The Control Room acts as a centralized server-based component that plays a important role in managing and monitoring automation activities.

Automation Anywhere Control Room Administrators can efficiently manage user accounts, roles and permissions within the Control Room.

It has also option for scheduling and triggering capabilities. Enabling automation tasks to be executed based on predefined conditions or specific time triggers.

Code analysis enables you to form certain code structures with which you can implement coding best practices and make the code maintainable, reliable, efficient, and secure.

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.

What is Git and why it is used?

Git is a version control system used for tracking changes in computer files. It is generally used for source code management in software development.

GIT(Global Information Tracker)🡪 a powerful version control system widely used for software development and other collaborative projects. GIT allows multiple developers to work on a project simultaneously while ensuring that their changes do not interfere with one another.

## 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.

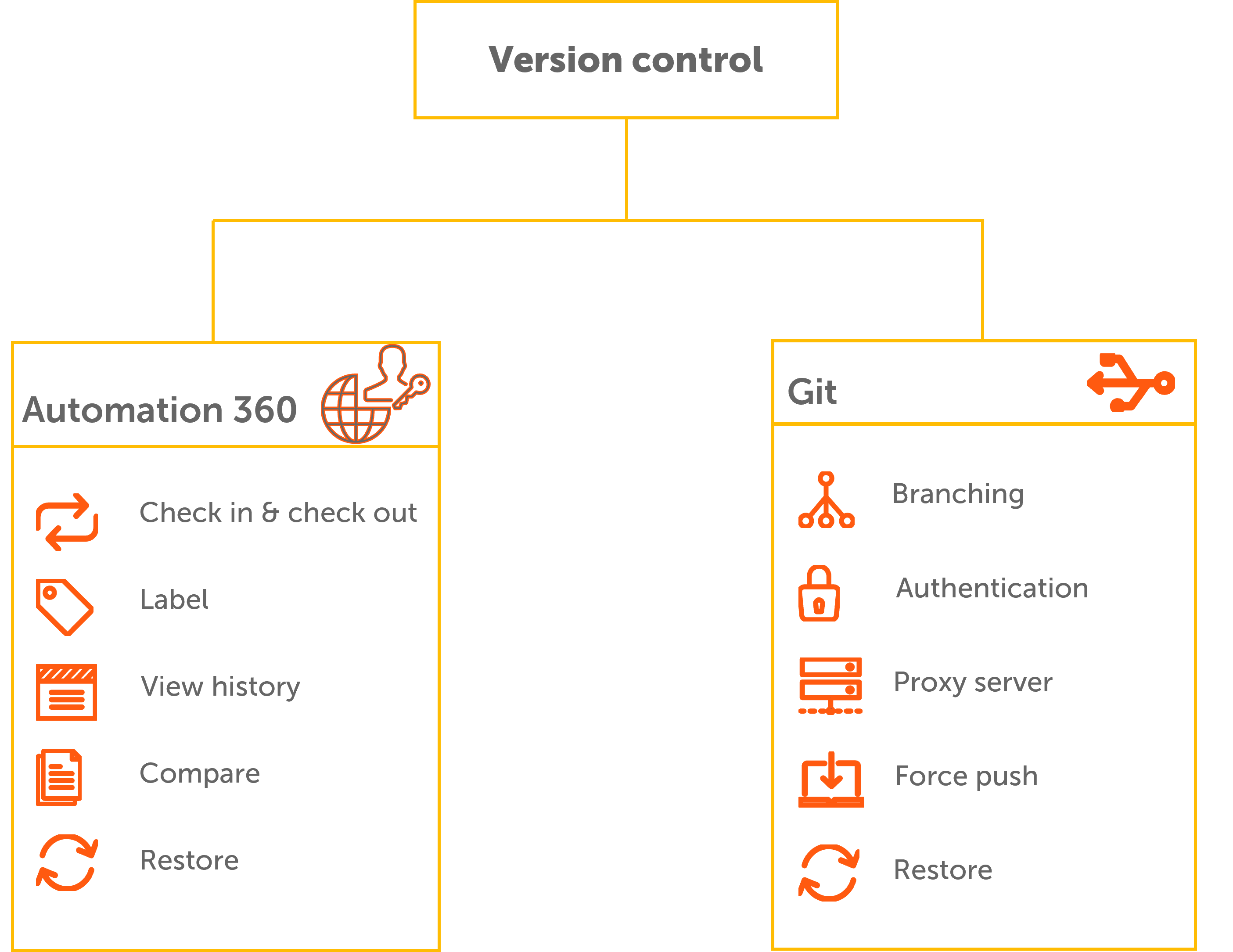
An SSH key is an access credential for the SSH (secure shell) network protocol.

