July 2, 2020

Automation Anywhere Version 11.3

Legal Notices

© 2020 Automation Anywhere, Inc. All Rights Reserved.
See the list of Automation Anywhere trademarks at https://www.automationanywhere.com/trademark.

All other customer or partner trademarks or registered trademarks are owned by those companies.

The information contained in this documentation is proprietary and confidential. Your use of this information and Automation Anywhere Software products is subject to the terms and conditions of the applicable End-User License Agreement and/or Nondisclosure Agreement and the proprietary and restricted rights notices included therein.

You may print, copy, and use the information contained in this documentation for the internal needs of your user base only. Unless otherwise agreed to by Automation Anywhere and you in writing, you may not otherwise distribute this documentation or the information contained here outside of your organization without obtaining Automation Anywhere's prior written consent for each such distribution.

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

Content

Using Enterprise Control Room. . . . 5
- Log on to Enterprise Control Room. . . . 6
  - Log on to Enterprise Control Room hosted in Single Sign On mode. . . . 7
  - Log on to Enterprise Control Room hosted in Non-Active Directory mode. . . . 7
  - Log on to Enterprise Control Room hosted in Active Directory/Kerberos mode. . . . 8
  - Log on to Bot Insight. . . . 9
  - Re-login to Enterprise Control Room when password policy is updated. . . . 9
  - Reset LDAP user credentials. . . . 10
- Getting Started with Enterprise Control Room. . . . 11
  - Enterprise Control Room overview. . . . 12
  - Enterprise Control Room interface overview. . . . 13
- Administration Overview. . . . 13
  - Settings overview. . . . 14
  - User management overview. . . . 32
  - Roles overview. . . . 40
  - Licenses - an overview. . . . 58
  - Migration overview. . . . 61
- Bots - Overview. . . . 77
  - Credentials- Overview. . . . 78
  - My bots- overview. . . . 91
- Activity overview. . . . 118
  - Monitor in progress activity. . . . 119
  - View in progress activity details. . . . 121
  - Manage historical activity. . . . 122
  - View details of selected activity from history. . . . 124
  - Schedule a bot. . . . 125
  - View and manage activities. . . . 128
  - View scheduled bot details. . . . 129
  - Edit a schedule. . . . 130
  - Delete a schedule. . . . 131
  - Activate or deactivate a schedule. . . . 131
- Devices overview. . . . 132
  - Manage devices. . . . 133
  - Manage device pools. . . . 137
- Workload overview. . . . 144
  - Workload Management guidelines. . . . 145
  - Manage workload queues. . . . 146
  - Run bot with queue. . . . 151
  - Workload. . . . 153
  - Manage workload SLAs. . . . 163
  - Sample Workload Management properties file. . . . 164
- Bot Store integration overview. . . . 169
  - Accessing Bot Store. . . . 170
  - Downloaded bots from Bot Store. . . . 170
  - Running protected bots. . . . 173
- Audit log overview. . . . 174
  - View audit details. . . . 175
  - Export data to CSV. . . . 176
  - Audit logs for run bot deployment and bot runner session. . . . 177
  - Audit logs for bots downloaded from the Bot Store. . . . 179
- Dashboards overview. . . . 181

Dashboards - home. . . . 182
Dashboards - bots. . . . 182
Dashboards - devices. . . . 182
Dashboards - audit. . . . 183
Dashboards - workload. . . . 183
Dashboards - Insights. . . . 184
Enterprise Control Room APIs. . . . 184
Audit API. . . . 186
Authentication API. . . . 191
Auto Login Credentials API overview. . . . 208
Automation Management API. . . . 213
Bot Execution Orchestrator API. . . . 215
APIs to manage credential vault. . . . 229
Bot Insight Data API. . . . 266
API to export and import Bot Lifecycle Management. . . . 284
API data migration from 10.x to 11.x Enterprise Control Room. . . . 288
API to add and remove manual dependencies. . . . 309
License API. . . . 312
Repository Management API overview. . . . 317
User management API overview. . . . 329
Workload Management API overview. . . . 372
Filters in an API request body. . . . 395
Whitelist file extensions to restrict upload of malicious files. . . . 402
Control room troubleshooting issues. . . . 403
Perform Enterprise Control Room health-check with Automation Anywhere diagnosis utility . . . 403
Troubleshooting bot deployment. . . . 404
Property to schedule triggers efficiently. . . . 404
Troubleshooting Automation File Permissions. . . . 405
Guidelines for General Data Protection Regulation. . . . 415

Using Enterprise Control Room

Enterprise Control Room is a central interface that allows you to manage and monitor all the processes of your RPA infrastructure

About • Bots - Overview • Dashboards overview	Setup • Getting started • Configuring Enterprise Control Room authentication options	For Administrators • Upgrade to a higher 11.x version • Post upgrade AD configuration
Using the Enterprise Control Room • Create and edit folders • Run a Bot • View Bot details	Development • Enterprise Control Room APIs • APIs to manage credential vault	Troubleshooting Troubleshooting Automation File Permissions

- Log on to Enterprise Control Room
  To log on to Enterprise Control Room, double-click the Automation Anywhere Enterprise Control Room icon on your desktop.
- Getting Started with Enterprise Control Room
  Here are some resources to help you get started with Enterprise Control Room.
- Administration Overview
  As a Enterprise Control Room admin you can use the administration module to complete the following tasks.
- Bots - Overview
  As a Enterprise Control Room user with administrator or My Bots privileges, you can use the bots module of Enterprise Control Room to do the following.
- Activity overview
  Use the Activity management page to view activities that are scheduled and are in progress. Also view a historical chronology of activities performed on a bot.
- Devices overview
  A device is an Automation Anywhere Enterprise client machine that connects you to the Enterprise Control Room to create or run bots.
- Workload overview
  Use the Workload Management page to divide your automations into small, yet logical work items. Process them simultaneously to ensure that time-based Service Level Agreements (SLAs) are met with optimum resource utilization. Additionally, integrate with a chat application to share the outcome of workload automation with your organization's customers.
- Bot Store integration overview
  The seamless integration of the Bot Store enables you to access Bot Store directly from the Enterprise Control Room. In the Enterprise Control Room, you can download bots and Digital Workers from Bot Store or create and package Digital Workers and bots to be uploaded to Bot Store.

©2020 Automation Anywhere. All rights reserved.

- Audit log overview
  Comprehensive and continuous audit logging capabilities in the Enterprise Control Room ensures enterprise-level security and quality compliance.
- Dashboards overview
  The Enterprise Control Room dashboard provides graphical insight into your RPA infrastructure so that you can analyze, interpret, and make informed decisions for your bots.
- Enterprise Control Room APIs
  The Automation Anywhere Enterprise Control Room provides various public APIs which allow you to customize your business automation for third-party applications.
- Whitelist file extensions to restrict upload of malicious files
  As a Enterprise Control Room Administrator you can add file extensions to the configuration file that restricts the user from uploading files that have extensions other than the ones whitelisted in it.
- Control room troubleshooting issues
  Known troublshooting issues and solutions related to the control room are documented here. Use the Send Feedback option at the bottom of every content page to provide constructive feedback and suggestions.
- Guidelines for General Data Protection Regulation
  The General Data Protection Regulation (GDPR) is one of the strictest compliance frameworks for maintaining privacy of personal data. The GDPR defines personal data as any data that can be used to identify a natural person (Data Subject).

Log on to Enterprise Control Room

To log on to Enterprise Control Room, double-click the Automation Anywhere Enterprise Control Room icon on your desktop.

The log on screens for Enterprise Control Room are different depending on whether it is hosted in Active Directory Kerberos mode or Non-Active Directory mode.

Note: Enterprise Control Room does not allow multiple sessions to the same account at the same time.

- Log on to Enterprise Control Room hosted in Single Sign On mode
  You can now provide your SSO credentials on the trusted identity provider (IdP) server page of your organization after the Enterprise Control Room is registered as a service provider with the IdP.
- Log on to Enterprise Control Room hosted in Non-Active Directory mode
  Type your credentials on the login screen to log in to the Enterprise Control Room hosted in a Non-Active Directory mode.
- Log on to Enterprise Control Room hosted in Active Directory/Kerberos mode
  To login to the Enterprise Control Room in Active Directory mode first select the domain and then enter your credentials.
- Log on to Bot Insight
  Bot Insight helps automation experts obtain real-time business insights and digital workforce performance measurements. Deployed bots generate, interact with, and process large amounts of data, which aids automation experts and consumers to interactively analyze task data and enhance widgets.
- Re-login to Enterprise Control Room when password policy is updated
  You must change your password when the Enterprise Control Room admin updates the password policy in Enterprise Control Room settings.

©2020 Automation Anywhere. All rights reserved.

- Reset LDAP user credentials
  When your LDAP user password expires or username is disabled or deleted, the Enterprise Control Room admin user must reset the credentials to enable you to login to the Enterprise Control Room.

Log on to Enterprise Control Room hosted in Single Sign On mode

You can now provide your SSO credentials on the trusted identity provider (IdP) server page of your organization after the Enterprise Control Room is registered as a service provider with the IdP.

To do that perform the following steps:

Procedure

1. Double-click the Automation Anywhere Enterprise Control Room icon on your desktop or type the Enterprise Control Room URL on your Web browser and press the Enter key.
   The Log in screen is displayed.
2. Click Login
   When your SSO credentials are authenticated through the IdP server page of your organization, on trying to login, you will be redirected to a trusted identity provider (IdP) of your organization (for example Okta) that has been preconfigured to accept authentication requests from multiple applications including the Enterprise Control Room.
   If the IdP Server URL is not valid or the server is down, you are shown appropriate message configured for it. For example, 404 or Bad Gateway.
3. Click Log In.
   You will be shown an error message and cannot log in:

   - If you provide incorrect credentials/IdP server credentials.
   - If your user account is disabled.
   - If you log in twice.

     You will be logged off the account you are logged into currently and asked to login again.
   - If your email address is not verified.

On successful authentication in the IdP server, you are logged into the Enterprise Control Room.

- You are automatically logged into the Enterprise Control Room if you open the Enterprise Control Room in the same browser or refresh the page as you are already authenticated by the IdP server.
- When you Logout (available when you click <username> in the profile) of the Enterprise Control Room, you are not logged out of other applications running with the same IdP Server.

Log on to Enterprise Control Room hosted in Non-Active Directory mode

Type your credentials on the login screen to log in to the Enterprise Control Room hosted in a Non-Active Directory mode.

©2020 Automation Anywhere. All rights reserved.

Procedure

1. Double-click the Automation Anywhere Enterprise Control Room icon on your desktop or type the Enterprise Control Room URL on your Web browser and press the Enter key.
   The Log in screen is displayed.
2. Enter your Automation Anywhere Enterprise (AAE) user name.
3. Optional: Select Remember my username to quickly login to the Enterprise Control Room.
4. Optional: Click Forgot password? to reset your password.
   - Admin users will have to provide answers to the security questions that were configured during user creation. After you provide correct answers, you are taken to the navigation page.
   - Non-admin users are directly taken to the change password page. If you provide incorrect credentials during log in, you are shown an error message.

   11.3.2 If using Automation Anywhere Enterprise Control Room Version 11.3.2 and higher, all users (admin and non-admin) have to provide answers to the security questions. After three incorrect attempts:
   a) Click the link sent to your registered email id for verification, if Email Notifications are enabled. See Configuring email notification settings.
   b) Fill in the CAPTCHA text to verify your credentials.
5. Type your Automation Anywhere Enterprise (AAE) password and click Log in.
   The credentials are authenticated directly with the CR database.
   Note:
   - Your account will be locked if you type the wrong password for a certain number of times depending on the password policy set by your administrator.
   - For security reasons, failed log in attempts are audited, which allows the administrator to analyze and take appropriate actions.

Log on to Enterprise Control Room hosted in Active Directory/ Kerberos mode

To login to the Enterprise Control Room in Active Directory mode first select the domain and then enter your credentials.

To log on to Enterprise Control Room hosted in Active Directory/Kerberos mode, perform the following steps.

Procedure

1. Double-click the Automation Anywhere Enterprise Control Room icon on your desktop or type the Enterprise Control Room URL on your Web browser and press the Enter key.
   The Log in screen is displayed.
2. In the Log in screen
   - For single forest multi-domain environment, do the following.
     - Domain: Select the domain of the Active Directory.
     - Username: Type your Active Directory user name.
     - Password: Type your Active Directory password.

       Click the Log in button. The log in details are authenticated directly with the Active Directory Domain Controller when you log in.

©2020 Automation Anywhere. All rights reserved.

- For Kerberos environment, click the Log in with Windows button.

  You do not need to enter your user name and password. You will be logged in with your current Windows account.

Note that,

- Your session will timeout in 20 minutes after you log in and the session is idle for that time period unless configured in settings. Refer details on login and session settings.
- Multiple sessions of the same user account is not allowed. If you are logged in at one instance and later log to another instance, for example different browser on same machine or different machine, you are allowed to log in with new session. However, when you perform a new request in the earlier session, you will be logged out.
- If the domain controller credentials, have expired, the list of domains is not available. To troubleshoot, refer Reset Active Directory credentials for details.

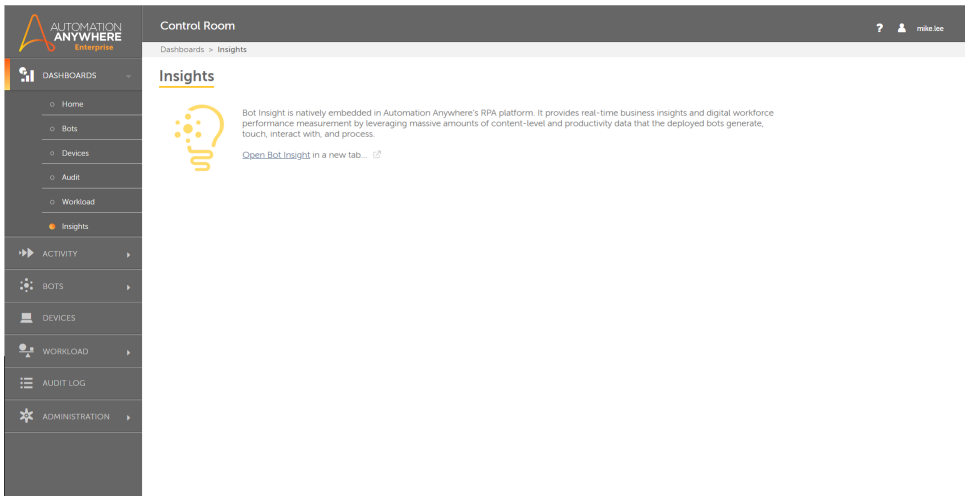
Log on to Bot Insight

Bot Insight helps automation experts obtain real-time business insights and digital workforce performance measurements. Deployed bots generate, interact with, and process large amounts of data, which aids automation experts and consumers to interactively analyze task data and enhance widgets.

When you are logged into one component of Automation Anywhere, you do not need to log into the other component. Single Sign On (SSO) automatically logs you into all the other components.

To use Bot Insight, the Enterprise Control Room must have Bot Insight licensing applied, and you must be logged in as a user with either `AAE_Bot Insight Expert` or `AAE_Bot Insight Consumer` roles.

In the Control Room, on the left pane, click DASHBOARDS > Insights.

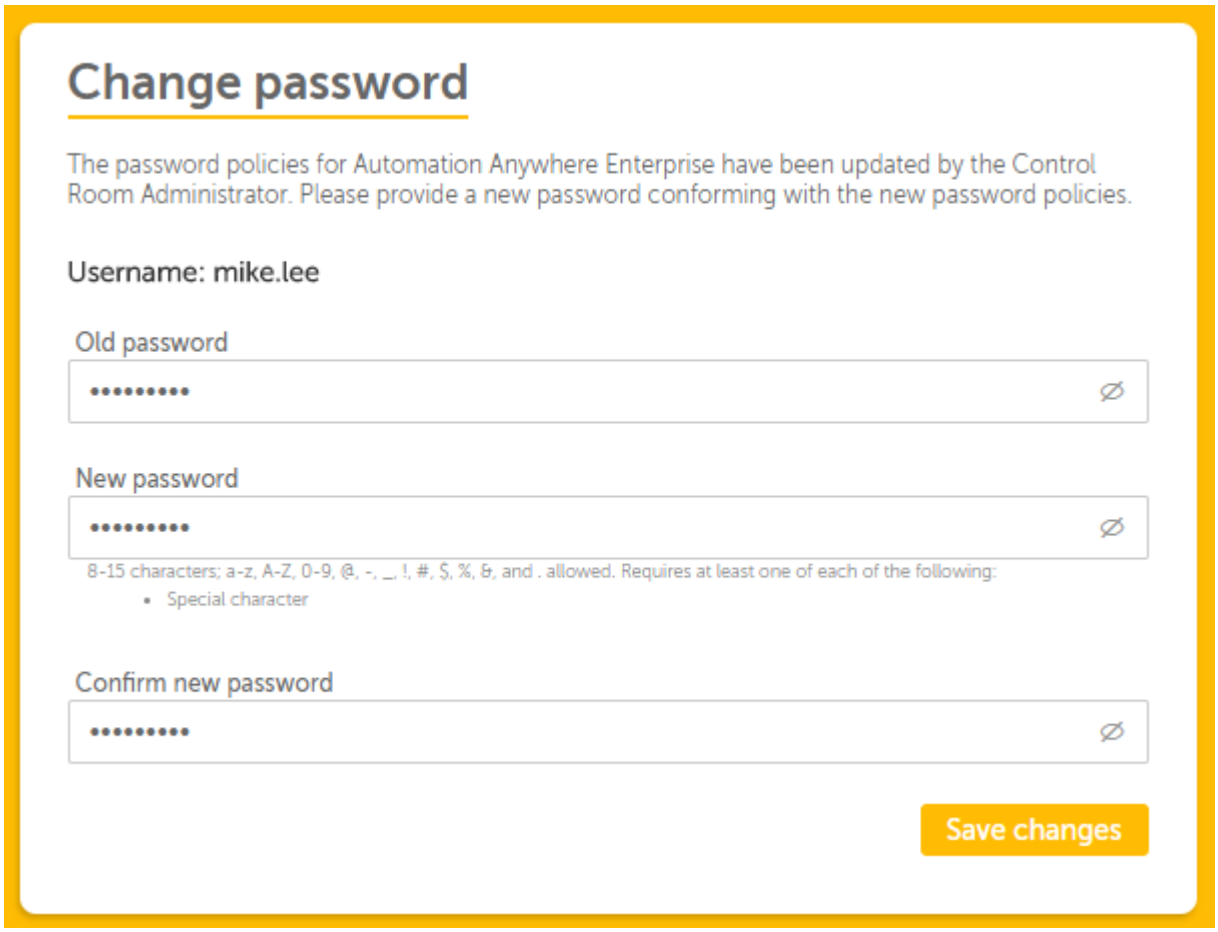


On the right pane, click Open Bot Insights. The system opens the Bot Insights application in a separate tab without the need for you to login again into Bot Insights.

Re-login to Enterprise Control Room when password policy is updated

You must change your password when the Enterprise Control Room admin updates the password policy in Enterprise Control Room settings.

If the policy is updated, next time you login to the Enterprise Control Room, the Change password screen is displayed, where you can update your password:



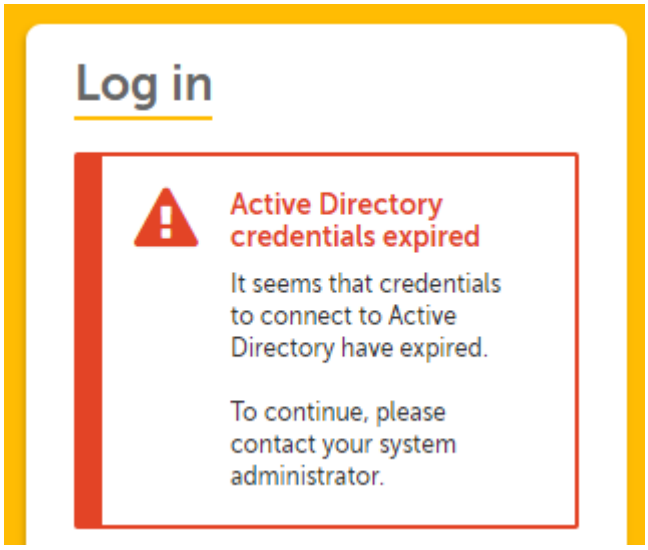
Click Save changes to login successfully.

Reset LDAP user credentials

When your LDAP user password expires or username is disabled or deleted, the Enterprise Control Room admin user must reset the credentials to enable you to login to the Enterprise Control Room.

When your LDAP user password expires or username is disabled/deleted, you will not be able to login to the Enterprise Control Room. In such cases, when a non-admin user tries to login to the Enterprise Control Room, following error message is shown:

©2020 Automation Anywhere. All rights reserved.



An Enterprise Control Room admin user must update the LDAP user's valid credentials after logging into the Enterprise Control Room.

Procedure

1. The admin user must enter credentials to login to the Enterprise Control Room.
   Ensure that the Username is in the NETBIOS\username format (example, domain.com\john.smith).
   After login the admin user will be directed to update the credentials of the LDAP user.
2. Enter the Domain username and password.
   Ensure that the Domain username is in the UPN (userPrincipleName) - username@domain.com format. Domain username in domainname\username format is not supported. For example, john.smith@aaspl-brd.com is supported; whereas, aaspl-brd\john.smith is not supported.

   11.3.2 In Version 11.3.2, after entering the username and password in the Change Active Directory configuration page, you can either enter the LDAP URL(s) manually by selecting Manually add connections or chose to Discover connections automatically.

Getting Started with Enterprise Control Room

Here are some resources to help you get started with Enterprise Control Room.

- Enterprise Control Room interface
- Configuring Enterprise Control Room for the first time
- Logging on to Enterprise Control Room
- Adding users to your installation of Enterprise Control Room
- Assigning roles to the users you have created

- Enterprise Control Room overview
  The Enterprise Control Room is the brain of the digital workforce platform. It is a Microsoft Windows server-based web application providing a single administrator interface for Enterprise-wide bot deployment, management, and control.

©2020 Automation Anywhere. All rights reserved.

- Enterprise Control Room interface overview
  The Enterprise Control Room interface provides multiple options to manage and monitor the different components of the RPA infrastructure.

Enterprise Control Room overview

The Enterprise Control Room is the brain of the digital workforce platform. It is a Microsoft Windows server-based web application providing a single administrator interface for Enterprise-wide bot deployment, management, and control.

Enterprise Control Room provides automated provisioning, orchestration, governance, and actionable analytics for Enterprise-wide implementation.

Why use Enterprise Control Room?

- Leverage multiple authentication options of Active Directory using LDAP, Active Directory using Kerberos, local authentication using the embedded Credential Vault, and Single Sign-On using Security Assertion Markup Language (SAML) 2.0.
- Ensure the secure digital workforce platform based on granular role-based access control (RBAC) and industrial grade encryption for data at rest and in transit.
- Control remotely running automations centrally.
- Access built-in version control feature for multi-user collaboration.
- Store system-managed credentials and critical system configuration data using secure Credential Vaults.
- Enforce best practices to meet stringent compliance mandates using Bot Lifecycle Management (BLM).

What you must know about access control, management, and monitoring

Access control

As an administrator, define custom roles and set permissions for the full suite of Enterprise Control Room objects and functions, including user management, licensing, Credential Vault, bot schedules, dashboards, and audit logs.

See Roles overview and User management overview for more information.

Centralized management

Meet the demands of dynamic service level agreements (SLAs) using dynamic workload management (WLM) for industrial-scale automation. WLM includes built-in SLA calculators with a human-in-the-loop flexibility to enable prioritization of high-value task queues.

See Workload overview for more information.

Monitor using reports

Capture event details for user and entity actions including the creation, modification, enablement, disablement, and removal of users, bots, Bot Creators, and Bot Runners.

Customize automated dashboards and reports to identify and alert you about abnormal activities. Export logs to use other analysis, reporting, and incident investigation/response infrastructure already in use by the organization, for example, Security Information and Event Management (SIEM) and advanced analytics tools.

©2020 Automation Anywhere. All rights reserved.

See Audit log overview and Dashboards overview for more information.

Enterprise Control Room interface overview

The Enterprise Control Room interface provides multiple options to manage and monitor the different components of the RPA infrastructure.

The Enterprise Control Room interface contains the following components:

- Navigation pane: Navigate to Dashboards, Activity, Bots, Devices, Workload, Audit log, or Administration. Each view differs depending on the assigned roles and permissions.
- Details area: View details of users, roles, bots, and so on, depending on the selected option. Create, edit, and delete single or multiple records.

  Navigational breadcrumb trail appears at the top. Use it to return to a previous view.

- Search and filter: Search or filter data shown in the Details area, and the results are shown in tables. The Control Room displays the last filter applied by each user for every session. The search feature is available on all pages of the Enterprise Control Room, including Bot Insight.
- Help: Access links to the following resources:
  - Help with the current page
  - Online documentation
  - Automation Anywhere Support
  - Automation Anywhere Sales
  - Automation Anywhere website
- 11.3.2 Language: Click the globe icon to choose a non-default language for the Enterprise Control Room interface.
- Profile: Personalize and maintain your Enterprise Control Room profile by selecting Edit Profile, Change Password, or Generate API-Key.
  - Change your password: Provide your new password in the Change password form.
  - Edit your profile: Update your first name, last name, or email address in the Edit Profile form.
  - 11.3.2 Generate API-Key: Create the API key to use for authentication when using the Enterprise Control Room Authentication API. This link is available only if the Enterprise Control Room admin user assigns the Generate API-Key permission to a user role.

    If a user generates a new API key when an API key is already available, it is overwritten. The user can copy the key and use it for authentication for an API call.

  Note: The process of managing your profile is different for an Enterprise Control Room configured with an Active Directory and one with a non-Active Directory environment. Users cannot configure or make changes to their profile in an Active Directory environment. Users configured with a non-Active Directory environment can change the password, first name, last name, and email address.

Administration Overview

As a Enterprise Control Room admin you can use the administration module to complete the following tasks.

©2020 Automation Anywhere. All rights reserved.

