**Configure the Control Room**

Before you start creating workflows for bot deployment and workload management using Control Room APIs, ensure you complete specific prerequisites and steps in the Control Room.

## **Prerequisites**

Ensure you have following licenses and permissions:

* One or more Bot Creator and unattended Bot Runner licenses.
* Control Room admin credentials to view, create, and configure users, roles, and device pools.
* The **Create device pools** feature permission or the **AAE\_Pool Admin** role must be assigned to you.

## **Procedure**

Follow these steps to configure your Control Room with users, roles, and bots.

1. Log in to the Control Room as an admin.
2. Create a Control Room user.

Ensure that the user is assigned the **AAE\_BASIC** role.

[Create a user](https://docs.automationanywhere.com/bundle/enterprise-v2019/page/enterprise-cloud/topics/control-room/administration/users/cloud-create-user.html)

# Create a user

Create a user and assign their specific license based role.

Ensure that you are logged in to the Control Room as the administrator.

## Procedure

1. Navigate to **Administration** > **Users**.
2. Click **Create user**.
3. Enter the required general details as follows:

| **Field** | **Value** |
| --- | --- |
| **Enable User** | Select for the user to be activated and log in immediately.  **Note:** If this option is not selected, user will be in the inactive state and cannot log in. |
| **Username** | Enter a unique user name. |
| **Description** | Enter a description for the user. |
| **First name** | Enter the first name for the user.  **Note:** The number of characters allowed in the **First name** field is 50. |
| **Last name** | Enter the last name for the user.  **Note:** The number of characters allowed in the **Last name** field is 50. |
| **Password** | Enter and confirm a password for the user. Ensure that the password follows all the necessary password policies. |
| **Email** | Enter and confirm the email address for the user.  If SMTP is enabled, an email is sent to this address to confirm the account. All important Control Room notifications are sent to this email address. |

1. Select the required role from the list of **Available roles**.
2. Click the right arrow (**→**) to add your selection.
3. Select **Allow** to allow multiple sessions.

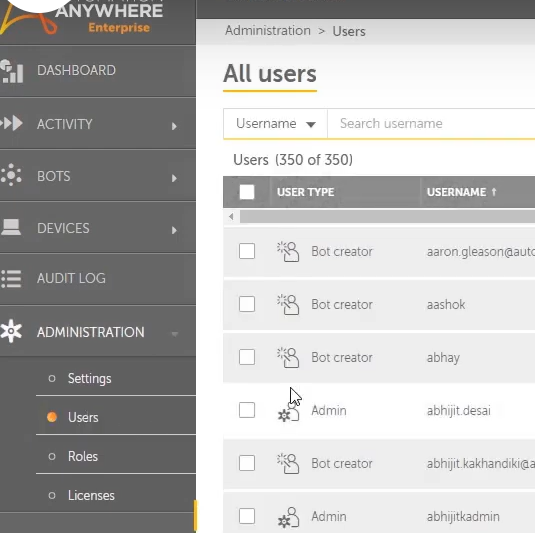
You must be Control Room administrator to set a user as a multi-login service user. It is possible to set a user as a multi-login user either in the UI or API, however a user may only access multiple sessions through the API.

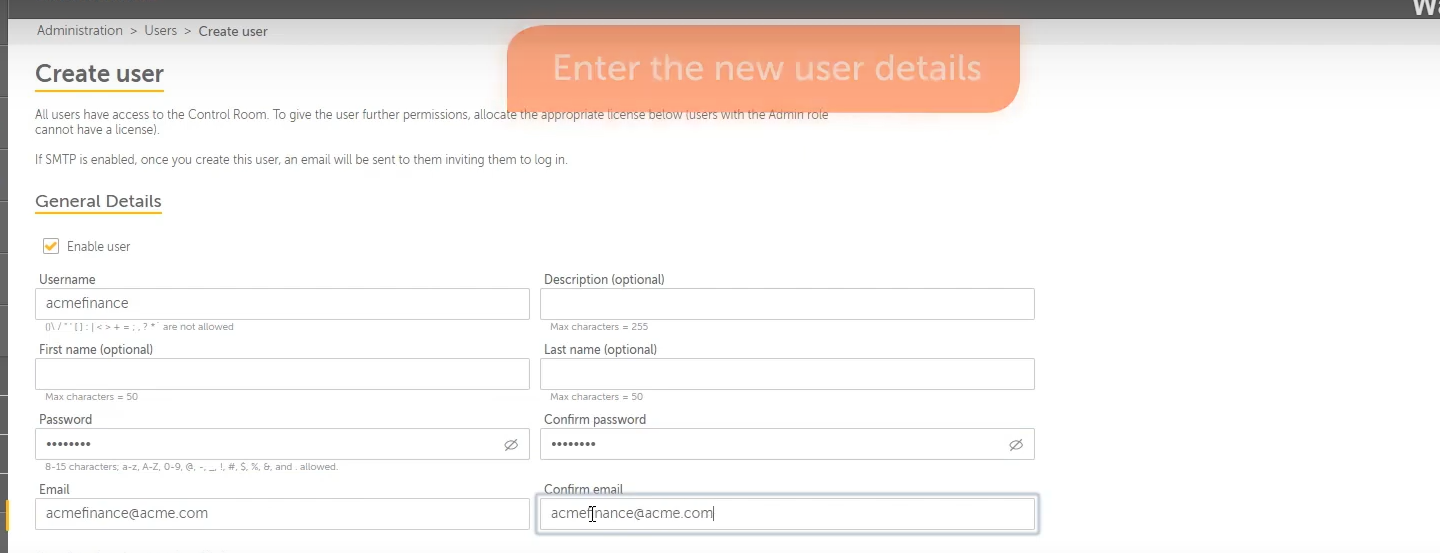
1. Assign a device license to the user.

