May 18, 2020

Automation Anywhere Version A2019

Legal Notices

Examples and graphics are provided only as reference information and might not match your site.

Content

Install and upgrade Enterprise A2019

This collection of topics guides you through the process of setting up Automation Anywhere Enterprise.

Legal disclaimer: The information provided in this workflow might vary depending on which offering is being used. Administrator steps might not be applicable to Enterprise A2019 or Community Edition.

1. System prerequisites: Enterprise A2019 (Cloud deployed) and Community Edition prerequisites:
   a) If you are using Community Edition, Register as a Community user.
   b) Verify your device meets Enterprise A2019 (Cloud deployed) and Community Edition device requirements.

   On-Premises administrators, verify your datacenter meets Enterprise A2019 On-Premises prerequisites.

2. Administrators set up bot users.

   These tasks only apply to administrators. Bot users, skip this step and proceed to the step 3.

   a) Receive your administrator credentials.

   Enterprise A2019 (Cloud deployed) administrators: Receive your login credentials, with administrator privileges, and your Enterprise A2019 dedicated URL from Automation Anywhere Enterprise.

   Enterprise A2019 (On-Premises) administrators: Receive your licensing information from Automation Anywhere Enterprise and install Enterprise A2019: Enterprise A2019 On-Premises Enterprise Control Room installation. The installation user is assigned administrator privileges.

   b) Log in to a supported device, open a supported web browser, and log in to your Enterprise Control Room using the dedicated URL: Enterprise A2019 (Cloud deployed) and Community Edition device requirements, Log in to Automation Anywhere Enterprise Control Room.
   c) Create your bot users by assigning a role and device license: Create user, Create an Active Directory user.
   d) Set up email notifications to Enterprise Control Room users when events affect them, such as changes to passwords or user information, and account activation or deactivation.
3. Receive your bot user login credentials and the Enterprise A2019 Enterprise Control Room dedicated URL.

   Community Edition users, if you do not have an Enterprise A2019 account, register for a free Community Edition account by visiting Automation Anywhere Community Edition.

   Credentials are sent to you from your company's Automation Anywhere Enterprise administrator or from Automation Anywhere Enterprise.

4. Log in to your Enterprise A2019 account.

   Log in to a supported device, open a supported web browser, and log in to your Enterprise Control Room: Enterprise A2019 (Cloud deployed) and Community Edition device requirements, Log in to Automation Anywhere Enterprise Control Room.

5. Register your device and install the Bot agent: Register device and install Bot agent.

Note: The Bot agent is installed only on devices running the supported Windows operating systems. See Enterprise A2019 (Cloud deployed) and Community Edition device requirements. However, you can still build bots using the Bot editor for creating bots.

6. Start creating bots: Create your first bot or Build a Go be Great bot.

- Getting started with Enterprise A2019 (Cloud deployed) and Community Edition
  Use these tasks to prepare for, and start creating and using bots with Automation Anywhere Enterprise A2019 (Cloud deployed) and Community Edition.
- Getting started with IQ Bot A2019, Cloud, and Community Edition
  Perform these tasks to set up IQ Bot A2019 Cloud deployed, On-Premises, and Community Edition and start using them with the same editions of Enterprise A2019.
- Run IQ Bot On-Premises database migration script
  IQ Bot On-Premises Builds 1089, 1598, and 2079 included five databases. Starting with IQ Bot On-Premises Build 2545, one unified database is supported. You have to run a migration script to migrate the databases of Builds 1089, 1598, 2079 to the latest build.
- Enterprise A2019 On-Premises prerequisites
  Determine whether the system has the required hardware and software to install Enterprise Control Room for A2019 On-Premises deployment.
- Enterprise A2019 On-Premises Enterprise Control Room installation
  Review the installation core tasks and topics for installing A2019 Enterprise Control Room in a data center on an On-Premises server or a cloud service provider server instance.
- Post-installation user management
  After completing the post-installation tasks, validate the setup by logging in to the Enterprise Control Room and installing a license. First time access to the Enterprise Control Room walks you through the configuration for your authentication method.
- Installed Enterprise Control Room directories and files
  When installing the Automation Anywhere Enterprise Control Room on different operating systems, the installer executes and installs files and folders in the following directories.
- Licenses
  The All Licenses page displays detailed information about current product and device licenses.
- Update Enterprise A2019
  If you are already using Enterprise A2019 On-Premises, you can update to the latest version of Enterprise A2019. For example, Enterprise A2019 On-Premises Build 3337 to Build 4105.
- Upgrade to Enterprise A2019
  Perform the tasks in this work flow to upgrade from Automation Anywhere 10.x or 11.x to Enterprise A2019, including migration of your 11.x and 10.x bots to A2019.
- Uninstall Enterprise A2019 On-Premises
  Uninstall the On-Premises Enterprise Control Room from your Linux server.
- Bot deployment and concurrent operations
  List of maximum concurrent operations and estimated deployment times.

Related tasks

Log in to Automation Anywhere Enterprise Control Room

Register as a Community user

Related reference

Enterprise A2019 (Cloud deployed) and Community Edition device requirements

Supported browsers for Enterprise A2019

Getting started with Enterprise A2019 (Cloud deployed) and Community Edition

Use these tasks to prepare for, and start creating and using bots with Automation Anywhere Enterprise A2019 (Cloud deployed) and Community Edition.

The following is a workflow for creating and using bots in Enterprise A2019 or Community Edition:

Prerequisites for Enterprise A2019 (Cloud deployed) and Community Edition prerequisites

Determine whether your device meets the required hardware and software requirements to register your device with Automation Anywhere Enterprise and create or run bots.

1. Receive your Enterprise Control Room URL and login credentials.

   The URL points to your Automation Anywhere Enterprise instance.

   - If you are an Automation Anywhere Enterprise Community Edition user, the login credentials are those you set when you registered.

     See Register as a Community Edition user and complete the steps.

   - If you are your company's principal administrator and ordered cloud-deployed Enterprise A2019, you receive an email from Automation Anywhere with your URL and credentials.

2. Log in to Automation Anywhere Enterprise Control Room.

   To log in to Enterprise A2019, open the Enterprise Control Room URL in your browser, enter your credentials in the login screen, and click Log in.

3. Register device and install Bot agent and Set device credentials.

   The Bot agent is a lightweight application that enables you to run bots on your device by connecting a local machine to the Enterprise Control Room. To run bots on a local machine, install the Bot agent and add the local device to the list of enabled host devices.
   To enable a device for running bots, set the local device credentials.

   Watch the following video on how to install the Bot agent in Enterprise A2019:

   Install the Bot agent

   If you are using an operating system other than Windows, you will not be able to install the Bot agent at this time. See system requirements. However, you can still build bots using the Bot editor.

4. Create your first bot.

   Follow these steps to create your first bot that prints the message, `Go be great!`, the Automation Anywhere version of `Hello World!`

   Watch the following video on how to build your first bot:

   Build your first bot

5. Run your first bot.

   Run a bot from the same device that you used to create the bot.

   Watch the following video on how to run your first bot in the Community Edition:

   Run your first bot

Watch the following video for an introduction to Enterprise A2019:

Introduction to Enterprise A2019

- Enterprise A2019 (Cloud deployed) and Community Edition prerequisites
  Determine whether your device meets the required hardware and software requirements to register your device with Automation Anywhere Enterprise and create or run bots.
- Register as a Community user
  Steps to register yourself in the Automation Anywhere Enterprise Community Edition for using the Community Control Room to create and run bots.
- Log in to Automation Anywhere Enterprise Control Room
  To log in to Enterprise A2019, open the Enterprise Control Room URL in your browser, enter your credentials in the login screen, and click Log in.
- Register device and install Bot agent
  The Bot agent is a lightweight application that enables you to run bots on your device by connecting a local machine to the Enterprise Control Room. To run bots on a local machine, install the Bot agent and add the local device to the list of enabled host devices.
- Create your first bot
  Follow these steps to create your first bot that prints the message, `Go be great!`, the Automation Anywhere version of `Hello World!`
- Run your first bot
  Run a bot from the same device that you used to create the bot.

Enterprise A2019 (Cloud deployed) and Community Edition prerequisites

Determine whether your device meets the required hardware and software requirements to register your device with Automation Anywhere Enterprise and create or run bots.

If your device meets the requirements, you then register your device with Automation Anywhere Enterprise, open a supported browser, log in to the Enterprise Control Room, and run your bot tasks. This includes creating and running bots.

- Enterprise A2019 (Cloud deployed) and Community Edition device requirements
  Review the machine hardware specifications, operating system versions, and browser types supported by Automation Anywhere Enterprise for creating and running bots as an Enterprise A2019 (Cloud deployed) or Community Edition user on your local machine.
- Community capacity and limitations
  Community users access and bot creation and running conditions.

Enterprise A2019 (Cloud deployed) and Community Edition device requirements

Review the machine hardware specifications, operating system versions, and browser types supported by Automation Anywhere Enterprise for creating and running bots as an Enterprise A2019 (Cloud deployed) or Community Edition user on your local machine.

Hardware requirements for registered devices

You communicate with the Enterprise Control Room, through a registered local machine (device). Part of registering a device with Enterprise A2019 is installing a Bot agent. The Bot agent can be installed on devices that meet the following hardware requirements.

For Enterprise Control Room operating system and platform compatibility, see Enterprise Control Room operating system compatibility.

Device	Processor	RAM	Storage (free disk space)	Network
Machine	Intel Core i5 2.6 GHz	4 GB minimum 8 GB recommended	32 GB	1 GbE
Bot Creator and Bot Runner	No additions to the machine requirements	No additions to the machine requirements	Add 100 through 150 KB per Automation Anywhere script Add 40 through 50 GB per long-term project	No additions to the machine requirements

RAM on Cloud or Community Edition devices

Add additional RAM to account for applications and services running on the Automation Anywhere Enterprise machine, for example:

- Microsoft Office applications (example: Excel)
- Browsers (example: Google Chrome)
- Enterprise applications (example: CRM, Oracle EBS, and SAP)
- VDI infrastructure applications
- Anti-virus software

Storage disk space on Cloud or Community Edition devices

- Automation Anywhere Enterprise scripts average approximately 100-150 KB. Additional free disk space is required to develop automation projects because temporary files such as screen shots, server logs, and audit files are created during the execution of the automation scripts.
- Free space required increases with the project size. Recommendation: Have at least 40-50 GB of free disk space for each long-term project.
- Increase storage space configuration after installation, as needed, depending on product usage. For example, depending upon the complexity of your bot, generating log files and logic creation require additional disk space later.

Platform compatibility for registered devices

A device used to connect to the Enterprise Control Room and perform bot tasks must meet the platform requirements.

Note: Platform requirements are different for Enterprise Control Room and Bot agent.

On-Premises machines

Physical machines running any of the supported operating systems.

Terminal servers

Using remote desktop (RDP) running any of the supported operating systems is supported is supported on Enterprise A2019 Version A2019.11 or later. .

Virtual machines

Bot agent is supported on all VMs where the supported Windows OS has been hosted on Version A2019.09 or later. For example, Virtual Desktop Infrastructure (VDI) are supported on Amazon Web Services, Microsoft Azure, VMware virtual machines, and Oracle Virtual Box.

Supported operating systems for registered devices

A device used to run the Bot agent, connect to the Enterprise Control Room, and perform bot tasks as a Bot Creator and Bot Runner must meet the operating system requirements.
Note:

- Bot Creator tasks are supported with all the listed operating systems.
- You cannot register a device that is running on a Linux system. The Bot agent cannot be installed on Linux systems. However, you can use a registered device running on a Windows system to access an Enterprise Control Room that is installed on a Linux system.

Windows version	Windows edition	Attended Bot Runner	Unattended Bot Runner	Bot Creator
Windows Server 2019[1]	Datacenter	Supported	Supported[2]	Supported
Windows Server 2016[1]	Datacenter	Supported	Supported[2]	Supported
Windows Server 2012 [1]	Standard	Supported	Supported[2]	Supported
Windows 10[1]	Professional and Enterprise	Supported	Supported[2]	Supported
Windows 8 [3]	Professional and Enterprise	Supported	Supported	Supported
Windows 7 [3]	Professional and Enterprise	Supported	Supported	Supported

(1) Credential Vault

Is supported on Enterprise A2019 versions newer than Version A2019 Builds 1598 and 1610.

(2) Auto-login

- Auto-login is only supported on 64 bit systems.
- If there is a legal disclaimer on the device then Auto-login fails.
- If the Auto-login fails, configure the Local Security Policy settings. For example, from Windows, select Security Settings > Local Policies > Security Options. Disable the Interactive logon: CTRL+ALT+DEL option.

(3) Supported OS

Windows 8 supported on Version A2019 Builds 1598 and 1610 or older.
Windows 7 supported on Version A2019.12 or later.

Supported browsers for registered devices

The user interface for Automation Anywhere Enterprise is through a browser. Login to your device, then login to Enterprise Control Room through a browser.

Browser	Browser version	Automation Anywhere Plug-in version[2]
Google Chrome[1]	57 or later	11 or 12
Microsoft Internet Explorer	11	N/A

(1) Google Chrome re-verification

CAUTION: Google Chrome requires re-verification of permissions when the Automation Anywhere Google Chrome extension is updated. If prompted, click Enable this item in the Google Chrome message. Alternatively, re-enable the extension through chrome web store. Similarly, if you are deploying your Bot Runners from a master image, accept the permission from within that image.

(2) Google Chrome plug-in extension versions

Enterprise A2019 supports Chrome extension version 11. If either Google Chrome extension 11 or 12 was installed and then uninstalled, additional steps are required. See Changing Google Chrome extensions.

Community capacity and limitations

Community users access and bot creation and running conditions.

Number of bot creators per Community Edition user

Each Community Edition user can use one Bot Creator in one Cloud Control Room at a time.

Number of bots created by Community Edition user

Each Community Edition user can create multiple bots,

Number of bots run by Community Edition user

Each Community Edition user can run one bot at a time on any one registered device.

Number of registered devices per Community Edition user

Each Community Edition user can register multiple devices, but only be logged into one at a time, and only run a bot on one device at a time.

Register as a Community user

Steps to register yourself in the Automation Anywhere Enterprise Community Edition for using the Community Control Room to create and run bots.

Procedure

1. From the Automation Anywhere website, https://www.automationanywhere.com/, scroll to and click the Get Community Edition button.
   Alternatively, select Customers & Partners > A People Community > Community Edition. Scroll to the registration form: GET COMMUNITY TODAY.
2. Enter your identification information in the form that appears.
   The form information includes: your first name, last name, email, country, phone number, and company.

   This information is used to create your Community Edition user login credentials.
3. Read and agree to the terms, privacy policy, and license agreement. Select and click Submit.

Next steps

Await the email from Automation Anywhere that contains the information for you to login to Automation Anywhere Enterprise Community Edition. This includes: Community Control Room URL, your username and assigned user password. After you login, you are prompted to reset your password.
To learn more, see Training - Create bots without installation. This course introduces you to learn how to download and register as a new Community Edition user.
Note: You must log in with a registered A-People Community account to access course.

Log in to Automation Anywhere Enterprise Control Room

To log in to Enterprise A2019, open the Enterprise Control Room URL in your browser, enter your credentials in the login screen, and click Log in.

Prerequisites

Receive your registration confirmation email.

Enterprise A2019 users
    This is sent by your system administrator.
Community Edition users

1. Register for the Community Edition. See Register as a Community user.
2. This is sent by Automation Anywhere using the information your provided when your registered.

This email contains:

- Enterprise Control Room URL.
- Username, credentials and provisioning tokens (where applicable).
- Temporary password. Reset this password when you login the first time.

Procedure

1. Open the URL in your browser.
2. In the Log in form, enter your username and password.
   If this is the first time you are logging in, use the password provided in your welcome email.
3. First-time users: Change your password, and for Cloud users, create your security questions.
   The change password and create security questions form automatically opens when your log in for the first time. Complete the form.
   a) Complete the Change password fields.
   Type your current password. Then type the new password twice. Passwords are 8-15 characters long and can only contain the characters: a-z, A-Z, 0-9, at sign (@), dash (-), underscore (_), exclamation (!), pound (#), dollar ($), percent (%), ampersand (&), and period (.).
   b) For Cloud users: In each field pair of Question # and Answer, type a question and an answer that you will remember in the event your forget your password or need to confirm your login.
   c) Click Save and log in.
   After first login, to change password, click your username, select Change password, and complete the form.
4. Optional: Select Remember my username to quickly log in to the Cloud Control Room.
5. Optional: Click Forgot password? to reset your password.

   An email is sent to you with a link to the necessary page to reset the account password.

6. Click Log in.
   The credentials are authenticated directly with the Cloud Control Room or Community Control Room database.
   Note: Your account is locked if you type the wrong password a specific number of times depending on the password policy set by your administrator. For security reasons, failed log-in attempts are audited. This allows the administrator to analyze and take appropriate actions.

Related tasks
Create your first bot
Register device and install Bot agent
Reset user password

Register device and install Bot agent

The Bot agent is a lightweight application that enables you to run bots on your device by connecting a local machine to the Enterprise Control Room. To run bots on a local machine, install the Bot agent and add the local device to the list of enabled host devices.

The Bot agent version available for download is the latest and compatible with the Enterprise Control Room version that is used.

Note: Use the mouse to roll over action icons to identify specific functions.

Procedure

1. Log in to the Enterprise Control Room through your Automation Anywhere Enterprise URL.
2. Navigate to MY DEVICES.
3. From the action icons, click Add local bot agent.
4. Click Connect to my computer.
5. Follow the steps outlined in the wizard.
   Authenticated proxy access:

If your device's access to the internet is controlled through an authenticating proxy server, you are prompted to provide the proxy server authentication details. These credentials are required for the device to communicate with the Enterprise Control Room.

To enable the authenticated proxy, register the device through a Chrome browser with the Automation Anywhere Chrome extension enabled.

6. Refresh the My Devices page and verify that the local device is added.

   Watch the following video on how to install the Bot agent in Enterprise A2019:

   Install the Bot agent

Next steps

Set device credentials. Optionally, Edit profile.

To learn more, see Training - Bot Runners and Control Room communicate without human intervention. This course introduces you to learn how to register devices in the Enterprise Control Room

To access this course, you must log in with a registered Automation Anywhere University or A-People account. .

- Manually switch the Bot agent
  Switch the Bot agent on a registered device to work with a different Enterprise Control Room.
- Set device credentials
  To enable a device for running bots, set the local device credentials.
- Connect Bot agent to an authenticating proxy
  If your bot cannot connect to the Enterprise Control Room due authentication proxy credentials, complete the steps in this task to add the authentication details.
- Set device credentials
  To enable a device for running bots, set the local device credentials.
- Edit profile
  Manage user profiles.

Related tasks
Create device pools
Related reference
Manage my device pools

Manually switch the Bot agent

Switch the Bot agent on a registered device to work with a different Enterprise Control Room.

Prerequisites

Ensure that you have the proper permissions to access and edit the Windows services.

The Bot agent, a lightweight application that enables you to run bots on your device, is associated with an Enterprise Control Room. This task provides steps on how to associate your device with a different Enterprise Control Room.

Procedure

1. Stop the Bot agent service from the local Windows Task Manager.
2. Optional: Go to the C:\Windows\System32\config\systemprofile\AppData\Local\AutomationAnywhere folder and delete the registration.properties file.
   Note: This is only required if you want to register the device in a different Enterprise Control Room environment. To see the Enterprise Control Room where the device is registered, open the Registration.properties file and check the value for the Enterprise Control Room URL.
3. Log in to the Enterprise Control Room.
4. Navigate to Devices > My devices.
5. Click the Add local device icon.
6. Download and install the latest Bot agent.
7. Return to Devices > My devices from the updated device.
   The Registration.properties file is not generated immediately after the Bot agent installation. It is generated only when a user accesses an Enterprise Control Room URL from that device. If the device registration is successful, the machine appears as Connected and the Registration.properties file is created at the given location on the Bot Runner machine.
8. Navigate to the C:\Windows\System32\config\systemprofile\AppData\Local\AutomationAnywhere folder and ensure that the registration.properties file is present to verify the Bot agent update.

   Watch the following video on how to update your Bot agent:

   Update the Bot agent

Related tasks
Register device and install Bot agent

Set device credentials

To enable a device for running bots, set the local device credentials.

Prerequisites

The Bot agent is a lightweight application that enables you to run bots on your device by connecting a local machine to the Enterprise Control Room. To run bots on a local machine, install the Bot agent and add the local device to the list of enabled host devices. Add the local device before editing the credentials. See Register device and install Bot agent.

For Automation Anywhere Enterprise Community Edition users, your profile contains only one set of credentials at a time. These credentials are applied to any device you select to run your bots. Ensure each device that you use accepts the credentials in your profile.

Automation Anywhere Enterprise Cloud users have the option to apply different credentials to registered devices.

Procedure

1. Click the Device icon and select Update credentials.
2. In the Device login credentials section, enter the Username and Password for the device.
   Device login credentials are required to run a bot from this device.
   Note: Enterprise A2019 does not validate the device login credentials until you run a bot.

If your username is part of a domain, include the domain within the format `domain\username`. Typically, home users are not part of a domain, unless they are specifically configured.

3. Click Update.

Next steps

Create your first bot

Connect Bot agent to an authenticating proxy

If your bot cannot connect to the Enterprise Control Room due authentication proxy credentials, complete the steps in this task to add the authentication details.

Typically, when you change your authenticating proxy settings, whether you added an authenticating proxy or changed the credentials to the authenticating proxy, the Bot agent prompts for the new credentials.

If you need to manually add or update the authenticating proxy credentials complete the following steps.

Procedure

1. On the registered device, open a PowerShell in Administrator mode.
2. List the proxy status by running the command:
   ```
   netsh winhttp show
                             proxy
   ```
3. If the command returns `Direct access`, then run the command:
   ```
   netsh winhttp import proxy source = ie
   ```
4. Restart the Bot agent.
5. Open a Google Chrome browser with the Automation Anywhere extension enabled.
6. Log out and log back in to the Enterprise Control Room.
   When you log in to the Enterprise Control Room now, it prompts for the proxy credentials.
7. From the Enterprise Control Room, check the device status and verify that it is connected.

Create your first bot

Follow these steps to create your first bot that prints the message, `Go be great!`, the Automation Anywhere version of `Hello World!`

Prerequisites

Log in to your instance of the Automation Anywhere Enterprise Community Control Room or Cloud Control Room.

These steps describe the guided workflow for first time users. The guided workflow is only displayed the very first time you complete these steps.

Procedure

1. Open a new bot:

a) From the Automation Anywhere Enterprise web interface, select Bots > My bots.
b) Click Create TaskBot.
c) Enter a bot name.
d) Accept the default folder location \Bots\.
To change where your bot is stored, click Choose and follow the prompts.
e) Click Create and Edit.

2. Insert a Message box package action.
   a) Click Actions.
   b) Search for the Message Box package.
   Click in the Actions search box and type the word, `message`. Click the arrow to expand the Message Box options.
   c) Double-click or drag the Message Box action to the Bot editor (open space to the right).
   A dialog box to configure the action opens.
3. Specify the conditions for the Message Box action.
   a) In the Enter the message box window title field, type `My first bot!`.
   b) In the Enter the message to display field, type `Go be great!`.
   c) Accept the defaults in the Scrollbar after lines field and Close message box after check box.
   d) Click the Apply button to save your message edits.
   The Message Box action is added to the flowchart in the Bot editor.
4. Click Save.
   Your bot is now ready to run.

Next steps

1. Click through the Bot editor options for viewing and editing bots:

   They are located at the top of the Bot editor.

   - Flow: Graphical representation of the process (default).
   - List: Sequential entries for each action.
   - Dual: Split screen of the Flow and List views.
2. Run your bot from your Automation Anywhere Enterprise device. See Run your first bot.

Run your first bot

Run a bot from the same device that you used to create the bot.

Prerequisites

Log in to your instance of the Automation Anywhere Enterprise Community Control Room or Enterprise Control Room.

Complete these previous steps:

1. Register device and install Bot agent
2. Set device credentials
3. Create your first bot

These steps describe the guided workflow for first-time users. The guided workflow is only displayed the very first time you complete these steps.

You can run a bot from the following devices:

- The same device you are using to log in to the Community Control Room or Enterprise Control Room.
- Another device you registered that has the same login credentials as the machine you are using to log in to your Community Control Room or a device with defined credentials in the Enterprise Control Room.

Note: Windows NT LAN Manager (NTLM) is a challenge or response authentication method that enables clients to provide their user name and password as encrypted credentials or plain text. Use Google Chrome browser to enable the Automation Anywhere extension and capture the proxy information. After the proxy information is captured, you can use any browser to run a bot in Enterprise A2019.

Procedure

1. Locate and select your bot.
   From your Community Control Room or Enterprise Control Room dashboard, select BOTS > My Bots.
2. Select the bot to run.

   From the Files and folders table, mouse over the ellipsis (three stacked dots) to the right of your bot's name.

   The Edit TaskBot panel appears.

3. Click the Run Task bot icon.
   The Run bot now window opens. In the Task Bots table, your bot is selected to run.
4. Click Next.
   The Device tab opens with a table of one or more registered devices.
5. If your device is not already selected, select your device to run the bot, and click the right arrow.
6. Click Run bot now.
   Automation Anywhere Enterprise uses the credentials in your profile to log in to the device you selected and runs the bot.
   The In progress activity window opens with the status of the running bot. When the bot is done, it disappears from this window.
7. Click Historical to see if your bot ran successfully.

   Watch the following video on how to run your first bot in the Community Edition:

   Run your first bot

Next steps

Build bots using variables, actions, and the Universal Recorder. See Get started building bots.

Getting started with IQ Bot A2019, Cloud, and Community Edition

Perform these tasks to set up IQ Bot A2019 Cloud deployed, On-Premises, and Community Edition and start using them with the same editions of Enterprise A2019.

IQ Bot A2019 Cloud deployed

Follow these steps to deploy and register as a user:

1. Receive your Enterprise Control Room URL and login credentials

   The URL points to your Automation Anywhere IQ Bot instance.

   If you are your company's principal administrator and ordered Cloud deployed IQ Bot A2019, you receive an email from Automation Anywhere with your URL and credentials.

2. Log in to Automation Anywhere Enterprise Control Room

   To log in to Enterprise A2019, open the Enterprise Control Room URL in your browser, enter your credentials in the login screen, and click Log in.

3. Create your user in the Enterprise Control Room.
   You can create user for the following roles:
   - AAE_IQBotAdmin
   - AAE_IQBotServices
   - AAE_IQBotValidator

   Use the assigned roles to connect to IQ Bot.
4. Go to the Enterprise Control Room dashboard to access the IQ Bot URL link.

   Connect to IQ Bot with the assigned user role, and begin creating learning instances.

IQ Bot A2019 Community Edition

Receive your IQ Bot URL and login credentials.

- The URL points to your Automation Anywhere Enterprise instance.
- If you are an Automation Anywhere IQ Bot Community Edition user, the login credentials are those you set when you registered.
- Complete the steps in Register as a Community user.

  The steps for IQ Bot Community Edition are the same as Automation Anywhere Enterprise registration.

- Begin using IQ Bot Community Edition by creating learning instances.

Watch the following video to understand how to create a learning instance in the IQ Bot A2019 Community Edition: Build an IQ BotCommunity Edition learning instance

IQ Bot A2019 On-Premises

The steps you perform to install IQ Bot A2019 On-Premises are the same as the installation steps for IQ Bot Version 6.5.2.

Installing IQ Bot

- Upgrading IQ Bot A2019
  Upgrade to the most recent version of IQ Bot A2019 On-Premises for all the latest features and enhancements.

Related concepts
Getting started with Enterprise A2019 (Cloud deployed) and Community Edition

Upgrading IQ Bot A2019

Upgrade to the most recent version of IQ Bot A2019 On-Premises for all the latest features and enhancements.

Prerequisites

Before you start the upgrade, ensure all the IQ Bot learning instances are backed up. If you are upgrading to IQ Bot Cloud, ensure you install the latest version of IQ Bot A2019 On-Premises.

Review the following version compatibility table to understand the available upgrade options for IQ Bot A2019:

IQ Bot version	IQ Bot A2019 (On-Premises)
Version 6.5.2	Yes
Version 6.5	Yes
Version 6.0	Yes
IQ Bot 5.3.1	Yes
IQ Bot A2019 (Builds 550, 1089, 1610, 2079, 2545, 3337, and 4088)	Yes

Note: Upgrade from IQ Bot 11.x to IQ Bot A2019 On-Premises is not supported.
Upgrade options:

- Upgrade from builds 1089, 1598, and 2079 to the latest version of IQ Bot A2019: Run IQ Bot On-Premises database migration script
- Update from newer builds to the latest version of IQ Bot A2019: Update IQ Bot A2019 to the latest version

- Upgrade from earlier IQ Bot versions to IQ Bot A2019 On-Premises
  Upgrade from an earlier IQ Bot version (5.3.x, 6.5, or 6.5.2) to IQ Bot A2019 (On-Premises) for the latest features and enhancements.
- Upgrade from IQ Bot A2019 On-Premises to Cloud
  IQ Bot Cloud offers all the IQ Bot A2019 On-Premises features through a browser-based interface.
- Update IQ Bot A2019 to the latest version
  If you are using any of the earlier versions of IQ Bot A2019, you can update to the latest version.

Upgrade from earlier IQ Bot versions to IQ Bot A2019 On-Premises

Upgrade from an earlier IQ Bot version (5.3.x, 6.5, or 6.5.2) to IQ Bot A2019 (On-Premises) for the latest features and enhancements.

The database schema can be upgraded to IQ Bot A2019 On-Premises only from IQ Bot Version 6.5.2.

Procedure

1. Uninstall any earlier IQ Bot version (5.3.x or 6.5).
   Note: Uninstalling an existing IQ Bot build does not delete the database.
2. Download and install Version 6.5.2 using the following link:
   https://automationanywhere-support.app.box.com/s/t4sg33si1fz0s3kvfv62t5e10rpz22fl.

Note: Contact support if you are unable to sign in.
3. While installing Version 6.5.2, connect to your existing database.
   The database schema is updated to Version 6.5.2.
4. Uninstall Version 6.5.2.
5. Download and install the latest IQ Bot A2019 build from the Automation Anywhere support site: Automation Anywhere Downloads.
   Note: During installation, a new IQ Bot database is created.

   Remember your database user name and password for updating the migration script value.

6. Run the data migration script to migrate data from Version 6.5.2 to the IQ Bot A2019 database.
   Run IQ Bot On-Premises database migration script
   Data from multiple databases is migrated to a single unified database.

Upgrade from IQ Bot A2019 On-Premises to Cloud

IQ Bot Cloud offers all the IQ Bot A2019 On-Premises features through a browser-based interface.

Prerequisites

You must install the latest version of IQ Bot A2019 On-Premises before you upgrade to IQ Bot Cloud. See Upgrade from earlier IQ Bot versions to IQ Bot A2019 On-Premises.

