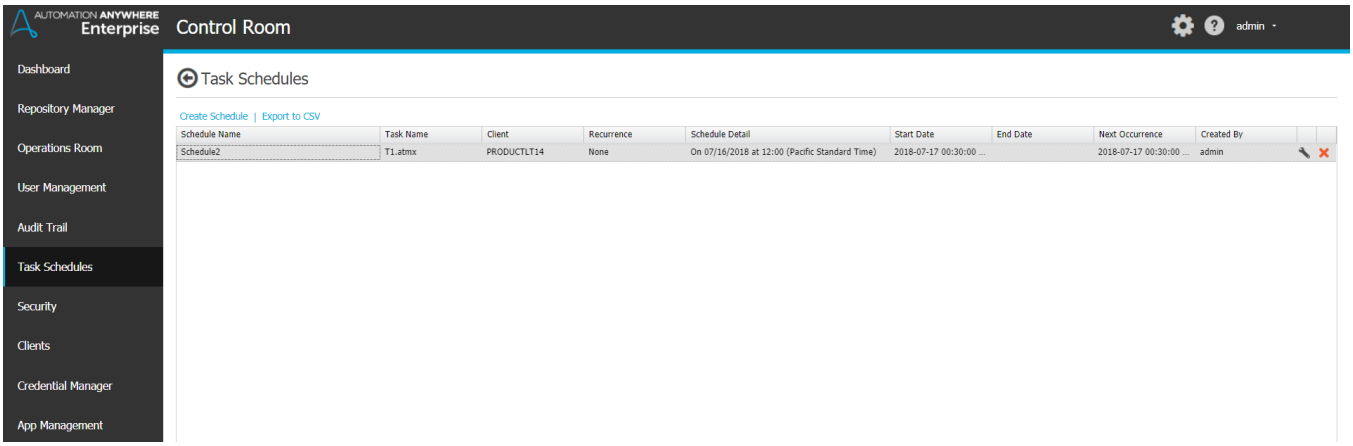
**Available from AAE 10 SP2 with product version 10.5.0*

Refer RDP Based Bot Deployment - Guidelines for details.

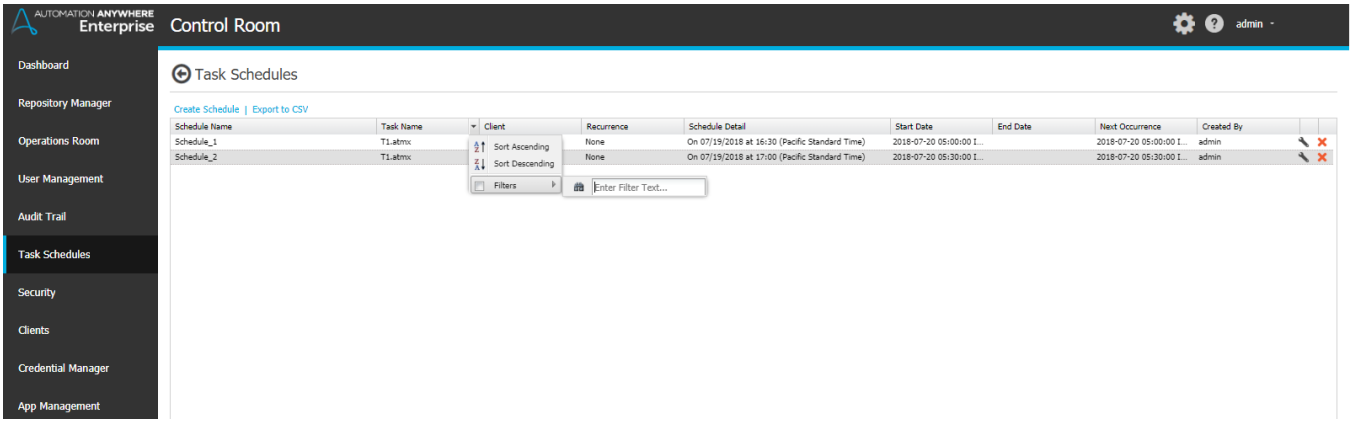
Note: The RDP session ends once the task is executed. However, if an RDP session is not possible, the Control Room machine uses the normal auto-login route.

6. Click **Schedule**.

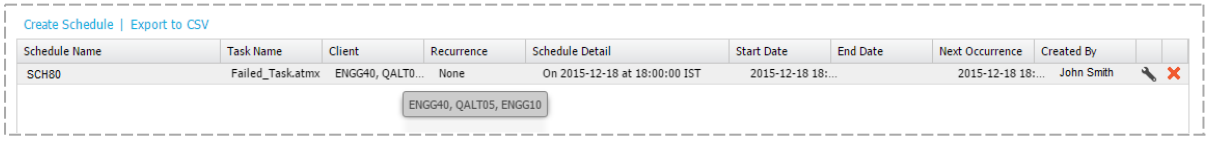
Once the schedule is created, you can see the list of all schedules in Task Schedule console.



Tip: You can sort the schedule columns in Ascending or Descending order.



To know about the various clients on which a particular task is scheduled, simply hover over the client and you will be able to see all the client names. Refer the image below:



Creating Schedules

Control room allows you to create schedules for running tasks on Client machines. With time-based scheduling capabilities, the Control Room Administrator can schedule tasks to run on particular days, weeks, or months of the year.

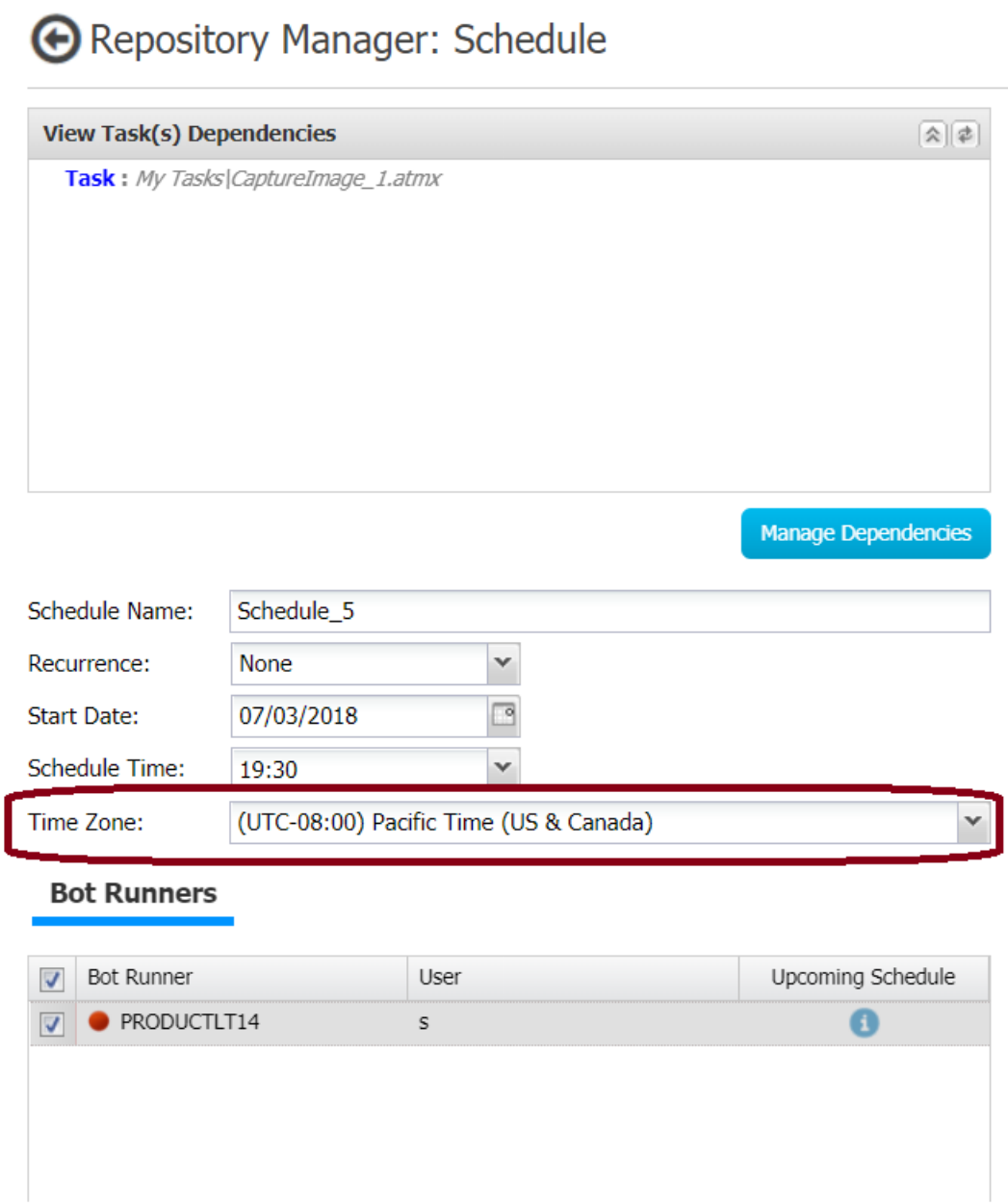
Before creating or editing a schedule, you must read about the Time Zone and Day Light Saving related notes so that your schedules are created correctly considering the time zone and day light saving. For more information about the time zone and running of schedules, see the Day Light Saving and Time Zone Selection in Schedules.

To create schedules when version control is disabled, perform the following steps:

- Click on 'Create Schedule'. This will navigate you to the Repository Manager.
- In the Repository Manager, select the task which you want to schedule and from Actions select **Schedule**.

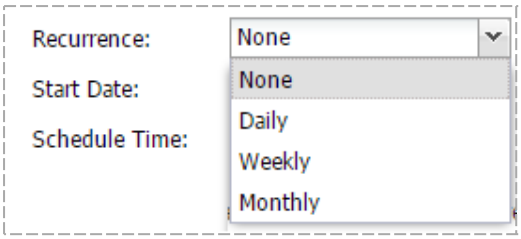
- Select the Runtime Clients on which you want to schedule the task from the **Bot Runners** section.

> **Note:** You can schedule tasks on client that are active and connected (identified with), and active and disconnected (identified with).



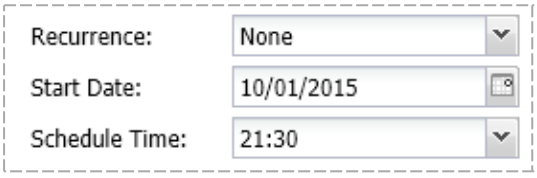
- Enter the name of schedule, recurrence, start date, schedule time, and time zone.

  You can select any one of the following options from the **Recurrence** drop-down list to run your tasks:



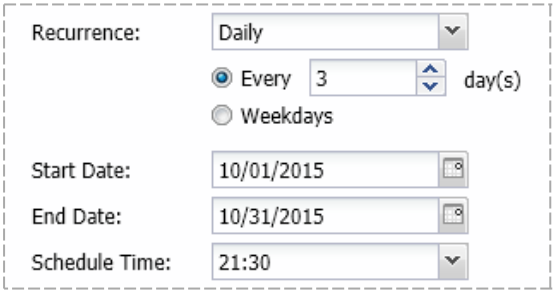
1. **None** - Use this to schedule the task if you want to run schedule only once. Select the required fields such as Start Date and Schedule Time:

   For instance, select 30th September to run the selected task at 21:30 hrs.



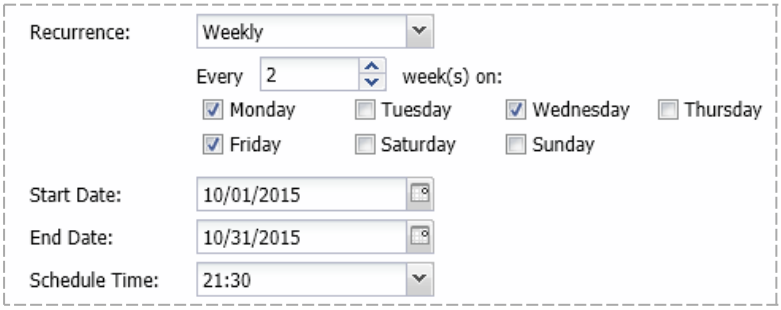
2. **Daily** - Use this to schedule a task that you want to run either for selected number of days - to be input in 'Every' field or on 'Weekdays'. Enter the Start and End Dates and Schedule Time:

   For instance, select/input '3' to in the 'Every' days field to play the selected task at 21:30 hrs for a month starting 1st October to end on 31st October.



3. **Weekly -** Use this to schedule a task to play for selected Days at an interval of specified Weeks. Enter the Start & End Dates and Schedule Time:

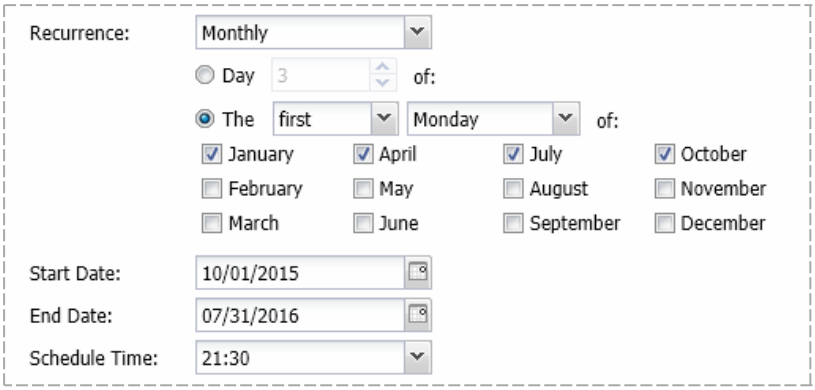
   For instance, schedule the selected task to play on 'Monday', 'Wednesday' and 'Friday' for '2' Weeks at 21:30 hrs for a month starting 1st October to end on 31st October.



4. **Monthly -** Use this to schedule a task to play for specific Days of selected Months or for specific Day of a Week of selected Months:

   For instance, schedule the selected task to play at 21: 30 hrs on the 'First' 'Monday' of first month of a

quarter, that is, 'January', 'April', 'July' and 'October' starting from October in current year to end in July of next year.



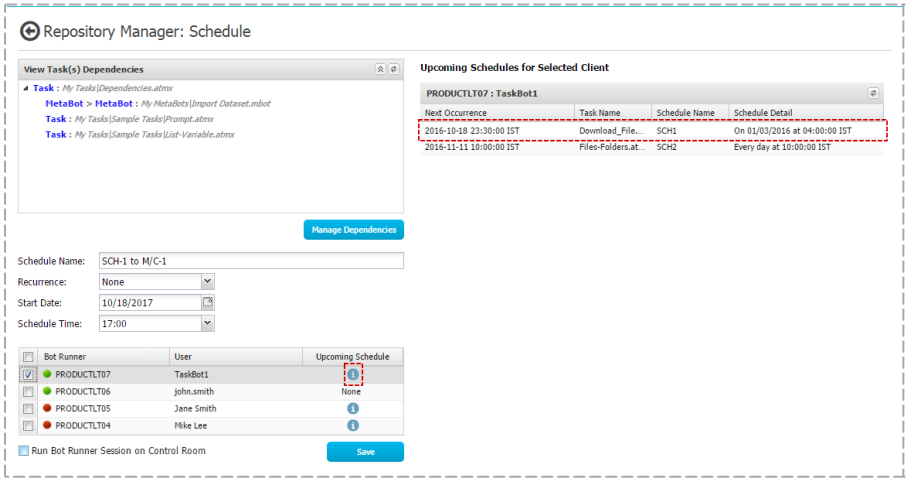
> **Tip:** Schedule the tasks based on the process requirement. You can also create a combination of schedules to run different tasks.

- Click on **Save** to confirm the schedule.

> **Note:** If you are unable to schedule a task on a client machine, refer to Troubleshooting Client and Server Communication.

Viewing Upcoming Task Schedules

While scheduling a task, you will need to verify what TaskBot Clients have upcoming schedules to avoid schedule conflicts. You can view these details by clicking .



> **Note:** If schedule does not exist for a particular TaskBot, 'None' is visible.

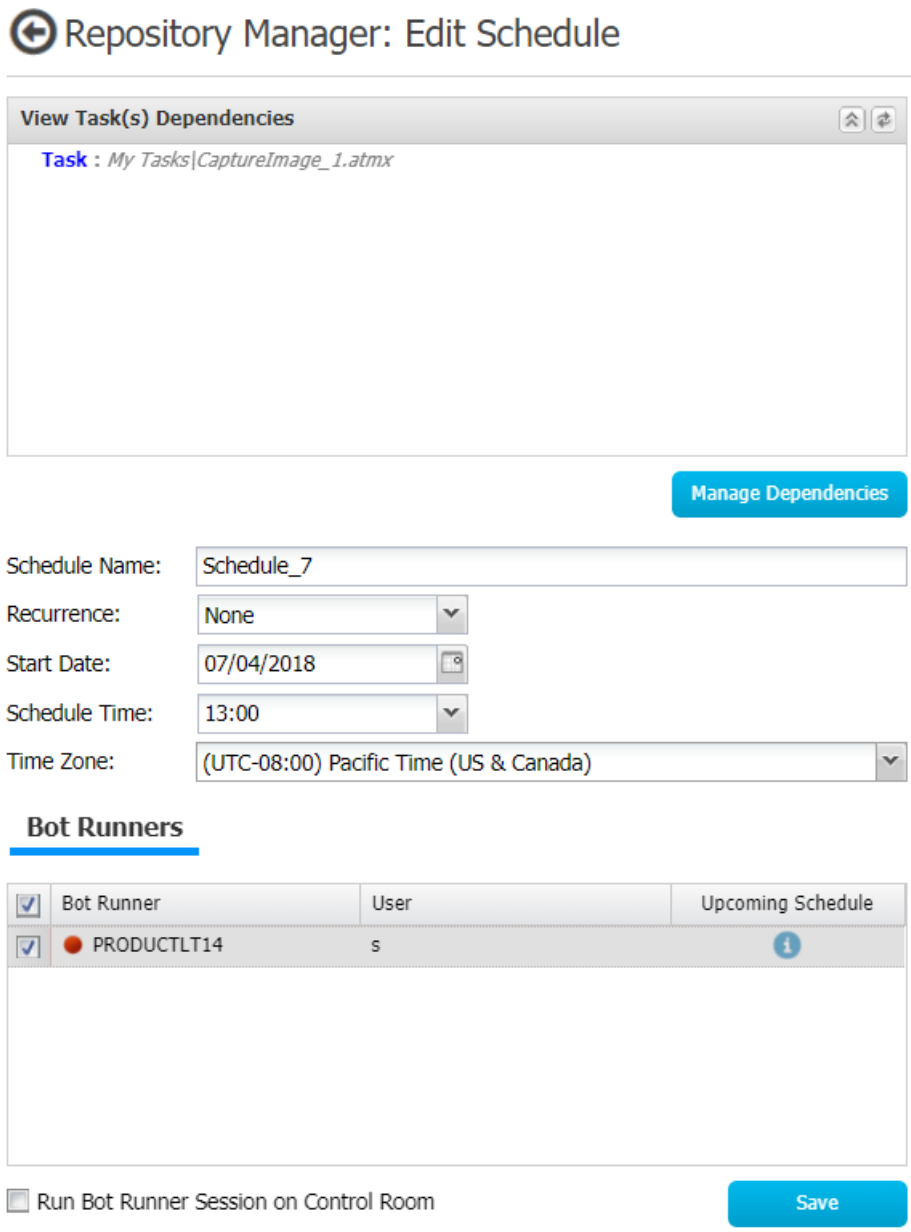
In the 'Upcoming Schedules...' view, you can verify when next the task is scheduled to play, that is, the Next Occurrence, Task Name, Schedule Name and Schedule Details. For instance, in the above image, the selected task 'Download_File' is scheduled to play once on 3rd January, 2016 at 4 pm.

Editing a Schedule

Control Room Administrator can choose to edit existing schedule by simply clicking on against a particular schedule.

Note: You cannot edit the schedule name while editing a schedule.

On clicking the edit icon, Edit Schedule page is displayed where the details of schedule can be changed as per requirement.



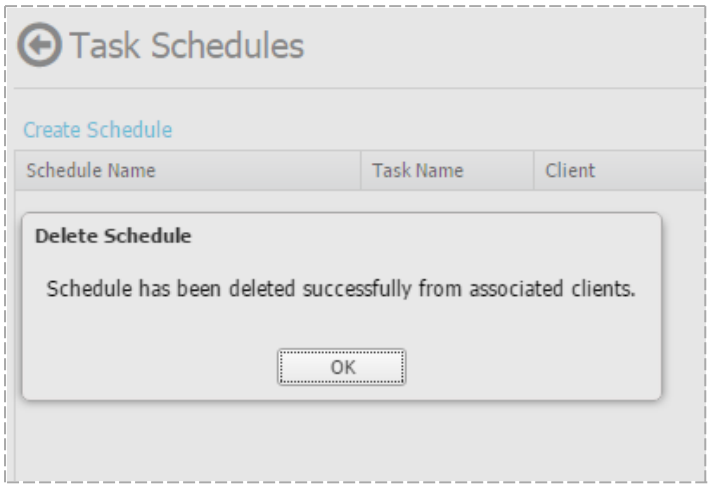
The Edit Schedule page displays pre-filled values in each fields (same as entered while creating and saving the schedule).

Field Names	Editable
Schedule Name	Yes
Recurrence	Yes
Start Date	Yes
Schedule Time	Yes
Time Zone	Yes

Note: The values in task dependencies, client status and upcoming schedule are dynamic and will be displayed as per the current situation at the time of editing the schedule.

Deleting a Schedule

To delete a schedule, click ✖. After confirmation, you will see a message informing you about successful deletion of the schedule.

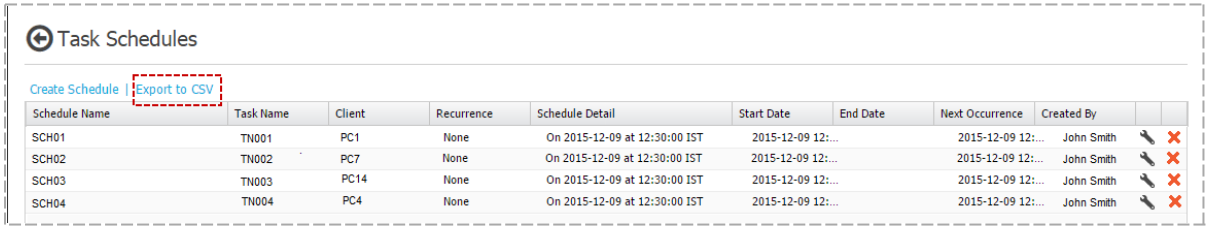


To return to the Task Schedules page, click .

Exporting Schedule Details to CSV

Available from version 10.2

A Control Room administrator can plan to reschedule tasks that are already deployed to run, during events such as routine maintenance, by exporting the upcoming task schedule details to a CSV file. To export, click on 'Export to CSV' link.



Next...

You can create and organize task schedules when Version Control is enabled. Learn More

Day Light Saving and Time Zone Selection in Schedules

When the Day Light Saving Time (DST) switch over occurs, the clock is set backward/forward during this time interval that is, 1 a.m. to 3 a.m. DST starts, the switch over occurs between 1 a.m. to 2 a.m. When DST ends, the switch over occurs between 2 a.m. to 3 a.m. If your schedules are set to trigger during this time interval, then check and ensure whether your schedules are run as expected when the DST switch over occurs.

Notes:

- All the application servers must be in the same time zone in the distributed mode for the Control Room login to work.
- If you have existing schedules, we recommend that you edit the time in the schedule to ensure that the schedule does not fall in between DST switch over time.
- If you do not update the existing schedules after updating CR v10.5.10 patch, the schedules will run as per the time zone stored in the database, which is generally Coordinated Universal Time (UTC) for Daily and None schedule types and server time zone for rest of the schedule types. Therefore, before Daylight Saving Time changes come into effect, it is recommended that you validate the time zone of schedules.

- For existing schedules, the time and time zone data stored in the customer's database is taken to run the schedules, which is generally Coordinated Universal Time (UTC) for Daily and None schedule type and server time zone for rest of the schedule types.

Because of the resetting of the clock due to Day Light Saving, schedule for running the bots is affected. Schedules are triggered as per the time defined while creating a new schedule and the selected time zone.

The following table explains creation of a schedule and running of a schedule in the context of the AEDT, the creator's time zone and the Control Room's server time zone, that is, EDT. For example, a user creates a schedule in the AEDT time zone on June 28th, 2018 at 2:00 a.m to be run at 4:00 p.m AEDT on Oct 7th, 2018.

Events	Description	Creator's Time Zone	Server's Time Zone	Date	Comments
Create a schedule	User creates a schedule in the AEDT time zone on June 28th, 2018. **Day Light Saving Time switch over occurs from EDT to EST in the Control Room server's time zone**	4:00 p.m. AEDT	2:00 a.m. EDT	June 28th, 2018	EDT is the time zone of the Control Room server
Run a schedule	Run this schedule in the AEDT time zone on Oct 7th, 2018.	4:00 p.m. AEDT	1:00 a.m. EST	Oct 7th, 2018	The schedule is run in Australia's AEDT time zone at 4:00 p.m.

Viewing and Managing Task Dependencies

As processes become complex, there's a need to manage multiple tasks. This can be achieved by either queuing one task after another or playing a task that includes sub-tasks.

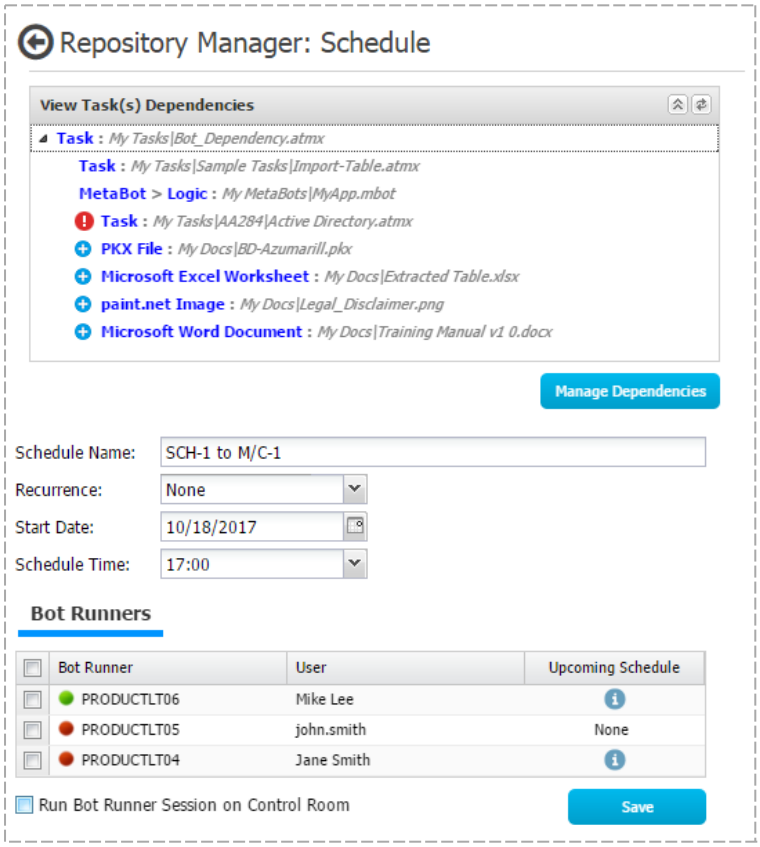
If a task includes sub tasks, it is termed to have 'Dependencies'. In Control Room for such tasks to play successfully, a user needs to upload the sub-tasks as well.

Similarly, if a task is password protected*, you will be required to input the password during deployment. This is also termed as a 'Dependency'.

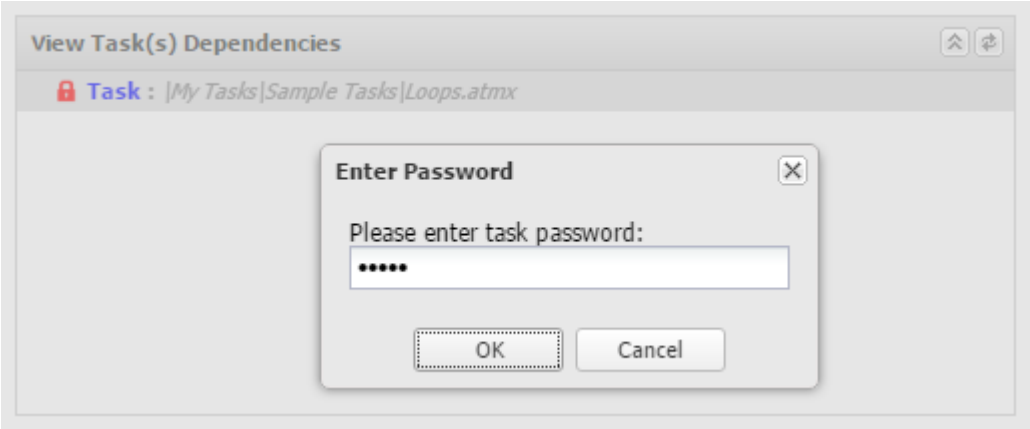
**This feature is applicable to Enterprise edition 10.1 and less.*

While deploying a task, the Control Room scans for the task dependencies and displays those in the 'View Task(s) Dependencies' window:

Note: View Task(s) Dependencies displays dependencies of TaskBots, IQBot, MetaBot, Sub tasks, and a particular task that is called using the Run Task command and files such as documents, certificate, exe & script.

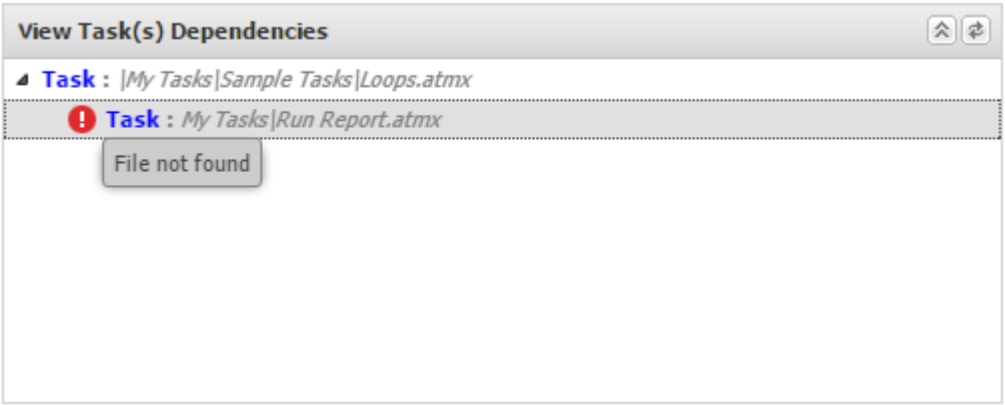


- A task that is password protected is indicated by . To unlock the task, input the password:



*Applicable to Enterprise edition 10.1 and less.

- A task with a sub-task that is unavailable in the Control Room repository is indicated by icon:



Note: You can deploy such tasks once you resolve the dependencies.

- Use to collapse/minimize the Dependency window, to expand/maximize and to refresh the view.

Managing File Dependencies

Available from version 10.3

Certain dependent files such as documents, certificates, exe, and scripts cannot be deployed automatically while scheduling tasks that comprise these dependencies.

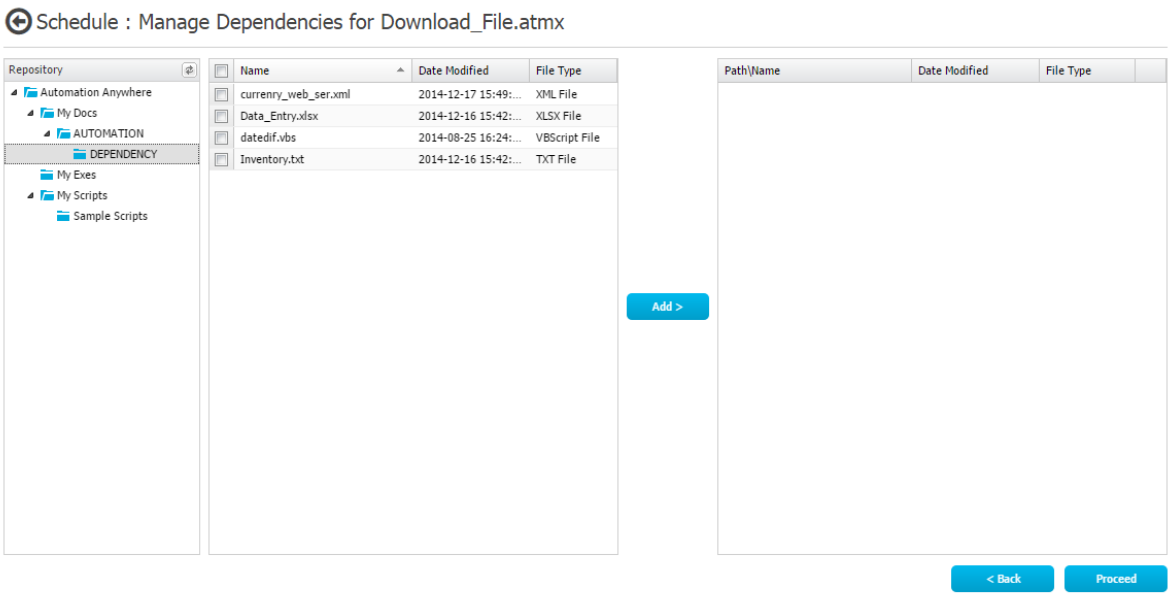
To enable a successful task run for tasks with dependencies, a Control Room Admin and/or a Control Room User with Run and Schedule permissions, can choose to add or remove dependencies manually while scheduling a task.