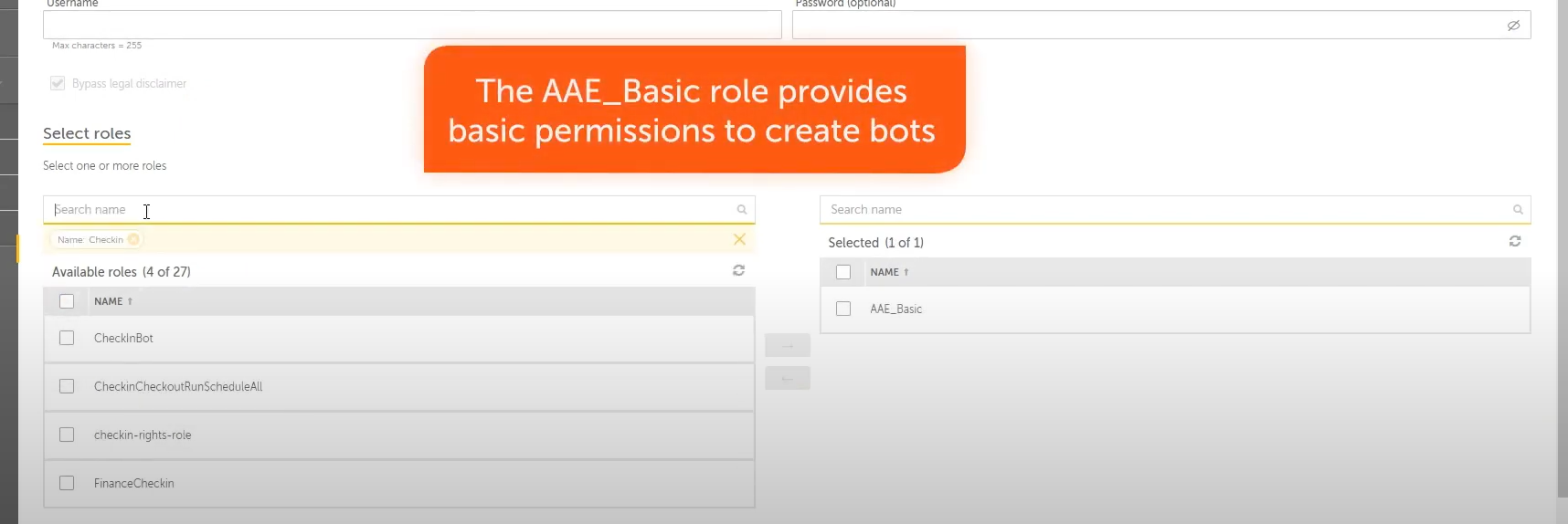
**Note:** When you logged in as administrator, you cannot allocate any device license to the user and **None** option is selected by default.

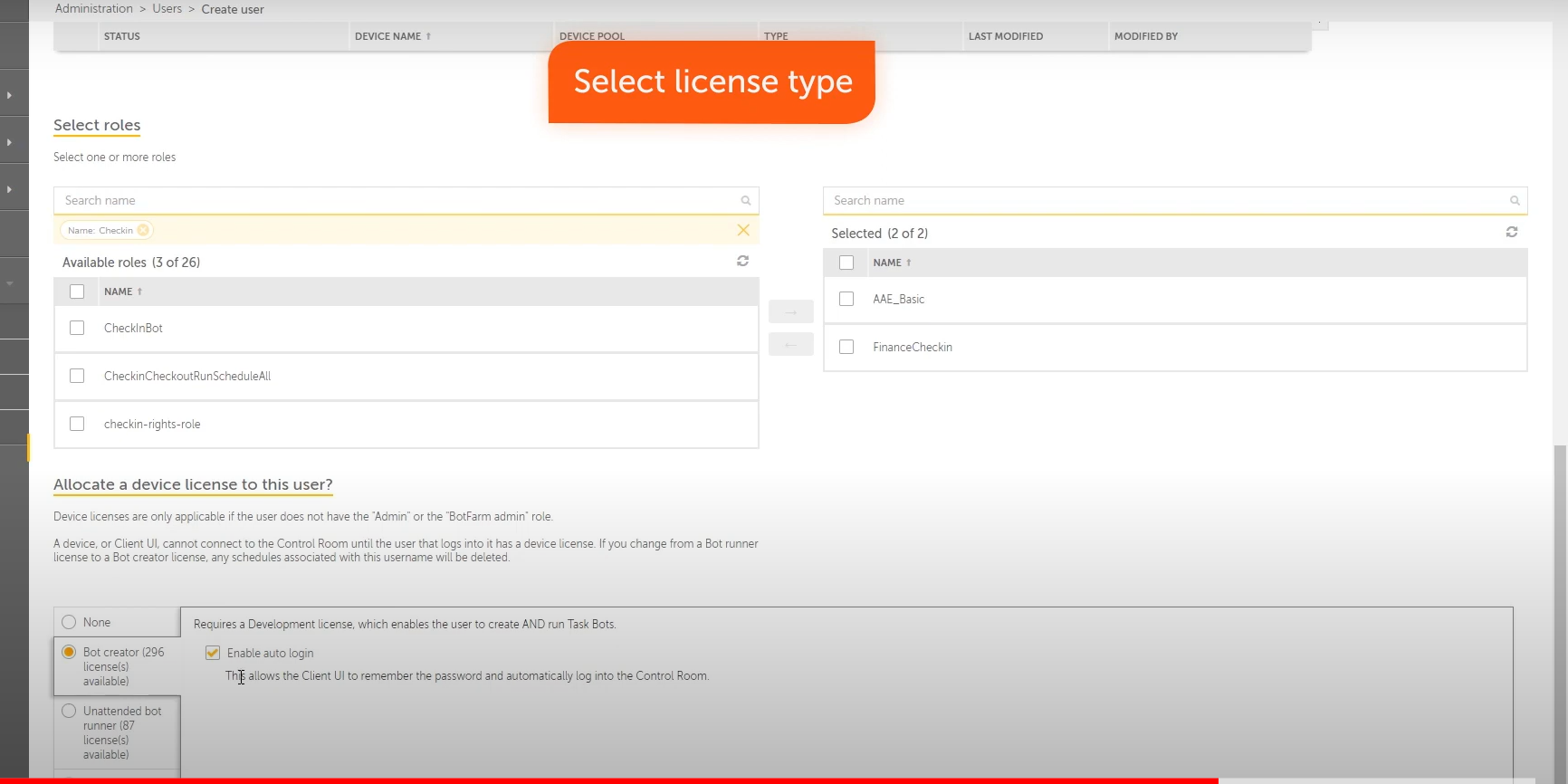
| **License** | **Privilege** |
| --- | --- |
| **None** | The user can access the Control Room only. |
| **Bot Creator- Development license** | Enables user to create and run bots. Auto login is enabled by default. |
| **Unattended Bot Runner - Run-time license** | Users with this license can perform all automation tasks that attended users can perform. Additionally, this license can also be used for Control Room deployment, centralized scheduling, and API-based deployment. |
| **Attended Bot Runner - Run-time license** | Users with this license can run bots on their devices and use any event trigger associated with their user account or role. However, these users cannot schedule bots. |
| **Citizen Developer - Development license** | Users with this license can create and run bots (including bots with triggers) on their devices. |