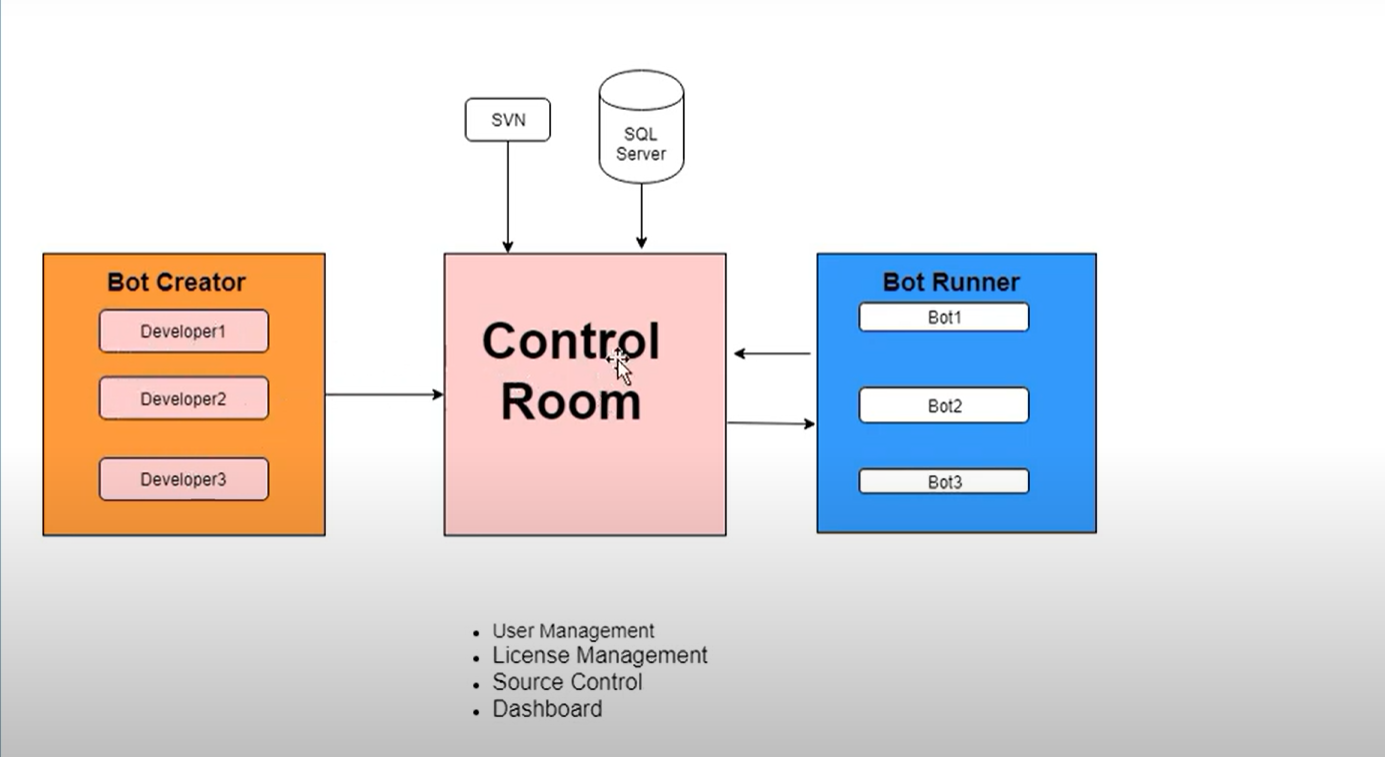
SSH is used for remote file transfer, network management, and remote operating system access.

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.