Procedure

1. Use the Migration Utility to export learning instances from IQ Bot A2019 On-Premises version.
2. Use API to upload the iqba file to IQ Bot Cloud.
   Note: Contact support for API upload instructions.
3. Open IQ Bot Cloud and import learning instances using Migration Utility.

All your learning instances from IQ Bot A2019 are imported and available on IQ Bot Cloud.
Important: Review the following points:

- If the learning instances are large, migrate them one at a time to avoid timeouts.
- Migrate custom domains if you use them.
- Import the custom domains in the same order as they were in the IQ Bot A2019 On-Premises version.

Update IQ Bot A2019 to the latest version

If you are using any of the earlier versions of IQ Bot A2019, you can update to the latest version.

Prerequisites

Latest version of IQ Bot A2019 offers enhancements and bug fixes. It is recommended that you review your existing IQ Bot A2019 version and back up your database, output path, and installation configuration files.

Uninstall the existing version of IQ Bot A2019 from your machine before updating to the latest version.

Procedure

1. Log in to Automation Anywhere Support site to download the latest version of the IQ Bot A2019 setup file.
   Automation Anywhere Downloads
2. Click the link to the latest IQ Bot A2019 setup file.
3. Click Installation Setup.
4. Download the Automation_Anywhere_IQ_Bot_A2019_Build_<build number>.exe file and install it.
   Installing IQ Bot

The latest installation file updates the existing IQ Bot A2019 installed on your device.

Run IQ Bot On-Premises database migration script

IQ Bot On-Premises Builds 1089, 1598, and 2079 included five databases. Starting with IQ Bot On-Premises Build 2545, one unified database is supported. You have to run a migration script to migrate the databases of Builds 1089, 1598, 2079 to the latest build.

Prerequisites

Before you run the migration script, you must be on the latest IQ Bot On-Premises build, and verify that the SQL command utility SQLCMD.exe is installed on your system.

Also, verify and ensure Microsoft ODBC Driver 17 for SQL Server is installed on the IQ Bot server. This can be obtained from: https://www.microsoft.com/en-us/download/details.aspx?id=56567

1. Uninstall the current build of IQ Bot On-Premises.
2. Install the latest IQ Bot On-Premises build.

   During installation, a new IQ Bot database is created.

   Note: Remember your database username and password in order to the update migration script value.
3. Navigate to your Binn folder.

   This might be located in C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\170\Tools\Binn.

4. Verify that SQLCMD.exe is installed.
   If SQLCMD.exe is not installed, follow these steps:
   a) Download and extract the Data Migration.zip from the Installation Setup folder onto the IQ Bot server.
   b) Navigate to DataMigration > UTILITY-MsSqlCmdLnUtils.
   c) Run MsSqlCmdLnUtils.msi to install SQLCMD.exe.

After SQLCMD.exe is installed, run the migration script.

Procedure

1. Access the AA.IQBot_Database_Migration.bat file within the DataMigration folder.
2. Edit the AA.IQBot_Database_Migration.bat file.
3. Update the values as follows:
   a) Set the `SQLCMD` value to the path of your Binn.

```
SQLCMD="C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\170\Tools
\Binn\SQLCMD.exe"
```

b) Set `LOGIN` value to your database username.

```
LOGIN="database username"
```

Note: The bulkadmin, dbcreator, and public roles are required to run the migration script.

c) Set the `PASSWORD` value to your database password.

```
PASSWORD="database password"
```

d) Set the `SERVER` value to the path of your database server hostname.

```
SERVER="path of database server hostname"
```

4. Run the migration script AA_IQBot_Database_Migration.bat file with administrator privilege.
   After the migration is complete, an output is created. Verify C:\Datamigrationlog.txt for log history and errors.
   Note: If an output is not displayed, contact support.

Enterprise A2019 On-Premises prerequisites

Determine whether the system has the required hardware and software to install Enterprise Control Room for A2019 On-Premises deployment.

Hardware requirements

Enterprise Control Room server requirements

The Enterprise Control Room is deployed on servers in data centers. The minimum Automation Anywhere hardware requirements include: server type, machine type, processor, RAM, disk storage, and network requirements.

Enterprise Control Room operating system compatibility

Enterprise A2019 Enterprise Control Room is installed on machines with supported operating systems.

Bot agent compatibility

Bot agent is the Automation Anywhere Enterprise plug-in that allows you to create and run bots. Bot agent is installed on devices used to access the Enterprise Control Room. Installing the Bot agent is part of registering a device.

Credential requirements

Login credentials are required at different stages of Automation Anywhere deployment and use. Credentials are required for installation and data center servers, access to Automation Anywhere components, and to run tools in bots.

Data center requirements

Database requirements

View the list of supported databases, database server type, version, hardware, and operating system requirements, and database backup and recovery requirements.

Working with SQL Servers

Configure Microsoft SQL Servers before setting up the Enterprise Control Room database.

Working with Azure SQL PaaS

Using PaaS SQL database with Azure requires configuration from the Azure instance.

Load balancer requirements
: View the load balancer requirements for Automation Anywhere installation. This includes load balancer minimums, and both TCP and HTTPS layer load balancing requirements.

Ports, protocols, and firewall requirements
: View the default and configurable firewall, port, and protocol requirements for Automation Anywhere deployment.

Supported browsers for Enterprise A2019
: The user interface for Enterprise A2019 (On-Premises or Cloud deployed) and Community Edition is through a browser.

HA and single-node deployments
: Identify your key requirements before selecting a deployment model. Automation Anywhere Enterprise offers multiple deployment options to meet various levels of enterprise cost/price performance and resiliency needs. This includes installation on single-nodes, and Highly Available (HA) clusters.

High Availability deployment model
: The High Availability (HA) deployment model provides failure tolerance for the Enterprise Control Room servers, services, and databases.

Single-Node deployment
: A single-node deployment is used for some proof-of-concept deployments.

Related concepts
Installing Enterprise Control Room on Microsoft Azure
Installing Enterprise Control Room on Amazon Web Services
Installing Enterprise Control Room using Custom mode
Related tasks
Installing Enterprise Control Room using Express mode
Installing Enterprise Control Room using scripts

Enterprise Control Room server requirements

The Enterprise Control Room is deployed on servers in data centers. The minimum Automation Anywhere hardware requirements include: server type, machine type, processor, RAM, disk storage, and network requirements.

Note: Automation Anywhere does not provide any monitoring functions for repository such disk space usage, memory or other alert mechanisms related to repository. There are commercial tools available from other third party independent software vendors (ISV) who provide such tools.
The installation wizard requires the following:

- IP addresses - Identify all the nodes (servers) IP addresses in the data center cluster before installation. You provide these IP addresses during Enterprise Control Room installation.
- Access hardware - To enable viewing the Automation Anywhere interface, provide:
  - keyboard
  - mouse or other pointing device
  - monitor with 1366 x 768 or higher resolution

Note: For IQ Bot server requirements, see IQ Bot hardware and software requirements IQ Bot hardware and software requirements .

Enterprise Control Room must be installed on a 64 bit, server level machine and there can only be one instance of it on the machine. All previous Enterprise Control Room versions must first be removed from the server machine before you begin the installation.

The following server requirements for Windows and Linux.

Component server	Processor	RAM	Storage (free disk space)	Network
Enterprise Control Room Servers	8 core Intel Xeon Processor	16 GB	500 GB	1 GbE

Note: We recommend you to configure the Enterprise Control Room network bandwidth to above 1 GbE, as the uplink traffic might quickly exceed 1 GbE, depending on the complexity of the automations that are run.

Enterprise Control Room operating system compatibility

Enterprise A2019 Enterprise Control Room is installed on machines with supported operating systems.

Enterprise Control Room supported operating systems and platforms

The Enterprise Control Room can be installed on machines running the following operating systems and platforms.

Microsoft operating system version 64-bit is supported.

For Bot agent operating system and platform compatibility, see Bot agent compatibility.

Note: Enterprise A2019 can be hosted on AWS, Microsoft Azure, Google Cloud Platform, IBM, and any public, private, or hybrid cloud service provided it meets the Enterprise Control Room and Bot agent hardware and software requirements.

Enterprise Control Room build version[1]	Windows Server 2019 Standard and Datacenter	Windows Server 2016 Standard and Datacenter	Linux CentOS 7.7 Red Hat Enterprise Linux 7.7
On-Premises Build 2545 Cloud Build 2545	On-Premises Amazon Web Services Elastic Compute Cloud (EC2) Microsoft Azure	On-Premises	On-Premises Amazon Web Services Elastic Compute Cloud (EC2)
On-Premises Build 2079 Cloud Build 2079	On-Premises Amazon Web Services Elastic Compute Cloud (EC2)	On-Premises	

Enterprise Control Room build version[1]	Windows Server 2019 Standard and Datacenter	Windows Server 2016 Standard and Datacenter	Linux CentOS 7.7 Red Hat Enterprise Linux 7.7
	Microsoft Azure		
On-Premises Build 1610 Cloud Build 1598	On-Premises Amazon Web Services Elastic Compute Cloud (EC2)	On-Premises	
On-Premises Build 1089 Cloud Build 1082	On-Premises Amazon Web Services Elastic Compute Cloud (EC2)	On-Premises	

Platforms supported by Enterprise A2019 version

Platform type	Cloud deploy	On-Premises deploy
Amazon Web Services Elastic Compute Cloud (EC2)	Cloud Build 2079 or later	On-Premises Build 2079 or later
Microsoft Azure VM	Cloud Build 1598 or later	On-Premises Build 1610 or later
On-Premises server	Cloud Build 1082 or later	On-Premises Build 1089 or later

Bot agent compatibility

Bot agent is the Automation Anywhere Enterprise plug-in that allows you to create and run bots. Bot agent is installed on devices used to access the Enterprise Control Room. Installing the Bot agent is part of registering a device.

Bot agent hardware requirements

The Bot agent can be installed on devices that meet the following hardware requirements.

Device	Processor	RAM	Storage (free disk space)	Network
Machine	Intel Core i5 2.6 GHz	4 GB minimum 8 GB recommended	32 GB	1 GbE
Bot Creator and Bot Runner	No additions to the machine requirements	No additions to the machine requirements	Add 100 through 150 KB per Automation Anywhere script Add 40 through 50 GB per long-term project	No additions to the machine requirements

RAM on Cloud or Community Edition devices

Add additional RAM to account for applications and services running on the Automation Anywhere Enterprise machine, for example:

- Microsoft Office applications (example: Excel)
- Browsers (example: Google Chrome)
- Enterprise applications (example: CRM, Oracle EBS, and SAP)
- VDI infrastructure applications
- Anti-virus software

Storage disk space on Cloud or Community Edition devices

- Automation Anywhere Enterprise scripts average approximately 100-150 KB. Additional free disk space is required to develop automation projects because temporary files such as screen shots, server logs, and audit files are created during the execution of the automation scripts.
- Free space required increases with the project size. Recommendation: Have at least 40-50 GB of free disk space for each long-term project.
- Increase storage space configuration after installation, as needed, depending on product usage. For example, depending upon the complexity of your bot, generating log files and logic creation require additional disk space later.

Bot agent platform compatibility

A device running the Bot agent to perform bot tasks must meet the platform requirements.

Note: Platform requirements are different for Enterprise Control Room and Bot agent.

On-Premises machines

Physical machines running any of the supported operating systems.

Terminal servers

Using remote desktop (RDP) running any of the supported operating systems is supported is supported on Enterprise A2019 Version A2019.11 or later. .

Virtual machines

Bot agent is supported on all VMs where the supported Windows OS has been hosted on Version A2019.09 or later. For example, Virtual Desktop Infrastructure (VDI) are supported on Amazon Web Services, Microsoft Azure, VMware virtual machines, and Oracle Virtual Box.

Bot agent operating system compatibility

The Automation Anywhere Enterprise Bot agent can be installed on machines running the following operating systems.

This applies to On-Premises, Cloud deployments, and Community Edition of Enterprise A2019.

Note:

- Bot Creator tasks are supported with all the listed operating systems.
- You cannot register a device that is running on a Linux system. The Bot agent cannot be installed on Linux systems. However, you can use a registered device running on a Windows system to access an Enterprise Control Room that is installed on a Linux system.

Windows version	Windows edition	Attended Bot Runner	Unattended Bot Runner	Bot Creator
Windows Server 2019[1]	Datacenter	Supported	Supported[2]	Supported
Windows Server 2016[1]	Datacenter	Supported	Supported[2]	Supported
Windows Server 2012 [1]	Standard	Supported	Supported[2]	Supported
Windows 10[1]	Professional and Enterprise	Supported	Supported[2]	Supported
Windows 8 [3]	Professional and Enterprise	Supported	Supported	Supported
Windows 7 [3]	Professional and Enterprise	Supported	Supported	Supported

(1) Credential Vault

Is supported on Enterprise A2019 versions newer than Version A2019 Builds 1598 and 1610.

(2) Auto-login

- Auto-login is only supported on 64 bit systems.
- If there is a legal disclaimer on the device then Auto-login fails.
- If the Auto-login fails, configure the Local Security Policy settings. For example, from Windows, select Security Settings > Local Policies > Security Options. Disable the Interactive logon: CTRL+ALT+DEL option.

(3) Supported OS

Windows 8 supported on Version A2019 Builds 1598 and 1610 or older.
Windows 7 supported on Version A2019.12 or later.

Auto login support

The following table identifies the OS support specific to the auto login functionality on Bot agent.

SID#	Scenario	Windows 2019	Windows 2016 R2	Windows 2012 R2	Windows 10	Windows 8	Windows 7
1	No user session established (user is not logged in)	Not applicable for virtual machines	Not applicable for virtual machines	Not applicable for virtual machines	Supported on local Windows 10 device and VirtualBox only	Not certified	Not certified
2	User session established	Not applicable for virtual machines	Not applicable for virtual machines	Not applicable for virtual machines	Supported on local Windows 10 device and VirtualBox only	Not certified	Not certified
3	User has logged in but locked the screen	Not applicable for virtual machines	Not applicable for virtual machines	Not applicable for virtual machines	Supported on local Windows 10 device and VirtualBox only	Not certified	Not certified
4	A different user (not the device login user used for deployment) is logged in	Not applicable for virtual machines	Not applicable for virtual machines	Not applicable for virtual machines	Supported on local Windows 10 device and VirtualBox only	Not certified	Not certified
5	A different user is logged in and locked the screen	Not applicable for virtual machines	Not applicable for virtual machines	Not applicable for virtual machines	Supported on local Windows 10 device and VirtualBox only	Not certified	Not certified
6	Fast user switching	Not applicable for virtual machines	Not applicable for virtual machines	Not applicable for virtual machines	Supported on local Windows 10 device and VirtualBox only	Not certified	Not certified
7	No active RDP session	Supported	Supported	Supported	Supported	Supported	Supported
8	User has active RDP session	Supported	Supported	Supported	Supported	Supported	Supported
9	User's RDP session is disconnected	Supported	Supported	Supported	Supported	Supported	Supported
10	User's RDP session is locked	Supported	Supported	Supported	Supported	Supported	Supported
11	Another user has active RDP session	Supported	Supported	Supported	Supported	Supported	Supported
12	Another user has a disconnected session	Supported	Supported	Supported	Supported	Supported	Supported
13	Another user has an active session and locked	Supported	Supported	Supported	Supported	Supported	Supported

Note:

1. Auto login is only supported on 64 bit systems.

2. Legal disclaimer on the device is not supported. If there is a legal disclaimer on the device then auto-login fails.
3. Auto-login is unable to sign-out the root Admin session, when trying with scenarios that involve 2 different auto-login users. Remember to login to console/RDP as a secondary user,
4. For scenarios 4,5, and 6 in the above table, the active user is logged off and a new session created with device credentials for deploying the bot.
5. Set the Local Security Policy. If the Auto-login fails, configure the Local Security Policy settings. For example, from Windows, select Security Settings > Local Policies > Security Options. Disable the Interactive logon: CTRL +ALT+DEL option.

Bot agent browser compatibility

The user interface for Automation Anywhere Enterprise is through a browser. Login to your device, then login to Enterprise Control Room through a browser.

Browser	Browser version	Automation Anywhere Plug-in version[2]
Google Chrome[1]	57 or later	11 or 12
Microsoft Internet Explorer	11	N/A

(1) Google Chrome re-verification

CAUTION: Google Chrome requires re-verification of permissions when the Automation Anywhere Google Chrome extension is updated. If prompted, click Enable this item in the Google Chrome message. Alternatively, re-enable the extension through chrome web store. Similarly, if you are deploying your Bot Runners from a master image, accept the permission from within that image.

(2) Google Chrome plug-in extension versions

Enterprise A2019 supports Chrome extension version 11. If either Google Chrome extension 11 or 12 was installed and then uninstalled, additional steps are required. See Changing Google Chrome extensions.

Related reference

Enterprise A2019 feature comparison matrix

Database requirements

View the list of supported databases, database server type, version, hardware, and operating system requirements, and database backup and recovery requirements.

Automation Anywhere installation creates a database to store bot data and metadata for the analytics dashboards. Note: Automation Anywhere does not provide any monitoring functions for database activities, such as disk space usage, memory, or other alert mechanisms related to databases. There are commercial tools available from database vendors and other third-party independent software vendors (ISV) who provide such tools.

Database server hardware requirements

Component server	Processor	RAM	Storage	Network
Microsoft SQL Server database	4-core Intel Xeon Processor	8 GB	500 GB	1 GbE

Database server version and operating system requirements

Microsoft SQL Server database is required.

Database type	Database version	Installed database OS	Configuration requirement
Microsoft SQL Server database	2017 2016 2014 SP1	Windows Server 2008 R2 Standard or later	Installed and configured. Only option for Express Installations Enable protocols for Named Pipes and TCP/IP.

Required database information for Automation Anywhere installation

When you install Automation Anywhere, you are prompted to provide information specific to the database type you are using. The following table summarizes the required information.

Microsoft SQL Server database	
Required information	Description
Database (SQL Server) authentication	Provide credentials for a Microsoft SQL Server user who has permission to connect to the database.
Database names	Database names cannot be blank, have spaces, or include a percent (%). Restrict the names to alphanumeric, period (.), dash (-), and underscore (_). Default name: AAE-Database
Database port	Default: 1433
Secure connection (optional) and certificate	Provide a CA certificate. Ensure the certificate host name and database connection are the same.
Service credentials	Provide Local system account user or Domain user account. This becomes the assigned user for the created databases and tables. The preferred method is to use the Domain user account. Provide the user with system administrator or database creator permission to create databases during installation.

Microsoft SQL Server database	
Required information	Description
Windows authentication	User-provided (or default) used to connect to the Microsoft SQL Server, test database exists, create database if not present, and set `db_owner` to the service account user.
Linux authentication	SQL Database server Login ID: `sa`SQL Database password: `Automation123`

Related concepts
Installing Enterprise Control Room on Amazon Web Services
Installing Enterprise Control Room on Microsoft Azure
Related tasks
Installing Enterprise Control Room on Linux

Working with Azure SQL PaaS

Using PaaS SQL database with Azure requires configuration from the Azure instance.

Configure the Azure instance before you install Automation Anywhere Enterprise.

Procedure

1. Login to your Azure account.
2. Navigate to the Azure SQL option .
3. Create a database based on your custom requirements.
4. Enable the firewall option.
5. Whitelist the IP address for accessing the database.

Next steps

Install Automation Anywhere Enterprise and point the database server to this instance of the SQL database. See Customize Enterprise Control Room installation on Microsoft Azure.

Load balancer requirements

View the load balancer requirements for Automation Anywhere installation. This includes load balancer minimums, and both TCP and HTTPS layer load balancing requirements.

Load Balancer Minimum Requirements

For best practice with Automation Anywhere, ensure the load balancer:

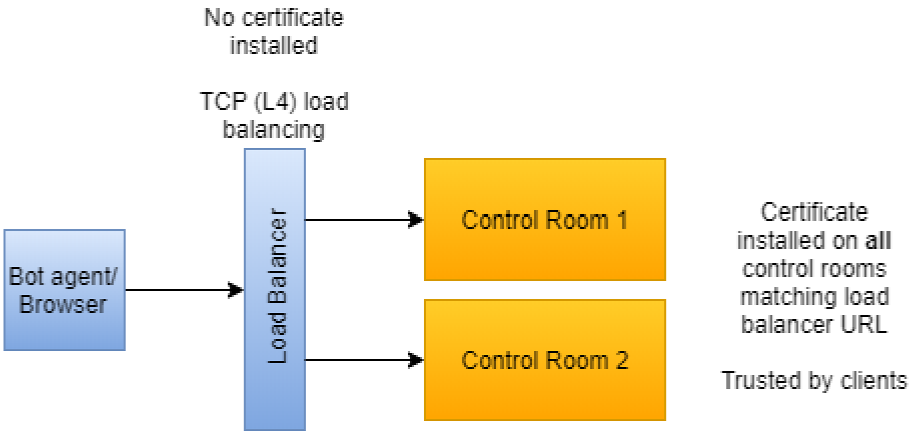
- (Required) Supports WebSocket protocol (RFC 6455)
- (Preferred) Has idle timeout set to 120 seconds
- (Preferred) Uses round-robin host selection. Is not configured to use persistent (sticky) sessions.
- (Preferred) Uses the appropriate TLS security layer:

- TCP (layer 4) load balancing
- HTTPS (layer 7) load balancing

  With a Nginx load balancer, set HTTPS termination at nodes by changing `http://Backend` to `https://Backend`.

TCP (Layer 4) Load Balancing

When TCP is applied at layer 4 with the load balancer, the certificate is installed on every Enterprise Control Room corresponding to the load balancer URL.



Pros

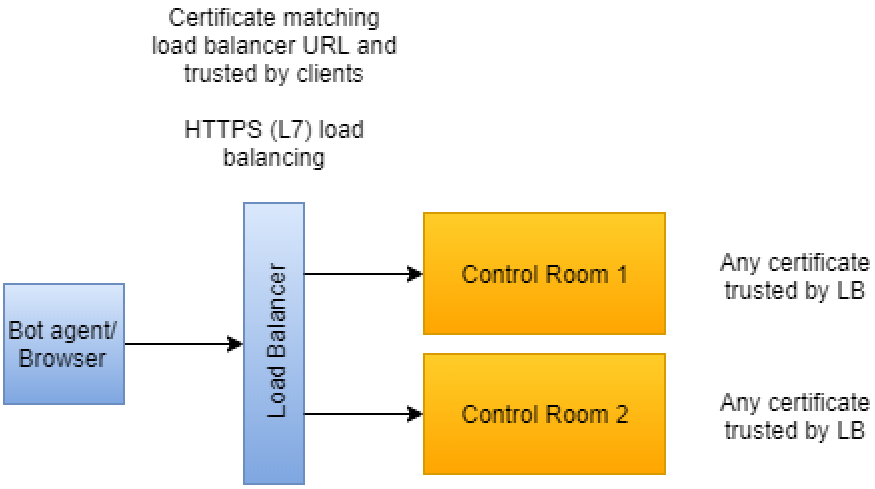
End-to-end encryption without the possibility of intercept at the load balancer.
Single certificate required.

Cons

If audit logging is required, the load balancer cannot report the requests from clients.
Does not use TLS hardware offloading, even if the load balancer supports it.

HTTPS (Layer 7) Load Balancing

When HTTPS is applied at layer 7 with the load balancer, the certificate corresponding to the load balancer URL is applied through the load balancer. The Enterprise Control Room trusts the certificates received from the load balancer.


Certificate matching load balancer URL and trusted by clients
HTTPS (L7) load balancing
Bot agent/ Browser
Load Balancer
Control Room 1
Control Room 2
Any certificate trusted by LB
Any certificate trusted by LB

Pros

- Allows request logging, when supported by the load balancer.
- Reduces load from TLS handshake through hardware offloading, when supported by the load balancer.

Cons

- Certificates must be managed both on the load balancer and on the control room nodes
- Possible interception of data at the load balancer hardware level, because TLS session is not end-to-end.

Ports, protocols, and firewall requirements

View the default and configurable firewall, port, and protocol requirements for Automation Anywhere deployment.

Add Automation Anywhere to the Windows Firewall exception list. Follow the steps as directed by Microsoft for your Windows version.

Configure the firewall rules for Enterprise Control Room. Refer to the following tables for lists of required ports and their use.

Enterprise Control Room

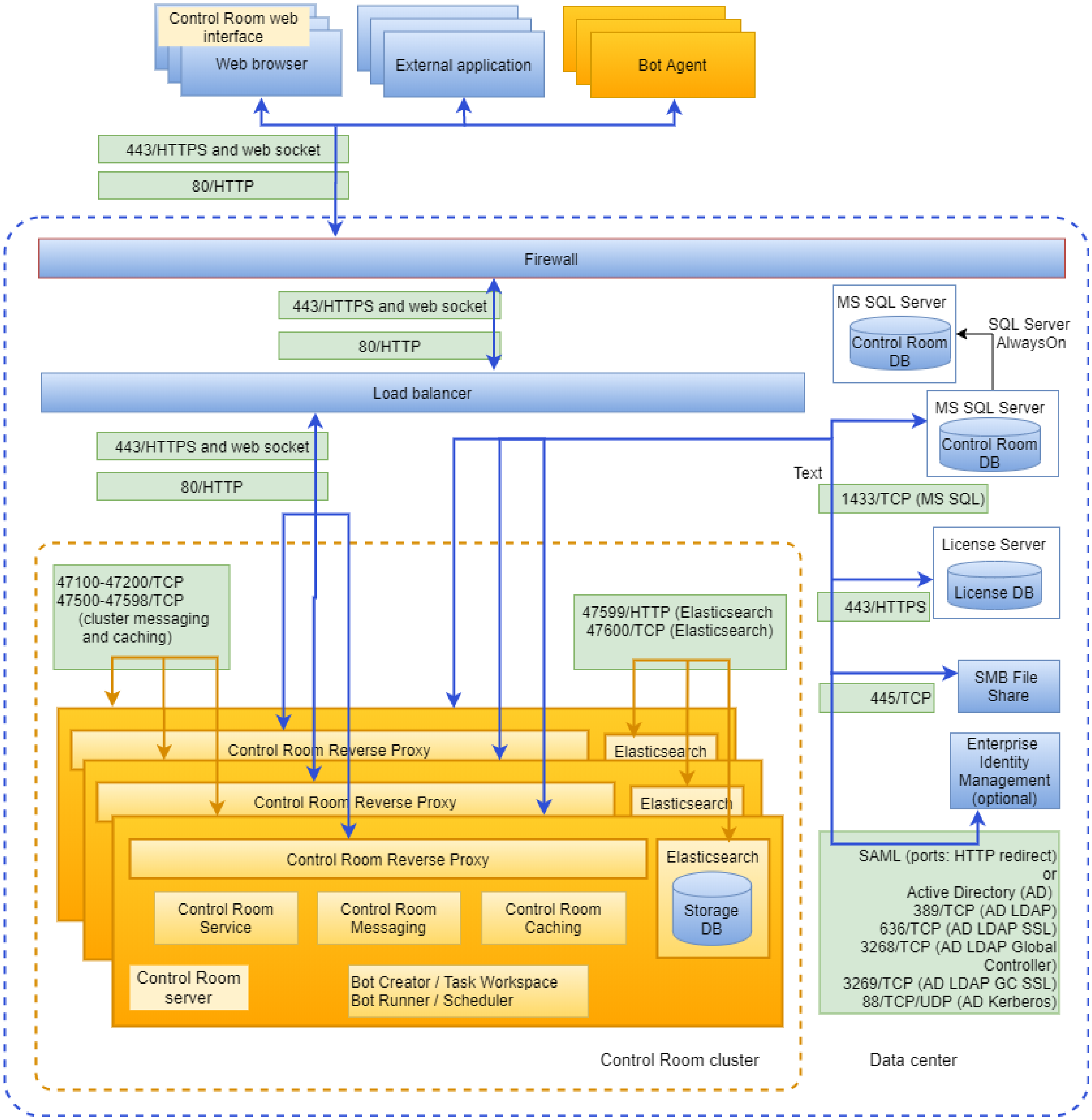
Warning: It is critical that communication between the Enterprise Control Room servers is properly protected. These Enterprise Control Room servers contain security sensitive information that is not encrypted. Therefore, excluding the Enterprise Control Room servers, you should block all other network hosts from accessing the listed Automation Anywhere cluster communication ports.

Protocol	Incoming Port	Usage	Clients
HTTP	80	HTTP	Web browsers
HTTPS	443	HTTPS and Web Socket	Web browsers

Protocol	Incoming Port	Usage	Clients
TCP	5672	Cluster Messaging	Enterprise Control Room Services
TCP	47500 – 47600	Cluster Messaging and Caching	Enterprise Control Room Services
TCP	47100 – 47200	Cluster Messaging and Caching	Enterprise Control Room Services
HTTP	47599	Elasticsearch	Enterprise Control Room Services
TCP	47600	Elasticsearch	Enterprise Control Room Services

Data center ports and protocols for Automation Anywhere Enterprise

Configure each of the data center components that are required for Enterprise Control Room integration.



Default ports are listed for illustration purposes. Some ports can have alternative port numbers specified during Enterprise Control Room installation. Some port numbers can be modified after Enterprise Control Room installation. Active Directory ports are listed as an example of an enterprise identity management.

All three objects, the web browser, Bot agent, and external applications each communicates with the Enterprise Control Room. A user logs in to the Enterprise Control Room through a browser, to do administrative tasks, such as creating users, or bot related tasks, such as deploying and scheduling bots. Bot agent communicates with the Enterprise Control Room when bots are deployed. External applications talk to the Enterprise Control Room directly through the Enterprise Control Room APIs to do tasks such as creating users or doing bot actions.

Data center object	Port default	Protocol default	Notes
Load balancer	443	HTTPS and web socket	
	80	HTTP	
Firewall	443	HTTPS and web socket	
	80	HTTP	
Enterprise identity management Example: Active Directory ports	389	TCP (LDAP)	
	636	TCP (LDAP SSL)	
	3268	TCP (LDAP Global controller)	
	3269	TCP (LDAP Global controller SSL)	
	88	TCP/UDP (Kerberos)	
Microsoft SMB file share	445	TCP	
Microsoft SQL database server	1433	TCP	Override default at Enterprise Control Room installation.

Microsoft Azure supported data center elements

Data center object	Version	Configuration
Enterprise Control Room operating system	Windows 2016	IaaS
Identity management: Azure	Azure Active Directory	IDaaS Windows 2016 for IaaS
	Azure File Share	PaaS
	Azure Load Balancer (Not Application Gateway)	PaaS

Data center object	Version	Configuration
	Azure SQL Database (Microsoft SQL Azure (RTM) - 12.0.2000.8)	PaaS

Microsoft Azure security policy recommended ports

Data center object	Port	Protocol
Enterprise Control Room	80, 443	Any
Azure Active Directory	53, 389	Any
LDAP	3268, 3269	Any
email SMTP	587	Any
SSH	22	Any
RDP	3389	TCP

Related tasks
Prepare for installation on Amazon Web Services
Verify readiness for installation on Microsoft Azure
Related reference
Enterprise A2019 On-Premises prerequisites

Supported browsers for Enterprise A2019

The user interface for Enterprise A2019 (On-Premises or Cloud deployed) and Community Edition is through a browser.