1. The **Bypass legal disclaimer** option is automatically enabled to allow the user to run bots on a device without having to manually acknowledge a disclaimer.
2. After you select a device license, the **Device login credentials** are enabled. If you have the **Attest device credentials** permission, you can choose to attest the device credentials for this user to bypass credential validation when you deploy bots. The Bot Runner user should have an unlocked and active user session.
3. **Note:** This works only if the auto login setting **Reuse an existing session** is selected in the Control Room by the administrator.
4. Click **Create user**.









---------------------End Create User -----------------------------

# Citizen Developer :

A Citizen Developer is a business user who can create and run bots, and share these automated tasks with peers. Citizen Developer is typically not a technical expert but a specialist such as a marketing analyst, HR manager, and accounts manager.

In an organization, an administrator typically creates the Citizen Developer role with the necessary bot permissions and specifies the database or folder access. The administrator assigns this role to existing or new users and allocates the Citizen Developer license to them.

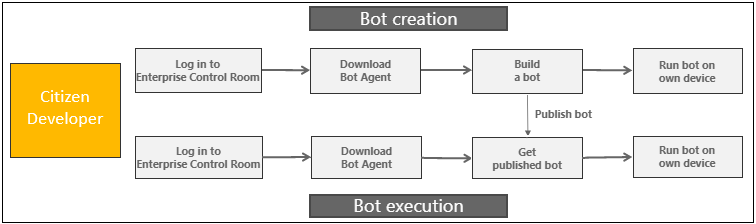
A Citizen Developer user can then perform the following tasks:

* Create bots and run them on their devices.
* Add and delete event triggers for bots on their devices.

Citizen developer user can create a private event trigger. However, the associated bot must be checked in to a public folder for other citizen developer or Bot Runner users to access that event trigger.

* Publish their bots to the public folder where other Citizen Developer users can access them.
* Access the public folder and clone published bots (including bots with triggers).
* Customize cloned bots and run them on their devices.
* Check in bots from their devices to the public folder.
* Check out bots from the public folder.

The following image illustrates the capabilities of a Citizen Developer user:



## Example

Consider a scenario where an organization has Marketing and Finance teams. The administrator creates the following two Citizen Developer roles:

* CD (Marketing): provides access to all Marketing team folders
* CD (Finance): provides access to all Finance team folders

The administrator then assigns the Citizen Developer license to users within each team. Citizen Developer users with the CD (Marketing) role can create and run bots on their devices. When a user with the CD (Marketing) role publishes a bot to a public folder, other Citizen Developer users within the Marketing team can clone and run this bot on their devices.

Similarly, Citizen Developer users with the CD (Finance) role will have the same capabilities within the Finance team folders. However, users from one team cannot access any folders and published bots from the other team.

## Comparing Citizen Developer and Bot Creator licenses

Understand the capabilities available for each user to help you choose license based on the automation requirements for your organization.

**Citizen Developer license**

Citizen Developers are business users who can create simple automations with little to no coding knowledge. A Citizen Developer license is designed for a business user such as marketing analyst, HR manager, and accounts manager. They have limited technical knowledge but have strong practical experience in the business processes. This helps them create simple, easy-to-use applications to improve the business processes. Based on the business requirements, an administrator can restrict package access for bot development to a Citizen Developer to provide a simplified developer experience. Complex packages are hidden from Citizen Developers so that they can focus on easy-to-complete automation.

**Bot Creator license**

Bot Creators are advanced developers who design, develop, and implement bots to improve business process efficiency and have substantial coding knowledge. A Bot Creator license is designed for professional developers who have strong technical knowledge and can build complex and critical applications. Depending on the privileges provided by the administrator, they can access more functionalities in the Automation 360 platform such as advanced and complex packages, ability to create API tasks, approve code reviews submitted by Citizen Developers, and so on.

Review the capabilities available for a Citizen Developer and Bot Creator license:

|  |  |
| --- | --- |
| **Citizen Developer** | **Bot Creator** |
| **Business user with strong process knowledge but limited coding skills** | Professional developer with strong technical skills and knowledge of system architecture |
| **Does not have access to advanced packages or features** | Has access to advanced packages and features |
| **Low coding knowledge** | In depth knowledge about coding and system architecture |
| **Builds simple applications to simply business processes** | Build complex and critical applications for business processes |
| **Does not have to follow the software development lifecycle to build applications** | Follows software development lifecycle to build applications |
| **Low cost and resource is easily available** | High cost and resource not easily available |

----------------------------------------------------Citizen Developer End -------------------------

# Create device pools

What is a device pool?

A device pool is a logical grouping of similar type of devices on which bots are run as work items from their respective queues. For example, you can group devices of a particular department/unit and create a device pool for it.

What is queue in Automation Anywhere?

A queue is one of the main building blocks of Workload Management. A queue holds data known as Work Items for further processing. The system distributes these Work Items to individual unattended Bot Runners in a device pool for processing.

What is audit log in Automation Anywhere?