- Manage roles by creating, editing, deleting, and viewing existing roles
- Manage users by creating, editing, deleting, and viewing existing users
- Change the general settings of Enterprise Control Room
- Purchase an extended license or install a new license

- Settings overview
  As a Enterprise Control Room administrator, you can customize the Enterprise Control Room by configuring settings related to the database, Credential Vault, version control, and so on.
- User management overview
  As an Enterprise Control Room admin, you can create, view, edit, delete, and enable or disable user accounts. Creating user accounts depends on the non-Active Directory, Active Directory, or single sign-on (SSO) credentials from an IdP server.
- Roles overview
  Administrators or users with roles permission can create, edit, and delete roles for various features and operations in the Enterprise Control Room.
- Licenses - an overview
  The Enterprise Control Room License page provides detailed information about the current license that is installed. It also enables the Admin user to monitor license details and usage statistics.
- Migration overview
  Migration is moving data using a systematic and phased process from Automation Anywhere v10.x to v11.x.x. As an Enterprise Control Room administrator with View and Manage Migration permissions, use the Migration Wizard tool to migrate data.

Settings overview

As a Enterprise Control Room administrator, you can customize the Enterprise Control Room by configuring settings related to the database, Credential Vault, version control, and so on.

- Configuration settings
- Bots
- Client applications
- Credentials
- Email
- 11.3.2 Configuring Syslog service
- 11.3.2 Configuring Active Directory Settings
- Enabling Two-factor authentication
- Managing domains

- Enterprise client application settings from Enterprise Control Room
  As an Enterprise Control Room administrator, you can configure settings relevant to your Enterprise client application.
- Configuration settings
  As an administrator, view and manage settings that are configured for the Enterprise Control Room.
- Configuring email notification settings
  Enterprise Control Room administrators can enable email notifications to users for certain activities such as account activation or deletion and changes to account information.
- Bots: Configure version control
  To control edits to files that might include TaskBots, MetaBots, docs, reports, scripts, exe files, and workflows, as an Enterprise Control Room admin, you can configure version control in the Enterprise Control Room settings.

©2020 Automation Anywhere. All rights reserved.

- Configuring Syslog service
  Configure the Enterprise Control Room to export Audit Log entries in Syslog format to remote Syslog compatible log management servers.
- Configuring Active Directory Settings
  As a Enterprise Control Room administrator you can edit the Active Directory configuration setting to either discover the available domains and sites automatically (auto mode) or manually enter the LDAP URLs (manual mode).
- Enabling Two-factor authentication
  Administrators can enable two-factor authentication (2FA) for users logging in to the Enterprise Control Room. 2FA provides a layered defense against any unauthorized users from accessing the database.
- Sequence to stop and start Enterprise Control Room services
  To restart the Enterprise Control Room services, you must stop and start the services in a specific sequence.

Enterprise client application settings from Enterprise Control Room

As an Enterprise Control Room administrator, you can configure settings relevant to your Enterprise client application.

You can perform these actions:

- Enable or disable secure recording
- Update settings to allows passing Credential Vault variables from one bot to another
- Change product help URLs
- Configure device health checks
- Configure audit entry to view local bot run
- Select time zone for scheduling a bot
- Turn Bot Insight on by default
- Tag Bot variables for data output
- 11.3.4 Automatically update bots and dependent files on attended Bot Runner machines

To configure the settings, log in to the Enterprise Control Room as an administrator, navigate to the Administration > Settings > Client application, and select the Edit option.

Secure recording

Secure recording offers you a choice between capturing or not capturing images and control values during business process recording by Bot Creators. For example, enable secure recording when automating secure applications such as bank accounts.

To modify secure recording settings:

1. Select Client application.
2. Click Edit.

   The page opens in edit mode. Secure recording is Off by default.

3. Select Secure recording is On.
4. Click Save changes.

©2020 Automation Anywhere. All rights reserved.

Pass Credential Vault variables to MetaBot

Control passing Credential Vault variables through the Pass Credential Vault variable to MetaBot setting. This setting enables passing credential variables stored in the Credential Vault from TaskBots to MetaBot Logic and from one Logic to another Logic in the same MetaBot.

Default setting is On.

To modify:

1. Select Client application.
2. Click Edit.

   The page opens in edit mode. Passing of Credential Vault variables to MetaBot is On.

   As the Bot Creator, to pass a credential variable from the TaskBot to a MetaBot Logic:

   a) From the MetaBot page, open Insert Variable panel.
   b) Select a variable and click Insert.

   The variable is added to the MetaBot Logic panel Input Parameters table.

3. Select Off to prevent the bot from passing the variable to another bot.
4. Click Save changes.

Product help URLs

Product help URLs allow you to redirect links to Automation Anywhere Support Site or to any Custom URL of your choice.

- Use Automation Anywhere URLs: Use this to navigate your users to the default Automation Anywhere Support site. This disables all the other options such as Live Chat with Support URL etc.

- Use Custom URLs Use this to navigate your users to your custom defined URLs for Product help. This allows your users to seek help from in-house automation experts.

- Use Product help URLs Use Product help URLs as described in the table.

URL	Description
Automation Anywhere Enterprise client application support	It allows you to add your customized Product Help URL and redirect users to your in-house support site.
Live chat with support	It allows you to access in-house Live Chat and speak to online Experts.
Example online	It allows you to look for available Online Examples.
Request live 1-on-1 demo	It allows you to request for live demonstration of features and experts would answer your questions.
Technical support	It allows you to access in-house Technical Support.

©2020 Automation Anywhere. All rights reserved.

Ask the expert	It allows you to speak to an expert and get their expert advice.

To modify the product help URL settings:

1. Select Client application.
2. Click Edit.

   The page opens in edit mode. Use Automation Anywhere URL is selected by default.

3. Select Use Custom URL as required.

   To redirect live chat support to a specific chat group, use HTTP in the URLs.

4. Click Save changes.

Device health check configuration

Set the time interval for Device Health checks for parameters such as CPU, Memory, and Disk usage. Set the frequency for data exchange between the Enterprise Control Room and connected Enterprise clients.

To modify Device health check configuration

1. Select Client application.
2. Click Edit.

   The page opens in edit mode. The Blip interval during bot execution default value is set to 60 seconds.

3. Enter a Blip interval time in seconds. The minimum value is 60 seconds. The value cannot be empty.
4. Click Save changes.

Local Bot Run Audit

To audit local bots run by the Bot Creators or Bot Runners, enable the setting in the Enterprise Control Room. When enabled, the Enterprise Control Room audits the bot run by the user on the Enterprise client machine.

Initiate a local bot run from the local Enterprise client machine by:

- Pressing the Run button on the Automation Anywhere Main Client or Workbench
- By Hotkey
- By Local Schedule
- By Local Trigger
- By Workflow

The entry in Audit Logs depicts the Action type as Run Bot (Local Client) started and Run Bot (Local Client) finished.

Audit Log details include:

- Description of bot action. For example, Run Bot (Local Client) started
- Status. For example, successful
- Action taken by. Name of user

©2020 Automation Anywhere. All rights reserved.

- Object type. For example, Action
- Source device. Name of machine
- Request ID. ID assigned to the action.
- Item name. Bot name
- Time. Timestamp of hour, minutes, seconds, timezone, and date
- Action type. For example, started
- Source. For example, client

Bot Insight configuration

Use Bot Insight setting to allow a Bot Creator to tag bot variables for analysis.

By default, Analytics tagging for Bots is set to Off.

To modify, select On. This enables the setting in the Add Variable window. See Create new variables.

The Bot Insight Configuration setting requires that a Business Analytics license or trial license is applied to the Enterprise Control Room.

API Deployment Configuration

11.3.2 Use API deployment configuration setting to allow a Bot Creator to tag the bot variables for data output.

11.3.2 By default, Allow bot output is set to Off.

11.3.2 To modify, select On. This enables the Include in Output check box in the Add Variables window. From there, the value of variables can be passed as output when the bot is deployed by the Bot Deployment API. See Create new variables.

Tip: 11.3.4 Use the Bot Execution Orchestrator > Activity > List API to view the output.

Whitelist File Extensions to Prevent Uploading of Malicious Files

To prevent uploading of malicious files on the Enterprise client, the Enterprise Control Room administrator uses Whitelisted file extensions feature.

As the Enterprise Control Room administrator, add file extensions to be whitelisted from the Enterprise client. Enterprise client users can upload only whitelisted file extensions included in this list.

Whitelist file extensions to restrict upload of malicious files

11.3.4 Automatically update bots

In the Automatic Update section, choose to automatically update bots and their dependent files when the are run on Attended Bot Runner machines.

- Select the option On to automatically update.
- Select the option Off to manually update.

©2020 Automation Anywhere. All rights reserved.

Note: By default, the Attended Bot Runners are allowed to Download the updated bots and dependent files manually using the Parent Tasks option in the Enterprise client.

Modification details

The modification details such as Modified by and Last modified date/time are captured. The Enterprise client application tab shows System and the Enterprise Control Room installation/configuration date and time by default when you launch the Settings page.

Audit Logs

All updates to the Enterprise client application settings are captured in the Audit Log page.

To view details of each audit entry:

1. Go to the required data and mouse in Settings.
2. Click View details.

   The Edit Settings Details panel is launched within the Audit log page. Only those setting that changed are listed in the details panel. The panel lists the changes in a table that includes: What Changed, Old Value, and New Value.

Related tasks
Create new variables
Whitelist file extensions to restrict upload of malicious files

Configuration settings

As an administrator, view and manage settings that are configured for the Enterprise Control Room.

To view the following configuration details, go to Administration > Settings > General:

- Enterprise Control Room installation type, access URL, and the program files destination folder from the Enterprise Control Room.
- Website security and configuration details, Enterprise Control Room users, database and repository details, deployment settings, and security details in the Enterprise Control Room database and software.

General settings

The general settings tab provide information about the installation type, the access URL, and the program files' destination folder. You cannot edit these settings as they are configured during installation.

The following table describes the general settings:

Settings	Description
Enterprise Control Room Installation type	The type of setup used to install the Enterprise Control Room: either `Express` or `Custom`. This setting is configured during installation and is not editable.

©2020 Automation Anywhere. All rights reserved.

Settings	Description
Enterprise Control Room access URL	The fully qualified name of the server that is used by the Bot Creator, Bot Runner, and users to access the Enterprise Control Room. Use the Enterprise Control Room access URL in the following scenarios: • For IQ Bot app registration in the Enterprise Control Room, use the access URL. • For all the SMTP alerts from the Enterprise Control Room, send the saved access URL. • For SSO, the access URL should be the load balancer, or the URL used to set metadata in the IDP server. Opt to change the access URL if the Enterprise Control Room is set up in custom mode. To modify the URL, perform these steps: 1. Click Edit. The General Settings page opens in edit mode. 2. Type the fully qualified name of the URL to access the Enterprise Control Room. 3. Click Save changes.

Edit and view Enterprise Control Room database and software configuration

The Enterprise Control Room database and software settings provide details about website security and configuration, Enterprise Control Room users, database, and repository, deployment, and security settings. Edit the settings for the Enterprise Control Room repository, deployment, and password.

The following table describes the Enterprise Control Room database and software settings:

Settings	Description
Website security	The type of security protocol used: `http` or `https`. This setting is configured during installation and is not editable.
Website configuration	The website configuration details such as the web server host name. If the Enterprise Control Room is configured for Express installation, only one host name is shown. If it is configured for Custom installation, multiple host names are shown. This setting is configured during installation and is not editable. The web server host name and port details of all registered and active users are listed. However, the user name and password values are not shown.
Enterprise Control Room users	The authentication type used to log in to the Enterprise Control Room instance by bots. It can be Active Directory, single sign-on (SSO) SAML, or database. This setting is configured during installation and is not editable.

©2020 Automation Anywhere. All rights reserved.

Settings	Description
	• Active Directory users are configured when bots of a specific domain have to be authenticated with their Active Directory credentials. • Single sign-on (SAML 2.0) users are configured when bots have to be authenticated using SAML 2.0 protocol and users have to log in using the organizations' IDP server credentials. • Database users or non-Active Directory users are configured when bots have to be authenticated using the Enterprise Control Room database.
Enterprise Control Room database	Shows the settings for: • 11.3.2 Database type: The database selected (SQL Server or Oracle) for storing Enterprise Control Room data. • Windows authentication: The authentication type used to connect to the database server. It shows Enabled when Windows authentication is selected for database configuration during installation. It shows Disabled when the default database authentication is used. • Server host name: The fully qualified name of the Enterprise Control Room database server. • Server port: The port to which the database is configured. 11.3.2 The default listening port number for SQL Server is 1433, Oracle is 1521, and Oracle with SSL is 2484. • Database name: The database that is used to store Enterprise Control Room data. 11.3.2 For Oracle, this is the database instance name that was created initially by the system admin. • Username: The SQL Server user name if the SQL Server authentication type is selected. If Windows authentication is selected, no value is displayed. 11.3.2 If Oracle is selected as the database, the value displayed is the Enterprise Control Room Username that was created initially by the system administrator. This setting is configured during installation and is not editable.
Enterprise Control Room repository	The location where all bots, application files, and supporting files are stored. The default path is set to C:\ProgramData\AutomationAnywhere\Server Files during installation, if this is not updated during installation. You can modify this path after installation through this setting. To modify, perform these steps: 1. Click Edit.

©2020 Automation Anywhere. All rights reserved.

Settings	Description
	The page opens in edit mode. 2. In the Repository path field, enter the location of the repository ending with `Server Files`: • Use the Network Drive folders for the repository path. • If you enter an invalid pathname, an error is displayed. 3. Click Save changes. 4. Stop these services for each node: • Automation Anywhere Control Room Caching • Automation Anywhere Control Room Messaging • Automation Anywhere Control Room Service Your devices will be disconnected from the Enterprise Control Room instance. 5. Copy all the files from the old repository to the new repository. 6. Restart these services for each node: • Automation Anywhere Control Room Caching • Automation Anywhere Control Room Messaging • Automation Anywhere Control Room Service
Session settings	• 11.3.5 The login settings enable you to automatically time out users from the Enterprise Control Room browser session after the specified minutes of inactivity. By default, this setting is Enabled and the default value for inactivity time is set to 20 minutes. To modify the setting, perform these steps: 1. Click Edit. The page opens in edit mode. 2. Enable or disable the session timeout for users by selecting Enabled or Disabled. If you select Enabled, specify the inactivity time in the range of 10 - 60 minutes. The change in the session timeout is updated only after a new token is generated. • The session settings allow or disallow users to be automatically logged in to the Enterprise Control Room when they navigate to the Enterprise Control Room URL through a browser if the Enterprise Control Room is configured for Kerberos-enabled Active Directory authentication. By default, this setting is Enabled.

©2020 Automation Anywhere. All rights reserved.

Settings	Description
	• To modify the setting, perform these steps: 1. Click Edit. The page opens in edit mode. 2. Select Enabled or Disabled to enable or disable auto-login for users to the Enterprise Control Room. • 11.3.4 The notification settings display a notification when a user with an active Enterprise Control Room login session tries to log in to the Enterprise Control Room from a different browser or device. By default, this setting is Disabled. To modify the setting, perform these steps: 1. Click Edit. The page opens in edit mode. 2. Select Enabled or Disabled to enable or disable the notification. Note: This feature is supported in only a non-Active Directory environment.
Deployment settings	Bot Runner deployment session: Shows whether users with run and schedule privileges are allowed to run a Bot Runner session on Enterprise Control Room when you deploy or schedule a bot. See Run a bot and Schedule a Bot. By default, this setting is Enabled. To modify the setting, perform these steps: 1. Click Edit. The page opens in edit mode. 2. Select Enabled or Disabled as required for the Bot Runner deployment session on the Enterprise Control Room.
11.3.2 Deployment settings	Callback URLs: Allows a user to configure known callback URLs for the Bot Deployment API to send the bot status and the bot output from variables after the bot has finished execution. To modify the setting, enter the Callback URL in the field and save your changes.
Security	This field defines the password policy settings for all Enterprise Control Room users. Customize the password length, password content, select the number of log-on attempts allowed, and enable or disable security-related questions and answers.

©2020 Automation Anywhere. All rights reserved.

Settings	Description
	The password policy is applicable for an Enterprise Control Room that is configured for Database authentication type. To modify this, perform these steps: 1. Click Edit. The page opens in edit mode. 2. In the Password length field, specify the Minimum and Maximum characters based on your company policy. This can include any or all Alphabetical character, Number, Capital letter, and Special character. 3. Specify the number of login attempts allowed before the user account is locked. Note: The user account is disabled in the Enterprise Control Room if it is locked out. You cannot type invalid values in the following: • Password length field • Log on attempts field 4. 11.3.2 Choose either Enabled or Disabled for security questions and answers. When the option is enabled, users provide answers to security-related questions when they click the Forgot password link. 5. Save changes.
Elasticsearch disaster recovery backup cluster	This field defines the disaster recovery server IP address for Elasticsearch disaster recovery. Enter the IP address for your Automation Anywhere Enterprise disaster recovery site. Elasticsearch is installed on the same server as the Enterprise Control Room.
11.3.2 API key duration	This defines the validity of the Authentication API key, in days or minutes, for a user. To specify the duration or validity of the API key in either day(s) or minute(s), click the plus and minus sign. • Default value is set to 1 day and the maximum limit is 45 days or 64800 minutes. • Validity of an existing API key for an authorized user is not affected if the Enterprise Control Room admin changes the duration. For example, when a user is authorized to use the API key for 2 days and the admin updates it to 5 hours in the interim, the user is allowed to use the API key for 2 days. However, an API key created after that is valid for 5 hours.

©2020 Automation Anywhere. All rights reserved.

Audit logs

All updates to the configuration settings are captured in the Audit Log page and all the actions performed to edit the general settings.

To view details of each audit entry:

1. Go to the required data and move your mouse over view details icon.
2. Click on the view Audit details icon.
3. View the entries that are changed in the details page that is launched.

   To view the details for successfully disabling a Bot Session, open the Enterprise Control Room and go to the password policy setting.

- Configure Credential Vault Connection Mode
  Credential Vault is a centralized location for securely storing credential information used by bots.

Configure Credential Vault Connection Mode

Credential Vault is a centralized location for securely storing credential information used by bots.

As a Enterprise Control Room admin, you can configure the Connection mode that allows you to connect to the Credential Vault using a Master key.

The connection mode is first configured during Enterprise Control Room's initial setup as illustrated below:

You can view the Connection mode details in Settings > Credentials .

To configure settings for Credential Vault, you have to choose between Express or Manual mode.

- Express Mode - Use this to auto connect to the Credential Vault with the master key that is stored in the system during Enterprise Control Room configuration.

- Manual Mode - Use this to manually connect to the Credential Vault using the master key that was available during Enterprise Control Room configuration.

  Note: You will have to provide this key every time you start or restart the Enterprise Control Room.
- Compared to Express, the Manual mode is more secure and recommended for use in production environment.
- While switching modes, you must provide the Master Key in the field and click Save for the changes to take effect.
  Note: An error message prompts if you do not enter a valid master key or the field is empty.
  Tip: Restart the server machine (on which the Enterprise Control Room is installed) or services to allow changes to take effect.

Audit Log

All updates to the Credential Vault connection mode are captured in the Audit Log page. For example, the following illustration lists all actions performed to connect and edit connection settings to the Credential Vault :

©2020 Automation Anywhere. All rights reserved.

To view details of each audit entry:

1. Go to the required data and mouse in Settings.
2. Click View details.

   The details page is launched. The illustration below shows details of successful Credential Vault connection switch from Express to Manual mode:

Configuring email notification settings

Enterprise Control Room administrators can enable email notifications to users for certain activities such as account activation or deletion and changes to account information.

Procedure

The following instructions help you configure the email notification settings:

1. Log in to the Enterprise Control Room and click Administration > Settings > Email.
2. Click Edit.
3. Select the Send email notifications check box.
   Note: If this check box is enabled, Send verification email on first time user setup is activated by default, and the user receives an account activation acknowledgment email.
4. Update the following details:
   a) From this email address is the address from which the notification is sent to the user.
   b) Email server host is the host name of the email server.
   c) Email server port is the port number between 1 and 6553.
   d) My server uses a secure connection (SSL/TLS): Select this check box if you have enabled the SSL/TLS protocol.
   e) My server requires authentication is enabled by default.
   f) Username and Password are the SMTP credentials.
5. Select any of the following conditions to send the email:
   - User initiates Forgot Password process from Login screen: An email notification is triggered when you a user clicks the Forgot Password link on the login screen.
   - User information changes, to the user: When you update the first name and last name of a user, an email notification about the user account information is sent.
   - Send verification email on first time user setup: Is enabled by default, and when a user account is set up for the first time, the user receives an email with a verification link. The user must click this verification link and set the login credentials for the Enterprise Control Room.

     If you disable this feature (clear the check box), user receives a welcome email without a verification link and can log in to the Enterprise Control Room through one of the following methods:

     - The credentials provided by the admin, if it is an Enterprise Control Room DB authenticated environment
     - Windows credentials, if it is an Active Directory environment
     - SSO credentials, if it is a SAML-enabled environment
   - A user is activated, deactivated or deleted: The user receives an email notification when you activate, deactivate, or delete their account.
   - A TaskBot stops running because it is unsuccessful, to the user who started or scheduled it: If a user schedules a bot to run on a Bot Runner machine and the bot fails to deploy or execute

©2020 Automation Anywhere. All rights reserved.

because it was stopped, timed out, or encountered an error, the user receives an email notification.
- A BLM package is exported or imported, to the user who performed BLM export or import: When a user exports or imports a BLM package, an email notification providing the status is triggered.

6. Click Save changes.
   a) To disable notifications, clear the Send email notifications check box and save changes.
   b) All updates to the email notification settings are captured in the Audit Log page.
7. To view details of each audit entry, point to the vertical ellipsis icon for the required data, and click the Audit Details icon.
8. View the changed entries in the details page that is launched.

Bots: Configure version control

To control edits to files that might include TaskBots, MetaBots, docs, reports, scripts, exe files, and workflows, as an Enterprise Control Room admin, you can configure version control in the Enterprise Control Room settings.

The Enterprise Control Room is integrated with Subversion Version Control so that the version, checkin or checkout, version history, and version rollback functionality can be leveraged with ease for all files. By default, the feature is disabled.

Version control prerequisites

- For version control to be enabled and integrated from the Enterprise Control Room, the SVN server must be installed and configured.
  Note: Automation Anywhere Enterprise Control Room supports various versions of the SVN. See Version control requirements.
- SVN administrator user should be created with required permissions.
- SVN repository should be created, which can be used to store all version control files.

  Reusing an SVN repository that is not empty for multiple Enterprise Control Room instances, such as development and UAT environments, might delete version details and the history of existing bots. If the Enterprise Control Room instances for development and UAT are different, then either reuse an empty SVN repository or create a new SVN repository.

  Note: After the Enterprise Control Room integration with SVN is up and running, all communication for version control operations from the Automation Anywhere Enterprise client to SVN take places only through the Enterprise Control Room.

Impact of enabling and disabling version control settings

When you enable and disable version control settings in the Enterprise Control Room, it affects the way the Enterprise client can access bots and upload those to the Enterprise Control Room. While enabling and disabling this setting, ensure you are aware about its impact, which is summarized in the following list:

- When you enable version control settings, the system uploads the bots from the Enterprise Control Room repository to the SVN repository.

  During SVN syncing, the Enterprise Control Room repository is in read-only mode and locked. You will not be able to perform actions such as upload, delete, set production version, checkout, checkin, undo checkout, and force unlock.

©2020 Automation Anywhere. All rights reserved.

- When you disable version control settings, the files that are in checked-out state are listed for force unlock by the Enterprise Control Room administrator. You are allowed to disable the settings only when you unlock the checked-out files.
- When you reenable version control settings, you can:
  - Connect to the repository where you uploaded the bots earlier. Version history of existing bots is also retained. As a result:
    - The version of the bots that are not updated remains the same.
    - A new version of the updated bots is created.
    - Production version is not set if the option Do not assign production version. I will do so manually is selected.
    - Production version is set to latest versions of the bots if the option Automatically assign the latest version of bots to production version is selected.
  - Connect to a new repository that is not empty. Your version history of the earlier repository is not retained. Also, you can choose to set the production version manually or automatically.

All updates to the Version control system settings are captured in the Audit Log page.

- Enabling Version Control
  You can upload the bots from Enterprise Control Room repository to SVN repository by enabling version control settings.

Enabling Version Control

You can upload the bots from Enterprise Control Room repository to SVN repository by enabling version control settings.

To enable version control for bots follow the steps given below:

Procedure

1. Select Administration →Settings →Bots
2. Click Edit.
   The page opens in edit mode.
3. Select Enabled.
4. Enter the following details:
   a) Subversion server name - Provide hostname of subversion server.
   b) Subversion repository path - Provide the SVN repository path.

   The Subversion repository path is case sensitive. For example, if your repository path is \svn \V11SVNRepo and you enter \SVN\V11SVNRepo, the Enterprise Control Room will not be able to connect to the Subversion Server.

   The SVN repository must be empty if you are enabling these settings or switching from an old configured repository to new SVN repository.

   You can configure only upto three levels of repository path.

   Tip: You can copy these details from the VisualSVN Server Manager as shown.
5. Select option for assigning bot production version manually or automatically when you enable version control or configure version control to another Subversion repository.

©2020 Automation Anywhere. All rights reserved.

The production version of a bot is must for a schedule to run on the selected bot, Your schedules will not be triggered unless the scheduled bots have their production versions set.

- Use Do not assign "Production versions." I will do so manually when you want to manually assign a production version for bots. Use this option when you want to set production versions in a controlled manner.

- Use Automatically assign the latest version of a bot to be its "Production version" when you want the Enterprise Control Room to automatically select the latest version of bots to production version.