Supported browsers for Enterprise A2019 and Bot agent

Access to the Enterprise A2019 is through a browser on a registered device. Registering a device includes installing the Bot agent.

Browser	Browser version	Automation Anywhere Plug-in version[2]
Google Chrome[1]	57 or later	11 or 12
Microsoft Internet Explorer	11	N/A

(1) Google Chrome re-verification

CAUTION: Google Chrome requires re-verification of permissions when the Automation Anywhere Google Chrome extension is updated. If prompted, click Enable this item in the Google Chrome message. Alternatively, re-enable the extension through chrome web store. Similarly, if you are deploying your Bot Runners from a master image, accept the permission from within that image.

(2) Google Chrome plug-in extension versions

Enterprise A2019 supports Chrome extension version 11. If either Google Chrome extension 11 or 12 was installed and then uninstalled, additional steps are required. See Changing Google Chrome extensions.

Supported browsers for bot tasks

Bot tasks supported by Enterprise A2019 and browser versions.

Enterprise A2019 version	Google Chrome	Microsoft Internet Explorer
Cloud Build 2545 On-Premises Build 2545 Bot agent 3.3	All bot tasks	All bot tasks
Cloud Build 2079 On-Premises Build 2079 Bot agent 2.0.2	All bot tasks, except Credential Vault	Unsupported
Cloud Build 1598 On-Premises Build 1610 Bot agent 1.0.2	All bot tasks	Debugger only
Cloud Build 1082 On-Premises Build 1089 Bot agent 1.0.1	All bot tasks	All bot tasks, except Credential Vault

Changing Google Chrome extensions

Ensure the Automation Anywhere Google Chrome extension you are using is appropriate for your Enterprise A2019 installation.

Automation Anywhere has created different versions of the Google Chrome extension. If you already are using a Google Chrome extension and want to install a different version, review the following information and complete the steps in the procedure that applies to you.

Automation Anywhere Enterprise version	Google Chrome extension version
Version A2019	• 12.x— supported; can coexist with 11.x acceptable • 11.x—supported • 1.0.3.1—not supported

Procedure

1. Check if the Bot agent is running.

   For example, open the Windows Task Manager and scan for Automation.BrowserAgent.exe.

   If the Bot agent is running with Google Chrome extension version 11 installed and enabled, no additional steps are required.

2. If you have never installed Automation Anywhere Enterprise Version 11.3 or later, and the Bot agent is not running:
   a) Verify that Google Chrome extension version 11 is installed and enabled.
   b) Check the Windows registry for Google Chrome: Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Google\Chrome\NativeMessagingHosts\automation.chrome.agent
   c) Verify that the registry entry points to the Enterprise A2019 global cache.
3. If you have installed Automation Anywhere Enterprise Version 11.3.3 or later and Enterprise A2019 simultaneously:
   a) Check for the following Windows registry key: Computer\HKEY_CURRENT_USER\Software\Google\Chrome\NativeMessagingHosts\automation.chrome.agent
   - b) If the above key is available, disable the Google Chrome plug-in version 11.x and enable the Google Chrome plug-in version 12.x.
   - c) If the above key is not available, disable the Google Chrome plug-in version 12.x and enable the Google Chrome plug-in version 11.x.

   d) Restart Google Chrome.
   e) Ensure that the Bot agent Automation.BrowserAgent.exe is running with Google Chrome extension installed and enabled.
4. If you uninstall Automation Anywhere Enterprise Version 11.3:
   a) Disable Google Chrome extension 12.x.
   b) Install and enable Google Chrome extension 11.x.
   c) Open the registry on the Windows system for editing.
   d) Remove: Computer\HKEY_CURRENT_USER\Software\Google\Chrome\NativeMessagingHosts\automation.chrome.agent
   e) Check the Windows registry for Google Chrome: Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Google\Chrome\NativeMessagingHosts\automation.chrome.agent
   f) Verify that the registry entry points to the Enterprise A2019 global cache.
   g) Restart Google Chrome.

Enterprise Control Room and bot dependencies

Enterprise Control Room and bots have additional third party requirements depending upon the Automation Anywhere Enterprise options you choose. Some are optionally installed with Automation Anywhere Enterprise deployment. Some require an Automation Anywhere specific plug-in.

Enterprise Control Room third party dependencies

Install the listed dependency if you plan to use the listed supported option.

Dependency	Supported Enterprise Control Room option
Amazon Web Services Elastic Compute Cloud (EC2)	Install Enterprise Control Room platform.
HTML	For Microsoft Azure: Use Load Balancer, not Application Gateway.
Java Database Connectivity (JBDC) driver	For Oracle Database.
Linux CentOS or Red Hat Enterprise Linux	Install Enterprise Control Room platform.
Microsoft Active Directory	Configure as either IDaaS or IaaS. For IaaS use Windows 2016.
Microsoft Azure	Install Enterprise Control Room platform.
Microsoft Internet Information Services (IIS) web server, version 8 or later.	Lightweight Directory Access Protocol (LDAP) and Kerberos supported.
Microsoft OLEDB Driver for Microsoft SQL Server	For Express Enterprise Control Room installations.
Microsoft Visual C++ Redistributable for Visual Studio, version 2013 or later	For Express Enterprise Control Room installations.
SMB File Share	Configure as PaaS (50 GB minimum). For Microsoft Azure installations, use Microsoft Azure SMB File Share.
Security Assertion Markup Language (SAML), version 2.0	For Single Sign-On (SSO).

Note 1

> On new machines, physical or virtual, install Microsoft .NET Framework before your install Microsoft Office. This ensures required Primary Interop Assemblies (PIA) re-distributables are installed.

Bot third party dependencies

Install the listed dependency for the listed bot action.

Dependency	Automation Anywhere Plug-in	Supported Bot action
ABBYY FineReader Engine version 12		For capturing images in the OCR package.
Citrix Receiver Version 4.4 LTSR or later	Automation Anywhere Citrix plug-in Automation Anywhere Citrix remote agent	For bot actions on Citrix server resident apps.
HTML		For recording Web tasks using Universal Recorder. Technology support for Bot Creator.
IBM WebSEAL		For reverse proxy for Bot Runner.
Java, JRE 6, 7, and 8		For Universal Recorder.
Microsoft Active Accessibility (MSAA)		Supported with Universal Recorder. To import/export datasets Technology support for Bot Creator.
Microsoft Cognitive Services Text Analytics API		For Microsoft LUIS NLP package language support.
Microsoft .NET Framework version 4.6.1		For the Recorder package.
Oracle Java versions: 1.6 (JRE 1.6.0_45), 1.7 (JRE 1.7.0_80), or 1.8(JRE 1.8_111) - Desktop and Web.		For recording Web tasks using Universal Recorder. Desktop (standalone) Java applications (running on JRE 6 or later versions) do not require the Automation Anywhere Java plug-in. Technology support for Bot Creator.
Proxy service		For web service commands.
SAP DLL for SAP Business Application Programming Interface (BAPI) integration version 3.0.21.0		To automate tasks in SAP. Supported with Universal Recorder.

Dependency	Automation Anywhere Plug-in	Supported Bot action
SAP GUI version 750 with patch 9, version 760 with patch 0, or version 760 with patch 5		To connect with a SAP environment.
SMB File Share		Configure as PaaS (50 GB). For Microsoft Azure installations, use Microsoft Azure SMB File Share.
Terminal emulator. Types: • TN3270 • TN5250		To access and control terminal hosts.
Windows Communication Foundation (WCF), Transport Layer Security (TLS)		For secure communications with Bot Runner.

Citrix integration on Cloud

Automation Anywhere Enterprise integration with Citrix enables you to create bots that run tasks on remote Citrix Virtual Apps servers.

Process overview

Ensure the following tasks are completed before you begin automating tasks in a Citrix environment:

Verify credentials and licensing

- Ensure you have the credentials to access the Citrix server.
- Ensure the appropriate Citrix license is available for the Automation Anywhere Enterprise system.

Install components

Specific Citrix and Automation Anywhere Enterprise components are required on both the local user machine and the Citrix Virtual Apps server.

Local machine

1. Install Citrix Receiver version 4.12 or later.
2. Install the Bot agent. This is automatically installed when you register the local machine with the Enterprise Control Room.

   The Bot agent and Automation Anywhere plug-in for Citrix are installed at the same time if the Citrix Receiver is installed on the local machine.

3. Install the Automation Anywhere plug-in for Citrix.

If the Bot agent is already installed, the Automation Anywhere plug-in for Citrix is automatically installed when the Universal Recorder is initiated.

Citrix server

1. Install the Automation Anywhere remote agent for Citrix.
2. Register the Automation Anywhere remote agent for Citrix as a Virtual App in the Citrix StoreFront.

Create a bot

1. From the Citrix StoreFront, run the AARemoteAgent and the target application.
2. From the Enterprise Control Room, create the bot, start the Recorder, select the target application, and record your actions on the Citrix server to build your bot.

Using Citrix architecture with bots

To create and run bots using applications that reside on a Citrix server, see the following resources:

Using the Recorder on Citrix Virtual Apps servers

The Record: Capture cloning action requires specific configurations to capture objects from applications available through the Citrix StoreFront on a remote Citrix Virtual Apps server. Ensure the required components are installed on the local machine and the remote Citrix Virtual Apps server.

Related tasks
Using the Recorder on Citrix Virtual Apps servers
Using Citrix XenDesktop on Cloud
Installing the Citrix required components on local machines
Installing Automation Anywhere remote agent for Citrix on Citrix servers

Using the Recorder on Citrix Virtual Apps servers

The Record: Capture cloning action requires specific configurations to capture objects from applications available through the Citrix StoreFront on a remote Citrix Virtual Apps server. Ensure the required components are installed on the local machine and the remote Citrix Virtual Apps server.

Prerequisites

Complete the steps listed in the following tasks:

- Installing the Citrix required components on local machines
- Installing Automation Anywhere remote agent for Citrix on Citrix servers

Create bots with applications running on a remote Citrix Virtual Apps server using the Automation Anywhere remote agent for Citrix.

Procedure

1. Log in to the Citrix Virtual Apps server StoreFront.
2. Run the Automation Anywhere remote agent for Citrix: Select Citrix server > Citrix StoreFront > AARemoteAgent. AARemoteAgent is the Citrix name for the Automation Anywhere remote agent for Citrix.
3. Run the target application from the Citrix StoreFront.

4. Log in to your registered local machine with the Bot agent and Citrix Receiver installed.
5. Log in to the Enterprise Control Room from your registered local machine.
6. Create a new bot or edit an existing bot.
7. Select the auto login feature to log in to a Citrix environment when it is locked or logged off.
   Note: To ensure the auto login works, always log off the Citrix Receiver associated with the Citrix Virtual Apps server before you disconnect.
8. Start the Recorder.
9. From the Automation Anywhere Record Application selection window, select the target application from the drop-down list in the Window or URL field, and click Start recording.
   Note: The remote application has `\\Remote` label at the end of the application name.
10. When the steps to record are completed, click End recording.

Related concepts
Citrix integration on Cloud
Related tasks
Installing the Citrix required components on local machines
Installing Automation Anywhere remote agent for Citrix on Citrix servers
Using Citrix XenDesktop on Cloud

Installing the Citrix required components on local machines

Install the Automation Anywhere Enterprise components to enable you to use bots on Citrix Virtual Apps servers. Two components are installed: Bot agent and Automation Anywhere plug-in for Citrix.

Procedure

1. Log in to your local machine.
2. Install Citrix Receiver version 4.12 or later.
   This Citrix component is required to communicate from a local machine to a Citrix virtual application server.

   To install the Citrix Receiver, see the Citrix documentation.

3. Register your local machine with the Enterprise Control Room. This installs the Bot agent.
   The Bot agent enables local machine communication with the Enterprise Control Room.

   To install the Bot agent:

   a) Log in to the Enterprise Control Room through your Automation Anywhere Enterprise URL.
   b) Navigate to MY DEVICES.
   c) From the action icons, click Add local bot agent.
   d) Click Connect to my computer.
   e) Follow the steps outlined in the wizard.
   f) Refresh the My Devices page and verify that the local device is added.
4. Install Automation Anywhere plug-in for Citrix on your local machine.
   The Automation Anywhere plug-in for Citrix provides the Citrix driver. This driver communicates with the Citrix server.

   To install the Automation Anywhere plug-in for Citrix:

   a) Log in to the Enterprise Control Room.
   b) Launch one of the designated events.

Designated events include: launch Recorder, use the Devices tab or Device Status tab, or run a bot from Editor.
c) Optional: Verify that the Automation Anywhere plug-in for Citrix is installed.
Check for the file C:\Program Files (x86)\Citrix\ICA Client\Automation.CitrixDriver.dll.

Related concepts
Citrix integration on Cloud
Related tasks
Using the Recorder on Citrix Virtual Apps servers
Installing Automation Anywhere remote agent for Citrix on Citrix servers
Using Citrix XenDesktop on Cloud

Installing Automation Anywhere remote agent for Citrix on Citrix servers

Install the Automation Anywhere remote agent for Citrix on the Citrix Virtual Apps server where the virtualized applications are installed.

Procedure

1. Log in to the Citrix Virtual Apps server.
2. Download the latest version of the Automation Anywhere remote agent for Citrix installer file to the Citrix Virtual Apps server.

   The Automation Anywhere remote agent for Citrix running on the Citrix server interprets data received from Automation Anywhere Enterprise and responds appropriately.

   a) Go to Automation Anywhere Downloads.
   b) Select and download the Automation Anywhere remote agent for Citrix.
3. Run the Automation Anywhere remote agent for Citrix installer.
   a) Extract the AARemoteAgent.zip file and double-click the AAE_Remote_Agent_1.0.0.exe file.
   b) On the Automation Anywhere Remote Agent Setup screen, click Next.
   c) On the License Agreement screen, accept the license agreement, and click Next.
   d) On the Select Destination Folder screen, click Browse to specify a non-default location for installing the remote agent. Click Next.
   The default location for installation is set to: C:\Program Files (X86)\Automation Anywhere \AARemoteAgent
   e) On the Setup Status screen, track the status of the installation process.
   f) On the Setup Wizard Complete screen, click Finish to complete the setup.
4. From the Citrix interface, add the Automation Anywhere remote agent for Citrix application to the Citrix Delivery Controller.
   This registers the Automation Anywhere remote agent for Citrix as a Virtual App in the Citrix StoreFront.
5. Verify that the Automation Anywhere remote agent for Citrix is available from the Citrix StoreFront.
   The Citrix StoreFront name for the Automation Anywhere remote agent for Citrix is AARemoteAgent.

Related concepts
Citrix integration on Cloud
Related tasks
Using the Recorder on Citrix Virtual Apps servers
Installing the Citrix required components on local machines
Using Citrix XenDesktop on Cloud

HA and single-node deployments

Identify your key requirements before selecting a deployment model. Automation Anywhere Enterprise offers multiple deployment options to meet various levels of enterprise cost/price performance and resiliency needs. This includes installation on single-nodes, and Highly Available (HA) clusters.

Planning

For best results, deploy the same operating systems across the Automation Anywhere Robot Process Automation (RPA) development, testing, and production environments. At minimum, have the exact same OS on both test and production environments.

Deployment models

At a high-level, there are three (3) ways to install Automation Anywhere, each depends on your business continuity requirements.

Single-Node deployment
: A single-node deployment is used for some proof-of-concept deployments.

High Availability deployment model
: The High Availability (HA) deployment model provides failure tolerance for the Enterprise Control Room servers, services, and databases.

Related concepts
High Availability overview

Single-Node deployment

A single-node deployment is used for some proof-of-concept deployments.

A single-node Enterprise Control Room installation is deployed without the need of a load balancer. It is useful for some proof-of-concept deployments.

CAUTION: Do not use single-node installation for production workloads.

Pros

- Easy to setup and configure
- Only a single server required

Cons

- No disaster recovery
- No high availability
- Susceptible to hardware failures

Use Cases

- Proof of concept
- Single-user use scenarios

High Availability overview

High Availability (HA) provides a failover solution in the event a Enterprise Control Room service, server, or database fails.

Automation Anywhere HA and DR solution

In the context of Automation Anywhere, implementation of High Availability (HA) reduces downtime and maintains continuity of business (CoB) for your bot activities.

- High Availability (HA)—refers to a system or component that is continuously operational for a desirably long period.

HA is required for production deployments of Automation Anywhere.

Automation Anywhere leverages your existing HA infrastructure. We do not provide an internal HA solution. Rather the Automation Anywhere components and configuration leverage your existing HA infrastructure, load balancing, and failover systems to protect your bots and related data. See your data center administrator for your approved local HA procedures.

Required HA and DR infrastructure elements

- Distributed Approach—Enterprise Control Room is flexible enough to process a large number of requests. Deploy multiple instances of Enterprise Control Room on multiple physical or virtual servers as needed.
- Load balancing—Performed by a load balancer, this is the process of distributing application or network traffic across multiple servers to protect service activities and allows workloads to be distributed among multiple servers. This ensures bot activity continues on clustered servers.

  For load balancer configuration details, see Load balancer requirements.
- Databases—Databases use their own built-in failover to protect the data. This ensures database data recovery.
  - Between the HA clusters, configure synchronous replication between the primary (active) and secondary (passive) clustered MS SQL servers in the data center. This ensures consistency in the event of a database node failure.

    For the required HA synchronous replication, configure one of the following:
    - Backup replica to Synchronous-Commit mode of SQL Server Always On availability groups
    - SQL to Server Database Mirroring

Sample scenario

Point all Enterprise Control Room instances within the same cluster to the same database and repository files. This is required to enable sharing data across multiple servers.

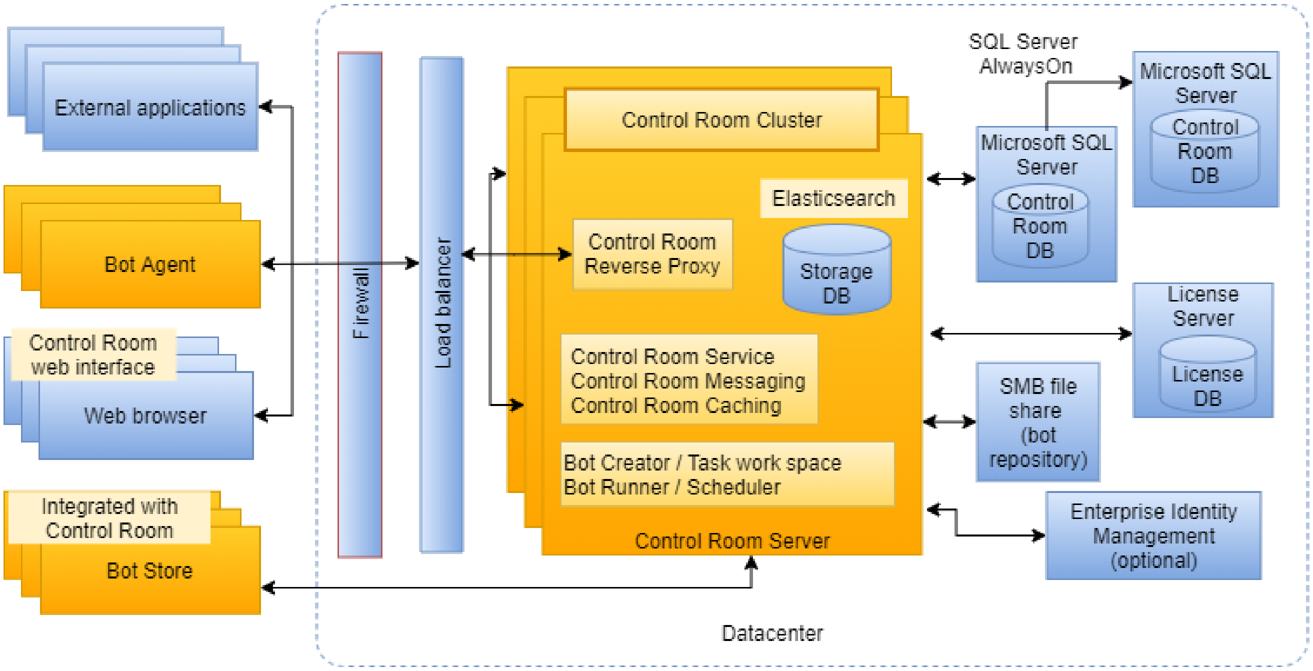
HA deployment model

To ensure your Automation Anywhere is protected by HA, configure your data centers according to the deployment models described in: High Availability deployment model

High Availability deployment model

The High Availability (HA) deployment model provides failure tolerance for the Enterprise Control Room servers, services, and databases.

The following shows the Automation Anywhere and data center components.



In this example, the Enterprise Control Room servers and Microsoft SQL Servers have HA redundancy.

- Multiple users have access the Enterprise Control Room cluster through their web browsers. The web browsers communicate to the Enterprise Control Room cluster through the load balancer.
- Multiple Bot Runners communicate to the Enterprise Control Room cluster through the load balancer.
- The server message block (SMB) file share and the Microsoft SQL Server store data from the Enterprise Control Room cluster.
- Microsoft SQL Server uses redundancy through replication syncing to the clustered Microsoft SQL Server.

Pros

Maintains availability when server failures occur within a single data center.

Cons

Does not provide protection against data center outage.

Use Cases

Small to medium-size businesses that do not require multi-site disaster recovery.

HA cluster configuration overview

To support Automation Anywhere in your data center, configure an HA cluster. Follow your company methods and procedures for implementing your data center cluster.

HA clusters protect services and data in the event of a server or service failure. The following is a list of processes associated with clusters.

- Database replication—Configure synchronous replication between the primary site (active) and secondary site (passive) MS SQL servers to ensure consistency in the event of a database node failure.
- Downtime—The amount of downtime depends on the number of restart attempts the administrator configures for the primary server services, the number of failovers allowed per number of hours, and the failback configuration.
- Failback—After the primary server is returned to normal, the workload can be failed back from the secondary servers to the primary servers. The primary server becomes the active server again.

  Restoring operations to the primary system or site after a failover or disaster recovery on a secondary system or site.

- Failover—If one of the primary servers fails, the workload of the failed server automatically shifts to the secondary server in the cluster. This automatic process is called failover. Failover ensures continuous availability of applications and data. When failover completes, the secondary server becomes the active server.

  When a (primary) system detects a fault or failure, it automatically transfers control to a (secondary) duplicate system. This applies to HA clusters, where failover is from one server to another.

- Graceful degradation—Process allowing cluster dependencies to operate gracefully on a degraded primary site.
- Redundancy—HA clusters use redundancy to prevent single points of failure (SPOF), such as a failed server or service. HA clusters include primary (active) servers that host services or databases and secondary (passive) servers that host replicated copies of the services and databases.
- Replication—The secondary servers have the same configuration and software as the primary servers, they are a duplicate (redundant copy) of the primary. Data is replicated (copied) from the primary servers to the secondary servers.

To support HA and DR for Automation Anywhere, configure the selected components in your data center for HA.

- Cluster components—A cluster is a set servers (nodes) that are connected by physical cables and software. In an HA environment, these clusters of servers are allowed to be in the same physical data center.
  Note: In the context of clusters, though the terms server, host, and node each have specific meaning, they are frequently used interchangeably.
  - Cluster group (role)—Group of clustered services that failover together and are dependent on each other.
  - Host—The cluster machine that is hosting the services.
  - Node—A generic term for a machine in a cluster.
  - Primary node—The active node in the cluster. The machine where the production activities run.
  - Secondary node—The machine that is designated as the target in the event of a failover. The secondary node is a passive duplicate of the primary node.
  - Server—The machine in the cluster installed with the server operating system.

HA cluster technologies guard against three specific types of failures:

- Application and service failures—affecting application software and essential services.
- Site failures in multisite organizations—caused by natural disasters, power outages, or connectivity outages.

- System and hardware failures—affecting hardware components such as CPUs, drives, memory, network adapters, and power supplies.

This ability to handle failure allows clusters to meet two requirements that are typical in most data center environments:

- High availability—the ability to provide end users with access to a service for a high percentage of time and reduces unscheduled outages.
- High reliability—the ability to reduce the frequency of system failure.

Enterprise A2019 On-Premises Enterprise Control Room installation

Review the installation core tasks and topics for installing A2019 Enterprise Control Room in a data center on an On-Premises server or a cloud service provider server instance.

The Enterprise Control Room provides centralized management for digital workforce. Interface for Bot Insight. It is deployed on a server in a data center. The installer executable, `Automation_Anywhere_Enterprise_<version_build>.exe`, is included in the `Automation_Anywhere_Setup.zip` file download.

Note: Linux is not supported for Cloud-enabled On-Premises installations.

Enterprise Control Room installation core tasks

Step 1: Pre-installation

Enterprise A2019 On-Premises prerequisites
: Determine whether the system has the required hardware and software to install Enterprise Control Room for A2019 On-Premises deployment.

Step 2: Installation

The Enterprise Control Room installer allows you to select installation modes (Express or Custom), and during the installation process, it also installs missing software dependencies.

Use Custom mode to install on a cloud-based platform such as Amazon Web Services.

Installing Enterprise Control Room using Express mode
: Login to the servers as an Administrator and install Automation Anywhere Enterprise Control Room in Express Mode using the default settings.

Installing Enterprise Control Room using Custom mode
: Login to the server as Administrator, and install Automation Anywhere Enterprise Control Room in Custom Mode to select installation and configuration options, including installing non-default requirements. Select this mode for a data center deployment.

Installing Enterprise Control Room on Linux
: You start installing the Automation Anywhere Enterprise Control Room in the Linux environment and complete the installation in the Enterprise Control Room.

Installing Enterprise Control Room using scripts

Silent Enterprise Control Room installation, also known as unattended installation, uses a customized Powershell script for a full setup or the command line for a hot fix patch. Silent install runs the entire installation process in the background without requiring user interaction or displaying messages.

Step 3: Post-installation

Configuring post installation settings

After you finish installing the Enterprise Control Room, configure the following items to ensure timely Automation Anywhere communications.

Verifying Automation Anywhere services

Automation Anywhere specific Services are installed on the Enterprise Control Room server.

Step 4: Validation

Configure Enterprise Control Room authentication options

The options for launching the Enterprise Control Room for the first time depend on the installation mode and, for Custom mode installation, the authentication method.

Install a license

A Enterprise Control Room Admin or a user with license management permission can install a license, and evaluate the latest version.

Installing Enterprise Control Room using Express mode

Login to the servers as an Administrator and install Automation Anywhere Enterprise Control Room in Express Mode using the default settings.

Prerequisites

- Verify Enterprise A2019 On-Premises prerequisites.
- Ensure that you have:
  - Automation Anywhere Enterprise Control Room installation file
  - SSL certificate
  - License file

The Express Mode installation quickly sets up the Enterprise Control Room with default parameters for the various components. This installation mode is ideal for showcasing a demo and training purpose. This installation mode is not recommended for the production environment.

Default Parameters

Microsoft SQL Server is the default database for Enterprise Control Room. .

The following parameters are installed by default:

Parameter	Default value
SQL database instance	SQLEXPRESS
Authentication type	Windows authentication

Parameter	Default value
Enterprise Control Room database	AAE-Database
Port	1433

To install Automation Anywhere Enterprise Control Room in Express Mode, follow these steps:

Procedure

1. Login to the installation server.
2. Start the installer wizard.
   a) Extract all files from the AutomationAnywhere_Setup.zip file.
   b) Right-click the AutomationAnywhere`.exe` file and select Run as administrator.
   For example: `AAE_MSSQL_Express_2014SP1.exe`
   The installation process creates the SQLEXPRESS instance that is used for the Enterprise Control Room and the Bot Insight databases. The installation process uses this instance to create a database with the name AAE-Database and configures the database as the default Enterprise Control Room database.
   The installation process checks for supported operating system and for minimum hardware requirements and shows the following message if the requirements are not met:
   ```
   This system does not meet all the installation prerequisites for Automation A
   nywhere Enterprise.
   Some features might not work as expected after installation. For details, ver
   ify the Control Room Installation Prerequisite.
   ```
   For more information, see Enterprise A2019 On-Premises prerequisites.
3. Click Next on the Welcome to the Setup Wizard page.
   The installation process checks the availability of the following components:
   - Microsoft Visual C++ 2013 Redistributable Package
   - Microsoft OLEDB Driver for SQL Server
   If any of the above components is not available, the system notifies you with an installation pop-up window. When both components are successfully installed, the License Agreement page appears.
4. Accept the licensing agreement and click Next.
   The Installation Type page appears.
5. Select the Express option and click Next.
   The Database Configuration page appears.
   a) Type the port you want to use to connect to the database server in the Port field.

   The default port is 1433. The installer uses the first available port and checks the availability of each consecutive port.

   b) Optionally, select the Use Windows Authentication option to use windows authentication to connect to the database server. The system disables the Username and Password fields.
   c) Optionally, select the Sql Server authentication option to use SQL server authentication to connect to the database server. Type the Username and Password to be used to connect to the database server.
   Note: The user who connects to the database server must have database creator privileges.
   d) Type the name of the database that you want to use for Enterprise Control Room in the Name of Control Room database field.
   e) Type name of the database you want to use for Bot Insight in the Name of Bot Insight databasefield.
6. Click Next.

   The Ready to Install the Program page appears.

7. Click Install and allow the installation process to complete.
   The InstallShield Wizard Completed page appears.
8. Click Finish.
   Launch Automation Anywhere is enabled by default.
   Enable Show installer settings to open the aae-installsummary.html file. By default, this is located at C:\Program Files\Automation Anywhere\Enterprise\. Use this file to view a summary of the installation.

Next steps

The Enterprise Control Room launches in your default browser with the Configure Enterprise Control Room settings page displayed. Proceed to Enterprise Control Room post-installation configuration .
Related concepts
Installing Enterprise Control Room using Custom mode

Installing Enterprise Control Room using Custom mode

Login to the server as Administrator, and install Automation Anywhere Enterprise Control Room in Custom Mode to select installation and configuration options, including installing non-default requirements. Select this mode for a data center deployment.

Step 1: Prepare for installation.

- Verify Enterprise A2019 On-Premises prerequisites.
- Ensure that you have:
  - Automation Anywhere Enterprise Control Room installation file
  - SSL certificate
  - License file

Step 2: Run Enterprise Control Room installer
: Run the installer to verify operating system and hardware requirements, accept the licensing agreement, and select the installation file path.

Step 3: Configure IP cluster
: Continue from the Enterprise Control Room installer to the Cluster Configuration wizard page. Use this page to setup the system IP addresses for configuring the Enterprise Control Room on single or multiple nodes (High Availability).

Step 4: Configure application Transport Layer Security
: Continue from the Enterprise Control Room installer to the Transport Layer Security (TLS) configuration wizard page. Use this configuration page to generate a self signed certificate on HTTP or import a security certificate to setup a highly secure Enterprise Control Room instance.

Step 5: Configure service credentials
: Continue from the Enterprise Control Room installer to the Service Credentials wizard page. Use the Service Credentials page to specify the account that will be used to run all Windows services that are created by Automation Anywhere installer.