Audit Log displays a read-only table of records of actions performed by users. These log records are searchable and exportable. Audit logs include both Successful and Unsuccessful actions attempted.

Create a device pool with a unique name and add Unattended Bot Runners to the device pool.

## **Prerequisites**

* Ensure that you have one of the following roles to view the **Device Pools** tab:
  + **Device pool owner**
  + **Device pool admin**
* Ensure that you have a role with **Create device pools** permission to create a device pool.

**Note:** A Control Room administrator without device pool admin rights cannot view or create a device pool.

* To add a device in the device pool, you must install it as a system-wide device (Bot Agent).
* After you add the device, you cannot add the same device to another device pool.
* You can add only those Unattended Bot Runners that are not part of any other pool.

**Restriction:** Unattended Bot Runners that are a part of other device pools are disabled for selection.

* You can use the **Scheduled automations** and **Run with Queue automations** options to run bots on that device.
* You can add Control Room user roles as consumers. Only users with these roles can use the pool for any automation.
* You can select only those devices with the Bot Runner installed at the system wide.
* If the devices in a device pool are more than the number of work items added to a queue, multiple entries equal to the number of devices are shown in the Control Room In-progress activity and Historical pages. For details, refer to the View queue details page on the actual user device on which the workload automation is deployed.

1. Create a custom role to map the users you created to Bot Runners and Bot folders.
   1. In the **Features** tab, ensure you select these permissions: **View my Scheduled Bots**, **Schedule my bots to run**, **Run my Bots**, **View my Bots**, and **Generate my API Key**.
   2. In the **Automation** tab, expand the **Bots** folder and select the root folder or subfolders you want to provide access for use. Ensure you select these permissions: **Run and schedule** and **View content**.
   3. In the **Run as** tab, select one or more Bot Runners from the list of **Available bot runners**.
   4. In the **Users** tab, select the new user created in Step 1 to assign the custom role to this new user.

To create a device pool, perform the following steps:

## Procedure

1. Navigate to **Manage** > **Device pools**.
2. Click **Create device pool**.
3. Enter the **Name**.
4. **Optional:**Enter a description.
5. Select the **Devices** from the list of Bot Runners.
6. Click the right arrow (**→**) to add your selection.
7. Click **Next**.
8. Select the Device Pool **Owners**.
9. Select user(s) from the **Available users** list.

**Tip:** Search the list of users based on their **Username**, **First name**, or **Last name**.

1. Click the right arrow (**→**) to add your selection.
2. Click **Next**.
3. **Optional:**Select the **Device Pool Consumers**.

Complete this step to enable device pool consumers to view the device pool when they run the automation for the bot with a queue by following the next set of steps.

1. **Optional:**Select a Role from the list of **Available roles**.
2. Click the right arrow (**→**) to add your selection.
3. Click **Create device pool**.

The device pools for which you have consumer privileges are listed in the **My Device Pools** page.

# Manage Automation 360

# <https://docs.automationanywhere.com/bundle/enterprise-v2019/page/enterprise-cloud/topics/aae-client/bot-creator/using-the-workbench/cloud-manage.html>

From the Control Room, you can also monitor and manage all activities to ensure a secure and seamless bot execution environment for your users.

## Activity and audit log

Monitor and manage automations, such as bot execution, scheduled and event trigger activities using the Activity console (**Activity** from the left menu). You can also review and troubleshoot any failed activities using the Audit log console (**Administration** > **Audit log**).

**Historical** **activity**

You can search, view, and run previously created bots in the **Activity**> **Historical** page.

The following image shows the **Time filter** option on the Historical activity page:  


For example, to view historical activities from May 10th to May 15th:

**Important:**

* Multiple workload automation entries equal to the number of devices are shown on the Historical activity page, if the work items added to a queue are less than the number of devices available in a device pool. For workload automation details, refer to the View queue details page on the actual user device on which the workload automation was deployed.
* Historical activity displays only the bots that are processing the work items, while each bot deployment can include multiple work items processed as one activity.

# Event triggers

An event trigger is a predefined action that runs an associated bot. All the bots with event triggers are listed under the **Event triggers** tab.

## Available role permissions for event triggers

A Control Room administrator must provide the required permissions to ensure the associated users can access event triggers. The following table lists the available permissions:

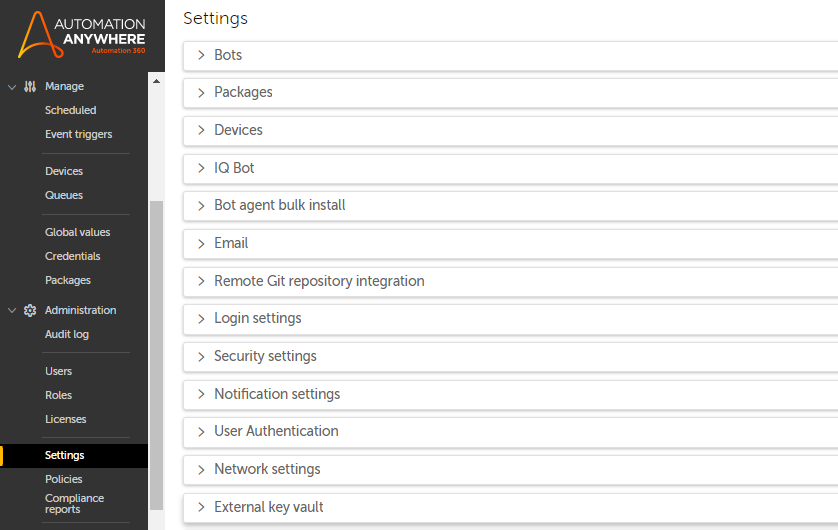
## Bot life cycle audit logs

The entry shows the status of each stage of the bot life cycle.

## Settings

After initial setup of the Control Room, you (as an administrator) might have to set up and edit some of the initial configurations to enable certain features. Go to **Administration**> **Settings** to configure and edit settings for bots, packages, devices, email, network, user authentication, security, Git repository, external key vault and so on.