**Explain the steps for run and schedule BOT from Automation Anywhere Control Room?**

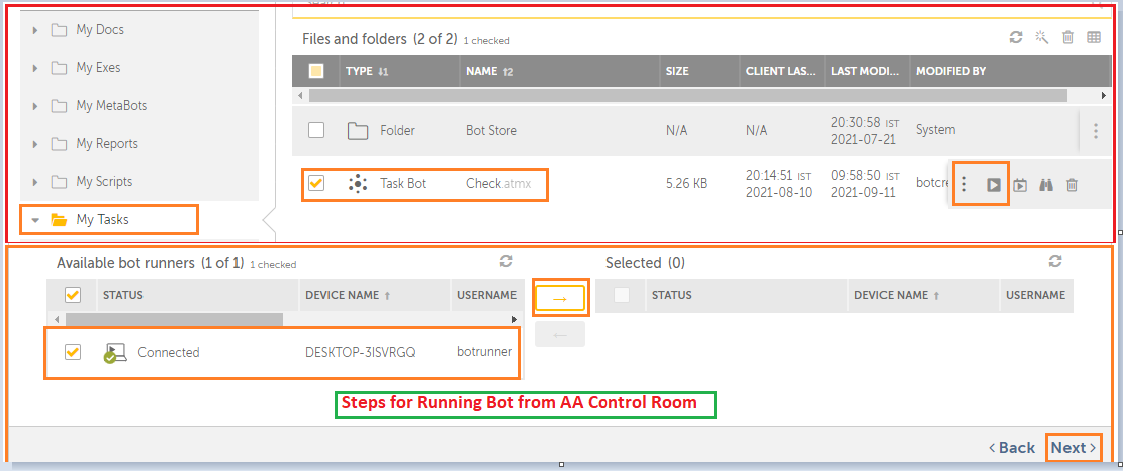
To Run Bot from Automation Anywhere Control Room we need to follow steps as mentioned below.

* First upload the BOT using Automation Anywhere Client including dependent files or sub tasks if any into Control Room.
* Go to Control Room > Bots > My bots > My Tasks > select the Task which you want to run or schedule
* Select Run Bot > Select Bot Runner (from the available List) and click on Arrow to add the Bot runner
* Click on Run Now button to start the BOT.

Steps for Scheduling Bot in Automation Anywhere Control Room.

* First upload the BOT using Automation Anywhere Client including dependent files or sub tasks if any into Control Room.
* Go to Control Room > Bots > My bots > My Tasks > select the Task which you want to run or schedule
* Click on Schedule Bot and it will take you to the page Called Scheduled Bot
* Select the Schedule type as Run Once or Run repeatedly to select the BOT Start Date and Start Time
* Add the Bot runner from Device option and click next
* Click on Schedule Bot Button in the next Page

You can refer to the attached image to understand the steps in detail.



#### ****Why Automation Anywhere 360 Control Room Bad Gateway error comes?****

The “Bad Gateway” error in Automation Anywhere Control Room usually occurs when there is a communication issue between Control Room and Bot Creator or Runner server. This error can occur due to various reasons, including network connectivity issues, server load, or incorrect configuration settings.

Here are some steps you can take to resolve the “Bad Gateway” error in Automation Anywhere Control Room:

* Check network connectivity: Ensure that the Control Room server and the Bot Runner server are connected to the same network and there are no network connectivity issues.
* Check server load: Check the server load on both the Control Room server and Bot Runner server. If the server load is high, it can cause the “Bad Gateway” error. In this case, wait for some time and try again later.
* Check configuration settings: Verify that the Control Room and Bot Runner server are configured correctly. Ensure that the correct URL is used to access the Control Room, and the Bot Runner server is added correctly to the Control Room.
* Restart the services: Restart the Automation Anywhere Control Room and Bot Runner services to resolve any potential issues that may be causing the “Bad Gateway” error.

If none of the above steps resolve the issue, contact [Automation Anywhere](https://www.automationanywhere.com/) support for further assistance.

## Starting the services on the Control Room

Start the following Control Room services in the listed sequence.

1. Automation Anywhere Licensing
2. Automation Anywhere Elastic Search Service
3. Automation Anywhere Control Room Reverse Proxy
4. Automation Anywhere Control Room Caching
5. Automation Anywhere Control Room Messaging
6. Automation Anywhere Control Room Service
7. Automation Anywhere Bot Insight Service

**Note:** Wait for an interval of 30 seconds before starting the next service.

## Stopping the services on the Control Room

## Stop the following Control Room services in the listed sequence:

1. Automation Anywhere Control Room Caching
2. Automation Anywhere Control Room Reverse Proxy
3. Automation Anywhere Control Room Messaging
4. Automation Anywhere Control Room Service
5. Automation Anywhere Licensing
6. Automation Anywhere Elastic Search Service
7. Automation Anywhere Bot Insight Service Discovery