Step 6: Configure database type and server
: Continue from the Enterprise Control Room installer to the Database type wizard page. Use the Database type page to configure the Microsoft SQL Server database for use with the Enterprise Control Room .

Step 7: Review the installation summary
: Continue from the Enterprise Control Room installer to the Ready to Install the Program wizard page. From this stage of the installation wizard, you finish the installation wizard and monitor the installation progress.

Step 8: Complete Enterprise Control Room configuration and validation

Enterprise Control Room post-installation configuration

After installing the Enterprise Control Room, complete the configuration settings to ensure timely Automation Anywhere communications are specified and confirm Automation Anywhere services are running.

Post-installation user management

After completing the post-installation tasks, validate the setup by logging in to the Enterprise Control Room and installing a license. First time access to the Enterprise Control Room walks you through the configuration for your authentication method.

Step 9: Prepare for users

Users management

As a Cloud user with administrator permissions, you can create, view, edit, delete, enable or disable a user. Creating users steps vary depending if the user is a non-Active Directory, Active Directory, or an Single Sign On user from an IdP server.

Related concepts

Understanding Enterprise A2019 migration

Run Enterprise Control Room installer

Run the installer to verify operating system and hardware requirements, accept the licensing agreement, and select the installation file path.

To install Automation Anywhere Enterprise Control Room in Custom Mode, follow these steps.

Procedure

1. Start the installer wizard.
   a) Extract all files from the AutomationAnywhere_Setup.zip file.
   b) Right-click the AutomationAnywhere`.exe` file and select Run as administrator.
   For example: `AAE_MSSQL_Express_2014SP1.exe`
   The installation process creates the SQLEXPRESS instance that is used for the Enterprise Control Room and the Bot Insight databases. The installation process uses this instance to create a database with the name AAE-Database and configures the database as the default Enterprise Control Room database.
   The installation process checks for supported operating system and for minimum hardware requirements and shows the following message if the requirements are not met:
   ```
   This system does not meet all the installation prerequisites for Automation A
   nywhere Enterprise.
   Some features might not work as expected after installation. For details, ver
   ify the Control Room Installation Prerequisite.
   ```
   For more information, see Enterprise A2019 On-Premises prerequisites.
2. Accept the licensing agreement and click Next.
   The Installation Type page appears.
3. Select the Custom option and click Next.
   The Destination Folder page appears. By default, the destination folder is C:\Program Files\Automation Anywhere\Enterprise\.
4. To make changes to the destination folder, click Change..., supply new destination folder name, and click OK.
   Note: It is NOT recommended to install the application directly in the root directory (C:\). You should create a folder, for example C:\Program Files\Automation Anywhere\Enterprise\.

5. Click Next to configure the IP cluster.

Configure IP cluster

Continue from the Enterprise Control Room installer to the Cluster Configuration wizard page. Use this page to setup the system IP addresses for configuring the Enterprise Control Room on single or multiple nodes (High Availability).

Prerequisites

Ensure that all nodes to be configured for IP Cluster are available for configuration in advance of installation. Also, provide the same list of IP addresses in all the nodes participating in the cluster when you install Enterprise Control Room in these nodes.

To configure the system IP addresses, do the following.

Procedure

1. Enable Cluster Setup.
   The check box is enabled by default if the machine on which the setup is being run has local IP addresses configured.
   To install the Enterprise Control Room without a cluster, disable the Enable Cluster Setup field.
2. Enter the IP addresses of the nodes for the cluster.

   a) Use a comma (,) to specify more than one IP address. For example, 192.161.1.1, 192.161.1.2, 192.161.1.3.

   If you supply invalid numbers or characters, an error message displays.

   b) After you correctly input the cluster IP addresses, a pop-up message prompts you to select a valid IP address that gives network access to this machine.
   c) Select the IP address from the Local IP Address drop-down list.

   If multiple local IP addresses are configured on the machine, select the IP address on which the Enterprise Control Room is installed because it will be used to access the Enterprise Control Room from other nodes.
3. Click Next to configure the application Transport Layer Security (TLS).

Related tasks
Configure application Transport Layer Security

Configure application Transport Layer Security

Continue from the Enterprise Control Room installer to the Transport Layer Security (TLS) configuration wizard page. Use this configuration page to generate a self signed certificate on HTTP or import a security certificate to setup a highly secure Enterprise Control Room instance.

Procedure

1. The TLS Configuration page allows you to configure the following:
   - Generate a Self-Signed Certificate

Enabling the Self-Signed Certificate option allows the installer to generate a unique private key and a self-signed certificate for the Enterprise Control Room.

- Import a Certificate

  To import a custom certificate, disable the Self Signed Certificate checkbox. This configuration allows you to import a certificate using the Certificate Path field.

  Note: The certificate file must be a PKCS12 format.
  Provide the following information:

  - Certificate Path: Click the Browse button to import the certificate.
  - Private Key Password: Type the password for the private key.

    Warning: Password Limitation: Do not use "@" in passwords. Using the special character "@" in the password causes the certificate file import to fail.
  - Webserver Port: Type the Web server port – either HTTP or HTTPS. If the port is already assigned, an error message displays.
    Attention: The port validation message is also displayed when you add 8080 for Web server and if that port is already in use for a Enterprise Control Room license service. Use a different unassigned port in the above cases.
  - Enable Force HTTP traffic to HTTPS: This option redirects all HTTP port requests to HTTPS. To access to the Enterprise Control Room via HTTPS using the generated self-signed certificate, ensure the port numbers are different for HTTP and HTTPS.
    To generate a custom certificate for HTTPS, ensure your custom certificate meets the following:
    - Create a `.pfx` certificate with a pass code from a CA trusted authority.
    - Combined Root, Intermediate and Machine level certificates into a single certificate.
    - Use the format: `[WS Machine Host Name].[DomainName].com` for the private key.
    - Include the host name as a fully qualified domain name (FQDN) in the certificate. You provide the host name during Enterprise Control Room installation.
    - In multi-node HA clusters, issue certificates to the Load Balancer DNS name.
    - Add individual URLs, that require access to all nodes, to the Subject Alternative Name field in the certificate.

2. Click Next to Configure service credentials.

Configure service credentials

Continue from the Enterprise Control Room installer to the Service Credentials wizard page. Use the Service Credentials page to specify the account that will be used to run all Windows services that are created by Automation Anywhere installer.

Procedure

1. The Service Credentials screen displays where you can choose from the listed options.

   The Windows Service credentials include a user name and password. The user specified must meet these requirements:

   - A member of the local system administrator group.
   - Have permission to manage services, including Automation Anywhere services.

These service credentials are used to create database tables and allow the Enterprise Control Room processes to access the database and repository.

- Local System Account—(default) The logged on user performing the installation.
- Domain Account—Specify a user that is not the local system account user.
  a) Uncheck the Local System Account check box.
  b) Enter the user name and password for the domain account.

  Reasons and requirements for using a domain account user include:

  - Do not use the Windows domain credentials

    Enter credentials valid for running Automation Anywhere services. Without the valid credentials, the Enterprise Control Room will fail to launch.

  - PowerShell script restrictions

    Specify a user with permissions to launch PowerShell scripts who is not a Windows domain user. Without the relevant permissions, database table creation can fail.

2. Click Next to configure the database types and server.

Configure database type and server

Continue from the Enterprise Control Room installer to the Database type wizard page. Use the Database type page to configure the Microsoft SQL Server database for use with the Enterprise Control Room .

Procedure

1. Select the Microsoft SQL Server database.
   An instance of SQL Server should be already configured.
2. Click Next.

   The Database Server page displays (only if you selected SQL Server for configuring your database.

3. Set connection and authentication for the database server.
   Note:
   - If possible, do not set the value for Database Server as `localhost`. If you must use `localhost`, understand that the Secure Connection to the database will not work.
   - Click the Browse button to select the SQL server instance where the Enterprise Control Room database will be created. Alternately, type a database server name or select one from the list.

     (Migration task) If you are migrating from 11.x to A2019, browse to the restored 11.x database.

   Provide the following details:

   Database Port
   	Use the default port (1433) or specify a custom value.
   Use Secure Connection
   	Select Use Secure Connection to use CA certificate as specified.
   	Note: Use the same host name for certificate and database connections.

Certificate

This option is enabled when you select secure connection. Browse to select a CA certificate. See Import HTTPS and CA certificates for details on how to import this certificate using the command line.

Windows authentication

This option is selected by default and allows for connecting to the SQL Server using Windows authentication.

Note: If you select Windows Authentication, then the user running the installer is used to test that the database exists, create it if necessary, and grant `db_owner` to the service account user (NT Authority/ System).

SQL Server authentication

Select this option to use SQL server Authentication to connect to the database. Provide the correct user name and password for SQL Authentication.

Name of Enterprise Control Room database

Enter the name for the Enterprise Control Room database.

4. Click Next to complete the Enterprise Control Room installation process and optionally see the Setup installation summary page.

Setup installation summary

Continue from the Enterprise Control Room installer to the Ready to Install the Program wizard page. From this stage of the installation wizard, you finish the installation wizard and monitor the installation progress.

Procedure

1. Click Next.

   The Ready to Install the Program screen appears.

2. Click Install and allow the installation process to complete.
   The InstallShield Wizard Completed screen appears.
3. Click Finish.
   Launch Automation Anywhere is enabled by default.
   Enable Show installer settings to open the aae-installsummary.html file. By default, this is located at C:\Program Files\Automation Anywhere\Enterprise\. Use this file to view a summary of the installation.

Next steps

Complete Enterprise Control Room configuration and validation.

Enterprise Control Room post-installation configuration

After installing the Enterprise Control Room, complete the configuration settings to ensure timely Automation Anywhere communications are specified and confirm Automation Anywhere services are running.

Post-installation user management

After completing the post-installation tasks, validate the setup by logging in to the Enterprise Control Room and installing a license. First time access to the Enterprise Control Room walks you through the configuration for your authentication method.

Users management

As a Cloud user with administrator permissions, you can create, view, edit, delete, enable or disable a user. Creating users steps vary depending if the user is a non-Active Directory, Active Directory, or an Single Sign On user from an IdP server.

Related tasks

Installing Enterprise Control Room using Express mode

Custom Enterprise Control Room configuration

After completing the installation in Custom Mode, configure the Enterprise Control Room in Custom Mode to authenticate users with either an Active Directory (AD), Enterprise Control Room database, or Single Sign-On.

Choose from the following authentication types for detailed configuration steps:

Installing Enterprise Control Room on Amazon Web Services

Login to an Amazon Web Services (AWS) server instance as Administrator. Then download and start the Enterprise Control Room installer and select Custom mode.

Note: There are many possible system configurations and requirements. These installation steps do not account for all those posibilities so your specific setup and installation steps will vary and Automation Anywhere does not make any warranties that these steps conform with your specific configurations.

Step 1: Prepare for installation

- Verify Enterprise A2019 On-Premises prerequisites.
- Ensure that you have:
  - Automation Anywhere Enterprise Control Room installation file
  - SSL certificate
  - License file

Step 2: Prepare for installation on Amazon Web Services

Use these steps to prepare the Amazon Web Services (AWS) instances for the Enterprise Control Room installation.

Step 3: Customize Enterprise Control Room installation on Amazon Web Services

Install and apply the customized configuration required for the Enterprise Control Room cluster on Amazon Web Services (AWS) after completing initial preparations.

Step 4: Complete Enterprise Control Room configuration and validation.

Enterprise Control Room post-installation configuration

After installing the Enterprise Control Room, complete the configuration settings to ensure timely Automation Anywhere communications are specified and confirm Automation Anywhere services are running.

Post-installation user management

After completing the post-installation tasks, validate the setup by logging in to the Enterprise Control Room and installing a license. First time access to the Enterprise Control Room walks you through the configuration for your authentication method.

Step 5: Prepare for users.

Users management
: As a Cloud user with administrator permissions, you can create, view, edit, delete, enable or disable a user. Creating users steps vary depending if the user is a non-Active Directory, Active Directory, or an Single Sign On user from an IdP server.

Prepare for installation on Amazon Web Services

Use these steps to prepare the Amazon Web Services (AWS) instances for the Enterprise Control Room installation.

Prerequisites

If you have not done so already, prepare your AWS Identity and Access Management (IAM) user account to login to the AWS Console.

Do the following:

1. Create AWS Elastic Compute Cloud (EC2) Instances for the Enterprise Control Room Servers.
2. If you use RDS, create Relational Database Service (RDS) Instances for the SQL Server Enterprise 2014 Database server.
3. Configure the AWS Load Balancer.

Note: There are many possible system configurations and requirements. These installation steps do not account for all those posibilities so your specific setup and installation steps will vary and Automation Anywhere does not make any warranties that these steps conform with your specific configurations.
To prepare AWS instances, do the following:

Procedure

1. Set up the on Amazon Web Services Elastic Compute Cloud (AWS EC2) or Relational Database Service (RDS). AAE supports both. For a comparison of the two, see Microsoft SQL Server on AWS.
2. Test the database connection with the Microsoft SQL Server.

    a) Install Microsoft SQL Management Studio on one of the AWS EC2 instances inside the Virtual Private Cloud (VPC).

    For more information, see Download SQL Server Management Studio.

    b) Connect to the Microsoft SQL Server.

    For configuration information, see Working with SQL Servers.

    c) (Skip this step if the master database user installs the Enterprise Control Room). Create the following empty database and assign `db_owner` privileges to the master database user for the AAE-Database database.
3. Set up the shared repository.

    a) Create an AWS EC2 instance as a Windows File Server with an additional volume of 100 GB.
    b) Join the Active Directory domain.
    c) Create a folder and set up the permissions for the repository.
    Assign the Enterprise Control Room admin full access to this folder.

Attention: Only the Enterprise Control Room admin is to have full access to this folder because this is the account from which all Enterprise Control Room services run.

4. Launch two AWS instances, one for each Enterprise Control Room server.

   a) Establish two AWS instances, each with the following configuration:

   - b) Type: c5.2xlarge or similar instance type (8 CPU, 16 GB RAM)
   - c) Storage: Root Device: 100 GB
   - d) Storage: Additional Device: D:\ 200 GB (For Automation Anywhere Install files)
   - e) Accidental Deletion Prevention: Enabled

   f) Access the two instances through Remote Desktop Protocol.

   g) Add the instances to the Active Directory domain.

   h) For each instance, add the Enterprise Control Room system admin as a local administrator on the computer and reboot the system.
5. Configure the firewall and port.
   See Ports, protocols, and firewall requirements.
6. Set up the AWS Application Load Balancer.
   See Details for Elastic Load Balancing Products.
   - Disable the stickiness attribute.
   - Set the idle time-out to 120 seconds.
7. Upload the SSL certificate to the Load Balancer.

Next steps

Continue with Customize Enterprise Control Room installation on Amazon Web Services.

Customize Enterprise Control Room installation on Amazon Web Services

Install and apply the customized configuration required for the Enterprise Control Room cluster on Amazon Web Services (AWS) after completing initial preparations.

Prerequisites

If you have not done so already, complete the initial installation steps in Prepare for installation on Amazon Web Services.

Note: There are many possible system configurations and requirements. These installation steps do not account for all those posibilities so your specific setup and installation steps will vary and Automation Anywhere does not make any warranties that these steps conform with your specific configurations.

To install the Enterprise Control Room in a cluster setup, do the following steps:

Procedure

1. Login to the first AWS instance as an Administrator.
2. Download `Automation Anywhere_<version>.exe`.
3. Click Next on the Welcome to the Setup Wizard page.
   The installation process checks the availability of the following components:
   - Microsoft Visual C++ 2013 Redistributable Package
   - Microsoft OLEDB Driver for SQL Server

   If any of the above components is not available, the system notifies you with an installation pop-up window. When both components are successfully installed, the License Agreement page appears.
4. Accept the licensing agreement and click Next.
   The Installation Type page appears.
5. Select the Custom option and click Next.

The Destination Folder page appears. By default, the destination folder is C:\Program Files\Automation Anywhere\Enterprise\.

6. To make changes to the destination folder, click Change..., supply new destination folder name, and click OK.
   Note: It is NOT recommended to install the application directly in the root directory (C:\). You should create a folder, for example C:\Program Files\Automation Anywhere\Enterprise\.
7. Click Next to configure the IP cluster.
8. Enable Cluster Setup.
   The check box is enabled by default if the machine on which the setup is being run has local IP addresses configured.
   To install the Enterprise Control Room without a cluster, disable the Enable Cluster Setup field.
9. Enter the IP addresses of the nodes for the cluster.

   a) Use a comma (,) to specify more than one IP address. For example, 192.161.1.1, 192.161.1.2, 192.161.1.3.

   If you supply invalid numbers or characters, an error message displays.

   b) After you correctly input the cluster IP addresses, a pop-up message prompts you to select a valid IP address that gives network access to this machine.
   c) Select the IP address from the Local IP Address drop-down list.

   If multiple local IP addresses are configured on the machine, select the IP address on which the Enterprise Control Room is installed because it will be used to access the Enterprise Control Room from other nodes.

10. Click Next to configure the application Transport Layer Security (TLS).
11. The TLS Configuration page allows you to configure the following:
    - Generate a Self-Signed Certificate

      Enabling the Self-Signed Certificate option allows the installer to generate a unique private key and a self-signed certificate for the Enterprise Control Room.

    - Import a Certificate

      To import a custom certificate, disable the Self Signed Certificate checkbox. This configuration allows you to import a certificate using the Certificate Path field.

      Note: The certificate file must be a PKCS12 format.
      Provide the following information:

      - Certificate Path: Click the Browse button to import the certificate.

      - Private Key Password: Type the password for the private key.

        Warning: Password Limitation: Do not use "@" in passwords. Using the special character "@" in the password causes the certificate file import to fail.
      - Webserver Port: Type the Web server port – either HTTP or HTTPS. If the port is already assigned, an error message displays.
        Attention: The port validation message is also displayed when you add 8080 for Web server and if that port is already in use for a Enterprise Control Room license service. Use a different unassigned port in the above cases.
      - Enable Force HTTP traffic to HTTPS: This option redirects all HTTP port requests to HTTPS. To access to the Enterprise Control Room via HTTPS using the generated self-signed certificate, ensure the port numbers are different for HTTP and HTTPS.
        To generate a custom certificate for HTTPS, ensure your custom certificate meets the following:

- Create a `.pfx` certificate with a pass code from a CA trusted authority.
- Combined Root, Intermediate and Machine level certificates into a single certificate.
- Use the format: `[WS Machine Host Name].[DomainName].com` for the private key.
- Include the host name as a fully qualified domain name (FQDN) in the certificate. You provide the host name during Enterprise Control Room installation.
- In multi-node HA clusters, issue certificates to the Load Balancer DNS name.
- Add individual URLs, that require access to all nodes, to the Subject Alternative Name field in the certificate.

12. Click Next to configure the service credentials.
13. The Service Credentials screen displays where you can choose from the listed options.

    The Windows Service credentials include a user name and password. The user specified must meet these requirements:

    - A member of the local system administrator group.
    - Have permission to manage services, including Automation Anywhere services.

    These service credentials are used to create database tables and allow the Enterprise Control Room processes to access the database and repository.

    - Local System Account—(default) The logged on user performing the installation.
    - Domain Account—Specify a user that is not the local system account user.
      a) Uncheck the Local System Account check box.
      b) Enter the user name and password for the domain account.

      Reasons and requirements for using a domain account user include:

      - Do not use the Windows domain credentials

        Enter credentials valid for running Automation Anywhere services. Without the valid credentials, the Enterprise Control Room will fail to launch.

      - PowerShell script restrictions

        Specify a user with permissions to launch PowerShell scripts who is not a Windows domain user. Without the relevant permissions, database table creation can fail.

14. Add the SQL Server and click Next.
    Select Microsoft SQL Server, type the Name, and click Next.
15. Click Finish.
    Launch Automation Anywhere is enabled by default.
    Enable Show installer settings to open the aae-installsummary.html file. By default, this is located at C:\Program Files\Automation Anywhere\Enterprise\. Use this file to view a summary of the installation.

Next steps

The Enterprise Control Room launches in your default browser with the Configure Enterprise Control Room settings page shown. Continue with Configure settings post-installation on Amazon Web Services.

Configure settings post-installation on Amazon Web Services

After installation is complete, configure Enterprise Control Room settings on Amazon Web Services.

Prerequisites

If you have not done so already, complete the installation steps in Customize Enterprise Control Room installation on Amazon Web Services.

Note: There are many possible system configurations and requirements. These installation steps do not account for all those posibilities so your specific setup and installation steps will vary and Automation Anywhere does not make any warranties that these steps conform with your specific configurations.

To install Automation Anywhere on Amazon Web Services (AWS), do the following steps:

Procedure

1. Configure the following Enterprise Control Room settings:

   a) Specify the host name URL by providing the AWS Load Balancer URL.

   This is the URL that users use to access your installation of Enterprise Control Room.

   b) Select the Active Directory authentication type. For more information, see Configure Enterprise Control Room for Active Directory: manual mode.
2. After you configure the Enterprise Control Room, install product licenses. For installation instructions, see Install a license.
3. Test Enterprise Control Room access using the AWS Load Balancer URL.
   This completes the Enterprise Control Room installation on AWS.

Next steps

Complete Enterprise Control Room configuration and validation.

Enterprise Control Room post-installation configuration

After installing the Enterprise Control Room, complete the configuration settings to ensure timely Automation Anywhere communications are specified and confirm Automation Anywhere services are running.

Post-installation user management

After completing the post-installation tasks, validate the setup by logging in to the Enterprise Control Room and installing a license. First time access to the Enterprise Control Room walks you through the configuration for your authentication method.

Users management

As a Cloud user with administrator permissions, you can create, view, edit, delete, enable or disable a user. Creating users steps vary depending if the user is a non-Active Directory, Active Directory, or an Single Sign On user from an IdP server.

Installing Enterprise Control Room on Microsoft Azure

Installing Enterprise Control Room on Microsoft Azure begins in the Azure environment and ends with configurations in the Enterprise Control Room.

Note: There are many possible system configurations and requirements. These installation steps do not account for all those posibilities so your specific setup and installation steps will vary and Automation Anywhere does not make any warranties that these steps conform with your specific configurations.

Step 1: Prepare for installation.

- Verify Enterprise A2019 On-Premises prerequisites.
- Ensure that you have:
  - Automation Anywhere Enterprise Control Room installation file
  - SSL certificate
  - License file

Step 2: Verify readiness for installation on Microsoft Azure
Use these steps to configure third-party products for the Enterprise Control Room installation.
Step 3: Begin Enterprise Control Room installation on Microsoft Azure
Initial steps for Enterprise Control Room installation on Microsoft Azure.
Step 4: Customize Enterprise Control Room installation on Microsoft Azure
Install and apply the customized configuration required for the Enterprise Control Room cluster on Microsoft Azure.
Step 5: Complete Enterprise Control Room configuration and validation.

Enterprise Control Room post-installation configuration
After installing the Enterprise Control Room, complete the configuration settings to ensure timely Automation Anywhere communications are specified and confirm Automation Anywhere services are running.
Post-installation user management
After completing the post-installation tasks, validate the setup by logging in to the Enterprise Control Room and installing a license. First time access to the Enterprise Control Room walks you through the configuration for your authentication method.

Step 6: Prepare for users.

Users management
As a Cloud user with administrator permissions, you can create, view, edit, delete, enable or disable a user. Creating users steps vary depending if the user is a non-Active Directory, Active Directory, or an Single Sign On user from an IdP server.

Verify readiness for installation on Microsoft Azure

Use these steps to configure third-party products for the Enterprise Control Room installation.

Note: There are many possible system configurations and requirements. These installation steps do not account for all those posibilities so your specific setup and installation steps will vary and Automation Anywhere does not make any warranties that these steps conform with your specific configurations.
To configure third-party products prior to installation, do the following steps:

Procedure

1. Ensure the installation environment meets the data center requirements and collect the necessary information about the following components:

   - Load balancer - IP address

   - Microsoft SQL Server - port credentials

- Azure SMB file share - address credentials
- Enterprise identity management system (optional)

  If you have Active Directory (AD) - AD server domain credentials
- SMTP - host port HTTP/S ports for TLS (optional)
- Enterprise Control Room servers - Have Windows credential manager installed

Refer to Supported data center component versions on Microsoft Azure for configuration and version information.

2. Configure the Network Security Group as per the recommended security policies for Inbound Port rules:

Data center object	Port	Protocol
Enterprise Control Room	80, 443	Any
Azure Active Directory	53, 389	Any
LDAP	3268, 3269	Any
email SMTP	587	Any
SSH	22	Any
RDP	3389	TCP

3. Configure the AD server.
   Ensure all users are part of the AD domain and the AD server is setup in IaaS mode for Azure cluster environment installations. To add user, navigate to Active Directory Users and Computers > <domain> > Users and add the necessary user.
   To configure the AD server on Azure with IDaaS, refer to the Microsoft Azure documentation.
4. Ensure the Enterprise Control Room servers in the cluster can ping each other.

   If the ping is not successful:

   a) Enable the following below file and printer sharing firewall rule:

   ```
   File and Printer Sharing (Echo Request - ICMPv4-In) File and Printer
   Sharing All Yes Allow No Any Any Any ICMPv4
   ```

   b) Ping the Enterprise Control Room after enabling the firewall rule change.

Next steps

When you have completed the pre-installation configurations, Begin Enterprise Control Room installation on Microsoft Azure.

Supported data center component versions on Microsoft Azure

The supported operating system versions for installing Automation Anywhere A2019 on the Microsoft Azure cluster environment are identified for each component.

Data center object	Version	Configuration
Enterprise Control Room operating system	Windows 2016	IaaS
Identity management: Azure	Azure Active Directory	IDaaS Windows 2016 for IaaS
	Azure File Share	PaaS
	Azure Load Balancer (Not Application Gateway)	PaaS
	Azure SQL Database (Microsoft SQL Azure (RTM) - 12.0.2000.8)	PaaS

Begin Enterprise Control Room installation on Microsoft Azure

Initial steps for Enterprise Control Room installation on Microsoft Azure.

Prerequisites

If you have not done so already, complete the pre-installation configuration in Verify readiness for installation on Microsoft Azure.

Note: There are many possible system configurations and requirements. These installation steps do not account for all those posibilities so your specific setup and installation steps will vary and Automation Anywhere does not make any warranties that these steps conform with your specific configurations.
To begin the installation:

Procedure

1. Use Remote Desktop Connection (RDC) to connect to the Enterprise Control Room server, as an Administrator, and run the Enterprise Control Room installer.
2. Click Yes to start the installer.
3. Click Next on the Welcome to the Setup Wizard page.
   The installation process checks the availability of the following components:
   - Microsoft Visual C++ 2013 Redistributable Package

- Microsoft OLEDB Driver for SQL Server

If any of the above components is not available, the system notifies you with an installation pop-up window. When both components are successfully installed, the License Agreement page appears.

4. Accept the licensing agreement and click Next.
   The Installation Type page appears.
5. Select the Custom option and click Next.
6. Click Next to setup the system IPs.
   The Cluster Configuration window displays.

Next steps

Continue with Customize Enterprise Control Room installation on Microsoft Azure.

Customize Enterprise Control Room installation on Microsoft Azure

Install and apply the customized configuration required for the Enterprise Control Room cluster on Microsoft Azure.

Prerequisites

If you have not done so already, complete the initial installation steps in Begin Enterprise Control Room installation on Microsoft Azure. This task requires the configuration information you gathered in the prerequisites stage. This includes IP addresses, certificates, and credentials for the the Enterprise Control Room servers, datacenter servers, and databases.

Note: There are many possible system configurations and requirements. These installation steps do not account for all those posibilities so your specific setup and installation steps will vary and Automation Anywhere does not make any warranties that these steps conform with your specific configurations.
To install the Enterprise Control Room in a cluster setup, do the following steps:

Procedure

1. Enable Cluster Setup.
   The check box is enabled by default if the machine on which the setup is being run has local IP addresses configured.
   To install the Enterprise Control Room without a cluster, disable the Enable Cluster Setup field.
2. Enter the IP addresses of the nodes for the cluster.

   a) Use a comma (,) to specify more than one IP address. For example, 192.161.1.1, 192.161.1.2, 192.161.1.3.

   If you supply invalid numbers or characters, an error message displays.

   b) After you correctly input the cluster IP addresses, a pop-up message prompts you to select a valid IP address that gives network access to this machine.
   c) Select the IP address from the Local IP Address drop-down list.

   If multiple local IP addresses are configured on the machine, select the IP address on which the Enterprise Control Room is installed because it will be used to access the Enterprise Control Room from other nodes.

3. Click Next to configure the application Transport Layer Security (TLS).
4. The TLS Configuration page allows you to configure the following:
   - Generate a Self-Signed Certificate

Enabling the Self-Signed Certificate option allows the installer to generate a unique private key and a self-signed certificate for the Enterprise Control Room.

- Import a Certificate

  To import a custom certificate, disable the Self Signed Certificate checkbox. This configuration allows you to import a certificate using the Certificate Path field.

  Note: The certificate file must be a PKCS12 format.
  Provide the following information:

  - Certificate Path: Click the Browse button to import the certificate.
  - Private Key Password: Type the password for the private key.

    Warning: Password Limitation: Do not use "@" in passwords. Using the special character "@" in the password causes the certificate file import to fail.
  - Webserver Port: Type the Web server port – either HTTP or HTTPS. If the port is already assigned, an error message displays.
    Attention: The port validation message is also displayed when you add 8080 for Web server and if that port is already in use for a Enterprise Control Room license service. Use a different unassigned port in the above cases.
  - Enable Force HTTP traffic to HTTPS: This option redirects all HTTP port requests to HTTPS. To access to the Enterprise Control Room via HTTPS using the generated self-signed certificate, ensure the port numbers are different for HTTP and HTTPS.
    To generate a custom certificate for HTTPS, ensure your custom certificate meets the following:
    - Create a `.pfx` certificate with a pass code from a CA trusted authority.
    - Combined Root, Intermediate and Machine level certificates into a single certificate.
    - Use the format: `[WS Machine Host Name].[DomainName].com` for the private key.
    - Include the host name as a fully qualified domain name (FQDN) in the certificate. You provide the host name during Enterprise Control Room installation.
    - In multi-node HA clusters, issue certificates to the Load Balancer DNS name.
    - Add individual URLs, that require access to all nodes, to the Subject Alternative Name field in the certificate.

5. Click Next to configure the service credentials.
6. The Service Credentials screen displays where you can choose from the listed options.

   The Windows Service credentials include a user name and password. The user specified must meet these requirements:

   - A member of the local system administrator group.
   - Have permission to manage services, including Automation Anywhere services.

   These service credentials are used to create database tables and allow the Enterprise Control Room processes to access the database and repository.

   - Local System Account—(default) The logged on user performing the installation.
   - Domain Account—Specify a user that is not the local system account user.
     a) Uncheck the Local System Account check box.
     b) Enter the user name and password for the domain account.

     Reasons and requirements for using a domain account user include:

- Do not use the Windows domain credentials

  Enter credentials valid for running Automation Anywhere services. Without the valid credentials, the Enterprise Control Room will fail to launch.