6. Select Connection Type under Server settings.
   You can select any of the following protocols to connect to SVN:
   - http - This is the default option
   - https - This can be selected when the SVN is configured to use the https protocol
   - svn+ssh - This option can be selected when the SVN is configured to use the SSH protocol. This option is recommended as it allows for faster and more secure processing of version control operations.
7. Provide the Subversion server port number that is assigned for SVN.
   Ensure the port number is between 1 and 65535.
8. Provide your SVN Login credentials - Username and Password.
   The details for Subversion path and Files last uploaded are updated after you configure version control. The default path of Enterprise Control Room files is also displayed.
9. Save changes.
   Note: If VCS was earlier configured and you switch to a different Subversion repository, the bot version history is not stored. See Impact of enabling and disabling version control section for details.

11.3.2

Configuring Syslog service

Configure the Enterprise Control Room to export Audit Log entries in Syslog format to remote Syslog compatible log management servers.

Prerequisites

Ensure the Syslog servers are configured and ready.

Pushing Audit Log entries to remote Syslog servers enables you to integrate and leverage advance searching and reporting features of security information and event management (SIEM) solutions. To configure server(s) where audit records will be sent in standard Syslog format do the following:

Procedure

1. Navigate to Administration > Settings > Syslog Service.
2. Click Edit.
3. Click the plus icon.
4. Enter the following Syslog server details.

Name	Description
Syslog Server Hostname	Fully Qualified Domain Name (FQDN) or IP Address of the remote Syslog server to send records.

©2020 Automation Anywhere. All rights reserved.

Name	Description
Port	Port that the remote Syslog server uses to receive incoming Syslog records (for example, 514)
Protocol	Network protocol that the Syslog server uses (TCP or UDP)
Use Secure Connection	Use a TLS encrypted channel to send Syslog records to the remote server. This option is available for TCP protocol only.

5. Click the plus icon to add more servers and enter server details.
6. Click Save changes.

Next steps

After you configure the Syslog server(s) in the Enterprise Control Room, each time there is an entry recorded in the Audit Log, a corresponding message is generated and sent to the configured Syslog server. Older entries of the Audit Log will not be available in the Syslog server.

11.3.2

Configuring Active Directory Settings

As a Enterprise Control Room administrator you can edit the Active Directory configuration setting to either discover the available domains and sites automatically (auto mode) or manually enter the LDAP URLs (manual mode).

Prerequisites

Here are some points to consider before you switch from one mode to another:

- If you switch from manual to auto mode, all discovered domains and sites are shown as selected. However, some of the manually entered URLs might be lost during discovery.
- If you switch from auto to manual mode, the previously discovered LDAP URLs will be pre-populated. You can add/remove URLs as required.

To change the configuration mode do the following:

Procedure

1. Navigate to Administration > Settings > Active Directory.
2. Click Edit.
3. Enter the Domain username and password
4. Select Manually add connections or Discover connections.
   If you select Discover connections, Enterprise Control Room retrieves all domains and sites from all forests to which the domain user has access.
   If you select Manually add connections, previously provided LDAP URLs are shown.
5. Edit the LDAP URLs if you have opted to add connections manually. Or, select/unselect the Domains and sites if you have opted for the Enterprise Control Room to discover connections.

©2020 Automation Anywhere. All rights reserved.

If you decide to continue with the auto mode, previously selected domains and sites will be shown as selected.
If only one domain and one site under it is discovered, then it is shown in read-only mode and cannot be edited.

6. Click Save and continue.

In the Active Directory configuration page, if the configured mode is Auto, the configured domains and sites are shown along with the configured URLs. And if the configured mode is Manual, the configured URLs are listed.

Enabling Two-factor authentication

Administrators can enable two-factor authentication (2FA) for users logging in to the Enterprise Control Room. 2FA provides a layered defense against any unauthorized users from accessing the database.

Two-factor authentication, a subset of multi-factor authentication (MFA), provides an additional security layer that is applied at the role level for users in the Enterprise Control Room. It can be set for all users or for users with specific roles.

Two-factor authentication is disabled by default.

When users are assigned a role that requires 2FA, they must set up an Authenticator application on their mobile devices and establish a connection between that application and Enterprise Control Room. On subsequent logins, users are prompted to enter a time-based one-time password (OTP) from the authenticator to complete the Enterprise Control Room login.

Two-factor authentication is supported only in Active Directory and non-Active Directory user environments; it is not supported for an SSO environment.

Procedure

1. Navigate to Administration > Settings > Two Factor Authentication.
2. Click Edit.
3. Select the Enabled check box.
4. Optional: Use the Maximum Tokens Per User drop-down list to set a limit on the user tokens.
5. Click Save changes.

Sequence to stop and start Enterprise Control Room services

To restart the Enterprise Control Room services, you must stop and start the services in a specific sequence.

When to stop and start the Enterprise Control Room services

Stop and start the Automation Anywhere Enterprise Control Room services in the following scenarios:

- When you are restarting the services manually during a maintenance window.
- When you are adding nodes to a cluster.
  Recommendation: Skip the License service when adding nodes to a cluster.
- If the service startup mode is set as manual, then after every machine or instance restart.
- When you are updating properties in the property file, which requires a services restart.

©2020 Automation Anywhere. All rights reserved.

Stopping the services on the Enterprise Control Room

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

1. Automation Anywhere Control Room Caching
2. Automation Anywhere Control Room Reverse Proxy
3. Automation Anywhere Control Room Messaging
4. Automation Anywhere Control Room Service
5. Automation Anywhere Licensing
6. Automation Anywhere Elastic Search Service
7. Automation Anywhere Bot Insight Service Discovery
   Note: Stop the Automation Anywhere Bot Insight Service Discovery if the Bot Insight services are up and running.

Starting the services on the Enterprise Control Room

Start the following Enterprise Control Room services in the listed sequence.

1. Automation Anywhere Licensing
2. Automation Anywhere Elastic Search Service
3. Automation Anywhere Control Room Reverse Proxy
4. Automation Anywhere Control Room Caching
5. Automation Anywhere Control Room Messaging
6. Automation Anywhere Control Room Service
7. Automation Anywhere Bot Insight Service
   Note: Wait for an interval of 30 seconds before starting the next service.

User management overview

As an Enterprise Control Room admin, you can create, view, edit, delete, and enable or disable user accounts. Creating user accounts depends on the non-Active Directory, Active Directory, or single sign-on (SSO) credentials from an IdP server.

Create users

Create a non-Active Directory user
: Add a non-Active Directory user by assigning a role and device license. Users can create TaskBots per the roles and device license assigned to automate the required process.

Add an Active Directory user
: Add an Active Directory (AD) user by selecting an AD domain, providing AD environment details, and assigning a role and device license. The user must be a part of the AD.

Add user from IdP server for SSO
: The task of adding a user from the IdP server in an Enterprise Control Room that is configured for single sign-on (SSO) is similar to creating an Active Directory user.

Tasks you can perform on user accounts

You can perform the following tasks on the user accounts by using the actions menu (vertical ellipsis) located to the right of each username:

©2020 Automation Anywhere. All rights reserved.

View user: Opens the View user page in read-only mode

User details, assigned roles, and general details, such as Last modified, Modified by, Object type, and User type are displayed. Additionally, you can edit the user details and enable or disable the user account.

Edit user details: Opens the Edit user page in write mode.

Enables you to update the user details, device login credentials, assigned roles, and device licenses. When you edit user details, a notification email is sent to the user.

Enable/disable user: You can activate or deactivate the user account.

This option is useful when you want to temporarily restrict a user's access. When you enable or disable a user account, a notification email is sent to the user.

Delete user: You can delete the user account.

If a user leaves the organization or is moved to another role, you can delete the user account. This ensures that the device to which the user was added and the allocated license are freed. When you delete a user account, an email notification is sent to the user.

Search for users

You can use the Users page in the Enterprise Control Room to view detailed information about existing users. Search for the user you want using the following options:

- Apply a search parameter:

  For ease of access, apply search parameters to the username, first name, last name, description, and user status columns.

  When you specify search parameters for the same column, the system searches using the OR operator. When you specify search parameters for different columns, the system searches using the AND operator.

  Note: When you use special keys "-" or "_", the system lists all the usernames instead of listing only those usernames that include these parameters.
- Sort the results by column actions:
  - Click a column header to sort by ascending or descending order.

    Sort up to three columns at a time by holding the Shift key as you click two or more column headers. This way the sorting is done on the entire table and not just the data that is currently visible to you.

  - Drag the column headers to the left or right.
  - Point to the end of a column and drag it to resize.

Perform actions on selected users

You can perform the following tasks by pointing to the icons at the top-right of the User table. These actions can be performed only at a table-level and not on individual items.

Create a role with checked items

Adds a role and assigns the selected users.

Delete checked items

Deletes the selected users. You cannot delete a user who is currently logged in.

©2020 Automation Anywhere. All rights reserved.

Export to CSV
: Exports the selected users in the table in CSV format.

Refresh
: Refreshes the table and displays the latest data.

11.3.4 Send a verification email
: Click this option to send a verification email to users.
Note: Only administrators or users with the Create and Edit user role permissions can use this option to send the verification email.

Customize columns
: Enables you to select the columns that you want to show or hide in the table.

Create a non-Active Directory user

Add a non-Active Directory user by assigning a role and device license. Users can create TaskBots per the roles and device license assigned to automate the required process.

Prerequisites

You must be logged in to the Enterprise Control Room with administrator privileges.

Procedure

1. Navigate to Administration > Users.
   The All users page appears, displaying information about the existing users.
2. Click Create user.
   The Create user page appears.
3. In the General Details section, perform the following steps:
   a) Clear the Enable User check box if you do not want the user to log in immediately.
   By default, this check box is selected.
   b) Enter a unique name in the Username field.
   Note: You can also include an email address. For example: `username@example.com`.
   c) Optional: Enter a description and include the first name and last name for the user.
   The maximum number of characters allowed for first name and last name is 50.
   d) Enter a Password and confirm your password.
   The password must follow the password policy.
   e) Enter your Email address and confirm the address.
   If SMTP is enabled, the user is sent an email to this address to confirm the account. All important Enterprise Control Room notifications are sent to this email address.
4. In the Select roles section, assign a role from the Available roles table.
   Each role includes specific privileges and permissions to access and perform actions in certain areas of Enterprise Control Room.

   System created roles

   a) In the Available roles list, select the check box next to the Role Name to select all roles.
   Alternatively, select multiple roles from the list.
   b) Add roles to the Selected list.
   - Any Enterprise Control Room user has access to these permissions by default: View Dashboard, Manage my credentials and locker, and View and manage my queues.

©2020 Automation Anywhere. All rights reserved.

- A non-admin user does not have access to these permissions: Admin, BotFarm Admin, Pool Admin, Locker Admin.

5. Assign a device license to the user.
   System default licenses
   Note: Device licenses are not available for users with the Admin or BotFarm admin roles. The number of available copies is shown next to each license.
6. Click Create user or Create user and add another.
   If SMTP is enabled, an email is sent to new users inviting them to log in.
   The new user is displayed in the User table.

Add an Active Directory user

Add an Active Directory (AD) user by selecting an AD domain, providing AD environment details, and assigning a role and device license. The user must be a part of the AD.

Procedure

1. Navigate to Administration > Users.
   The All users page appears, displaying information about the existing users.
2. Click Create user.
   The Create user page appears.
3. In the General Details section, perform the following steps:
   a) Clear the Enable User check box if you do not want the user to log in immediately.
   By default, this check box is selected.
   b) Click Active Directory domain to assign an active directory name for the user.
   The list displays all the domains available in the Active Directory domain controller.
   Note: Enterprise Control Room Active Directory supports a single forest multi-domain environment.
   c) Enter a name in the Username field, and click CHECK NAME IN ACTIVE DIRECTORY.
   - d) If the user name is present in the AD, the First name, Last name, Email, and Confirm email fields are already populated.
   - e) If the user name is not present in the AD, an error message is displayed. Contact your network administrator to resolve this issue.
4. In the Select roles section, assign a role from the Available roles table.
   Each role includes specific privileges and permissions to access and perform actions in certain areas of Enterprise Control Room.

   System created roles

   a) In the Available roles list, select the check box next to the Role Name to select all roles.
   Alternatively, select multiple roles from the list.
   b) Add roles to the Selected list.
   - Any Enterprise Control Room user has access to these permissions by default: View Dashboard, Manage my credentials and locker, and View and manage my queues.
   - A non-admin user does not have access to these permissions: Admin, BotFarm Admin, Pool Admin, Locker Admin.
5. Assign a device license to the user.
   System default licenses
   Note: Device licenses are not available for users with the Admin or BotFarm admin roles. The number of available copies is shown next to each license.
6. Click Create user or Create user and add another.

©2020 Automation Anywhere. All rights reserved.

If SMTP is enabled, an email is sent to new users inviting them to log in.
The new user is displayed in the User table.

Add user from IdP server for SSO

The task of adding a user from the IdP server in an Enterprise Control Room that is configured for single sign-on (SSO) is similar to creating an Active Directory user.

Prerequisites

Before adding a user in your Enterprise Control Room, ensure the following:

- The user already exists in the IdP server.

  If the username is not present in the IdP server, the user is not allowed to log in using SSO. You must contact your IdP server administrator to resolve this issue.

- You must be logged in to the Enterprise Control Room with administrator privileges.

Procedure

1. Navigate to Administration > Users.
   The All users page appears, displaying information about the existing users.
2. Click Create user.
   The Create user page appears.
3. In the General details section, perform the following steps:
   a) Clear the Enable User check box if you do not want the user to log in immediately.
   By default, this check box is selected.
   b) Enter a Username. Ensure that the name is the same as that provided in the IdP server.
   Note: You can also include an email address-for example, username@example.com.
   c) Optional: Enter a description and include the first name and last name for the user.
   The maximum number of characters allowed for first name and last name is 50.
   d) Enter your Email address and confirm the address.
   If SMTP is enabled, the user is sent an email to this address to confirm the account. All important Enterprise Control Room notifications are sent to this email address.
4. In the Select roles section, assign a role from the Available roles table.
   Each role includes specific privileges and permissions to access and perform actions in certain areas of Enterprise Control Room.

   System created roles

   a) In the Available roles list, select the check box next to the Role Name to select all roles.
   Alternatively, select multiple roles from the list.
   b) Add roles to the Selected list.
   - Any Enterprise Control Room user has access to these permissions by default: View Dashboard, Manage my credentials and locker, and View and manage my queues.
   - A non-admin user does not have access to these permissions: Admin, BotFarm Admin, Pool Admin, Locker Admin.
5. Assign a device license to the user.
   System default licenses

©2020 Automation Anywhere. All rights reserved.

Note: Device licenses are not available for users with the Admin or BotFarm admin roles. The number of available copies is shown next to each license.

6. Click Create user or Create user and add another.
   If SMTP is enabled, an email is sent to new users inviting them to log in.
   The new user is displayed in the User table.

View user

User details, assigned roles, and general details, such as Last modified, Modified by, Object type, and User type are displayed in read only mode.

USER DETAILS

- First name: The first name of the user.
- Last name: The last name of the user
- Description: The description of the user.
- Email: The email address of the user
- Password: The password of the user.

  For Active Directory users, the password field is not displayed.

- User status: The status of the user, whether enabled or disabled.
- License: The license type of the user, such as unattended bot runner, attended bot runner, bot creator and other license types.
- License status: The status of the user license:
  - Verified: Any user created in the Enterprise Control Room.
  - Unverified: If the user has not verified the license (clicked the verification link) when the SMTP is enabled.
  - Registered: When the user logs into any client machine.
- Auto login: If a user can auto-login after logging out.

Roles
The roles assigned to the user.

GENERAL DETAILS

- Last modified: Displays the last time changes were made to the user in date and time.
- Modified by: Displays the name of the user who last made changes to the user in date and time.
- Object type: Displays the type of the bot, such as TaskBot, MetaBot, or IQ Bot.
- User type: The type of user, such as Bot Creator, Unattended Bot Runner, Attended Bot runner, Admin or Other.

Edit user details

Edit the details of an Active Directory, non-Active Directory, or IDP user, such as changing the role, first name, last name, email address, or license.

You can edit the user details, when you want to change a user's role, when users forget their password, or when a user's email address has changed.

©2020 Automation Anywhere. All rights reserved.

- You cannot change the Username for a user.
- You cannot change or edit your own details except from User Profile option. .
- In cases where email notification is enabled and you edit the details of a user, an email is sent to the user. Configuring email notification settings.
- If roles or permissions for users are updated, the user must log in again or refresh the browser for the changes to be immediately updated in the Enterprise Control Room.

Procedure

1. Log in to Enterprise Control Room as an administrator.
2. Navigate to Administrator > Users.
   The All users page appears.
3. Hover over the action menu (vertical ellipsis) and select Edit user task.
4. In the Edit user page, edit the users details depending on your requirements.
5. Click Save Changes.

The changes are updated and a success message appears. Additionally, these changes are logged in the audit logs (authorized users can view the logs).

Delete user

The process to delete a user from the Enterprise Control Room varies based on the user role, device status, and schedule status.

Prerequisites

Before you delete a user, ensure the following:

- There are no active or inactive schedules associated with the user.

  If the user has created schedules that are running or pending for execution, you cannot delete the user.

- There are no automation processes running on the registered user device.
- The user is not a member of lockers in the Credential Vault.
- The user does not own a queue or a device pool.
- The user is not a part of any device pool.

Attention: When you delete a user from the Enterprise Control Room, the bots created by the user are not deleted. Instead, the status appears as `Inactive` for the bots that were uploaded by the user, the entries in the Historical Activity page, the folders created by the user, and so on. However, the user is removed from the User table, and the user's license is released. The device name with which the user is registered is removed from the My devices table.

When a user is deleted, Credential Vault variables associated with the user are deleted.

Procedure

1. Navigate to the Administration > Users.
   The All users page appears, displaying information about the existing users.
2. Delete one or more users.

©2020 Automation Anywhere. All rights reserved.

- To delete a user, hover your mouse over the action menu (vertical ellipsis) and select Delete user.
- To delete multiple users, select the check boxes and click Delete checked items located above the Users table.

3. Review the message and confirm the delete action.
   The following messages are shown depending on the assigned license:

License type	Message
Attended Bot Runner license	Do you want to permanently delete the user <username>? This releases the Attended bot runner license allocated to the user. There can be one or more schedules created by this user. If you delete this user, those schedules will not run.
Unattended Bot Runner license	Do you want to permanently delete the user <username>? This releases the Unattended bot runner license allocated to the user and remove the device <devicename> the user has registered with. There can be one or more schedules created by this user. If you delete this user, those schedules will not run.
Bot Creator license	Do you want to permanently delete the user <username>? This releases the bot creator license allocated to the user and remove the device <devicename> the user has registered with. There can be one or more schedules created by this user. If you delete this user, those schedules will not run.
None	There can be one or more schedules created by this user. If you delete this user, those schedules will not run.

4. Click Close if you see the following message:
   11.3.4
   ```
   Unable to delete this user due to one or more of the following reasons
   1. The user has created some schedules which are running or pending for execu
   tion
   2. The user's device is busy running an automation process
   3. The user has created some credentials in the credential vault
   4. The user is a member of some lockers in the credential vault
   5. The user owns a queue or a device pool
   6. The user's device is part of a device pool
   To continue, please check the Audit Log details and try again.
   ```
5. Resolve the relevant issue and follow steps 1 to 3.

©2020 Automation Anywhere. All rights reserved.

Tip: From the Edit user page, set the Allocate a device license to this user? option to None to free up a user license. This ensures that the user can only access the Enterprise Control Room and not the TaskBots.

Roles overview

Administrators or users with roles permission can create, edit, and delete roles for various features and operations in the Enterprise Control Room.

RBAC (role-based access control) grants access to users based on the assigned roles and the access provided to the user.

Following are the benefits of creating roles:

- Increased security by controlling user access based on their assigned roles.
- Decreased dependency on customer support.
- Efficient monitoring of use and access of data, which leads to better research management.

Manage roles

- Create roles
  - System created roles

    These are the roles that are preconfigured during Enterprise Control Room installation.

  - User-created roles

    These are the roles that are created by users, and can be customized accordingly.

    If a custom role or user-created role is created with all the Enterprise Control Room permissions, then it is not considered as a Enterprise Control Room Admin role. Only a system-created Admin role has this privilege.

- 11.3.5 Export or import roles and users

  the Enterprise Control Room enables you to export or import custom roles and the users associated with the roles.

Tasks you can perform on roles

You can perform the following tasks on the created roles by using the actions menu (vertical ellipsis) located on the right of each role name:

View a role
: Opens the View role details in read-only mode. An administrator or a user with permission to view or manage role can access the View role page.

Edit a role
: Opens the Edit user role in write mode. Only an administrator or a user with permission to edit role can access the Edit role option to modify information such as feature permissions, bots, devices, users and security.

©2020 Automation Anywhere. All rights reserved.

Delete a role
: You can delete a redundant role. An admin user or a user with delete permission can remove the redundant roles from Enterprise Control Room.

Copy a role
: You can create a similar role. Only an administrator has the permission to copy a role in the Enterprise Control Room. This ensures that you can create similar roles in the system without having to perform the action manually.

Search for roles

You can use the All Roles page in the Enterprise Control Room to view detailed information about system and user created roles. Search for the role you want using the following options:

- Apply a search parameter:

  For ease of access, filter roles according to role name and type.

  When you specify search parameters for the same column, the system searches using the OR operator. When you specify search parameters for different columns, the system searches using the AND operator.

- Sort the results by column actions:
  - Click a column header to sort by ascending or descending order.

    Sort up to three columns at a time by holding the Shift key as you click two or more column headers. This way the sorting is done on the entire table and not just the data that is currently visible to you.

  - Drag the column headers to the left or right.
  - Point to the end of a column and drag it to resize.

Perform actions on selected roles

You can perform the following tasks by pointing to the icons on the top-right of the Roles table. These actions can be performed only at a table-level and not on individual items.

Create user
: Enables you to create users from the Roles page.

  User management overview

Refresh
: Refreshes the roles table and displays the latest data.

Delete checked items
: Deletes the selected roles from the table.

Customize columns
: Enables you to select the columns that you want to show or hide in the table. By default, all the columns are displayed.

©2020 Automation Anywhere. All rights reserved.

For Active Directory users

Map Active Directory roles
: You can define a role and assign permissions to access various features of the Enterprise Control Room. Only an admin or Enterprise Control Room user with roles permission can assign roles to users and provide access to them for various features and operations.

Synchronize role mappings
: You can synchronize the role mappings from the Active Directory role mappings page, or automate it to synchronize when the user role sync background process is triggered.

View Active Directory role mappings
: An administrator or a user with permission to view and manage role can access the View Active Directory role mapping page.

Delete Active Directory role mappings
: An administrator or a user with permission to view and manage role can delete role mappings.

Audit logs

All the create, update, and delete actions are tracked and stored in the Audit log page for future use.

System created roles

When planning your Automation Anywhere deployment, consider the licensing, roles, and users required to perform the Automation Anywhere functions. This topic describes the default roles and their associated permissions.

Access to Automation Anywhere functions is defined by a combination of licensing applied to the Enterprise Control Room and the roles assigned to the user.

System created roles are pre-configured during Enterprise Control Room installation. These roles cannot be deleted or edited. You can only assign or unassign these roles to users.

Default Roles	Description
AAE_Admin (ID: 1)	Permits access to all features, including creating other Admin users and access to all folders and files. The only role that can access Enterprise Control Room settings.
AAE_Basic (ID: 2)	Permits users to upload and download TaskBots in the My Tasks folder. Limited access to other features.
AAE_Bot Insight Admin (ID: 3)	Permits users to view and manage data in Bot Insight. Limited access to Enterprise Control Room features. (If Bot Insight license is installed).

©2020 Automation Anywhere. All rights reserved.

Default Roles	Description
	It allows a user to access Bot Insight RESTful APIs to get access to the data logged by the Enterprise Control Room, and by a task during 'Production' run.
AAE_Bot Insight Consumer (ID: 5)	Permits users to view data in Bot Insight and limited access to Enterprise Control Room features. (If Bot Insight license is installed)
AAE_Bot Insight Expert (ID: 6)	Permits users to manage data in Bot Insight and limited access to Enterprise Control Room features. (If Bot Insight license is installed)
AAE_Bot Store Consumer (ID: 15)	Permits users to download a bot package or a Digital Worker from the Bot Store to the Enterprise Control Room repository.
AAE_BotFarm Admin (ID: 8)	Permits users access to BotFarm admin privileges.
AAE_BotFarm Agent (ID: 7)	Permits users to view and manage privileges to the user.
AAE_COE Admin (ID: 16)	Permits users to view and manage Operational and Business Analytics dashboards and data.
AAE_IQ Bot Admin (ID: 14)	Permits users to access the IQ Bot admin privileges.
AAE_IQ Bot Services (ID: 9)	Permits users to access the IQ Bot console and limited access to Enterprise Control Room features.
AAE_IQ Bot Validator (ID: 4)	Permits users to access the IQ Bot Validator screen and limited access to Enterprise Control Room features. (For a Bot Runner with an IQ Bot license)
AAE_Locker Admin (ID: 3)	Permits users to view all credentials and all lockers. A Locker Admin can change the owner of a credential that they do not own. For lockers they do not own, they can delete the locker, edit permissions, and remove credentials.

©2020 Automation Anywhere. All rights reserved.

Default Roles	Description
	Note: This permission is not applicable to Enterprise Control Room Admin role.
AAE_MetaBot Designer (ID: 13)	Permits users to access Bot Creator MetaBot Designer from Enterprise client but does not allow the user to see any bots or supporting files. Note: Migrated users (Bot Creator) who had access to MetaBot Designer in Enterprise Control Room 11.1 and less shall continue to have access to Designer.
AAE_Pool Admin (ID: 11)	Permits users to view and manage all device pools. Note: Users with AAE_Pool Admin do not have permission to see any bots and supporting files.
AAE_Queue Admin (ID: 10)	Permits users to view and manage all queues.

Bot Insight, BotFarm, and IQ Bot roles are displayed only if you have respective licenses. Bot Insight, BotFarm, and IQ Bot roles are displayed only if you have respective licenses.

Related tasks
Create a non-Active Directory user

Bot Permissions for a Role

You can assign Bot permissions when creating a role. When you select a folder, that means the role will automatically have permission to any bots or files that are added to the folder in the future.