When the task is deployed on BotRunners, the dependencies added manually, are copied at the Automation Anywhere Enterprise application path, on the BotRunner machines.

Note that the any updates to the dependent files are automatically reflected and the user need not manage the dependencies at every file update instance.

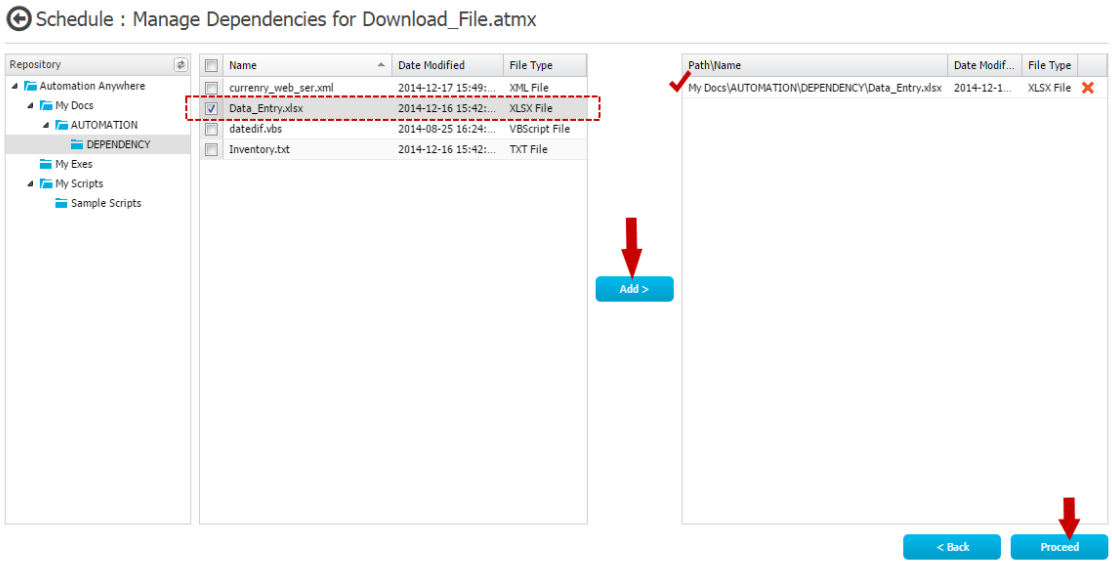
Adding Dependencies

To include a dependent file - documents, certificate, exe, and script, click on 'Manage Dependencies'. You are guided to the Manage Dependencies page:

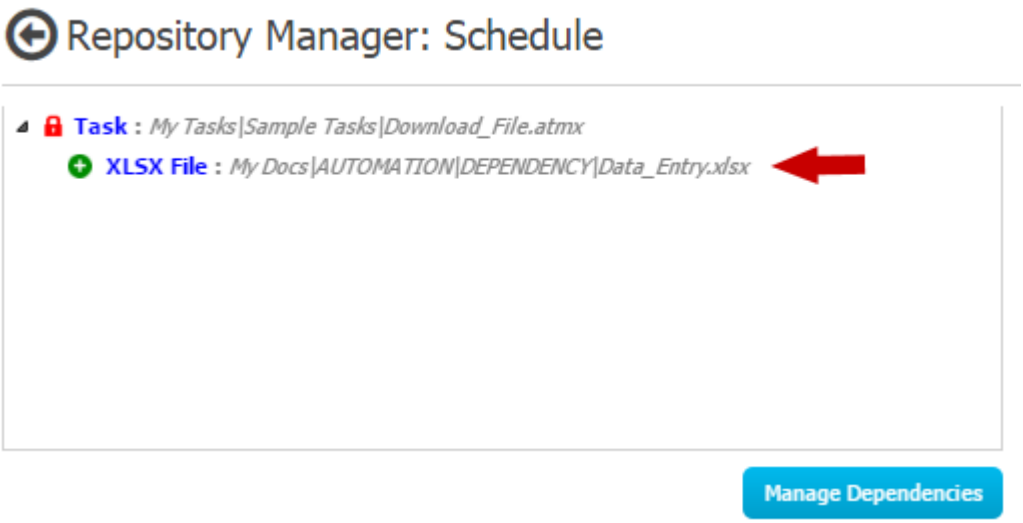


Note: Only dependent files from My Docs, My Exes, and My Scripts are considered for deployment.

1. Go to the folder that comprises dependent files.
2. Select file(s) from the panel list on the left and click on 'Add'.
3. The files are added to the panel list on the right.
4. Click on Proceed.



5. The files are included in the task.



Tip: To return to the Schedule page without saving the changes, click on 'Back'.

Removing Password Dependencies

Note that from Enterprise edition 10.2, password protection in tasks is deprecated and hence it is recommended Client users edit, save and re-upload password protected tasks.

If a password protected task exists in Control Room, while scheduling, you will be displayed a message recommending to edit, save and re-upload the task to the Control Room. This ensures that the previously set password is removed for the task and any of its sub-tasks.

Note: The message will continue to display until the Client user does not edit and re-upload the task.

Assigning BotRunners To Run/Scheduling Role

Available from version 10.3

As the Control Room provides role based access to its users, when the Control Room Admin grants task run and/or scheduling permissions to a role, that user is allowed to run and/or schedule tasks only on those BotRunners that are assigned to that role.

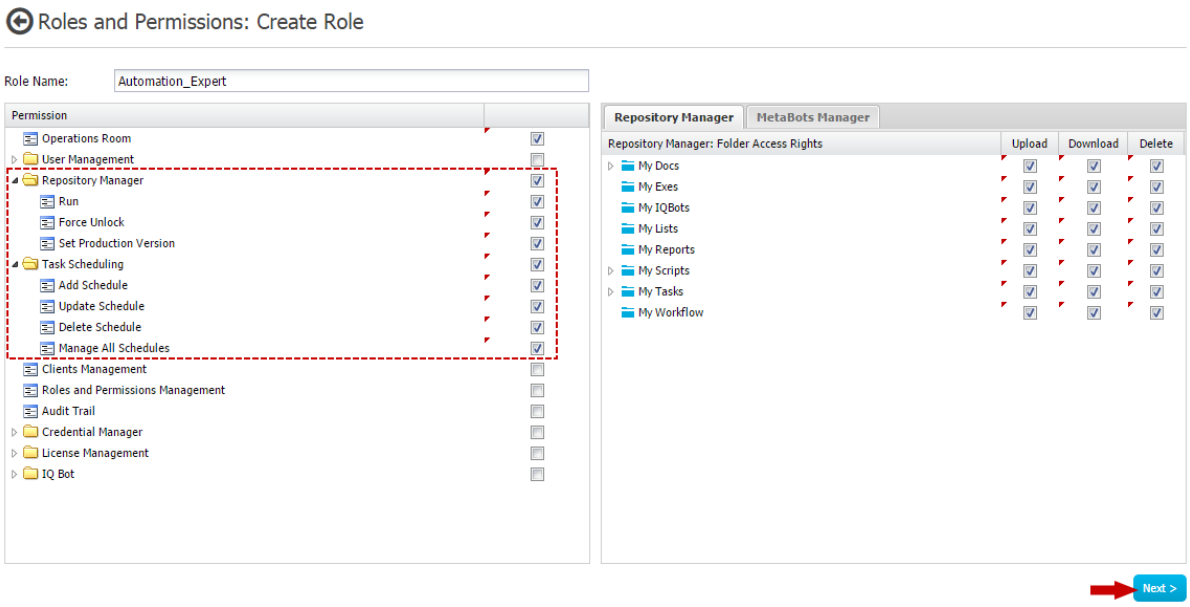
Note that roles created in version 10.2.1 and earlier, all BotRunners are assigned to the Run/Scheduling role, by default.

The Control Room admin can choose to assign BotRunners during role creation or modification. However, if the Admin does not assign any BotRunner to a Run/Scheduling role, the user assigned this role is informed that no BotRunners are assigned when the user attempts to deploy/schedule a task.

When the Admin decides to delete a BotRunner that is already assigned to a user with Run/Schedule permissions, the Admin is allowed to delete the BotRunner only if no tasks are scheduled to run on that particular BotRunner. In fact, the Admin will be able to delete the BotRunner after deleting the schedule(s).

Assigning BotRunners

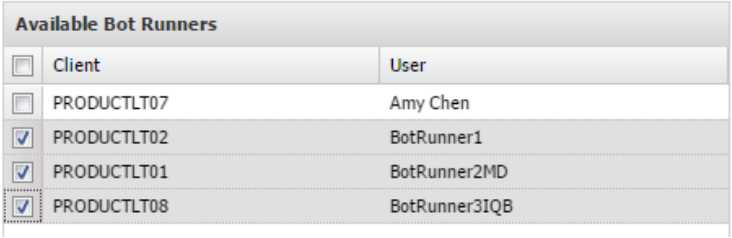
You can choose to create a new role or modify an existing role to assign BotRunners to a Role that has run and/or scheduling permissions.



Note: On enabling the permissions, the Next button is visible at the bottom right of the page.

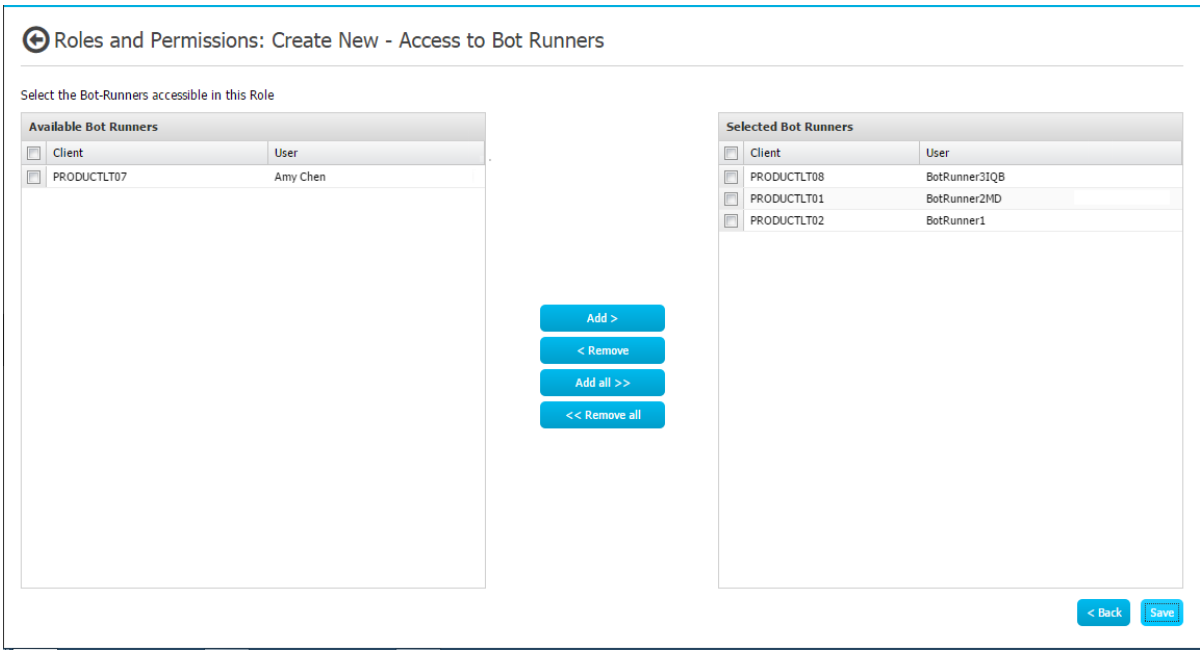
Click Next to launch the Create Role - Access to Bot-Runners page.

Select BotRunner(s) from the list of available BotRunners.



Note: Only those BotRunners that are registered and logged in will be visible in the list.

To add the BotRunner(s) to the list of selected BotRunners click on Add.



Tip: You can choose to Add all roles to the list. Also, you can choose to Remove or Remove all BotRunners from the list.

To save the role with the selected list, click Save. Or to return to the previous page without saving, click Back.

Tip: You can update the list of BotRunners, by editing the role. Refer article on 'Managing Roles and Permissions'.

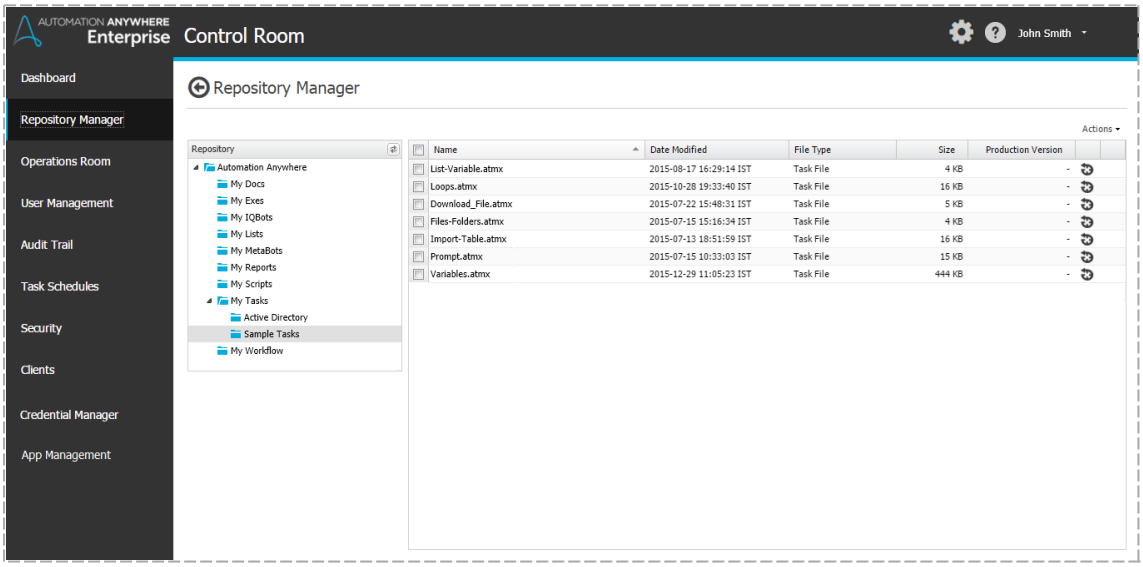
Scheduling Tasks in Control Room (Version Control Enabled)

The Control Room Administrator can schedule tasks to play on Client(s) machines when Version Control is enabled in the Control Room.

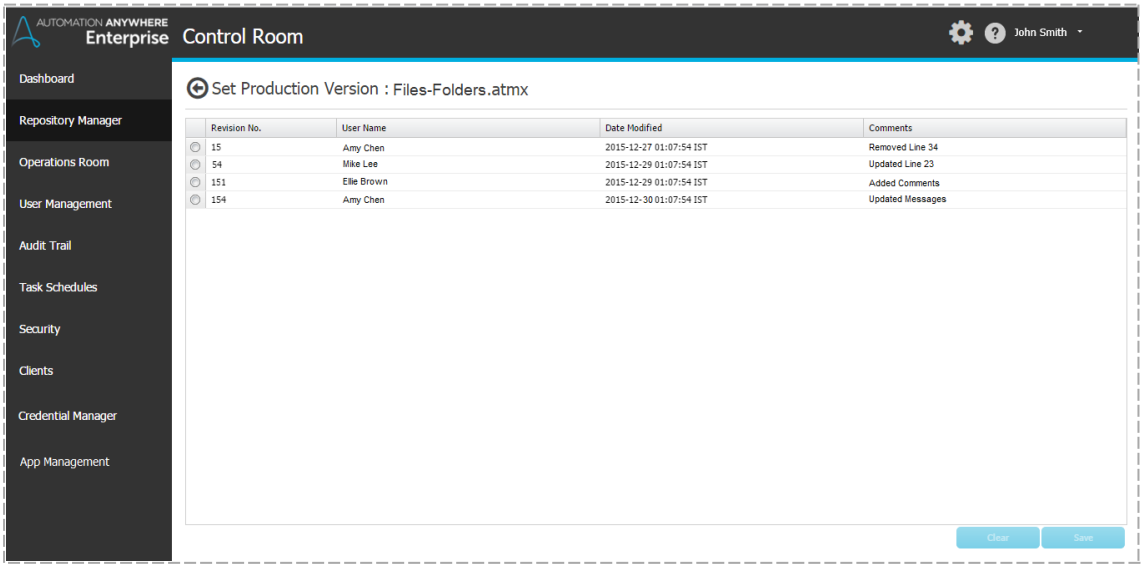
To create schedules, follow the steps below:

1. Click on 'Create Schedule'. This will navigate you to the Repository Manager
2. In Repository Manager select the task which you wish to schedule and set its 'Production Version' by clicking on .

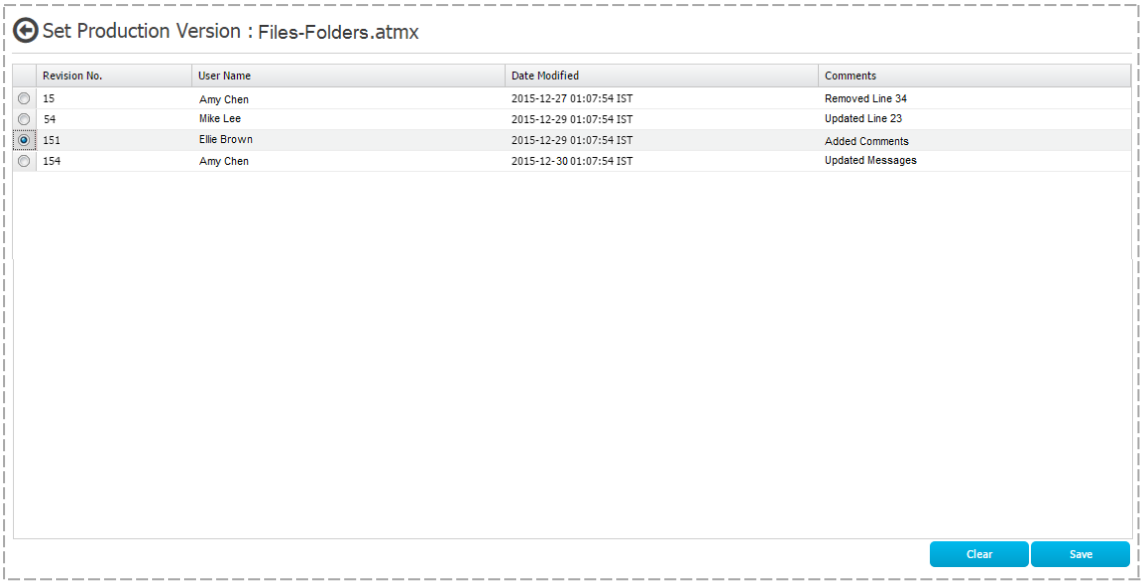
> Note: When Version Control is enabled, it is important to set the 'Production Version' of a task before you schedule it. Learn More.



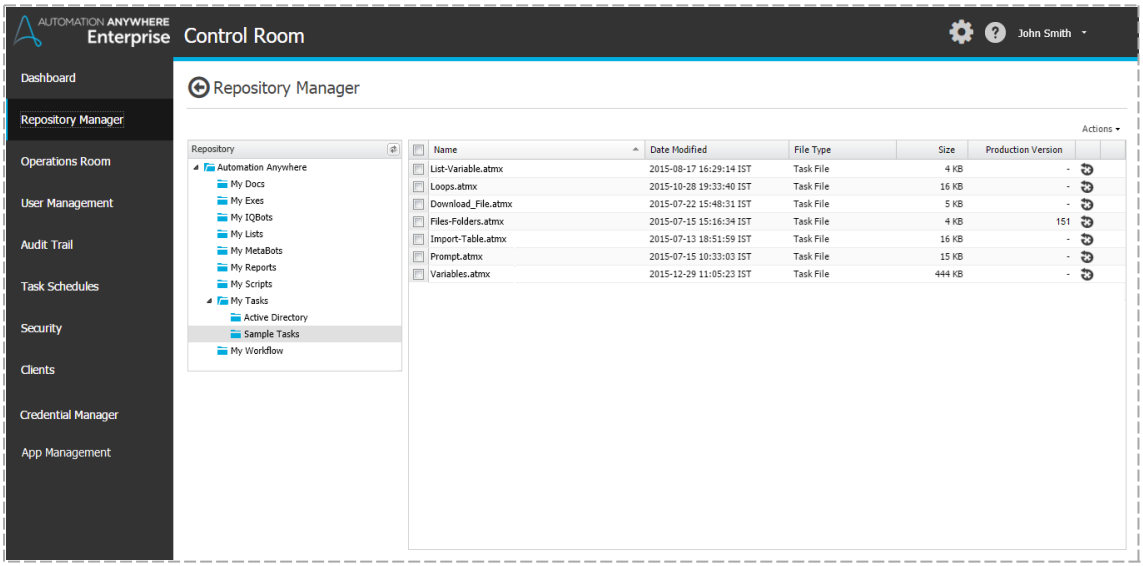
3. This will navigate you to 'Set Production Version' page that shows the version history of the task. Here you can select the revision number that you wish to assign as Production Version.



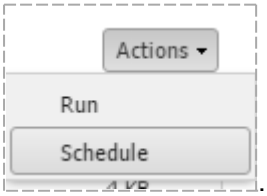
4. Select the appropriate Revision Number and click Save to confirm.



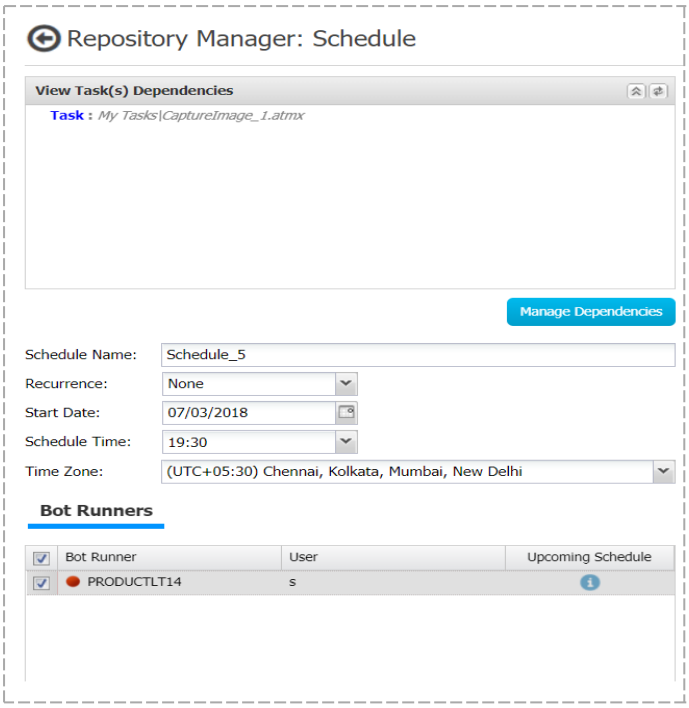
5. After you have set the Production Version of a task, you will be taken back to the Repository Manager where you can Schedule the task.



6. Select the task and click on Schedule from Actions on the top right.

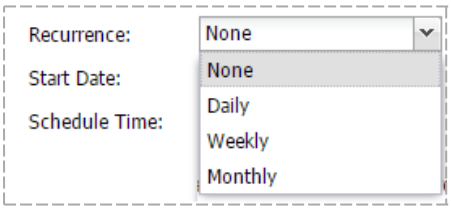


7. Select Runtime Client(s) on which you wish to schedule the task play.



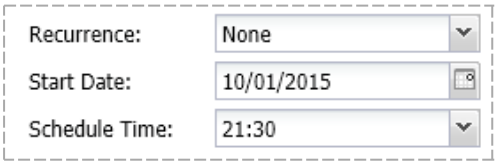
8. Input the name of schedule, recurrence, start date and schedule time.

   You can choose any of the following schedules to play your tasks:



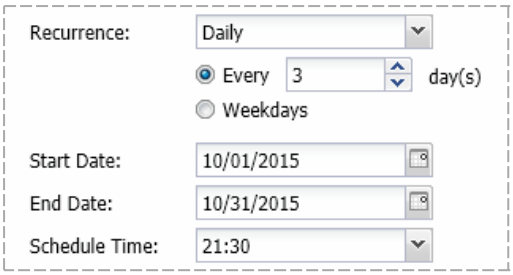
- **None**- Use this to schedule the task if you want it to play only once. Select the required fields such as Start Date and Schedule Time:

  For instance, select 30th September to play the selected task at 21:30 hrs.



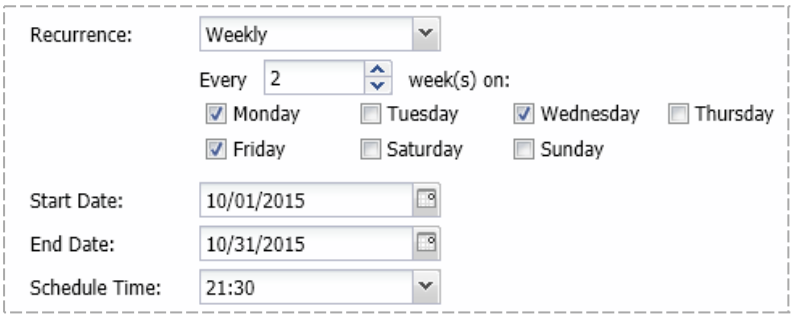
- **Daily**- Use this to schedule a task that will play either for selected number of days - to be input in 'Every' field or on 'Weekdays'. Input the Start & End Dates and Schedule Time:

  For instance, select/input '3' to in the 'Every' days field to play the selected task at 21:30 hrs for a month starting 1st October to end on 31st October.



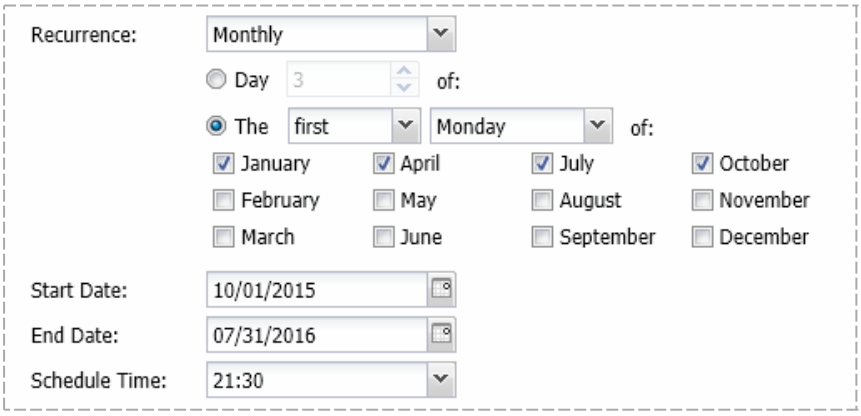
- **Weekly** -Use this to schedule a task to play for selected Day(s) at an interval of specified Week(s). Input theStart & End Dates and Schedule Time:

  For instance, schedule the selected task to play on 'Monday', 'Wednesday' and 'Friday' for '2' Weeks at 21:30 hrs for a month starting1st October to end on 31st October.



- **Monthly** -Use this to schedule a task to play for specific Day(s) of selected Month(s) or for specific Day of a Week of selected Month(s):

  For instance, schedule the selected task to play at 21: 30 hrs on the 'First' 'Monday' of first month of a quarter i.e. 'January', 'April', 'July' and 'October' starting from October in current year to end in July of next year.



> Tip: Schedule the tasks based on the process requirement. You can also create combination of schedules to run different tasks.

9. Click on Save to confirm the schedule.

Production Version

When Version Control is enabled various revisions of a single tasks are created on the server by different users. While scheduling a task the Control Room Administrator needs to specify on which revision of the task must be considered as 'Production Version'.

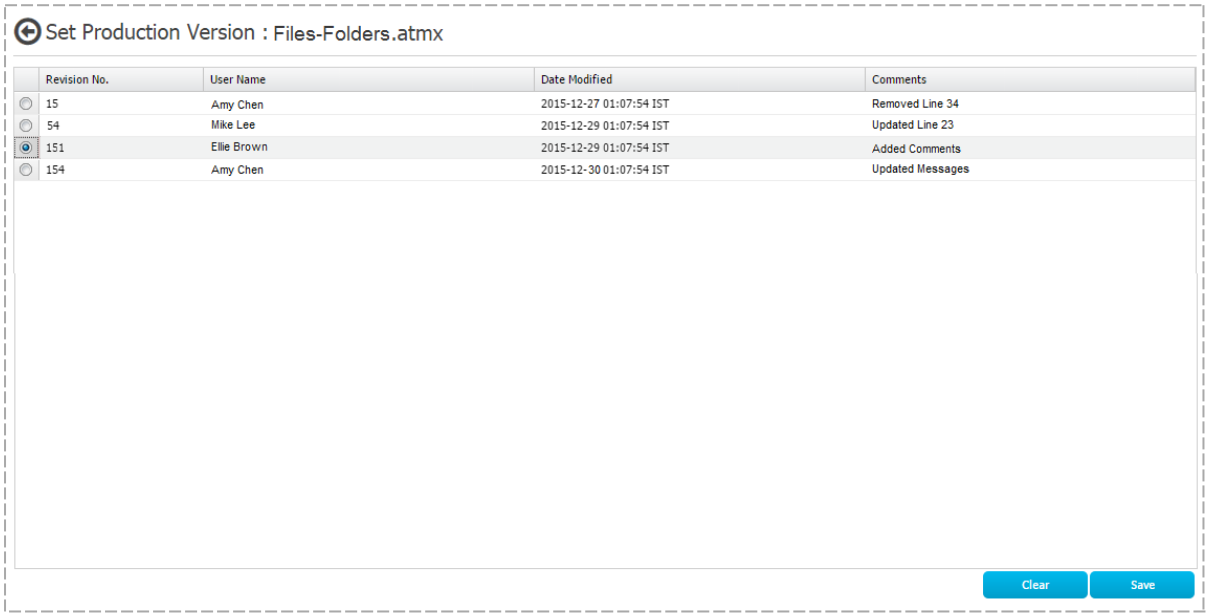
Production Version basically indicates the revision of the task that will be used to run the task on the production environment.

Note: A scheduled task will always run on the latest Production Version even if various revisions of the task exist or are newly created.

All the revision numbers for a task can be seen when you click on besides that particular task.

Note:'Production Version' for every task is not set by default.

To set a particular revision number as 'Production Version', simply select the appropriate revision number from 'Set Production Version' page.



In case, you wish to reset the 'Production Version', repeat the above steps and simply choose another revision number.

Note: If you change the Production Version of a task that has been scheduled on a client machine, the next occurrence of the schedule will run on the latest Production Version automatically.However, if the task (and its sub task) has some manual dependency or is password protected or doesn't have a production version, the schedule will not run on the latest production version.

You can also choose to clear any previously set 'Production Version' by clicking on Clear button on the 'Set Production Version' page.

Next...

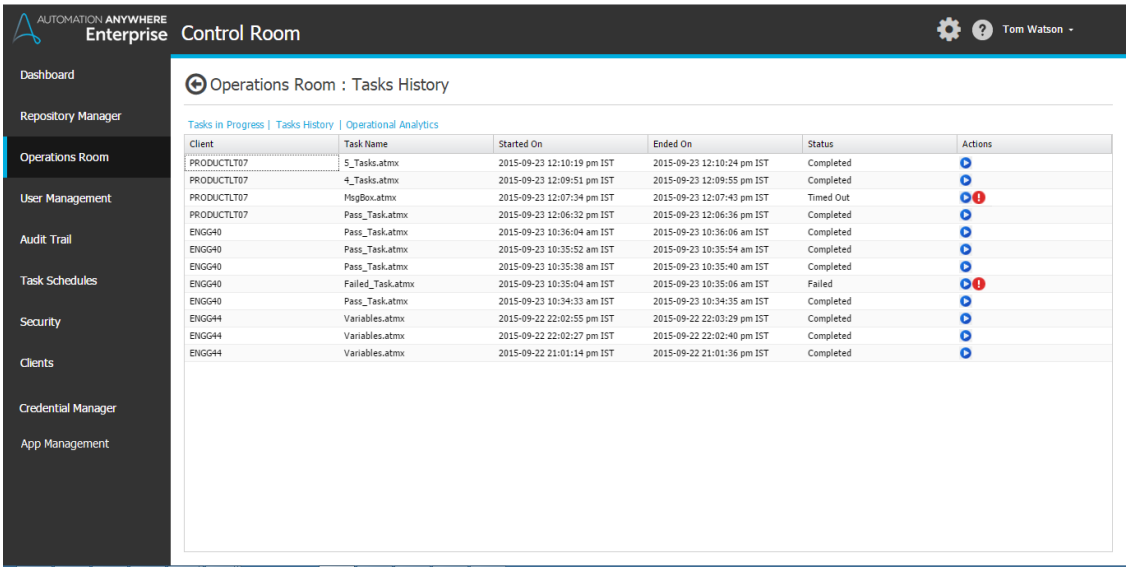
You can monitor your task status in the Operations Room. Learn More

Managing the Operation Room

One of the most important responsibilities of the Administrator is to monitor automated tasks that are deployed to client machines. Monitoring task progress and status helps to enforce internal compliance regulations, as well as to prevent tampering with mission-critical processes.