The following image shows some of these settings:



Use the **Settings** tab to configure the connection to the Credential Vault, enable email notifications, integrate the Control Room with a Git repository, enable secure recording mode, and configure user authentication.

## Bots

* Secure recording mode ensures that sensitive data is not stored in the bots. When secure recording mode is enabled, the bots do not capture values of certain properties or store application images. You can enable this setting for some or all users of the Control Room.

**Note:** Secure recording mode only applies to bots that are created or edited after the mode is enabled.

Click **Edit** in the **Bots** tab to enable or disable secure recording mode. See [Secure recording](https://docs.automationanywhere.com/bundle/enterprise-v2019/page/enterprise-cloud/topics/security-architecture/cloud-secure-recording.html).

* Bot validation performs an additional compile time validation on migrated bots at the preprocessing stage to save your time and effort. By default, the Bot validation feature is set to **Off**.

**Note:** You must be a Control Room administrator to view and edit the validation option.

Navigate to **Administration** > **Settings** > **Bots** and set the bot validation option to **On** to detect compilation errors with bots.

Validation happens at the time of running the bot, for new bots. For migrated bots, this check is performed immediately after bot migration, per configuration.

For example, if a parent bot calls a child bot and the child bot has compilation errors, these errors are displayed when you try to run the parent bot. This ensures that an error does not occur in the middle of an automation or make it an incomplete automation.

In the Bot migration results page, select a bot that needs review. Click the three dots under **Reason** tab to see the details. With the Bot validation feature set to **On**, the bots that have compile time errors are displayed as a separate line entry in the migration report.

Migrated bots with compilation errors are shown in **Successful with Review** section of the migration report and ensures that you can get a list of bots that require your attention.

* Loop package enables you to run a sequence of actions repeatedly for a specific number of times or until a specific condition is met.

For bots that were created using the Loop action in Automation 360 v.26 or earlier releases, you can enable the **Legacy Loop behavior** option from the **Administration** > **Settings** to iterate the loop based on the specified value.

In the **Legacy Loop behavior** tab, click **Edit** to select one of the following options:

* 1. **Enabled**: Loop is iterated based on the specified value. When you select this option and either increment or decrement the variable value in the end condition, loop iterations will not vary dynamically based on the new value generated.
  2. **Disabled**: Loop iterations will continue to vary dynamically based on the variable value generated in the end condition.

## Policies

**Code Analysis**: Enable the code analysis feature to run code analysis on your automations. This feature analyzes the code and displays a list of violations based on a set rules. You can review and fix any coding or stylistic errors for your automation.

[Code analysis](https://docs.automationanywhere.com/bundle/enterprise-v2019/page/enterprise-cloud/topics/control-room/administration/settings/code-analysis.html)| [Code analysis policy management](https://docs.automationanywhere.com/bundle/enterprise-v2019/page/enterprise-cloud/topics/control-room/administration/settings/ca-policy-management.html)

## Devices

When there is a new version of the Bot Agent, it is automatically updated.

## IQ Bot

View the website address where IQ Bot is currently installed, if applicable. Click **Edit** to update the IQ Bot URL.

## Email

All users must confirm email accounts by clicking the confirmation link that they receive, set the password, and security questions before user can log in to the Automation Anywhere Control Room. By default, email notifications are disabled. Hover over the **Edit** icon to make changes.

[Edit email notifications](https://docs.automationanywhere.com/bundle/enterprise-v2019/page/enterprise-cloud/topics/control-room/administration/settings/cloud-edit-email-notification.html)

## Git integration

Remote Git repository must support Git LFS (Large File Support). Bots are synced using standard Git push over HTTPS.

## CoE Manager

Enable access to CoE Manager from the Control Room so that you can access CoE Manager from the quick links section on the Control Room home page.

[Enable CoE Manager](https://docs.automationanywhere.com/bundle/enterprise-v2019/page/enterprise-cloud/topics/coe-manager/topics/enable-coe-manager.html)

## Login settings

For security, privacy, or any other pertinent announcement, you can provide an additional statement, such as consent text, in the **Login settings** section. The statement is visible to users every time they log in to the Control Room.

This statement on the login page is disabled by default. If you enable it, you can also provide an option (using a check box) for users to read and accept the statement before logging in to the Control Room.

## Security settings

**Password Configuration**

Administrators can configure password requirements for users to log in to the Control Room. This configuration prevents users from setting weak or most commonly used passwords that might prevent unauthorized access to the Control Room.

**Password length (characters)**: Password length determines the strength of a password.

* **Minimum**: Set the minimum number of characters allowed for the password. By default, the minimum number of characters is set to eight and the number cannot be reduced further.
* **Maximum**: Set the maximum number of characters allowed for the password. By default, the maximum number of characters is set to 50 and cannot be set to more than 64 characters.

You can also enforce the users to include one of the following characters in the password:

* A number
* An alphanumeric letter
* A symbol
* A capital letter

**Note:**

* On-Premises users: The check-boxes for **Alphabetical character**, **Number**, **Capital letter**, and **Special character** are enabled, and the user can select or deselect the options.
* Cloud users: The check-boxes for **Alphabetical character**, **Number**, **Capital letter**, and **Special character** are disabled, and the user cannot select or deselect the options.

**Repetitive Characters**: Repetitive characters such as aaaa, bbbb, cccc, and so on in passwords make it easier for attackers to guess the password and are considered to be weak passwords.

* **Allow unlimited repetitive characters**: This option is set as default and allows users to use unlimited repetitive characters in their passwords. Selecting this option might allow users to set weak passwords and vulnerable to attacks.
* **Limit repetitive characters**: Select this option to restrict the users from using repetitive characters in their passwords. Set the repetitive characters limit in the **Maximum characters can be repeated** option. If you set this limit as one, then no characters in the password can be repeated. If you set this limit as two, users can use two repetitive characters in their passwords. For example, users can use aa, bb, and so on in their passwords.

**Sequence Characters**: Sequential characters such as qwerty, 123456, abc123, and so on in passwords make it easier for attackers to guess the password and are considered to be weak passwords.