- PowerShell script restrictions

  Specify a user with permissions to launch PowerShell scripts who is not a Windows domain user. Without the relevant permissions, database table creation can fail.

7. Click Next to configure database type and server.
8. Set connection and authentication for the database server.
   Note:
   - If possible, do not set the value for Database Server as `localhost`. If you must use `localhost`, understand that the Secure Connection to the database will not work.
   - Click the Browse button to select the SQL server instance where the Enterprise Control Room database will be created. Alternately, type a database server name or select one from the list.

     (Migration task) If you are migrating from 11.x to A2019, browse to the restored 11.x database.

   Provide the following details:

   Database Port

   Use the default port (1433) or specify a custom value.

   Use Secure Connection

   Select Use Secure Connection to use CA certificate as specified.
   Note: Use the same host name for certificate and database connections.

   Certificate

   This option is enabled when you select secure connection. Browse to select a CA certificate. See Import HTTPS and CA certificates for details on how to import this certificate using the command line.

   Windows authentication

   This option is selected by default and allows for connecting to the SQL Server using Windows authentication.
   Note: If you select Windows Authentication, then the user running the installer is used to test that the database exists, create it if necessary, and grant `db_owner` to the service account user (NT Authority/System).

   SQL Server authentication

   Select this option to use SQL server Authentication to connect to the database. Provide the correct user name and password for SQL Authentication.

   Name of Enterprise Control Room database

   Enter the name for the Enterprise Control Room database.

9. Click Next.

   The Ready to Install the Program page appears.

10. Click Install and allow the installation process to complete.
    The InstallShield Wizard Completed page appears.
11. Click Finish.
    Launch Automation Anywhere is enabled by default.

Enable Show installer settings to open the aae-installsummary.html file. By default, this is located at C:\Program Files\Automation Anywhere\Enterprise\. Use this file to view a summary of the installation.

Next steps

The Enterprise Control Room launches in your default browser with the Configure Enterprise Control Room settings page shown. Continue with Configure settings post-installation on Microsoft Azure.

Configure settings post-installation on Microsoft Azure

After Enterprise Control Room installation is complete, use the Microsoft Azure Portal to configure the clusters. Use the Azure Portal to configure Windows credentials, Enterprise Control Room settings for repository and URL, master key for Credential Vault, Active Directory authentication, and optionally SMTP settings.

Prerequisites

If you have not done so already, complete the installation steps in Customize Enterprise Control Room installation on Microsoft Azure.
Note: There are many possible system configurations and requirements. These installation steps do not account for all those posibilities so your specific setup and installation steps will vary and Automation Anywhere does not make any warranties that these steps conform with your specific configurations.

Procedure

1. From the Azure Portal where SMB File Share is setup, get the Connection String to retrieve following parameters:
   - Internet or network address
   - User name
   - Password
2. Locate the Window Credential Manager on the control room server and click Add a Windows Credential.
3. Enter the credential information.
   Note: Adding a user under Windows Credential Manager needs to be repeated on all the servers used for testing in the cluster environment (Enterprise Control Room, Clients/Devices).
4. Enter information and click Save and Continue.

   Repository path is extracted from SMB File Share and Enterprise Control Room access URL in is a load balancer Public IP.

5. Copy the Master Key and save it (it will be needed to restart the services).
6. Select Express mode and click Save and Continue.
7. Enter the Active Directory authentication configuration information, including URL, Domain username, and password, then click Check Connection. If settings are correct, click Next.
8. Enter the AD user created previously and click Check name in Active Directory. Upon validation, click Save and Log in.
   Create additional users as needed and create corresponding users in the Enterprise Control Room.
9. Optional: Continue with installing other control room nodes in the cluster.
10. Perform the SMTP registration.
    Note: A real SSL certificate is recommended for use with deployments.

    This completes the Enterprise Control Room installation on Microsoft Azure.

Next steps

Complete Enterprise Control Room configuration and validation.

Enterprise Control Room post-installation configuration
After installing the Enterprise Control Room, complete the configuration settings to ensure timely Automation Anywhere communications are specified and confirm Automation Anywhere services are running.

Post-installation user management
After completing the post-installation tasks, validate the setup by logging in to the Enterprise Control Room and installing a license. First time access to the Enterprise Control Room walks you through the configuration for your authentication method.

Users management
As a Cloud user with administrator permissions, you can create, view, edit, delete, enable or disable a user. Creating users steps vary depending if the user is a non-Active Directory, Active Directory, or an Single Sign On user from an IdP server.

Installing Enterprise Control Room on Linux

You start installing the Automation Anywhere Enterprise Control Room in the Linux environment and complete the installation in the Enterprise Control Room.

Note: The installation steps do not list any specific configurations or requirements and therefore your setup might be different. Automation Anywhere does not provide any warranties that the installation steps conform with your system configurations or requirements.

This task is run from the Linux OS command line.

This task applies to first time installation and Enterprise A2019 On-Premises updates.

Prerequisites

Ensure the following:

- The Microsoft SQL Server database is installed and running.

  The Microsoft SQL Server database can be installed on either a Windows server or a Linux server.

- The Enterprise A2019 installation server is connected to the Microsoft SQL Server database.

Procedure

1. Verify the installation prerequisites.
   a) Verify the Enterprise A2019 On-Premises prerequisites.
   b) Have the following files available:
      - c) SSL certificate
      - d) License file

   e) Go to the Apeople downloads site, Automation Anywhere Downloads, and download the AutomationAnywhereEnterprise_A2019_<linux-version>_<build>.bin installation file to the Linux server.

f) Verify if the Microsoft SQL Server is running, and execute the command:

```
$ sudo systemctl status mssql-server
```

If Microsoft SQL Server is not running, install it. Quickstart: Install SQL Server

2. Log in to the installation server.
3. Run the installer command as a superuser:

   a)

   ```
   $ sudo chmod a + x
                               AutomationAnywhereEnterprise_A2019_<linux
   -version>_<build>.bin
   ```

   b)

   ```
   $ sudo
                               ./AutomationAnywhereEnterprise_A2019_<lin
   ux-version>_<build>.bin
   ```

   The installation wizard verifies the installation requirements and proceeds with the installation.

   Tip:

   - Enter the
     ```
     back
     ```
     command to return to a previous command step.
   - Press the return key to accept default values, or enter an alternate value and then press the return key.
4. To accept the license agreement, enter
   ```
   Y
   ```
   .

   The installation wizard continues with the installation.
5. In the Transport Layer Security (TLS) screen, configure the following:

   a) `Control Room HTTP Port (Default: 80)`

   b) `Control Room HTTPS Port (Default: 443)`

   c) To enable the `Self Signed Certificate`, enter
   ```
   1
   ```
   or enter
   ```
   2
   ```
   to disable it.

   d) To `Force HTTP Traffic to HTTPS`, enter
   ```
   1
   ```
   to disable it or enter
   ```
   2
   ```
   to enable it.

   Configure application Transport Layer Security
6. In the Cluster Configuration screen, enter
   ```
   1
   ```
   to disable it or enter
   ```
   2
   ```
   to enable it.
   - If you choose to enable cluster configuration, enter the IP addresses of the cluster nodes. Use a comma (,) to specify more than one IP address. Do not add space between IP addresses. For example:
     ```
     192.161.1.1,192.161.1.2
     ```
   - If multiple local IP addresses are configured on the machine, select the IP address on which the Enterprise Control Room is installed.

   Configure IP cluster
7. In the Database Configuration screen, configure the following:

   a) `Database Server address (default: localhost)`

   b) `Database port (default: 1433)`
   c) `Control Room Database (default:AAE-Database)` or enter a name.
   d) `SQL Server Login credentials`: provide the login ID and SQL Server password.

   Configure database type and server
8. Review the pre-installation summary.
9. Press Enter to install the Automation Anywhere Enterprise in the default directory: `/opt/automationanywhere/enterprise`

   A message appears stating the installation is successfully completed.
10. Configure the post-installation settings.

    Configuring post installation settings
11. Validate the installation.

    Configure Enterprise Control Room authentication options
12. Install a license.

    Install a license

Next steps

After the Enterprise Control Room installation and configuration is complete, users can register their devices to create and run bots.

Register device and install Bot agent

Related reference
Enterprise A2019 On-Premises Enterprise Control Room installation

Installing Enterprise Control Room using scripts

Silent Enterprise Control Room installation, also known as unattended installation, uses a customized Powershell script for a full setup or the command line for a hot fix patch. Silent install runs the entire installation process in the background without requiring user interaction or displaying messages.

Prerequisites

- Verify Enterprise A2019 On-Premises prerequisites.
- Ensure that you have:
  - Automation Anywhere Enterprise Control Room installation file
  - SSL certificate
  - License file

Create a Powershell script. Refer to the installation parameters and sample scripts. Run the script in Powershell.

Procedure

1. Review the parameters and identify the settings you require.

Enterprise Control Room installation parameters	
Variable Name	Description
AA_CRCLUSTERCONFIG	if AA_SETCLUSTERMODE=1 then cluster IP comma separated
AA_CRDBPORT	Enterprise Control Room database port. Default value is 1433
AA_CRDBSSLMODE	Secure SQL Connection
AA_CRFORCEHTTPSCONFIG=" "	-
AA_CRFORCETOHTTPS="1"	Force traefik from HTTP to HTTPS
AA_CRHTTPPORT	CR HTTP port. Default is 5432
AA_CRHTTPSPORT	CR HTTPS port
AA_CRLISTENPORT	Web server port. Default value is 80
AA_CRSERVICECONFIRMPASSWD	if AA_CRSETLOCALSERVICECRED= 0 then confirm password
AA_CRSERVICEPASSWD	if AA_CRSETLOCALSERVICECRED= 0 then password
AA_CRSERVICEUSERNAME	if AA_CRSETLOCALSERVICECRED= 0 then domain \user name
AA_CRSETLOCALSERVICECRED	1 if service logon as System 0 if service logon as specific user

Enterprise Control Room installation parameters	
Variable Name	Description
AA_CRWCCERTPASSWD	Certificate password
AA_CRWCCERTPATH	Certificate path

AA_SDSFEATURE	true=Cloud deployment type
	false=OnPremises deployment type

AA_SETCLUSTERMODE	For cluster set 1 else 0
AA_SETUPTYPE	Setup type Custom or Express
INSTALLDIR	Installation Directory
IS_SQLSERVER_AUTHENTICATION	0 for Windows authentication
IS_SQLSERVER_DATABASE	SQL Database name
IS_SQLSERVER_SERVER	SQL server name (host name)
Elasticsearch Related Parameters	
AA_ELASTICSEARCHSYSIP	valid IP

2. Option: Edit the sample script to use an Microsoft SQL Server database.
   Use the script to install the Enterprise Control Room with the configuration options available in the installer.
   a) Correct values for variables such as: `$service_username`, `$service_pwd`, `$db_server`, `$cr_port`.
   b) Run the script with a Credentials in Service logon, and a non-secure connection using Microsoft SQL Server authentication with a new database.
   Sample Microsoft SQL Server script.

```
$cr_port=80


$service_username= "domain\username" #e.g."aaspl-brd\archana.patel"
$service_pwd="password"
```

```
#$certpath = "C:\SilentInstall\test256.pfx"
#$certpass = "changeit"

$db_server="localhost"
$cr_db_name="CRDB-NEW-SI-3"
$db_user="sa"
$db_pwd="Admin@123"



$installation_path="C:\Program Files\Automation Anywhere"

#Install latest setup
$static_installation_path="\Enterprise\"""""
$silent_details=" /s ","v""" -join "/"
$installpath_details=
        "/qn INSTALLDIR=\"""

$deployment_details=
        " /AA_SDSFEATURE=true"

$custom_details=
        " /vAA_SETUPTYPE=Custom
        /vAA_CUSTOMMODETYPE=1"

$port_cluster_details=
        " /vAA_SETCLUSTERMODE=0
        /vAA_CRLISTENPORT=$cr_port"

#$service_details=
        " /vAA_CRSETLOCALSERVICECRED=0
        /vAA_CRSERVICEUSERNAME=$service_username
        /vAA_CRSERVICEPASSWD=$service_pwd
        /vAA_CRSERVICECONFIRMPASSWD=$service_pwd"
```

```
$service_details=
        " /vAA_CRSETLOCALSERVICECRED=1"

#$db_details=
        " /vAA_BIMETADATADBTYPE=AA_BIMETADATADBTYPE
        /vIS_SQLSERVER_SERVER=$db_server
        /vIS_SQLSERVER_DATABASE=$cr_db_name
        /vIS_SQLSERVER_DATABASE1=$bi_db_name"

$db_details=
        "
        /vIS_SQLSERVER_SERVER=$db_server
        /vIS_SQLSERVER_USERNAME=$db_user
        /vIS_SQLSERVER_PASSWORD=$db_pwd
        /vIS_SQLSERVER_DATABASE=$cr_db_name
        /vIS_SQLSERVER_AUTHENTICATION=1



$other=
        "
       /vAA_CRWCHTTPPORT=80
        /vAA_CRWCHTTPSPORT=443
        /vAA_CRSELFSIGNCERT=1
        /vAA_OPTIONALCACERT=0
        /vAA_CRWCCERTPATH=$certpath
        /vAA_CRWCCERTPASSWD=$certpass
        /vLAUNCHPROGRAM=1
        /v""
        /LIweamoruc! log.txt"""

$final_commandline = -join($silent_details,
        $installpath_details,$installation_path,
        $static_installation_path,$custom_details,
        $port_cluster_details,$service_details,
        $db_details,$pg_details,$other)
```

```
Write-Host $final_commandline
$a=Get-ChildItem $PSScriptRoot\* -Include *.exe
#$a = "C:\Silent\AutomationAnywhereEnterprise_A2019_<build>.exe"

Write-Host $a
Write-Host "Starting the installation wait for sometime..."

$processdetail=(Start-Process -FilePath
        $a -ArgumentList $final_commandline
         -Wait -PassThru).ExitCode

Write-Host $a.Name execution is done.
If installation is not proper check msi logs in the temp folder.
pause
```

3. Save the script you edit to the server for installation.
4. On the installation server, logged on as an Administrator, open Powershell in admin mode and execute:
   ```
   Set-ExecutionPolicy Unrestricted -Scope CurrentUser
                            -Force
   ```
5. Start Powershell in admin mode and execute:
   ```
   .\install.ps1
   ```
   Note: The silent install logs are stored in the folder from which the install script is executed. For example, if you run the script from C:\Silent Install, the logs are stored in C:\Silent Install folder.

Next steps

Complete Enterprise Control Room configuration and validation.

Enterprise Control Room post-installation configuration
: After installing the Enterprise Control Room, complete the configuration settings to ensure timely Automation Anywhere communications are specified and confirm Automation Anywhere services are running.

Post-installation user management
: After completing the post-installation tasks, validate the setup by logging in to the Enterprise Control Room and installing a license. First time access to the Enterprise Control Room walks you through the configuration for your authentication method.

Users management
: As a Cloud user with administrator permissions, you can create, view, edit, delete, enable or disable a user. Creating users steps vary depending if the user is a non-Active Directory, Active Directory, or an Single Sign On user from an IdP server.

Enterprise Control Room post-installation configuration

After installing the Enterprise Control Room, complete the configuration settings to ensure timely Automation Anywhere communications are specified and confirm Automation Anywhere services are running.

Configuring post installation settings
: After you finish installing the Enterprise Control Room, configure the following items to ensure timely Automation Anywhere communications.

Verifying Automation Anywhere services
: Automation Anywhere specific Services are installed on the Enterprise Control Room server.

Configuring post installation settings

After you finish installing the Enterprise Control Room, configure the following items to ensure timely Automation Anywhere communications.

Post-installation tasks and settings

Exclude Anti-virus
: Exclude anti-virus scans from running in the Automation Anywhere local repository because they interfere with running bots.

Set the Language locale
: Select English (United States) as the Region Setting.
: From Windows, select Control Panel > Region > Administrative > Change system locale.

Set the Region
: Select English (United States) as the Region Format.
: From Windows, select Control Panel > Region > Format.

Set Time synchronization
: Enable Network Time Protocol (NTP) on the Enterprise Control Room. For additional information about setting the NTP, contact your system administrator.

For Microsoft Azure platform installation

Use the Microsoft Azure Portal to configure:

- Windows credentials
- Enterprise Control Room settings for repository, URL, and master key for Credential Vault
- Microsoft Active Directory authentication
- Optionally, SMTP settings.

Related concepts
Enterprise Control Room post-installation configuration
Related reference
Verifying Automation Anywhere services
Working with SQL Servers

Verifying Automation Anywhere services

Automation Anywhere specific Services are installed on the Enterprise Control Room server.

To verify installed Windows services

From your Windows device:

1. Select Control Panel > Administrator Tools > Services.

   The specific path to Services can vary, depending upon your specific Windows version.

2. Scroll through the list to find the listed service name. Note the Status.

Enterprise Control Room services

Verify that the following Windows services are installed by the Automation Anywhere Enterprise Control Room installer.

To verify installed Linux services

1. Log in to the installation server.
2. Run the commands as a superuser.
3. Run the commands to verify the following services:
   - AACRcaching :
     ```
     sudo systemctl status
                                     controlroomcaching.service
     ```
   - AACRreverseproxy :
     ```
     sudo systemctl status
                                     controlroomreverseproxy.service
     ```
   - AACRservice:
     ```
     sudo systemctl status
                                     controlroombackend.service
     ```
   - AAmessaging:
     ```
     sudo systemctl status
                                     controlroommessaging.service
     ```
   - AAelasticsearach:
     ```
     sudo systemctl status
                                     controlroomelasticsearch.service
     ```
   - AAbotcompiler:
     ```
     sudo systemctl status
                                     controlroombotcompiler.service
     ```

Installed services

Service Name	Service Command Line Name	Description
Automation Anywhere Control Room Caching	`AACRcaching`	Used for distributed cache storage.

Service Name	Service Command Line Name	Description
Automation Anywhere Control Room Reverse Proxy	`AACRreverseproxy`	Receives all incoming HTTP and HTTPS requests for Automation Anywhere products and forwards to the correct service.
Automation Anywhere Control Room Service	`AACRservice`	Receives and processes API requests for the Enterprise Control Room.
Automation Anywhere Control Room Messaging	`AAmessaging`	Allows Enterprise Control Room services to communicate asynchronously.
Automation Anywhere Elastic Search Service	`AAelasticsearch`	Stores all logs and related activities for search functionality. Details regarding Elastic search can be found here.

Note: All the services can be configured either in Local System or Domain account when the Enterprise Control Room is installed in Custom mode. For a Enterprise Control Room installed in Express mode, all the services are run in Local System account.
Related concepts
Installing Enterprise Control Room using Custom mode
Related tasks
Installing Enterprise Control Room using Express mode
Installing Enterprise Control Room on Linux

Configure Enterprise Control Room for HTTPS self-signed certificate

Configure Enterprise Enterprise Control Room for HTTPS mode using a self-signed certificate either before or after doing a custom Enterprise Control Room configuration.

To configure Enterprise Control Room for HTTPS mode using a self-signed certificate, do the following steps:

Procedure

1. Double-click the Enterprise Control Room icon.
   The Enterprise Control Room instance launches in Microsoft Internet Explorer.
2. Change the Enterprise Control Room URL setting and port to
   ```
   HTTPS
   ```
   and port number to
   ```
   443
   ```
   .
   The Website Security Warning page launches.
3. Continue to this website to access the Enterprise Control Room.

Next steps

Proceed to Custom Enterprise Control Room configuration. If you have already configured it, then log in to the Enterprise Control Room.
Related tasks
Import HTTPS and CA certificates
Related reference
Custom Enterprise Control Room configuration

Import HTTPS and CA certificates

After installing Enterprise Control Room, import a certificate for HTTPS and/or Certificate Authority (CA) using the Windows/Linux command prompt.

To import a CA or HTTPS certificate for configuring the Enterprise Control Room for secure connection using the command prompt, do the following steps:

Procedure

1. Run the command prompt in administrator mode.
2. Copy the Automation Anywhere installation path.
   The default installation path is C:\Program Files\Automation Anywhere\Enterprise.
3. Type or paste the following at the command prompt:
   - For HTTPS certificate, enter the command:

     ```
     jdk\jre\bin\java -jar certmgr.jar -appDir "C:\Program Files\Automatio
     n Anywhere\Enterprise" -setServerCert "C:\Users\cradmin\Desktop\test_a
     utomationanywhere_com.pfx" -privateKeyPass <PFX Password>
     ```

   - For CA certificate, enter the command:

     ```
     jdk\jre\bin\java -jar certmgr.jar -appDir "C:\Program Files\Automatio
     n Anywhere\Enterprise" -importTrustCert "D:\<user name>\My Downloads\C
     A31.cer"
     ```

4. Add the following parameters to the boot.db.properties file that is located in the config folder, in the Automation Anywhere installation path.

   ```
   root:\Program Files\Automation Anywhere\Enterprise\config
                           trustServerCertificate=false
   ```

Post-installation user management

After completing the post-installation tasks, validate the setup by logging in to the Enterprise Control Room and installing a license. First time access to the Enterprise Control Room walks you through the configuration for your authentication method.

Configure Enterprise Control Room authentication options

The options for launching the Enterprise Control Room for the first time depend on the installation mode and, for Custom mode installation, the authentication method.

Validate services

Validate that the following services are running in automatic mode:

- Automation Anywhere Control Room Caching
- Automation Anywhere Control Room Messaging
- Automation Anywhere Control Room Reverse Proxy
- Automation Anywhere Control Room Service
- Automation Anywhere Elastic Search Service

Install a license

A Enterprise Control Room Admin or a user with license management permission can install a license, and evaluate the latest version.

Users management

As a Cloud user with administrator permissions, you can create, view, edit, delete, enable or disable a user. Creating users steps vary depending if the user is a non-Active Directory, Active Directory, or an Single Sign On user from an IdP server.

Related concepts
Enterprise Control Room post-installation configuration

Configure Enterprise Control Room authentication options

The options for launching the Enterprise Control Room for the first time depend on the installation mode and, for Custom mode installation, the authentication method.

After completing the installation in Custom Mode, configure the Enterprise Control Room in Custom Mode to authenticate users with either an Active Directory (AD), Enterprise Control Room database, or Single Sign-On.
Note: These topics apply to Enterprise A2019, not the Community Edition.
Related tasks
Express Enterprise Control Room configuration
Configure Enterprise Control Room for Active Directory: manual mode
Configure Enterprise Control Room for Active Directory: auto mode
Configure Enterprise Control Room database
Configure Enterprise Control Room for HTTPS self-signed certificate

Express Enterprise Control Room configuration

After completing the installation in Express Mode, configure the Enterprise Control Room in Express Mode using the default settings.

To configure Enterprise Control Room when you start it for the first time, do the following steps:

Procedure

1. Double-click the Automation Anywhere Enterprise Control Room icon on the desktop.
   The Getting Started wizard appears.
2. Fill in the following fields:
   - Username Supply a user name.
   - First name Enter the first name.
   - Last name Enter the last name.
   - Email Supply email address.
   - Password Enter a password.
   - Confirm password Type the password again to confirm.
3. Click Next.
   The Create security questions page appears.
4. Type three security questions and answers.
5. Click Next.
   The Credential settings page appears.
6. Select from the following options:
   - Express mode: The system stores your master key to connect to the Credential Vault. This option is not recommended for a production environment.
   - Manual mode: You store the Master Key on your own, and then provide the Master Key when the Credential Vault is locked. Users use the Master Key to connect to the Credential Vault to secure their credentials and access them when creating and running TaskBots.
     Warning: If you lose the key, you will not be able to access the Enterprise Control Room.
7. Click Save and log in.

   You are logged in to the Enterprise Control Room as an administrator. You can now configure and manage the overall RPA environment with Enterprise Control Room and clients.

Next steps

After configuring the Enterprise Control Room, install product licenses.

Configure Enterprise Control Room for Active Directory: manual mode

Configure the Enterprise Control Room to authenticate users using Active Directory by manually adding the Lightweight Directory Access Protocol (LDAP) URLs.

To configure the Enterprise Control Room when you start it for the first time, do the following:

Procedure

1. Double-click the Automation Anywhere Enterprise Control Room icon on your desktop.

   The Configure Enterprise Control Room settings page appears.

2. Type the repository path.
   This is the location where the uploaded automation files, for example, IQ Bots, and TaskBots are stored. For example, C:\ProgramData\AutomationAnywhere\Server Files.

3. Type the access URL.
   This is the URL for accessing your installation of Enterprise Control Room.
4. Click Save and continue.
   Warning: The back button of your automatically disables after you click Save and continue. This ensures that the Credential Vault Master Key that generates matches the repository path and Enterprise Control Room access URL.

   To return to the Configure Enterprise Control Room settings page, press

   ```
   Ctrl plus
                           F5
   ```

   and restart.

   The Credential Vault settings page appears.
5. Select from the following options:
   - Express mode: The system stores your master key to connect to the Credential Vault. This option is not recommended for a production environment.
   - Manual mode: You store the Master Key on your own, and then provide the Master Key when the Credential Vault is locked. Users use the Master Key to connect to the Credential Vault to secure their credentials and access them when creating and running TaskBots.
     Warning: If you lose the key, you will not be able to access the Enterprise Control Room.
6. Click Save and continue.
   Warning: The back button of the automatically disables after you click Save and continue. No further changes to the Enterprise Control Room configuration or Credential Vault settings are allowed.

   To make changes, reinstall the Enterprise Control Room.

   The Authentication type for Enterprise Control Room users page appears.
7. Select Active Directory.
   Automation Anywhere supports Active Directory Multi-Forest authentication for the Enterprise Control Room. Before providing the Authentication Type, ensure the following:
   - One-way or two-way trust is set up between all forests. For a one-way trust, this is from the Enterprise client forest to the Enterprise Control Room forest (Enterprise Control Room forest must always be the trusting forest).
   - Two-way trust is set up for every domain in a forest.
   - The root certificate of the LDAP server is imported using the provided CertMgr tool via command.
   - The provided LDAP URLs per forest cannot be behind a load balancer. Also, all LDAP URLs must point to the root (main) domain controllers.
   - The node that runs the Enterprise Control Room is in the same domain network where the Active Directory runs.
   - The user is in the parent domain and the URL points to the parent.

     This ensures that when there are two or more forests, and one of the forest has a subdomain with a different name space, a user from the other forests does not have permission to access that subdomain.

8. Type the Global Catalog URL.

   For example, ldap://server01.domain.com.

   For failsafe authentication, click the plus option to provide additional LDAP URLs.

   Note: For users and groups from one or more Active Directory domains, to access the Enterprise Control Room, use a fully qualified host name of the Global Catalog (GC) server, listening on port 3268 (3269 if SSL).

When adding LDAP URLs, ensure that you provide a fully qualified host name like ldap://server01.ldap.com.

Provide URLs of multiple Global Catalogs per forest so that if one Global Catalog in a forest goes down, the other can serve. This feature does not provide support for the load-balanced URL.

You must enter the Domain username and password and click Manually add connections to enter the LDAP URLs.

9. Provide service account credentials

   Ensure that the username provided is a user in the Domain Users group and ideally and be set up in Active Directory with a password never expires option. If otherwise, there will be some downtime in RPA authentication as the service account password is reset. Provide the username in a User Principal Name (UPN) in the username@domain.com format and password.

10. Click Check connection.

    If Enterprise Control Room is unable to connect to the Active Directory database, an error message appears.

11. Click Next.
    The Enterprise Control Room first administrator page appears.
12. Select the Active Directory domain from the drop-down list and type the Enterprise Control Room administrator username.
13. Click Check name in Active Directory.
    If the username is in the Active Directory the following user details are shown:
    - First name
    - Last name
    - Email

    You can edit these prepopulated fields.

14. Click Save and log in.

    You are logged in to the Enterprise Control Room as an administrator. You can now configure and manage the overall RPA environment with Enterprise Control Room and clients.

Next steps

After configuring the Enterprise Control Room, install product licenses.

Related tasks
Configure Enterprise Control Room for Active Directory: auto mode

Configure Enterprise Control Room for Active Directory: auto mode

Configure the Enterprise Control Room to authenticate users using Active Directory by enabling the Enterprise Control Room to discover and list domains and sites in your organization.

To configure the Enterprise Control Room when you start it for the first time, do the following:

Procedure

1. Double-click the Automation Anywhere Enterprise Control Room icon on your desktop.

   The Configure Enterprise Control Room settings page appears.

2. Type the repository path.
   This is the location where the uploaded automation files, for example, IQ Bots, and TaskBots are stored. For example, C:\ProgramData\AutomationAnywhere\Server Files.
3. Type the access URL.
   This is the URL for accessing your installation of Enterprise Control Room.
4. Click Save and continue.
   Warning: The back button of your automatically disables after you click Save and continue. This ensures that the Credential Vault Master Key that generates matches the repository path and Enterprise Control Room access URL.

   To return to the Configure Enterprise Control Room settings page, press

   ```
   Ctrl plus
                               F5
   ```

   and restart.

   The Credential Vault settings page appears.
5. Select from the following options:
   - Express mode: The system stores your master key to connect to the Credential Vault. This option is not recommended for a production environment.
   - Manual mode: You store the Master Key on your own, and then provide the Master Key when the Credential Vault is locked. Users use the Master Key to connect to the Credential Vault to secure their credentials and access them when creating and running TaskBots.
     Warning: If you lose the key, you will not be able to access the Enterprise Control Room.
6. Click Save and continue.
   Warning: The back button of the automatically disables after you click Save and continue. No further changes to the Enterprise Control Room configuration or Credential Vault settings are allowed.

   To make changes, reinstall the Enterprise Control Room.

   The Authentication type for Enterprise Control Room users page appears.
7. Select Active Directory.
   Automation Anywhere supports Active Directory Multi-Forest authentication for the Enterprise Control Room. Before providing the Authentication Type, ensure the following:
   - One-way or two-way trust is set up between all forests. For a one-way trust, this is from the Enterprise client forest to the Enterprise Control Room forest (Enterprise Control Room forest must always be the trusting forest).
   - Two-way trust is set up for every domain in a forest.
   - The root certificate of the LDAP server is imported using the provided CertMgr tool via command.
   - The provided LDAP URLs per forest cannot be behind a load balancer. Also, all LDAP URLs must point to the root (main) domain controllers.
   - The node that runs the Enterprise Control Room is in the same domain network where the Active Directory runs.
   - The user is in the parent domain and the URL points to the parent.

     This ensures that when there are two or more forests, and one of the forest has a subdomain with a different name space, a user from the other forests does not have permission to access that subdomain.

8. Type the Domain username.

   Ensure you use the User Principal Name (UPN) in the username@domain.com format.

   The username you enter is for a user who has access to all domains using the same credentials.

9. Type the Domain password.
   This user is not expected to use the Enterprise Control Room. Although you have an option to update the password, use an Account with the password never expires option. If it expires, it can be updated but with some downtime.
10. Click Discover connections.
    All discovered Active Directory domains with one or more sites per domain are shown.
    By default all domains and sites are selected. If only one domain and one site under it is discovered, then it is shown in read-only mode and cannot be edited.
11. Select the domains and sites to use for authentication.