MetaBot supports role based access control (RBAC) on individual MetaBot files, and folders containing MetaBots. When a MetaBot is uploaded to Enterprise Control Room, it inherits permission of the immediate parent folder. To change or modify permission on individual MetaBot file, you must perform the action manually.
Note: If the applied permissions are different on a MetaBot file and its folder, precedence is given to permission applied at the MetaBot file level.

TaskBots and MetaBots permissions

You can select from the following permissions for the TaskBots and the MetaBots:

- Select all: This permission includes Run+Schedule, Upload, Download, Execute (only for MetaBots), and Delete actions.
- Run+Schedule: This permission includes run and schedule permission. It allows user to run or schedule the TaskBots and MetaBots. This permission is enabled only if user has either Run my bots or Schedule my bots to run permission.

©2020 Automation Anywhere. All rights reserved.

Note: The Run+Schedule permission replaces the earlier behavior of 11.0 where a user was allowed to run or schedule a bot when that user had download permission for a folder.
  - This permission is termed as Run when the user has Run my bots feature permission. You can explicitly select Run permission on a specific folder to allow the user to run all bots that belong to this folder.
  - Similarly, this permission is termed as Schedule when the user has Schedule my bots to run feature permission. You can explicitly select Run permission on a specific folder to allow the user to schedule all bots that belong to this folder.
  - It is termed as Run+Schedule when user has both feature permissions. This allows the user to run and schedule bots that belong to this specific folder on which the permission is selected.
- Upload: This permission includes uploading TaskBots and MetaBot files/ folder to Enterprise Control Room.
- Download: This permission includes downloading TaskBots and MetaBot files/ folder from Enterprise Control Room to Enterprise client.
  Note: If you grant Download permission to a user, the Execute permission is automatically enabled so that a user can choose to either view or edit the content of a MetaBot that is downloaded.
- Execute: This permission is available only for MetaBots that enables to use MetaBots in a task.
- Delete: This permission includes removing file/ folder from Enterprise Control Room.

Feature permissions for a role

The role based accessibility model ensures that users have the necessary privileges to view information or data that are relevant to the roles assigned by the Enterprise Control Room administrator.

Only an administrator or a user with roles permission can assign roles to other users and provide access to various features and operations.

Note: The User Management API uses numeric values for permission features when creating roles. The (ID: nn) is the corresponding numeric identifier for a feature.
The option you select for users determines the features accessible to them. You can assign the following permissions:

- Dashboard permissions
- Activity permissions
- Bots permissions
- Metabot permissions
- Devices permissions
- Workload permissions
- Bot Store permissions
- Audit Log permissions
- Administration permissions
- API permissions
- IQ Bot permissions

Features	Permissions
DASHBOARDS	View dashboards Available by default for all users. Note: The data populates in the dashboard based on the role permissions.

©2020 Automation Anywhere. All rights reserved.

Features	Permissions

ACTIVITY	• View my In progress activity (ID: 30)
	
	Available by default and enables all the users to view their own activity.
	
	• Manage my In progress activity (ID: 51)
	
	Enables you to monitor and manage (pause, resume and cancel) your own In progress activities. You can also archive your finished activities.
	
	• View everyone's In progress activity from my folders (ID: 36)
	
	Enables you to monitor those In progress automations for which the run or schedule access on the respective TaskBots are available.
	
	• Manage everyone's In progress activity from my folders (ID: 52)
	
	Enables you to monitor and manage (pause, resume and cancel) other users' In progress activities. You can also archive your finished activities.
	
	• View All in progress activity (ID: 101)
	
	Enables you to see all ongoing automations irrespective of Bot folder permission.
	
	• View my scheduled bots (ID: 28)
	Enables you to view their bots, even if they are scheduled to run later or by others.
	  • Schedule my bots to run (ID: 10)
	
	  Can schedule a bot on which the user has 'Schedule' privileges.
	
	  • Edit my scheduled activity (ID:5)
	
	  Can edit the schedules that the user has created.
	
	  • Delete my scheduled activity(ID: 11)
	
	  Can delete the schedules that the user has created.
	
	  • View and manage ALL scheduled activity from my Folders (ID: 53)
	
	  Users can view, edit, and delete all bots schedules from the folders that they have access. These schedules can also be created by other users.
	
	  • View and manage ALL scheduled activity (ID: 52)
	
	  Can view, edit, and delete all the schedules in the system.

BOTS	• View my bots (ID: 29)

©2020 Automation Anywhere. All rights reserved.

Features	Permissions
	• Run my bots (ID: 7) Can run the bots from the folder on which the user has 'Run' permission. • Export bots (ID: 31) Can create a bot package to export bots and their dependencies. This requires download permission. • Import bots (ID: 32) Can import a bot package. This requires upload permission. • Create Folders (ID: 54) Can create folders in the Enterprise Control Room repository. • Rename Folders (ID: 55) Can rename folders in the Enterprise Control Room repository • Manage my credentials and lockers (ID: 59) Available by default for all the users. • Manage my lockers (ID: 26) Can manage the lockers that the user has created or owns. • Administer ALL lockers (ID: 3) Can view and manage all the lockers and is available only with the AAE_Locker Admin role. • Create standard attributes for a credential (ID: 61) Can create the Standard attributes for a credential in addition to the User-provided attributes. • View and edit ALL credential attributes value (ID: 63) Can view and edit all the credential attributes that the user has created or owns in the Enterprise Control Room. Also, can use the Credential Vault API to edit other users' attributes. • Bot Auto-Login Credentials API (ID: 35) Can set the auto-login credentials of a Bot Creator or Bot Runner through the Bot Auto Login Credentials API. See Auto Login Credentials API overview.

©2020 Automation Anywhere. All rights reserved.

Features	Permissions
MetaBot	Access to MetaBot Designer (ID: 62) Enable Bot Creators to access MetaBot Designer to view, create and update MetaBots. This permission is available by default for the system role AAE_MetaBot Designer and it is disabled for other roles (System and User created).
DEVICES	View and manage my Bot runners, Bot creators and device pools (ID: 30) Enables you to view, run and schedule bots on the devices or the device pools. • Create device pools (ID: 40) Can create and manage one or more device pools. • Administer ALL device pools (ID: 66) Can manage all pools in the system and is available only with the AAE_Pool Admin role. • View and manage (ID: 60) Only users with the system-created Admin role can view and manage BotFarm functionality.
WORKLOAD	View and manage my queues (ID: 58) Enables you to view, create, and manage the queues that the user has created. • Create queues (ID: 41) Can create and manage one or more queues. • Administer ALL queues (ID: 45) Can manage all queues in the system and is available only with the AAE_Queue Admin role. • SLA Calculator (ID: 42) Can calculate the number of Bot Runner or the time-frame required to process all the work items in a queue.
BOT STORE	• View Bot Store (ID: 97)

©2020 Automation Anywhere. All rights reserved.

Features	Permissions
	Enables you to access the Bot Store tab in the navigation pane of the Enterprise Control Room. Available by default for all the users. • Download Bot Storebots to the Enterprise Control Room repository (ID: 15) Enables you to download bots from the Bot Store to the Enterprise Control Room repository and is available only with the AAE_Bot Store Consumer role.
AUDIT LOG	View everyone's audit log actions (ID: 14) Enables you to view your own and other users action in the audit logs.
ADMINISTRATION	View and manage settings (ID: 85) Enables you to view and manage all the Enterprise Control Room settings. • View users (ID: 1) Enables you to only view all the users in the system. • Create users (ID:3) Can create one or more users in the system. • Edit users (ID:4) Can edit one or more users in the system. • Delete users (ID: 2) Can delete other users. • 11.3.4 View user basic (ID: 102) Can view basic information about other users. This permission restricts a user from viewing basic information about other users when performing the following operations: • Creating, viewing, and editing a device pool. • Creating, viewing, and editing a locker. • Creating and editing a role. • Adding queue owners, participants, and consumers.

©2020 Automation Anywhere. All rights reserved.

Features	Permissions

	The system displays "No permission" in the "Modified by" column on all the pages of the ACTIVITY and BOTS tab, and the Users and Roles pages in the ADMINISTRATION tab
	
	• View roles (ID: 90)
	
	Enables you to only view roles.
	
	• Manage roles (ID: 12)
	
	Can manage (create, edit, and delete) roles in addition to viewing.
	
	• View and manage Migration (ID: 86)
	
	Enables you to view migration details and is able to create or manage an existing migration.
	
	• View licenses (ID: 20)
	Enables you to view the license details.
	  • Manage user's device licenses (ID: 48)
	
	  Can manage licenses for other users.
	
	  • Install licenses (ID: 49)
	
	  Can install licenses for other users.

API	Bot Insight • Data API (ID: 47) Enables you to use the Bot Insight data API. See Bot Insight Data API. • Generate API-Key (ID: 91) Enables you to generate an API key used for authenticating the Enterprise Control Room user when making an authentication API call. The permission is not available by default and must be assigned to a user defined role separately.
IQ BOT	View IQ Bot (ID: 68) Enables you to view all the default dashboards in the IQ Bot portal. • View Learning Instances (ID: 69) Can view all the learning instances. • View Domains (ID: 70)

©2020 Automation Anywhere. All rights reserved.

Features	Permissions
	Can view all the domains in the IQ Bot portal. • View Administration (ID: 71) Can view the Administration tab in the IQ Bot portal. IQ Bot user roles and permissions

Active Directory role mappings

The Role Mappings feature maps Active Directory (AD) security groups to one or multiple roles in the Enterprise Control Room. This allows the Enterprise Control Room to synchronize with the AD and assigns the correct roles to the users, and accessing objects such as bots, devices, folders, credentials, Credential Vault lockers).

You can add various role mappings in the Enterprise Control Room: Map Active Directory roles

Based on the mapping information, user roles are assigned in multiple ways:

User creation
: All the security groups that a user belongs to in the AD are retrieved and roles are automatically assigned to that user based on the mappings.

User login
: Every time a user logs in, the Enterprise Control Room validates the mappings, the current security group memberships, and assigned roles before confirming any required changes.

Automated background process
: This process is initiated based on the defined time period set on the Active Directory role mappings page. It synchronizes all the mappings before synchronizing roles for every user in the Enterprise Control Room based on the updated mappings: Synchronize role mappings
All the roles assigned through role mappings are designated as system-assigned roles. The Enterprise Control Room admin can assign additional roles to users if required. However, the system-assigned roles of the users cannot be removed.
Note: The system-assigned roles can be changed or removed only from mappings.

Map Active Directory roles

Map a single AD security group to one or more Enterprise Control Room roles. Create the mapping before synchronizing user and roles during the user login or background process.

While there is a nested grouping relationship in the AD, there is no such relationship in the Enterprise Control Room as they are all one to one mappings.

Procedure

1. Navigate to Administration > Roles.

©2020 Automation Anywhere. All rights reserved.

2. Click the ACTIVE DIRECTORY ROLE MAPPING tab.
3. Click Create Role Mapping.
   This enables you to create a mapping between an existing AD security group and the available role.
4. Enter a name for your mapping in the Mapping name field.
5. Click the Active Directory domain drop-down list, and select an available domain.
6. Use the Active Directory security group field to search for a group.
   For example, if you have a group named `Certified Publishers`, search for `Certified`. All the groups that contain `Certified` in their name are listed under GROUPS.
7. Click the right arrow to add the selected group.
8. Use the Available Roles to assign a role.
   You can also use the Search name field to search for an available role.
9. Select the roles you want to assign, and click the right arrow to add it.
   The selected roles are listed under the Selected field.
10. Click Create Mappings.

Synchronize role mappings

You can synchronize the role mappings from the Active Directory role mappings page, or automate it to synchronize when the user role sync background process is triggered.

You can use the Cancel Sync option to turn off the periodic automatic sync. This process can then be triggered manually using the Sync roles from Active Directory option, which starts immediately and continues to run based on the time interval set.

Recommendation: As this can be a time consuming and an expensive operation, set the role synchronization time period to the default value of 1440 minutes (1 day).
Note: Nested mapping is currently not supported.

For example, assume that an AD has a parent group and a child group called 'pGroup' and 'cGroup' respectively. The user 'Paul' is part of the 'pGroup'. In the Enterprise Control Room, and a mapping is created to map 'pGroup' to Role1 and Role2. Another mapping is created to map 'cGroup' to Role3.

As only direct mapping is supported in the Enterprise Control Room, 'Paul' is automatically mapped to only role1 and role2.

The role mappings must be synchronized during the following scenarios:

- Changes to AD groups.

  If any group that is mapped is deleted from the AD, the mappings must be validated before being deleted as the group is no longer available.

- Update to the license file.

  Updating the license file can change the available roles. Mappings must be synchronized before updating the roles.

  Note: After a sync, user must wait a few seconds for the updated changes to appear.

©2020 Automation Anywhere. All rights reserved.

View Active Directory role mappings

An administrator or a user with permission to view and manage role can access the View Active Directory role mapping page.

View the details of the available role mappings listed in the Role Mapping table.

Procedure

1. Navigate to Administration > Roles.
2. Click the ACTIVE DIRECTORY ROLE MAPPING tab.
   All the available role mappings are listed in the Role Mappings table.
3. Enter an available mapping name in the search box next to the Mapping Name drop-down list.
   Optionally, you can use the Active Directory security groups to search for any available AD security groups.
   One or more available role mappings that match your search criteria appear in the Role Mapping table.
4. Hover over the action menu (vertical ellipsis) and select the View role mapping option.
   All the associated MAPPING DETAILS and Mapped Roles are listed.

Delete Active Directory role mappings

An administrator or a user with permission to view and manage role can delete role mappings.

Delete the required role mappings listed in the Role Mapping table.

Procedure

1. Navigate to Administration > Roles.
2. Click the ACTIVE DIRECTORY ROLE MAPPING tab.
   All the available role mappings are listed in the Role Mappings table.
3. For a specific role in the roles list, hover over the action menu (vertical ellipsis) and select the Delete role mapping option.
4. Click Yes, delete to delete the selected role.

Edit Active Directory role mappings

Starting from Version 11.3.5, an admin user can edit role mappings in the Enterprise Control Room.

You can edit the required role mappings listed in the Role Mappings table.

Procedure

1. Navigate to Administration > Roles.
2. Click the ACTIVE DIRECTORY ROLE MAPPING tab.
   All the available role mappings are listed in the Role Mappings table.

©2020 Automation Anywhere. All rights reserved.

3. For a specific role in the roles list, hover over the action menu (vertical ellipsis) and select the Edit role mapping option.
4. In the Edit an Active Directory role mapping window, edit the Mapping name.
   Ensure that the mapping name is unique and cannot be duplicated. If you rename a map with an existing mapping name, an error message appears stating that the same name already exists. .
5. Edit the roles by either adding or removing roles from the Available roles list except Bot Insight roles.
   If you assign Bot Insight roles, an error message appears stating that the role mapping cannot be updated as it contains unsupported roles.
   Note: The rest of the fields cannot be edited.
6. Click Save changes.
   Changes to mapping name or roles are updated in the audit log.

Conflicting roles

There are some roles in the Enterprise Control Room that cannot coexist due to certain restrictions and result in an error.

For example, an error appears if you assign an Enterprise Control Room user with an Admin role, along with one of the following roles:

- AAE_Bot Insight Admin
- AAE_Bot Insight Consumer
- AAE_Bot Insight Expert

This validation also applies to the system-scheduled sync process of user and roles. In the above scenario, the roles sync for that particular user is ignored, before proceeding to the next user.

An audit log is captured in the system logs when:

- A mapping is created or deleted.
- A role sync is triggered from either a user login or by the background process.

  All role syncs are audited.

- There are role conflicts.

Additionally, user roles will not synchronize for the following scenarios even if the system scheduled process is triggered:

- There are role conflicts in the combination of mappings and user-assigned roles, or just in the mapping itself as these are not validated when mapping is created.
- If a mapping was deleted and associated users have no other roles assigned.

  A user must have at least one role (no empty roles) for a successful sync.

Note: A user's AD security group cannot be retrieved if there are no URLs with the same domain.

For example, assume that the Enterprise Control Room has the following URLs configured:

- 'ldap://host.domainA.com'

©2020 Automation Anywhere. All rights reserved.

- 'ldap://host.domainB.com'

If a user with 'user@domainC.com' tries to log in, no AD security group is returned as there is no URL with the 'domainC.com'.

Create a role

You can define a role and assign permissions to access various features of the Enterprise Control Room. Only an admin or Enterprise Control Room user with roles permission can assign roles to users and provide access to them for various features and operations.

Procedure

1. Navigate to Administration > Roles.
2. Click Create Role.
3. Enter the name and description for the role.
4. In the FEATURES tab, select the required features and permissions that are relevant to the role you are creating.

   For the available permissions for each feature, see Feature permissions for a role.

5. Click Next.
6. Optional: In the Bots tab, assign the permissions with respect to TaskBots and MetaBots.
   Note: The Bots tab is visible only if View my bots permission is selected in the Features tab. See Bot Permissions for a Role.
7. Click Next.
8. In the DEVICES tab, select the devices your role will have access to.
   A non-admin user has access to Bot Runners that are tagged to user's role.
9. In the USERS tab, assign your role to the existing users and click the arrow pointing to right.
   Users deactivated by the Admin cannot be selected.

   Note: 11.3.4 You must have the View user basic permission to view information about other users if you want to assign them the role.
   Tip: You can select multiple users for your role in the Users tab. This allows more than one user to be assigned the same role at a time, which reduces effort, unlike the Users landing page.
10. Optional: In the SECURITY tab, select the Require Two Factor Authentication check box to enable 2FA.
    Note: Two Factor Authentication is disabled by default. See Enabling Two-factor authentication.
11. Click Create role.

Export or import roles and users

Starting from Version 11.3.5, the Enterprise Control Room enables you to export or import custom roles and the users associated with the roles.

Prerequisites

- Administrators or users with admin rights can export or import the custom roles and the users associated with the roles.
- The source and the target Enterprise Control Room must be running the same version.

©2020 Automation Anywhere. All rights reserved.

Recommendation: The source and the target Enterprise Control Room should be of same setup type: SSO with SSO, AD with AD, and non-AD with non-AD.

With this feature, you can use the already created roles and users in your Enterprise Control Room without manually creating them.

For exporting or importing custom roles and the associated users, consider the following:

- With custom roles, the role name, role description, two-factor authentication settings for individual roles, and all the associated feature-level permissions are exported and imported.
- If the SMTP option is disabled in the target Enterprise Control Room, users exported from the source Enterprise Control Room where SMTP is enabled will be automatically verified and they can log in to the target Enterprise Control Room.
- Bot level permissions , file permissions, and device permissions associated with the role are not exported.
- If the target Enterprise Control Room has insufficient user licenses (Bot Creator, and unattended Bot Runner and attended Bot Runner), then users are not imported.
- The AD security group role mappings are not exported or imported.
- Multi-factor authentication token values associated with the user are not exported or imported.
- From an AD or SSO Enterprise Control Room, only the roles can be exported or imported in a non-AD Enterprise Control Room, not the associated users.
- 4500 roles and 4500 users can be exported or imported.

Procedure

- Export roles and users
  1. Navigate to Administration > Roles.
  2. In the ALL ROLES page, click Export roles.
     The Export roles & users page appears.
  3. In the Roles tab, select the required custom roles that you want to export.
  4. Optional: Select the Include users check box to export all the users associated with the roles.
     For users, the license assignment information of the users is also exported.
  5. Click Next.
  6. In the PACKAGE SUMMARY tab, enter the Export package name and provide a Password to encrypt the package.
     Note: The password that is set in this step will be used for decryption when importing the package.
     In the Items to export, search or view the roles and the users that are selected to export.
  7. Click Export.

  All the information associated with the exported roles and the users is available for download and import in the target Enterprise Control Room.
- Import roles and users
  1. Navigate to Administration > Roles.
  2. In the ALL ROLES page, click Import roles.
  3. The Import roles & users page, browse for the .aaepkg file to import the roles and users.
  4. Enter the same Password that was used for encryption to decrypt the package you want to import.
  5. Click Import.

  All the information associated with the roles and users is imported from the source Enterprise Control Room to the target Enterprise Control Room.

©2020 Automation Anywhere. All rights reserved.

View a role

An administrator or a user with permission to view or manage role can access the View role page.

Procedure

1. Navigate to Administration > Roles.
2. Select a role you want to view.
3. Hover over the action menu (vertical ellipsis) and select View role option.

   Choose one of the following read-only options:

   - Features: List of features and permissions the role can access.
   - Bots: List of bots and supporting files the role can access.
   - Devices: List of devices the role can access.
   - Users: List of users having access to the respective role.

     Note: 11.3.4 You must have the View user basic permission to view information about other users that are assigned the role.

   Note: A user with View and Manage Role permission can view all the roles. However, the user cannot view details of Admin and Locker Admin roles. If the user clicks the View role icon, the view page appears with an error.

   You can also edit a role from the view page, if you have edit role permission.

Edit a role

Only an administrator or a user with permission to edit role can access the Edit role option to modify information such as feature permissions, bots, devices, users and security.

If a role or permission is updated, the respective users must re-login or refresh the browser for the changes to appear on Enterprise Control Room.

Procedure

1. Navigate to Administration > Roles.
2. For a specific role in the roles list, hover over the action menu (vertical ellipsis) and select Edit role option.

   The Edit role page appears.

3. You can edit or update any of the following options:

   - Features: Allows you to add or revoke role permissions.

   - Bots: Allows you to add or revoke access to folders on the Bots tab.

     Also, you can select the actions a user can perform on files within the folder.

   - Devices: Allows you to add or remove devices that a the selected role has access to on the Devices tab.

©2020 Automation Anywhere. All rights reserved.

Note: If a bot is scheduled on a device, the device is shown disabled in the selected area.
- Users: Allows you to add or remove users who have permission to access the role.

  Note: 11.3.4 You must have the View user basic permission to view information about other users.
- Security: Enable Two Factor Authentication.
  Note: The Two Factor Authentication is disabled by default. See Enabling Two-factor authentication.

4. Click Save changes.
   Note: A user with View and Manage Role permission can view all the roles. However, the user cannot edit details of Admin and Locker Admin roles.

Copy a role

Only an administrator has the permission to copy a role in the Enterprise Control Room. This ensures that you can create similar roles in the system without having to perform the action manually.

Procedure

1. Go to Administration > Roles
2. For a specific role, hover over the action menu (vertical ellipsis) and select Copy role option.
   Note: System-created roles cannot be copied. These roles are pre-configured during Enterprise Control Room installation.
   Note: When you copy a user role, two-factor authentication from the role is not copied and has to be manually enabled on the copied role. Enabling Two-factor authentication.
   A new role page is launched, wherein the role is created with "copy" appended to the Role Name.
   Example: In the previous image, role "HR" is copied, so a new role "HR_copy" is created. All the permissions that were selected are pre-filled in the new role.
3. Click Create role.
   A success notification is displayed creating a similar role.

Delete a role

An admin user or a user with delete permission can remove the redundant roles from Enterprise Control Room.

Procedure

1. Navigate to Administration > Roles
2. For a specific role in the roles list, hover over the action menu (vertical ellipsis) and select Delete role option.
   Note: System-created roles cannot be deleted.
3. Click Yes, delete to delete the selected role.
4. Optional: You also select the desired roles and click the Delete checked items option at the top of the table to remove multiple roles.

©2020 Automation Anywhere. All rights reserved.

Licenses - an overview

The Enterprise Control Room License page provides detailed information about the current license that is installed. It also enables the Admin user to monitor license details and usage statistics.

Therefore, an Admin user can view these details any time and avail information about the number of products purchased, the number of device licenses purchased, and number of licenses that are exactly in use.

Product licenses

Enterprise Control Room integrates with other Automation Anywhere products such as BotFarm, Bot Insight and Cognitive Platform. The product license details shows the list of purchased products, along with license version and product license status as used, not used, or N/A.

If you have a Bot Insight license, Business Analytics is available by default with Enterprise Control Room v11.0 and later.

Column	Value
Type	Product Name
Version	Latest version number of the current installed product
Purchased	Product has been purchased or not purchased
Used	Product is in used, not used, or N/A status

Device licenses

Bot user license detail shows the number of device licenses that have been purchased and are currently in use.

Bot Creator (Development): Users with privilege to automate bot(s) in Enterprise client.

Bot Runner

- Attended Bot Runner(Runtime): Users with privilege to run bot(s). Users with an Attended Bot Runner license can run bots only on their workstations using the Enterprise client. These users can also make use of local schedules and triggers for time or event based automation.

  11.3.4 Users with an Attended Bot Runner license can no longer create, edit, or delete schedules using the Enterprise client. TaskBots already scheduled by the same user or a different user from the same machine will continue to be executed based on the previously defined schedule.

- Unattended Bot Runner(Runtime): Users with an Unattended Bot Runner license can perform all automation tasks that Attended users can perform. Additionally, this license can also be used for Enterprise Control Room deployment, centralized scheduling, and API based deployment.
- IQ Bots: Users with an IQ Bot license can run IQ Bots within the parent TaskBots. The IQ Bot licenses can be distributed between Unattended and Attended Bot Runners. For example, if you have 50 licenses, you can allot any number between 0-50 to Unattended or Attended Bot Runners. But the total licenses distributed to Unattended and Attended Bot Runners cannot exceed 50.
  Note: In the Enterprise Control Room, the IQ Bot license shows the number of pages allowed for use.

©2020 Automation Anywhere. All rights reserved.

BotFarm (Runtime): bot user count of licenses is measured in number of hours used by all runtime clients within BotFarm to execute a bot.

Bot Insight: It shows the number of user count having Business Analytics role - Bot Insight Consumer or Expert. And API count is measured in number of rows that the API fetches from the Bot Insight database.

Column	Value
Type	Type of license
Purchased	No. of licenses purchased
Used	No. of licenses in use

- Installing a license
  A Enterprise Control Room administrator or a user with license management permission can install a license and evaluate the latest version.