**Note:** Stop the Automation Anywhere Bot Insight Service Discovery if the Bot Insight services are up and running.

#### ****Explain the steps for creating user in Automation Anywhere Control Room?****

Here are the steps for creating a new user in Automation Anywhere Control Room:

* Log in to the Automation Anywhere Control Room as an administrator.
* Navigate to the “Users” section from the left-hand menu.
* Click on the “Create User” button in the top right-hand corner of the screen.
* Fill in the user details, such as username, email address, first name, last name, and password. You can also assign roles to the user.
* Click on the “Create User” button to create the user account.
* Once the user is created, you can configure additional settings for the user. Such as access to specific folders or actions.
* You can also modify or delete the user account from the “Users” section.

Note: Depending on the version of Automation Anywhere Control Room. The steps for creating a new user may vary slightly. Additionally, you may need to configure other settings. Such as access permissions or roles, to allow the user to perform specific actions or access certain resources.

#### ****What is secure recording in Automation Anywhere? How and where to setup this feature?****

Secure Recording is a feature in Automation Anywhere that allows users to record sensitive data securely. When enabled, it prevents the recording of sensitive data. Such as passwords or credit card numbers, from being stored in clear text in the automation task. Instead, the sensitive data is masked or encrypted to protect it from being accessed by unauthorized users.

Here are the steps to enable Secure Recording in Automation Anywhere:

* Open Automation Anywhere Client and go to “Options” in the “Tools” menu.
* Click on the “Security” tab and then click on the “Secure Recording” button.
* In the “Secure Recording” dialog box, select the “Enable Secure Recording” checkbox.
* Choose the type of encryption or masking you want to use for sensitive data. You can choose from options like “Masking with Asterisks” or “Encrypt with Password.”
* Click “OK” to save the changes.

Secure Recording is now enabled and any sensitive data entered during the recording process will be masked or encrypted according to the settings you have configured.

Note that Secure Recording is a feature that needs to be set up on individual machines where the Automation Anywhere Client is installed. It is recommended to enable Secure Recording on all machines where sensitive data may be accessed during automation tasks.

#### ****What is Credentials Vault in Automation Anywhere? What are advantages of using it.****

Credentials Vault is a feature in Automation Anywhere that allows users to securely store and manage login credentials. Such as usernames and passwords for various applications and systems used in automation tasks.

Advantages of using Credentials Vault in Automation Anywhere include:

* Improved security: Credentials Vault provides a secure and centralized location to store sensitive information. Such as login credentials, and helps prevent unauthorized access to the information.
* Time-saving: Credentials Vault enables users to store login credentials for multiple applications and systems in one location. Eliminating the need to enter them manually every time they are required in an automation task.
* Simplified maintenance: By storing login credentials in a central location, it is easier to manage and update them as needed. Changes made in the Credentials Vault automatically update all the tasks that use the credentials.
* Audit trail: Credentials Vault provides an audit trail of who has accessed the stored credentials and when. Helping to maintain compliance with organizational policies and regulations.
* Integration: Credentials Vault can be integrated with other security tools. Such as Active Directory or LDAP, making it easier to manage access rights and permissions.

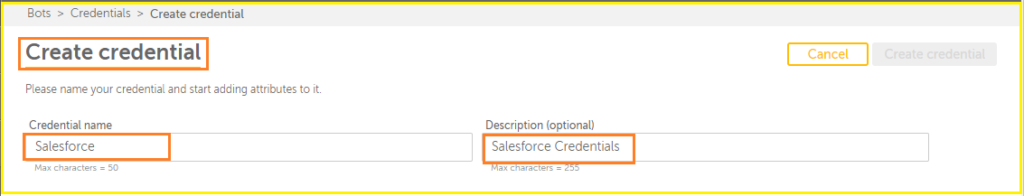
Overall, using Credentials Vault in Automation Anywhere helps to enhance security, save time, and simplify credential management in automation tasks.