    Select the domains and sites to use for authentication. Select a minimum of one site for each domain that is selected

12. Click Test connections to register the sites to use for authentication.
13. Click Check connection.

    If Enterprise Control Room is unable to connect to the Active Directory database, an error message appears.

14. Click Next.
    The Enterprise Control Room first administrator page appears.
15. Select the Active Directory domain from the drop-down list and type the Enterprise Control Room administrator username.
16. Click Check name in Active Directory.
    If the username is in the Active Directory the following user details are shown:
    - First name
    - Last name
    - Email

    You can edit these prepopulated fields.

17. Click Save and log in.

    You are logged in to the Enterprise Control Room as an administrator. You can now configure and manage the overall RPA environment with Enterprise Control Room and clients.

Next steps

After configuring the Enterprise Control Room, install product licenses.

Related tasks
Configure Enterprise Control Room for Active Directory: manual mode
Configure Enterprise Control Room database

Configure Enterprise Control Room database

Configure the Enterprise Control Room to authenticate users using the database option.

To configure the Enterprise Control Room when you start it for the first time, do the following:

Procedure

1. Double-click the Automation Anywhere Enterprise Control Room icon on your desktop.

   The Configure Enterprise Control Room settings page appears.

2. Type the repository path.
   This is the location where the uploaded automation files, for example, IQ Bots, and TaskBots are stored. For example, C:\ProgramData\AutomationAnywhere\Server Files.
3. Type the access URL.
   This is the URL for accessing your installation of Enterprise Control Room.
4. Click Save and continue.
   Warning: The back button of your automatically disables after you click Save and continue. This ensures that the Credential Vault Master Key that generates matches the repository path and Enterprise Control Room access URL.

   To return to the Configure Enterprise Control Room settings page, press

   ```
   Ctrl plus
                                  F5
   ```

   and restart.

   The Credential Vault settings page appears.
5. Select from the following options:
   - Express mode: The system stores your master key to connect to the Credential Vault. This option is not recommended for a production environment.
   - Manual mode: You store the Master Key on your own, and then provide the Master Key when the Credential Vault is locked. Users use the Master Key to connect to the Credential Vault to secure their credentials and access them when creating and running TaskBots.
     Warning: If you lose the key, you will not be able to access the Enterprise Control Room.
6. Click Save and continue.
   Warning: The back button of the automatically disables after you click Save and continue. No further changes to the Enterprise Control Room configuration or Credential Vault settings are allowed.

   To make changes, reinstall the Enterprise Control Room.

   The Authentication type for Enterprise Control Room users page appears.
7. Select the Enterprise Control Room database.
8. Click Next.
   The Enterprise Control Room first administrator page appears.
9. Fill in the following fields:
   - Username Supply a user name.
   - First name Enter the first name.
   - Last name Enter the last name.
   - Email Supply email address.
   - Password Enter a password.
   - Confirm password Type the password again to confirm.
10. Click Next.
    The Create security questions page appears.
11. Type three security questions and answers.
12. Click Save and log in.

You are logged in to the Enterprise Control Room as an administrator. You can now configure and manage the overall RPA environment with Enterprise Control Room and clients.

Next steps

Install a license.

Related tasks
Configure Enterprise Control Room for Active Directory: manual mode
Configure Enterprise Control Room for Active Directory: auto mode

Configure Enterprise Control Room for HTTPS self-signed certificate

Configure Enterprise Enterprise Control Room for HTTPS mode using a self-signed certificate either before or after doing a custom Enterprise Control Room configuration.

To configure Enterprise Control Room for HTTPS mode using a self-signed certificate, do the following steps:

Procedure

1. Double-click the Enterprise Control Room icon.
   The Enterprise Control Room instance launches in Microsoft Internet Explorer.
2. Change the Enterprise Control Room URL setting and port to
   ```
   HTTPS
   ```
   and port number to
   ```
   443
   ```
   .
   The Website Security Warning page launches.
3. Continue to this website to access the Enterprise Control Room.

Next steps

Proceed to Custom Enterprise Control Room configuration. If you have already configured it, then log in to the Enterprise Control Room.
Related tasks
Import HTTPS and CA certificates
Related reference
Custom Enterprise Control Room configuration

Import HTTPS and CA certificates

After installing Enterprise Control Room, import a certificate for HTTPS and/or Certificate Authority (CA) using the Windows/Linux command prompt.

To import a CA or HTTPS certificate for configuring the Enterprise Control Room for secure connection using the command prompt, do the following steps:

Procedure

1. Run the command prompt in administrator mode.
2. Copy the Automation Anywhere installation path.
   The default installation path is C:\Program Files\Automation Anywhere\Enterprise.
3. Type or paste the following at the command prompt:
   - For HTTPS certificate, enter the command:

     ```
     jdk\jre\bin\java -jar certmgr.jar -appDir "C:\Program Files\Automatio
     n Anywhere\Enterprise" -setServerCert "C:\Users\cradmin\Desktop\test_a
     utomationanywhere_com.pfx" -privateKeyPass <PFX Password>
     ```

   - For CA certificate, enter the command:

     ```
     jdk\jre\bin\java -jar certmgr.jar -appDir "C:\Program Files\Automatio
     n Anywhere\Enterprise" -importTrustCert "D:\<user name>\My Downloads\C
     A31.cer"
     ```

4. Add the following parameters to the boot.db.properties file that is located in the config folder, in the Automation Anywhere installation path.

   ```
   root:\Program Files\Automation Anywhere\Enterprise\config
                               trustServerCertificate=false
   ```

Preparing for users

After completing initial installation and depending upon your deployment option, the post-installation configuration and validation, you are ready to prepare for users to login and work with bots.

See Users management.

Set up SAML authentication

Switch an authenticated environment Enterprise Control Room database to a SAML identity provider (IDP).

Prerequisites

Sign in to the Enterprise Control Room as an Admin user. The SAML IDP side setup must be validated before configuring the Enterprise Control Room.

To set up the Enterprise Control Room as a service provider in the SAML IDP, follow these steps:

1. Set the ACS or service provider URL to <Enterprise Control Room URL>/v1/authentication/saml/assertion.

2. Create an Entity ID, that is, any name that identifies the Enterprise Control Room on the SAML IDP.
3. Map the following Enterprise Control Room attributes to the corresponding IDP attributes:
   - UserID
   - FirstName
   - LastName
   - EmailAddress
4. Get the service provider metadata, generated as an XML file, from the SAML IDP for the Enterprise Control Room.

   This is required for setup within the Enterprise Control Room.

   Note: You have to add the values from Steps 2 and 4 in the Enterprise Control Room to complete the setup.

Procedure

To switch the Enterprise Control Room to a SAML authenticated environment, follow these steps:

1. Navigate to Administration > Settings.
2. Access User Authentication > Edit.
3. Select the Use SAML option to enter the SAML information.
   Note: The Use Control Room database option is selected by default.
4. In the SAML metadata field, enter the data from the SAML IDP.
5. In the Unique Entity ID for Control Room (Service Provider) field, enter the Entity ID.
6. In the Encrypt SAML Assertions field, select one of the following options:
   - Do not encrypt: the SAML assertions are not encrypted.
   - Encrypt: the SAML assertions are encrypted.
7. Optional: Enter the Public key and Private key values.
   Note: Enter keys if you require encrypted SAML assertions.
8. Click Validate SAML Settings.
   You have to validate your SAML settings before you can save your changes.
   When you click this option, you will be redirected to a SAML service provider web page where you will be prompted to enter credentials and other data. After validation is complete, you will be redirected back to this configuration page.
9. Log in to the page and perform these steps:
   a) Navigate to the Metadata Manager and add the new service provider.
   b) Enter Enterprise Control Room metadata in the required field.
   c) Enter the Entity ID for the Enterprise Control Room service provider.
   d) Select the option to retrieve the user's information such as username, first name, last name, email.
   e) Save the new service provider.
10. Click Save changes.
    After you have successfully saved your settings, you will be logged out of the Automation Anywhere Enterprise Control Room.
11. Log back in to the system with your new credentials.

Edit profile

Manage user profiles.

For users of Enterprise Control Room configured with a non-directory environment, change the password, first name, last name, and email address.

Procedure

1. Click the Device icon and select Update credentials.
2. In the Device login credentials section, enter the Username and Password for the device.
   Device login credentials are required to run a bot from this device.
   Note: Enterprise A2019 does not validate the device login credentials until you run a bot.

   If your username is part of a domain, include the domain within the format `domain\username`. Typically, home users are not part of a domain, unless they are specifically configured.

3. Click Update

Installed Enterprise Control Room directories and files

When installing the Automation Anywhere Enterprise Control Room on different operating systems, the installer executes and installs files and folders in the following directories.

Window OS directory structure

When you install the Automation Anywhere Enterprise Control Room on Windows OS, the default installation directory for many configuration files is located:

```
C:\Program Files\Automation Anywhere\Enterprise\
```

Linux OS directory structure

When you install the Automation Anywhere Enterprise Control Room on Linux OS, the installer creates the following directories.

Directory path	Description	Comments
`/opt/automationanywhere/enterprise`	All binary files	
`/opt/automationanywhere/enterprise/config`	Config files	
`/var/log/automationanywhere/enterprise`	Log files	
`/tmp`	Temporary files	Directory that contains temporary files created by the system and users. Files under this directory are deleted when the system is rebooted.

Directory path	Description	Comments
`/opt/automationanywhere/enterprise/appdata`	Server files	Enterprise Control Room repository folder.
`/opt/automationanywhere/enterprise/_Automation\ Anywhere\ Enterprise_installation/Logs/`	Installer logs	Installation logs provide details about issues during installation, if any.

Licenses

The All Licenses page displays detailed information about current product and device licenses.

Product licenses

The Automation Anywhere Enterprise Control Room is the web-based application at the center of the Digital Workforce providing enterprise-wide management and control. The Enterprise Control Room ensures reliable, scalable, and secure bot deployment and execution. From this central vantage point, operators can receive tasks from the Bot Creator and push to the Bot Runners for execution with simple mouse clicks. The Automation Anywhere Enterprise Control Room monitors and audits all scheduled and running bots, in real time.

The Automation Anywhere Enterprise Control Room provides an automated mechanism for tracking and controlling the use of licensed software across Bot Creators and Bot Runners, addressing NIST Change Management CM-10.

Device licenses

Bot Creator

The Bot Creator license provides the capability to create, schedule, trigger, and edit bots.

Bot Runner

The Bot Runner license provides authorization to execute bots, independently and asynchronously.

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 Automation Anywhere Enterprise Control Room deployment, centralized scheduling, and API-based deployment.

Attended Bot Runner - Run-time license

Users with privilege to run bots on their workstations. These users can also make use of local schedules and triggers for time-based or event-based automation.

IQ Bot A2019

IQ Bot automates business processes that rely on semi-structured or unstructured data. IQ Bot licenses are purchased based on the number of pages of processing required.

Bot Insight

Bot Insight provides real-time, RPA native analytics for both business insights and operational intelligence. Bot Insight Analytics license is purchased on a per user basis.

Entitlement models

Two licensing models are available for Automation Anywhere Enterprise Version A2019:

File-based entitlements

When Version A2019 operates in a file-based entitlement mode:

- A license file is configured, generated, and installed for each Control Room.
- The Control Room administrator can then issue these licenses to specific user accounts.
- Each user consumes a license within a Control Room. If the same user is created in multiple Control Rooms, they will use up a license entitlement for each Automation Anywhere Enterprise Control Room.
- File-based entitlements only supports a floating user license model.

Cloud-based entitlements

Available and accessed from a cloud-based license server. Information exchanged between the Control Room and the license server meet GDPR compliance requirements. If you cannot allow access to an external service, such as the License Service, because of network or security constraints, contact Automation Anywhere support.

- The cloud-based GUID can be installed only if there are no users file licenses in use.
- Administrators can reallocate user licenses after installing the cloud-based GUID.

RBAC on License Management

Access to License Management is deny-all and allow by exception based on roles and domains as defined in RBAC. Only those users who have access to License Management permission can view the entitlement details from the Automation Anywhere Enterprise Control Room.

Baseline inventory controls: Bot Creators, Bot Runners, and Bots

The Automation Anywhere Enterprise Control Room manages all automation operations. Inventory controls are maintained through the application of RBAC to establish a single point of control for Base Line Configurations (NIST CM-2), access restrictions for configuration management (NIST CM-5 and 6). Automated baseline reporting can be configured.

- Licensing and entitlements
  Any new customer who orders Automation Anywhere Enterprise products are to receive license confirmation from Automation Anywhere.
- Installing licenses
  Upload a new license into the Automation Anywhere Enterprise Control Room.
- Configure new Enterprise Control Room licenses
  The Enterprise Control Room in your order now requires configuration to generate and download new licenses.
- Enterprise Control Room Fail-Safe status
  When the Enterprise Control Room is unable to connect to the license server, it moves into Fail-Safe status.
- Installing licenses
  Upload a new license into the Automation Anywhere Enterprise Control Room.
- Enterprise Control Room Fail-Safe status
  When the Enterprise Control Room is unable to connect to the license server, it moves into Fail-Safe status.

Licensing and entitlements

Any new customer who orders Automation Anywhere Enterprise products are to receive license confirmation from Automation Anywhere.

The designated person responsible for configuring licenses for their company receives two email confirmations.

The SSO email from sso@automationanywhere.com grants you access to set up a new password for your Automation Anywhere Single Sign-On (SSO) account. The Orders email from orders@automationanywhere.com grants you access to your license entitlement information.

Do the following:

Procedure

1. Open SSO email → access link.
2. Enter and confirm new password.
3. Access A-People Community.
4. There are two options to access your license entitlements.

Option	Action
A-People	Navigate to LICENSES.
Orders email	Access link to redirect to license page.

   Note: Your license entitlement validation date is provided within the context of the Orders email and on the A-People License configuration page.
5. You now have access to your license entitlements.

   On this page, you have access to more information of your order. The Product Versions shows your current license entitlement version, the License Entitlements shows the number of license entitlements in your order, and the Control Rooms shows the number of control rooms in your order, and allows to configure each licenses.

Installing licenses

Upload a new license into the Automation Anywhere Enterprise Control Room.

Prerequisites

Administrative privileges are required to make changes to the licenses.

Note:

- The cloud-based GUID can be installed only if there are no users file licenses in use.
- Administrators can reallocate user licenses after installing the cloud-based GUID.

Be logged into the Automation Anywhere Enterprise Control Room as the administrator.

Procedure

1. Navigate to Administration > Licenses.
2. Select Install license from server or Install license from file.

Option	Action
Install license from server	a) Release all file based license allocations from users. b) Supply the unique Control Room GUID. c) Click Install license from server.
Install license from file	a) Browse to and select the license. b) Click Install license.

Related reference
Users management
Roles
Settings

Configure new Enterprise Control Room licenses

The Enterprise Control Room in your order now requires configuration to generate and download new licenses.

The numbers of Enterprise Control Rooms are listed in the Control Rooms section. The status of current Enterprise Control Rooms are shown as:

- Available - Enterprise Control Room available for license configuration.
- Draft - Enterprise Control Room license configuration in progress.
- Pending Generation - Enterprise Control Room license generating in progress.
- Active - Enterprise Control Room available to view, download, and reconfigure.

Do the following:

Procedure

1. Navigate to Control Rooms > CR-1.
2. Select CR-1 to configure new Enterprise Control Room license.
   Note: The CR Name, Status, and Version fields are filled depending on your license.
3. Enter a Location value.
4. Select an Enviroment option.
   Note: Depending on your use cases, your options are Production, Environment, or UAT.
5. Enter a number for Bot Runner Attended, Bot Runner Unattended, and Bot Creator.
6. Check Analytics > Bot Insight User (Analytical User) and enter the number of users.
7. Select Save & Generate.
8. Select Yes to confirm and generate new license.
   Note: An email confirmation is sent for your newly generated license. The license page automatically refreshes and the CR-1 status now changes from Available to Pending Generation.
9. Select Refresh, the CR-1 status updates to Active.
10. Select CR-1 to view your generate Enterprise Control Room license information.
11. Select Download.
    Note: The downloaded file is now installable to your development Enterprise Control Room environment.

12. Close CR-1 and repeat process on remaining CR files.

- Reconfigure existing Enterprise Control Room licenses
  The Enterprise Control Room license can be reconfigured and updated at anytime.

Reconfigure existing Enterprise Control Room licenses

The Enterprise Control Room license can be reconfigured and updated at anytime.

In cases where new license entitlements are added or mistakes were made, reconfiguring an existing Enterprise Control Room license is simple.

Do the following:

Procedure

1. Navigate to Control Rooms > CR-1.
2. Select CR-1 to reconfigure existing Enterprise Control Room license.
   Note: The CR Name will vary depending on user.
3. Select Reconfigure.
4. Select Yes to confirm reconfiguration.
5. Select Edit.
6. Update your values.
   Note: The CR-1 status now displays Draft as file is in reconfiguration.
7. Update the Bot Runner Unattended number for newly added license entitlements.
8. Select Save & Generate.
9. Select Yes to confirm edits.
   Note: An email confirmation is sent with a link to access A-People License and to download the generated license. The license page automatically refreshes and the CR-1 status now changes from Draft to Pending Generation.
10. Select Refresh, the CR-1 status updates to Active.
11. Select CR-1 to view your updated Enterprise Control Room license information.
12. Select Download.
    Note: The downloaded file is the most recent Active. The downloaded file is now installable to your development Enterprise Control Room environment.
13. Close CR-1 and repeat process for any CR files needing reconfiguration.
    Note: Administrators with a Cloud Control Room using a file license and wants to change to cloud license can manually disable all user licenses and then proceed to GUID installation, then reassign the user licenses.

Enterprise Control Room Fail-Safe status

When the Enterprise Control Room is unable to connect to the license server, it moves into Fail-Safe status.

With respect to the Enterprise Control Room license server database, the Enterprise Control Room can be in one of three status states. These states indicate what user licensing actions can be done. With each state change, an entry is made in the audit log.

Active
    Normal operations. All API calls from the Enterprise Control Room are accepted by the license server.

Users can be assigned floating licenses as they log on. Floating licenses can be released as users log off.

Fail-Safe

Only the heartbeat API call is allowed to the license server. All other calls from the Enterprise Control Room are stopped.

Operations, such as granting logging in users a license, or deleting a license assigned to a logged in user are restricted.

Fail-Safe-Expired

The Enterprise Control Room stops all operations, all users are logged out of the Enterprise Control Room.

Fail-Safe mode actions

When the Enterprise Control Room loses connection with the licensing server and moves into Fail-Safe mode:

- The Enterprise Control Room administrator is sent an email notification, saying the Enterprise Control Room is in Fail-Safe mode. The administrator can take remedial action to re-establish the connection.
- Currently logged in users continue to have access and can do tasks.
- User licenses cannot be allocated to or de-allocated from users.

Fail-Safe-Expired mode actions

When the Fail-Safe time limit expires, the Enterprise Control Room moves into Fail-Safe-Expired state:

- All connected users are shut down.
- The Enterprise Control Room reports Shutdown status to the license server.
- The Enterprise Control Room shuts down.

Active mode actions

When the Enterprise Control Room is restarted and operational, and connectivity to the license server established, the Enterprise Control Room is in Active state:

- Users who had assigned licenses prior to the Fail-Safe, have their original licenses re-allocated.
- New users can request and be allocated licenses.

Update Enterprise A2019

If you are already using Enterprise A2019 On-Premises, you can update to the latest version of Enterprise A2019. For example, Enterprise A2019 On-Premises Build 3337 to Build 4105.

Prerequisites

Back up your database, repository, and installation configuration files.

If you are upgrading from Automation Anywhere Enterprise version 10.x or 11.x to Enterprise A2019, see Upgrade to Enterprise A2019.

Procedure

1. Log in to Automation Anywhere Support site to download the latest version of the Enterprise A2019 setup file.
   Automation Anywhere Downloads
2. On the Downloads page, click the link to the latest Automation Anywhere Enterprise A2019 setup file.
3. Click Installation Setup, and then click either Linux Setup or Windows Setup based on the operating system of the machine on which you want to install Enterprise A2019.
4. Download the AutomationAnywhereEnterprise_A2019.<file-extension> file.
5. Install the latest version of Enterprise A2019 without uninstalling the current version of Enterprise A2019.
   Enterprise A2019 On-Premises Enterprise Control Room installation
   Important: You must use the SQL database of the current version in the newer version of Enterprise A2019.

Upgrade to Enterprise A2019

Perform the tasks in this work flow to upgrade from Automation Anywhere 10.x or 11.x to Enterprise A2019, including migration of your 11.x and 10.x bots to A2019.

If you are updating an existing Enterprise A2019 On-Premises version, for example, from Enterprise A2019.10 to Enterprise A2019.12, see Update Enterprise A2019.

Procedure

1. Plan your upgrade:
   - Review the 10.x and 11.x versions that are supported for upgrade to Enterprise A2019.

     Understanding Enterprise A2019 migration (certified versions)
   - Compare the Enterprise A2019 and the Automation Anywhere Enterprise 11.x features to understand feature equivalency in A2019.

     Enterprise A2019 feature comparison matrix
   - Use the Bot Scanner to analyze your bots and identify commands and variables used in the bots that are supported for migration in Enterprise A2019.

     Using Bot Scanner
   - Review information about packages mapping and variables mapping to understand how 11.x commands and variables differ from the equivalent A2019 packages and variables.

     Package mapping for migration | Variable mapping for migration
2. Prepare for upgrade:
   - We recommend that you take a backup of the 11.x or 10.x database to avoid failure of any automation task that is using the 11.x or 10.x database.
   - Restore the database you have backed up in the previous step in the same or different SQL instance.
   - For 11.x: Copy and paste the 11.x Enterprise Control Room repository and Credential Vault files.

     Copy and paste 11.x information to A2019

3. Install Enterprise A2019 On-Premises:

    a) Ensure you meet the system requirements.
    Enterprise A2019 On-Premises prerequisites
    b) Install Enterprise A2019 On-Premises Enterprise Control Room in custom mode to a staging environment.
    Installing Enterprise Control Room using Custom mode

    For 11.x only: During the installation, configure the A2019 On-Premises Enterprise Control Room to use the restored 11.x database. For example, if your 11.x database name is CRDB-Version 11.3.2, then point your A2019 Enterprise Control Room to that database. This configuration upgrades the 11.x database to A2019.

    For 10.x only: You must install Enterprise A2019 with a new database.

4. Complete the following pre-migration tasks:

    a) For 11.x only: Update the Enterprise Control Room access URL and repository path.
    b) Create users and roles with the required permissions to migrate bots and data to Enterprise A2019.
    c) Install Bot agent on the device that you want to use for migration.
    To complete the tasks in Steps 4a, 4b, and 4c, see Pre-migration tasks
    d) For 10.x only: Copy the 10.x data to Enterprise A2019.
    Copy 10.x data
5. Migrate the 10.x or 11.x bots to A2019.
    Migrate Enterprise bots
6. Verify the migration is complete:
    - Migration reports
    - Verifying the bot migration
    - Export to CSV

Understanding Enterprise A2019 migration

The migration feature enables you to convert and migrate bots (TaskBots and MetaBots) created using the Enterprise client version 10.x or 11.x to A2019. The migration capability is available in A2019 from Build 2079 onwards for On-Premises deployment. Review information about the certified versions supported for migration.

To give our customers an opportunity to participate and improve the migration process, the product provides early development access to all customers. The first generally available (GA) migration tool will be released in an upcoming release with 100% migration coverage added in a subsequent release. Contact your Customer Success Manager (CSM) for details about the release dates.

The tools provided for migration perform the following functions:

Bot Scanner

Previously called the pre-migration utility, the Bot Scanner scans your existing bots (TaskBots and MetaBots) and generates reports. These reports provide information about the commands and variables used in these bots and how many of these commands and variables are supported for migration in A2019.

A new version of Bot Scanner is released on a monthly basis. You can use the latest version of the Bot Scanner to monitor which commands and variables are supported for migration in A2019 with each update. You can run the tool without installing A2019.

The Bot Scanner is available from the Automation Anywhere Downloads page. See Using Bot Scanner for instructions on using the tool.

Important: You can help improve migration to A2019 by sharing the reports generated by the Bot Scanner. These reports help our engineering team focus on supporting the components that are more frequently used by our customers. No personally identifiable information (PII) is included and you can review the reports before sharing. Contact your Customer Success Manager (CSM) or Partner Enablement Manager (PEM) for more details.

This video demonstrates how to use the Bot Scanner to analyze your bots (TaskBots and MetaBots) and determine whether or not you are ready for migration from Enterprise version 11.x or 10.x to Enterprise A2019.

Migration wizard

This tool is integrated in A2019 Enterprise Control Room and guides you through the process after you have completed the prerequisites steps. The migration wizard enables you to migrate multiple bots (TaskBots and MetaBots) and their dependent bots. The migration wizard migrates a bot only if all of the components used in that bot are supported for migration in A2019. If a bot uses other dependent files such as .txt, .doc, and .png, you have to add these files as dependencies manually after migrating the bots.

This video demonstrates how to migrate 11.x Enterprise bots (TaskBots and MetaBots) in .atmx and .mbot format to .bot format for Enterprise A2019.

Unsupported features for migration

The following 11.x features and functionalities are not yet available for migration with this release:

- Schedules: Schedules created in 11.x are migrated to A2019 as disabled schedules. The migrated schedules point to 11.x bot files without associated Bot Runner devices, which make the migrated schedules unusable. Instructions for reconfiguring these schedules to make them usable in A2019 will be available in a future release.
- Audit log: Audit log migration for versions 11.3.0 and later is currently not supported. They will be available in subsequent releases. Audit log migration is supported for 11.x versions earlier than 11.3.0 and certified for migration.
- Workload management: Queues and work items created in 11.x are not yet available for migration.

The 11.x Bot Runner and Bot Creator devices are not included in the migration process, so are not migrated to A2019. You must install A2019 Bot agent on the relevant devices to replace the Bot Runners. Use the A2019 web-based Bot editor to replace the Bot Creators.

Certified versions

The following 11.x and 10.xbots are supported for migration to A2019:

11.x Versions	10.x Versions
11.3.2.2	10.5.16
11.3.2.1	10.5.11
11.3.2	10.5.5
11.2.1.3	10.3.11

11.x Versions	10.x Versions
11.2.1.2	10.3.9
11.2.1	10.3.5

Related reference
Bot Scanner overview

Bot Scanner overview

The Bot Scanner enables you to analyze the bots (TaskBots and MetaBots) created in Enterprise Control Room 11.x and 10.x and generates reports.

The Bot Scanner enables you to identify if you are ready for migration from version 10.x or 11.x to A2019 or not. If not, the Bot Scanner identifies the reasons why the bots (TaskBots and MetaBots) cannot be migrated.

The Bot Scanner scans the bots (.atmx and .mbot files) at the location you specify and generates a summary report that provides the following information:

- The number of bots scanned
- The number of bots that can and cannot be migrated to A2019.
- The commands and variables that are used in the scanned bots and supported in A2019

It generates the summary report in HTML format and a separate report for each bot in XML format.

The objective of the Bot Scanner is to get information about the Automation Anywhere components used by the customers and accordingly prioritize support for the same in migrating the customer to A2019.

System requirements

Hardware

Processor	2.66 GHz or higher (64-bit)
RAM	1 GB or higher
Disc space	20 MB

Software requirements

Operating systems: Windows 7 or later (32-bit and 64-bit)

Using Bot Scanner

The Bot Scanner enables you to analyze the bots (TaskBots and MetaBots) created in Enterprise Control Room 11.x and 10.x and generates reports.

Procedure

1. Download the latest version of Bot Scanner from the Automation Anywhere Support site.
   a) Open the Automation Anywhere Downloads.
   b) On the Downloads page, click the Automation Anywhere Enterprise A2019 setup file.
   c) Click Installation Setup, and then click AAE Bot Scanner setup file.
2. Extract the files from the zip file you have downloaded.
   The extracted folder contains the following files and folders:
   - jre: Contains Java 11 runtime files.
   - aae-bot-scanner-x.x.x.jar: The Bot Scanner that evaluates the bots.
   - process.txt: Use this file to run the Bot Scanner utility after updating information in the file.
3. Open the process.txt file and update the following values:
   - SOURCE FOLDER: Replace the text with the location of the folder that contains the bots that you want to evaluate.
     Recommendation: Create a copy of the repository folder and provide the location of the copied folder instead of the actual repository folder.
   - OUTPUT FOLDER: Replace the text with the location where you want to save the generated report.

   Note: Ensure that you specify the location of the source folder and output folder in double quotes. For example,
   ```
   java -Dbots-folder="C:\TaskBots" -Doutput-folder="C:\Output Report" -jar
   "%~dp0aae-bot-scanner-2.0.0.jar"
   ```
4. Save the process.txt file as a batch file (process.bat).
5. Open the Microsoft command prompt.
6. Drag the process.bat file into the Microsoft command prompt.
   The utility starts analyzing the bots available at the location you have specified in the process.bat file. After successfully analyzing the bots, the utility creates a summary report and reports for each bot in the output location you have specified.
   Note: If Windows protection is enabled on the machine in which you are using the Bot Scanner, the system displays a notification requesting you to allow the Bot Scanner scripts to be run.
7. After the execution is completed, follow the steps provided in the Microsoft command prompt to open the summary.html file.

Next steps

Analyze reports
Related reference
Bot Scanner overview
Analyze reports

Analyze reports

You can analyze the report generated by the Bot Scanner to get information about the bots (TaskBots and MetaBots) that can be migrated.

The Bot Scanner provides the following key information about the bots:

- Number of bots you have
- Number of bots you can and cannot migrate to A2019
- Commands and variables that are used in the bots
- Frequency of the commands used in your bots
- Percentage of commands used in the bots that are supported for migration in A2019

Important: Automation Anywhere Enterprise A2019 is updated frequently in order to achieve 100% functional equivalency with Automation Anywhere Enterprise 10.x or 11.x. The percentage of commands and variables that are supported for migration in A2019 will increase until it reaches 100% over the next upcoming releases. That is, for every function you do in 10.x or 11.x, an equivalent capability is in A2019.

Most of the 10.x or 11.x features are available as is; however, some features are implemented differently to support client-less (web) operations. For these features, you have to change the way bots are written.

The Bot Scanner is designed to scan bots (TaskBots and MetaBots) created using both 10.x and 11.x versions of Enterprise client. The total file count includes the number of files that were skipped and not scanned.

The reports are available at the output location you specified in the process.bat file. The Bot Scanner generates a summary report and a separate report for each bot that it scanned. It creates a separate report for each logic available in a MetaBot.

A raw-data folder is created that contains the reports (in XML format) for each bot scanned. Our engineers can use these reports for further analysis, if required. No personally identifiable information (PII) is included in the summary report or the individual reports of the scanned bots.

If you choose to share the reports with us to help improve the product, compress the files in the OUTPUT FOLDER and coordinate with your Customer Success Manager (CSM) or Partner Enablement Manager (PEM). No data is automatically shared with Automation Anywhere.

