

**Download the CloudFormation template from the AWS Marketplace and bring it up in your AWS Console, the following screen should show:**

Step 1  
Specify template

Step 2  
**Specify stack details**

Step 3  
Configure stack options

Step 4  
Review

## Specify stack details

**Stack name**

Stack name

*Enter a stack name*

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

**Parameters**

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

**Network Configuration**

Which VPC should this be deployed to?  
VpcId of your existing Virtual Private Cloud (VPC)

SubnetId  
The list of SubnetIds in your Virtual Private Cloud (VPC)

**Remote Desktop Access**

Lockdown RDP Access to Specific IP. For example, set CIDR to 0.0.0.0/0 to allow all IP addresses access, x.x.x.x/32 to allow one specific IP address, or another CIDR range.

**The following is a sample filled in request for the various parameters that the CF template needs:**

**Specify stack details**

Step 3  
Configure stack options

Step 4  
Review

**Stack name**

Stack name

a2019byol

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

**Parameters**

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

**Network Configuration**

Which VPC should this be deployed to?  
VpcId of your existing Virtual Private Cloud (VPC)

vpc-e87f3392 (172.31.0.0/16)

SubnetId  
The list of SubnetIds in your Virtual Private Cloud (VPC)

subnet-980b3bff (172.31.0.0/20)

**Remote Desktop Access**

Lockdown RDP Access to Specific IP. For example, set CIDR to 0.0.0.0/0 to allow all IP addresses access, x.x.x.x/32 to allow one specific IP address, or another CIDR range.

35.172.76.209

**Application Access**

Lockdown of Application Access to Specific IP. For example, set CIDR to 0.0.0.0/0 to allow all IP addresses access, x.x.x.x/32 to allow one specific IP address, or another CIDR range.

35.172.76.209

**Amazon EC2 Configuration**

**SubnetId**  
The list of SubnetIds in your Virtual Private Cloud (VPC)

subnet-980b3bff (172.31.0.0/20)

**Remote Desktop Access**  
Lockdown RDP Access to Specific IP. For example, set CIDR to 0.0.0.0/0 to allow all IP addresses access, x.x.x.x/32 to allow one specific IP address, or another CIDR range.

35.172.76.209

**Application Access**  
Lockdown of Application Access to Specific IP. For example, set CIDR to 0.0.0.0/0 to allow all IP addresses access, x.x.x.x/32 to allow one specific IP address, or another CIDR range.

35.172.76.209

**Amazon EC2 Configuration**

**InstanceName**  
name of instance

a2019byol

**InstanceType**  
EC2 Instance type

m5.xlarge

**KeyName**  
Name of an existing EC2 KeyPair to enable RDP access to the instances

tejmarketplace

Cancel Previous Next

**Once you click next, the EC2 instance will be deployed. Give a few minutes so that the Public DNS has propagated and then start the following:**

**Configuring the A2019 application once the EC2 Instance has been deployed by the CF Template**

### 1. Go the public DNS for the EC2 instance that has been just deployed:

xperience  
u think

ard New

Launch Instance Connect Actions

Filter by tags and attributes or search by keyword

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)
awsbyoltest	i-0fce73f40b6329c0	m4.xlarge	us-east-1a	running	2/2 checks ...	None	ec2-34-229-194-163.compute-1.amazonaws.com

es

### 2. The following A2019 application screen show up:

**Automation ANYWHERE Enterprise**

Control Room

Control Room settings

### Configure Control Room settings

Save and continue

There are some settings that need to be configured before continuing to Control Room.

**Repository path**

Specify the path or the shared path of the Control Room repository where the automation files are stored.

e.g. C:\ProgramData\AutomationAnywhere\Server Files

**Control Room Access URL**

Specify the host name, URL, or IP of reverse proxy or load balancer.

e.g. CRServer, http://example.com, or 192.163.2.100:8096

**Please make sure the IP address in the security group is the same as you entered while deploying the EC2 instance on the Cloud formation template. If not go into the security group and update it.**

**This is the first time configuration of the Control room, here is a sample entry for Repository path and Control room URL which should be the same as the Public DNS above.**

**Automation ANYWHERE Enterprise**

Control Room

Control Room settings

### Configure Control Room settings

Save and continue

There are some settings that need to be configured before continuing to Control Room.