The Operations Room is a powerful monitoring console that provides detailed information about all automation on the network. You can use this console to monitor, in real time, all running tasks that have been deployed on BotRunners. You can also track the task progression based on status; whether In Progress, Paused, Completed, or Unknown.

Filters to view history and tasks in progress allow you to pinpoint information about the tasks for specific time periods.

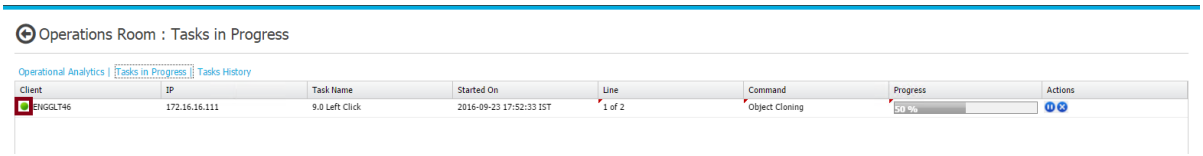


Note: Since Control Room allows for role based access to its users, you will be able to view, run, and schedule only those tasks that belong to the folder to which you have access privileges.

Viewing Tasks in Progress

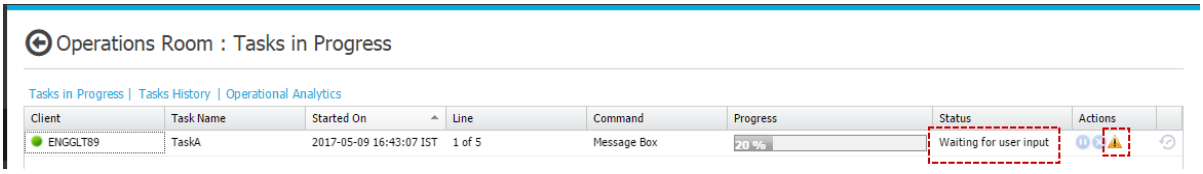
You can monitor task progression in the Operations Room when you select the 'View Tasks in Progress': It is effective for Audit and Compliance purposes to ensure that Bot's are audited even when they go offline.

Note: The highlighted icon in the above image turns 'Red' when Client is disconnected.



You can pause the task by clicking and abort by clicking .

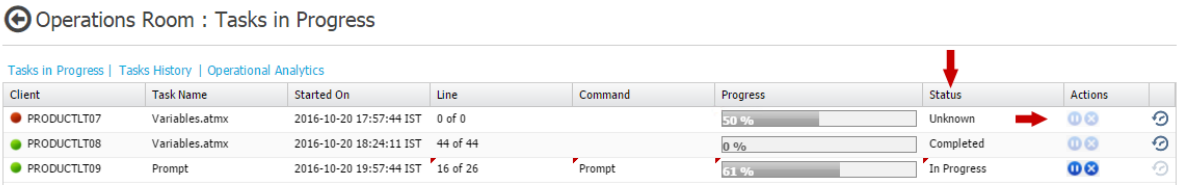
If any task requires user intervention in the form of message, prompt, and/or error, the Actions column shows a warning with the status **Waiting for user input**.



Note: If the BotRunner on whose machine the task is being executed does not perform the required action within couple of minutes, the Control Room user scheduling tasks as well as the BotRunner shall receive an email notification provided SMTP and Task Execution Status notifications are enabled.

Tracking an 'Unknown' Task Status

At times a task that is deployed to BotRunner machines crashes and/or resumes, if the Client disconnects due to network failure, crash or application restart. Given this scenario, the Control Room administrator or a user with Run and/or Scheduling permissions is given an indication in the Task in Progress view. The status of such tasks is displayed 'Unknown'.



The Control Room admin and/or user is not allowed to either pause or stop the task; the and buttons are disabled.

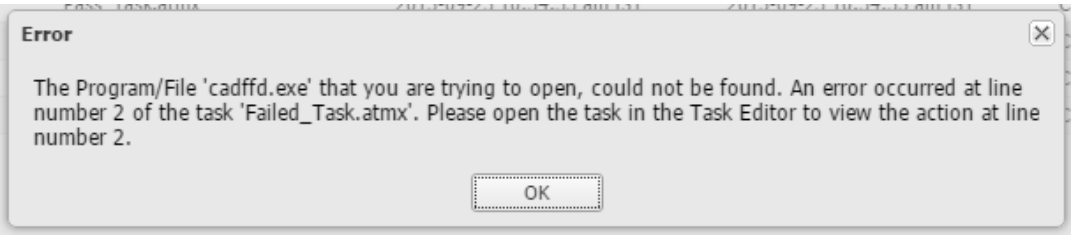
The entry for unknown tasks can then be moved to history by clicking

Viewing Task History

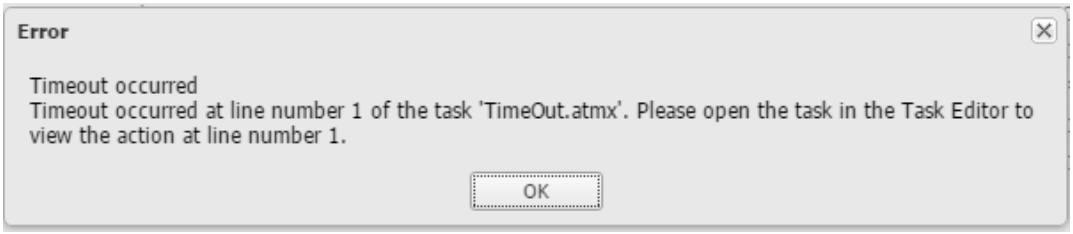
You can view the status of tasks that have been played successfully or have error-ed out during play time when you select 'View History'.

Tip: To view the status of tasks immediately in history, you can opt to refresh your browser.

The task line number at which it failed is displayed in the error message when you click on for the selected task.



In case your task timed out, you can see details of error by clicking on for the selected task.

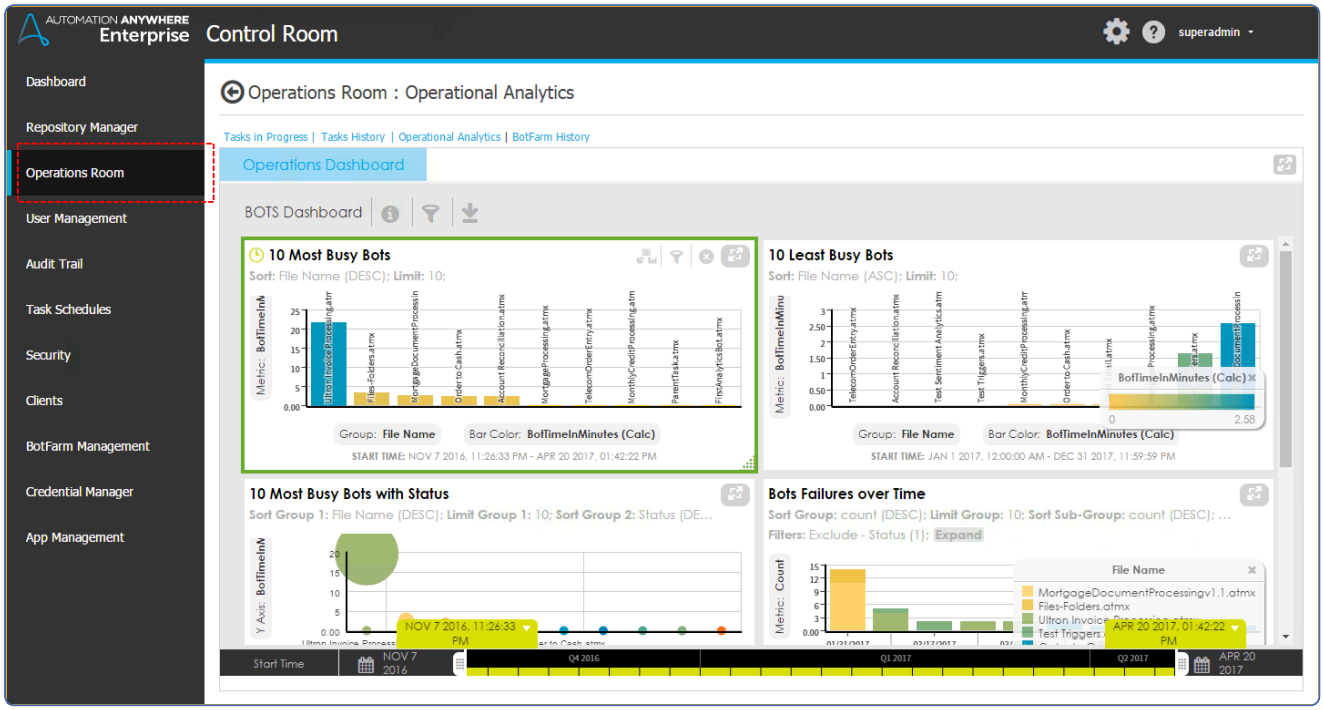


You can also run the selected task from here by clicking

Note: For tasks with status 'Unknown', the Ended On column does not display any data.

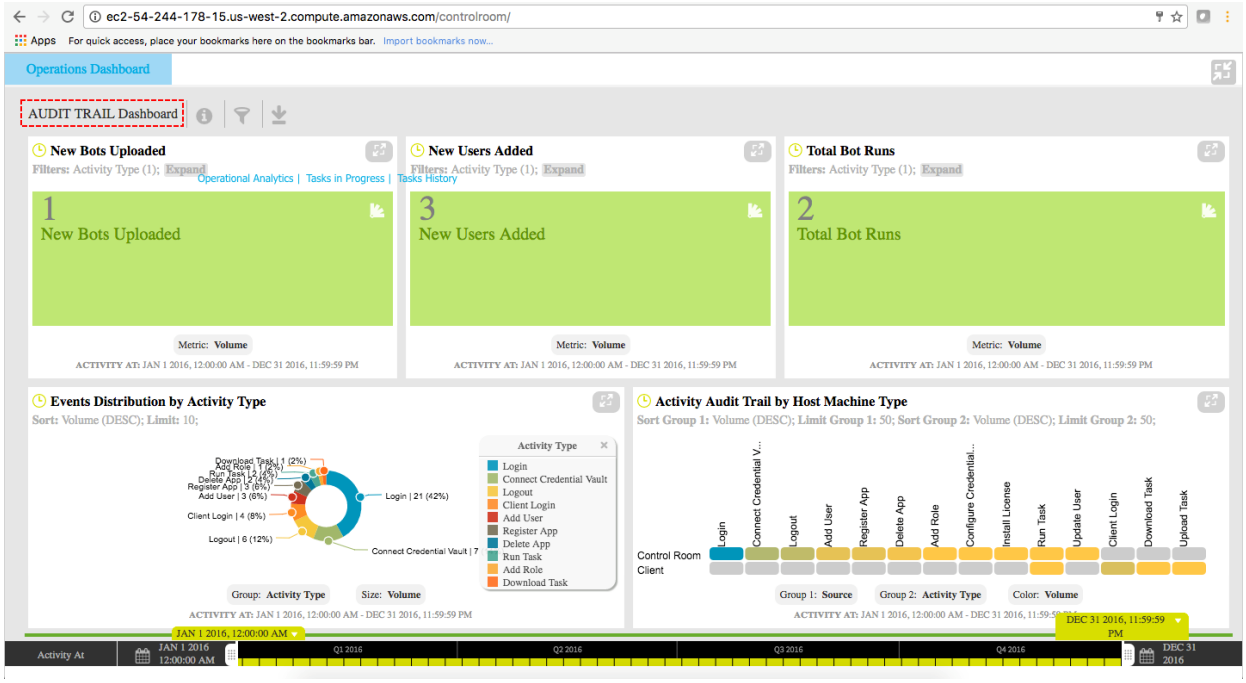
Operational Analytics Dashboard

The Operational Analytics Dashboard is visible to **only those users** who have installed BotInsight on their machine.



To view the **Operational Analytics Dashboard**, click on Operations Room.

- You will be able to see the Operations Dashboards loading up with the **AUDIT TRAIL Dashboard**.



- This means that the Bot Insight App was able to successfully register with the Control Room.

> Note: To learn how to integrate Analytics in Control Room, refer Application Management in Control Room

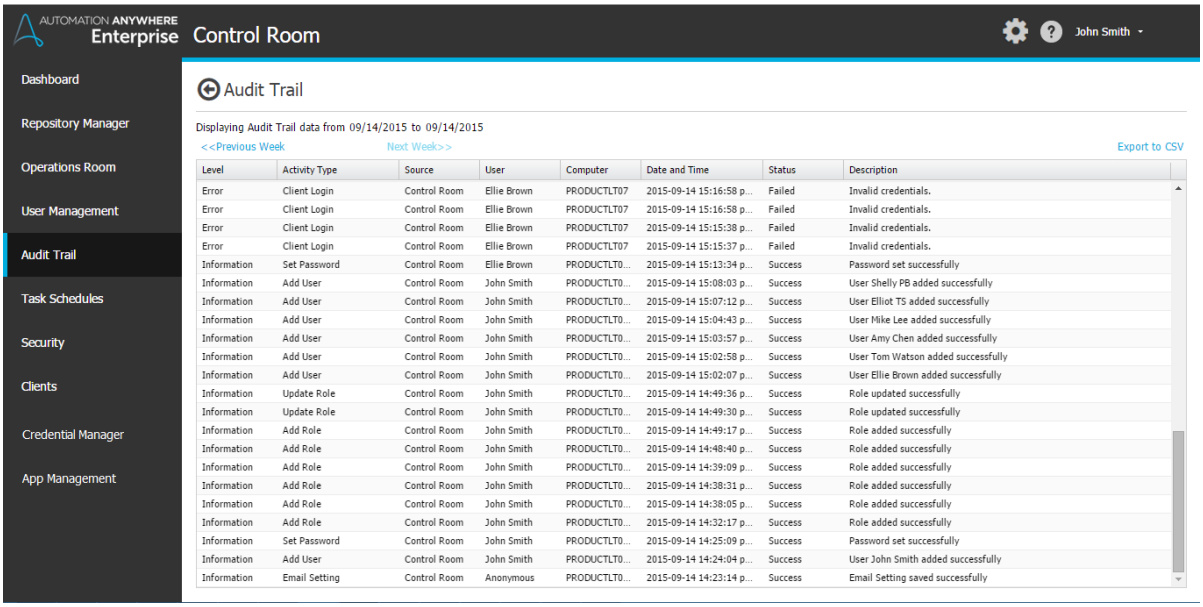
Next…

You can monitor the Control Room activities in the Audit Trail. Learn More

Monitoring the Audit Trail

An Audit Trail provides an administrator and/or user important data to monitor task progress and status to enforce internal compliance regulations, as well as to prevent tampering with mission-critical processes.

Note: Since Control Room Users are managed based on roles, this console is available for view provided a User has relevant access privileges.

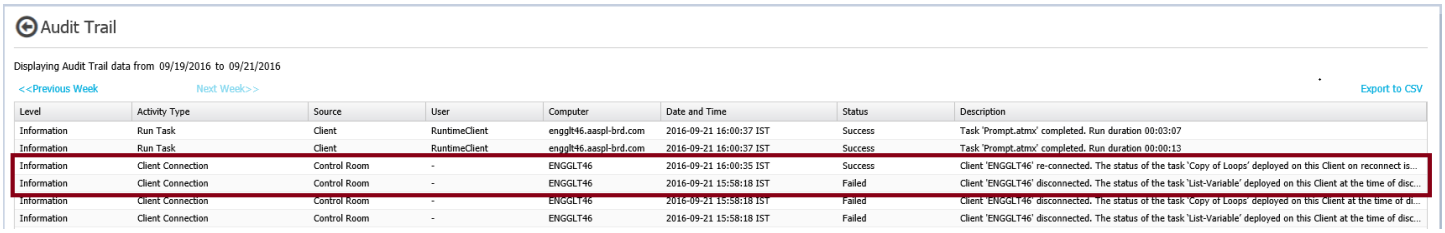


Level	Activity Type	Source	User	Computer	Date and Time	Status	Description
Error	Client Login	Control Room	Ellie Brown	PRODUCTLT07	2015-09-14 15:16:58 p...	Failed	Invalid credentials.
Error	Client Login	Control Room	Ellie Brown	PRODUCTLT07	2015-09-14 15:16:58 p...	Failed	Invalid credentials.
Error	Client Login	Control Room	Ellie Brown	PRODUCTLT07	2015-09-14 15:15:38 p...	Failed	Invalid credentials.
Error	Client Login	Control Room	Ellie Brown	PRODUCTLT07	2015-09-14 15:15:37 p...	Failed	Invalid credentials.
Information	Set Password	Control Room	Ellie Brown	PRODUCTLT0...	2015-09-14 15:13:34 p...	Success	Password set successfully
Information	Add User	Control Room	John Smith	PRODUCTLT0...	2015-09-14 15:08:03 p...	Success	User Shelly PB added successfully
Information	Add User	Control Room	John Smith	PRODUCTLT0...	2015-09-14 15:07:12 p...	Success	User Elliot TS added successfully
Information	Add User	Control Room	John Smith	PRODUCTLT0...	2015-09-14 15:04:43 p...	Success	User Mike Lee added successfully
Information	Add User	Control Room	John Smith	PRODUCTLT0...	2015-09-14 15:03:57 p...	Success	User Amy Chen added successfully
Information	Add User	Control Room	John Smith	PRODUCTLT0...	2015-09-14 15:02:58 p...	Success	User Tom Watson added successfully
Information	Add User	Control Room	John Smith	PRODUCTLT0...	2015-09-14 15:02:07 p...	Success	User Ellie Brown added successfully
Information	Update Role	Control Room	John Smith	PRODUCTLT0...	2015-09-14 14:49:36 p...	Success	Role updated successfully
Information	Update Role	Control Room	John Smith	PRODUCTLT0...	2015-09-14 14:49:30 p...	Success	Role updated successfully
Information	Add Role	Control Room	John Smith	PRODUCTLT0...	2015-09-14 14:49:17 p...	Success	Role added successfully
Information	Add Role	Control Room	John Smith	PRODUCTLT0...	2015-09-14 14:48:40 p...	Success	Role added successfully
Information	Add Role	Control Room	John Smith	PRODUCTLT0...	2015-09-14 14:39:09 p...	Success	Role added successfully
Information	Add Role	Control Room	John Smith	PRODUCTLT0...	2015-09-14 14:38:31 p...	Success	Role added successfully
Information	Add Role	Control Room	John Smith	PRODUCTLT0...	2015-09-14 14:38:05 p...	Success	Role added successfully
Information	Add Role	Control Room	John Smith	PRODUCTLT0...	2015-09-14 14:32:17 p...	Success	Role added successfully
Information	Set Password	Control Room	John Smith	PRODUCTLT0...	2015-09-14 14:25:09 p...	Success	Password set successfully
Information	Add User	Control Room	John Smith	PRODUCTLT0...	2015-09-14 14:24:04 p...	Success	User John Smith added successfully
Information	Email Setting	Control Room	Anonymous	PRODUCTLT0...	2015-09-14 14:23:14 p...	Success	Email Setting saved successfully

You can export and save the Audit Trail data to a CSV file by clicking .

Also, if a Client gets disconnected while the task is being executed, there appears an entry in the Audit Trail log pertaining to details such as: Client name that got disconnected, the exact time and what is the last step that was executed before the Client got disconnected.

If a Client resumes connection while the task is being executed, there appears an entry in the Audit Trail log showing that it has been reconnected, pertaining to details such as: exact time and step at which it resumed the task execution.

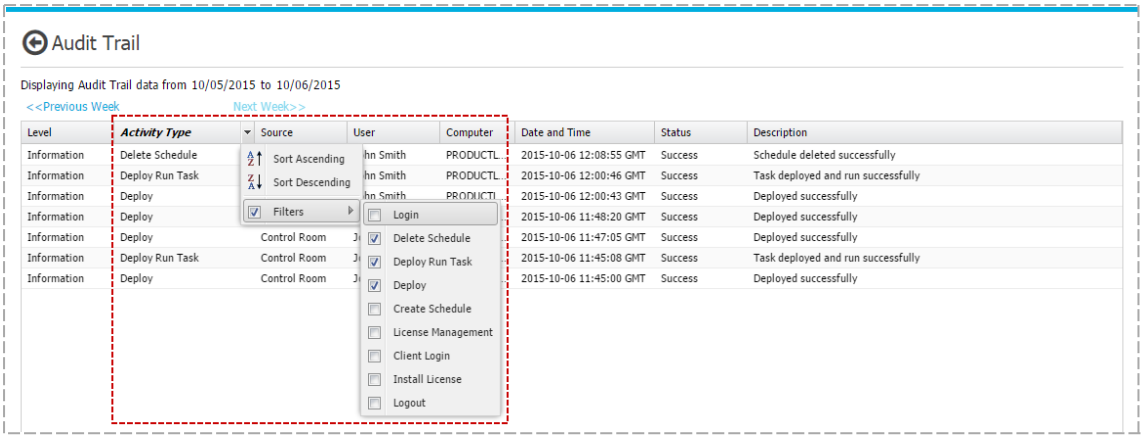


Level	Activity Type	Source	User	Computer	Date and Time	Status	Description
Information	Run Task	Client	RuntimeClient	engglt46.aaspl-brd.com	2016-09-21 16:00:37 IST	Success	Task 'Prompt.atmx' completed. Run duration 00:03:07
Information	Run Task	Client	RuntimeClient	engglt46.aaspl-brd.com	2016-09-21 16:00:37 IST	Success	Task 'Prompt.atmx' completed. Run duration 00:00:13
Information	Client Connection	Control Room	-	ENGGLT46	2016-09-21 16:00:35 IST	Success	Client 'ENGGLT46' re-connected. The status of the task 'Copy of Loops' deployed on this Client on reconnect is...
Information	Client Connection	Control Room	-	ENGGLT46	2016-09-21 15:58:18 IST	Failed	Client 'ENGGLT46' disconnected. The status of the task 'List-Variable' deployed on this Client at the time of disc...
Information	Client Connection	Control Room	-	ENGGLT46	2016-09-21 15:58:18 IST	Failed	Client 'ENGGLT46' disconnected. The status of the task 'Copy of Loops' deployed on this Client at the time of di...
Information	Client Connection	Control Room	-	ENGGLT46	2016-09-21 15:58:18 IST	Failed	Client 'ENGGLT46' disconnected. The status of the task 'List-Variable' deployed on this Client at the time of disc...

Adding Filters

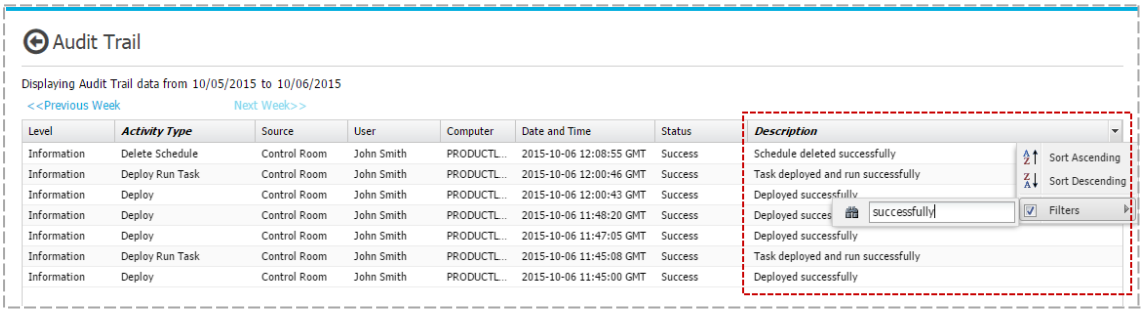
You can filter the 'Audit Trail' data as per your requirement. Apply filters to view activities for specific week and data types. Also sort the data in 'Ascending' or 'Descending' order.

- To view activities for a specific week click <<Previous Week and Next Week>> to arrive at the week you are looking for.
- To sort the data, click on the arrow given in column(s) and click Sort Ascending or Sort Descending.
- Now, to view data of specific type, enable 'Filters' and either select from available list and/or search using keywords.



Note: If you apply a filter, the column name is displayed in bold italics.

- For instance, apply filters to the 'Activity Type' column to display data relevant to 'Delete Schedule', 'Deploy Run Task' and 'Deploy' (refer above image). Subsequently, filter the data for 'Description' by using the search text option:



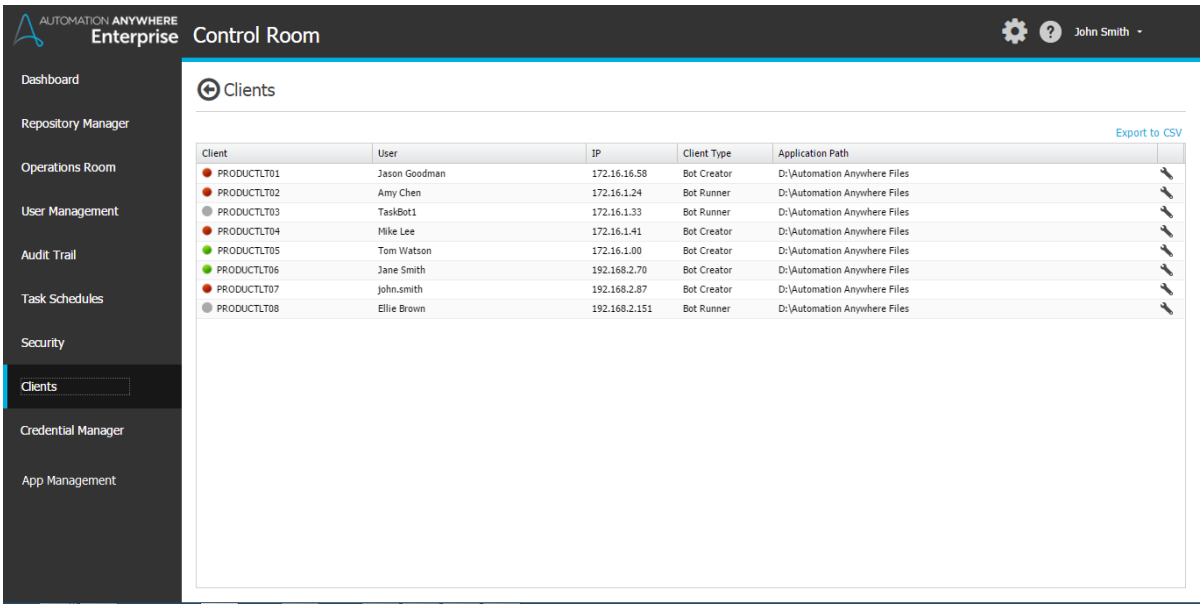
Note: The filtered view remains unchanged even after switching between consoles.

Next...

You can view and manage Client relevant details in the Clients console. Learn More

Managing Clients

Client relevant details are displayed in the Clients console. Details such as the Client status, Client HostName, User, IP and Application Path - where Automation Anywhere files such as tasks, reports, workflow are stored, can be viewed by the Control Room Administrator and Users with access to the console.



Viewing and Updating Client Information

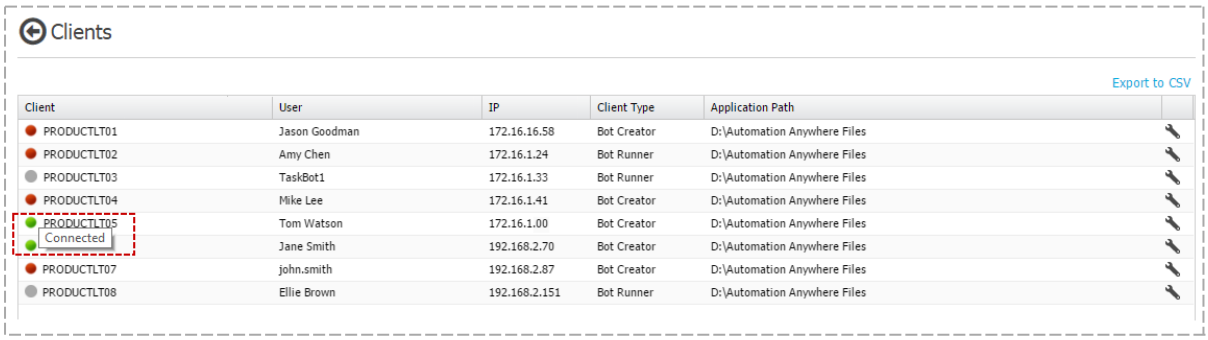
You can view whether a Client is connected and active or not based on the icons that appear before the Client name.

indicates the Client is active and connected,

indicates the Client is active but disconnected

indicates the Client has been deactivated by the Control Room Administrator.

Tip: The tool tip ' Connected ' or ' Disconnected ' indicates Client status:



Exporting Client Details to CSV

The Client details can be exported to a CSV file for data sharing by the Control Room administrator or a User with Client Management permission. For instance, you can view the status of Clients; whether 'Active', 'Disconnected' or 'Deactivated' in the CSV file.

To export user details, click on Export to CSV at the top right:

Export to CSV

Next…

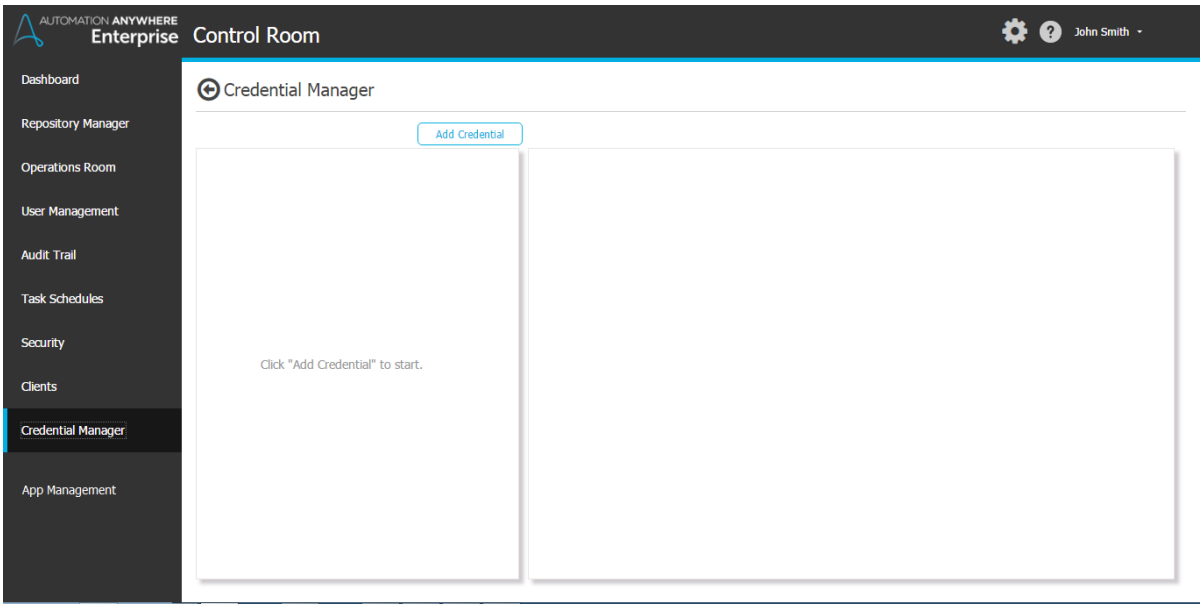
You can manage Credentials using the Credential Manager. Learn More

Defining Credential Keys in Credential Manager

Available with Enterprise Edition from version 10.2.1

The Credential Manager is a centralized location for securely creating and storing sensitive information that is included in automation tasks in the form of Credentials.

The Credential Manager allows you to add a Credential Key and Attributes in the Control Room Credential Vault that can be assigned in commands as Credential Variables. Learn More.



Benefits of Defining Credentials

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.

Defining the Credential Keys and Attributes

The Credential Manager is visible only to the Control Room administrator or anyone who has the required access privileges.

To define Credentials, you will have to build a repository of Credential Keys and its Attributes.

Creation of Credential Keys involves providing a Key Name, its Description (optional) and its Attributes. The Attributes hold the key information regarding the credentials that are being used such as hostname, servername, username, password; in fact any information that involves use of credentials.

Tip: It is recommended you first identify the Credentials that are required in different commands.