* **Allow unlimited sequence characters**: This option is set as default and allows users to use unlimited sequential characters in their passwords. Selecting this option might allow users to set weak passwords and vulnerable to attacks.
* **Limit sequence characters**: Select this option to restrict the users from using sequential characters in their passwords. Set the sequential characters limit in the **Maximum characters can be used in sequence** option. If you set this limit as one, then no characters in the password can be used in a sequence. If you set this limit as two, users can use two sequential characters in their passwords. For example, users can use 12, ab, and so on in their passwords.

**Restrict common passwords from the system**: Allowing users to use common passwords such as 123456, qwerty123, 1q2w3e, and so on makes it easier for attackers to guess the passwords and are considered to be weak passwords.

* **Do not restrict common passwords**: This option is set as default and allows users to use commonly used passwords. Selecting this option might allow users to set weak passwords and vulnerable to attacks.
* **Restrict common passwords**: Select this option to restrict the commonly used passwords. Add the commonly used passwords on separate lines in the text box to avoid users using such passwords.

**Set minimum number of days before a user can change their password**: If you allow users to change their passwords anytime, they can continue to use the same password even if there is a restriction about not using the last few instances of their passwords. Fox example, if a user is prompted to change their password and restricted to not use any of their last three passwords, the user can change the password three time continuously and set their existing password the fourth time. Setting a minimum number of days before a user can change their password restricts the user from using the same password when they are prompted to change their password.

* **Disabled**: This option is set as default and allows users to change their passwords anytime. Selecting this option might allow users to use the same password and vulnerable to attacks.
* **Enabled**: Select this option to set the number of days users are restricted from changing their passwords. The maximum number of days that you can set is 10. For example, if you set the days to five, a user can change their password again only after five days of changing their password.

**Captcha and user lockout**: This option prevents attackers from using scripts or bots to guess user credentials and locks the user account after certain unsuccessful login attempts.

* **Captcha on**: This option is set as default and prompts users to solve a captcha before logging into their account. Set the **Lock the user out after unsuccessful login attempts** option to lock the user after the set number of unsuccessful login attempts.
* **Lockout on**: Set the **Lock the user out after unsuccessful login attempts** option to lock the user after the set number of unsuccessful login attempts.

**API-Key duration**

The generated API-Key is used to authenticate users. You can customize how long the generated API-Key is valid to authenticate users until either:

* A selected duration is reached (in minutes or days), or
* A new API-Key is generated

**Note:** You determine the validity duration based on your organization's requirements. Maximum supported API-Key duration is 1 to 14,398,560 minutes, or 1 to 9,999 days.

**Time-out session settings**

You can enable time-out settings to automatically sign out users from the Control Room browser session after the specified minutes of inactivity. You can set the **Time-out session setting** field to one of the following values: 10 minutes, 20 minutes, 30 minutes, 40 minutes, 50 minutes, 1 hour, 2 hours, 4 hours, 8 hours, 12 hours, 24 hours, or 7 days. You can configure the session using increments of 10 minutes or 1 hour. The default value is 20 minutes, which means you will be logged out of the session after 20 minutes of inactivity.

**File upload settings**

As an Administrator, you can restrict the upload of executable files (dll files, media type application/x-msdownload) to prevent a security breach. To use this feature, enable the **File upload settings** in **Administration** > **Settings** > **Security settings**.

**Two factor authentication (2FA)**

Enable 2FA to provide an additional layer of defense against unauthorized users from accessing the Control Room. As an administrator, you can set up 2FA so that the users can validate their identity when logging in to the Control Room using both their user credentials and a second authentication factor.

[Two-factor authentication](https://docs.automationanywhere.com/bundle/enterprise-v2019/page/enterprise-cloud/topics/control-room/administration/settings/two-factor-authentication.html)

**Audit log retention**

If you want to retain audit log entries for only a limited period to save storage space or if you do not want to retain historical audit log entries, configure your settings to automatically purge (delete) such entries.

* **Do not purge**: Audit log entries are retained and never deleted.
* **Purge older than 15 months**: Audit log entries that are older than 15 months are automatically deleted.
* If you are updating to v.30 release from a previous release, then you must manually enable the **Purge older than 15 months** option.
* If you are directly setting up v.30 or later releases, the **Purge older than 15 months** option is enabled by default.
* The audit log entries are deleted once a week from the time the **Purge older than 15 months** option is enabled.

**Bot promotion settings**

Add the approved list of target URLs so that you can move bots and files between Control Room instances in a single flow, thus avoiding the multi-step export and import process.

[Move bots across environments](https://docs.automationanywhere.com/bundle/enterprise-v2019/page/move-bots-across-environments.html)

## Notification settings

Manage the notification settings for notification categories and channels. The notification settings defined by the Control Room administrator are applicable for all the Control Room users. Based on these defined settings, Control Room users will be notified about the events.

[Administer notifications for Control Room](https://docs.automationanywhere.com/bundle/enterprise-v2019/page/enterprise-cloud/topics/control-room/administration/administering-alerts-notifications.html).

## User authentication

Configure the to authenticate users through the database option or switch to a SAML Identity Provider (IdP).

[Set up SAML authentication](https://docs.automationanywhere.com/bundle/enterprise-v2019/page/enterprise-cloud/topics/control-room/getting-started/cloud-switch-saml.html)

## Network settings

**Forward Proxy Configuration**

Configure a forward proxy so that Control Room features can connect to Cloud-hosted Control Room services outside of customer's internal network.

[Configure forward proxy settings](https://docs.automationanywhere.com/bundle/enterprise-v2019/page/configure-forward-proxy.html)

## External key vault

[External key vaults](https://docs.automationanywhere.com/bundle/enterprise-v2019/page/enterprise-cloud/topics/control-room/key-vault/external-key-vault-overview.html) provide a way to securely store and retrieve credentials using a third-party key manager such as CyberArk, Azure, and AWS Secrets Manager.