**Repository path**

Specify the path or the shared path of the Control Room repository where the automation files are stored.

e.g. C:\ProgramData\AutomationAnywhere\Server Files

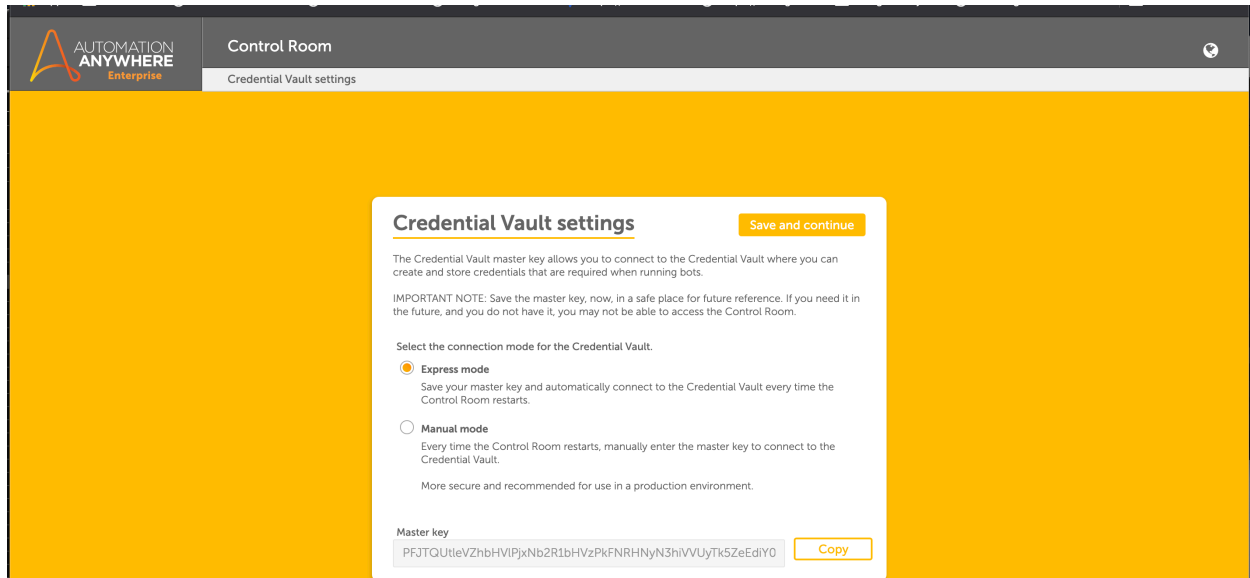
**Control Room Access URL**

Specify the host name, URL, or IP of reverse proxy or load balancer.

e.g. CRServer, http://example.com, or 192.163.2.100:8096

**Click Save and Continue:**

**Now select Express or Manual mode (Express is the recommended way for general users). Copy the Master key and keep in a safe place in case.**



The screenshot shows the 'Control Room' interface with the 'Credential Vault settings' page. The page has a yellow background. At the top left is the 'AUTOMATION ANYWHERE Enterprise' logo. The top navigation bar is dark grey with 'Control Room' and a 'Credential Vault settings' link. The main content area is white and contains the following text:

**Credential Vault settings** Save and continue

The Credential Vault master key allows you to connect to the Credential Vault where you can create and store credentials that are required when running bots.

IMPORTANT NOTE: Save the master key, now, in a safe place for future reference. If you need it in the future, and you do not have it, you may not be able to access the Control Room.

Select the connection mode for the Credential Vault.

☒ **Express mode**  
Save your master key and automatically connect to the Credential Vault every time the Control Room restarts.

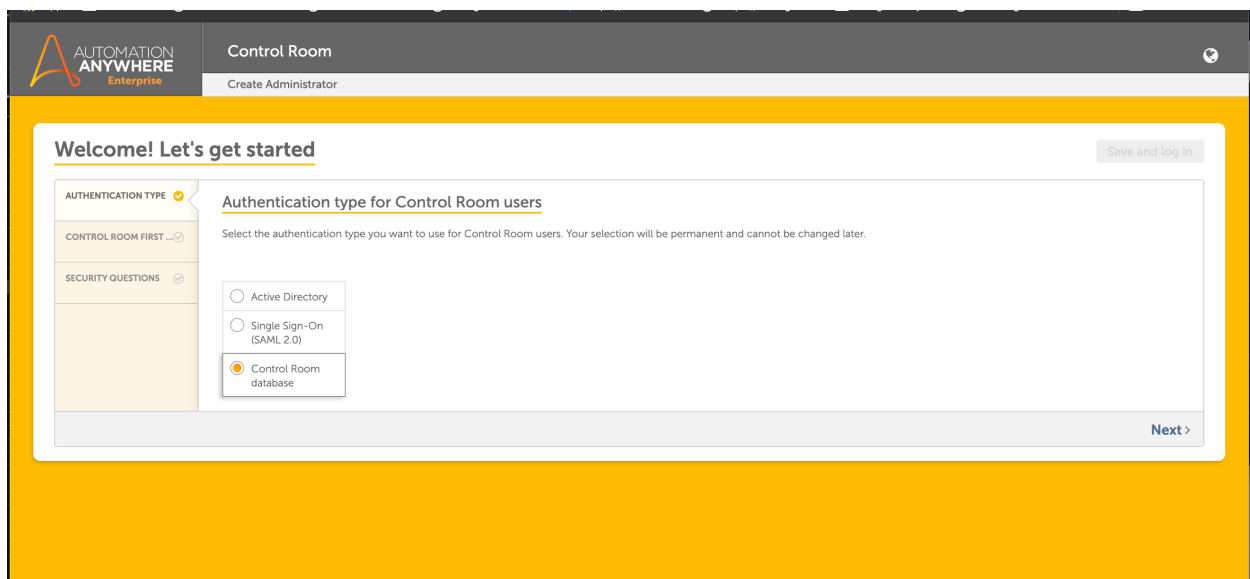
☐ **Manual mode**  
Every time the Control Room restarts, manually enter the master key to connect to the Credential Vault.  
More secure and recommended for use in a production environment.