Summary report for all bots

The summary report provides the following information:

- Summary section: Provides information about the total number of bots scanned and the bots supported for migration to A2019 (in percentage). The section also provides information about the commands that are used in the scanned bots and supported for migration in A2019 (in percentage).

  For example, consider the Bot Scanner has scanned 10 bots and the bots use 50 commands. Of the 50 commands, if A2019 supports 45 commands, the commands available in A2019 are 90%.

- Separate tables are included for:
  - List of bots that are supported in A2019.
  - List of bots that are not supported in A2019.
  - List of commands and variables that are supported in A2019.
  - List of commands and variables that are not supported in A2019.

  Frequency of usage is the number of times a command is used in all the bots scanned.

Note: For commands and variables that are currently not supported, support will be added in upcoming releases.

Report for an individual bot

The report for each bot provides information about its dependencies, variables, and commands used.

The individual bot report looks similar to the following code:

```
            <analysis version="1.3.0">
                <stat>
                    <dependencies ucount="0" count="0"/>
                    <errors ucount="6" count="12">
                        <error count="1">System variable $AAApplicationPath$</e
rror>
                        <error count="1">Command [If FolderNotExist]
                        is not supported</error>
                        <error count="3">System variable $CurrentDirectory$</er
ror>
                        <error count="3">System variable $Extension$</error>
                    </errors>
                </stat>
                <commands>
                    <command target-action="assign" name="VariableOperation" li
ne="1"
                    grp="VariableOperation" api="VarOpe">
                        <msg type="error" review="true" category="variable">Sys
tem
                        variable $AAApplicationPath$</msg>
                        <msg type="info" review="false" category="default">Comm
and
                        parameter [Option] of type [String] is not required.</m
sg>
                    </command>
                    <command target-action="createFolder" name="createFolder" l
ine="3"
                    grp="FilesFolders" api="CreateFolder"/>
                    <command target-action="copyFiles" name="CopyFiles" line="5
"
                    grp="FilesFolders" api="CreateFolder"/>
                    <command target-action="connect" name="Connect" line="3"
                    grp="Database" api="Connect"/>
                    <command target-action="OpenCSVTXT" name="ReadFrom" line="9
"
```

```
                    grp="CsvText" api="Csv"
                        <msg tpye="info" review="false" category="command">Lin
e
                        in 11.x client, there is no separate option given for C
SV
                        and TEXT in Enterprise A2019</msg>
                            <msg type="error" review="true" category="variable"
>System
                            variable $CurrentDirectory$</msg>
                            <msg type="error" review="true" category="variable"
>System
                            variable $Extension$</msg>
                            <msg type="error" review="true" category="variable"
>System
                            variable $FileName$</msg>
                        </command>
                    </commands>
                    <variables>
                        <variable name="$CSV-TXT-Default-DATA$"
                        type="TABLE" value-type=""/>
                    </varaibles>
                </analysis>
```

The following table describes the various attributes available in the XML report shown in the previous image:

Node	Attribute	Description
Stat	--	Provides information about the number of dependencies, error, and warnings.
--	dependencies	Specifies the number of dependencies for the bot. The `ucount` indicates the number of unique dependencies and the `count` indicates the total number of dependencies.
--	error	Specifies the number of errors for the bot. The `ucount` indicates the number of unique errors and the `count` indicates the total number of errors.
Command	--	Provides information about the various commands and actions used in the bot.
--	command target-action	Specifies the action being performed for the command.
--	name	Specifies the name of the command.
--	line	Specifies the line number where the command is available in the bot.

Node	Attribute	Description
--	grp	Specifies the command group the command belongs to.
--	api	Specifies the name of the API the command uses.
--	msg type	Provides information about the message type. The `error` type indicates that the command cannot be migrated to A2019, and an `info` type indicates that the command can be migrated but some of its attributes will be changed during migration.
--	review	Provides information about whether the command has to be reviewed. This attribute is always true for `error` type messages, which indicates that migration of that command to A2019 is not yet supported. For `info` type messages, if the attribute is true, you must review the value in the `category` attribute. You can decide whether you want to take any action on the migrated bot based on the value available in the `category` attribute.
--	category	Provides information about the command or variable for which the message is displayed.
Variables		Provides information about the system variables used by the bot.
--	variable name	Specifies the name of the variable.
--	type	Specifies the type of variable.
--	value type	Specifies the type of value provided for that variable.

Package mapping for migration

This page contains support information about 10.x and 11.x commands and how they map to respective Enterprise A2019 actions or packages. In some cases, a 10.x or 11.x command migrates to more than one A2019 action. This is to ensure that the behavior of the migrated bot is unchanged.

A2019 has a new package called Legacy Support. This package provides the additional support needed during migration and includes the following new expression. The Legacy Support package is for use during migration; we do not recommend using this package for new bot development. This package has the following expressions:

- `ParseLegacyKeys` – Ensures that the 11.x key strokes of the 11.x bots stored in variables are successful upon execution. This expression converts them into equivalent A2019 key strokes during the execution.
- `ParseVariableOperation` – Parses the expression provided in the 11.x variable operation command. This exression ensures that A2019 returns the same output as 11.x bots upon execution.

The following are some key behavior differences:

- In A2019, the single dollar sign ($) is reserved for Automation Anywhere Enterprise use, so all user entries of a single dollar sign are automatically replaced with two dollar signs ($$). For example, if you have a text field, "Pay $5.00", we convert that field to read "Pay $$5.00" in A2019 for it to display properly to users.

- For 11.x command using a windows title field configured with a user defined variable, the migration process migrates the bot by adding the Set Title action just above the respective command. A2019 does not allow user variables in the Windows Title field. Use the Set Title action to achieve the same behavior.
- 11.x provides various pre-sets as part of the windows title selection and they are migrated to respective pre-sets in A2019.

11.x Options	A2019 Options
Current Active Window	Current Active Window
Desktop	• For the Insert mouse click command, use the Screen for window title option. • For the Insert keystroke command, use the Current Active Window opition. • For Screen > Capture area, use the Screen for window title option.
Wallpaper	Desktop
Taskbar	Taskbar

- In 11.x, loop indexing of table starts with 1 and increments by 1. A2019 starts indexing with 0 and increments by 1.
- 11.x actions that store the return values to the $Clipboard$ system variable are not supported in A2019. When you migrate bots with this functionality, the migration process assigns the values to a temporary variable and then assigns the value to the A2019 $System:Clipboard$ system variable by adding the Copy To action to the Clipboard package.
- The migration process migrates IF and Loop commands that contain multiple conditions of a variable.
- In 11.x, some String operation commands use Tab, Enter, and Separator special characters. In A2019, these characters are system variables in the String package.

11.x	A2019
[Tab]	$String:Tab$
[Enter]	$String:Enter$
[Separator]	$String:Separator$

  See String package.

- If a command is disabled and is converted into multiple actions during migration, then those actions appear as disabled in A2019.

The following table lists the packages available for migration in this build and how they map to A2019. N/A means there are no changes. A2019.

Package	How it is migrated to A2019	What you n
App Integration	App Integration in A2019 does not have actions for each technology, unlike in 11.x. In A2019, all actions are divided into individual actions. Capture text from All 11.x App Integration commands that capture text from a window is migrated to the App Integration > Capture text from window action in A2019.	N/A – the m process ma automatica

<table>
<tr><th>Package</th><th>How it is migrated to A2019</th><th>What you n</th></tr>
<tr><td>Clipboard</td><td>All commands of Clipboard are migrated to equivalent actions of the A2019 Clipboard package. There is no change in behaviour or command name.
See Clipboard package.</td><td>N/A – the m process ma automatica</td></tr>
<tr><td>Comment</td><td>Comment is migrated to A2019 Comment action.</td><td>N/A – the m process ma automatica</td></tr>
<tr><td>Database</td><td>11.x uses ODBC drivers and A2019 uses JDBC drivers.
The SQL Query action is called Read from in A2019.
The following table shows the commands that currently can be migrated.
<table>
<tr><th>11.x</th><th>A2019</th></tr>
<tr><td>Connect</td><td>Migrates to the Connect command. If you encounter an unsupported connection string in A2019, the reasons might vary based on your environment. More details are available as part of the migration process. Contact Technical Support if you need assistance resolving the issue.</td></tr>
</table>
See Database package.</td><td>N/A – the m process ma automatica</td></tr>
<tr><td>Delay</td><td>Delay command is migrated to the Delay action in A2019. "Delay in Milliseconds" and "Delay in Seconds" options (11.x) have changed to radio options within the Time unit area (A2019). See Delay package.</td><td>N/A – the m process ma automatica</td></tr>
<tr><td>Email</td><td>There is no concept of session for Email commands in 11.x. However, A2019 has Connect and Disconnect actions to make sure email session are started and closed. Hence during migration, the system places the Connect action before the respective email action and the Disconnect action after the respective email action.
The Save attachment option of the Get All Messages command is now a dedicated action called Save attachment in the Email package in A2019.
See Email package.</td><td>N/A – the m process ma automatica</td></tr>
<tr><td>Error Handling</td><td>Begin Error Handling and End Error Handling is migrated to the Try/Catch block of the Error handler package in A2019. Many options available in Begin Error Handling are migrate to respective A2019 actions. Refer the below table for details:
<table>
<tr><th>11.x</th><th>A2019</th></tr>
<tr><td>Continue</td><td>By default, execution continues after executing the Catch block in A2019.</td></tr>
<tr><td>Stop</td><td>Stop action of the Task package is added in the Catch block.</td></tr>
</table></td><td>N/A – the m process ma automatica</td></tr>
</table>

Package	How it is migrated to A2019	What you n
	<table><tr><th>11.x</th><th>A2019</th></tr><tr><td>Take Snapshot</td><td>Capture screen of the Screen package is added in the Catch block in A2019. Additionally, 11.x captures the screen with the error dialog; where as A2019 does not show the error dialog while capturing the screen.</td></tr><tr><td>Run Task</td><td>Run action of the Task package is added in Catch block.</td></tr><tr><td>Log Data into File</td><td>Log to File action is added in Catch block.</td></tr><tr><td>Send Email</td><td>Not yet supported for migration.</td></tr><tr><td>Variable Assignment</td><td>Assign action of the String package is added with respective the condition in the Catch block.</td></tr></table> See Error handler package.	
Excel	The 11.x Excel commands are migrated to respective A2019 actions of the Excel Advanced package. In 11.x, data returned by Get Multiple Cells and Get All Cells commands are returned to the Loop > Each Row in an Excel Dataset command. In A2019, the functionalities of Get Multiple Cell and Get All Cells are available in Loop > Each Row in an Excel Dataset action, so values from these commands are migrated to the loop instead of actual actions. The following table shows action name changes:<table><tr><th>11.x</th><th>A2019</th></tr><tr><td>Save Spreadsheet</td><td>Save workbook</td></tr><tr><td>Open Spreadsheet</td><td>Open</td></tr><tr><td>Close Spreadsheet</td><td>Close</td></tr><tr><td>Get Cells</td><td>Divided into Get single cell and Get multiple cells actions</td></tr><tr><td>Activate Sheet</td><td>Switch to sheet</td></tr><tr><td>Find/Replace</td><td>Divided into Find and Replace actions</td></tr></table> See Excel advanced package.	N/A – the m process ma automatica
File/Folder	All commands of File/Folder have been split into File and Folder packages.	N/A – the m process ma automatica

<table>
<tr><th>Package</th><th>How it is migrated to A2019</th><th>What you n</th></tr>
<tr><td></td><td>The following File related actions have changed in A2019:
<table>
<tr><th>11.x</th><th>A2019</th></tr>
<tr><td>Copy Files</td><td>Copy</td></tr>
<tr><td>Create Files</td><td>Create</td></tr>
<tr><td>Delete Files</td><td>Delete</td></tr>
<tr><td>Open Files</td><td>Open</td></tr>
<tr><td>Print Files</td><td>Print</td></tr>
<tr><td>Rename Files</td><td>Rename</td></tr>
<tr><td>Unzip Files</td><td>Unzip</td></tr>
<tr><td>Zip Files</td><td>Zip</td></tr>
</table>
The following Folder related actions have changed in A2019:
<table>
<tr><th>11.x</th><th>A2019</th></tr>
<tr><td>Copy Folder</td><td>Copy</td></tr>
<tr><td>Create Folder</td><td>Create</td></tr>
<tr><td>Delete Folder</td><td>Delete</td></tr>
<tr><td>Open Folder</td><td>Open</td></tr>
<tr><td>Rename Folder</td><td>Rename</td></tr>
</table>
See File package) and Folder and Folder package.</td><td></td></tr>
<tr><td>FTP/SFTP</td><td>All commands of FTP/SFTP are migrated to equivalent A2019 actions of the FTP/SFTP package. There is no change in behavior or command name.</td><td>N/A – the m
process ma
automatica</td></tr>
<tr><td>If/Else > Variable</td><td>Value type variable containing string
We migrate IF with the following operators as a String condition in A2019:
• =
• < >
• Include
• Does not Include
Value type variable containing number
We migrate IF with the following operators as a Number condition in A2019:
• &gt;=
• &lt;=</td><td>If a conditio
date, under
situation, y
change the
informatior
condition a
migration.</td></tr>
</table>

<table>
<tr><th>Package</th><th>How it is migrated to A2019</th><th>What you n</th></tr>
<tr><td></td><td><ul><li>></li><li><</li></ul>
<p>Value type variable containing date</p>
<p>The system tries to evaluate if a condition on a variable has a date value. If found, it migrates IF with the Datetime condition in A2019. Otherwise, the system migrates it as a string or number condition based on the operator used. In those cases, you must change it to a date condition after the bot migration if a date operation is involved.</p>
<p>Additionally, you might also need to change the date format to one that is compatible with your data. The default format used to convert a date to string is <code>MM/dd/yyyy HH:mm:ss</code>.</p>
<p>See If package.</p></td><td></td></tr>
<tr><td>If/Else (Other conditions)</td><td><p>Refer to the table below to see how various conditons are migrated to the respective A2019 conditions.</p>
<table>
<tr><th>11.x</th><th>A2019</th></tr>
<tr><td>Task Successful or Task Unsuccessful</td><td>Migrated to the equivalent If condition of Task Bot package.</td></tr>
<tr><td>Script Successful or Script Unsuccessful</td><td>Script successful/unsuccessful is migrated to respective the JavaScript or VBScript package based on the script file extension.</td></tr>
<tr><td>Object Properties</td><td>Migrated to the Object condition of the Recorder package.</td></tr>
<tr><td>Application Running or Application Not Running</td><td>Migrated to the equivalent If condition of the Application package.</td></tr>
<tr><td>File Exists, File Does Not Exist, File Date, File Size</td><td>Migrated to the equivalent If condition of the File package.</td></tr>
<tr><td>Folder Exists or Folder Does Not Exist</td><td>Migrated to the equivalent If condition of the Folder package.</td></tr>
<tr><td>Ping Successful Or Ping Unsuccessful</td><td>Migrated to the equivalent If condition of the Ping package.</td></tr>
<tr><td>Web Control Exists or Web Control Does Not Exists</td><td>Migrated to the equivalent If condition of the Legacy Support package.</td></tr>
</table>
<p>Image Recognition</p>
<p>The If command with the Image Recognition condition in 11.x can become one of the following actions in A2019 based on the selected options:</p>
<ul><li>If > Image file is found in image file – Created if Image1 has the "From File" option selected and Image2 has the "From File" option selected 11.x.</li>
<li>If > Image file is found in a window – Created if Image1 has the "From File" option selected and Image2 has the "From Window" option selected 11.x.</li></ul></td><td>N/A – the m
process ma
automatica</td></tr>
</table>

<table>
<tr><th>Package</th><th>How it is migrated to A2019</th><th>What you n</th></tr>
<tr><td></td><td>
<ul>
<li>If &gt; Window is found in image file – Created if Image1 has the "From Window" option selected and Image2 has the "From File" option selected 11.x.</li>
<li>If &gt; Window is found in a window – Created if Image1 has the "From Window" option selected and Image2 has the "From Window" option selected 11.x.</li>
</ul>
See If package.</td><td></td></tr>
<tr><td>Image Recognition</td><td>The Image Recognition command is split into Find file image inside window image and Find window image inside another window image actions in A2019.
In A2019, Advance is the default comparison mode and actions with the Gray-Scale, Normal, or Monochrome option selected are migrated as Advance. The migration process maps the information automatically and does not impact related bots.
Migration of bots with the Image Recognition command might fail if the command is using any file type other then:
<ul>
<li>.jpg</li>
<li>.jpeg</li>
<li>.jpe</li>
<li>.jfif</li>
<li>.bmp</li>
<li>.gif</li>
</ul>
See Image Recognition package.</td><td>N/A – the m process ma automatica</td></tr>
<tr><td>Insert Keystrokes</td><td>This command is called Simulate Keystrokes in A2019.
The following keystroke conventions have changed:
<table>
<tr><th>11.x</th><th>A2019</th></tr>
<tr><td>[PAGE UP]</td><td>[PAGE-UP]</td></tr>
<tr><td>[NUM LOCK]</td><td>[NUM-LOCK]</td></tr>
<tr><td>[SCROLL LOCK]</td><td>[SCROLL-LOCK]</td></tr>
<tr><td>[PAGE DOWN]</td><td>[PAGE-DOWN]</td></tr>
<tr><td>[CAPS LOCK]</td><td>[CAPS-LOCK]</td></tr>
<tr><td>[UP ARROW]</td><td>[UP-ARROW]</td></tr>
<tr><td>[LEFT ARROW]</td><td>[LEFT-ARROW]</td></tr>
<tr><td>[RIGHT CLICK]</td><td>[MENU]</td></tr>
<tr><td>[RIGHT ARROW]</td><td>[RIGHT-ARROW]</td></tr>
<tr><td>[DOWN ARROW]</td><td>[DOWN-ARROW]</td></tr>
<tr><td>[ALT GR DOWN]</td><td>[ALT-GR DOWN]</td></tr>
</table></td><td>N/A – the m process ma automatica</td></tr>
</table>

<table>
<tr><th>Package</th><th>How it is migrated to A2019</th><th>What you n</th></tr>
<tr><td></td><td><table><tr><th>11.x</th><th>A2019</th></tr><tr><td>[ALT GR UP]</td><td>[ALT-GR UP]</td></tr><tr><td>[$]</td><td>[DOLLAR]</td></tr></table>
In 11.x, the delay time is divided by the total characters and applied between each character stroke. In A2019, the delay you specify applies to the time between each keystroke.

See Simulate keystrokes package.</td><td></td></tr>
<tr><td>Launch Website</td><td>This command is migrated to Launch website of the the Browser package in A2019.

Microsoft Edge is not yet supported in the Launch Website action in A2019. Commands with "Edge" or "Override default browser" option unselected in the legacy product is automatically changed to use Default Browser upon migration.

See Browser package.</td><td>N/A – the m
process ma
automatica</td></tr>
<tr><td>Log to File</td><td>This command is migrated to Log to file action in A2019.

See Log To File package.</td><td>N/A – the m
process ma
automatica</td></tr>
<tr><td>Loop</td><td>The following list explains how various iterator conditions of Loop are migrated to A2019.

• Loop with Times is migrated to loop with For n times iterator of the Loop package.
• Loop with List is migrated to loop with For n times iterator of the Loop package.
• Loop with Each Row in an Excel Dataset is migrated to loop with For each row in worksheet iterator of the Excel Advance package. The system variable $Excel Column$ used inside the loop is now a user defined variable specified in the same iterator.
• Loop with Each Row In A SQL Query Dataset is migrated to loop with For each row in a SQL query Dataset iterator of the Database package. The system variable $Dataset Column$ used inside the loop is now a user defined variable specified in the same iterator.
• Loop with Each File In A Folder is migrated to loop with For each file in a folder iterator of the File package. The system variables $Filename$ and $Extension$ are now keys name and extension of a dictionary variable specified in the same iterator.
• Loop with Each Folder In A Folder is migrated to loop with For each folder in a folder iterator of the Folder package. The system variable $Folder name$ used inside the loop is now a user defined variable specified in the same iterator.
• Loop with Each Row In A CSV/Text File is migrated to loop with For each row in CSV/TXT iterator of the CSV/TXT package. The system variable $Filedata Colum$ used inside the loop is now a user defined variable specified in the same iterator.
• Loop with Each Email Message On Mail Server is migrated to loop with For each mail in mailbox iterator of the Email package. The system variables $Email Cc$, $Email From$, $Email Message$, $Email Received Date$, $Email Received Time$, $Email Subject$, and $Email To$ are now keys emailCc, emailFrom, emailMessage, emailReceivedDate, emailReceivedTime, emailSubject, and emailTo respectively of a dictionary variable specified in the same iterator.</td><td>N/A – the m
process ma
automatica</td></tr>
</table>

<table>
<tr><th>Package</th><th>How it is migrated to A2019</th><th>What you n</th></tr>
<tr><td></td><td><ul><li>Loop with Each Node In An XML Database is migrated to loop with For each node in an XML database iterator of the XML package. The system variable $XML Data Node$ used inside the loop is now a user defined variable specified in the same iterator.</li></ul></td><td></td></tr>
<tr><td>Loop > Condition > Variable</td><td>
<p>Value type variable containing string</p>
<p>We migrate IF with the following operators as a String condition in A2019:</p>
<ul><li>=</li><li>< ></li><li>Include</li><li>Does not Include</li></ul>
<p>Value type variable containing number
We migrate IF with the following operators as a Number condition in A2019:</p>
<ul><li>>=</li><li><=</li><li>></li><li><</li></ul>
<p>Value type variable containing date</p>
<p>The system tries to evaluate if a condition on a variable has a date value. If found, it migrates IF with the Datetime condition in A2019. Otherwise, the system migrates it as a string or number condition based on the operator used. In those cases, you must change it to a date condition after the bot migration if a date operation is involved.</p>
<p>Additionally, you might also need to change the date format to one that is compatible with your data. The default format used to convert a date to string is <code>MM/dd/yyyy HH:mm:ss</code>.</p>
<p>List type variable</p>
<p>Loop on a variable condition of type List is migrated to either String or Number condition based on the operator used in the condition. The system uses the list index to validate the condition.</p>
</td><td>N/A – the m
process ma
automatica</td></tr>
<tr><td>Loop > Condition (other)</td><td>
<p>Refer to the table below to see how various conditons are migrated to the respective A2019 conditions.</p>
<table>
<tr><th>11.x</th><th>A2019</th></tr>
<tr><td>Web Control Exists or Web Control Does Not Exists</td><td>Migrated to the equivalent If condition of the Legacy Support package.</td></tr>
<tr><td>Object Properties</td><td>Migrated to the Object condition of the Recorder package.</td></tr>
<tr><td>Application Running or Application Not Running</td><td>Migrated to the equivalent If condition of the Application package.</td></tr>
<tr><td>File Exists, File Does Not Exist, File Date, File Size</td><td>Migrated to the equivalent If condition of the File package.</td></tr>
</table>
</td><td>N/A – the m
process ma
automatica</td></tr>
</table>

<table>
<tr><th>Package</th><th>How it is migrated to A2019</th><th>What you n</th></tr>
<tr><td></td><td>
<table>
<tr><th>11.x</th><th>A2019</th></tr>
<tr><td>Folder Exists or Folder Does Not Exist</td><td>Migrated to the equivalent If condition of the Folder package.</td></tr>
<tr><td>Ping Successful Or Ping Unsuccessful</td><td>Migrated to the equivalent If condition of the Ping package.</td></tr>
</table>

Web Control Exists or Web Control Does Not Exist

Loop with Web control exists and Web control does not exist conditions are migrated to Loop > While conditions Web control exists and Web control does not exist of the Legacy Automation package respectively.</td><td></td></tr>
<tr><td>Loop (supporting commands)</td><td>The following table shows the Loop commands supported for migration and their respective mappings in A2019.
<table>
<tr><th>11.x Command</th><th>A2019 Actions</th></tr>
<tr><td>Exit Loop</td><td>Break</td></tr>
<tr><td>Continue</td><td></td></tr>
</table>
</td><td>N/A – the m process ma automatica</td></tr>
<tr><td>Message Box</td><td>This command is migrated to Message box action in A2019.

See Message box package.</td><td>N/A – the m process ma automatica</td></tr>
<tr><td>Object Cloning</td><td>This command is migrated to Recorder package > Capture action in A2019. Migration is supported for the following technologies:

• MSAA (Standard desktop technology
• Chrome browser
• Internet Explorer browser
• Java desktop
• Web Java
• UI Automation (advanced)

The 11.x GetAllChidrenName and GetAllChidrenValue actions returns string type variable values. In A2019, they return list values. The migration process joins the list values and stores them into a string variable to maintain consistent bot behaviors across releases.

Object Cloning with the "Export to CSV" action in 11.x is migrated into the following packages/ actions combinations because the action does not exist in A2019:

• The Capture action saves the captured data into a table variable.
• Then we use the Write to file action of the Data table pakcage to save the data from the table variable to the CSV file.

See Using the Capture action.</td><td>N/A – the m process ma automatica</td></tr>
</table>

<table>
<tr><th>Package</th><th>How it is migrated to A2019</th><th>What you n</th></tr>
<tr><td>OCR</td><td>All commands of OCR are migrated to equivalent A2019 actions of the OCR package. There is no change in behavior or command name.
See OCR package.</td><td>N/A – the m process ma automatica</td></tr>
<tr><td>Open Program/File</td><td>This command is migrated to the Open program/file action of the Application package.
In 11.x, this command does not throw an error if you provide an incorrect value in the Start In field. A2019 validates the value entered for the same field and throws an error during bot execution.
See Application package.</td><td>Users must bot accordi want to cor the Start In incorrect.</td></tr>
<tr><td>PDF</td><td>Migration is supported for the following PDF commands.
<table>
<tr><th>11.x</th><th>A2019</th></tr>
<tr><td>PDF to Image</td><td>Extract image</td></tr>
<tr><td>Extract Text</td><td>Extract text</td></tr>
<tr><td>Split Documents</td><td>Split documents</td></tr>
<tr><td>Encrypt Document</td><td>Encrypt document</td></tr>
<tr><td>Decrypt Document</td><td>Decrypt document</td></tr>
</table>
See PDF package.</td><td>N/A – the m process ma automatica</td></tr>
<tr><td>PGP</td><td>All commands of PGP are migrated to equivalent A2019 actions of the PGP package. There is no change in behavior or command name.</td><td>N/A – the m process ma automatica</td></tr>
<tr><td>Play Sound</td><td>All commands of Play Sound are migrated to its equivalent actions of the Sound package in A2019.
A2019 supports only .mp3 and .wav file types in Play media file action.
See Play Sound package.</td><td>N/A – the m process ma automatica</td></tr>
<tr><td>Printer</td><td>Default Printer, Remove Printer, and Select Default Printer are migrated to the equivalent actions of the Printer package in A2019.
See Printer package.</td><td>N/A – the m process ma automatica</td></tr>
<tr><td>Prompt</td><td>All commands of Prompt are migrated to equivalent A2019 actions of the Prompt package.
The following table shows commands that can be migrated with name changes.</td><td>N/A – the m process ma automatica</td></tr>
</table>

<table>
<tr><th>Package</th><th>How it is migrated to A2019</th><th>What you n</th></tr>
<tr><td></td><td><table><tr><th>11.x</th><th>A2019</th></tr><tr><td>Prompt For Value</td><td>Converts to the For value action. In addition, Simulate keystroke action is added below the For value action to perform the keystrokes on the specific window title. This is to retain the execution behavior of old bots.</td></tr><tr><td>Prompt for File</td><td>For file</td></tr><tr><td>Prompt for Folder</td><td>For folder</td></tr><tr><td>Prompt For Yes/No</td><td>For yes/no</td></tr></table>
See Prompt package.</td><td></td></tr>
<tr><td>Read from CSV/TXT</td><td>The Read from CSV/Text is converted to Open, Read, and Close actions in the A2019 CSV/TXT package.
If your 11.x bot is using a variable as a session name and the Loop action used to read all rows of the CSV/TXT is using a hard-coded session name instead of a variable, then you must review the migrated bot and set the output variable of the CSV/TXT > Read action in the respective loop. Otherwise, you will get a UI error when you edit the A2019 bot.</td><td>Review the and set the variable of t Read actio respective l</td></tr>
<tr><td>Run Logic</td><td>Run logic command is migrated to the Run action of the Task Bot package in A2019.</td><td>N/A – the m process ma automatica</td></tr>
<tr><td>Run Script</td><td>Run Script command is converted to the Open, Run, and Close actions of either JavaScript or VBScript package in A2019 based on the script file extension.
A2019 supports the Nashhorn JS JavaScript engine, which supports ECMAScript 5 and ECMAScript 6 standards. Support of WScript in JavaScript is not yet available.
See JavaScript package and VBScript package.</td><td>N/A – the m process ma automatica</td></tr>
<tr><td>System</td><td>Lock computer, Logoff, Restart, and Shutdown actions are migrated to the equivalent actions of the System package in A2019.
See System package.</td><td>N/A – the m process ma automatica</td></tr>
<tr><td>Task</td><td>The following table shows the different commands that are migrated to the respective actions of the A2019 Task Bot package.<table><tr><th>11.x Command</th><th>A2019 Action</th></tr><tr><td>Pause</td><td>Pause</td></tr><tr><td>Stop Task</td><td>Stop</td></tr></table></td><td>N/A – the m process ma automatica</td></tr>
</table>

<table>
<tr><th>Package</th><th>How it is migrated to A2019</th><th>What you n</th></tr>
<tr><td></td><td><table><tr><th>11.x Command</th><th>A2019 Action</th></tr><tr><td>Run Task</td><td>Run. The output returned by child bots is stored in a dictionary variable and then mapped to the respective variable in the parent bots.</td></tr></table></td><td></td></tr>
<tr><td>Terminal Emulator</td><td>Encrypt text is not supported in the Send Text and Set Field actions for A2019. Automation Anywhere recommends that you use Credential Vault instead of of plain text.
A2019 does not support legacy technology and by default supports all capabilities of Advance Technology of the 11.x bots.
The following features are not yet supported in A2019:
• SSH1
• Session sharing. Without session sharing, you should close each session within the same session.
See Terminal Emulator package.</td><td>N/A – the m
process ma
automatica</td></tr>
<tr><td>Variable Operation (Assign)</td><td>Value type variables
The functionality for this command has been divided into multiple packages in A2019.
In 11.x, this command was performing assignment operations for all the supported datatypes. A2019 has built a dedicated Assign action for each data type. The migration process handles the mapping of the corrected packages and action based on the assignment that the respective variable operation is performing.
Array type variables
Operations involving on array assignment is migrated to Set value of a single cell action of the Datatable package to set a value for specific rows and columns.
System variable $Date$
The 11.xVariable Operation command that uses the $Date$ system variable is migrated to A2019 by adding new date actions based on the operation being performed using $Date$. The migration process also converts the date value to a default string format – mm/dd/yyyy HH:mm:ss.
Random variable of sub type string
We migrate and map directly.</td><td>N/A – the m
process ma
automatica</td></tr>
<tr><td>Variable Operation (Reinitialize)</td><td>List variable
For the Variable Operations that reinitialize the list variable in 11.x, the migration process creates a temporary list variable with new values and assign it to the destination list variable in A2019.</td><td>N/A – the m
process ma
automatica</td></tr>
</table>

Package	How it is migrated to A2019	What you n
	Array variable declared by reading a Text file The Array variable type is migrated as a Table variable type in A2019. The system uses the CSV/TXT package to read and load the respective data into the table variable in the bot. Array variable declared by reading an Excel/CSV file The migration process addresses this use case by migrating the Array variable type as a Table variable type in A2019. The system adds Open, Get Multiple Cells, and Close actions of the Excel Advance package and populates the table variable.	
Variable Operation (resetting system variables)	The following system variables are migrated as user defined variables in A2019. The system adds a respective action to clear the value of the equivalent variable created in A2019. • Email Cc • Email From • Email Message • Email Received Date • Email Received Time • Email Subject • Email To • Error Description • Error Line Number	N/A – the m process ma automatica
Wait	Wait for window and Wait for screen change in A2019 throws an exception error if the respective window is not open/close in the specified time or the screen is not found in specified time. In these cases, the system adds try and catch block if the command was configured to stop the bot and adds the Stop task action in the catch block. This is to ensure that the execution behaviour of migrated bots is the same as 11.x. Because we are migrating commands with the Stop bot action is encapsulated with the try and catch block in A2019, the bot also stops if the action fails due to some other reason.	N/A – the m process ma automatica
Web Recorder	All commands (except those mentioned below explicitly) of Web recorder are migrated to respective actions within the Legacy Automation package in A2019. The Legacy Automation package ensures that the migrated bots give the same results as 11.x. However, it is not recommended to use the Legacy Automation package for new development. Find broken links is migrated to Browser > Find broken links package. Additionally, 11.x has the "Find broken links timeout" and "Find broken links" options within the Tools > Options. A2019 has these options as part of the action and the timeout defaults to 10 seconds and the number of parallel threads value defaults to 10. Download files is migrated to Browser > Download files package.	N/A – the m process ma automatica
Window Action	All commands of Window Action are migrated to its equivalent actions of the Window package in A2019.	N/A – the m process ma automatica

<table>
<tr><th>Package</th><th>How it is migrated to A2019</th><th>What you n</th></tr>
<tr><td></td><td>See Window package.</td><td></td></tr>
<tr><td>XML</td><td>All commands of XML are migrated to its equivalent actions of the XML package in A2019. The following command name have changed.
<table>
<tr><th>11.x</th><th>A2019</th></tr>
<tr><td>End XML session</td><td>End session</td></tr>
<tr><td>Start XML session</td><td>Start session</td></tr>
<tr><td>Delete Node/Attribute</td><td>Delete node</td></tr>
<tr><td>Update Node/Attribute</td><td>Update node</td></tr>
<tr><td>Get nodes action with the "Single Nodes" option selected</td><td>Get single node action</td></tr>
<tr><td>Get nodes action with the "Multiple Nodes" option selected</td><td>Get multiple node action</td></tr>
</table>
See XML package.</td><td>N/A – the m process ma automatica</td></tr>
</table>

Variable mapping for migration

Some variables map directly from previous product versions to A2019 while others behave differently or contain configuration changes.