Installing a license

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

A Trial license is valid for 30 days. Once it expires, you cannot access the Enterprise Control Room. Contact the System Administrator or Automation Anywhere Sales to purchase a new license. To install a license:

Procedure

1. Login to the Enterprise Control Room as an Administrator, and select Administration > Licenses.
2. Click Install license or you can click Show details on the notification bar in the Enterprise Control Room header, then click Install a new license.
3. Click Browse to select a .license file from the list of licenses.
4. Click Install license.
   An error occurs when:
   - A user has an invalid or an expired license file.
   - A user selects a file with a different extension other than .license.
   - A user selects a file that has been deleted or moved to another location.

Next steps

Enterprise Control Room installation and configuration is complete. Proceed to Preparing for users.

- Trial license
  Automation Anywhere Enterprise Control Room ships trial License with an evaluation period of 30 days. Use a trial license to assess the product and make an informed purchasing decision.
- How to change license service port
  The Automation Anywhere Enterprise Control Room default license service port is 8080. If the port is busy or blocked, for example, due to a firewall between the license server and clients, you have the option to change the license service port.

Related concepts

©2020 Automation Anywhere. All rights reserved.

Licenses - an overview
Related tasks
Logging in to Enterprise client
Related reference
Trial license

Migration overview

Migration is moving data using a systematic and phased process from Automation Anywhere v10.x to v11.x.x. As an Enterprise Control Room administrator with View and Manage Migration permissions, use the Migration Wizard tool to migrate data.

Complete the migration process from the Enterprise Control Room v11.x.x interface by doing the following steps:

Step 1: Plan migration
As an Enterprise Control Room administrator, use the considerations to understand your current environment and then create a migration plan.

Step 2: Prepare for migration
Prepare the environment at the source and destination Enterprise Control Room. This involves ensuring access to applications in the source Enterprise Control Room, installing and setting up the destination Enterprise Control Room, other configuration setting changes in both, and more.

Step 3: Start migration wizard.
Start the Migration wizard from the Enterprise Control Room interface..

Step 4: Connect to source Control Room database
Provide the source Enterprise Control Room database setting and configuration details.

Step 5: Connect to source Bot Insight database
If installed, provide the source Enterprise Control Room Bot Insight database setting and configuration details.

Step 6: Select migration type
Choose to migrate data from your source Enterprise Control Room based on roles, users, or bots.

Step 7: Select entities for migration
Select one of the following options:

- Roles - Migrate all or selected roles from the source to the destination Enterprise Control Room. When you select roles, other related data, for example, licenses, users, credentials, historical activity, and schedules are also migrated.
- Users - Migrate all or selected users from the source to the destination Enterprise Control Room. When you select users, other related data, for example license, roles, credentials, bots, historical activity, and schedules are also migrated.
- Bots - Migrate all or selected bots from the source to the destination Enterprise Control Room. When you select the bots, schedules associated with the bots are also migrated.

Step 8: Verify data and migrate
Review and confirm data related to the selected roles, users, or bots, with the dependent or associated data, for example MetaBots, schedules, credentials, and so on.

Step 9: Analyze migration status
Analyze the results after the migration process completes to track missing or incomplete data and decide if the migration process must be rerun.
Depending on the results repeat Steps 6, 7, and 8.
You can switch to another migration type in subsequent migration runs.

©2020 Automation Anywhere. All rights reserved.

Step 10: Complete post-migration activities

After all intended entities are migrated, do the post-migration tasks before using the v11.x.x Enterprise Control Room.

Plan migration

As an Enterprise Control Room administrator, use the considerations to understand your current environment and then create a migration plan.

Before planning your data migration, review the following considerations:

- If you are using a version lower than 10 LTS, migrate to 10 LTS using the 10 LTS Migration utility and then migrate from 10 LTS to 11.x.x.
  Note: The hot fixes on 10 LTS are supported for migration to 11.2.
- If you are using Automation Anywhere Enterprise v10.2, migrate to either Automation Anywhere Enterprise v10 LTS or Automation Anywhere Enterprise v10 SP2 using the Automation Anywhere Enterprise Migration utility before migrating to v11.x. This also ensures MetaBots created in Automation Anywhere Enterprise v10.2 or lower are compatible.
- You cannot migrate from Automation Anywhere v9.x. First migrate from v9.x to v10 LTS. See the Control Room Installation section of the AAE 10 LTS Installation Guide and the Migrating Data from 9.x to 10.3.0 section in the AAE 10 LTS Data Migration Utility - User Guide.
- Migration from 11 GA (11.0) to 11.2 is not supported.
- You cannot migrate data from a source Enterprise Control Room configured for one user type to a destination Enterprise Control Room configured for another user type. For example, data for an Enterprise Control Room configured for Active Directory cannot be migrated to Enterprise Control Room with either Non Active Directory or Single Sign On users.
- SAML configuration data migration is not supported.
- Automation Anywhere Licensing service should be running on port 8080 by default, which can also be changed, see How to change license service port.
- Automation Anywhere Licensing service must be running under a domain user account.
- The domain user account used for Automation Anywhere Licensing service should have access to Enterprise Control Room v10.x* repository path using a shared drive.
- The Subversion repository is different in both source and destination Enterprise Control Room. The status of version control is the same in both Enterprise Control Rooms. If it is enabled in the source Enterprise Control Room, manually configure version control in the destination Enterprise Control Room using a Subversion repository that is independent/separate from the 10.x version.
- Create a new unused database for 11.x. You cannot use the 10.x database for 11.x.
- Do the database migration after the platform upgrade.
- Migration of data includes the following:
  - Application settings
  - Automation bots with version history, if applicable
  - Automation schedules (migration of schedules from different time zones is not supported)
  - Bot Insight data
  - Metadata in database
  - Repository data
  - System-defined credentials
  - Users, roles, licenses, and permissions
  - 11.3.3 Historical Activity
- Migration of data excludes the following:
  - Audit logs
  - Devices/Clients

©2020 Automation Anywhere. All rights reserved.

    - License information of the source Enterprise Control Room
    - Schedule history
    - User-defined credentials
    - Version control settings

Use the following specific guidelines to plan your migration process:

- Backup the following:
    - Enterprise Control Room v10.x* SQL database
    - Enterprise Control Room v10.x* shared repository
    - Enterprise Control Room v10.x* Subversion database (if applicable)
    - Bot Insight SQL database (if applicable)
    - Bot Insight metadata database (if applicable)
- Ensure that the Automation Anywhere 10.x environment is controlled and monitored after the migration process is initiated as follows:
    - Do not create users, roles, schedules, and permissions.
    - Do not create and upload any metadata.
    - Do not check out bots (if version control is enabled)
    - Schedule and deploy only on-demand bots.

*includes Automation Anywhere 10 LTS, 10 SP2, and hot fixes with these as the base version.

After you finish

Prepare the systems hosting the source and destination Enterprise Control Room as a migration prerequisite.

Related concepts
Prepare for migration

Prepare for migration

Prepare the environment at the source and destination Enterprise Control Room. This involves ensuring access to applications in the source Enterprise Control Room, installing and setting up the destination Enterprise Control Room, other configuration setting changes in both, and more.

Plan the migration process by reviewing the considerations before preparing the source and destination Enterprise Control Room.

The required activities in the system hosting the source Enterprise Control Room are as follows:

- Access the Enterprise Control Room v10.x* repository path through a shared drive. Map the 10.x repository path set to the local drive to a shared path and provide read access to the 11.x administrator.
- Gather and make a record of the following information:
    - Credentials to connect to Enterprise Control Room v10.x* SQL Server database.
    - Master key to connect to the Credential Vault of Enterprise Control Room v10.x*.
    - Credentials to connect to the Bot Insight SQL database (applicable only if using bot Insight with Enterprise Control Room v10.x*).
    - URL of Bot Insight metadata database.

The required activities in the system hosting the destination Enterprise Control Room are as follows:

©2020 Automation Anywhere. All rights reserved.

- Set up a new infrastructure (that is separate from a 10.x* environment) with Automation Anywhere v11.x.x Enterprise Control Room already installed.
- Install the Enterprise Control Room 11.x.x license.
- Access the migration wizard by logging in to the Enterprise Control Room as an administrator.

  The administrator has View and Manage Migration permission.

- Configure the Credential Vault.
- Configure version control settings.

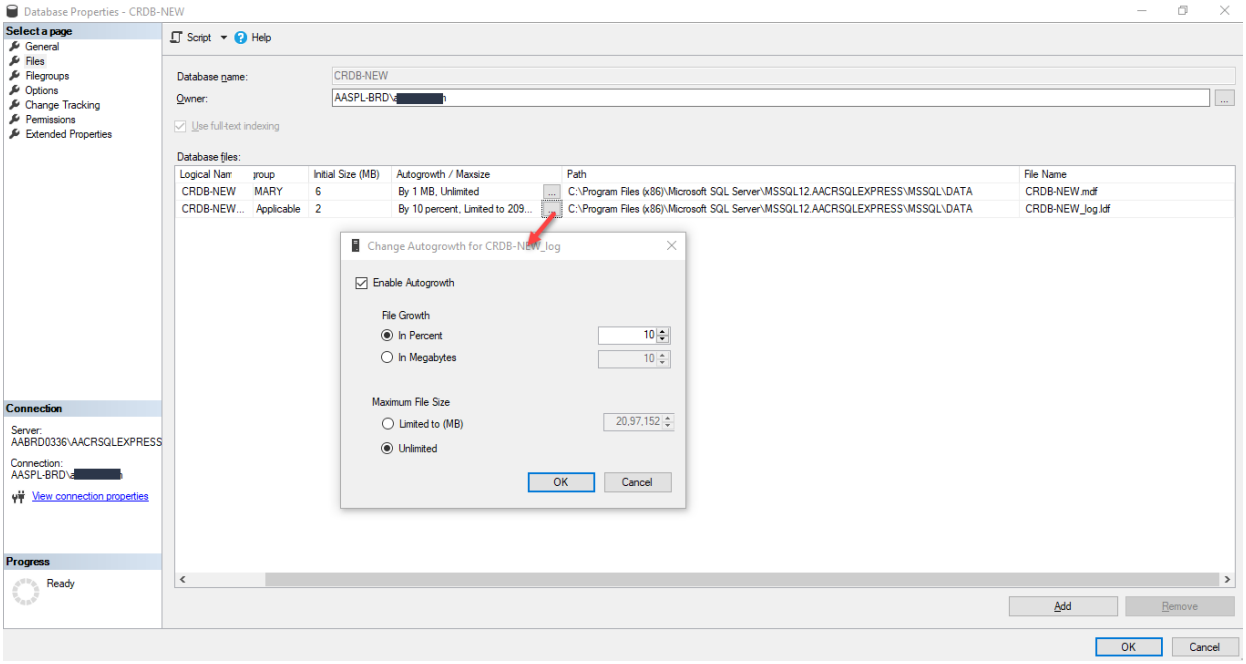
  If version control is enabled in 10.x Enterprise Control Room, enable the same in the 11.x.x Enterprise Control Room manually because the settings for version control are not migrated. Use a fresh Subversion database for 11.x.x which is different from a 10.x Subversion database. See Enterprise Control Room settings.

- Start the SQL database service if it is not running.
- Provide the user, who has the permission to run the destination Enterprise Control Room Microsoft Windows Services on the source database, access on the source database, if Windows Authentication is used to connect to the source database.
- Import the source Enterprise Control Room certificates to the Java trust store if using a secure connection, as follows:
  1. Run the command prompt in administrator mode.
  2. From the Automation Anywhere installation path, for example, C:\Program Files\Automation Anywhere\Enterprise, type or paste the following command at the prompt:

     ```
     jre\bin\java -jar certmgr.jar -appDir "C:\Program Files\Automation Any
     where\Enterprise" -importTrustCert "<Certificate Path>"
     ```

- Set the property of log files in the 11.x.x database to Enable Autogrowth to allow for maximum data processing during migration. See the following figure of the Windows UI screen:

©2020 Automation Anywhere. All rights reserved.



*includes Automation Anywhere 10 LTS, 10 SP2, and hot fixes with these as the base version.

After you finish

Start the migration process from the destination Enterprise Control Room interface.

Related tasks
Start migration wizard

Start migration wizard

Start the Migration wizard from the Enterprise Control Room interface.

Prerequisites

After meeting the prerequisites, start the migration process by doing the following steps:

1. Log in to the Enterprise Control Room 11.x.x using your first administrator credentials.
2. Go to Administration > Migration, and click Migrate data or migrate data now.
   The Migration wizard appears, containing the following tabs:
   - Database: Enables you to configure database parameters
   - Settings: Enables you to select the migration type
   - Roles/Users/Bots: Enables you to select the entities to migrate
   - Data: Enables you to review associated migration data and start the process

   Note: The migrate data now link is visible only when the migration process is initiated for the first time.

Next steps

Next, connect the source Control Room database from the source Control Room.

©2020 Automation Anywhere. All rights reserved.

Related tasks
Connect to source Control Room database

Connect to source Control Room database

Provide the source Enterprise Control Room database setting and configuration details.

Prerequisites

After starting the Migration wizard, connect to the source Enterprise Control Room 10.x database by doing the following steps:

Procedure

1. In the Database tab of the Migration wizard, keep the Use secure connection selected if the SQL instance hosting the 10.x Enterprise Control Room database is configured with a secure connection. Clear this selection if the source SQL Server is not configured with a secure connection.
2. Provide the Server host name and Server port number of the SQL Server where the Enterprise Control Room 10.x database is hosted.
3. Depending on the configured authentication method for SQL Server, do the following:
   a) Microsoft Windows: Keep the Use Windows authentication selected if the source SQL Server is configured using Microsoft Windows authentication.
   b) SQL Server: Clear the selection and provide the Username and Password, if the SQL Server is configured with SQL authentication.
4. Type the source Enterprise Control Room database name.
5. Copy the source Enterprise Control Room master key and paste it in the Master key field.
   You can now connect to the Credential Vault of the source Enterprise Control Room. The master key is shown as encrypted after you save the migration process.
6. Type the source Enterprise Control Room Repository path.
   This must be a shared path and accessible to the user on the machine doing the migration process in the destination Enterprise Control Room. Share the source Enterprise Control Room repository path up to the Automation Anywhere folder path.
   For example, D:\\Data\Automation Anywhere Server Files.
   For a stand-alone source Enterprise Control Roomwith a repository path set to a local drive, map the 10.x repository path to a shared path and provide read access to the 11.x administrator. However, if it is pointing to a local drive, the settings page of the Enterprise Control Room 10.x requires no changes.
   Important: Ensure the 10.x repository path is accessible during migration because bot migration fails if the path is inaccessible.
7. Click Save to skip migrating the Bot Insight database.

   For steps to migrate the Bot Insight database, see Connect to source Bot Insight database.

   Note: You can change the Database connection settings until the migration process starts. The database tab is disabled when the process starts.
   After you click Save, the Enterprise Control Room verifies the data provided in the preceding steps.
   - If a connection to the SQL server cannot be established, a message is shown suggesting the following:
     - The secure connection is not set correctly.
     - The server host name, port, or database name is incorrect.
     - The Use Windows authentication option is not selected.
     - The username or password is incorrect.

©2020 Automation Anywhere. All rights reserved.

- If the Master key is invalid, a message instructs you to retry.
- If the Repository path is incorrect, not shared, or inaccessible, a message advises you to verify that the path is correct and mapped to a shared drive with the required permissions.

8. Click Next to select migration of data based on roles, users, or bots.

Next steps

If installed, provide the source Enterprise Control Room Bot Insight database setting and configuration details as the next task. Otherwise, select the type of migration.
Related tasks
Connect to source Bot Insight database
Select migration type

Connect to source Bot Insight database

If installed, provide the source Enterprise Control Room Bot Insight database setting and configuration details.

Prerequisites

The Connect to source Control Room database task must be completed successfully before you can complete this task.
Connect to the source Bot Insight database by doing the following steps:

Procedure

1. In the Database tab of the Migration wizard, select Connect to 10.x Bot Insight database.
   All fields for the Bot Insight database connection are enabled.
2. Select the Use secure connection option if the SQL instance hosting the source Bot Insight database is configured with a secure connection.
3. Provide the host name and port number of the SQL Server on which the source Bot Insight database is hosted.
4. Depending on the configured authentication method for SQL Server, do the following:
   a) Microsoft Windows: Keep the Use Windows authentication selected if the source SQL Server is configured using Microsoft Windows authentication.
   b) SQL Server: Clear the selection and provide the Username and Password, if the SQL Server is configured with SQL authentication.
5. Type the source Enterprise Control Room Bot Insight database name.
6. Type the Server URL where the Bot Insight Visualization Server Port is configured.
   For example: http://productlt.example.com:82/analytics.
7. Click Save to connect to the database.
   After you click Save, the Enterprise Control Room verifies the data provided in the preceding steps.
   - If a connection to the SQL server cannot be established, a message is shown suggesting the following:
     - The secure connection is not set correctly.
     - The server host name, port, or database name is incorrect.
     - The Use Windows authentication option is not selected.
     - The username or password is incorrect.
   - If the Master key is invalid, a message instructs you to retry.
   - If the Repository path is incorrect, not shared, or inaccessible, a message advises you to verify that the path is correct and mapped to a shared drive with the required permissions.

8. Click Next to select migration of data based on roles, users, or bots.

Related tasks
Select migration type

Select migration type

Choose to migrate data from your source Enterprise Control Room based on roles, users, or bots.

Prerequisites

Complete the Connect to source Control Room database task before selecting the migration type.

If a migration process is running and you try to change the migration type, a message instructs you to retry after the previous migration completes.

However, if the machine restarts when the migration is in progress, start the migration process although the status is shown as In Progress.

Procedure

1. In the Settings tab of the Migration wizard, select the migration option:
   - Roles and associated data: In addition to the roles, data associated with those roles, for example, users, licenses, bots, folder access permissions, information about the user who created the bot, credentials, historical activity, and schedules are also migrated. Use this option. To skip migrating the data associated with the selected roles, select Exclude bots and schedules.
   - Users and associated data: In addition to the users, data associated with those users, for example, roles, licenses, bots, credentials, historical activity, and schedules are also migrated. To skip migrating the data associated with the selected users, select Exclude bots and schedules.

     If you select this option, the roles that are not associated with any user are not migrated and the schedules that are associated with the users that were not selected for migration are also not migrated.

   - Bots and Schedules: In addition to the selected bots dependent data, for example, subtasks, files, historical activity, and schedules are migrated automatically. The roles and users are not migrated.
2. If you choose to migrate data based on Bots and Schedules, do the following:
   a) Select the Exclude MetaBots option to skip migrating the MetaBots and dependent MetaBots of TaskBots.
   b) Select the Overwrite if bot already exists option, if you have the updated/latest version of bots in the source database and you must overwrite the same bot which was previously migrated to 11.x.
   c) 11.3.3 Select the Include Historical Activity option to include the task run history of the bots that are selected for migration.
   Note: Before you migrate the Historical Activity, you must migrate the associated Users and the Bots and ensure that you log in to the same Device as that of 10.x version to prevent the failure of the historical activity migration.
3. Click Next.

©2020 Automation Anywhere. All rights reserved.

Next steps

- If the Roles and associated data option is selected, the Roles page appears.
- If the Users and associated data option is selected, the Users page appears.
- If the Bots and schedules option is selected, the Bots page appears.

Related tasks
Select bots to migrate
Select MetaBots to migrate
Select users to migrate
Select roles to migrate

Select roles to migrate

Migrate all or selected roles from the source to the destination Enterprise Control Room. When you select roles, other related data, for example, licenses, users, credentials, historical activity, and schedules are also migrated.

Prerequisites

This tab is shown only if you select Roles and associated data in the Settings tab.

Before selecting the roles, review the following considerations:

- Bots and files are migrated based on users having at least one folder permission specifically, Upload, Download, or Delete.
- Migrate all system roles before migrating bots and schedules to ensure that the folder permissions are assigned properly to system roles.
- The system defined roles from source 10.x Enterprise Control Room are mapped automatically to the corresponding destination Enterprise Control Room.
- Similarly, user permissions from source 10.x Enterprise Control Room are mapped to the destination Enterprise Control Room.
- Roles that have any of the Upload, Download, or Delete permissions, are given Run/Schedule permission by default on migration.
- User-defined roles with the same name have _1 as a suffix to the name.
- Schedules from the source Enterprise Control Room that are already in the destination Enterprise Control Room are migrated with the same name.
- For the next migration run, the Available roles list shows all roles, regardless of whether they are migrated.

Procedure

1. In the Available roles list, click the check box next to Role Name to select all roles.
   Alternatively, select each role from the list.
   Note: The Available roles show all roles (both system and user-defined) that exist in the 10.x Enterprise Control Room database.
2. Add roles to the Selected list.
3. Click Next.

©2020 Automation Anywhere. All rights reserved.

Next steps

To review and verify data, see the Verify data and migrate task.
Related tasks
Verify data and migrate

Select users to migrate

Migrate all or selected users from the source to the destination Enterprise Control Room. When you select users, other related data, for example license, roles, credentials, bots, historical activity, and schedules are also migrated.

Prerequisites

This tab is shown only if you select Users and associated data in Settings tab.

Before selecting the users, review the following considerations:

- Bots and files are migrated based on the user having at least one folder permission, specifically, Upload, Download, or Delete.
- Users with same name have _1 as a suffix to the name.
- Deleted users are not migrated.
- All dependencies for a user or role are migrated based on the user's folder permissions for the assigned role.
- All user licenses are migrated automatically when you migrate the users. However, license migration is not visible on the Enterprise Control Room user interface.
- System-defined credentials related to Auto-login and Email Settings that are set in Automation Anywhere 10.x Enterprise client by the user are automatically migrated.
- A license migration for the user might fail if the destination Enterprise Control Room does not have sufficient user licenses.
- For Active Directory users, if the domain user with same name already exists in the destination Enterprise Control Room, then these users and their dependencies are skipped during migration.
- For the next migration run, the Available users list shows all users regardless of whether they are migrated.

Procedure

1. In the Available users list, click the check box next to User Name to select all users.
   Alternatively, select each user from the list of users.
2. Add users to the Selected list.
3. Click Next.

Next steps

To review and verify data, see the Verify data and migrate task.
Related tasks
Verify data and migrate

©2020 Automation Anywhere. All rights reserved.

Select bots to migrate

Migrate all or selected bots from the source to the destination Enterprise Control Room. When you select the bots, schedules associated with the bots are also migrated.

Prerequisites

This tab is shown only if you select Bots and schedules in Settings tab.

Before selecting the bots, review the following considerations:

- If the source Enterprise Control Room has Version Control enabled then:
  - The version history of both the bots and bot dependencies is migrated
  - The production version which is last set is migrated. Configure version control in the destination Enterprise Control Room manually because the source 10.x Version Control settings are not migrated.
  - Locked bots and files are unlocked and then migrated to 11.x.
  - Client Last Modified and Modified by fields for each version of the migrated bot is set to the name of the current Enterprise Control Room user running the migration process. The Modified by field of the migrated bot is set to SYSTEM if the user referencing this field is not migrated in 11.x.
  - The date of the folder creation is set to the date of the migration to the destination Enterprise Control Room when a bot is migrated for the first time. The date of the bot file is set to the system date and time when the bot file was uploaded in the source Enterprise Control Room. If version control is set, then the date of the latest version of the bot file is taken. By default, version control is not set.
- Only the selected bots with associated dependencies and schedules are migrated. Migrate roles and users separately.
- When migrating a bot and its schedule, if the user who created the schedule is not migrated to 11.x or deleted in 10.x, then these schedules are not migrated.
- Manual dependencies associated with the bot are also migrated.
- Password-protected bots and the corresponding schedules are not supported in 11.x and they cannot be migrated.
- Schedules that are password-protected are also not migrated.
- Migrating a folder is not possible. To migrate all the files in a folder, select all the files in that folder.
- If a 10.x bot to be migrated already exists in 11.x, then it is not migrated.
- If you select a bot from 10.x that has the same name in 11.x, the bot and the corresponding schedules are not migrated.
- If the Modified by field for bot(s) fails to migrate, the field shows the name as SYSTEM in the My bots and Edit page.
- When the following options are selected, do the following:
  - When Exclude MetaBots is selected, you must migrate those separately. This also means that if MetaBots are part of a TaskBot as dependency they shall NOT be migrated. Also, the My MetaBots folder is not displayed in the Folders list of the repository.
  - When Overwrite if bot already exists is selected, existing bots are overwritten if the bots were migrated from the 10.x Enterprise Control Room in a previous migration run. However, bots with same name that are created or uploaded in 11.2 are not overwritten. The migration of these bots fails.
    - The dependent subtask bots, MetaBots, and files are overwritten but schedules are not overwritten when the system overwrites bots.
    - If version control is enabled in both systems, selecting this option overwrites the version history and new version numbers are allotted to the bots.

©2020 Automation Anywhere. All rights reserved.

- 11.3.3 When Include Historical Activity is selected, the task run history of the selected bots and their dependencies are migrated from the 10.x Enterprise Control Room to the 11.x version on successful migration. If the bots were already migrated in the previous migration run and the history was not, when migrating the data next time, the migration process skips to migrate the bots and migrates the corresponding task run history. The historical activity migration fails because of the following reasons:
  - If you have not migrated the associated User and TaskBot.
  - If you have not used the same Device as that of 10.x for migration.

Procedure

1. Go to the folder from which you want to migrate the bots in the Folders list.
   The bots corresponding to the selected folder appear in the Available bots list.
2. Select the check box next to Type to select all bots from that specific folder.
   Alternatively, select specific TaskBots from the list of bots.
   Browse through all the folders and select bots from the individual folders. If the selected folder has subfolders, those also appear in this list as disabled. To migrate all bots from a subfolder, expand and select the subfolder from the Folders list and select the bots separately.
3. Add the bots to the Selected list.

   11.3.5 An unprotected bot created in 10.x and migrated to 11.x can have a duplicate GUID. Enterprise Control Room will create a new unique GUID for the migrated bot to avoid data conflict in the Bot Insight dashboard.
4. Click Next.

Next steps

Verify data and migrate
Related tasks
Verify data and migrate
Select MetaBots to migrate

Select MetaBots to migrate

MetaBots can be migrated separately by selecting the option Bots and schedules in the Settings tab. The procedure is similar to that of migrating bots.

Prerequisites

This tab is shown only if you select Bots and schedules in Settings tab.