A. Adding Credentials

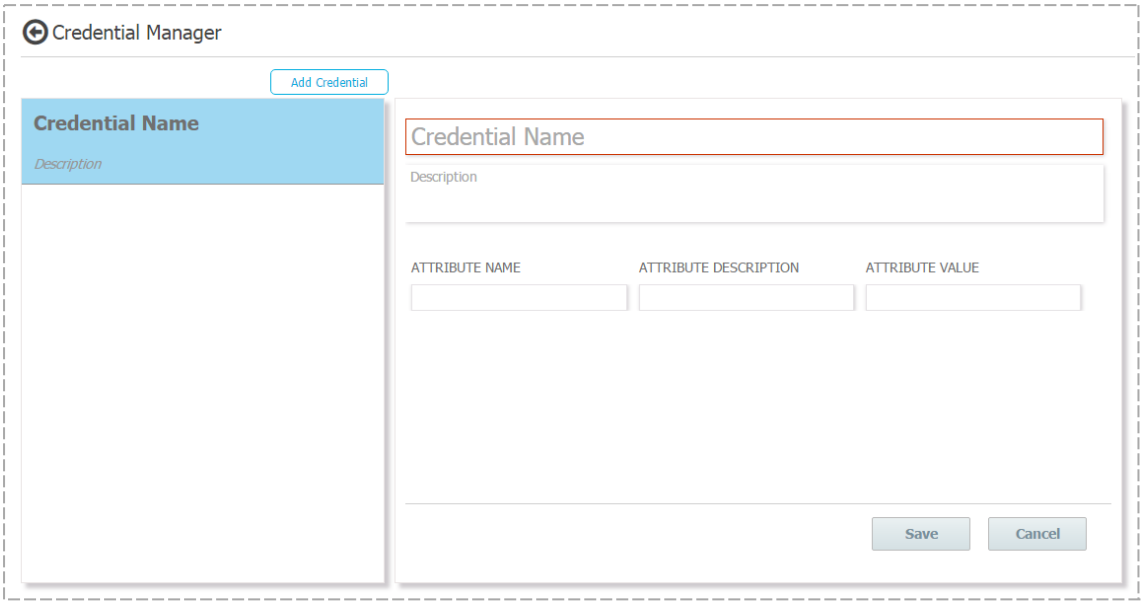
You can add a Credential, which comprise Key-name and its Description as well as the Attribute Name, its Description and Values.

1. To add a Credential, click on the 'Add Credential' button given at the top of the Credentials list.

   Add Credential

2. Provide a name in the 'Credential Name' field that reflects the purpose of the Credential key and optionally its Description.

3. Define the Key's Attributes - Name, Description and Value.



Note: Description is optional.

4. Click Save.

B. Editing Credentials
You can edit a Credential Name and its Description as well as the Attribute Name, its Description and Values.

Note that when you edit an Attribute Name, the Control Room performs two operations; it first deletes the first instance of attribute and then creates a new attribute.

1. To edit a Credential, select the Credential Key from the list and Click on

2. Save once it's modified.

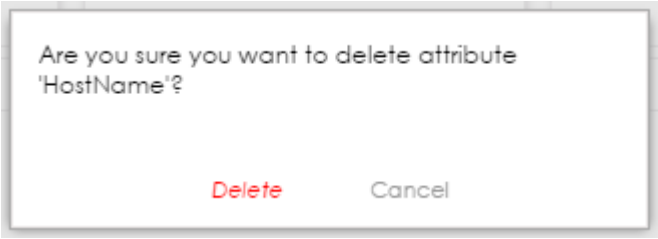
C. Deleting Credentials and its Attributes
You can delete a Credential Name and its Description as well as the Attribute Name, its Description and Values. You can opt to remove only Attributes or the Key itself.

- **Deleting an Attribute**

    1. To remove a Credential Attribute, click on

2. Select ⊖ (available at the end of each Attribute label).

3. Confirm



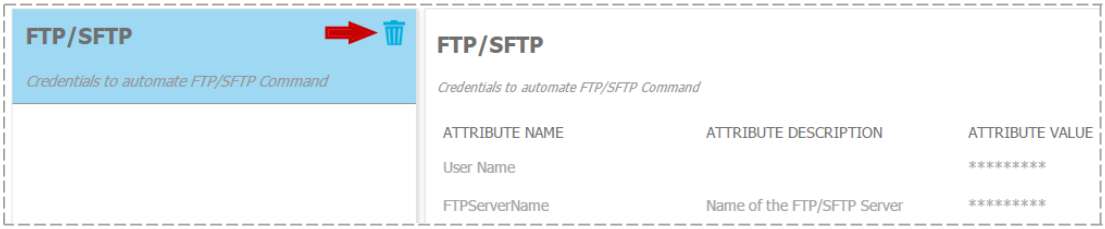
4. Save.

- **Deleting a Credential**

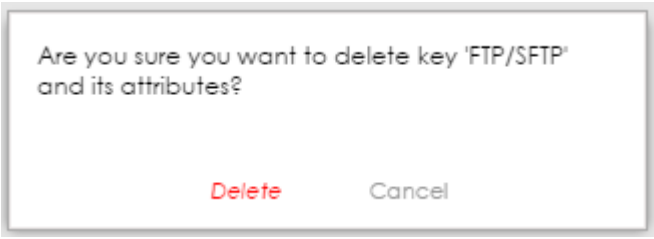
1. To delete a Credential, select the Credential Key from the list.

> ⚠ **Important:** Remember, if you remove the Key, all Attributes are deleted.

2. Click on 🗑 at the top .



3. Confirm



Next...

You can configure and manage Control Room settings. Learn More

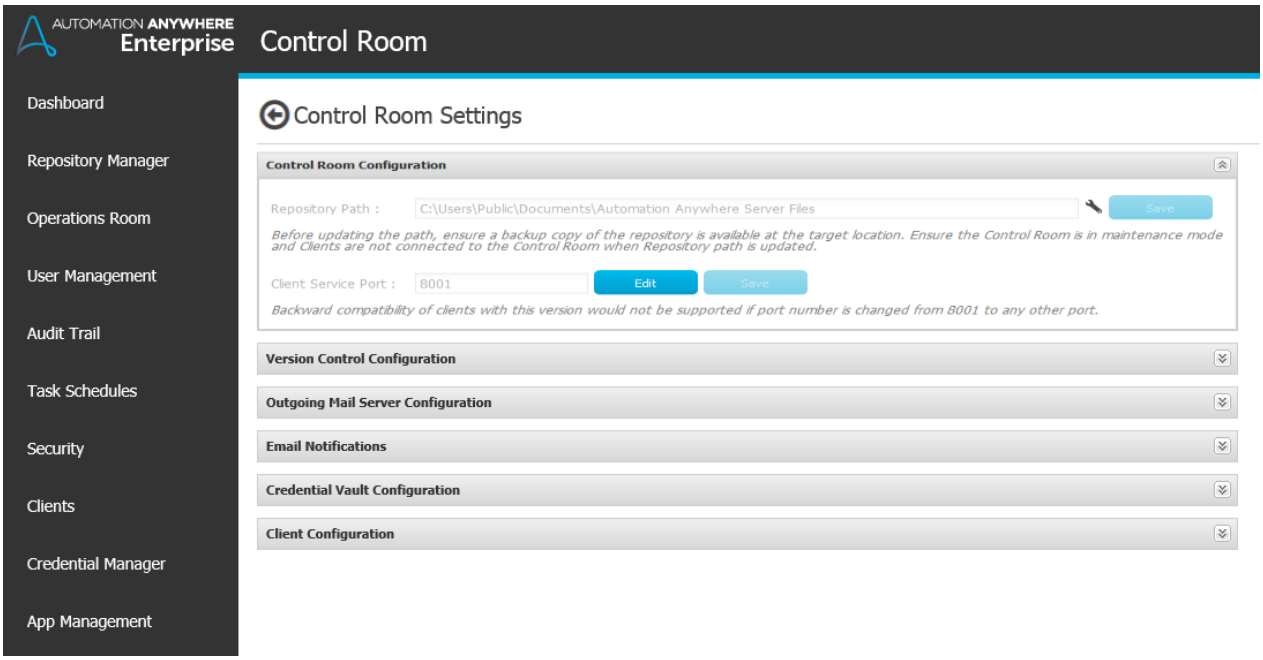
Section 2: Control Room - Manage

Control Room Settings

Users with admin privileges can configure and update settings for Control Room such as Repository Path, WebSocket Service, Control Room Access URL, Version Control, Outgoing Mail Server, Email Notifications, Credential Vault, and URLs for Client Configuration.

To update Control Room Settings click on the Settings icon given at the top right corner:

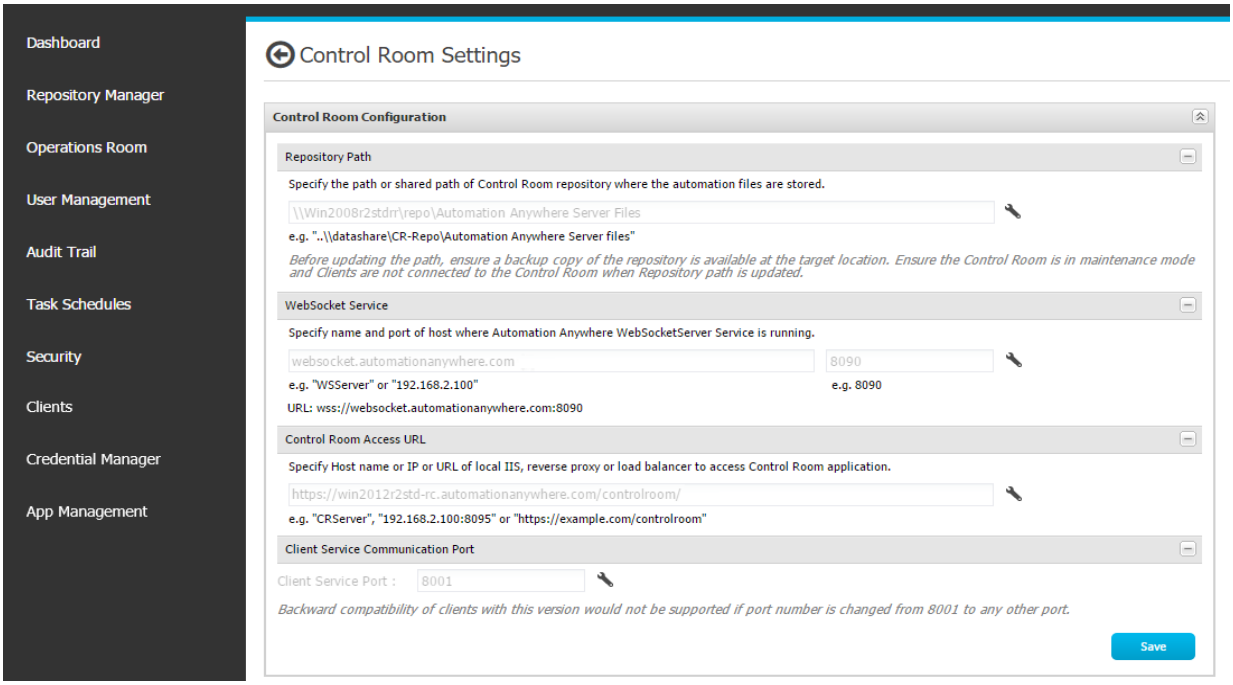
This will launch the Control Room Settings page:



(Control Room as seen in Custom - Standalone Mode of Installation)

If you have configured the Control Room environment for high availability using distributed installation type*, your Control Room displays:

* Available in Enterprise edition from version 10.1.0



(Control Room as seen in Custom - Distributed Mode of Installation)

Here, you can,

1. Configure Control Room Components
2. Configure Version Control
3. Configure Mail Server Settings
4. Enable or Disable Email Notifications
5. Configure Credential Vault

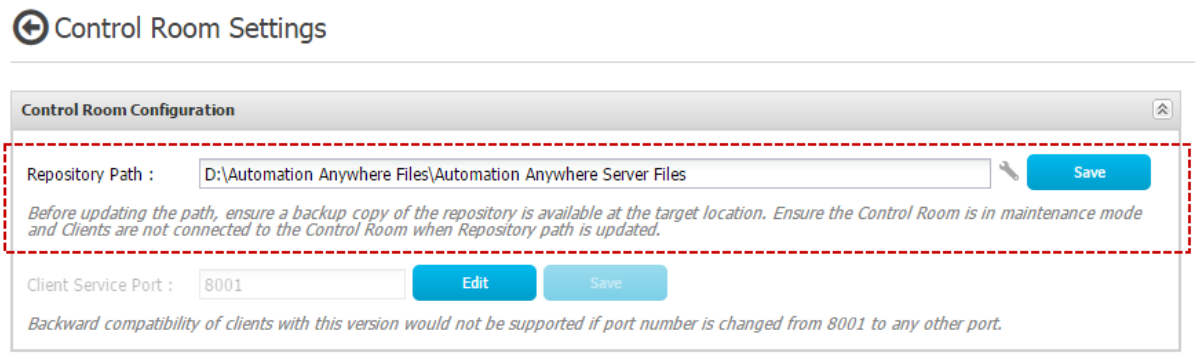
Configuring Control Room Components

Use this option to configure settings for different components of the Control Room - Repository Path, Client Service Port, WebSocket Service, and Control Room Access URL.

1. Changing the Repository Path and Client Service Port

- The 'Repository Path' is the shared path of Control Room repository where physical files are stored.
- The ''Client Service Port' is the default port used to communicate with the Enterprise Client.

Changing Repository Path for Standalone Installation - When the Control Room is configured using the Standalone mode of installation, you can opt to update the Repository Path. While updating the repository path, you must ensure that the files in the earlier repository path are manually copied to the newer one. Also, you can map the path to a folder for which you have access privileges.

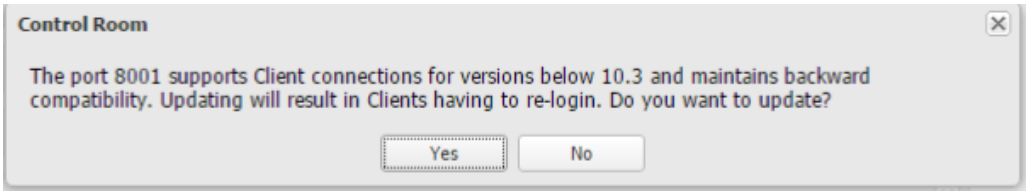


Important: It is recommended that you reconnect to the Version Control System when you change the Control Room repository.

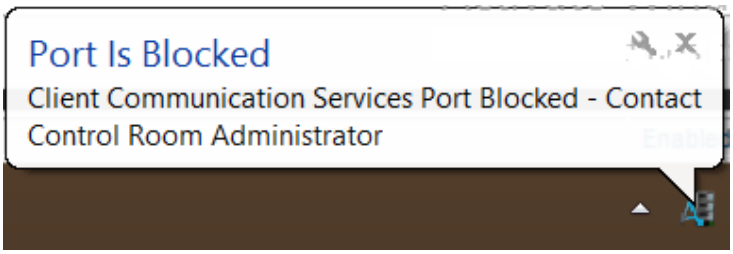
Configuring Client Service Port

The port number is configurable by the Control Room administrator. Although, the default port will be displayed as 8001. The Control Room administrator has the flexibility to edit the default port number and save it.

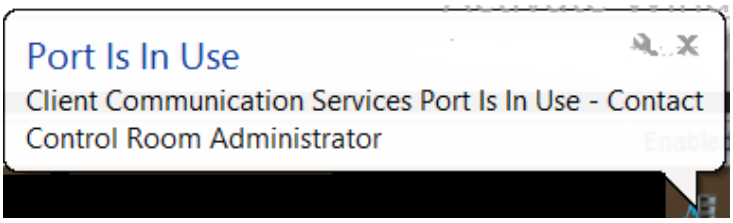
Also, Control Room admin receives a prompt for confirmation before saving any changes to the port.



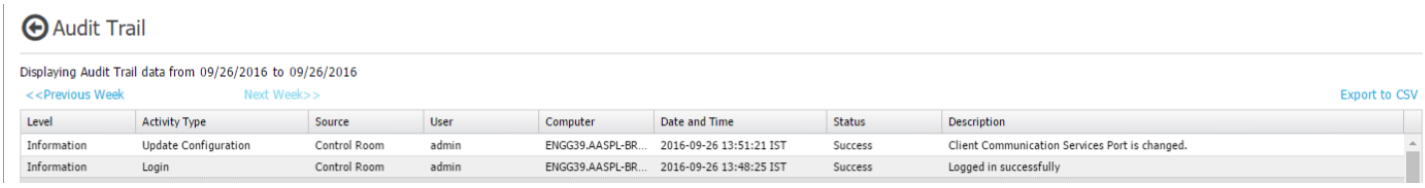
If the newly defined port is blocked on the Client side, then a notification is prompted to the Client user informing that the port is blocked. Also, the following pop-up message appears:

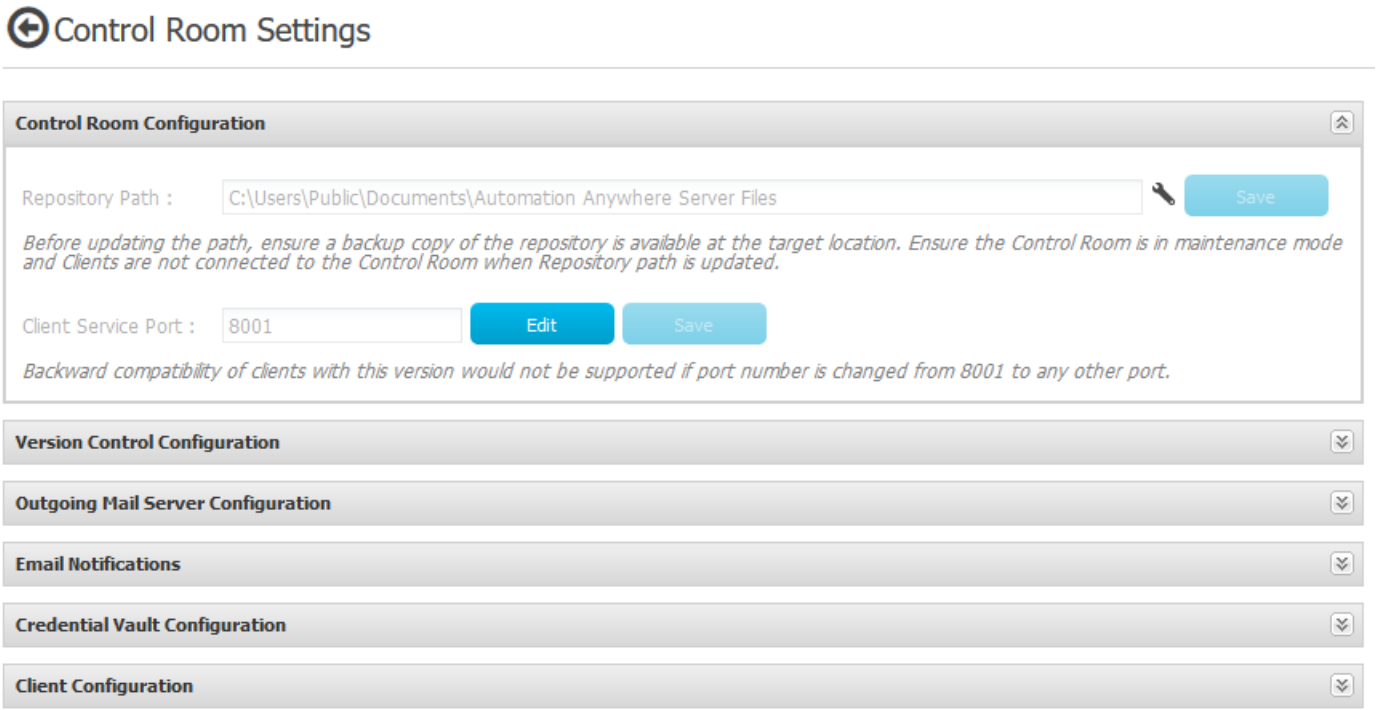


If a port is in use by some other services then the following pop-up appears:

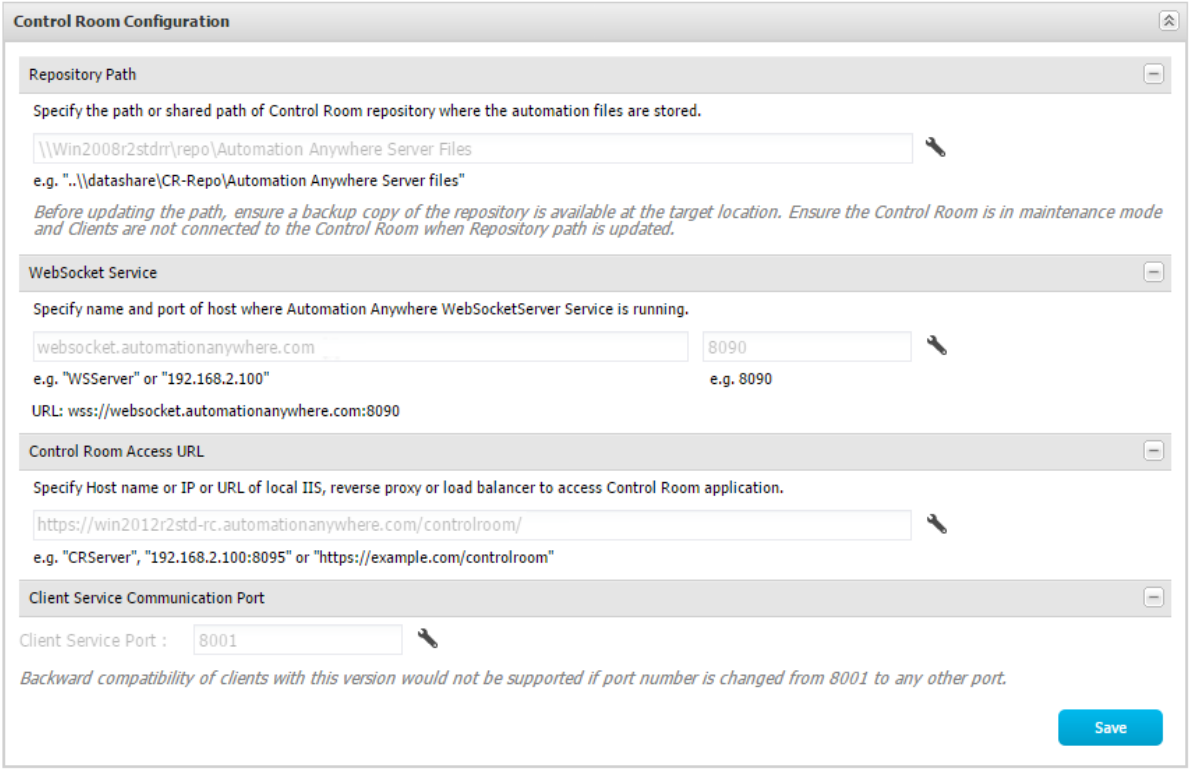


If you make changes in the port number an audit entry appears in the Control Room as "Client Communication Services Port is changed"





Changing Repository Path for Distributed Installation - When the Control Room is configured for high availability and disaster recovery using the Distributed Installation type, the settings for Repository Path, WebSocket Service and Control Room Access URL have to be filled in as soon as the Control Room is launched.



Important: It is recommended that you reconnect to the Version Control System when you change the Control Room repository.

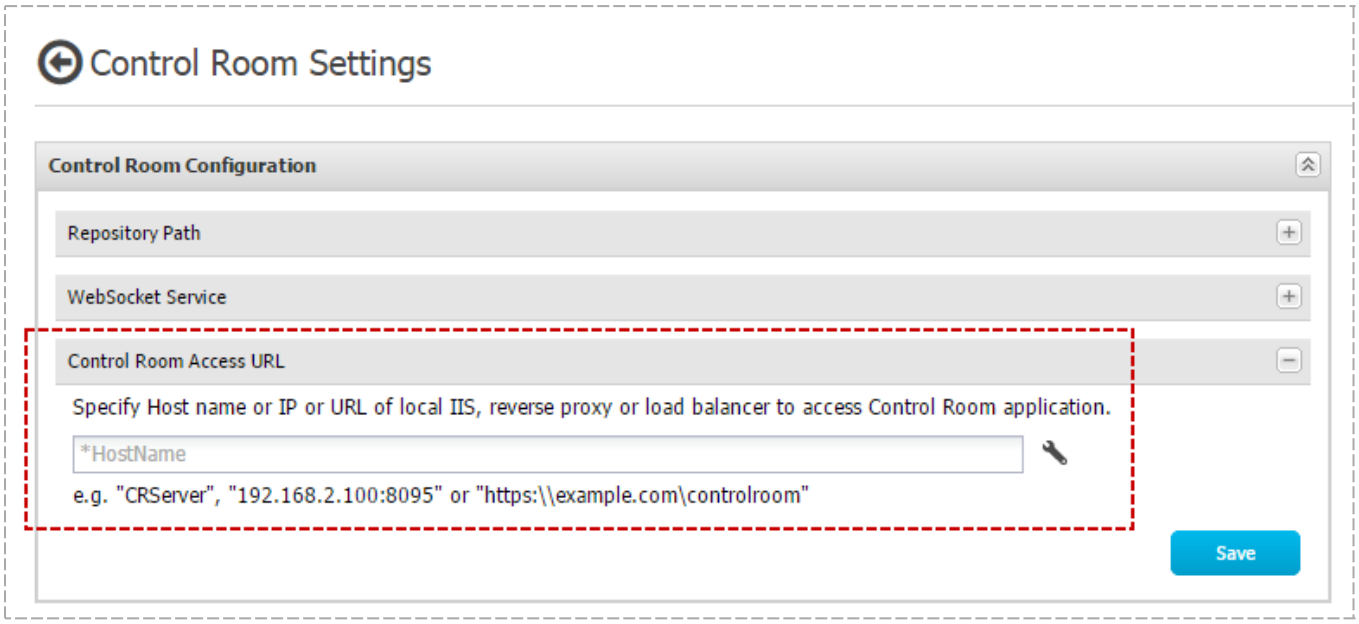
2. Specifying WebSocket Service Path

The WebSocket Service Path indicates the location of the machine from where the WebSocket service is hosted. Click on to open in edit mode and input the IP or Hostname and Port.

Note: It is mandatory to configure WebSocket Service and Control Room Access URL settings.

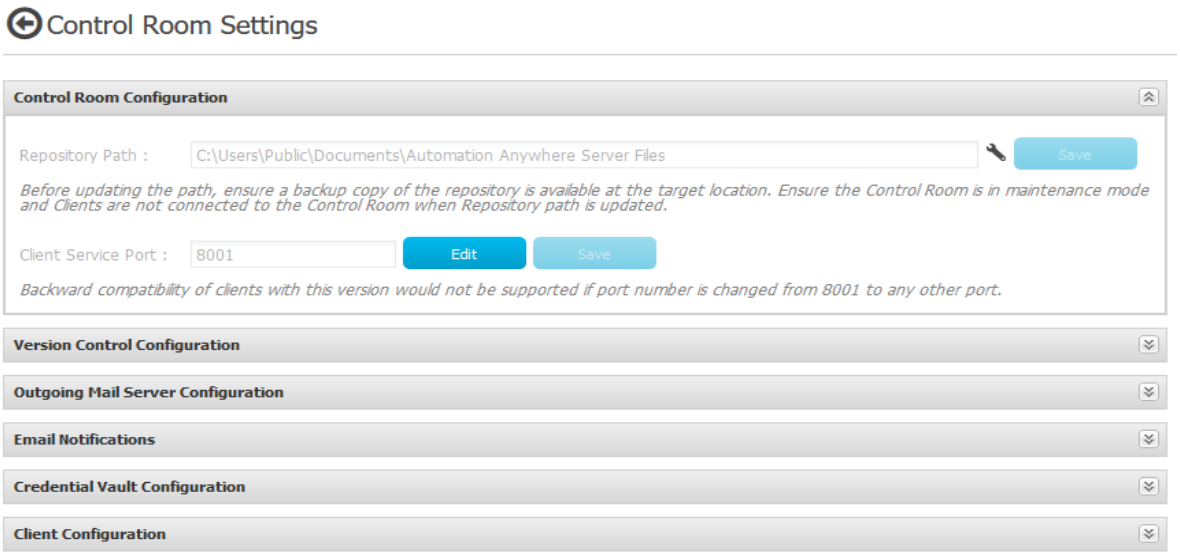
3. Specifying Control Room Access URL

The Control Room Access URL indicates the path to either local IIS, reverse proxy or load balancer - whichever is used for your web environment. Click on to open in edit mode and input the IP or Hostname and Port.



4.Setting the Client Services Communication Port in Control Room Settings

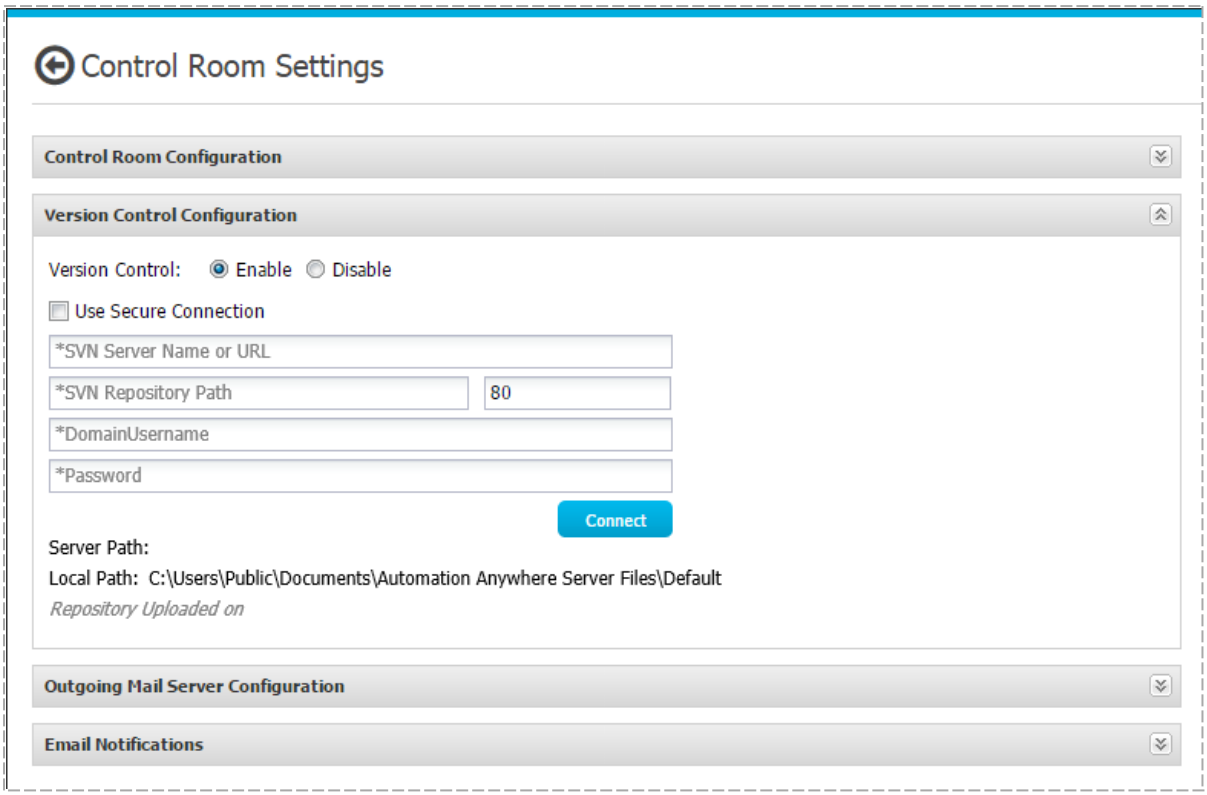
The port number is configurable by the Control Room administrator. Although, the default port will be displayed as 8001. The Control Room administrator has the flexibility to edit the default port number and save it.



Configuring Version Control

To manage controlled edits of files that could include TaskBots, VisionBots, Reports and Workflows, you can enable and configure the Version Control Settings.

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

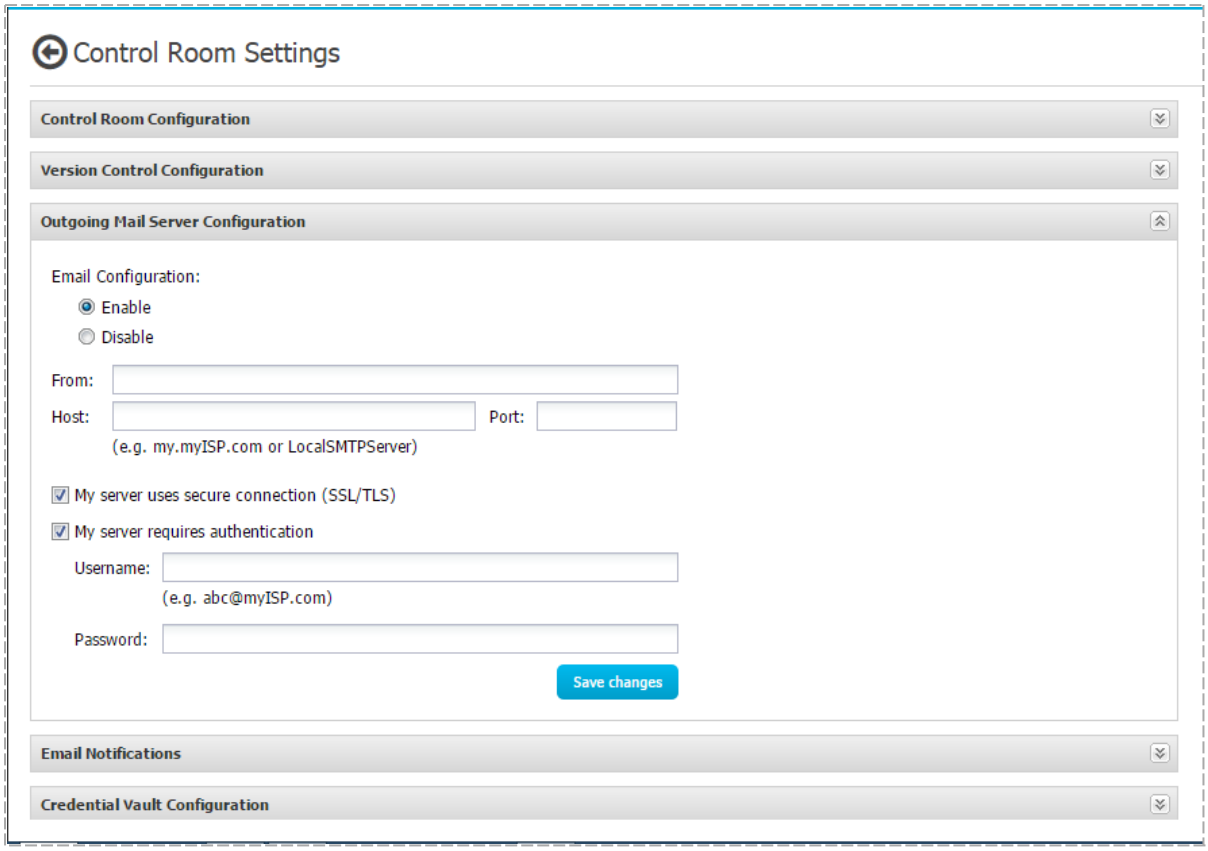


Learn More

Configuring Outgoing Mail Server

The outgoing mail server (SMTP server) that is used to send email notifications can be updated. You can update details such as From email id, Server hostname, Port number, User name, and Password.