In A2019, all variables defined in bots are created as "Use input" or "Use output" types during migration to exchange values between parent bots and child bots.

Additional variables available with A2019.12

The following table lists the variables available for migration with this release and how they map to A2019. N/A means there are no changes.

Variable	How it differs from 11.x	What you need to do
List	The List variable can be declared a random in 11.x. The migration process adds a new action to get the list size and adds the Assign a random number action to find the random position and use it to get a random list item.	N/A – information is mapped automatically during migration.
System variables	The $Excel Cell$ system variable is migrated to Excel > Get cell address action just above the command that is using it.	N/A – information is mapped automatically during migration.

Variable	How it differs from 11.x	What you need to do
	In 11.x, the AAInstallationPath system variable returns the Enterprise client installation path. In A2019, it returns the Bot agent installation path.	

Additional variables available with A2019 Build 3337

When Boolean variables in 11.x are converted to strings, they return "True" or "False" (note the capitalization). Boolean variables in A2019 that are converted to strings return "true" or "false" (note the capitalization).

The following table lists the variables available for migration with this release and how they map to A2019. N/A means there are no changes.

Variable	How it differs from 11.x	What you need to do
System variables	The 11.x variable operation on Array variables is migrated as Set value of a single cell action within the Data Table package. The following additional system variables are supported with this build: • $AATaskName$ in 11.x becomes $System.AATaskName$ in A2019. Additionally, the 11.x variable returns the value to your computer path directory (for example Automation Anywhere \My Tasks\My Folder\My Folder2\AATaskName.atmx); the A2019 variable returns the value to the bot path relative to the Enterprise Control Room (for example Bots/ AATaskName). • The $AAApplicationPath$ system variable in 11.x returns the path set by users in the Tool > Option setting of what is known as the "client application" in 11.x. In A2019, it becomes a global value. The migration process maps this change automatically. See Global values. • $Date$ in 11.x returns the current date and time in a format specified in the AA.Settings.XML file. In A2019, it return in the Date Time and the user must use a command to change it in to string. To minimize disruption to the user, the migration process does the following to each $Date$ instance: ◦ Creates a temp variable $SystemDateInString$ of type String. ◦ Adds a Datetime.ToSting action with customer format as mm/dd/yyyy HH:mm:ss and store the output into above string variable. ◦ Uses this string variable where ever $Date$ is used.	N/A – information is mapped automatically during migration.

Variable	How it differs from 11.x	What you need to do
	Depending on how your bot is configured, you might need to update the date/time configuration. • $Current Directory$ is deprecated in A2019 and automatically converted to a user defined variable during migration. No action is required from the user. • CPUUsage$ in 11.x becomes $System:CPUUSage$ in A2019 during migration.	

Additional variables available with A2019 Build 2545

The following table lists the variables available for migration with this release and how they map to A2019. N/A means there no are changes.

Variable	How it differs from 11.x	What you need to do
List	In 11.x, index position is not required to fetch the list item from a list variable inside a loop. A2019 uses the index position of the list to fetch the list item. In A2019, an empty list variable used outside a loop returns a run time error, where as in 11.x the bot returns an empty value and executes without error. See Loop package.	
System variables	$Counter$ system variable is deprecated in A2019. The migration process creates a user defined variable and modifies the bot to ensure it provides the same output as the 11.x bot. If a variable is defined at the index position for the following system variables, you might need to fix the migrated bots because the migration process could not determine if the variable contains an index or column name. The migration process defaults to a column name in the variable, but if it is an index, you must change it accordingly. • $Filedata Column$ • $Dataset Column$ • $XML Data Node$ • $Excel Column$ The following additional system variables are supported in A2019:	N/A – information is mapped automatically during migration.

<table>
<tr><th>Variable</th><th>How it differs from 11.x</th><th>What you need to do</th></tr>
<tr><td></td><td>
<ul>
<li>$ArrayColumns($arrayVariable$)$ becomes $arrayVariable.DataTable:columnCount$ in A2019</li>
<li>$ArrayRows($arrayVariable$)$ becomes $arrayVariable.DataTable:rowCount$ in A2019</li>
<li>$AAControlRoom$ becomes $System:AAControlRoom $ in A2019</li>
<li>$RAMUsage$ becomes $System:RAMUsage$ in A2019</li>
<li>$TotalRAM$ becomes $System:TotalRAM$ in A2019</li>
<li>$OSName$ becomes $System:OSName$ in A2019. 11.x returns the Microsoft Windows 10 Pro 64-bit value; A2019 returns Windows 10 64-bit.</li>
<li>PDF – In A2019, this system variable is part of the dictionary variable returned in the respective PDF command. See Using dictionary variable for PDF properties.</li>
<li>$Excel Cell Row$ is the Get row number action in A2019.</li>
<li>$Excel Cell Column$ is the Get column name action in A2019.</li>
</ul>
Specific to the $Excel Cell Row$ and $Excel Cell Column$:
<table>
<tr><th>Use Case</th><th>11.x</th><th>A2019</th></tr>
<tr><td>
<ul>
<li>Excel is opened with or without "contains header" checked containing 10 rows.</li>
<li>Set active cell as F10</li>
<li>A loop is performed to row read</li>
<li>Put a messagebox with $Excel Cell Column $ in it</li>
<li>Run the bot</li>
</ul>
</td><td>When the active cell selected is F10, the system returns A as cell column</td><td>When the active cell selected is F10, the system returns F as value</td></tr>
</table>
</td><td></td></tr>
</table>

Additional variables available with A2019 Build 2079

The following table lists the variables available for migration with this release and how they map to A2019. N/A means there are no changes.

Variable	How it differs from 11.x	What you need to do
System variables	In 11.x, these were system variables; they are user defined variables in A2019. • $Dataset Column$ – Defined in Loop > For each row in a SQL query dataset • $Extension$ – Access the value by using the "extension" key • Email related variables – The following 11.x system variables are user defined variables in A2019 and should be declared in the Email package > Loop action: $Email Cc$, $Email From$, $Email Message$, $Email Received Date$, $Email Received Time$, $Email Subject$, and $Email To$ • $FileName$ – Defined in Loop > For each file in folder. Access the value by using the "Name" key. • $FolderName$ – Defined in Loop > For each folder in folder • $XML Data Node$ – Defined in Loop > Each node in XML dataset The 11.x "Filedata Column" system variable (used in the the Loop action when interating CSV/Text rows) has been deprecated in A2019. Automation Anywhere creates a user variable during the migration process that works as the Filedata Column. Additionally, A2019 does not remove the leading spaces from the value retrieved from "Filedata Column" in the loop by default. The following additional system variables are supported in A2019: • Machine – Returns the machine name of the device on which the bot is executed. • MiliSecond – Returns the value that is copied to the clipboard.s	N/A – information is mapped automatically during migration.
Array	In 11.x, you can declare an Array variable by referring to a text or CSV file. In A2019 • This variable is called Table. • You must use the CSV/TXT package to read and load the respective data table variable in the bot	N/A – information is mapped automatically during migration.

Variable	How it differs from 11.x	What you need to do
	• bots add Open, Get Multiple Cells, and Close actions to the Excel Advance package and populate the table variable. The index position starts with 1 in legacy. In A2019, the Table variable starts with 0. For example, `$arrayVariable(1,1)$` becomes `$arrayVariable[0][0]$` in A2019.	

Variables available with A2019 Build 1610

The following table lists the variables available for migration with this release and how they map to A2019. N/A means there are no changes.

<table>
<tr><th>Variable</th><th>How it differs from 11.x</th><th>What you need to do</th></tr>
<tr><td>Clipboard</td><td>In 11.x this variable is represented as $clipboard $. In A2019, it is represented as $Clipboard:Clipboard$.</td><td>N/A – information is mapped automatically during migration.</td></tr>
<tr><td>System</td><td>The following syntaxes for the system variable have changed in A2019.
<table>
<tr><th>11.x</th><th>A2019</th></tr>
<tr><td>$Day$</td><td>$System:Day$</td></tr>
<tr><td>$Month$</td><td>$System:Month$</td></tr>
<tr><td>$Year$</td><td>$System:Year$</td></tr>
<tr><td>$Hour$</td><td>$System:Hour$</td></tr>
<tr><td>$Minute$</td><td>$System:Minute$</td></tr>
</table>
See System variables for more information.</td><td>N/A – information is mapped automatically during migration.</td></tr>
<tr><td>List</td><td>In A2019, the List sub-type has dedicated String, Numeric, Boolean, and Datetime datatypes. After you migrate the bot, Automation Anywhere creates a list of the String datatype.
List variables outside the loop can be accessed by index. For example,
$listVariable[0]$
where 0 represents the first value in the list.</td><td>Automation Anywhere will convert the String value to Numeric if an attribute of an action accepts Numeric values during the migration.
However, we cannot determine the actual value type for some of the complex legacy commands, like variable operations, so you must review the bot after migration to take corrective steps.</td></tr>
</table>

Variable	How it differs from 11.x	What you need to do
Value	In A2019, we have String, Numeric, Boolean and Datetime as core data types instead of generic type Value. All variables of type Value are created as String in A2019 upon migration.	Automation Anywhere will convert the String value to Numeric if an attribute of an action accepts Numeric values during the migration. However, we cannot determine the actual value type for some of the complex legacy commands, like variable operations, so you must review the bot after migration to take corrective steps.

Copy and paste 11.x information to A2019

11.x server repository files and the credential vault file are required in the A2019 environment. The most efficient way to get this data is to copy them from the 11.x environment into A2019.

The following table shows information you must copy from 11.x and lists where to paste them before you have installed in A2019.

11.x environment	A2019 environment
Copy all the files and folder in <CR Repo>\Server Files \Default\AutomationAnywhere. This directory contains the bot files and dependency files required to migrate your bots.	Paste or unzip them into \ProgramData \AutomationAnywhere\Server Files\Default \0\Automation Anywhere\Bots If you do not see the necessary directories within ProgramData\AutomationAnywhere in A2019, manually create them.
Copy the CredentialVault.dat file, which by default is contained in <CR Repo>\Server Files This file unlocks the Credential Vault in A2019.	Paste it to the same location in the A2019 environment.

After you paste the relevant files and folders into your A2019 environment, log in to A2019, navigate to Bots > My Tasks, and verify that all the relevant 11.x folders and .atmx files are available.

Prerequisite tasks for migrating bots

After you have installed Enterprise A2019 On-Premises, you must perform certain tasks before migrating 10.x or 11.x bots.

Prerequisites

Ensure you complete the preparatory tasks listed in Steps 1 and 2 in the Upgrade to Enterprise A2019 procedure. Upgrade to Enterprise A2019

Procedure

1. For 11.x only: Update the Enterprise Control Room access URL and repository path. Run the following SQL commands to update the access URL and repository path:
    a) To update the access URL: update CONFIGURATION set value = '[A2019 Control Room URL]' where category = 'CR_setup_general' and config_key = 'AccessUrl'
    Example query: update [AAE-Database].[dbo].[CONFIGURATION] set value ='http://A2019-crurl.com' where config_key='AcessUrl'
    Note: Do not include '/' at the end of the access URL that you provide in the above command.
    b) To update the repository path: update CONFIGURATION set value = A2019 Control Room repository path where category = 'CR_setup_general' and config_key = 'RepositoryPath'
    Example query: update [AAE-Database].[dbo].[CONFIGURATION] set value ='C:\ProgramData \AutomationAnywhere\Server Files' where config_key='RepositoryPath'
2. Create users who will migrate bots from the Enterprise Control Room. Grant these users the following permissions and folder permissions for the Bots>My Tasks and My MetaBots folder.
    Migrate bot user account – This account has access to the Administration > Migration page and can create a migration instance. Create a custom role that meets the following criteria:
    - Have the View Migration permission.
    - Have the Manage Migration permission.
    - Have permission on the 11.x folder containing the bots and MetaBots you want to migrate.
    - Be in a role that has access to Bot Runners that you want to select for running the migration (on the Administration > Migration > Run As page).

    Bot Runner user account – This account runs the migration and must be available for selection on the Administration > Migration > Run As page. This user account must meet the following criteria:

    - Have an unattended Bot Runner license.
    - Have the Autologin Set status.
    - Have the Allow a bot-runner user to run migrations permission.
3. Install the Bot agent on the device that you want to use for migration.
    Register device and install Bot agent

Next steps

For 10.x: Copy 10.x data

For 11.x: Migrate Enterprise bots

Copy 10.x data

You must copy the 10.x data to Enterprise A2019 before you convert the 10.x bots.

Procedure

1. Log in to your A2019 staging environment.
2. Click Administration > Migration.
3. Click Copy 10.x data.
4. Provide the following information on the GENERAL page.

Option	Action
Name	Enter a migration name or use the default one. The default migration name shows the name of the user who is logged in, current date, and time stamp.
Description	Enter a description for the migration.

5. Click Next.
6. Provide the following information on the DATABASE page.

Option	Action
Use secure connection	Select this option to use a secure connection to connect with the database.
Server host name	Enter the host name of the database server that contains the 10.x data you want to migrate.
Server port	Enter the port you want to use to connect with the database server.
Use database credentials	Select this option to use database credentials for authentication when establishing a connection with the database server. If you have selected this option, provide the credentials you want to use to connect to the database server in the Username Password fields.
Use Windows authentication	Select this option to use Windows authentication for establishing a connection with the database server.
Database name	Enter the database name that contains the 10.x data you want to migrate.
Connect	Click this option to establish a connection with the database.

7. Click Next.
8. Provide the following information on the REPOSITORY page.

Option	Action
Repository path	Enter the location of the 10.x data is available on the device.

Option	Action
Master key	Enter the master key for 10.x.
Validate	Click this option to validate the connection before you copy the 10.x data.

9. Click Copy data.

Next steps

Migrate Enterprise bots

After you have successfully copied the 10.x data to Enterprise A2019, convert the 10.x bots.

Migrate Enterprise bots

The bot migration process converts 11.x or 10.x bots (TaskBots and MetaBots) in .atmx and .mbot format to the .bot format used in A2019 and uploads the successfully migrated bots to the Enterprise Control Room public workspace.

All manual dependencies of bots are automatically converted as Enterprise Control Room dependencies during migration. The Download Control Room file action downloads these dependencies from the Enterprise Control Room to the respective locations.

Migrating to A2019 is available for On-Premises deployment only.

Procedure

1. Log in to your A2019 staging environment from a machine with the Bot agent installed.
2. Click Administration > Migration.
   Note: If you have migrated bots from 10.x to 11.x, the information about that migration is not displayed on the All migrations page.
3. Click Migrate bots.
4. Provide information on the General page.

Option	Action
Name	Enter a migration name or use the default one. The default migration name shows the name of the user who is logged in, current date, and time stamp.
Description	Enter a description for the migration.
Overwrite	Select this option to overwrite an existing bot if a bot with the same name exists in the folder.
Do not overwrite	Selecting this option does not migrate the bot if a bot with the same name exists in the folder.

5. Click Next.
6. Click Bots > My Tasks.

7. Select the bots (TaskBots and MetaBots) you want to migrate and click the right arrow.
   The Last Migrated column indicates when the bot was migrated previously. N/A means the bot has not been migrated before.
8. Click Next.
9. Select one or more usernames from the list to run the migration and click the right arrow.
   Only users with the Autologin Set status and Allow a bot-runner user to run migrations permission are available for selection.
   Usernames can display either the message `Picked at run time` or the device name in the Device column. A device name indicates the registered device for that user. `Picked at run time` is shown when a user does not have a default device, for example, a user who has not registered a device and a system administrator has assigned a device to that user.
   When you select multiple Bot Runner users, the following rules apply:
   - Bots are distributed across selected Bot Runner users in a round-robin method.
   - The first Bot Runner user on the selected list is the first one used.
   - A parent bot and its dependencies are assigned to a single Bot Runner user.
10. Click Next.
11. Optional: Review the dependent TaskBots and MetaBots on the Bot and Dependent Bots page before you migrate them.
    Dependent bots (TaskBots and MetaBots) are migrated before the primary bot.
    The table shows the primary bot at the bottom and its dependencies above. For example, the following information means that Sample05.atmx has a dependency on Sample04.atmx, and Sample04.atmx has a dependency on the MessageBox.atmx and MetaTask.mbot.

Type	Name	Path
MetaBot (mbot)	MetaTask.mbot	Bots\My Metabots \MetaTask.mbot
TaskBot (atmx)	MessageBox.atmx	Bots\MyTasks\MessageBox.atmx
TaskBot (atmx)	Sample04.atmx	Bots\MyTasks\Sample04.atmx
TaskBot (atmx)	Sample05.atmx	Bots\MyTasks\Sample05.atmx

12. Click Migrate Bot.
    After a migration, the system uploads successfully migrated bots to the public workspace of the A2019 Enterprise Control Room (in the same folder in which the .atmx file is available). Only bot migrations initiated from the Enterprise Control Room are stored in the public workspace.

    The All migrations page shows the current status of the migrated bot and other related information. You can also click the View migration icon associated with each migration instance to see additional information, such as any unsupported commands or attributes associated with the migrated bot and its dependencies.

    You can view in-process migration activities from the Activity > In progress page.

    Note: Bots that are not migrated successfully are not uploaded to the Enterprise Control Room.

Next steps

Verifying the bot migration
Related tasks
Migration reports

How MetaBots are migrated

When you migrate a MetaBot to A2019, equivalent bots are created for the various logics available in the MetaBot, except for application screens. After successful migration, each logic in a .mbot file is converted to a TaskBot files.

A MetaBot contains assets and logic. Assets are the application screens or DLLs that are used to automate a task on an application. Logic is a set of commands to perform an operation and interact with other logic and bots.

We will use the following MetaBot to explain how it is migrated to A2019:

- MetaBot name: MetaTask
- Assets:
    - Login screen
    - General.dll
    - DLL\Binary.dll
- Logic:
    - Common
    - Logic\Connect
    - Logic\Disconnect
    - Logic\Operations\Numeric

MetaBot migration process

The system creates a folder with the same name as the MetaBot within the My Metabots folder available in the Bots folder, and the same folder structure as 11.x is retained. For example, if the folder structure in 11.x is Accounts/Tax/MetaTask.mbot, the system retains the folder structure as Accounts/Tax/MetaTask.mbot. All the components of a MetaBot are stored in the folder created for that MetaBot. In this example, the system creates the MetaTask folder in the Bots\My Metabots folder and stores all the components the MetaBot in that folder.

Migration of assets

The system does not maintain the folder structure for assets in order to maintain the references between the DLLs. For the above example, General.dll and Binary.dll are stored in the MetaTask folder although the Binaary.dll is stored in the DLL subfolder.

Important: Migration of MetaBots with screens to A2019 is not supported.

Migration of logic

Each logic in a MetaBot is converted to a TaskBot and each command used in a logic is converted to the equivalent action in A2019. The variable used in a logic is converted to an equivalent variable in A2019. If the Parameter Type of a variable is input or output, the same is maintained after that variable is migrated to A2019. For example, if the Parameter Type of the variable ABC is set as Input, the variable ABC created in A2019 has the Use as input option selected after it is migrated. The system retains the internal folder structure of the logics. For the above example, all the migrated logics are stored as listed in the following table:

Folder	Entry
MetaTask	Common
MetaTask\Logic	Connect

Folder	Entry
MetaTask\Logic	Disconnect
MetaTask\Logic\Operations	Numeric

Migration of Run Logic command

The Run Logic command is used in a bot to run a specific logic from a MetaBot in 11.x. When you migrate that bot, the Run Logic command is converted to the Run action of the Task bot package. The input variables are converted to equivalent variables in A2019 and the output variables are migrated to a dictionary variable. You use the key in the dictionary variable to use the associated value.

Migration of Execute command

The DLLs in the MetaBots use the Execute command to run a function from that DLL. After migration to A2019, each Execute command is converted to Open, Run function, and Close actions of the DLL package. Information about which function to run from the DLL, which parameters to use, and other details in the Execute command is migrated to the Run action.

Verifying the bot migration

It is important that you verify the migration completion and the migrated bot runs successfully in the A2019 environment. The bot might have been converted to .BOT, but it could contain errors that bot might have converted to .BOT, but it could contain errors that prevent it from running successfully.

Procedure

1. Log in to your A2019 environment from a machine with the Bot agent installed using a bot creator account with a Bot Runner license and the "View Migration" permission.
2. Verify that the migration completed successfully by clicking Administration > Migration.
3. Confirm that your migration instance has the "successful" status (indicated by the green checkmark) and the Migrated Item column shows "1" to indicate that 1 bot was migrated. If the Migrated Item column shows "0", your bot has not migrated successfully and will not be available on the My Bots page.
   If your migration instance stays in the "in-progress" status for an extended time period, confirm the following:
   - Dependent bots are TaskBots; A2019 does not support MetaBots at this time.
   - You selected one user to run the bot. This current migration release supports one user only.
4. Verify that the bot runs successfully by clicking Bots > My bots.
5. Navigate to the migrated bot.
   For example, if you migrated a bot from the "My Tasks" folder, then navigate to the same folder to find your migrated .BOT bot.
6. Click the bot and fix any errors.
7. Run the bot to confirm that all errors have been fixed.

Related concepts
Understanding Enterprise A2019 migration

Migration reports

Use the reports to analyze the status of individual bot migrations and identify any unsupported commands or attributes associated with the migrated bot and its dependencies. You must have the "View migration" permission to access these reports.

Prerequisites

You must have the `View migration` permission to access these reports.

The migration reports provide information about bot migration and data migration. The bot migration refers to the conversion of 10.x or 11.x bots to A2019 and data migration refers to copying 10.x data to A2019.

Procedure

Access the reports from the Administration > Migrations > View migration icon associated with the migration instance for which you want to view the report.

- For 10.x and 11.x: View the following information bot migration:
  - Migration details such as name of the migration instance, its description, and status.
  - Migration results such as the start and end time of the migration process, status of the migration, and the number of items migrated.
  - General: Whether the option to overwrite files was selected.
  - Run-as: Information about the run-as user selected for the migration instance.
  - Bot migration results such as all the bots (parent bots and their child bots) that are migrated and their status.

    Click the View migration issues icon associated with an unsuccessfully migrated bot to see the unsupported commands or attributes.
  - General details about the user who created the migration instance, last modification date, and its object type.
- For 10.x only: View the following information for data migration:
  - Migration details such as about name of the migration instance, its description, and status.
  - Data migration results such as the start and end time of the migration process, status of migration, and number of items migrated.
  - Roles that are copied and their status.
  - Users that are copied and their status.
  - Auto-login credentials that are copied and their status.
  - Bots that are copied and their status.
  - Schedules that are copied and their status. The copied schedules are disabled in Enterprise A2019 because migration of the associated devices is not supported and therefore they are not available.
  - General details about the user who created the migration instance, last modification date, and its object type.

Export to CSV

The export process exports all data (including hidden data columns), but only for the current page. If you have migration instances on additional pages, you must navigate to those pages to export that data.

To export migration data to CSV:

Procedure

1. Click Administration > Migrations.
2. Select the migration instances you want export.
3. Click the Export checked items to CSV icon.
4. Open the CSV file to see the exported data.

Migrate Community Edition bots

Bots created in the 11.x Community Edition environment must be migrated to the A2019 Community Edition to allow users to use these bots in A2019. You use the Bot Migration package available in the A2019 Community Edition to manually migrate the bots.

Prerequisites

Before you start migrating bots, do the following:

- Use the Bot Scanner utility to determine if your 11.x bots can be migrated successfully. See Bot Scanner overview.
- Get access to A2019 Community Edition.
- Register a device in A2019 Community Edition to run bots. See Register device and install Bot agent.

This procedure migrates one bot at a time. To migrate all bots within the same folder, you can create a complex bot by iterating files in a folder in a loop or add multiple Migrate Bot actions for each .atmx file you want to migrate.

Important: If a bot has dependencies on other bots, you must migrate the dependent bots first and then the parent bot. For example, the main.atmx parent bot has a dependency on child1.atmx, which also has a dependency to child2.atmx, then add the Migrate bot actions in following order: child2.atmx, followed by{{child1.atmx}} and then {{main.atmx}}.

Procedure

1. Log in to A2019 Community Edition.
2. Use the Bot Migration package to migrate your bots.
   a) Navigate to Bots > My bots.
   b) Click Create New > Bot.
   c) Expand the Bot Migration package and double-click the Migrate bot action.
   d) Select Desktop file within the Bot file path section.
   e) Enter the complete path of the 11.x .atmx file you want to migrate.
   f) Optional: Enter the output folder path into the Output folder path field to specify where you want package conversion information and errors to be stored.
   A report showing relevant information is generated for each migrated bot.
   g) Leave the Overwrite the file if exists option selected (default setting) if you want this migrated bot to overwrite any bots of the same name in the A2019 Community Edition environment.
   h) Save the bot.
   i) Run the bot on the connected device to perform the migration.

Successfully migrated bots are uploaded to the A2019 private repository of the user who performed the migration. Only successfully migrated bots are migrated. Use the reports in the specified Output folder path to see the migration errors.

Related tasks
Using Bot Scanner
Related reference
Bot migration package

Uninstall Enterprise A2019 On-Premises

Uninstall the On-Premises Enterprise Control Room from your Linux server.

Prerequisites

Ensure that the Enterprise A2019 installation server is disconnected from the Microsoft SQL Server database.

Procedure

1. Log in to the installation server.
2. Run the uninstaller command as a superuser:

   ```
   $ sudo /opt/automationanywhere/enterprise/_Automation\ Anywhere\
   Enterprise_installation/Change\ Automation\ Anywhere\ Enterprise\
   Installation
   ```

   The installation wizard verifies the installation and proceeds with the uninstallation.

   Tip:

   - Enter the

     ```
     back
     ```

     command to return to a previous command step.
   - Press the return key to accept default values, or enter an alternate value then press the return key.
3. Confirm the uninstallation by entering

   ```
   Y
   ```

   .

   The Automation Anywhere Enterprise components are removed from the Linux system.

   The databases with associated Automation Anywhere Enterprise information about users and bots remains stored in the database and remain connected to any other Enterprise Control Room in your cluster.

Bot deployment and concurrent operations

List of maximum concurrent operations and estimated deployment times.

Overview

Automation Anywhere supports up-to 1000 simultaneous bot deployments and executions across the Enterprise Control Room cluster.

Entity Types and Counts	
Entity Type	Count
Users	5000
Roles	2000
Audit entries	5,000,000
Lockers	100
Credentials	5000
Repository files	2500
Repository folders	1250

- Manually switch the Bot agent
  Switch the Bot agent on a registered device to work with a different Enterprise Control Room.

Manually switch the Bot agent

Switch the Bot agent on a registered device to work with a different Enterprise Control Room.

Prerequisites

Ensure that you have the proper permissions to access and edit the Windows services.

The Bot agent, a lightweight application that enables you to run bots on your device, is associated with an Enterprise Control Room. This task provides steps on how to associate your device with a different Enterprise Control Room.

Procedure

1. Stop the Bot agent service from the local Windows Task Manager.
2. Optional: Go to the C:\Windows\System32\config\systemprofile\AppData\Local\AutomationAnywhere folder and delete the registration.properties file.
   Note: This is only required if you want to register the device in a different Enterprise Control Room environment. To see the Enterprise Control Room where the device is registered, open the Registration.properties file and check the value for the Enterprise Control Room URL.
3. Log in to the Enterprise Control Room.
4. Navigate to Devices > My devices.
5. Click the Add local device icon.
6. Download and install the latest Bot agent.
7. Return to Devices > My devices from the updated device.
   The Registration.properties file is not generated immediately after the Bot agent installation. It is generated only when a user accesses an Enterprise Control Room URL from that device. If the device registration is successful, the machine appears as Connected and the Registration.properties file is created at the given location on the Bot Runner machine.
8. Navigate to the C:\Windows\System32\config\systemprofile\AppData\Local\AutomationAnywhere folder and ensure that the registration.properties file is present to verify the Bot agent update.

Watch the following video on how to update your Bot agent:

Update the Bot agent

Related tasks
Register device and install Bot agent