Before selecting the MetaBots, review the following considerations:

- MetaBots are migrated based on the user having at least one folder permission, specifically upload, download, delete, or execute.
- A MetaBot is not migrated if it is a dependency of a TaskBot and the option Exclude MetaBots is selected. Migrate dependent MetaBots separately using the steps in this section.
- A MetaBot is migrated regardless of its associated role or user being migrated to the 11.x Enterprise Control Room.

©2020 Automation Anywhere. All rights reserved.

- Duplicate MetaBots are overwritten on migration only when the option Overwrite if bot already exists is selected.

- 'My MetaBots' folder permissions are not propagated when a new folder is migrated in the destination Enterprise Control Room.

Procedure

1. Go to the My MetaBots folder to migrate the bot(s) in theFolders list.
   The MetaBots corresponding to the selected folder appear in the Available bots list.
2. You have two options:
   a) Click the check box next to MetaBot to select all MetaBots from that specific folder.
   b) Select specific MetaBot from the list of MetaBots.
3. Add the bots to the Selected list.
4. Click Next.

Next steps

To review and verify data, see the Verify data and migrate task.
Related tasks
Verify data and migrate

Verify data and migrate

Review and confirm data related to the selected roles, users, or bots, with the dependent or associated data, for example MetaBots, schedules, credentials, and so on.

Prerequisites

Based on your selected options in the Settings tab, the ROLES, USERS, BOTS, SCHEDULES, and CREDENTIALS tabs are shown.

Procedure

1. Verify that the selected ROLES are available for migration:
   If the Exclude Bots and Schedules option is selected in the Settings tab, the BOTS and SCHEDULES tabs are not displayed.
2. Verify that the selected Users and the users included based on the selected roles are available for migration.
3. Verify that the selected Bots are available for migration.
   The BOTS tab does not show dependent bots or files that are added to a parent bot. After the migration process completes, the dependent bots and files are shown on the Migration Details page.
4. Verify that the Schedules associated with the bots are available for migration.
5. Verify that the system Credentials associated with the users are available for migration.
6. Click Migrate data and confirm when prompted.

©2020 Automation Anywhere. All rights reserved.

Next steps

After the migration process completes, the status of each entity (roles, users, bots, schedules, history, and credentials) appears in separate tabs. You can export details of the migration to a CSV file for record keeping and compliance.

Analyze the migration status to decide if the migration process must be rerun.

Related reference
Analyze migration status

Analyze migration status

Analyze the results after the migration process completes to track missing or incomplete data and decide if the migration process must be rerun.

Before you begin

Ensure the migration process is successfully completed before you analyze the results.

During the first migration run, the entities related to Enterprise Control Room settings, for example, the mail server configuration, email notification, and client configuration are migrated automatically.

The Migration Details page shows the status and the corresponding reasons for the status of each entity (roles, users, bots, schedules, history, and credentials) selected for migration. The status of an entity is Success, Skipped, or Failed.

- Analyzing the Success details helps to understand how the data was successfully migrated. For example, if a user or role already exists in v11.x.x, then, migration of that user or role shows a Success status. However, the migrated user or role is renamed with the suffix _1. The existing entity is not modified in v11.x.x.
- Analyzing the Skipped details helps to understand if the entity must be included in the next migration run. For example, if you select a bot from 10.x that has the same name in 11.x.x, the bot and the corresponding schedules are skipped. Make the required changes to include it in the next migration run.
- Analyzing the Failed details helps to understand the configuration changes required to ensure that the entity is migrated in the next run. For example, password-protected bots and schedules are not supported in 11.3.x and they cannot be migrated.

After you finish

You can now complete the post-migration activities.

Related tasks
Complete post-migration activities

Complete post-migration activities

After all intended entities are migrated, do the post-migration tasks before using the v11.x.x Enterprise Control Room.

©2020 Automation Anywhere. All rights reserved.

Prerequisites

To analyze the migration status, see the Analyze migration status task.

- By default, all migrated schedules are disabled. To activate schedules post-migration, manually add the devices to the migrated schedules.
- To bookmark the Dashboards for quick access and retrieval, re-create them.

Procedure

1. Do the following to on-board the migrated schedules:
   a) Install the Automation Anywhere Enterprise client v11.x.
   b) Register the Enterprise client devices with the migrated user.
   See Bot creators and bot runners - an overview .
   c) Edit the schedules to add the required devices.
   d) Enable the schedule.
   See Schedule a bot for the last two steps.
2. Remove dependencies manually from the bot.
   Manual dependencies of a schedule in 10.x are automatically migrated. Because these are static, an updated bot (new version) does not update the dependent files. The manual dependencies cannot be deleted from the bot repository. Remove them manually from the bot. Manual dependencies also do not get downloaded from the Enterprise Control Room when a bot with dependencies is downloaded.
3. Do the following to add a schedule's manual dependencies created in the source Enterprise Control Room that has version control configured:
   a) Download the required file or files, that is, do a rollback from version history.
   b) Manually add the reference dependencies.
   c) Save the task.
   d) Set the production version to run the task.
4. Migrate the dashboard bookmarks.

Migration: FAQs

Find answers to questions on specific scenarios related to migration.

1. Are the schedules created by a user existing in the destination Enterprise Control Room or deleted from source Enterprise Control Room migrated?

   No, these schedules are not migrated.

   - If an Active Directory user who created a schedule in the source, exists in the destination, then the first run of the migration shows the status for Schedules as Failed because of the following reason:
     ```
     Unable to continue as the user with same name already exists
     ```
   - If a non-Active Directory user who created a schedule in the source does not exist or is deleted in the destination, then the first run of the migration shows the status for Schedules as Failed because of the following reason:

     ```
     User <username> for this schedule does not exist
     ```

   For more information on migrating users, see Select users to migrate.

©2020 Automation Anywhere. All rights reserved.

2. IQ Bots and My Lists are deprecated from 11.2. What happens to the bots that have IQ Bots as dependent files or the files that are present in My Lists?

   IQ Bot dependency and My Lists are filtered out because they are deprecated in 11.2. These are not listed in the preview.

   For more information on migrating bots, see Select bots to migrate.

3. I am currently on Enterprise Control Room LTS and I want to migrate to Enterprise Control Room 11.2. What happens to the Repository Path field value?

   The Repository Path remains the same and this field is disabled after migrating to 11.2.

   For more information on providing the source Repository Path details, see Connect to source Control Room database.

4. I have migrated from Automation Anywhere 11.2 or earlier 11.x version to Automation Anywhere 11.3. What are the precautionary steps to recover schedules, which had disappeared in version 11.2 or earlier 11.x versions?

   Once you upgrade to version 11.3, for schedules that already exist and are visible in the Schedules page, we recommend that you first deactivate and then reactivate those schedules so that they do not go missing in the first week from the Schedules page.

   Important: (This note applies to the 11.x version before Version 11.3.2). You can deactivate and then activate only those schedules that were initiated on different weekdays than the present day. For example if a weekly schedule is set to run on Monday and the initial execution of the schedule is also Monday at 13:00 hrs, then first deactivate/activate it on any day other than Monday. You can deactivate/activate on Monday only after it runs at 13:00 hrs. See table for reference:

Schedule name	Schedule date, day, and time	Action
Schedule-1	01/07/19, Monday, 13:00 hrs	Do not deactivate and reactivate. Perform this action only after the schedule runs.
Schedule-2	01/08/19, Tuesday, 13:00 hrs	Deactivate and then reactivate
Schedule-3	01/09/19, Wednesday, 13:00 hrs	Deactivate and then reactivate

   For details on how to recover the schedules, see topic Recover schedules post upgrade after upgrading to Automation Anywhere Enterprise 11.3.

   Customers upgrading from Automation Anywhere 11.2.1 need not perform the recovery steps given in the topic as the issue was fixed in that version.

5. What are the specific considerations for migrating from 10.x to Version 11.3.x.x?

   Enterprise Control Room provides a built-in migration tool that allows existing customers to migrate their data from earlier versions of Automation Anywhere viz. 10 SP2, 10 LTS to Version 11.3.x.x. For versions before 10 LTS (10.3), customers will have to undergo a two-step migration process – first upgrading to 10 LTS and then to Version 11.3.1.

©2020 Automation Anywhere. All rights reserved.

Attention: Data can be migrated only from one SQL database instance to another SQL database instance for Enterprise Control Room DB and from PostgreSQL instance to another PostgreSQL instance for Bot Insight DB.

Migration from Microsoft SQL Server to Oracle Server for Enterprise Control Room DB and PostgreSQL Server to Microsoft SQL Server for Bot Insight DB is not supported in the current version.

6. 11.3.3 What are the specific considerations for migrating the Historical Activity from version 10.x to version 11.x?
   - You must migrate the corresponding Users and Bots from version 10.x. See Select bots to migrate.
   - You must log in with the same migrated user, using the same Device or Client with the same Fully Qualified Domain Name (FQDN) as that of 10.x.

     For example: If John was logged in MY-DEVICE-NAME.COM device in 10.x, the same user in 11.x, John must be logged in to the same MY-DEVICE-NAME.COM device.

7. 11.3.3 Is it possible to migrate the Historical Activity using API?

   Yes, migration of historical activity is supported by API and UI both.

8. 11.3.3 My machine is affected by virus and is destroyed. Will I be able to migrate the Historical Activity?
   No, you cannot migrate the Historical Activity. You require the same machine to migrate the Historical Activity. The migration process can also fail if the same device is unavailable due to the following reasons:
   - If the virtual machine is destroyed.
   - If the same machine is used but the host name is changed.

Bots - Overview

As a Enterprise Control Room user with administrator or My Bots privileges, you can use the bots module of Enterprise Control Room to do the following.

- Run and schedule uploaded bots
- Run bot with queue
- Export bot files for Business Life-cycle Management
- Import bot files for Business Life-cycle Management
- Work with secure and centralized credentials

Note: To perform these actions, you must be an administrator or have the following roles and privileges.

- View my bots
- Run my bots
- Export bots
- Import bots
  Note: You can not schedule or run Attended Bot Runners from the Enterprise Control Room. Only Unattended Bot Runners are available for Run operation.

©2020 Automation Anywhere. All rights reserved.

- Credentials- Overview
  Passwords and other sensitive information such as user credentials, account number, and social security numbers included in automation tasks are encrypted and stored as credentials centrally in the Credential Vault.
- My bots- overview
  As a Bot Creator, when you upload files from Enterprise client, the files are displayed on the My bots page.

Credentials- Overview

Passwords and other sensitive information such as user credentials, account number, and social security numbers included in automation tasks are encrypted and stored as credentials centrally in the Credential Vault.

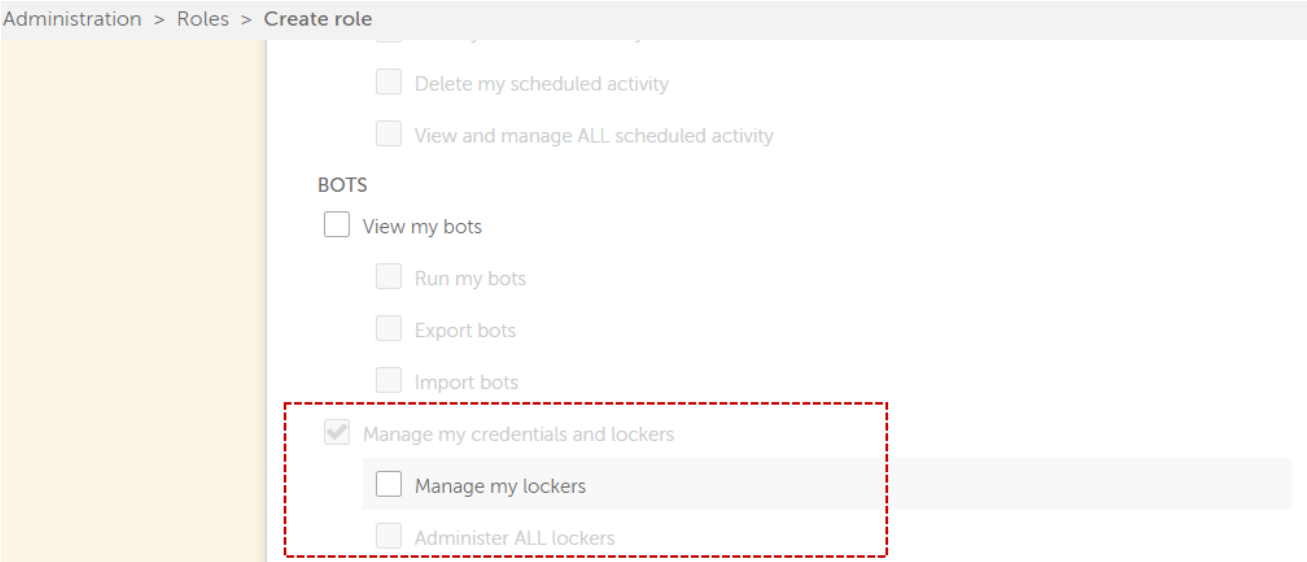
All Enterprise Control Room users can create credentials.

Benefits of creating credentials

Apart from providing a secure and centralized location for storing credentials, it:

- Minimizes the possibility of credential fraud.
- Provides an environment to enable improved security.
- Enables businesses to adhere to processes and credential management compliance.
- Offers increased automation opportunities with secure data or applications.

Roles permission for credential and locker management



Manage my credentials and lockers: By default, you (all users) can see the Credentials tab and manage your own credentials. In addition, you can interact with locker of other users, if they provide locker access permission.

Lockers- Overview.

My Credentials

This tab consists the list of credentials created by a user. All users have permission to see their credentials.

In case you have AAE_Locker Admin permission, then you can view credentials of all the users. In the search pane you can filter credentials according to the credential name.

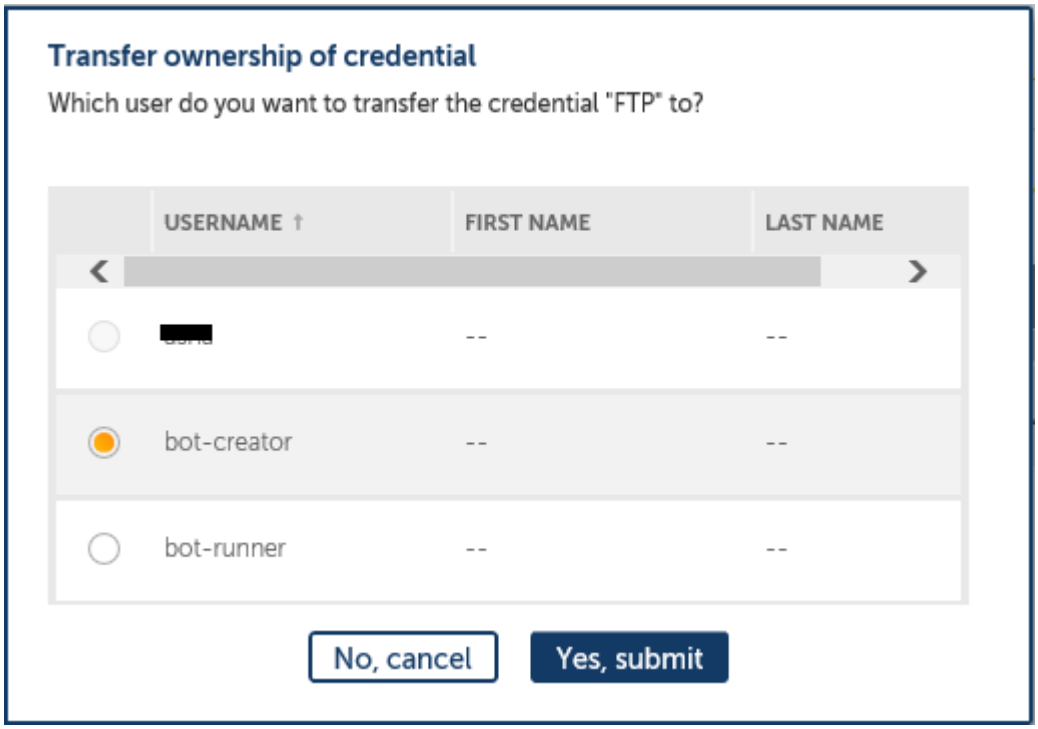
The following table describes the list of items that can be viewed:

Table Item	Description
Type	Shows the type of credential as user-provided or standard.
Name	Name of the credential.
Locker Name	Name of the assigned locker for the credential.
My Access	Credential owner: Credential has been created by you. Credential non-owner: Credential has been created by other user.
Request Status	All values provided: Value has been given. Requests sent: Request has been sent to users to input credential value.
Credential Owner	Name of the user who has created the credential.
Last Modified	Date and time when the credential was last edited.
Modified By	Name of the user who has modified/edited the credential. Note: 11.3.4 You must have the View user basic permission to view information about the user who last modified the folder.

The following describes the list of actions that can be done on individual entries in the table:

Actions	Description
View	Allows you to view credential details. .Learn more
Edit	Allows you to edit a credential. Learn more
Delete	Allows you to delete a credential.

©2020 Automation Anywhere. All rights reserved.

Actions	Description
	• To delete a credential, user must be a credential owner • To delete a credential, click Accept. Learn more
Transfer Credential Ownership	Allows you to transfer the ownership of the credential. If locker is assigned to your credential then the ownership can be transferred to any member of the locker. Else it can be transferred to any user in the system. After the ownership is transferred to another user, the previous owner can no longer access the credentials. Also, only a Locker Admin has permission to transfer credential ownership. Select the user and click Submit. 

Alternatively, you can select all credentials and perform the following table-level actions:

Table Item	Description
Refresh	Allows you to refresh the list of credentials.
Delete	Allows you to delete multiple credentials.

©2020 Automation Anywhere. All rights reserved.

Table Item	Description
Customize columns	Allows you to show or hide specific columns. By default, all the columns are displayed.

Audit Logs

Create, Update, Delete, and Transfer Credential Ownership actions are tracked in audit logs for record keeping and future use. You can refer those entries in the Audit log page.

- Create a credential
  As an automation expert, Credential Vault provisions you to securely create and store your credentials. Therefore, it ensures that your credentials can be used in bots without compromising security with safe deployment of tasks. Any authorized user can create credentials.
- View a credential
  As an authorized user, you can view details such as the credential details, attribute name, description, credential type and value, and general details of any credential.
- Edit a credential
  Enterprise Control Room user can edit details of a credential. This is useful in scenarios where you might want to make changes to your credential definition and value.
- Delete a credential
  A credential owner can select the delete option to remove redundant credentials from the system. If you are not a credential owner, then you cannot delete a credential.
- Lockers- Overview
  A locker is used to group related sensitive information, which is included in automation tasks in the form of credentials and shared with other users.
- Set up a locker and assign relevant credentials
  A locker is used to group related sensitive information and can be shared with other users. A locker can be included in automation tasks in the form of credentials. You set up a locker and assign the necessary credentials to allow your bots secure access to relevant systems.
- Create a locker
  A user with locker admin or manage my locker permission is authorized to create a locker. A locker can be used to group similar credentials and share it with other users.
- View a locker
  Any user with Manage my lockers permission can view their own lockers. This provides information such as credentials assigned to the locker, locker owners, locker managers, locker consumers, and locker participants.
- Edit a locker
  Enterprise Control Room users with AAE_Locker Admin role or any user having edit permission can edit their own lockers and access this feature.
- Delete a locker
  To eliminate redundant lockers from the system, a locker owner can perform the delete action.
- Credential requests
  A Enterprise Control Room user can send credential requests to locker consumers. That means, when a user-provided credential is added to a locker, all locker consumers receive a credential request to fill in their credential values.
- Credential Vault email notifications
  In Enterprise Control Room, if the email notification setting is enabled, users are notified if any important changes are made to the credentials and lockers.

©2020 Automation Anywhere. All rights reserved.

Related tasks
Create a credential
View a credential
Edit a credential
Delete a credential

Create a credential

As an automation expert, Credential Vault provisions you to securely create and store your credentials. Therefore, it ensures that your credentials can be used in bots without compromising security with safe deployment of tasks. Any authorized user can create credentials.

To create credential, follow the steps mentioned below:

Procedure

1. Login to Enterprise Control Room, click Bots > Credentials.
2. Click the Create credential button or click create a credential under the credentials tab (This option is displayed only when you are creating your first credential.)
   This opens the Create credentials page in which you can add maximum 50 attributes to your credentials. When you create the 50th attribute, the page updates to show the message: "Credentials can only have a maximum of 50 attributes".
3. Provide Credential details such as Credential name and Description (optional).
4. Enter the following Attribute details:
   - Attribute name
   - Description (optional)
   - Value:
     - Standard: The credential owner must enter the value. All consumers see the same credential value set by the credential owner.
     - User-provided: The value field is grayed out as the values are to be provided by the consumer and not preset during creation. Only consumers of the locker containing this credential can provide the value.

   You can chose the following security related options to be applicable on the value you input:

   - Masked: To hide the value that you type behind special characters (bullets) so that the actual value of the attribute is not visible.
   - 11.3.2 This is a password: To mark a particular attribute as password type.

     An attribute with this option selected will only be available in those credential variables supported commands in Automation Anywhere Enterprise client where the fields are of Password type.

     This ensures the attribute is not exposed and its value cannot be printed in a notepad or any other 'plain text' application.

     For commands supporting fields that are of Password type, see Credential variables.

5. Click Create credential.
   If you already have an existing locker, then you can assign your credential to the respective one while adding Credential details. If no locker has been created then you must create a locker and then assign your credential.

©2020 Automation Anywhere. All rights reserved.

A notification is displayed when your credential has been successfully created. After your credential is successfully created, it is visible in the list of credentials tab.

If email notification setting is enabled and credentials are added to a locker, then all the locker consumers shall receive an email.

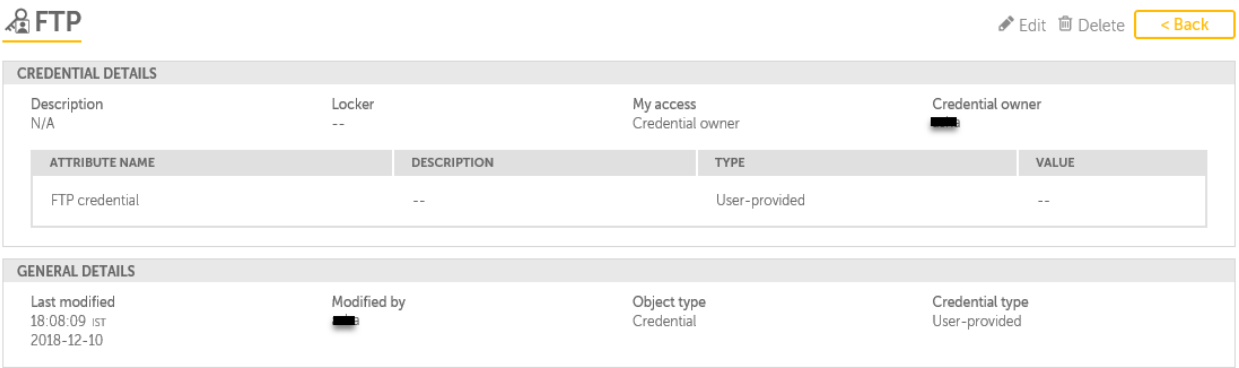
Related tasks
Create a locker

View a credential

As an authorized user, you can view details such as the credential details, attribute name, description, credential type and value, and general details of any credential.

Procedure

1. Go to Bots > Credentials.
2. In My Credentials tab, choose the credential. Go to action list and click View credential.
   View credential page is displayed with the following details:



- Edit credential- Allows you to modify the your credential.
- Delete credential- Allows you to delete your credential.
- Credential details- Description and credential owner.
- Attribute name, credential description, type, value

- General details- last modified (date and time), modified by, object type, credential type.

Edit a credential

Enterprise Control Room user can edit details of a credential. This is useful in scenarios where you might want to make changes to your credential definition and value.

If a credential type is user-provided, then locker consumers have permission to edit the credential and their credential value.

©2020 Automation Anywhere. All rights reserved.

Procedure

1. Click Bots > Credentials
2. Select the credential and click Edit credential.
   If your credential is assigned to a locker, then you can only edit the value of common attribute. And if the attribute is user-provided, then the locker consumers can edit the value.
3. In the Edit credentials page, and make the required changes.

   If email notification setting is enabled and credentials are added to a locker, then all the locker consumers shall receive an email. Learn more

   - A credential can be edited by a credential owner, or if the credential type is user-provided then locker consumers can edit the credential value.
   - In case of user-provided credential, you can only edit General information such as adding or removing a locker.
   - In case of standard credential, you can edit General information such as adding or removing a locker and Attribute detail such as the credential value.

4. After you complete editing the credential, click Save changes or click Cancel to undo the changes.
   The maximum limit of credential attributes that is allowed is 50. Hence, if you have upgraded to the current version from 11.1.2 or less, and have migrated credentials that have more than 50 attributes, when editing that particular credential, the following message is displayed:
   Credentials can only have a maximum of 50 attributes.
   To continue, remove the additional attributes that cannot be saved and add those to a new credential.

Delete a credential

A credential owner can select the delete option to remove redundant credentials from the system. If you are not a credential owner, then you cannot delete a credential.

Prerequisites

Procedure

1. Click Bots > Credentials.
2. Select the credential under the My credentials tab.
3. Hover over the actions list and click .
   If a locker is assigned to a credential, then it cannot be deleted.
4. Click Yes, delete to delete your credential and No, cancel to cancel deletion.
5. To delete multiple credentials, you must perform table level delete action. Select the multiple credentials and click .

Lockers- Overview

A locker is used to group related sensitive information, which is included in automation tasks in the form of credentials and shared with other users.

©2020 Automation Anywhere. All rights reserved.