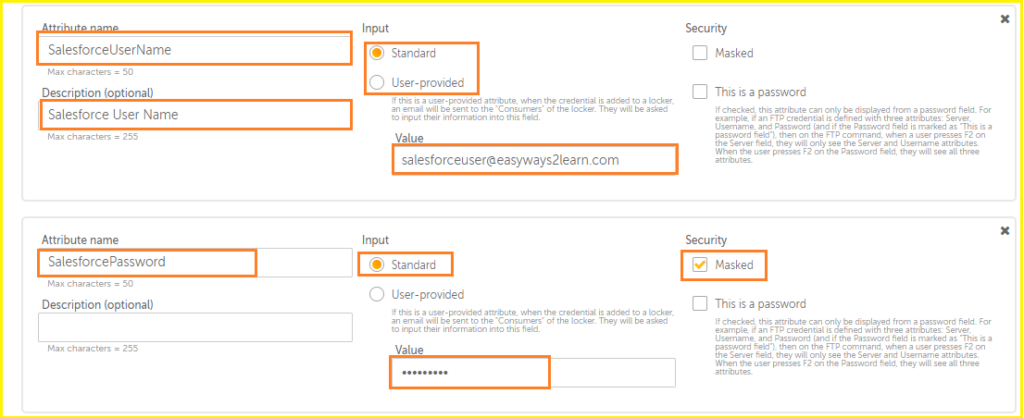
#### ****Explain the steps for creating Credentials in Automation Anywhere Control Room?****

Here are the steps for creating Credentials in Automation Anywhere Control Room:

* Log in to the Automation Anywhere Control Room as an administrator.
* Navigate to the “Credentials” section from the left-hand menu.
* Click on the “Create Credentials” button in the top right-hand corner of the screen.
* Fill in the credential details, such as the credential name, username, password, and domain (if applicable).
* Click on the “Create” button to create the credential.
* Once the credential is created, you can configure additional settings for the credential, such as access permissions or expiry date.
* You can also modify or delete the credential from the “Credentials” section.

Note: Depending on the version of Automation Anywhere Control Room. The steps for creating Credentials may vary slightly. Additionally, you may need to configure other settings. Such as access permissions or roles, to allow users or bots to access the credentials for use in automation tasks.

Creating Credentials in Automation Anywhere



**What is two-factor Authentication in Automation Anywhere? Explain the steps for enabling this feature.**

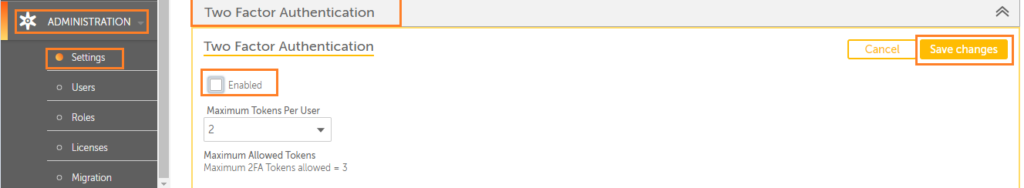
Two-factor authentication is a security feature in Automation Anywhere.  It’s adds an extra layer of protection to user accounts by requiring a second form of authentication in addition to a password.

Here are the steps for enabling Two-factor Authentication in Automation Anywhere:

* Log in to the Automation Anywhere Control Room as an administrator.
* Navigate to the “Settings” section from the left-hand menu.
* Click on the “Security” tab and then click on the “Two-Factor Authentication” button.
* In the “Two-Factor Authentication” dialog box, select the “Enable Two-Factor Authentication” checkbox.
* Choose the type of second factor authentication you want to use, such as a Time-based One-Time Password (TOTP) or SMS authentication.
* Configure the settings for the second factor authentication method you have chosen.
* Click “Save” to save the changes.

After enabling Two-factor Authentication, users will need to enter their password as well as a second form of authentication to log in to Automation Anywhere.

Note that Two-factor Authentication is a security feature that needs to be set up on individual accounts in the Control Room. It is recommended to enable Two-factor Authentication for all users with access to sensitive information or critical automation tasks.

Steps for enable Two-factor Authentication in Automation Anywhere Control Room.

#### ****What is the difference between Bot creator and Bot runner role in Control Room?****

A bot creator role is responsible for creating and designing Bots. While a Bot runner role is responsible for running and monitoring bots. Bot creators can design bots and upload them to Control Room, while Bot runners can execute and monitor these bots.

#### ****How does Automation Anywhere Control Room help in bot management?****

Control Room provides a centralized platform for bot management. It helps in deploying bots to various environments. Scheduling bots to run at specific times, monitoring bot performance, and managing user access to bots and related resources.

#### ****What are the security features available in Automation Anywhere Control Room?****

Automation Anywhere Control Room provides various security features. Which includes role-based access control, encryption of sensitive data, secure communication protocols, and user authentication.