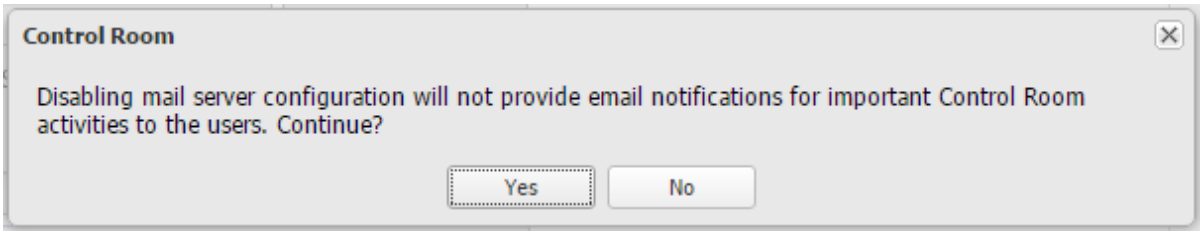
- **From -** input the email id of the admin user whose credentials shall be used to connect to the SMTP server. **e.g. cr_admin@automationanywhere.com**
- **Host -** input the hostname for the outgoing mail server. **e.g. smtp.automationanywhere.com**
- **Port number -** input the default port assigned to the SMTP server. **e.g. 587**
- **User name -** input the user name of the admin who shall login to the SMTP server. **e.g. John Smith**
- **Password -** input the password of the user specified in the 'User Name' field.



You can choose to 'Enable' or 'Disable' the 'Outgoing Mail Server' settings.

Tip: Disable email configuration only if your organization does not support the option.

Remember though, disabling this option will stop all email notifications that are sent to Control Room users regarding activities relevant to the Control Room.



Select the 'My Server uses a secure connection' option to establish a secure connection to the SMTP server.

Alternately, in case the SMTP server does not require authentication, disable the 'My server requires authentication' option to allow the Control Room to bypass authentication to the SMTP Server for sending email notifications.*

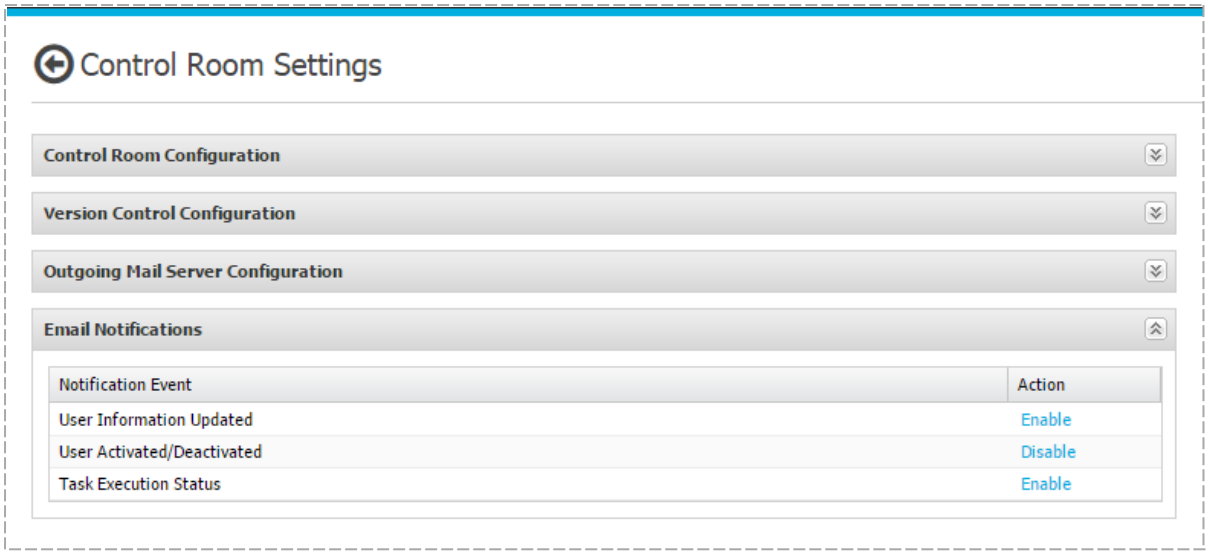
**Available from version 10.3*

Note: Both options are enabled by default.

On saving the configuration, the Control Room verifies the authentication details and provides the required response.

Enabling or Disabling Email Notifications

Email Notifications enables you to send notifications to Control Room users. You can opt to send these notifications by enabling any or all the 'Notification Events' available in the Email Notifications panel.



The following notifications can be sent to users:

1. **User Information Updated -** Enable this to send a notification to the Control Room user whose information such as First Name, Last Name, email address has been updated from Control Room → User Management page.

> Dear Mike Lee-Chang,
>
> Your Automation account user details have been modified.
>
> 1. First Name: Mike
> 2. Last Name: Lee-Chang
> 3. Email: mike.lee@automationanywhere.com
> 4. Role(s): Bot Creator
>
> For details, contact your Automation Admin.
>
> Regards,
> Automation Admin

2. **User Activated/Deactivated -** Enable this to send a notification to the Control Room user whose account is activated or deactivated from Control Room → User Management page.

> Dear Mike Lee-Chang,
>
> Your Control Room account Mike Lee has been activated.
>
> For details, contact your Automation Admin.
>
> Regards,
> Tom Watson|Admin

3. **Task Execution Status -** Enable this to send a notification to the Control Room user who has deployed a task from the Control Room → Repository Manager or Task Schedules. The notification is sent:
   a. If the task has failed to execute to the user who deploys or schedules the task. It also conveys the reason for task failure.

   Dear Ellie Brown,

   The task Variables.atmx set to run on Mike Lee at 2017-12-01 11:19:46 UTC has been aborted.
   For details, contact your Automation Admin.

   Regards,
   Automation Admin

   b. If the ask is 'Waiting for user input' and if the user does not handle that input such as a message box, prompt, and Automation Anywhere error message on the Bot Runner machine. The notification email in this case is sent out to the user who has deployed the task from Control Room and to the Bot Runner.

   Dear Ellie Brown,

   The task Prompt is waiting for user input onto your Bot Runner Mike Lee.
   Kindly do the needful.

   Regards,
   Automation Admin

Customizing email notifications

An email can also be customized to suit your requirements. To configure the same in html, open the email template in edit mode from:

```
<Application Path>\Automation Anywhere Enterprise 10.0\Web Control Room\Web\webcrsvc\App_Data\EmailTemplates
```

You can now choose to edit the format and language to suit your purpose.

UpdateUser.html

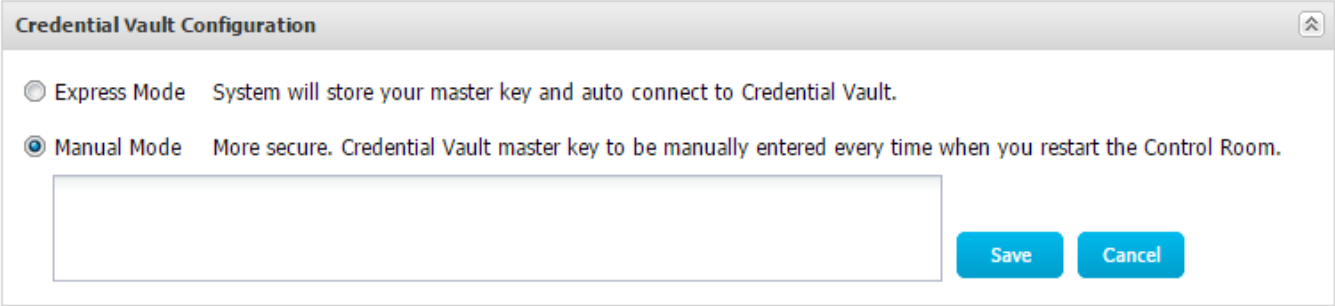
```
1  <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
2  <html xmlns="http://www.w3.org/1999/xhtml">
3  <head>
4      <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
5      <meta name="viewport" content="width=device-width, initial-scale=1.0" />
6  </head>
7  <body>
8      <div>Dear #Name#, </div>
9      <div> </div>
10     <div>Your Automation account user details have been modified.</div>
11     <div> </div>
12     <div>1. First Name: #FirstName# </div>
13     <div>2. Last Name: #LastName# </div>
14     <div>3. Email: #Email#  </div>
15     <div>4. Role(s): #UserRoles#  </div>
16     <div> </div>
17     <div>For details, contact your Automation Admin.</div>
18     <div> </div>
19     <div> Regards, </div>
20     <div> Automation Admin </div>
21 </body>
22 </html>
```

⚠ Do not change the variables - denoted within '#' as these values are pre-defined in the application.

Configuring the Credential Vault

Available from version 10.2.1

The Credential Vault is a centralized location for securely storing credential information used in automation tasks. To configure settings for Credential Vault, a Super Admin has to choose between Express or Manual mode.

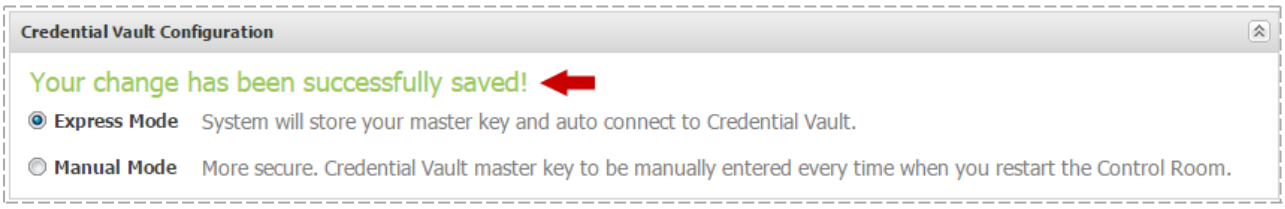


- **Express Mode -** Use this to auto connect to the Credential Vault with the master key that is stored in the system during Control Room configuration.
- **Manual Mode -** Use this to manually connect to the Credential Vault using the master key that was available during Control Room configuration.

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

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. A successful switch is denoted with:



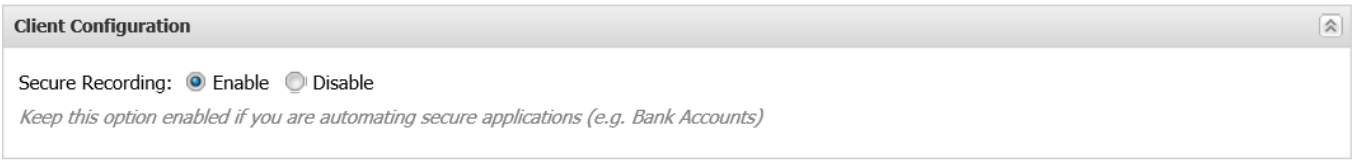
> **Important:** For some reason, if you must retrieve the master key, it is stored in the 'CredentialVault.dat' file of the repository path provided you have configured directly in Express mode or have upgraded from AAE 10.2.0 to the current version.
>
> **E.g.** C:\Users\Public\Documents\Automation Anywhere Server Files\CredentialVault.dat

Client Configuration

1. Secure Recording

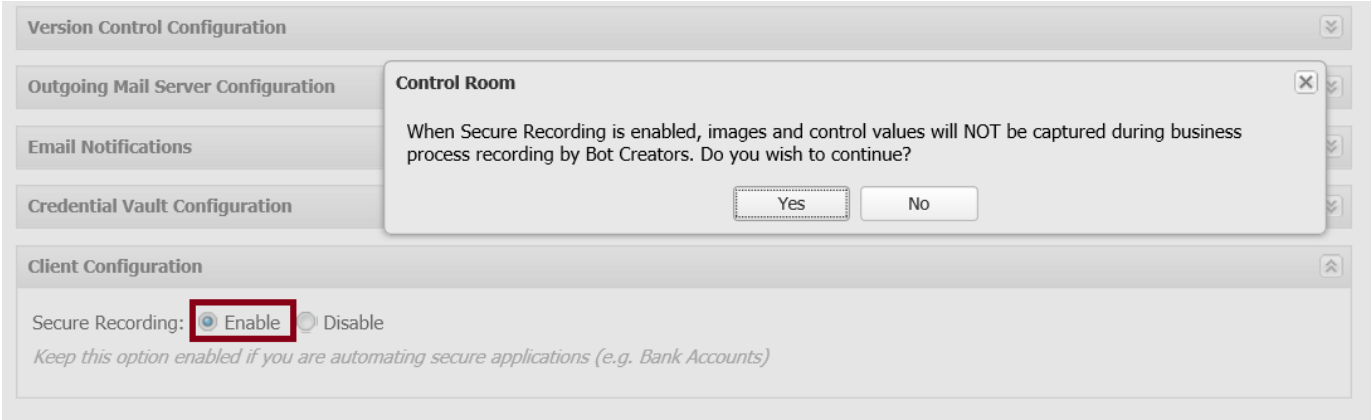
Client Configuration enables you to control the mode of recording done by a Client for business processes. If the process requires a secure mode of recording, you can 'Enable' the 'Secure Recording' mode. This ensures none of the objects and properties that comprise sensitive information are captured.

Control Room Administrator can select in the Control Room Setting> Select Client Configuration, where an option of Secure Recording is available.



Note: Default mode selected is 'Disable'.

When you **'Enable',** Control Room Administrator receives the following prompt:



If the Administrator, clicks on 'Yes' the setting is enabled and if the Administrator clicks on 'No', then the setting remains disabled.

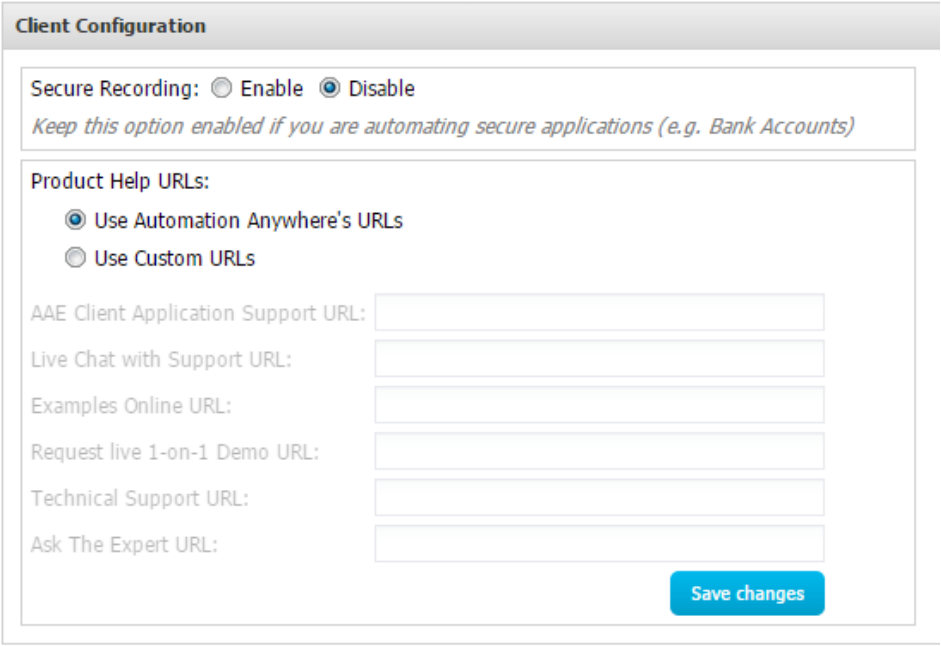
When you**'Disable'**, Control Room Administrator receives the following prompt:

If the Administrator, clicks on 'Yes' the setting is disabled and if the Administrator click on 'No', then the setting remains enabled.

In **Control Room Settings> Client Configuration,** Product Help URLs enables you to redirect links to Automation Anywhere Support Site or you can redirect to any Custom URL of your choice.

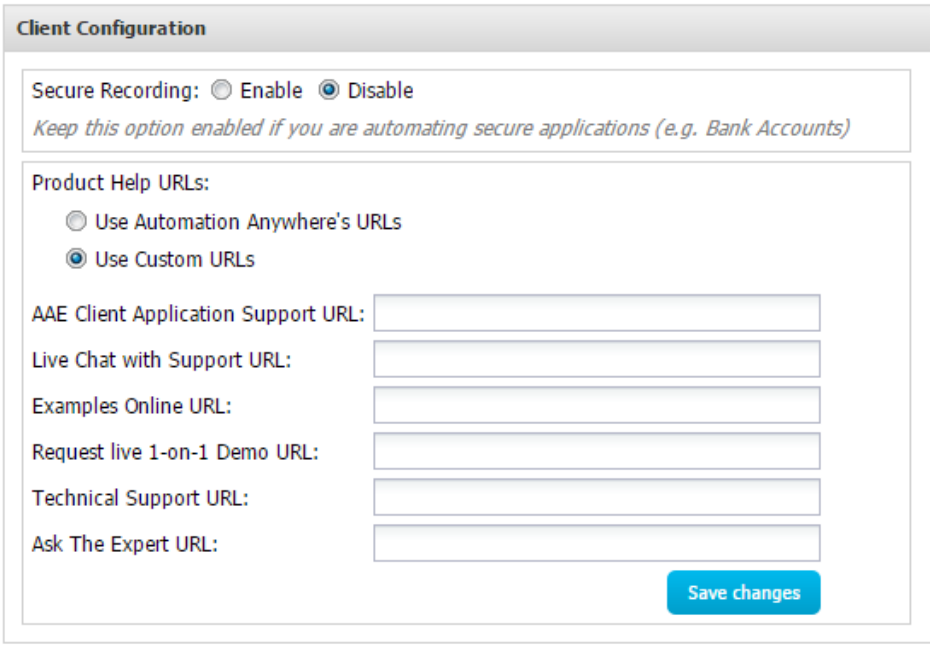
- **Use Automation Anywhere's URLs**

  If you Click on *Use Automation Anywhere'S URLs*, you are navigated to the default Automation Anywhere Support site. This disables all the other options such as Live Chat with Support URL etc.



- **Use Custom URLs**
  ** Available in Enterprise Edition 10 SP2 with product version 10.5.0*

  A user can change the default Automation Anywhere URLs (AA Support site) to any other Custom URLs for Product Help in **Control Room Settings > Client Configuration**. This allows you to navigate users in the Automation Environment to the local support and access help from in-house Automation Experts.



Note: Changes will not be saved unless you click on **Save changes**

The fields of the **Client Configuration> Product Help URLs** are described in the following table:

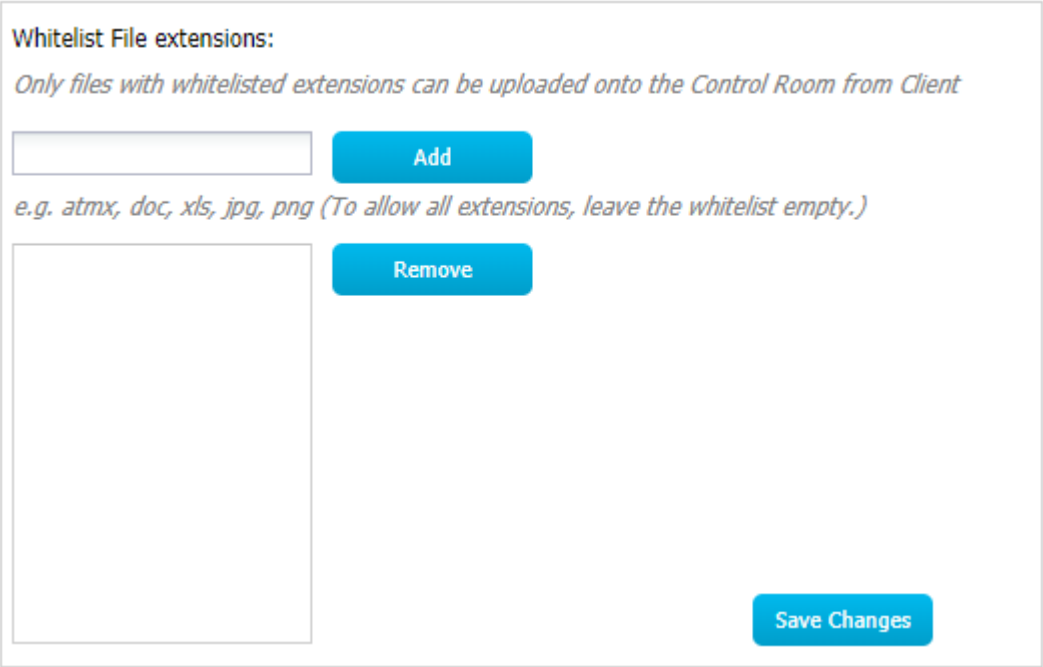
Field	Description
AAE Client Application Support URL	It allows you to add your customized Product Help URL and re-direct users to your in-house support site.
Live Chat with Support URL	It allows you to access in-house Live Chat and speak to online Experts.
Examples Online URL	It allows you to look for available Online Examples.
Request live 1-on-1 Demo	It allows you to request for live demonstration of features and experts would answer your

URL	questions.
Technical Support URL	It allows you to access in-house Technical Support.
Ask the Expert URL	It allows you to speak to an expert and get their expert advice.

Whitelist File Extensions to Prevent Uploading of Malicious Files

** Available in Control Room10.5.9 and later*

To prevent uploading of malicious files on Automation Anywhere Enterprise Client, the Control Room administrator uses Whitelist File Extensions feature. The Control Room administrator can add the file extensions that need to be whitelisted from Client. Client users can upload only whitelisted file extensions included in this list.



To include file extensions to the whitelist:

1. Log into the Control Room.
2. Click on Cog symbol and select **Control Room Settings** on the top right of the Control Room window.
3. Click on in the **Client Configuration** section.

4. Scroll down to the **Whitelist File extensions** section.
5. Enter the extension that you want to whitelist and click **Add**.

The extension is added in the list box.

Note: If you want to remove any file extension, click **Remove.**

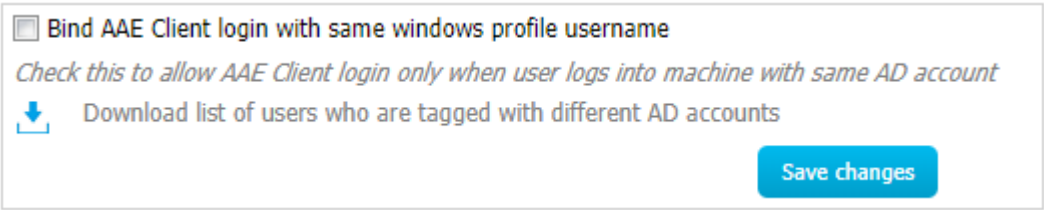
Click **Save Changes**.

Configuring Client Configurations Settings

The Control Room administrator can configure the **Bind AAE client login with same windows profile username** option and thus allow or prevent the newly created users to log into AAE Client only when their Control Room user name is same as their windows username. Select this check box if you want to allow users to log into AAE Client and if you want to prevent users from logging into AAE Client, then clear this check box.

This ensures that users are prevented from logging into AAE Client within any other user's Windows session and thus it provides an extra layer of security. By default, this option is cleared.

Note: The change in this option is applicable to only newly created users for Active Directory (AD) set up and 10.5.x and 10.7.x AAE Clients.



Version Control Integration

To manage controlled edits of files that could include TaskBots, VisionBots, Reports and Workflows, you can configure Version Control in Control Room Settings page.

The Control Room is tightly integrated with SubVersion version control system so that the versioning, check-in/checkout and other functionality can be leveraged with ease for all files.

Version Control Pre-requisites

1. 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 v1.8.13 and v1.8.14 with Visual SVN Server 3.3.x.

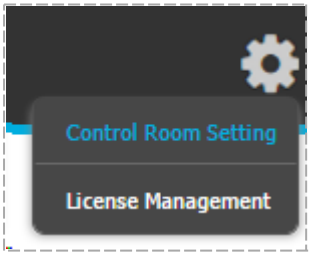
2. An SVN Administrator user should be created with required permissions.
3. An SVN repository should be created, which can be used to store all version control files.
4. Control Room will be the basis of communication with SVN. Clients will not communicate with SVN directly.

   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.

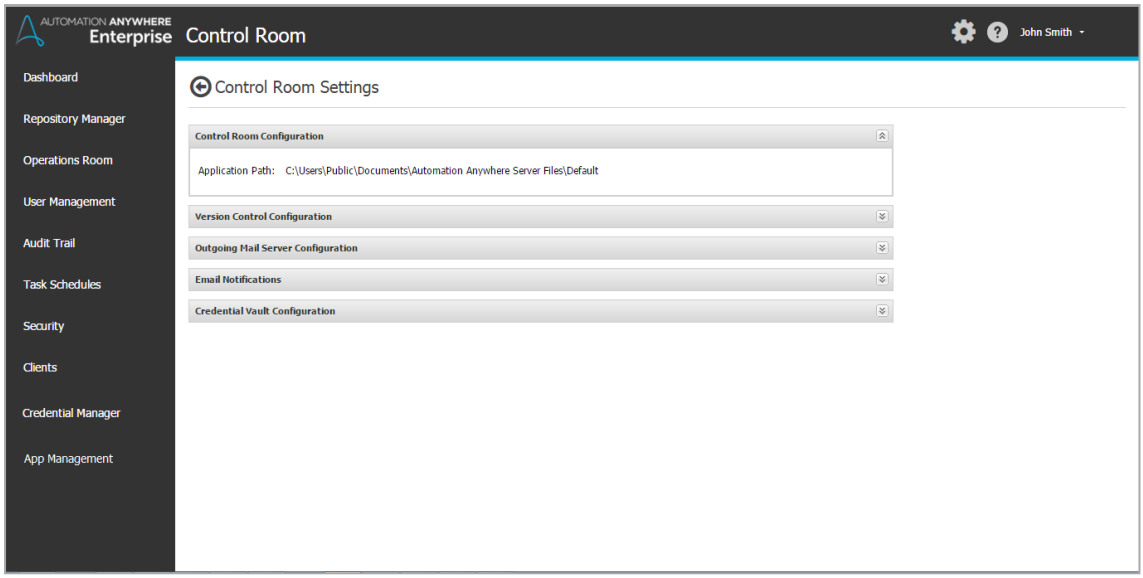
Enabling 'Version Control'

To be able to use 'Version Control' you need to 'Enable' the feature from the Control room. Follow the below mentioned steps to enable Version Control:

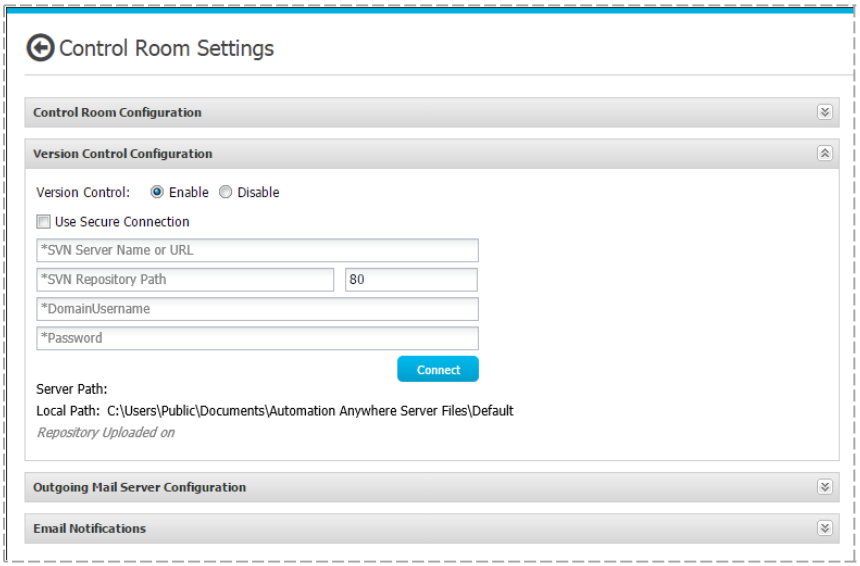
1. Click on button on the top right on the Control Room panel and select Control Room Settings.



   Following image shows the default view of the Control Room Settings.



2. Click on Version Control Settings tab.

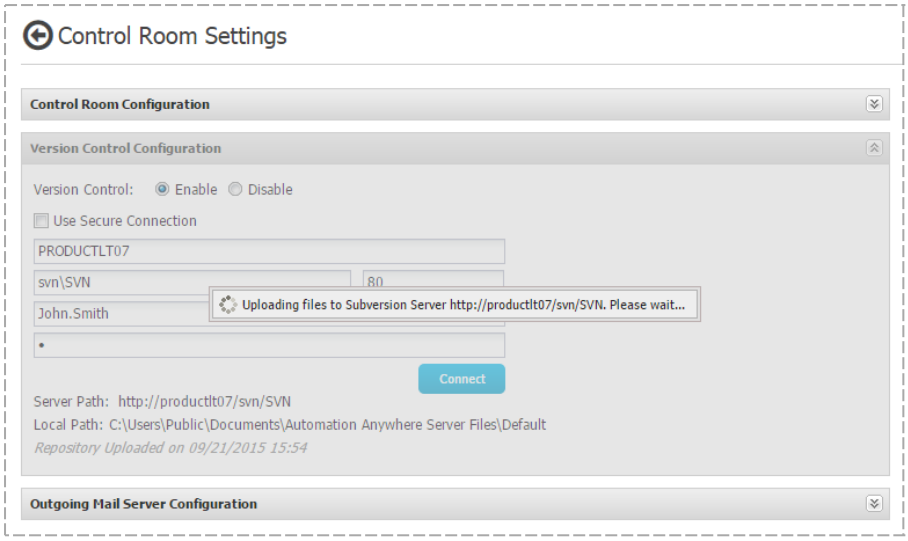


3. Input the required details and click 'Connect'.
4. Once the connection is established successfully, the Server path will be auto-populated.

Uploading the Base Version

Though creating base version is optional, for existing users it is highly recommended as the first step towards versioning.

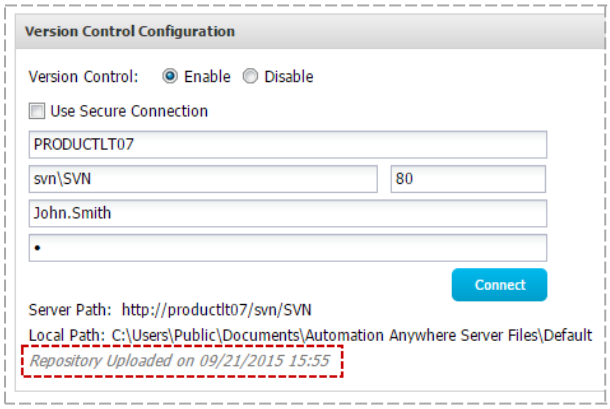
When a Client performs the first version control operation on a file, it will automatically be reflected in the Version Control Repository.



Note: The upload Date and Time are displayed after the files are uploaded to SVN.

The total files on SVN will be same as the Repository Manager.

Note: Uploading base version may take time since it depends on the size of local repository being uploaded. Once the uploading is completed, the time-stamp is set beside the Upload files link for the last upload process.

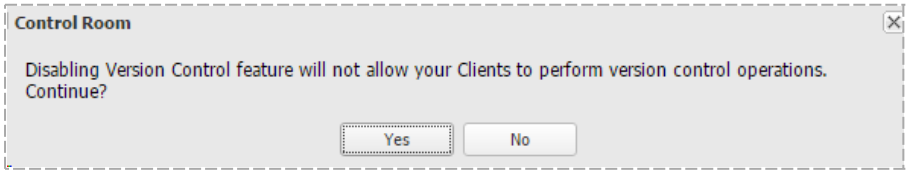


Important: It is recommended that you reconnect to the Version Control System when you change the Control Room repository.

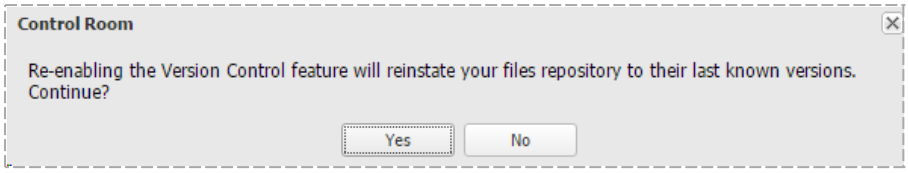
Disabling Version Control

The Control Room Super Admin has the privilege of disabling and re-enabling the Version Control feature.