This enables separation of duties for credential management and consumption. Users with the following permissions can work with lockers:

- Manage my lockers: This permission allows you to create and manage your own locker.
- Administer ALL lockers: This permission allows you to view all the lockers and perform limited actions on them. This permission is available for AAE_Locker Admin role only

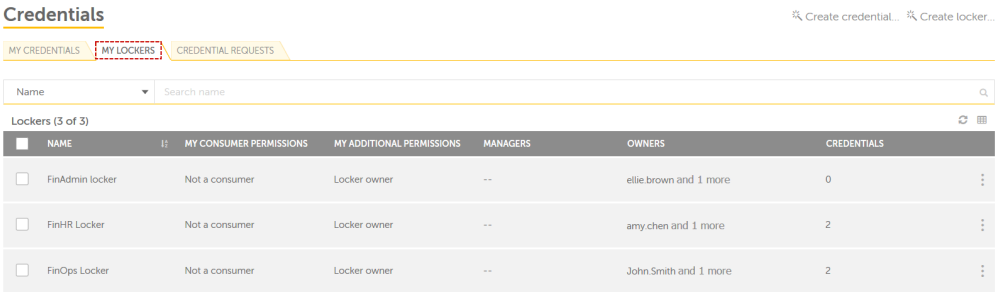
The roles and permissions related to locker management are:

- Locker Owner: A locker owner can edit, view, and delete a locker, and can add or remove other owners.
- Locker Manager: A locker manager has access to all the functions of a locker owner, but does not have permission to add owners, managers, or participants to the locker.
- Locker Participants: A locker participant has access to view a locker and its participants, and can also add their own credentials to a locker. A locker participant can not access or view credentials created by other users.
- Locker Consumers: Locker consumers have access to view a locker and input a credential attribute value (if the attribute is configured for user-input). When you select one or more user-defined roles, the users who have these selected roles become consumers of the locker.

My Lockers

My Lockers tab in Bots → Credentials shows the list of lockers that has been created by a user. A locker can only be created by an authorized user with Locker_Admin permission or a user having Manage my locker permission.

Note: Users can see lockers only if they have created them or if they are a member of that locker.



In the search pane you can filter lockers based on locker name.

The following describes the list of items that can be viewed in the table:

Table Item	Description
Name	Name of the locker.
My consumer permission	Consumer or not a consumer.
My additional permission	Locker participant, Locker manager, Locker owner.

©2020 Automation Anywhere. All rights reserved.

Table Item	Description
Managers	Users having locker manager permission.
Credentials	No. of credentials assigned to a locker.
Owners	Name of user who created the locker.
Last Modified	Date and time when the locker was last edited/modified.
Modified By	Name of the user who has modified/edited the locker.

Actions	Description
View	Enables you to view locker. Learn more
Edit	Enables you to edit a locker. Learn more
Delete	Enables you to delete a locker. Learn more

Alternatively, you can select all lockers and perform the following actions:

Table Item	Description
Refresh	Enables you to refresh the list of lockers.
Delete	Enables you to delete multiple lockers. Learn more
Customize columns	Enables you to show or hide specific columns. By default, all the columns are displayed.

Audit Logs

All the Create, Update, Delete actions are tracked in audit logs for record keeping and future use. You can refer those entries in the Audit log page.
Related tasks
Create a locker
View a locker
Edit a locker
Delete a locker

©2020 Automation Anywhere. All rights reserved.

Set up a locker and assign relevant credentials

A locker is used to group related sensitive information and can be shared with other users. A locker can be included in automation tasks in the form of credentials. You set up a locker and assign the necessary credentials to allow your bots secure access to relevant systems.

Do the following to set up your locker and assign the credentials:

Step 1: Create a role
You can define a role and assign permissions to access various features of the Enterprise Control Room. Only an admin or Enterprise Control Room user with roles permission can assign roles to users and provide access to them for various features and operations.

Step 2: Create a credential
Log in to Enterprise Control Room as a locker administrator and create a credential. As an automation expert, Credential Vault provisions you to securely create and store your credentials. Therefore, it ensures that your credentials can be used in bots without compromising security with safe deployment of tasks. Any authorized user can create credentials.

Step 3: Create a locker
As part of the locker creation procedure, assign the newly created credential and role to the locker. A user with locker admin or manage my locker permission is authorized to create a locker. A locker can be used to group similar credentials and share it with other users.

Related reference
Default licenses and roles for bot tasks

Create a locker

A user with locker admin or manage my locker permission is authorized to create a locker. A locker can be used to group similar credentials and share it with other users.

Prerequisites

You must have created one or more user-defined roles so that you can assign Locker consumers.
To create a locker, follow the steps mentioned below:

Procedure

1. Go to Bots > Credentials
2. In My Lockers tab, click Create locker.
   The Create locker page is displayed.
3. Enter locker name and locker description.
4. Enter Credentials.
   Shows the available credentials owned by the user. You can select one or multiple credentials from the list and add it to the locker.
   If email notification setting is enabled and credentials are added to a locker, then all the locker consumers shall receive an email. Learn more
5. Add Owners.
   A locker owner can edit, view, delete a locker and can add or remove other owners. Also, an owner can be a locker consumer but cannot be a manager or participant within the same locker.

©2020 Automation Anywhere. All rights reserved.

Note: 11.3.4 You must have the View user basic permission to view information about other users to add them as locker owners.

6. Enter Managers.
   A locker manager has access to all the functionality like a locker owner, but they do not have permission to add owners, managers, or participants to the locker. Disabled users cannot be selected as locker managers if they were already selected as owners in the previous tab.

   Note: 11.3.4 You must have the View user basic permission to view information about other users to add them as locker managers.
7. Add Participants.
   A locker participant has access to view a locker and participants can also add their own credentials to a locker. A locker participant does not have access or visibility of credentials created by other users.

   Note: 11.3.4 You must have the View user basic permission to view information about other users in order to add them as locker participants.
8. Add Consumers.
   You must select one or more roles. The users belonging to these selected roles are the consumers of the lockers. These users have access to view a locker and input credential value.
   System-created roles are not displayed in the consumer list.
   If the credential type is:
   - Standard: Locker consumers can view the locker and all the credentials inside the locker. They are able to use credentials in the locker when running a bot. All consumers see the same credential value set by the credential owner.
   - User-provided: Locker consumers can input their information in user-provided credentials with user-provided attributes (i.e. credential value). Consist of same usability as Standard credential.
9. Click Create locker.
   If email notification setting is enabled, all locker consumers receive an email to edit the credential value if the credential type is user-provided.

Related tasks
Configuring email notification settings
Related reference
Credential Vault email notifications

View a locker

Any user with Manage my lockers permission can view their own lockers. This provides information such as credentials assigned to the locker, locker owners, locker managers, locker consumers, and locker participants.

Procedure

1. Go to Bots > Credentials
2. In My Lockers tab, choose the locker. Go to action list and click View locker.
   View locker page displays the following details:
   - Edit locker- Allows you to modify your locker.
   - Delete locker- Allows you to delete your locker.
   - Credentials- Shows list of credentials added to the locker.
   - Owners- Shows list of locker owners.

     Note: 11.3.4 You must have the View user basic permission to view information about other users in order to add them as locker owners.
   - Managers- Shows list of locker managers.

Note: 11.3.4 You must have the View user basic permission to view information about other users to added as locker managers.

- Participants- Shows the list of locker participants. Locker participants can view this locker. They can add their own credentials to a locker. They can view their credentials, but not other credentials in the locker.

  Note: 11.3.4 You must have the View user basic permission to view information about other users to added as locker participants.
- Consumers- Shows the list of locker consumers. Locker consumers can view this locker and all the credentials inside the locker. A locker consumer with user-provided credential type have two additional permissions:

  a) They will be able to input their information in user-provided credentials with user-provided attributes.

  b) They will be able to use credentials in this locker when running a bot.

Related tasks
Edit a locker

Edit a locker

Enterprise Control Room users with AAE_Locker Admin role or any user having edit permission can edit their own lockers and access this feature.

Prerequisites

To edit a locker, follow the steps mentioned below:

Procedure

1. Go to Bots > Credentials
2. In My Lockers tab, select the locker to edit. Then on the action list, click edit locker.
   Only a locker owner or locker admin has permission to edit a locker. You can make changes to the following:

   - Credentials- Add or remove credentials that are assigned to a locker.

   - Owners- Add or remove locker owners.

     Note: 11.3.4 You must have the View user basic permission to view information about other users in order to add them as locker owners.
   - Managers- Add or remove locker managers.

     Note: 11.3.4 You must have the View user basic permission to view information about other users to added as locker managers.
   - Participants- Add or remove locker participants.

     Note: 11.3.4 You must have the View user basic permission to view information about other users to added as locker participants.
   - Consumers- Add or remove locker consumers.

     If email notification setting is enabled and credentials are added to a locker, then all the locker consumers shall receive an email.

©2020 Automation Anywhere. All rights reserved.

3. Click Save changes after you finish editing the locker.

Related reference
Credential Vault email notifications

Delete a locker

To eliminate redundant lockers from the system, a locker owner can perform the delete action.

Procedure

1. Go to Bots > Credentials.
2. In My Lockers tab, choose the locker. Mouse over to actions list and click .
3. Click Yes, delete to delete your locker and No, cancel to cancel deletion.

Credential requests

A Enterprise Control Room user can send credential requests to locker consumers. That means, when a user-provided credential is added to a locker, all locker consumers receive a credential request to fill in their credential values.

Prerequisites

To generate credential request, follow the steps mentioned below:

Procedure

1. Go to Bots > Credentials.
2. Create a credential with credential type as user-provided.
3. Assign your credential to a locker.
4. After all the consumers input the credential value, the status of the credential changes to complete. If email notification setting is enabled and credentials are added to a locker, then all the locker consumers shall receive an email to input the credential value.

Related tasks
Create a credential
Related reference
Credential Vault email notifications

Credential Vault email notifications

In Enterprise Control Room, if the email notification setting is enabled, users are notified if any important changes are made to the credentials and lockers.

Email notifications are sent for each scenario:

Credential is added to a locker

©2020 Automation Anywhere. All rights reserved.

When a new credential is added to a locker a notification is sent to all consumers of the locker to their email address registered in the Enterprise Control Room. The email consists of a link to the credential that is added to the locker. The consumers are redirected to edit the credential page wherein they must input the credential value.

Member is added or removed from a locker

An email notification is sent when a new member (co-owner or participant) is added to a locker or removed from the locker as a member of participant.

Change in permission for locker members

When a locker owner/ admin, grants or removes locker membership permissions from a locker, an email notification is sent to the locker members at their email address. This ensures that members are notified of their membership changes within the locker.

Locker consumer gets added or removed from a role assigned to a locker, and consumer role gets added or removed from a locker

When a role assigned to a locker is modified by addition or removal of users, an email notification is sent to the new or existing user at their email address so that the consumers are notified that credentials are pending for their input in the locker.

Also when a new role added to a locker or an existing role is revoked from the locker, an email notification is sent to the new or existing consumers at their email address so that the consumers are made aware of the changes.

My bots- overview

As a Bot Creator, when you upload files from Enterprise client, the files are displayed on the My bots page.

This page is divided into the following areas.

- Folders
- Files and folders

Note: As a Enterprise Control Room user, you must have the right privileges to access this page. Folders for which you do not have access to will not be visible to you.

The My bots page also allows you to perform tasks, such as exploring your documents, executable files, MetaBots, reports, scripts, tasks, and workflows from the Folders area. It also allows you to:

- Import bot files
- Export bot files
- Run a Bot
- Schedule a bot
- Run bot with queue

You can apply search parameters to the Name column.

You can specify the search parameters in the search bar for Name.

©2020 Automation Anywhere. All rights reserved.

- Files and folder(s)
  When you click a folder from the Folders area in the My bots page, the contents of the folder are displayed in the Files and Folders area.
- Create and edit folders
  As a Enterprise Control Room user with View my bots and Create Folder privileges, you can create folders in the Enterprise Control Room repository.
- View Bot details
  The View bot page provides information such as the name and other details of the bot. You can also either run the bot or schedule when to run the bot.
- View folder details
  You can use the View folder page to view the details of the folder and search for items within the folder.
- Folders area
  Use the folders area to explore and browse your documents, executable files, MetaBots, reports, scripts, tasks, and workflows.
- Run a Bot
  The bots must be checked into a Control Room repository so that they are available for production deployment. Users with Run my Bots privileges might then deploy and execute the bots from the In progress, Scheduled, or My Bots page.
- Delete bots and folders
  As an Enterprise Control Room admin or user with Delete Bot privileges, you can delete one or more bots and folders that are uploaded by a Bot Creator from the Enterprise client. This option is not available when version control is enabled.
- Force unlock bots
  As an Enterprise Control Room user with Unlock Bot privileges, you can forcefully unlock one or more bots that are checked out by a Bot Creator in the Enterprise client. This option is available only when version control is enabled.
- Bot Lifecycle Management (BLM) - an overview
  As a Enterprise Control Room user with export or import bots module permission, you can move your bots (new or updated) from one environment to another using Bot Lifecycle Management module in the Enterprise Control Room. For example, you can move the bots that are verified as production ready from staging to production.
- Export bots
  As an Enterprise Control Room user with BLM Export module permission and download privileges for Tasks, Docs, Workflows, and Reports and execute permission for MetaBots, you can export bots and dependent files in different automation environments to help manage your organization's Bot Lifecycle Management (BLM).
- Import bots
  As a Enterprise Control Room user with BLM Import module permission, and Upload privileges for Tasks, MetaBots, Docs, Workflows, and Reports, you can import bots and dependent files that were exported by another Enterprise Control Room user in different automation environments to help manage your organization's Bot Lifecycle Management (BLM).

Files and folder(s)

When you click a folder from the Folders area in the My bots page, the contents of the folder are displayed in the Files and Folders area.

When Version Control is enabled, the version related columns are displayed. If production version is set for a file, the information displayed in the rest of the columns, such as size is for that version.

©2020 Automation Anywhere. All rights reserved.

The columns of the Files and folders table are described in the following table.

Item	Description
Type	The type of file- Folder or TaskBot. This is based on the type of the file in the folder.
Name	The name of the folder or file.
Size	The size of the file.
Client last modified	• The date on which the file was last modified on the Bot Creator machine before it was uploaded to the Enterprise Control Room. • If version control is enabled and the Production Version is set, the date is the one when that particular production version was last modified before it was uploaded to the Enterprise Control Room.
Last Modified	The date and time when the file was last updated.
Modified by	Name of the user who last modified the file or folder.

You can perform the following actions on a column to help you work efficiently.

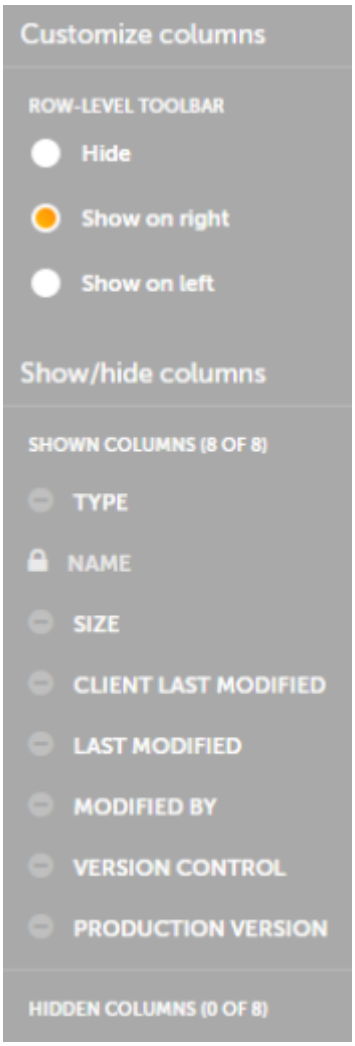
- Click a column to sort it in ascending and descending order. You can sort up to three columns by holding the Shift key when you click two more columns. This gives you the option of sorting two additional columns. This way the sorting is done on the entire table and not just the data that is currently visible to you. The last sorting is stored in memory applied by a user per session.
- Use a drag-and-drop operation to move the column left or right.
- Move your mouse cursor at the end of the column and drag to re-size.

You can perform the following tasks on an individual file or folder in the Files and folders area.

Action	Description
Run	Enables you to Run the selected Bot.
Unlock bot	Enables you to forcefully unlock the selected bot if locked for editing by the Bot Creator in Enterprise Client.
Schedule	Schedule the bot to run.
Edit folder	Enables you to rename a folder.
View	Enables you to view details of the file or folder.
Delete Folder / bot	Enables you to delete a bot, file or folder. Note: This option is not available when Version Control is enabled.
Note: Only Edit, View and Delete options are available for folders.	

©2020 Automation Anywhere. All rights reserved.

Alternatively, you can select all Bots or Folders and perform the following actions. Note that these actions can be performed only at a table level and not on individual items.

Item	Description
Create folder	Enables you to create a folder from the Files and folders section.
Customize columns	Enables you to customize columns such as show or hide specific columns. By default, all columns are displayed:  Note: Columns Version Control and Production Version are only visible when version control is enabled.
Actions column	To show the Actions column on the left, click the Customize columns and click the Show on left radio button. To show it on the right, click the Show on right radio button.

©2020 Automation Anywhere. All rights reserved.

Item	Description
	To hide the Actions column, click the Hide radio button.
Unlock checked items	Enables you to forcefully unlock selected Bots (multiple) if locked for editing by the Bot Creator in Enterprise client. Note: This option is available only when Version Control is enabled.
Delete checked items	Enables you to delete the selected or all Bots or Folders (multiple). Note: This option is not available when Version Control is enabled.

Create and edit folders

As a Enterprise Control Room user with View my bots and Create Folder privileges, you can create folders in the Enterprise Control Room repository.

This enables you to grant access privileges to Bot Creators or Bot Runners to specific folders so that they can upload, download, delete, and execute (MetaBots only) their bots to the Enterprise Control Room.

If you have Edit Folder privileges, you can also rename the folders to which you have access.

Create a folder

1. Go to Activity → My Bots →Folders area
2. Click a folder in the Folders tree view to open it. For example My Task → Sample Tasks:
3. Click Icon that is given above the Files and folders list
4. The Create folder page is launched:
5. Provide an appropriate name. For example, you might want the Bot Creator with analytics license to store tasks to the Analytics-Task folder.
6. Click Create Folder to save the folder.

   Alternatively, click Cancel if you do not want to save changes and go back to the My Bots page.

7. The folder is added which can be viewed in the Folders tree view and Files and folders list:

Rename a folder

For some reason, such as a typo or change in naming conventions, you might want to rename a folder. This section describes how to rename the folder.

1. Go to Activity → My Bots →Folders area
2. Click a folder in the Folders tree view to open it. For example My Task → Sample Tasks.
3. In the Files and folders list, hover over the Settings for the folder that you want to rename. This slides open the actions panel.
4. Click Edit. The Edit folder page is launched:
5. Update the folder name as required:

©2020 Automation Anywhere. All rights reserved.

6. Click Save changes.

   Alternatively, click Cancel if you do not want to save changes.

Audit Logs

When you create or rename a folder, the audit entries are logged.

View Bot details

The View bot page provides information such as the name and other details of the bot. You can also either run the bot or schedule when to run the bot.

When you click the View icon for a bot in the Files and folders area of the My bots page, the View bot page opens.

When version control is enabled and the production version is set, the View bot page also displays the Production version and Version control fields.

If the Automatically assign the latest version option is selected in the Settings > Bots (Version Control) page, all the production versions of the bot are set to the latest version. See Bots - Configure Version Control.

Notes:

- When version control is enabled, the dependencies that are displayed are based on whether production version is enabled or not.
- When production version is enabled, the dependencies for that production version of the bot and its dependents are displayed.
- When production version is not enabled for any dependent file, the dependency information for that bot is not displayed.

The following table lists the different areas of the View bot page.

Area	Description
TaskBot details	Use this area to view the following details of the folder: • Size: Displays the size of the bot in KB or MB. • Path: The location of the bot. • Production version: The production version that is set either manually or assigned automatically. • Version Control: The status of the bot, whether it is locked or unlocked for editing by the Bot Creator. • Client Last Modified: The date on which the file was last modified on the Bot Creator machine before it was uploaded to the Enterprise Control Room.

©2020 Automation Anywhere. All rights reserved.

	If version control is enabled and the production version is set, the date is when that particular production version was last set by Enterprise Control Room user. Note: Production version and version control details are visible only when version control is enabled.
Manage dependencies	Enables you to manually add or remove dependencies to or from the TaskBot during bot deployment from the Enterprise Control Room. You can access the My Docs, My Exes, and My Scripts folders to add dependencies. Note: You must have Run or Schedule, or Run + Schedule permissions to access these folders.
Review dependencies for <bot name>	Displays the bot and its dependencies. The dependency icon will display red if you do not have sufficient privileges for the dependent bot or file. 11.3.1.5 The manually added dependencies are tagged as `Manual`.
General details	Use this area to view the following details for the folder: • Last modified: Displays the date and time when changes were last made to the folder. • Modified by: Displays the name of the user who last made changes to the folder. Note: 11.3.4 You must have the View user basic permission to view information about the user who last modified the folder. • Bot type: Displays the type of the bot, such as TaskBot or MetaBot. • Object type: Displays the object type, such as bot.

- Add or remove manual dependencies
  Use the Manage Dependencies option from the Enterprise Control Room to manually add or remove dependent files to or from a TaskBot during bot deployment.

Add or remove manual dependencies

11.3.1.5 Use the Manage Dependencies option from the Enterprise Control Room to manually add or remove dependent files to or from a TaskBot during bot deployment.

Prerequisites

Note: This feature is available only for Enterprise Control Room Version 11.3.1.5.

©2020 Automation Anywhere. All rights reserved.

You require the following permissions:

- Ensure you have Run my bots or View and manage ALL scheduled activity, or both feature permissions.
- If Version Control System is enabled, a user with Schedule bots permission must set the production version.

Procedure

1. Navigate to Bots > My bots.
2. From the left panel, select a folder from the Folders list that contains the TaskBot.
   Important: The folder containing the TaskBot must have Run or Schedule, or Run + Schedule permissions to manage the dependencies.
3. Click the vertical ellipsis of the TaskBot (.atmx file) to which you want to add the dependent files.
4. Select the View bot option.
   The details of the TaskBot appears.
5. Click the Manage Dependencies option.
6. On the left panel, select a folder from the Folders list to add dependent files to the TaskBot.
   Note: You can manage dependencies only from My Docs, My Exes, and My Scripts folders or subfolders. You must have Run or Schedule, or Run + Schedule permissions on these folders.
7. On the page that appears, choose one of the following actions:

Option	Action
Add dependencies	Select the dependencies listed in the Available items and move them to the Selected items. You can add the same file as a Reference dependency as well as a Manual dependency to the TaskBot. Recommendation: The best practice is not to add TaskBots (.atmx files) as manual dependencies. If they are added, the dependency will not be deployed on the Bot Runner machine.
Remove dependencies	Select the dependencies listed in the Selected items and move them to the Available items items.

8. Click Update to save the changes.
   The manual dependencies are added to the Review dependencies for <taskbot> section on the View bot page and tagged as `Manual`.

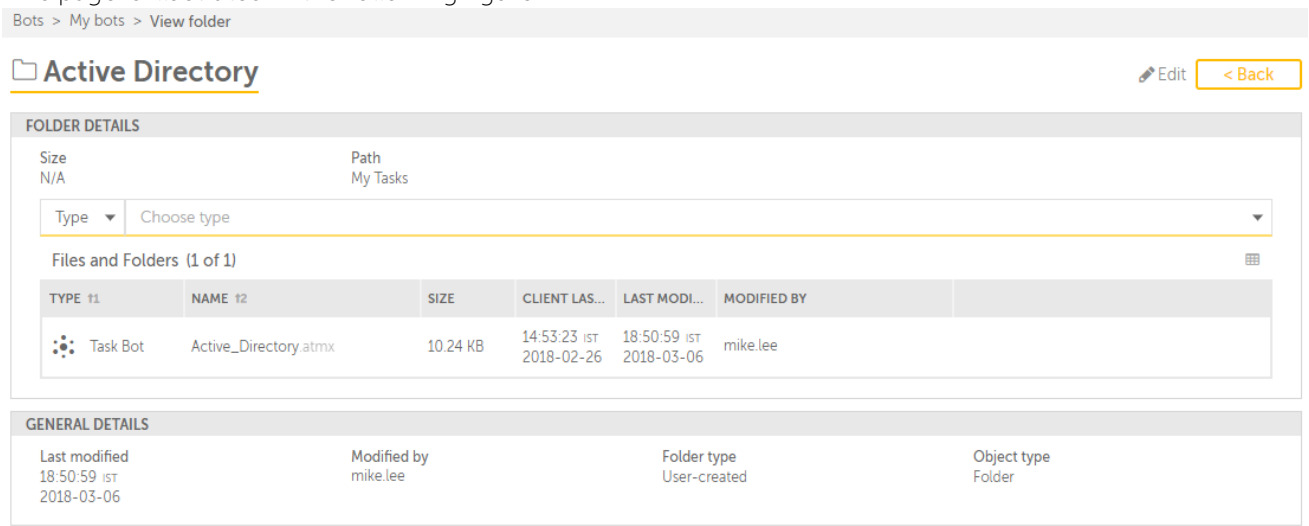
After the manual dependencies are added to the TaskBot, the dependencies are resolved during bot automation.

View folder details

You can use the View folder page to view the details of the folder and search for items within the folder.

©2020 Automation Anywhere. All rights reserved.

When you click the View icon for a folder in the Files and folders area, the View folder page is opened. This page is illustrated in the following figure.



The View folder page is divided into the following areas.

- Folder details
- Items in folder
- General details

These are explained in the following table.

Area	Description
Folder details	Use this area to view the following details of the folder • Size: Displays the size of the folder. • Path: The path of the folder.
Items in folder	Use this area to search and view the following details for items in the folder. • Type: The type of the item, such as TaskBot,MetaBot, or IQ Bot. • Name: The name of the item. • Size: The size of the item in KB or MB. • Client Last Modified: The date on which the file was last modified on the Bot Creator machine before it was uploaded to the Enterprise Control Room. If the version control is enabled and the production version is set, the date is the one when that particular production version was last set by Enterprise Control Room user. • Last Modified: Displays the last time changes were made to the item in time and date.

©2020 Automation Anywhere. All rights reserved.