Master key  
PFJTQutleVZhbHVPjxNb2R1bHVzPkFNRHNyN3hiVVUyTk5ZeEdiY0 Copy

**Click Save and Continue:**

**Now select:** Authentication type for Control Room users

**The example below shows how to connect to CR DB directly and get started:**



The screenshot shows the 'Control Room' interface with the 'Create Administrator' page. The page has a yellow background. At the top left is the 'AUTOMATION ANYWHERE Enterprise' logo. The top navigation bar is dark grey with 'Control Room' and a 'Create Administrator' link. The main content area is white and contains the following text:

**Welcome! Let's get started** Save and log in

**Authentication type for Control Room users**

Select the authentication type you want to use for Control Room users. Your selection will be permanent and cannot be changed later.

☐ Active Directory

☐ Single Sign-On (SAML 2.0)

☒ Control Room database

Next >

**Automation ANYWHERE Enterprise**

Control Room

Create Administrator

**Welcome! Let's get started** [Save and log in](#)

**Control Room first administrator**

The Control Room first administrator is automatically assigned the system-created "Admin" role which has permissions for all functionality.

**Authentication Type**

**Control Room First**

**Security Questions**

**Username**

[ \ / ' " { } : | < > + = , . ? \* " are not allowed

**Description (optional)**

Max characters = 255

**First name (optional)**

Max characters = 50

**Last name (optional)**

Max characters = 50

**Email**

**Confirm email**

**Password**

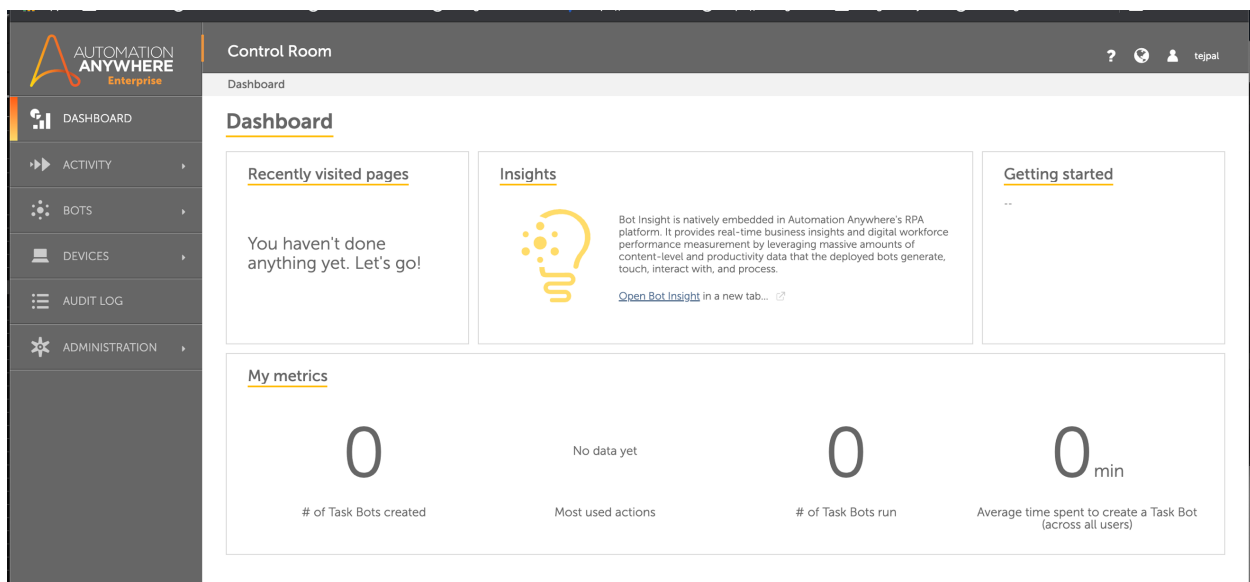
8-15 characters: a-z, A-Z, 0-9, @, -, \_ , !, #, \$, %, &, and . allowed.

**Confirm password**

[< Back](#) [Next >](#)

Please type your credentials and also security questions to recover the password.

Finally the following screen shows that you are all set to go:



From here you can create more users, check and update license key and start developing Bots.

**For more help on how to develop Bots and manage the Control Room please visit A2019**

<https://university.automationanywhere.com/2-course-list/74-build-your-first-bot-a-step-by-step-tutorial/>

<https://www.automationanywhere.com/blog/learn-rpa/how-to-get-started-with-enterprise-a2019>

**To get a demo of the product go to and you can schedule a demo about the product.**

<https://www.automationanywhere.com/request-live-demo>