Clicking 'Disable' will not allow Clients configured to the Control Room to perform versioning operations such as Check Out, Upload Files, Upload Comments and view Version History.



Note: It's possible to re-enable Version Control at a later stage if required. Simply click 'Enable' to continue using versioning operations from where you left off!



Note: Disabling Version Control will also disable the Configure and Upload files link.

Allocation and Management of Licenses

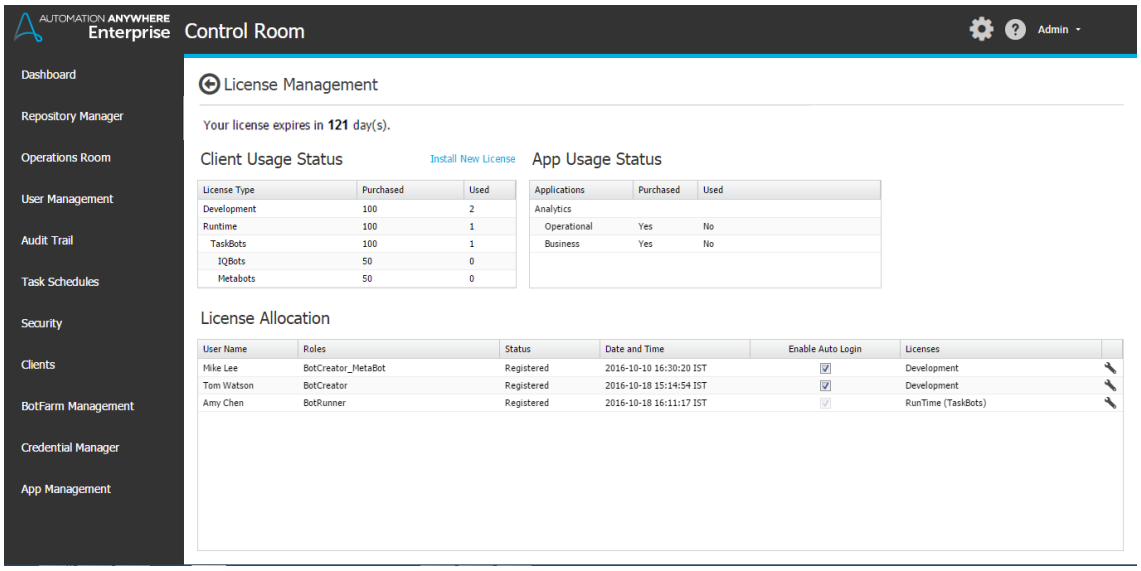
The Control Room administrator manages the installation, distribution and allocation of licenses to Clients. Two aspects of Licensing can be managed from the License Management console:

- New License Installation
- License Allocation

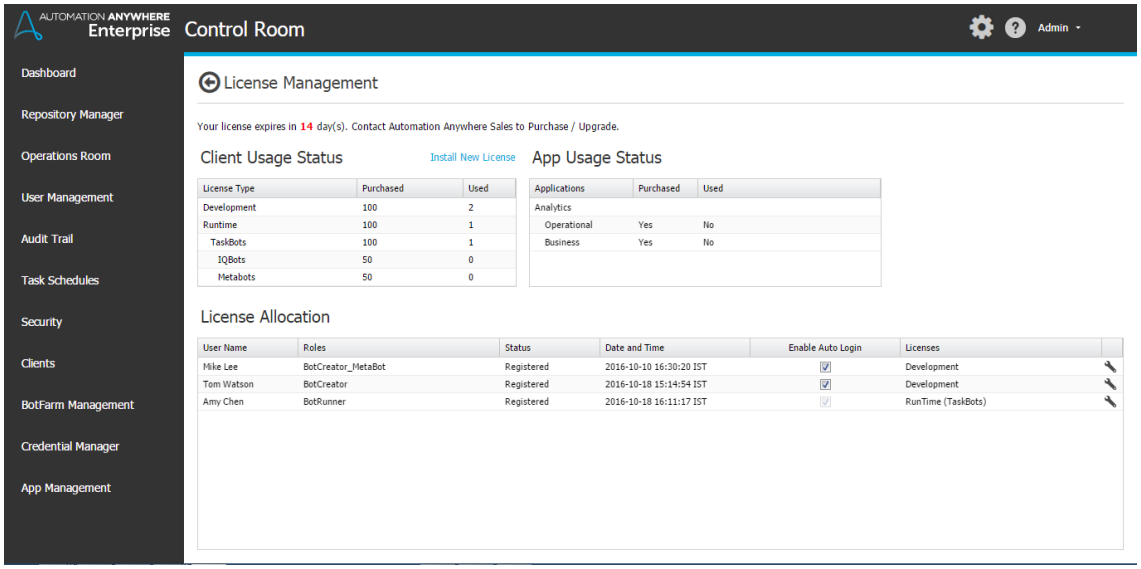
Note: Purchase and subsequent license allocation is subject to the type of Enterprise Clients that need to be defined - Bot Creator or Bot Runner.

In License Management, the Control Room Administrator can also view how many days are remaining for the license to expire.

- If more than 30 days are left for license expiry, the following License Management screen is displayed:



- If less than 30 days are left for license expiry, the following License Management screen is displayed:



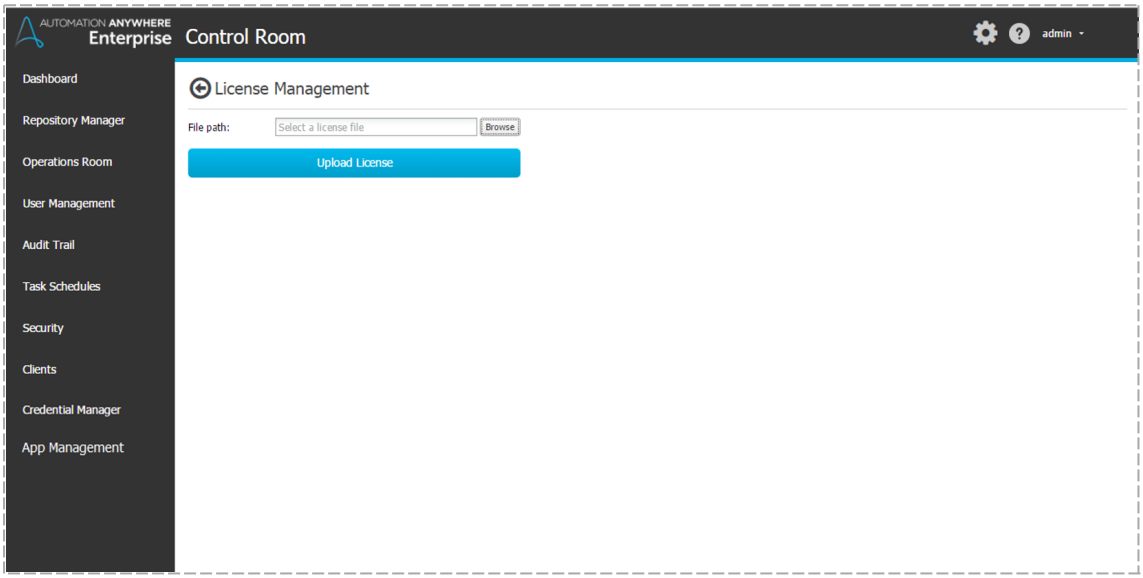
Note: If your Control Room license has expired, refer to Purchasing and Installing Control Room license for details.

Apart from licensing, the Control Room Administrator can enable or disable 'Auto Login' for BotCreators. BotCreators are Clients, who have Development privileges.

Installing a New License before Expiry

The Control Room Administrator can install a license during evaluation, post-evaluation or if you have purchased more licenses to support growing number of Client users.

1. When you click on the 'Install New License' link, choose a license from your repository of licenses and click 'Upload License':

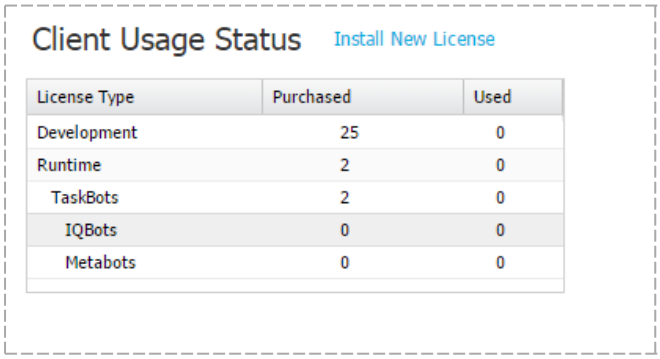


2. Log into the Control Room again.

For more information about the detailed steps, see the Control Room Installation Guide.

Viewing License Usage

Once the license is installed, you can verify the details in the 'Usage Status' view.



License Type	Purchased	Used
Development	25	0
Runtime	2	0
TaskBots	2	0
IQBots	0	0
Metabots	0	0

Here you can view:

- **License Type -** You can allocate licenses to two types of Client users - Development and Runtime.
    1. Development Clients can create tasks in the Enterprise Client.
    2. Runtime Clients can run tasks. If IQBots and MetaBots are purchased, they can also run them.
- **Purchased -** Displays the number of licenses purchased for the Development Clients and TaskBot Clients.
    - Development Client users can create tasks that could include IQBot and/or MetaBot if the required plug-ins are installed.

- The Runtime Client users can enable the Scheduling Manager. The Runtime Client user can scheduling and run tasks on the TaskBot Client user machines.

  You can allocate licenses to Runtime Clients depending on your requirements. For instance, you could either allocate all Runtime licenses to TaskBots Clients or divide the licenses between IQBot and/or MetaBot if the plug-ins have been installed.

- **Used -** Displays the number of licenses that have been consumed by Development and Runtime Clients (including TaskBots, IQBots and MetaBots).

Monitoring App Usage Status

You can monitor your App Analytics Usage status in License Management.

You need to register your applications App Management to be able to monitor your app usage.

Here, you can view:

- **Application License Type -** The status of licenses for Analytics is displayed in the Applications column. When you purchase a license for Operational and/or Business Analytics, the status under Purchased column is displayed as Yes.
- **Usage Status -** The status for Operational and Business Analytics is based on license allocation to AnalyticsExpert and AnalyticsConsumer.

Note: The Operational Analytics licenses is assigned to the Analytics Expert, while the Business Analytics license is assigned to the AnalyticsConsumer. For more information, see Managing Roles and Permissions.

Installing a Downgraded License

**Applicable for Enterprise Control Room 10.5.8 and later*

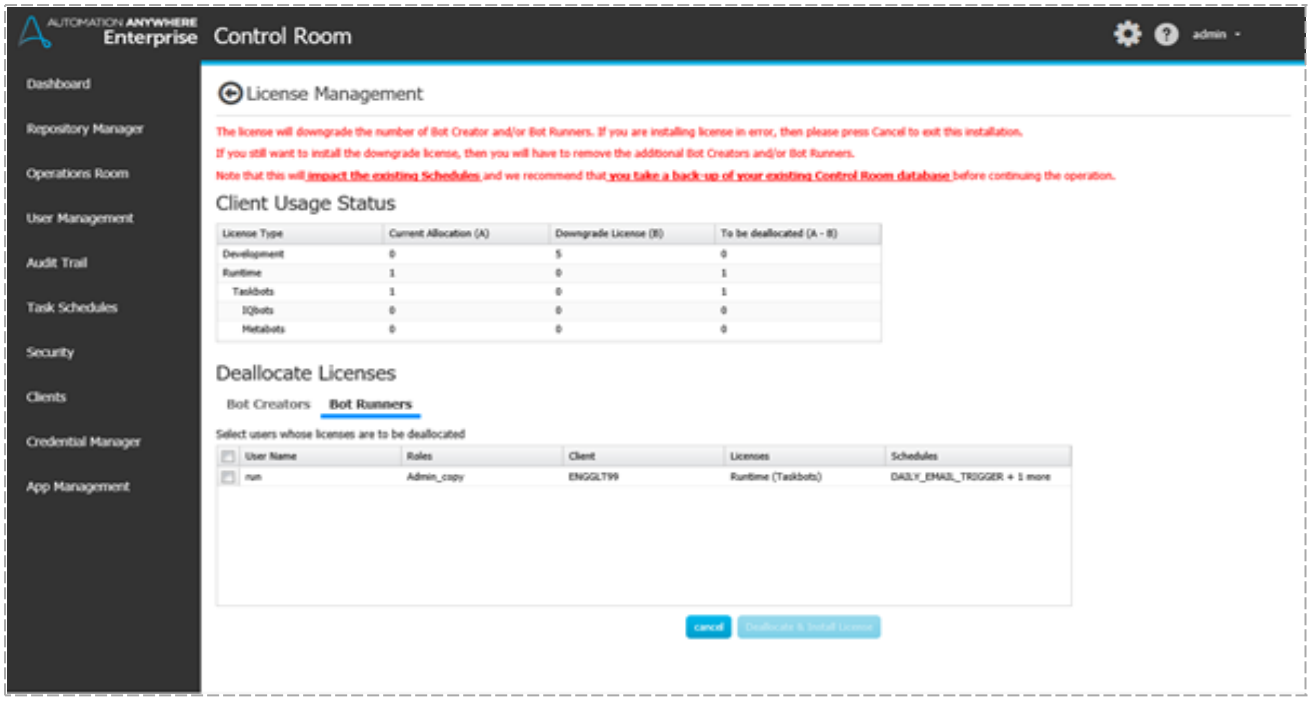
The downgraded license scenario is applicable when the current count of used licenses for Bot Creators and Bot Runners is greater than in the new license that you are installing as a Control Room administrator.

In some cases if you install downgraded license dimensionally or dimensionally, the Control Room displays a warning on the License Management page. It allows the Control Room administrator to handle downgrading of license easily by allowing you to select the users you want to remove from the license.

You must remove the additional Bot Creators and Bot Runners licenses from the Control Room to be able to install a downgraded license successfully.

Note: Back up your Control Room database before removing the additional Bot Creators and Bot Runners during installation of downgraded licenses.

The following screen with a warning message is displayed to prevent accidental installation of the downgraded license.

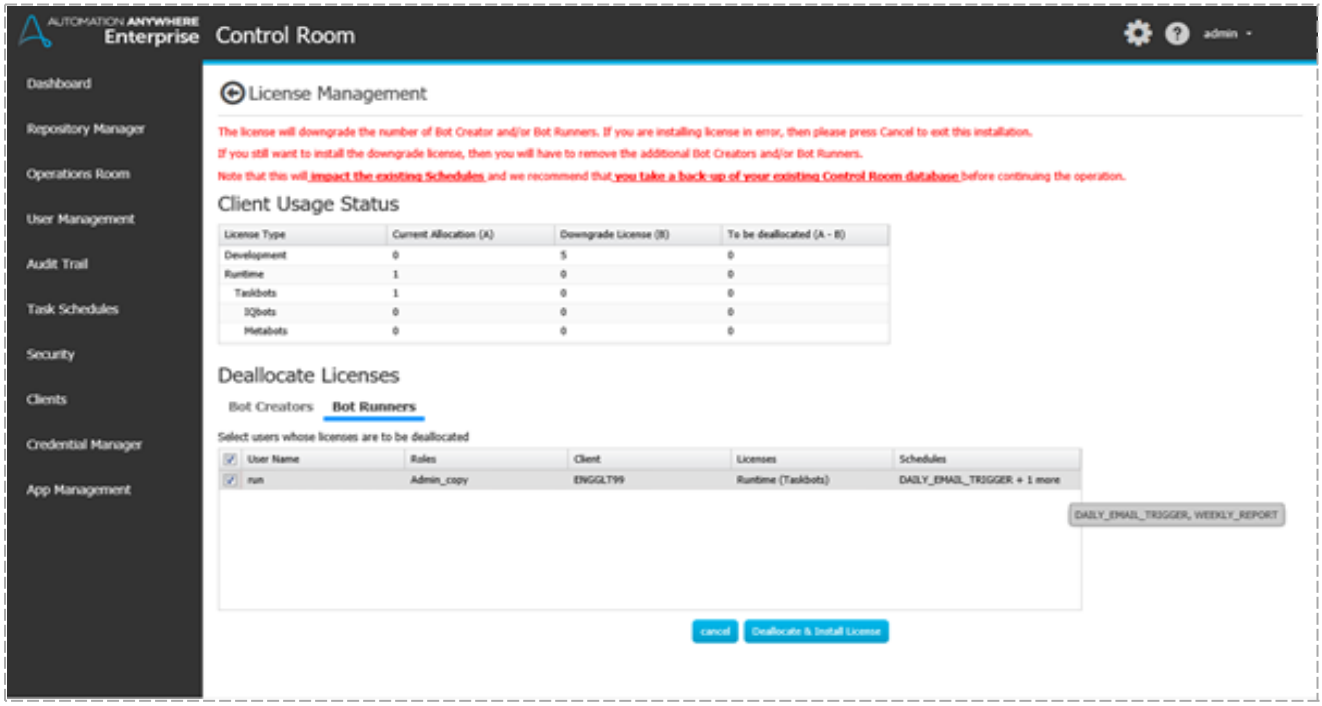


This screen displays the license count for all types of used licenses such as Development and Runtime, Duckboards, IQBots, MetaBots. You can see all the licenses currently allocated in the **Current Allocation (A)** column, downgraded license count as per the new license in the **Downgrade License (B)** column, and the additional license count to be allocated in the **To be deallocated (A - B)** column.

In the Deallocate Licenses section, select the users whose license you want to deallocate either from Bot Creator or Bot Runner or from both tabs based on the values in the **To be deallocated (A - B)** column till all the values become zero in this column.

The Deallocate License section also displays the current role or roles of the user, host name of the AAE Client where the user is last logged in, and also name of schedules for the Bot Runners, which helps you in deallocating the licenses.

The **Deallocate & install license** button is disabled till the **To be deallocated (A - B)** number does not become zero.



Click **Deallocate & install license**. A confirmation message is displayed "Are you sure you want to deallocate and install downgraded license?". If you confirm by clicking **Yes**, the licenses for selected users is deallocated and a new license is installed.

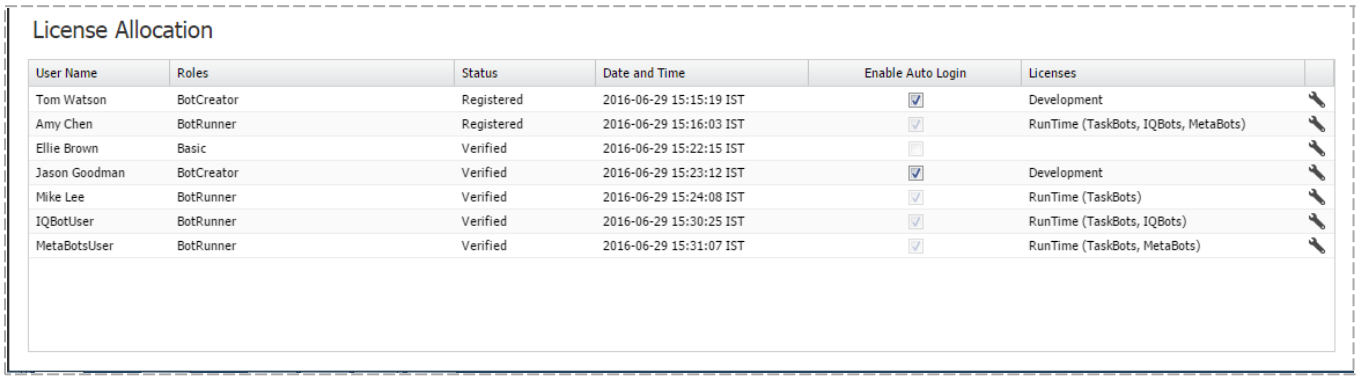
If you want to cancel installation of downgraded license, click **cancel**. The Install license page is displayed.

Note: You can also downgrade more number of licenses than the licenses listed in the **To be deallocated** column.

License Allocation

After installing appropriate license, you are now ready to allocate the licenses to your Clients.

The User list depicts all the Clients that are registered to the Control Room.

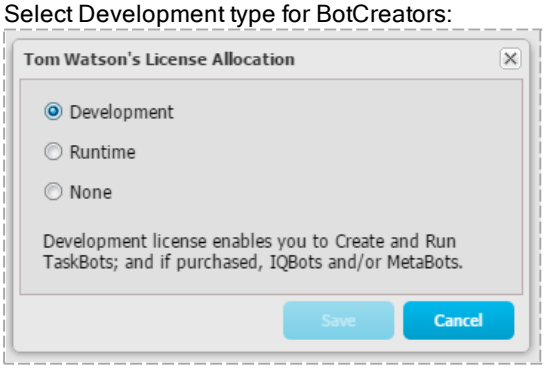


User Name	Roles	Status	Date and Time	Enable Auto Login	Licenses
Tom Watson	BotCreator	Registered	2016-06-29 15:15:19 IST	☑	Development
Amy Chen	BotRunner	Registered	2016-06-29 15:16:03 IST	☑	RunTime (TaskBots, IQBots, MetaBots)
Ellie Brown	Basic	Verified	2016-06-29 15:22:15 IST	☐	
Jason Goodman	BotCreator	Verified	2016-06-29 15:23:12 IST	☑	Development
Mike Lee	BotRunner	Verified	2016-06-29 15:24:08 IST	☑	RunTime (TaskBots)
IQBotUser	BotRunner	Verified	2016-06-29 15:30:25 IST	☑	RunTime (TaskBots, IQBots)
MetaBotsUser	BotRunner	Verified	2016-06-29 15:31:07 IST	☑	RunTime (TaskBots, MetaBots)

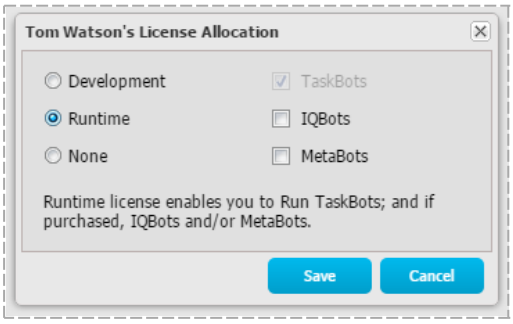
```
Note:
 • Licenses can be allocated to only those Client Users who have been created or verified.
 • A Client user cannot connect to the Control Room, if a license is not allocated to the user. When
the Client user logs in, the user is registered to the Control Room and the license is indicated as con-
sumed.
 • You can choose to switch Client user types, that is, Development to Runtime or the other way round.
Click on  to change the user type.
```

1. To allocate a license to a Client user, click on to launch the Client 'License Allocation' window and select the Client type.

    1. Select Development type for BotCreators:

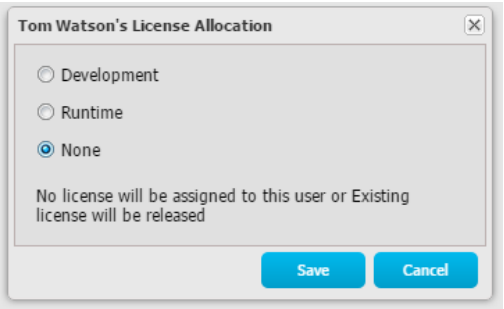


- Select Runtime for BotRunners.



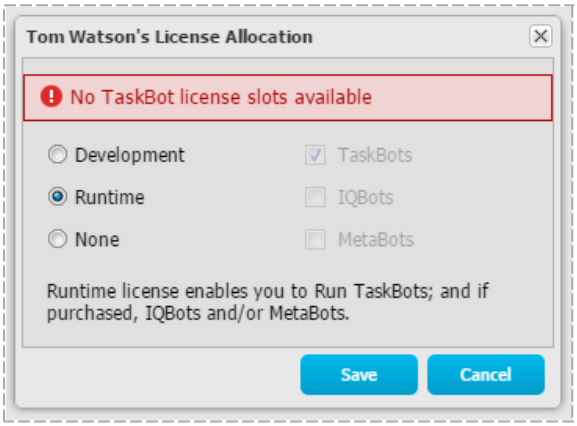
- None, when you want to either not allocate a license to the user, that is, create a Control Room user only or to release an existing license in order to convert a BotCreator to BotRunner (works the other

way round also).



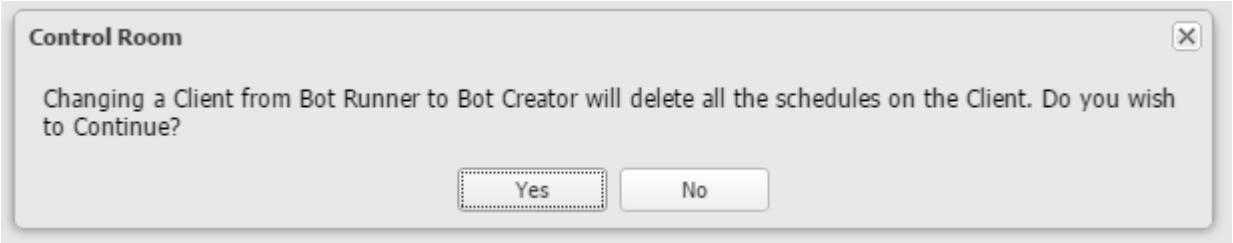
2. Click to 'Save'.

Note: If licenses are unavailable for consumption, a notification is displayed on the License Allocation:

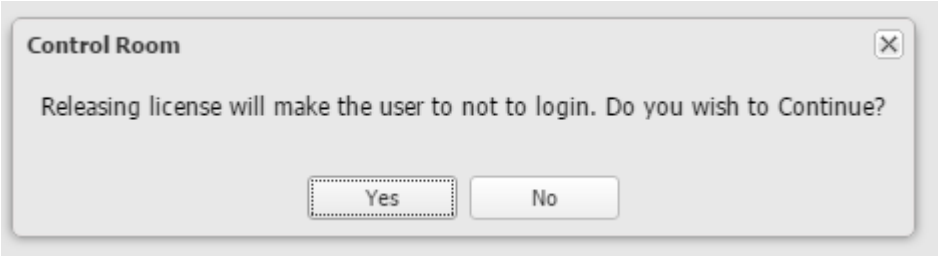


3. You can also modify the type of licenses allocated by clicking .

- If you modify a Bot Runner Client to Bot Creator, the existing schedules for that Client is deleted.

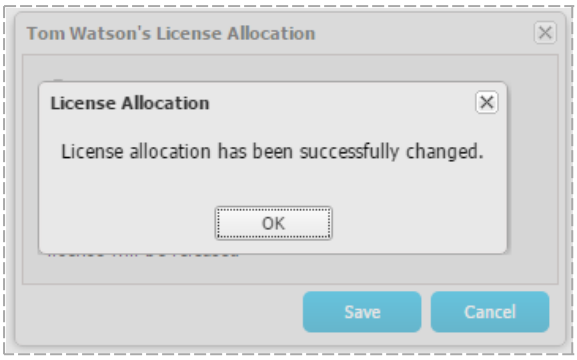


If you select the 'None' option for an existing Client user who has been allocated Development or Runtime license, the license is released:



- The user is not able to log into the Client.

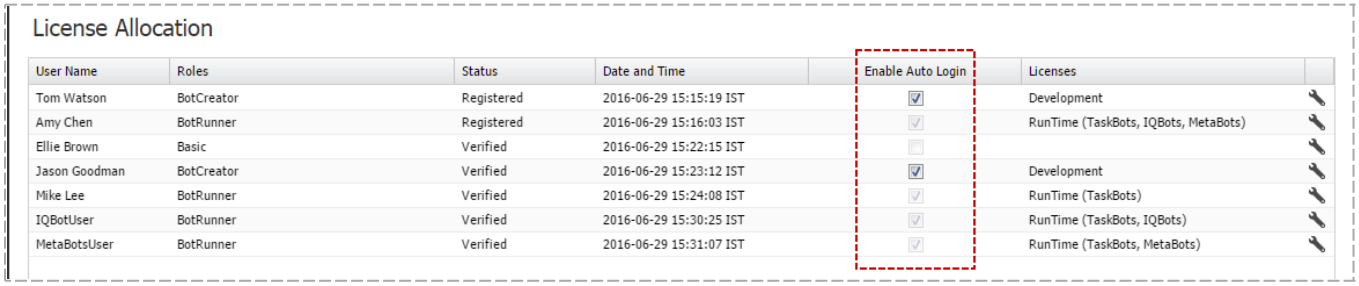
4. A success message indicates the updates are saved:



If you run out of licenses, contact support@automationanywhere.com.

Enabling or Disabling Auto Login

The Control Room Administrator can manage the Client auto login behavior of Bot Creators, that is, Clients with the development rights by enabling or disabling 'Auto Login'.



User Name	Roles	Status	Date and Time	Enable Auto Login	Licenses
Tom Watson	BotCreator	Registered	2016-06-29 15:15:19 IST	☑	Development
Amy Chen	BotRunner	Registered	2016-06-29 15:16:03 IST	☑	RunTime (TaskBots, IQBots, MetaBots)
Ellie Brown	Basic	Verified	2016-06-29 15:22:15 IST	☐	
Jason Goodman	BotCreator	Verified	2016-06-29 15:23:12 IST	☑	Development
Mike Lee	BotRunner	Verified	2016-06-29 15:24:08 IST	☑	RunTime (TaskBots)
IQBotUser	BotRunner	Verified	2016-06-29 15:30:25 IST	☑	RunTime (TaskBots, IQBots)
MetaBotsUser	BotRunner	Verified	2016-06-29 15:31:07 IST	☑	RunTime (TaskBots, MetaBots)

A BotCreator for whom this setting is disabled has to provide login credentials while accessing the Client.

By default, this setting is enabled for new BotCreators.

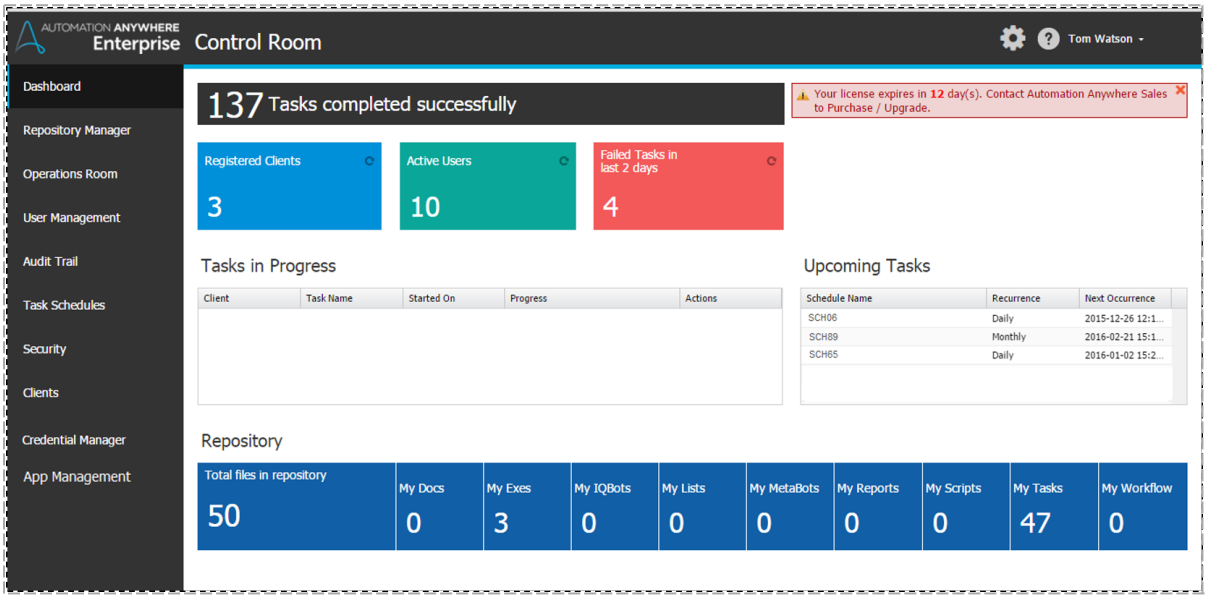
Note: Client Users that are allotted 'BotRunner' role have this setting enabled by default.

Purchasing and Installing Control Room License

This topic describes the recommended method to install a license file after expiry, in order to re-activate the Automation Anywhere Enterprise Control Room.