* [**Manage device settings**](https://docs.automationanywhere.com/bundle/enterprise-v2019/page/enterprise-cloud/topics/control-room/administration/settings/configure-default-device-setting.html)  
  Control Room administrator can configure the device settings to automatically set a user's default device when that user logs into Control Room.
* [**Switch device registration between Control Room instances**](https://docs.automationanywhere.com/bundle/enterprise-v2019/page/enterprise-cloud/topics/control-room/administration/settings/switch-device-cr-settings.html)  
  Configure the device settings in the Control Room to enable single-user devices to easily switch between different instances of the Control Room to run bots in multiple environments. This option enables you to register the Bot Agent on multiple Control Room instances without uninstalling the Bot Agent.
* [**Add access public IP addresses**](https://docs.automationanywhere.com/bundle/enterprise-v2019/page/enterprise-cloud/topics/control-room/administration/settings/cloud-add-addresses.html)  
  Use this setting to limit user login access to the Control Room URL based on IP addresses or subnets that you specify in a list. You add IP address ranges using the Classless Inter-Domain Routing (CIDR) format, and you can add multiple CIDR ranges.
* [**Set callback URLs**](https://docs.automationanywhere.com/bundle/enterprise-v2019/page/enterprise-cloud/topics/control-room/administration/settings/cloud-callback-urls.html)  
  You can specify valid callback URLs, enabling the Control Room to post the results of the task execution only to defined and secure URLs for more granular security over the network.
* [**Two-factor authentication**](https://docs.automationanywhere.com/bundle/enterprise-v2019/page/enterprise-cloud/topics/control-room/administration/settings/two-factor-authentication.html)  
  Two-factor authentication (2FA) provides an additional layer of defense against unauthorized users from accessing the Control Room. As an administrator, you can set up 2FA so that the users can validate their identity when logging in to the Control Room using both their user credentials and a second authentication factor.
* [**Configure forward proxy settings**](https://docs.automationanywhere.com/bundle/enterprise-v2019/page/configure-forward-proxy.html)  
  For On-Premises deployments that are using a proxy to connect to the internet, the forward proxy configuration feature enables Control Room features that require internet connectivity to function seamlessly.
* [**Configure Credential Vault Connection mode**](https://docs.automationanywhere.com/bundle/enterprise-v2019/page/enterprise-cloud/topics/control-room/administration/settings/cloud-configure-credential-vault-connection.html)  
  Credential Vault is a centralized location for securely storing credential information used by bots.
* [**Manage domain**](https://docs.automationanywhere.com/bundle/enterprise-v2019/page/enterprise-cloud/topics/control-room/administration/settings/cloud-manage-domain.html)  
  Administrators can use the **Display domain options** to hide a single domain or multiple domains, and use the **Select default domain** option to set any of the available (unhidden) domains as the default.
* [**Editing SQL user information**](https://docs.automationanywhere.com/bundle/enterprise-v2019/page/enterprise-cloud/topics/deployment-planning/on-prem-install/cloud-edit-sql-information.html)  
  Edit MS-SQL configuration related settings, including username, password, database server name, database server IP and port numbers.
* [**Syslog server integration**](https://docs.automationanywhere.com/bundle/enterprise-v2019/page/enterprise-cloud/topics/control-room/administration/settings/syslog-config.html)  
  The Automation Anywhere Control Room supports ingesting tenants' audit log entries in Syslog format to any Syslog server.
* [**Edit email notifications**](https://docs.automationanywhere.com/bundle/enterprise-v2019/page/enterprise-cloud/topics/control-room/administration/settings/cloud-edit-email-notification.html)  
  You can edit the email settings to select scenarios in which a Control Room sends email notifications.
* [**Version control in Automation 360**](https://docs.automationanywhere.com/bundle/enterprise-v2019/page/enterprise-cloud/topics/control-room/administration/configuring-version-control.html)  
  Version control helps you to manage the changes that you make to files that include Task Bots, documents, reports, scripts, executable files, and workflows. With version control, you can track and monitor changes to your bot logic.
* [**Integrating Control Room with Git repositories**](https://docs.automationanywhere.com/bundle/enterprise-v2019/page/enterprise-cloud/topics/control-room/git-integration/cloud-cr-git-integration.html)  
  Git integration with the Control Room ensures one-to-one mapping of the bots checked in to the public workspace of the Control Room and the remote Git file structure. Git commits enable you to enforce security, compliance, and code standards, and ensures that an organization's established best practices can be applied to their bot development processes.
* [**Usage statistics**](https://docs.automationanywhere.com/bundle/enterprise-v2019/page/enterprise-cloud/topics/control-room/administration/settings/cloud-usage-statistics.html)  
  Automation Anywhere collects usage statistics from Automation 360 for product improvements.
* [**Set up instances for Cloud-enabled deployments**](https://docs.automationanywhere.com/bundle/enterprise-v2019/page/enterprise-cloud/topics/control-room/administration/settings/cloud-enabled-instance-setup.html)  
  Manage trust relationship between the cloud-deployed Automation 360 Cloud-enabled instance and the On-Premises applications.
* [**Generate registration key to install Bot Agent in bulk**](https://docs.automationanywhere.com/bundle/enterprise-v2019/page/enterprise-cloud/topics/control-room/administration/settings/generate-registration-key-bot-agent.html)  
  The Control Room administrator can generate a registration key to install the Bot Agent on multiple devices at a time in bulk.
* [**Configure integration with SIEM**](https://docs.automationanywhere.com/bundle/enterprise-v2019/page/enterprise-cloud/topics/control-room/administration/settings/cloud-siem-integration-configuration.html)  
  The Automation Anywhere Control Room supports security information and event management (SIEM) tools ingesting logs from your tenant's Audit logs.
* [**Use AuthConfig App to enable OAuth2 services**](https://docs.automationanywhere.com/bundle/enterprise-v2019/page/enterprise-cloud/topics/control-room/administration/settings/authconfig-app-enable-oauth2.html)  
  As an Organization Administrator with access to the Licenses and Cloud Services portal, you use the AuthConfig App to manage the relationship between a set of Automation 360 Control Room instances and our OAuth2 (Open Authorization) services. OAuth2 services are used to interact with the Automation 360 Control Room by third-party applications. Currently, you can only use the PixieBrix extension to use the OAuth services to interact with the Control Room.