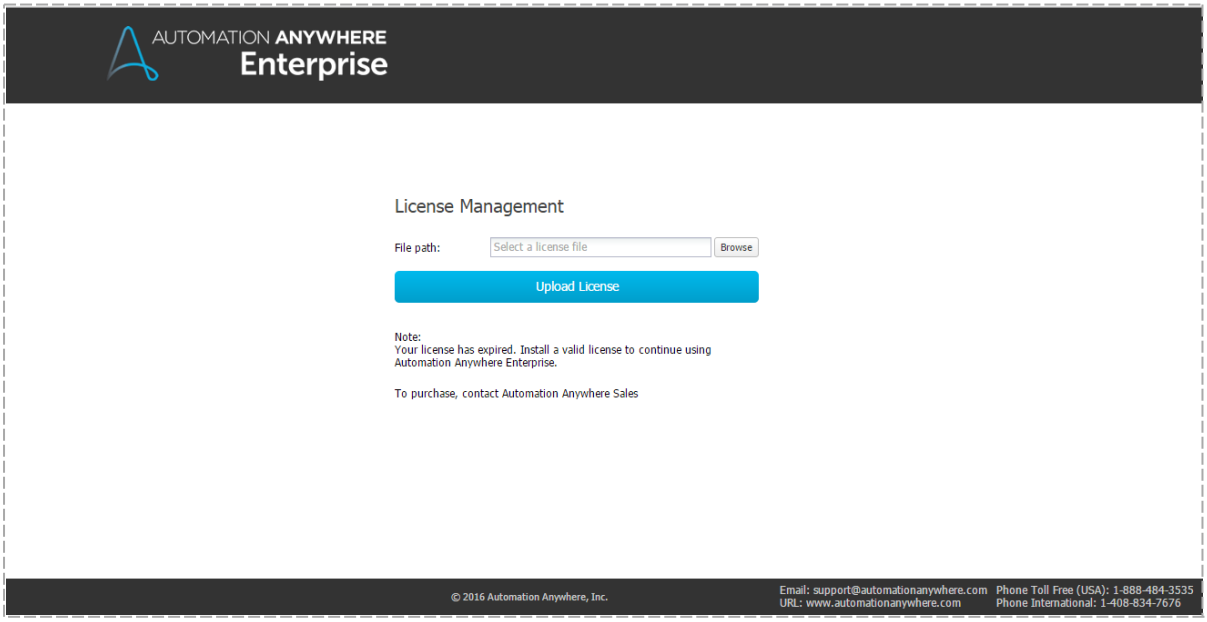
When less than 30 days are left for license expiry, you will also be informed about it on the Dashboard.

Note: The license expiry information will be seen on your Dashboard only if you have Admin privileges.



Admin - the Control Room Administrator can install a new license from License Management console. Learn More.

However, if your Control Room License has expired before you were able to install a new license, then you will be shown the below screen when you login to the Control Room:



If you have the new license file, you can simply upload it here. However, if you don't have a new license file, you can contact Automation Anywhere Sales and place your order for the Control Room license.

After the completion of your order, you will receive an email from Automation Anywhere containing a registration license file. Download and save the file to a desired location on your computer.

Once you have uploaded the valid license file, you will be able to login to the Control Room and continue monitoring activities.

RDP Based Approach To Bot Deployment - Guidelines

Overview

Typically, when a Bot is deployed from the Automation Anywhere Enterprise Control Room to any Bot Runner, the Bot will attempt to auto-login into the Bot Runner (if the Bot Runner is locked or logged off).

However, auto-login is prone to the security policies set on the machine because of which certain policies may need to be relaxed for auto-login to function.

To mitigate these issues, you can use RDP based Bot Deployment that is introduced in Control Room from AAE 10SP2 with product version 10.5.0.

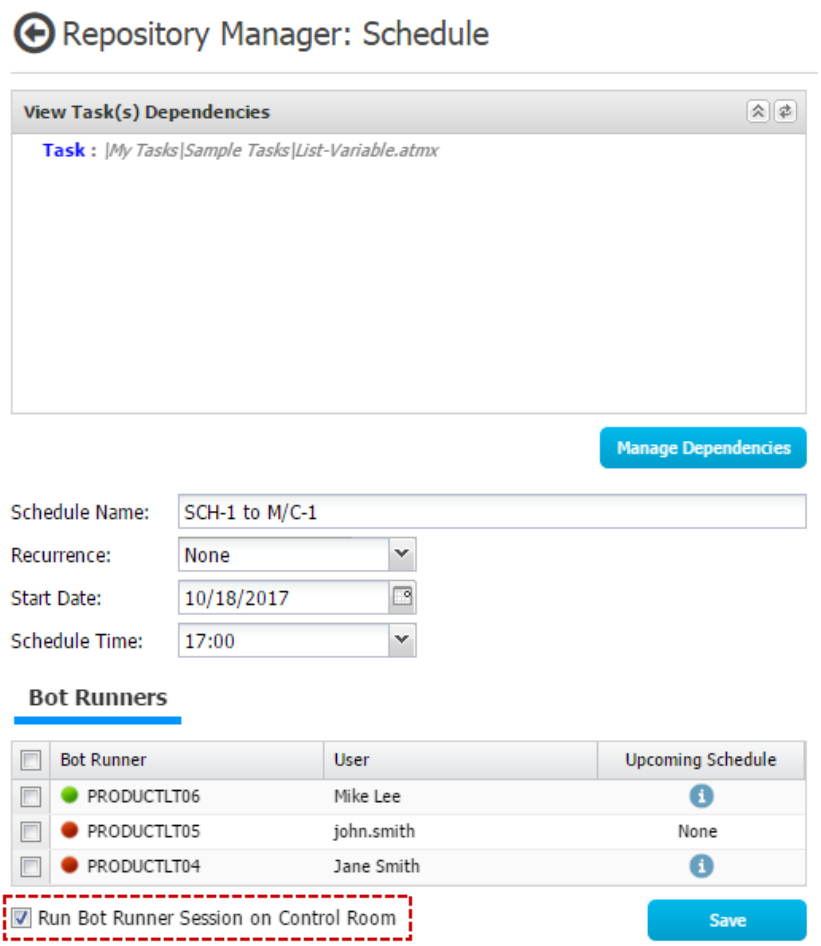
What is RDP Based Bot Deployment?

When the Bot is deployed from Control Room onto the Bot Runner, the Control Room will take the Bot Runner session via RDP (Remote Desktop Protocol) and will execute the Bot.

Key features and benefits of this approach

- The Bot runs in the Bot Runner's RDP session in the Control Room in the background; no window is visible on the Control Room.
- Auto-Login issues are mitigated as auto-login is not attempted; auto-login will ONLY be attempted if RDP fails in the first place.
- As Bot Runner machine is not auto-logged in; the security issues related to 'live monitor' scenarios are mitigated.

An option has been provided in the Control Room Run/Schedule Page so as to enable RDP based Bot Deployment:



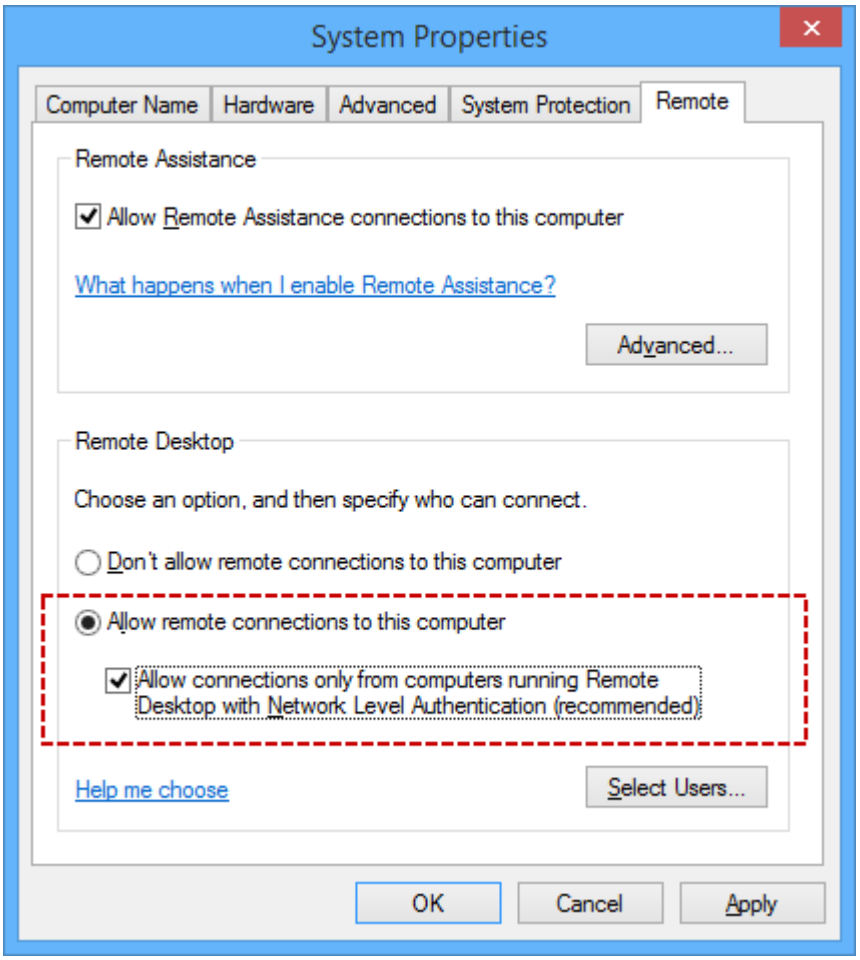
To ensure that the RDP based Bot Deployment works seamlessly, there are certain prerequisites and settings that will be need to be done on the Control Room and the Bot Runner machine. The following section elaborates those prerequisites.

Prerequisites for RDP Based Bot Deployment

Settings on Bot Runners

On the Bot Runner machine, there are 2 main settings that need to be done.

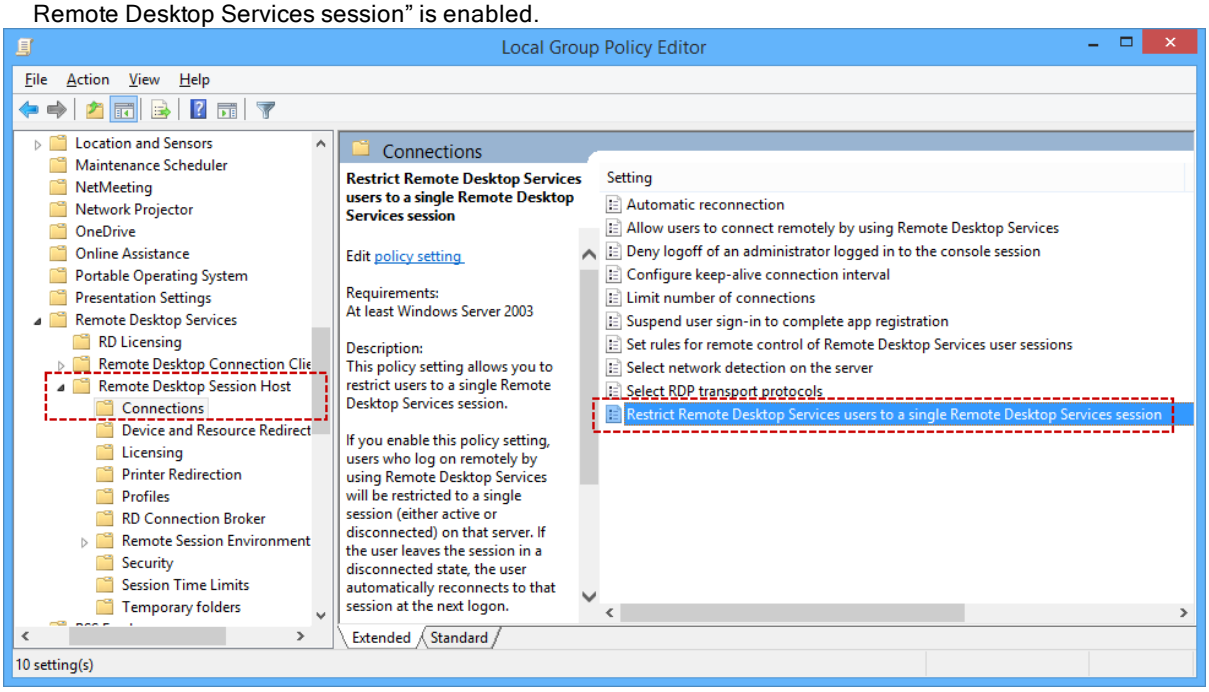
- **No Legal Disclaimer on Bot Runners -** There should not be any legal disclaimer dialogs coming up when the user logs in into the Bot Runner. Legal disclaimers can be disable via group or local policies.
- **The RDP connection must be enabled on Bot Runner -** Following are the steps to enable RDP connection for various machine types of Bot Runners
  1. Enabling RDP on Bot Runner on Physical Machine
     On the Bot Runner machine, ensure that remote connections to Bot Runner are allowed from **My Computer's properties**. Also, make sure a checkbox "Allow connections only from..." should be checked.



  2. Enabling RDP on Bot Runner on Virtual Machine (Azure, VMWare, Oracle Virtual Box)
     To enable RDP on Virtual Machine, please refer to the appropriate documentation of the Virtual Machine host.
  3. Enabling RDP on Bot Runner hosted on Citrix XenDesktop
     To enable RDP on Citrix XenDesktop, please refer to its documentation at: https://support.citrix.com/article/CTX129184/
  4. Enabling RDP on Bot Runner hosted on Terminal Server
     Refer to the documentation on Managing Remote Desktop Services Connections. For Windows Server 2008 R2, the documentation is at: https://technet.microsoft.com/en-us/library/cc772051(v=ws.11).aspx

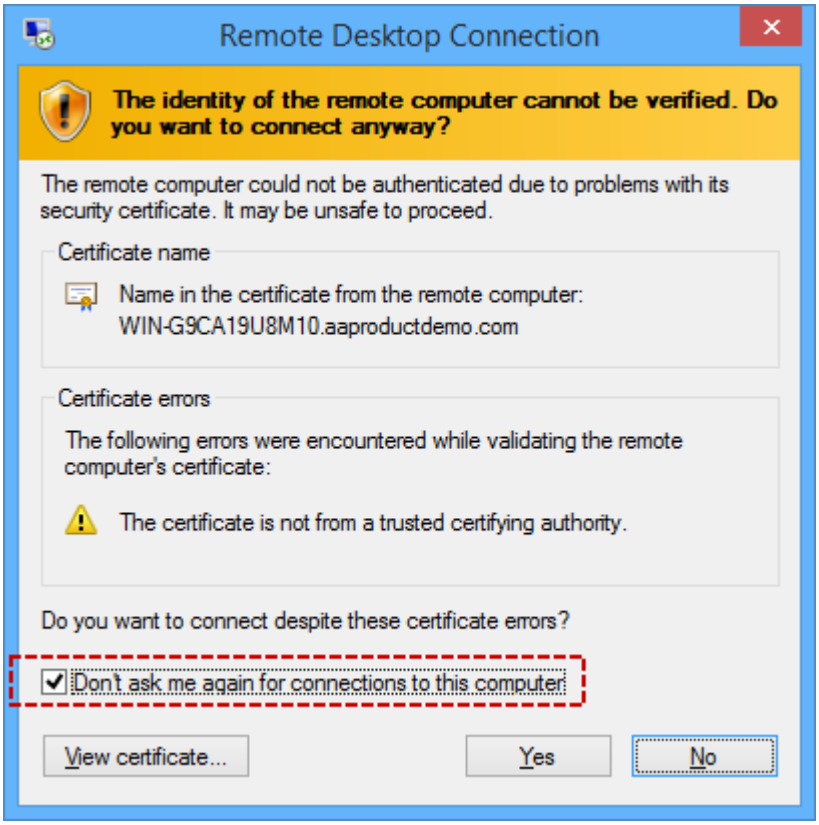
     Also, the user session on Terminal Server must be restricted to a Single Remote Desktop Services session.

Navigate to Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Connections and ensure that “Restrict Remote Desktop Services users to a single Remote Desktop Services session” is enabled.



Settings on Control Room machine

- Allow Connection despite certificate errors.
  1. On the Control Room machine, ensure that “Don’t ask me again for connections to this computer” is checked.



Changing screen resolution for Bot Runner session on Control Room

To ensure your automation runs seamlessly during RDP based deployment even when the resolution of screen varies between Bot Runners and Control Room, it is recommended that you add the screen resolution configuration of the Bot Runner machine.

For this you can configure the **Enterprise.Settings.xml** file of the Control Room that is available in the repository path.

For example,

- In standalone mode the repository path could be "C:\Users\Public\Documents\Automation Anywhere Server Files"
- In distributed mode the reposiotry path could be "\\<SharedPath>\Automation Anywhere Server Files"

To configure, add the following inside the <Sections> tag in **Enterprise.Settings.xml** file:

```
<Sections>
....
<RemoteMachineConnector>
<Default>
<Setting>
<Height>768</Height>
<Width>1366</Width>
<Port>3389</Port>
</Setting>
</Default>
</RemoteMachineConnector>
</Sections>
```

Note: You must configure height, width, and port value according to your requirement.

FAQs

Q: Will there be one RDP session per Bot Runner?

A: Yes

Q: Do I need to ramp up the Control Room RAM for RDP Based Deployment?

A: You may want to depending on the Bot Deployment scenarios. A typical RDP session takes around 150MB of RAM. So, if you are deploying onto 10 Bot Runners, 1.5GB RAM will be consumed. We recommend that you increase the RAM to 16 GB if extensive Bot deployment is required. Refer the Hardware Requirements section for Control Room in the AAE - Installation Guide that is shipped with the product.

Q: Will the RDP sessions terminated once the Bot has finished executing?

A: Yes

Q: Can a Control Room user see the active RDP Session?

A: No. User will not be able to see the active RDP Session as it runs as a background process. However, the user can see in task manager running processes list.

Q: While the Bot is executed in an RDP session on the Control Room, if the Bot Runner user logs in into the Bot Runner, will it impact the Bot execution?

A: As soon as the user logs in into the Bot Runner, the RDP session on the Control Room will terminate. The Bot will continue to run, and the user will see that running on the Bot Runner.

Q: In the above scenario, if the user locks/logs off the machine, what will happen to the current executing Bot?

A: If the user locks the machine, the Bot will continue to run in the background; however, the screen based commands may error out. If the user logs off the machine, the Bot execution will be terminated.

Q: While selecting Remote based Bot deployment, the AA player is taking more time to come up. Has the performance been affected by new functionality?

A: No, there will be some delay in the AA player to come up as first the RDP connection must be made. And in environment where there is high latency, the RDP connection itself might be bit slow.

Q: What is the impact if RDP connection is very slow?

A: If Control Room takes say 30 Seconds to RDP, then the Bot execution start-up will be delayed by 30 secs for that Bot Runner. Beyond that, if RDP session does not get connected, then the Control Room will deploy Bot with legacy route (auto-login).

Q: If there is already active RDP (manually done by the user) and if the Bot starts, will the existing RDP session be taken from user?

A: Older RDP session will be disconnected and the task will be executed on new RDP Session which is created by Control Room.

Q: If RDP Session crashes in between Bot Execution, would Control Room know and restart the session without impacting Bot execution?

A: YES, RDP has in-build capability of reconnect. But that works only for certain duration. So, if Bot Runner gets disconnect for longer time, then it will impact the execution of the Bot.

Q: With the answer given in above, there is possibility of Bot erroring due to RDP disconnection. How would a developer/Control Room User differentiate a failure between RDP Error Vs Actual Bot Error? If not, a developer may spend long time (impacting production execution) deciphering code while the actual impact was due to RDP session, which may not require any code change.

A: If Bot errors out, then it will automatically be audited in the Control Room. For RDP disconnect case, we have kept list of reasons for disconnection and we are storing this into log file. The link for various reasons for disconnection, https://msdn.microsoft.com/en-us/library/aa382170(v=vs.85).aspx

Q: If RDP Session crashes will Audit log show of that occurrence and status of Bot even though the RDP crashed?

A: YES, the Bot will be still running on Bot Runner and it will log required audit log of success or failure.

Q: We have occasional RDP session timeouts. Will Control Room RDP be impacted by it?

A: Ideally, there should not be any RDP TIMEOUT; otherwise it will impact the execution of the Bot.

Q: Will RDP based Bot Deployment work with Bot Schedules as well?

A: YES, there will an option for use to select the RDP based Bot Deployment while scheduling the Bot from Control Room.

Q: Can it be configurable with other RPD tools like VM Ware client? If not now in future.

A: Not for now

Q: When Control Room tries to RDP, If the user's AD password is changed; will Control Room connect with new password by syncing up with Active Directory?

A: NO. Control Room will only fetch the password which is set in Automation Anywhere Enterprise Credential Vault.

Q: If a Bot is scheduled to deploy onto 100 Bot Runners, will Control Room invoke RDP onto all 100 Bot Runners asynchronously or sequentially?

A: RDP sessions will be created on the Control Room box and Control Room will deploy Bot asynchronously on these Bot Runners.

Q: If a Bot is deployed onto 10 Bot Runners, If Control Room is unable to RDP onto 5th Bot Runner, will it move onto 6th Bot Runner or entire process will be killed?

A: As it is happening in parallel, RDP failure of one Bot Runner does not impact the other. The Control Room will move onto the 6th Bot Runner.

Q: If Control Room is unable to terminate the RDP session, will it notify the Control Room Admin or will it log in Audit trail?

A: No. The Control Room user should manually terminate the Bot Runner's RDP session.

Q: Will this work if the Control Room is hosted in load-balanced high-availability disaster recovery (HA-DR) mode; where multiple Control Room Application Servers are installed? If yes, on which Control Room machine will the RDP sessions run?

A: Yes. This will work in HA-DR mode. In that case, the RDP sessions will be deployed on the Control Room Server which deploys the Bots.

Copyright © 2018 Automation Anywhere, Inc.

Control Room Authentication API

The Authentication API can be used to authenticate the Control Room credentials.

API:/controlroomapi/v1/authenticate

The external application must pass two parameters in JSON Format.

1. Control Room Username
2. Control Room Password

Input for the API (as JSON string): **{"username":"admin","password":"12345678"}**

Note the user must have privileges to run/schedule Bots and should also have access to the Bot Runners on which Bot is to be deployed.

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": "eyJ0eXAiOiJKV1QiLCJh-
bGciOiJIUzI1NiJ9.eyJ1c2Vyl-
joiMSIslmlzcyl6Imh0dHA6Ly9sb2NhbGhvc3Qvd2ViY3JzdmMvliwiYXVkljoiaHR0cDovL2xvY2FsaG9zdC93ZWJjcnN2Yy8iLCJle
HAiOjE0OTUwOTAwOTksIm5iZiI6MTQ5NTA4OTE5OX0.qPPhpti0j7LGAmWkj3XFymFfJXzA1P4zPehIjVYfulc"

}

Authentication is successful

401

{

"message": "Invalid credentials."

}

- The password is invalid
- User does not exist

401

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

{

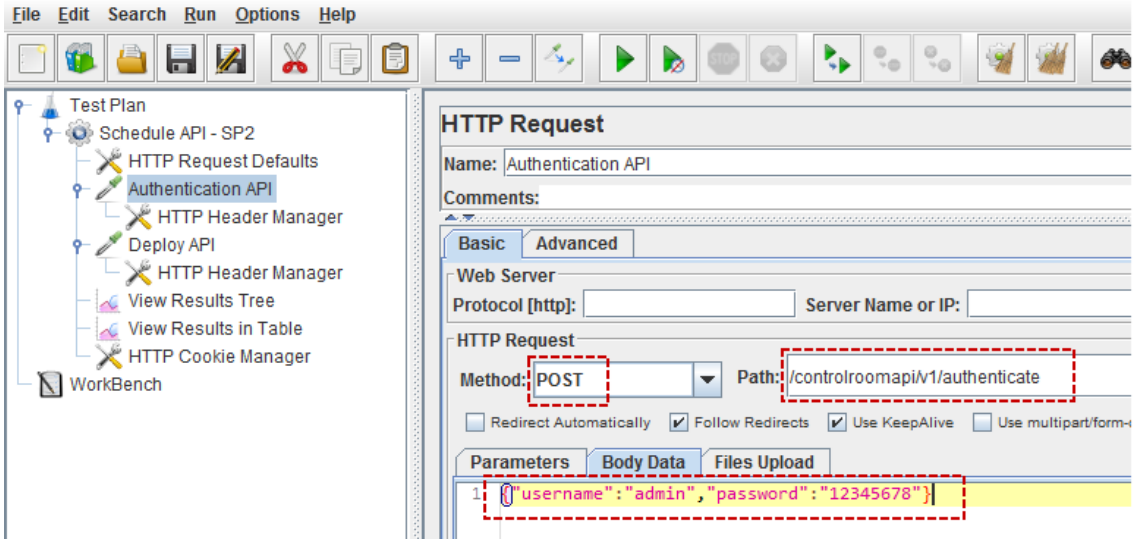
"message": "Your account is not activated. Please contact the admin."

}

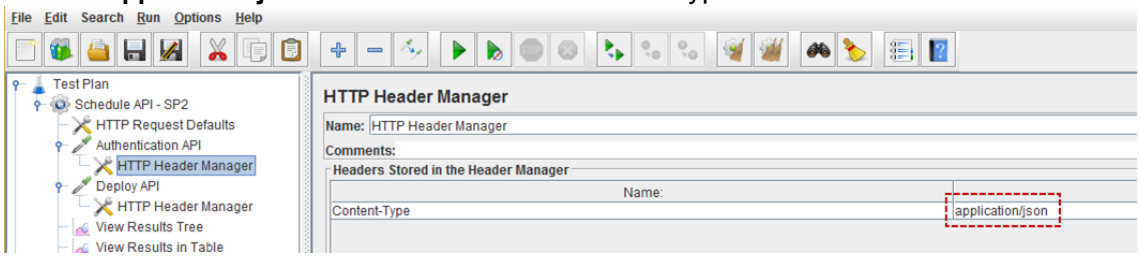
User is deactivated

Testing Authentication API using Jmeter

1. Under 'Authentication API', select the method as 'POST', provide the Path as **/controlroomapi/v1/authenticate** and the Control Room Credentials in JSON format (e.g. **{"username":"admin","password":"12345678"}**) under the 'Body Data'



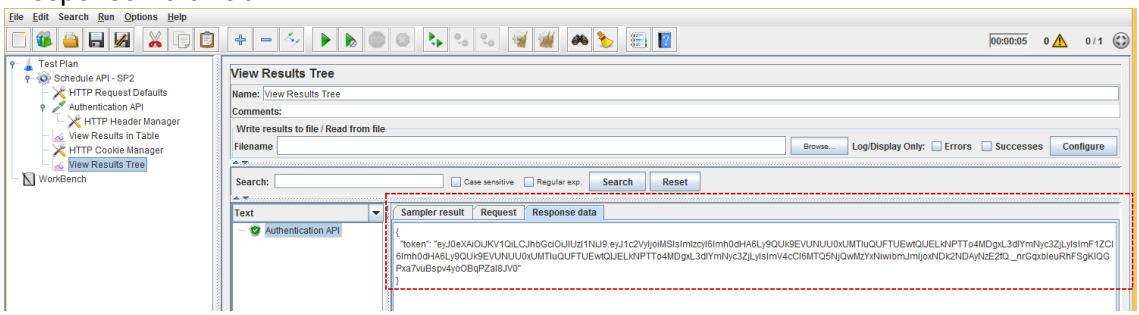
2. Under the 'Authentication API' node, add one more node by right clicking on the node and selecting Add > Config Element > HTTP Header Manager.
3. Provide **application/json** as the Value under Content-Type.



4. Add the 'View Results Tree' node by right clicking on 'Schedule API - SP2' and clicking on Add > Listener > View Results Tree.

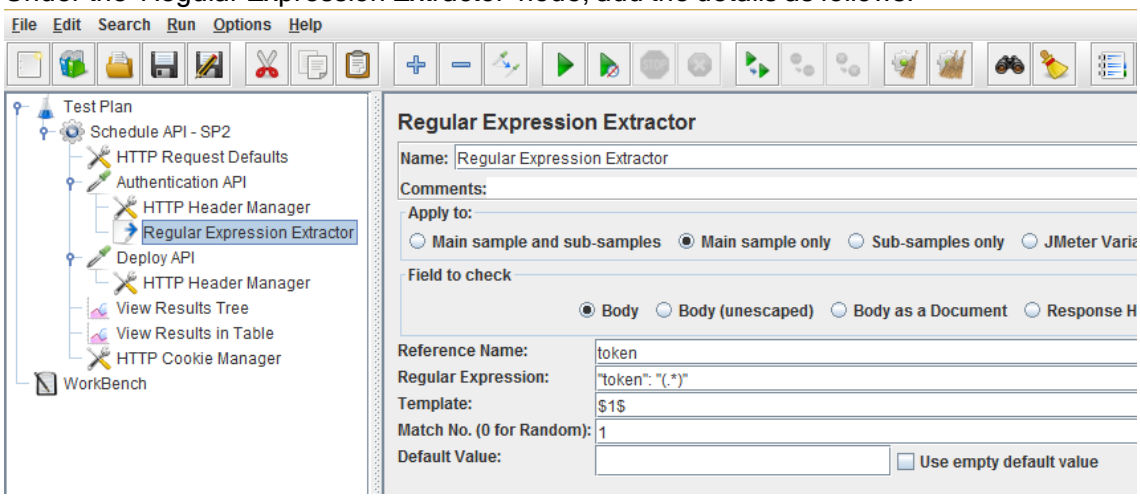
5. Click on **Play**

6. If authentication is successful, in the 'View Results Tree' node you will get the authentication token under the 'Response Data' tab.



7. Right click on 'Authentication API' node and click on Add -> Post Processors -> Regular Expression Extractors.

8. Under the 'Regular Expression Extractor' node, add the details as follows.



Note: This variable "token" will be used as a header parameter to pass authentication token to other APIs.

Bot Deployment API

Available from Enterprise edition 10 SP2 with product version 10.5.0

Overview

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.

This article for Automation Anywhere Enterprise (AAE) Control Room summarizes the following:

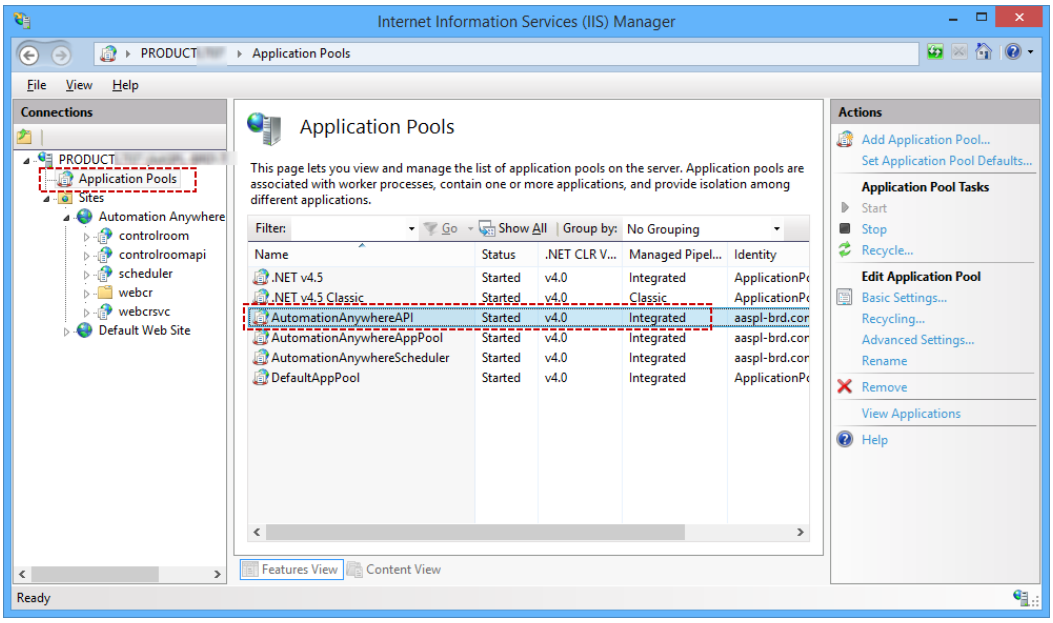
- Describes the new Control Room APIs to enable integration of third party/external applications with AAE to execute business processes.
- Provides the parameters used to authenticate and deploy Bots (Tasks).
- Provides steps to test the APIs using JMeter.
- Provides sample codes used to authenticate and deploy Bots to BotRunner systems.
    1. APITest Java Class
    2. APIClient Java Class
    3. RestHelper Java Class
    4. Sample Bot CSV
    5. VBScript to Deploy APIs

Control Room APIs

Two Control Room APIs that have been published:

- Authentication API – This will be used to authenticate the Control Room credentials
- Deployment API – This will be used to deploy Bots onto the Bot Runners.

A new Application Pool for APIs has been introduced by Automation Anywhere available from **Internet Information Services (IIS) Manager > Application Pools**. These APIs are configured by default during Control Room installation.



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.

Authentication API

The Authentication API can be used to authenticate the Control Room credentials.

API: /controlroomapi/v1/authenticate

The external application must pass two parameters in JSON Format.

1. Control Room Username
2. Control Room Password

Input for the API (as JSON string): **{"username":"admin","password":"12345678"}**

Note the user must have privileges to run/schedule Bots and should also have access to the Bot Runners on which Bot is to be deployed.

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": "eyJ0eXAiOiJKV1QiLCJh-
bGciOiJIUzI1NiJ9.eyJ1c2Vyl-
joiMSIslmlzcyI6Imh0dHA6Ly9sb2NhbGhvc3Qvd2ViY3JzdmMvliwiYXVkljoiaHR0cDovL2xvY2FsaG9zdC93ZWJjcnN2Yy8iLCJle
HAiOjE0OTUwOTAwOTkslm5iZiI6MTQ5NTA4OTE5OX0.qPPhpti0j7LGAmWkj3XFymFfJXzA1P4zPehIjVYfulc"

}

Authentication is successful

401

{

"message": "Invalid credentials."

}

- The password is invalid
- User does not exist

401

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

Deployment API

The Deployment API is used to deploy Bots to BotRunners.

API: /controlroomapi/v1/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"}]}

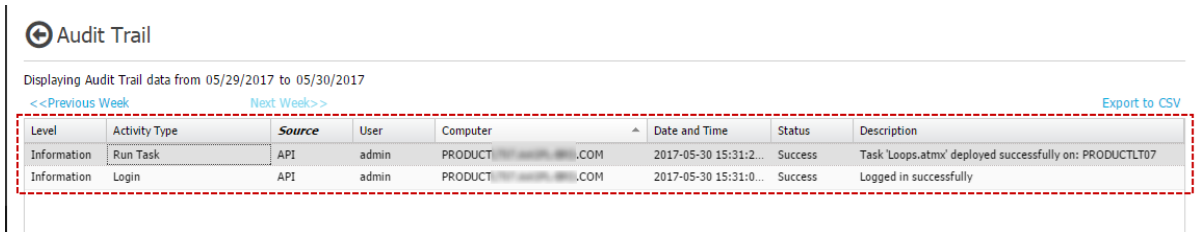
Deployment API Response Codes

Http Status Code	Response	Description

200	{ "deploymentFailOn": [], "message": "Task 'TestSetText.atmx' deployed successfully on selected client(s)." }	Task is deployed successfully on all clients
200	{ "deploymentFailOn": [{ "Client": "product", "User": "m" }], "message": "Task 'TestSetText.atmx' could not be deployed on selected client(s)." }	Task is deployed successfully on some clients.
401	{ "message": "Requested user does not have permission." }	• Token has expired • Token is invalid
402	{ "message": "License expired." }	License has expired
403	{ "message": "Insufficient privileges." }	• User does not have task permission • User does not have deploy permission • User does not have deploy permission on any of client. • Client details provided are incorrect
500	{ "message": "Credential Vault not opened" }	The Credential Vault is closed
500	{ "message": "Invalid parameter(s)." }	Any value in parameters is blank.
500	{ "message": "Task does not exists." }	Task does not exist
500	{ "message": "Unable to run task. Ensure all dependencies are available and their production version is set." }	SVN is enabled and production version is not set for task or dependant task(s)

API Audit Trail in Control Room

The data is logged in the Audit Trail section of the Control Room

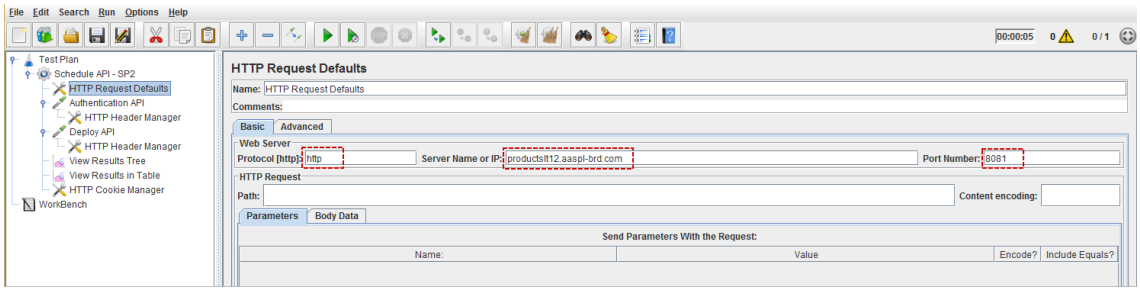


Testing APIs with JMeter

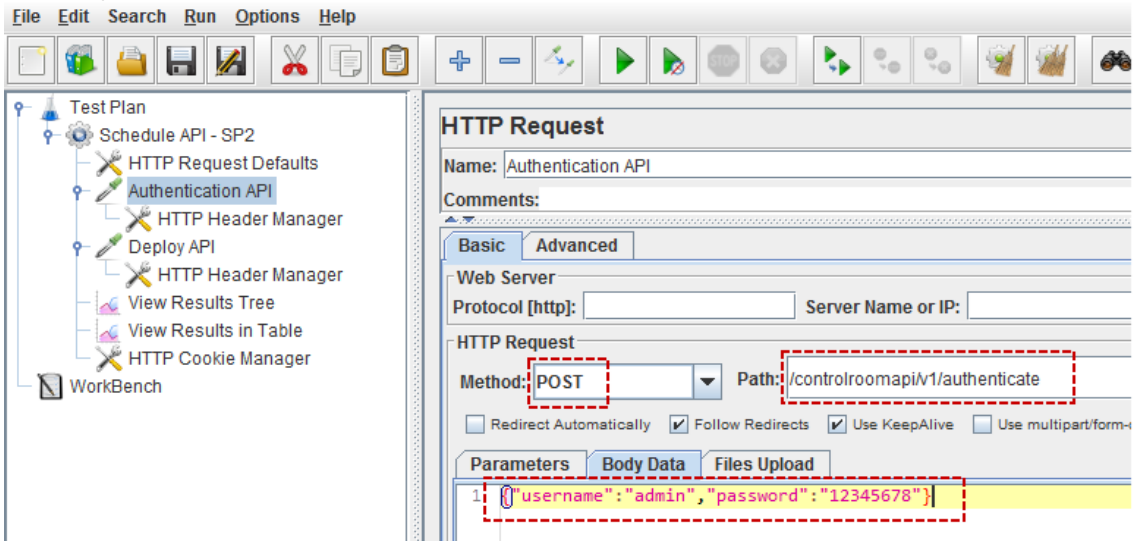
To test the APIs, you can use tools such as Apache JMeter.

Configuration Steps in JMeter:

1. Create a new Thread Group; in our case we have created a Thread Group named 'Schedule API - SP2' under the 'Test Plan' node.
2. Create a new 'HTTP Request Defaults' node under 'Schedule API - SP2'. You can do this by right clicking on 'Schedule API - SP2' and then clicking on Add > Config Element > HTTP Request Defaults.
3. In the 'HTTP Request Defaults' provide the **Web Server** details such as **Protocol, Server Name or IP** and **Port Number**.

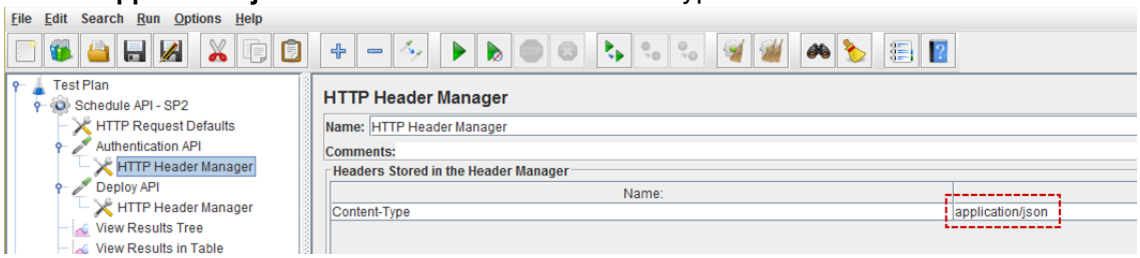


4. Create a new 'HTTP Request' node under 'Schedule API - SP2'. You can do this by right clicking on 'Schedule API - SP2' and then clicking on Add -> Sampler -> HTTP Request.
5. You can rename the 'HTTP Request' node to a user-friendly 'Authentication API'.
6. Under 'Authentication API', select the method as 'POST', provide the Path as **/controlroomapi/v1/authenticate** and the Control Room Credentials in JSON format (e.g. **{"username":"admin","password":"12345678"}**) under the 'Body Data'



7. Under the 'Authentication API' node, add one more node by right clicking on the node and selecting Add > Config Element > HTTP Header Manager.

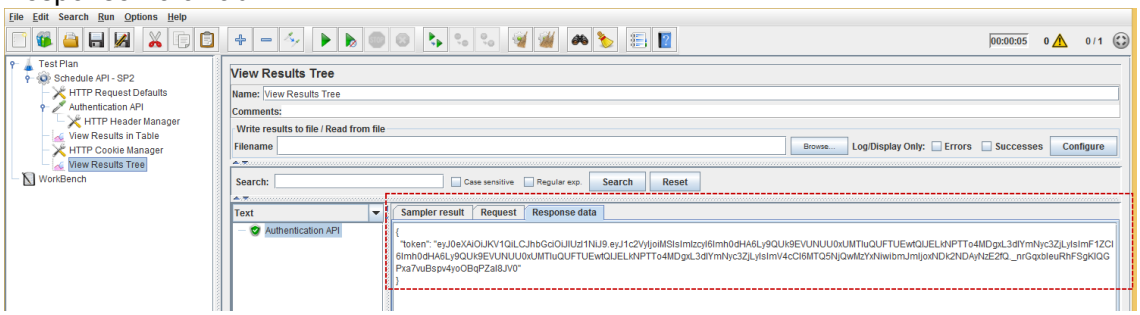
8. Provide **application/json** as the Value under Content-Type.



9. Add the 'View Results Tree' node by right clicking on 'Schedule API - SP2' and clicking on Add > Listener > View Results Tree.

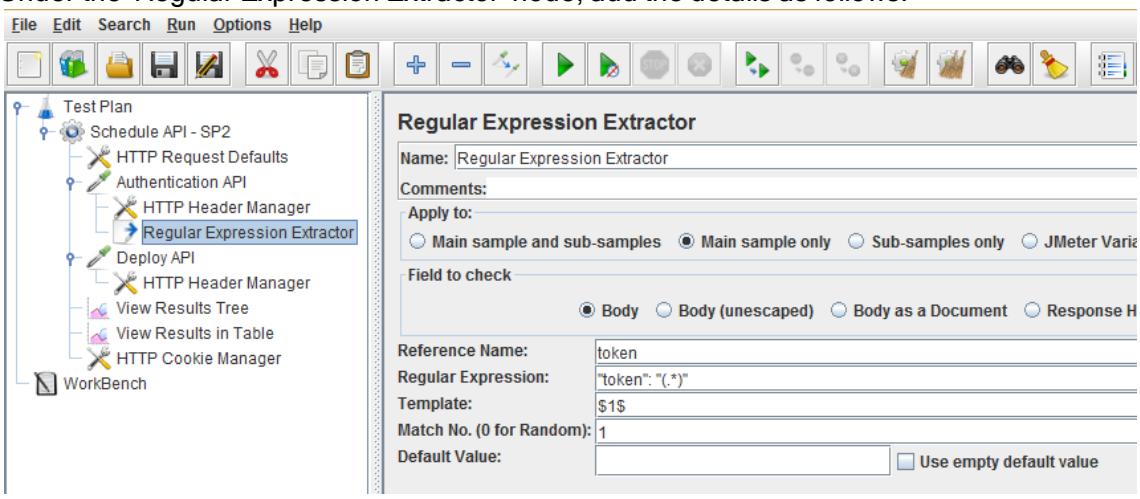
10. Click on **Play**

11. If authentication is successful, in the 'View Results Tree' node you will get the authentication token under the 'Response Data' tab.



12. Right click on 'Authentication API' node and click on Add -> Post Processors -> Regular Expression Extractors.

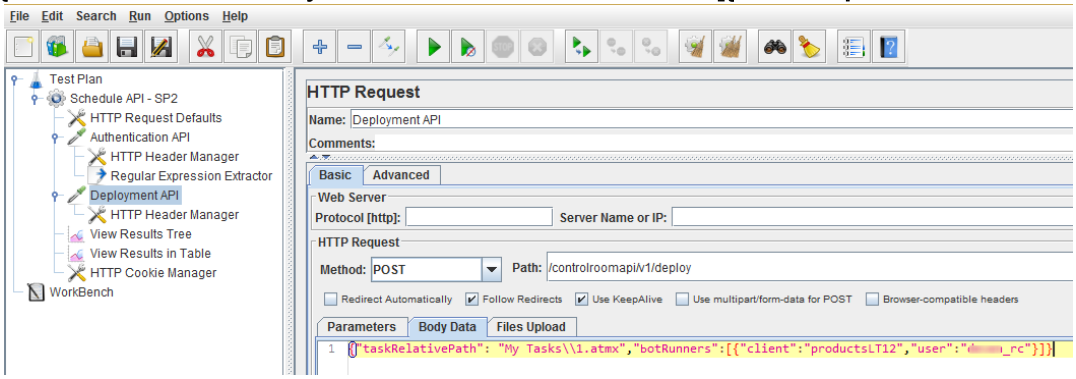
13. Under the 'Regular Expression Extractor' node, add the details as follows.



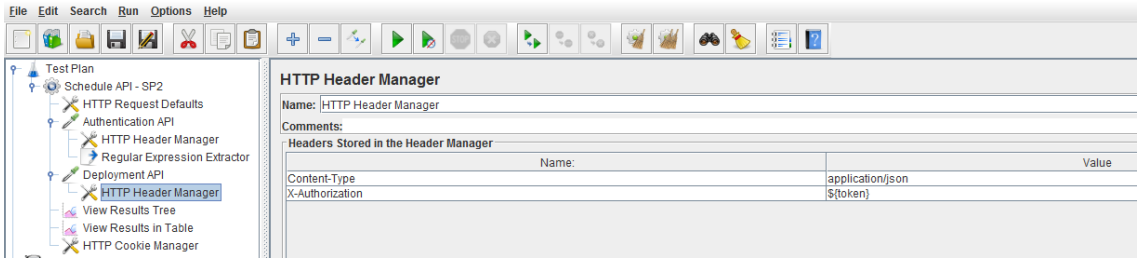
14. Add one more 'HTTP Request' node (named 'Deployment API') by right clicking on 'Schedule API - SP2' and clicking on Add -> Sampler -> HTTP Request.

15. In the 'Deployment API' node, specify the Method as **POST**, the Path as **/controlroomapi/v1/deploy** and the input JSON string.
JSON input for Deployment API - Example Scenario:
    - The Bot is 1.atmx under 'My Tasks' Folder.
    - The Bot Runner machine host name is productslt12
    - The Bot Runner user name is mike_rc, then the JSON string will be

{"taskRelativePath": "My Tasks\\1.atmx","botRunners":[{"client":"productsIt12","user":"mike_rc"}]}

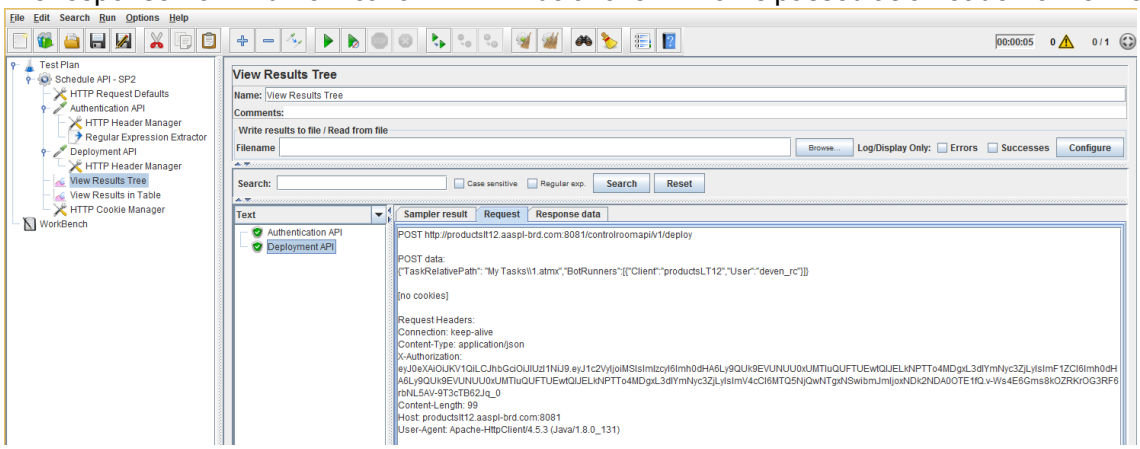


16. Add a ‘HTTP Header Manager’ node under ‘Deployment API’ by right clicking on ‘Deployment API’ node and selecting Add -> Config Element -> HTTP Header Manager.
17. Under the ‘HTTP Header Manager’ provide the input as shown in the image below.

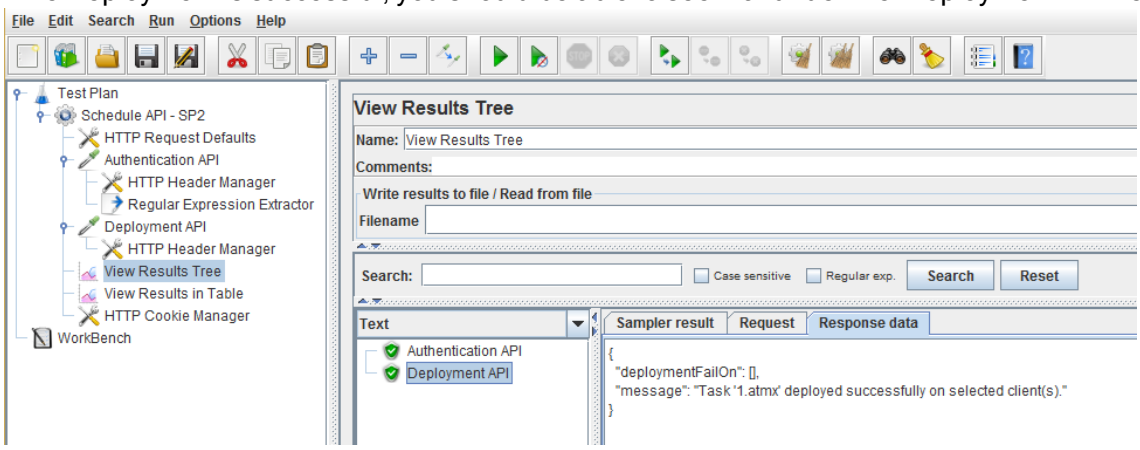


18. Click on **Play**

19. Under the ‘View Results Tree’ node, you will see the responses from both the APIs.
20. The response from ‘Authentication API’ will be a token which is passed as a header to the ‘Deployment API’



21. If the Deployment is successful, you should be able to see that under the 'Deployment API' response.



22. **More importantly,** the Bots should be deployed onto the Bot Runners specified in the JSON input for Deployment API.

Sample Code

APITest Java Class

```
package com.automationanywhere.sample;

import java.io.IOException;

public class APITest

{

   public static void main(String[] args) throws IOException

  {

   APIClient apiClient = new APIClient();

   apiClient.deployBotViaAPI();

   apiClient.deployBotViaAPIReadCSV();

 }

}
```

APIClient Java Class

```
package com.automationanywhere.sample;

import java.io.*;

import javax.json.*;

public class APIClient {

    private final static String AUTHENTICATE_API_URL = "http://product.aaspl-brd.-
com/controlroomapi/v1/authenticate";

    private final static String DEPLOY_API_URL = "http://product.aaspl-
brd.com/controlroomapi/v1/deploy";

    /* Deploy bot on single client using API */

    public void deployBotViaAPI() throws IOException {

        //Create authenticate request parameters

        String credential = getAPICredential();
```

```
        //Authenticate REST request
        String tokenResponse = RestHelper.restPostRequest(AUTHENTICATE_API_URL, credential,null);
        //Parse Authorization token token form authenticate REST request
        InputStream inputStream = new ByteArrayInputStream(tokenResponse.getBytes());
        JsonReader jsonReader = Json.createReader(inputStream);
        JsonObject object = jsonReader.readObject();
        jsonReader.close();
        String apiToken = object.getString("token");
        //Create deploy request parameters
        String deployParms = getBotDeployParameter();
        //deploy on bot using REST API
        String response = RestHelper.restPostRequest(DEPLOY_API_URL,deployParms,apiToken);
        System.out.println(response);
    }
    /* Read client information from CSV file, and deploy bot on multiple client using API. */
    public void deployBotViaAPIReadCSV() throws IOException {
        //Create authenticate request parameters
        String credential = getAPICredential();
        //Authenticate REST request
        String tokenResponse = RestHelper.restPostRequest(AUTHENTICATE_API_URL, credential, null);
        //Parse Authorization token token form authenticate REST request
        InputStream inputStream = new ByteArrayInputStream(tokenResponse.getBytes());
        JsonReader jsonReader = Json.createReader(inputStream);
        JsonObject object = jsonReader.readObject();
        jsonReader.close();
        String apiToken = object.getString("token");
        //Create deploy request parameters,read botRunners details from CSV
        String deployParms = getBotDeployParameterCSV();
        //deploy on bot using REST API
        String response = RestHelper.restPostRequest(DEPLOY_API_URL,deployParms,apiToken);
        System.out.println(response);
    }
    //create Json object for authenticate request
    private String getAPICredential() throws IOException {
        String userName = "admin";
        String userPass = "12345678";
```

```
        JsonObject model = Json.createObjectBuilder().add("username", userName).add("password", user-
Pass).build();

        return getJsonString(model);

    }

    //create Json object for deploying bot

    private String getBotDeployParameter() throws IOException {

        JsonObject model = Json.createObjectBuilder()

                .add("taskRelativePath", "My Tasks\\My Tasks\\Support\\TestSetText.atmx")

                .add("runWithRDP", "false")

                .add("botRunners", Json.createArrayBuilder()

                        .add(Json.createObjectBuilder().add("client", "product").add("user", "m")))

                .build();

        return getJsonString(model);

    }

    //Read botrunners from CSV file and create Json object for deploying bot

    private String getBotDeployParameterCSV() throws IOException {

        JsonArrayBuilder jsonArrayBuilder = Json.createArrayBuilder();

        String csvFile = "D:\\sample\\bots.csv";

        BufferedReader bufferedReader;

        String line = "";

        String cvsSplitBy = ",";

        bufferedReader = new BufferedReader(new FileReader(csvFile));

        while ((line = bufferedReader.readLine()) != null) {

            String[] bot = line.split(cvsSplitBy);

            jsonArrayBuilder.add(Json.createObjectBuilder().add("client",bot[0]).add("user",bot[1]));

        }

        bufferedReader.close();

        JsonObject model = Json.createObjectBuilder()

                .add("taskRelativePath", "My Tasks\\My Tasks\\Support\\TsetSetText.atmx")

                .add("WitrunhRDP", "false")

                .add("botRunners", jsonArrayBuilder)

                .build();

        return getJsonString(model);

    }

    //Generate Json string from model

    private String getJsonString(JsonObject model) throws IOException {

        StringWriter stringWriter = new StringWriter();
```

```
        JsonWriter jsonWriter = Json.createWriter(stringWriter);
        jsonWriter.writeObject(model);
        jsonWriter.close();
        stringWriter.close();
        return stringWriter.toString();
    }
}
```

RestHelper Java Class

```
package com.automationanywhere.sample;
import java.io.BufferedReader;
import java.io.IOException;
import java.io.InputStreamReader;
import java.io.OutputStream;
import java.net.HttpURLConnection;
import java.net.URL;
//Rest request helper
public class RestHelper {
    //Make REST API call
    public static String restPostRequest(String spec, String params, String token) {
        try {
   URL url = new URL(spec);
            HttpURLConnection conn = (HttpURLConnection) url.openConnection();
            conn.setDoOutput(true);
            conn.setRequestMethod("POST");
            conn.setRequestProperty("Content-Type", "application/json");
             if (token != null)
                conn.setRequestProperty("X-Authorization", token);
             OutputStream os = conn.getOutputStream();
            os.write(params.getBytes());
            os.flush();
            if (conn.getResponseCode() != HttpURLConnection.HTTP_OK) {
                throw new RuntimeException("Failed : HTTP error code : " + conn.getResponseCode());
            }
            BufferedReader bufferedReader = new BufferedReader(new InputStreamReader((con-
n.getInputStream())));
```

```
    String output;

            StringBuilder content = new StringBuilder();

            while ((output = bufferedReader.readLine()) != null) {

                content.append(output);

            }

            conn.disconnect();

            bufferedReader.close();

            return content.toString();

        } catch (IOException e) {

            e.printStackTrace();

            return "";

        }

    }

}
```

Sample Bot CSV (Applicable to above Java Scripts)

Data in csv should be specified as shown:

	A	B
1	client	user
2	client1	user1
3	client2	user2
4	client3	user3
5	client4	user4
6	client5	user5
7	client6	user6
8	client7	user7
9	client8	user8
10	client9	user9

VB Script to Deploy APIs

```
'AUTHENTICATION API - START
Set objStream = CreateObject("ADODB.Stream")
objStream.CharSet = "utf-8"
objStream.Open
objStream.LoadFromFile("D:\Mike.Lee\Office\Products\Product Demos - HandsON\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://products.mydomain.com:8081/controlroomapi/v1/authenticate", False

oWinHttp.setRequestHeader "Content-Type", contentType

oWinHttp.Send restRequest
```

```
response = oWinHttp.StatusText

MsgBox response

Dim AuthToken

AuthToken = oWinHttp.ResponseText

MsgBox AuthToken

'AUTHENTICATION API - ENDS

'--------------------------------------------------

'RESPONSE HEADER PARSING - START
Dim sToken

sToken = Right(AuthToken, Len(AuthToken) - 15)

'MsgBox(sToken)

sToken = Left(sToken, Len(sToken) - 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:\Mike.Lee\Office\Products\Product Demos - HandsON\deploy-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://products.mydomain.com:8081/controlroomapi/v1/deploy", False

oWinHttp.setRequestHeader "Content-Type", contentType

oWinHttp.setRequestHeader "X-Authorization", sToken

oWinHttp.Send restRequest

response = oWinHttp.StatusText

MsgBox response

Dim DeployResponse

DeployResponse = oWinHttp.ResponseText

'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
{"TaskRelativePath": "My Tasks\\InvoiceProcess.atmx","BotRunners":[{"Client":"ProdMachine1","User":"mike.lee"}]}

Control Room API to Get a List of Registered Clients

Available from Control Room 10.5.9 onwards

The Get Client API helps you to get a list and connection status of registered Clients in json format.

Notes:

- The Get Client API can ONLY be invoked once the system/user has been authenticated using the Authentication API. Refer Control Room Authentication API for details.
- The Control Room users must have the Client Management access permission.

Get Client API

Control Room URL and the path of the Get Client API:

API: /controlroomapi/v1/clients/get

Get Client API Response Codes

Http(s) Status code	Response	Description

200	{
	"clientDetails": [
	{
	"status": "Disconnected",
	"client": "WIN8PROX",
	"user": "runtime1",
	"clientType": "BotRunner",
	"applicationPath": "C:\\Users\\serviceuser\\Documents\\Automation Anywhere Files"
	},
	{
	"status": "Connected",
	"client": "WIN7PROX",
	"user": "devuser",
	"clientType": "BotCreator",
	"applicationPath": "C:\\Users\\serviceuser\\Documents\\Automation Anywhere Files"
	}
	]
	}
	{
	"status": "Disconnected",
	"client": "WIN7PROX64-TK",
	"user": "devtoRuntime",
	"clientType": "BotCreator",
	"applicationPath": "C:\\Users\\svc_cr_user.SYMPHONY\\Documents\\Automation Anywhere Files"
		A list of registered Bot Runners and Bot Creators is fetched successfully.

},

{

"status": "Disconnected",

"client": "WIN7PROX64-TK",

"user": "runtimetoDev",

"clientType": "BotCreator",

"applicationPath": "C:\\Users\\svc_cr_user.SYMPHONY\\Documents\\Automation Anywhere Files"

}

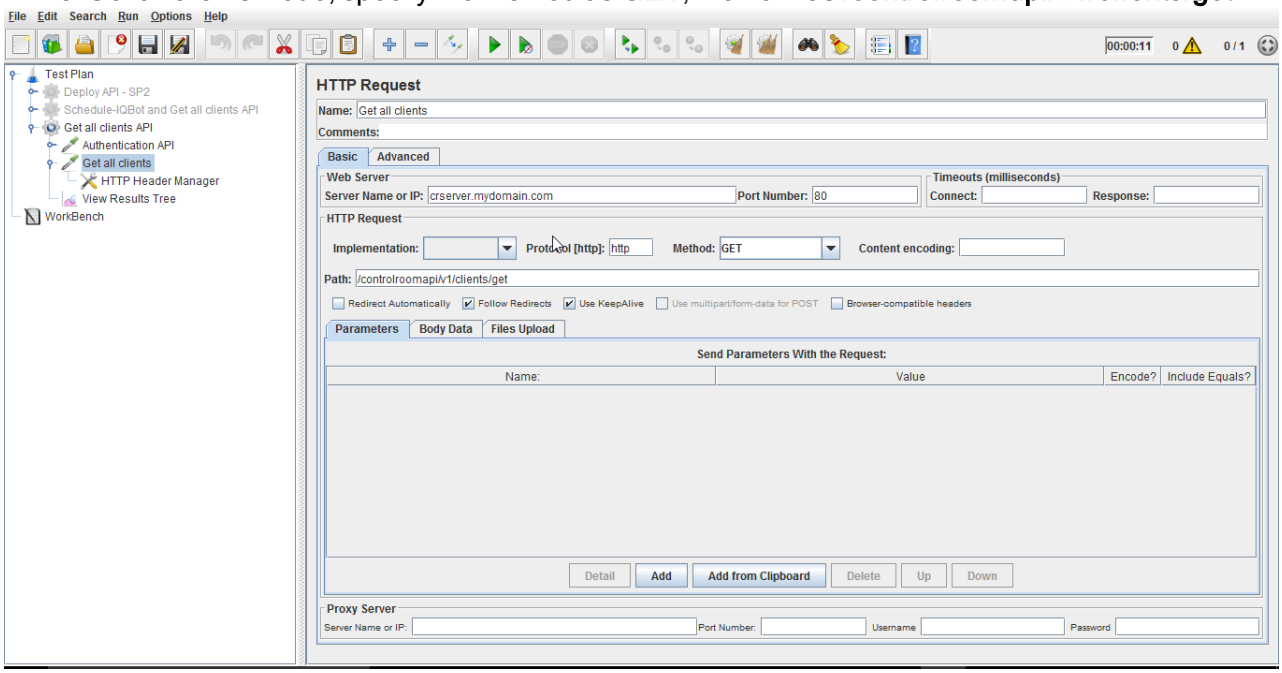
]

}

401	{ "message": "Requested user does not have permission." }	The token has expired, or token is invalid, license has expired, or when Control Room credentials/ details are invalid.
403	{"message": "Insufficient privileges."}	A user does not have sufficient privileges.

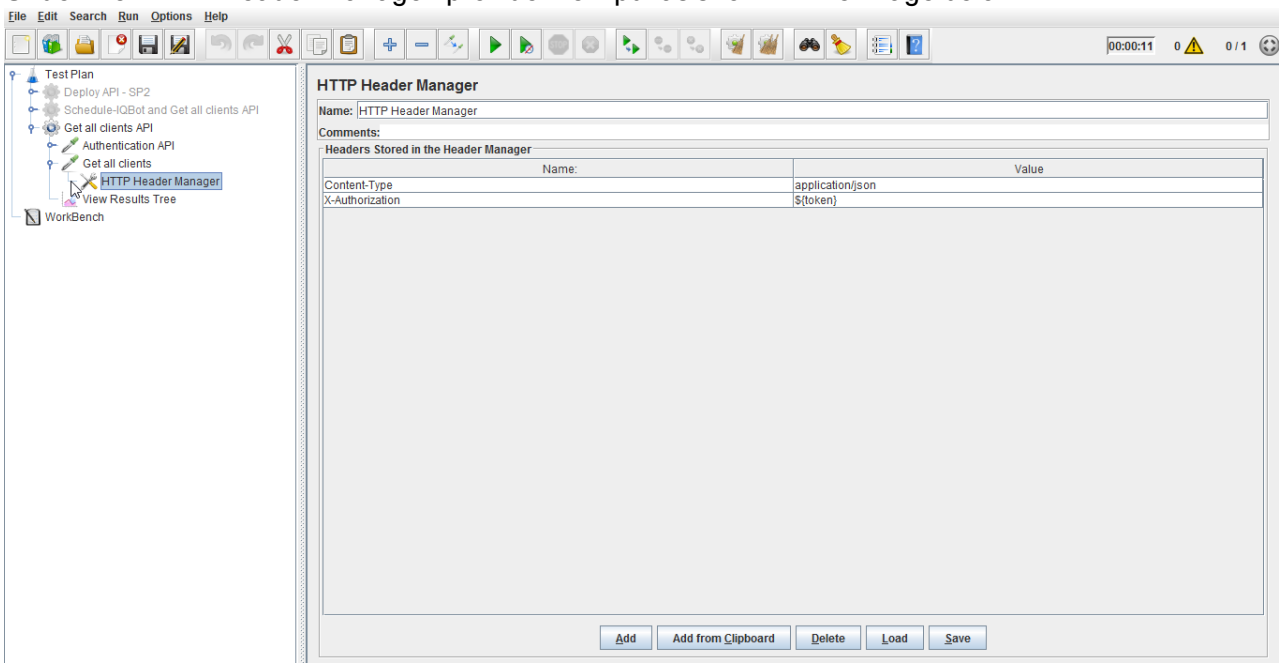
Sample for getting list of registered clients using Jmeter

1. Add one more 'HTTP Request' node (named 'Get all clients') by right clicking on the thread group and click on Add -> Sampler -> HTTP Request.
2. In the 'Get all clients' node, specify the Method as **GET**, the Path as **/controlroomapi/v1/clients/get**.



3. Add a 'HTTP Header Manager' node under 'Get all clients' by right clicking on the node and select Add -> Config Element -> HTTP Header Manager.

4. Under the 'HTTP Header Manager' provide the input as shown in the image below.



Note: The response from 'Authentication API' will be a "token" which is passed as a header to the 'Get all clients' as X-Authorization header parameter.

5. Click on **Play**

6. The response of the API will be visible in the View Results Tree.