# Manage licenses

# <https://docs.automationanywhere.com/bundle/enterprise-v2019/page/enterprise-cloud/topics/control-room/administration/licenses/cloud-cr-licenses.html>

The Automation Anywhere Control Room provides an automated mechanism for tracking the use of licensed software across multiple Control Room instances and share these entitlements in real-time.

## All licenses

Automation Anywhere Control Room administrators can view and manage user license entitlements for your account. Navigate to **Administration** > **License** to view a summary of product licenses.

The following image displays licenses information for a Control Room:

# 

The **Licenses** page provides the following information:

|  |  |
| --- | --- |
| Field/option | Description |
| 1 | Indicates whether the Control Room license is a purchased or trial license. |
| 2 | Displays when the **Licenses** page was last updated. |
| 3 | Displays the license expiration date and time. |
| 4 | Indicates whether the license is available for the specified product. |
| 5 | When a license type is available, the link to the license is activated and you can click the link to view the license details. |
|  |
| Displays license details for: |
|  |
| **Total available**: Displays the total number of available licenses. |
| **Used in this Control Room**: Displays the total number of licenses used in the Control Room where you are viewing the license information. |
| **Used in other Control Room**: Displays the total number of licenses used in other Control Rooms. |
| **Remaining licenses**: Displays the number of unassigned licenses. |

Automation 360 licenses

# <https://docs.automationanywhere.com/bundle/enterprise-v2019/page/enterprise-cloud/topics/control-room/dashboards/cloud-administration-licenses.html>

# Version control in Automation 360

# <https://docs.automationanywhere.com/bundle/enterprise-v2019/page/enterprise-cloud/topics/control-room/administration/configuring-version-control.html>

Version control helps you to manage the changes that you make to files that include Task Bots, documents, reports, scripts, executable files, and workflows. With version control, you can track and monitor changes to your bot logic.

With version control, you can identify the version of a bot that you want to modify and compare your recent changes against the changes made to the bot previously. As a Control Room admin, you can configure version control in the Control Room settings.

Automation 360 includes version control capabilities, and you can use these capabilities irrespective of whether you have integrated your Control Room with Git. Review the capabilities available in Automation 360 and Git.

# 

## Version control in Automation 360

* **Check out and check in Task Bots:**You can check out one version of a bot (version 1) from public to your private workspace, make changes to it, and then check in the bot to the public workspace. This creates a new version (version 2) of the bot, which is the latest version. Every time you check out, make changes to, and check in a bot, a new version of the bot is created as the latest version.

**Note:** You can run either the latest version of a bot or the version that has the production label.

You can roll back to a particular version of a bot by selecting **Advanced options** in the check out action to select a specific version of the bot to check out. Also, you can select the dependencies to check out. By doing this, you can make changes to a specific version of a bot and its dependencies. When you check in this bot, it becomes the latest version. For example, if the latest version of a bot is version 8 and you want to roll back to version 3, you must first check out version 3 of the bot and then check it back in, which creates version 9. This latest version, which is identical to version 3, is now available in the public workspace for bot operations.

[Check in a bot](https://docs.automationanywhere.com/bundle/enterprise-v2019/page/enterprise-cloud/topics/aae-client/bot-creator/working-with-automation-tasks/cloud-bot-check-in.html) | [Check out a single bot](https://docs.automationanywhere.com/bundle/enterprise-v2019/page/enterprise-cloud/topics/aae-client/bot-creator/working-with-automation-tasks/cloud-bot-check-out.html)

* **Label Task Bot**: You can also roll back to a specific version of a bot by assigning a label to that version of the bot. You can use this label to choose the version with which you want to perform certain bot operations. With the version of your choice, you can schedule, run, queue, export, and trigger bot development workflows.

[Assign label to a bot](https://docs.automationanywhere.com/bundle/enterprise-v2019/page/enterprise-cloud/topics/aae-client/bot-creator/working-with-automation-tasks/label-a-bot.html)

* **View Task Bot history**: You can view the version history of your Task Bots in the public workspace. With **View history**, you can view the history of changes that have occurred in your Task Bots and identify the actions performed by a user. The list of all the versions of a bot is shown in reverse chronological order. The information displayed includes version number, check-in message, date and time of check-in, and the name of the user who checked in the version.

[View Task Bot version history](https://docs.automationanywhere.com/bundle/enterprise-v2019/page/enterprise-cloud/topics/aae-client/bot-creator/working-with-automation-tasks/cloud-bot-version-history.html)

* **Compare versions**: You can compare any two versions of your Task Bots to view the differences between those two versions.

[Compare bot versions](https://docs.automationanywhere.com/bundle/enterprise-v2019/page/enterprise-cloud/topics/control-room/bots/my-bots/cloud-compare-bot-versions.html)

* **Restore bots from Git**: Even if your Control Room is not integrated with Git, you can restore bots from Git to your public workspace. For example, if you have 50 bots in your public workspace and 75 bots in Git, you can restore the remaining 25 bots from Git to your public workspace.

**Note:** This restore option is available only for On-Premises deployments and not supported on Cloud deployments.

## Version control with Git

If your Control Room is integrated with Git, all the versions of the bots and files in Automation 360 are synced with Git, and you can use the following additional capabilities:

* Integrate with a Git branch.
* Integrate with Git through SSH authentication.
* Integrate with Git through a proxy server.
* Restore bots or files to an empty public repository from an existing Git configuration.
* Configure force push when connecting to Git.

An SSH key is an access credential for the SSH (secure shell) network protocol.

SSH is used for remote file transfer, network management, and remote operating system access.

What is the SSH used for?

SSH is often used to "login" and perform operations on remote computers but it may also be used for transferring data.

 Git branches are effectively a pointer to a snapshot of your changes. When you want to add a new feature or fix a bug—no matter how big or how small—you spawn a new branch to encapsulate your changes.