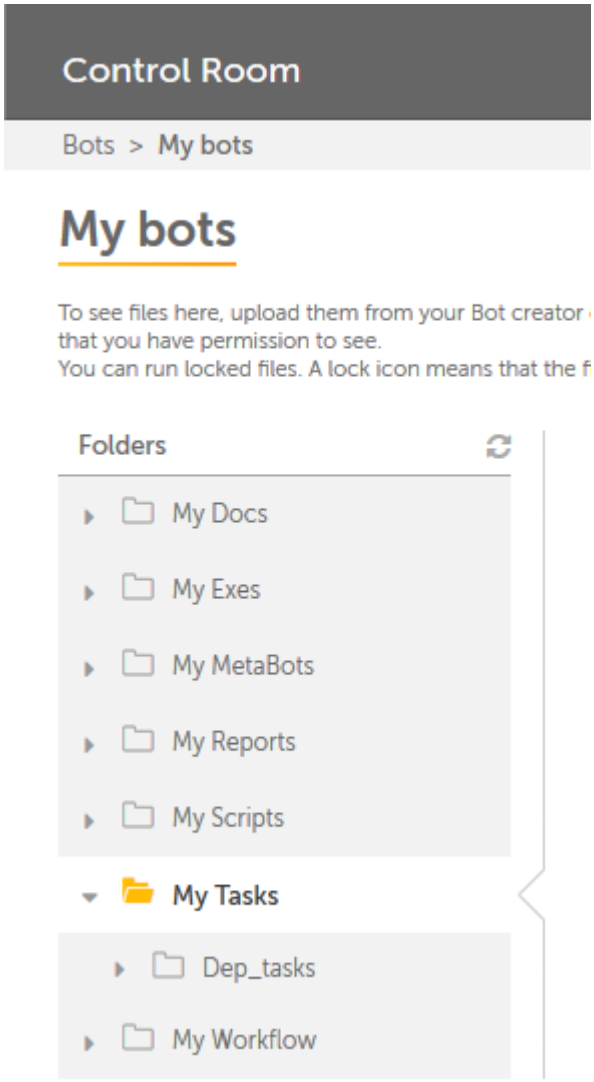
	• Modified: Displays the name of the user who last made changes to the item
General details	Use this area to view the following details for the folder. • Last Modified: Displays the last time changes were made to the folder in date and time. • Modified by: Displays the name of the user who last made changes to the folder in date and time. • Object type: Displays the type of Object, such as folder or sub-folder.

Folders area

Use the folders area to explore and browse your documents, executable files, MetaBots, reports, scripts, tasks, and workflows.

The view might differ for various users depending on their roles and privileges. When you click a folder, the contents of the folder are displayed in the Files and Folders area.

©2020 Automation Anywhere. All rights reserved.



Run a Bot

The bots must be checked into a Control Room repository so that they are available for production deployment. Users with Run my Bots privileges might then deploy and execute the bots from the In progress, Scheduled, or My Bots page.

Prerequisites

- Ensure you have Run my bots privilege.
- Ensure a client with Bot Runner license is connected to the Enterprise Control Room.

Procedure

1. Login to Enterprise Control Room.

©2020 Automation Anywhere. All rights reserved.

2. Click Bots > My bots.
   My bots page that has only the bots created by users with Unattended Bot Runner license is displayed.
   Note: You cannot run bots created by users with attended Bot Runners license.
3. Click Run bot > Run bot now.
   Run bot now page is displayed.
4. Under Select a TaskBot tab, select a folder that contains bots.

   The TYPE and NAME of the bot are displayed.

   Note: You can only access the folders for which you have Run Schedule privileges.
5. Select a TaskBot.
6. Click the → icon.

   The bot is added to the Review dependencies for Files-Folders section.

   Note: When you run a bot, automation can fail if:
   - Any of the bot dependencies are missing.
   - You do not have folder privileges for the dependencies.
   - You do not have Run Schedule privileges (icon appears).
7. Click Next.

   Available devices and bot runners in the Enterprise Control Room are displayed.

8. (Optional) Select Run Bot Runner Session on Control Room.

   This allows the Enterprise Control Room to take Remote Desktop Protocol (RDP) of the Bot Runner machine to run a scheduled task, if it is in locked or logged off state. This method is recommended when Bots are deployed on virtual machines and terminal servers. See Guidelines for RDP-based bot deployment.

9. Select any bot under the Available bot runners section, and click the → icon.
   Note: You can only select a connected Bot Runner devices, as disconnected devices are not enabled. Also, if a device is not displayed, ensure the device has an active Bot Runner session.
10. Click Next.
11. (Optional) Under the General tab, update the Name and Description.
    The [bot name].[DD.MM.YY][HH.MM.SS].[USERNAME] format is available by default, which you can change as per your preference.
12. Click Run Now.
    The selected bot is initiated and you can view the progress under the In Progress activity page.
    Note: Run now is disabled if the device is disconnected or the required fields are not filled.

- Guidelines for RDP-based bot deployment
  When you deploy a bot from the Enterprise Control Room to any Bot Runner, it attempts an auto-login (if the Bot Runner is locked or logged off). However, auto-login is prone to security policies set on the machine. Therefore, certain policies might have to be relaxed for the auto-login function.

Related reference
Guidelines for RDP-based bot deployment

©2020 Automation Anywhere. All rights reserved.

Guidelines for RDP-based bot deployment

When you deploy a bot from the Enterprise Control Room to any Bot Runner, it attempts an auto-login (if the Bot Runner is locked or logged off). However, auto-login is prone to security policies set on the machine. Therefore, certain policies might have to be relaxed for the auto-login function.

To reduce these issues, you can use Remote Desktop Protocol (RDP) based bot deployment that is introduced in the Enterprise Control Room from Automation Anywhere Enterprise 10SP2.

RDP-based bot deployment: When a bot is deployed from the Enterprise Control Room on a Bot Runner, the Enterprise Control Room handles the Bot Runner session through RDP and executes the bot.

Key features and benefits

- The bot runs in the Bot Runner RDP session in the Enterprise Control Room in the background. This ensures that no activities are visible in the Enterprise Control Room.
- Auto-login issues are reduced as it is not attempted.
  Note: Auto-login is only attempted if RDP fails.
- As the Bot Runner machine does not log in automatically, security issues related to `live monitor` scenarios are also reduced.

To ensure that the RDP-based bot deployment works seamlessly, there are certain prerequisites and settings necessary in the Enterprise Control Room and the Bot Runner machine.

Prerequisites

Settings on Bot Runner

- The `Run Bot Runner` session on Enterprise Control Room (RDP-based deployment) succeeds with legal disclaimer enabled.
  If the Bypass Legal Disclaimer option is enabled on the Bot Runner (Tools > Options > Login Settings in Enterprise client), the `Run Bot Runner session on Enterprise Control Room` (RDP-based deployment) succeeds even if the Enterprise client has legal disclaimers enabled.
  Note: Ensure the Enterprise Control Room and Enterprise client are upgraded to Version 11.3.4 before deploying the bot with the `Bot Runner` session on `Enterprise Control Room` and Legal Disclaimer enabled.
- The RDP connection must be enabled on the Bot Runner.
  1. Enabling RDP on Bot Runner machine.

     On the Bot Runner machine, ensure that remote connections to Bot Runner are allowed from My Computer properties. Ensure you select the Allow connections only from check box.

  2. Enabling RDP on Bot Runner on the virtual machine (Azure, VMware, Oracle Virtual Box).

     To enable RDP on the virtual machine, see the specific documentation on the virtual machine host.

  3. Enabling RDP on the Bot Runner hosted on Citrix XenDesktop.

     https://support.citrix.com/article/CTX129184/

©2020 Automation Anywhere. All rights reserved.

4. Enabling RDP on the Bot Runner hosted on the terminal server.

   See the documentation on Managing Remote Desktop Services Connections.

   For Windows Server 2008 R2, see https://technet.microsoft.com/en-us/library/cc772051(v=ws.11).aspx.

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

Click Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Connections. Ensure the Restrict Remote Desktop Services users to a single Remote Desktop Services session is enabled.

Note: The same user cannot log in multiple times to the terminal server. However, multiple users are not restricted from connecting to the terminal server.

Ensure the Bot Runner machine is allowed to accept incoming RDP requests and connection with saved credentials. You can ensure this by disabling the group policy Bot Runner machine in Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Security Always prompt for password upon connection.

When the group policy is enabled, during RDP Client login (for example, AARemoteMachineConnector.exe), a request to input the credentials is prompted because the target machine does not accept incoming connections through any RDP client in which the user has supplied credentials.

Enterprise Control Room settings

- Allow connections even when there are certificate errors.

  On the Enterprise Control Room, ensure the Don't ask me again for connections to this computer option is enabled.

- In the Enterprise Control Room AppServer machine, in order to run the RDP sessions, the user executing the Automation Anywhere Control Room Service (service logon user) must have administrator rights on that machine. When an RDP session is run, AARemoteMachineConnector.exe will be run in the Task Manager. The service logon user must have administrator rights in order to run AARemoteMachineConnector.exe.
- If the Enterprise Control Room cannot resolve the IP address of the Bot Runner in the Devices tab, the `RDP deployment not getting triggered` message appears. Use the nslookup command (for example, C:\> nslookup WIN-56888IBQ23P) to review this issue, and contact the administrator for further assistance.
  Note: It is mandatory that the Enterprise Control Room obtains the IP address with the Bot Runner name that is displayed in the Devices tab.

Changing screen resolution for Bot Runner session on Enterprise Control Room

It is recommended that you add the screen resolution configuration of the Bot Runner machine. This ensures your automation runs seamlessly during RDP-based deployment, even if the resolution of the screen varies between the Bot Runner and Enterprise Control Room. You can do this by configuring the deployment properties file of the Enterprise Control Room at the following location:

C:\Program Files\Automation Anywhere\Enterprise\Config\deployment.properties
Add the following:

©2020 Automation Anywhere. All rights reserved.

```
rdp.desktop.height=768
```

```
rdp.desktop.width=1366
```

```
rdp.port=3389
```

Note: Configure the height, width, and port value based on your requirement.

- FAQs
  While every effort is made to address all possible questions, please contact us if you have additional questions that must be included.

Related reference
FAQs

FAQs

While every effort is made to address all possible questions, please contact us if you have additional questions that must be included.

Is there one RDP session per Bot Runner?
Yes.

Do I need to ramp up the Enterprise Control Room RAM for RDP Based Deployment?
You might ramp it up depending on the bot deployment scenarios. A typical RDP session takes around 150MB of RAM. So, if you are deploying onto 10 Bot Runner, 1.5GB RAM is consumed. It is recommended that you increase the RAM to 16 GB if extensive bot deployment is required. Refer the Hardware Requirements section for Enterprise Control Room in the AAE - Installation Guide that is shipped with the product.

Will the RDP sessions terminate when the bot is executed?
Yes.

Can a Enterprise Control Room user see the active RDP Session?
No. User cannot see the active RDP Session as it is a background process. However, the user can see it under the Task Manager > Processes tab.

While the bot is executed in a RDP session on the Enterprise Control Room, if the Bot Runner user logs in to the Bot Runner, does it impact the bot execution?
As soon as the user logs in to the Bot Runner, the RDP session on the Enterprise Control Room terminates. The bot continues to run, and is visible to the user on the Bot Runner.

In the above scenario, if the user locks/logs off/disconnects the RDP session on the machine, what happens to the current executing bot?
If a user locks/disconnects the RDP session, the bot continues to run in the background. However, the screen based commands might display errors. If a user logs off the RDP session, the bot execution is terminated.

©2020 Automation Anywhere. All rights reserved.

While selecting Remote based bot deployment, the AA player is taking more time to come up. Is the performance affected by new functionality?

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

What is the impact if RDP connection is very slow?

Let us assume that the Enterprise Control Room takes about 30 seconds to RDP. The bot execution start-up is delayed by 30 seconds for that Bot Runner. Beyond that, if RDP session does not get connected, then the Enterprise Control Room deploys the bot through the legacy route (auto-login).

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

Older RDP session is disconnected and the task is executed on new RDP Session, which is created by Enterprise Control Room.

If RDP Session crashes in between bot execution, does the Enterprise Control Room restart the session without impacting bot execution?

Yes, RDP has an inbuilt capability to reconnect. But that works only for certain duration. So, if Bot Runner gets disconnect for longer time, then it impacts the execution of the bot.

Further to the above scenario, there is possibility of bot displaying errors due to RDP disconnection. How would a developer/Enterprise Control Room User differentiate a failure between RDP and Actual bot error? If not, a developer might spend long time (impacting production execution) analyzing the code while the actual impact was due to RDP session, which might not require any code change.

If bot displays errors, then it is automatically audited in the Enterprise Control Room. For RDP disconnect case, we have kept the list of reasons for disconnection and we are storing this in a log file. See IMsTscAxEvents.

If RDP Session crashes, is the occurance and status of bot captured in the Audit log even though the RDP crashed?

Yes, the bot continues to run on Bot Runner and the required audit of success or failure is logged.

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

Ideally, there cannot be any RDP TIMEOUT as it can impact the execution of the bot.

Does the RDP based Bot Deployment work with Bot Schedules as well?

Yes, there is an option to select the RDP based Bot Deployment while scheduling the bot from Enterprise Control Room.

Can it be configured with other RPD tools like VMware clients?

It cannot be configured currently, but might be in one of the future updates.

If a user's Active Directory (AD) password has changed when the Enterprise Control Room tries to RDP, will it update the new password by syncing with the AD?

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

If a bot is scheduled to deploy onto a 100 Bot Runner, will the Enterprise Control Room invoke RDP onto all 100 Bot Runners asynchronously or sequentially?

RDP sessions is created on the Enterprise Control Room box and deploys the bot asynchronously on these Bot Runners.

©2020 Automation Anywhere. All rights reserved.

Consider a scenario where a bot is deployed onto 10 Bot Runners. If Enterprise Control Room is unable to RDP onto the fifth Bot Runner, will it move onto the sixth Bot Runner, or the entire process is aborted?

As it is happening in parallel, RDP failure of one Bot Runner does not impact the other. The Enterprise Control Room moves onto the next Bot Runner.

If Bot Runner is unable to terminate the RDP session, is the Enterprise Control Room admin notified or is it logged in the Audit trail?

The Enterprise Control Room admin must manually terminate the Bot Runner's RDP session.

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

Yes, this works in the HA-DR mode. In that case, the RDP sessions are deployed on the Enterprise Control Room Server that deploys the bots.

Delete bots and folders

As an Enterprise Control Room admin or user with Delete Bot privileges, you can delete one or more bots and folders that are uploaded by a Bot Creator from the Enterprise client. This option is not available when version control is enabled.

Delete a bot

You can delete a (single) bot that is uploaded by the Bot Creator from the Enterprise client.

Note: 11.3.5 For audit and compliance purposes, even if a bot is deleted, the run history of the bot is not deleted from the Historical Activity page.

To delete a bot from the Enterprise Control Room:

1. Click Bots > My Bots.

   The My Bots page appears.

2. In the Files and folders list, hover over the action menu (vertical ellipsis) for the bot that you want to delete.
3. Click Delete bot.
4. Select Yes, delete to confirm.

   The bot is deleted permanently.

   Select No, cancel to go back to the Files and folders list without deleting the bot.

Note: 11.3.2 You cannot delete a bot that is listed in one or more active or inactive schedules. You must delete the schedule before deleting the bot.

Delete multiple bots

You can delete selected (multiple) bots that are uploaded by the Bot Creator from the Enterprise client.

To delete bots from the Enterprise Control Room:

©2020 Automation Anywhere. All rights reserved.

1. Go to Bots > My Bots.

   My Bots page appears.

2. In the Files and folders list, select the bots that you want to delete by selecting the corresponding check boxes.
3. Click Delete checked items option above the table.
4. Select Yes, delete to confirm.
5. Click No, cancel to go back to the Files and folders list without deleting the bots.

Note: 11.3.2 If any of the selected bots is listed in one or more active or inactive schedule, that bot cannot be deleted.

Delete folders

The method to delete one or more folders is similar to deleting bots. You can choose to delete multiple folders from the table level or individually from the files and folders list.

The folder that you want to delete should be empty.

Delete dependent bots and files

When you delete one or more bots, its dependent bots and files are not deleted automatically. If you do not require these, you have to delete them manually from the folder where they reside.

When you try to delete a bot that is part of another bot as a dependency, you cannot delete that bot and an error message appears listing the dependencies. If you want to delete the bot, you must remove the dependent bots first and try the delete action again.

Audit Log

For all the bots that are deleted, audit entries are logged in the Audit Logs page.

Force unlock bots

As an Enterprise Control Room user with Unlock Bot privileges, you can forcefully unlock one or more bots that are checked out by a Bot Creator in the Enterprise client. This option is available only when version control is enabled.

Unlock a bot

You can forcefully unlock a bot (single) if locked for editing by the Bot Creatoror in Enterprise client.

To unlock a checked out bot from the Enterprise Control Room:

1. Go to Bots > My Bots.

   The My Bots page is launched.

2. In the Files and folders list for the bot that is locked, hover over ⋮.

©2020 Automation Anywhere. All rights reserved.

3. Click .
    - Select Yes, unlock to confirm. The bot is unlocked successfully.
    - Select No, cancel to go back to the Files and folders list without unlocking the bot.

Unlock multiple bots

You can forcefully unlock selected bots (multiple) if locked for editing by the Bot Creator in Enterprise client.

To unlock checked out bots from the Enterprise Control Room:

1. Go to Bots > My Bots.

   The My Bots page is launched.

2. In the Files and folders list, select bots that are locked by clicking the corresponding check boxes.
3. Click the icon above the table.

   The system display a message box that provides information about the user that has locked the bot.

   Note: 11.3.4 You must have the View user basic permission to view information about the user that has locked the bot.

- Select Yes, unlock to confirm.
- Click No, cancel to go back to the Files and folders list without unlocking the bots.

  If Bots that are already in Unlocked state are selected, the Enterprise Control Room skips unlocking them.

Audit Logs

For all the bots that are forcefully unlocked, audit entries are logged in the Audit log page.

The status of an unsuccessful unlock is shown with its reason in the Results column of the Audit logs details page.

Bot Lifecycle Management (BLM) - an overview

As a Enterprise Control Room user with export or import bots module permission, you can move your bots (new or updated) from one environment to another using Bot Lifecycle Management module in the Enterprise Control Room. For example, you can move the bots that are verified as production ready from staging to production.

The process can be performed in two stages:

1. Export Bots from one environment of a source Enterprise Control Room
2. Import Bots to another environment of a destination Enterprise Control Room

You can choose to Export and Import using two methods:

- Enterprise Control Room user interface

©2020 Automation Anywhere. All rights reserved.

- API to export and import Bot Lifecycle Management

Export bots

As an Enterprise Control Room user with BLM Export module permission and download privileges for Tasks, Docs, Workflows, and Reports and execute permission for MetaBots, you can export bots and dependent files in different automation environments to help manage your organization's Bot Lifecycle Management (BLM).

The exported package can then be imported into another Enterprise Control Room environment. See Import bots.

Export bot files - version control disabled

1. Go to the Bots > My Bots page.
2. Click Export bot files.

   This opens the Select Bots page where you must select the bots that you want to export.

3. Select Task Bot from the list of Available items.

   You can choose either all the files by selecting the check box in the header row or certain files by selecting the check boxes beside each file.

4. Select the check box for the bots you want to export, and then click the right arrow icon.
   Note: The Selected bots panel will be available either below the Available items list or on the right of the list based on your screen's resolution. If it is below, the down arrow is displayed, and if it is on the right, the right arrow is displayed for bot selection.
5. Click Next.
6. In the Summary page that opens, provide the Export package name and choose to exclude a bot or dependency file from the list.
   a) Rename the package if you want to change the default export package name assigned by the system.
   b) Optionally, provide a password that will be used to import the package.

   The password should be set based on the Enterprise Control Room password policy and one that can be easily remembered.

   Note: The provided password is not stored anywhere in the Enterprise Control Room. If you provide a password, the package is encrypted with AES 256-Bits and cannot be accessed outside of the Enterprise Control Room.
   c) Select the Exclude MetaBots option if you do not want to include the MetaBot associated with the task in the package.
   If the TaskBot comprises of dependent bots (TaskBots, MetaBots) and files, they are also automatically selected for export. The dependency type for these bots is shown as User selected if the bot or file was added by a user manually or as Supports <bot path>/<bot name> if it was included automatically by the system. This allows you to include or exclude a bot from the export package based on your automation flow.
   Note: If any dependent file appears more than once, it is included in the package only once.
7. Click Export.

©2020 Automation Anywhere. All rights reserved.

The package is successfully exported to the default folder for downloads.

For messages related to export, see the section Export bot files - Validations

Export bot files- version control enabled

Before you use export bot files in an Enterprise Control Room that has version control, ensure that the production version of bots and their dependencies is already set.

To export bot files:

1. Go to the Bots > My Bots page.
2. Click Export bot files.

   This opens the Select Bots page where you must select the bots that you want to export.

3. Select TaskBot from the list of Available items. You can choose either all the files by selecting the check box in the header row or certain files by selecting the check box beside each file.
4. Select the check box for the bots you want to export, and then click the right arrow icon.
   Note: The Selected bots panel is displayed either below the Available items list or on the right of the list based on your screen's resolution. If it is below, the down arrow is displayed, and if it is on the right, the right arrow is displayed for bot selection.
5. Click Next.
6. In the Summary page that appears, provide the Export package name and or choose to exclude a bot or dependency file from the list.
   a) Rename the package if you want to change the default export package name assigned by the system.
   b) Optionally, provide a password that will be used to import the package.

   The password should be set based on the Enterprise Control Room password policy and one that can be easily remembered.

   Note: The provided password is not stored anywhere in the Enterprise Control Room. If you provide a password, the package is encrypted with AES 256-Bits and cannot be accessed outside of the Enterprise Control Room.
   - c) Only those TaskBots and MetaBots are available for selection for which production version is set. Hence, if the production version is not set for TaskBots and MetaBots, they cannot be exported. For other types such as Docs, Workflows, and Reports, the files with the latest version are allowed for export.
   - d) If the TaskBot comprises of dependent bots (TaskBots, MetaBots) and files, they will also be selected for export. The dependency type for these bots is shown as User selected if you select the bot manually or as Supports <bot path>/<bot name> if it is included automatically because it is a dependency. This allows you to include or exclude a bot from the export package based on your automation flow.
     Note: If any dependent file appears more than once, it is included in the package only once.

   e) Select the Exclude MetaBots option if you do not want to include the MetaBot associated with the task in the package.
7. Click Export.
   - Click Cancel if you do not want to proceed.
   - Click Back to go to the previous page.

   Note: You can export bots without having the AAE_ADMIN role. However, the dashboard related information will not be exported. To export dashboards, you must have the AAE_ADMIN role assigned to you.

©2020 Automation Anywhere. All rights reserved.

The package is successfully exported to the default folder for downloads.

For messages related to export, see the section Export bot files - Validations

Note: If the Email settings are enabled for export and Import operations of a BLM package, an email notification is sent to the user who performs the export whether the action succeeded or failed.

Export bots - validations

When you export bot files, the system checks for the following validations during export:

- Whether the bot or dependent file is available in the Enterprise Control Room
- Whether you have download permission (Execute permission for MetaBot) on one or more bot or dependent files of the selected bots
- Whether the production version is set for all the selected bots or dependent files

If any of the validation fails for one or more bot, those are automatically excluded from the package and shown in the Items not allowed to export section. You can choose to either fix those error messages and come back to export or you can export the rest of the bots shown in the Items to export section.

Audit logs

An audit entry is logged in the Enterprise Control Room audit log page when you export bots.

Related concepts
Audit log overview

Import bots

As a Enterprise Control Room user with BLM Import module permission, and Upload privileges for Tasks, MetaBots, Docs, Workflows, and Reports, you can import bots and dependent files that were exported by another Enterprise Control Room user in different automation environments to help manage your organization's Bot Lifecycle Management (BLM).

11.3.5 An unprotected bot imported through the Bot Lifecycle Management package import can have a duplicate GUID. Enterprise Control Room will create a new unique GUID for the imported bot to avoid data conflict in the Bot Insight dashboard. If a protected bot or multiple protected bots having duplicate GUID are imported through the Bot Lifecycle Management package import, a validation message is displayed stating the reasons why the bot cannot be imported.

Before you import bots and files

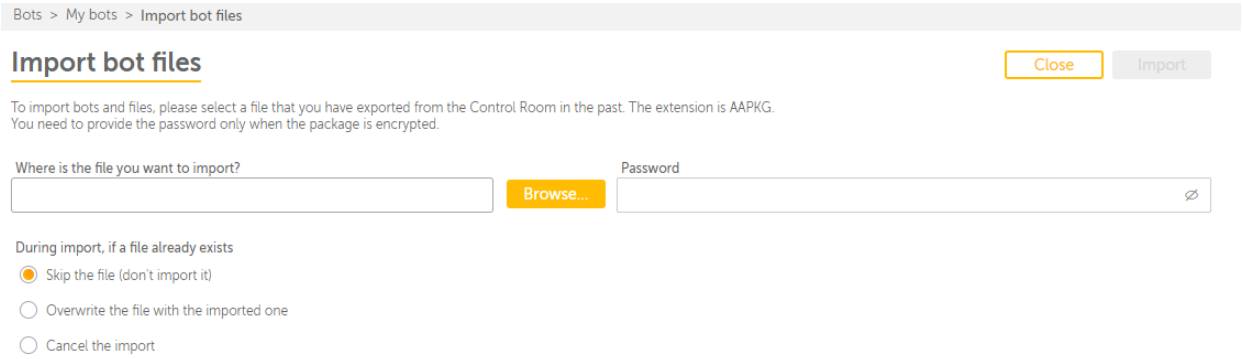
Before you import bots from Enterprise Control Room versions earlier to 11.2.x to Enterprise Control Room Version 11.3.1, ensure the bot names do not comprise of Unicode characters. If the bot names have Unicode characters, rename the bot in the earlier 11.2.x version and export again or export the same bot from 11.3 and then import to Enterprise Control Room 11.3.1.
Note: You can import bots without having the AAE_ADMIN role. However, the dashboard related information will not be imported. To import dashboards, you need to have the AAE_ADMIN role assigned to you.

©2020 Automation Anywhere. All rights reserved.

Import bot files - version control disabled

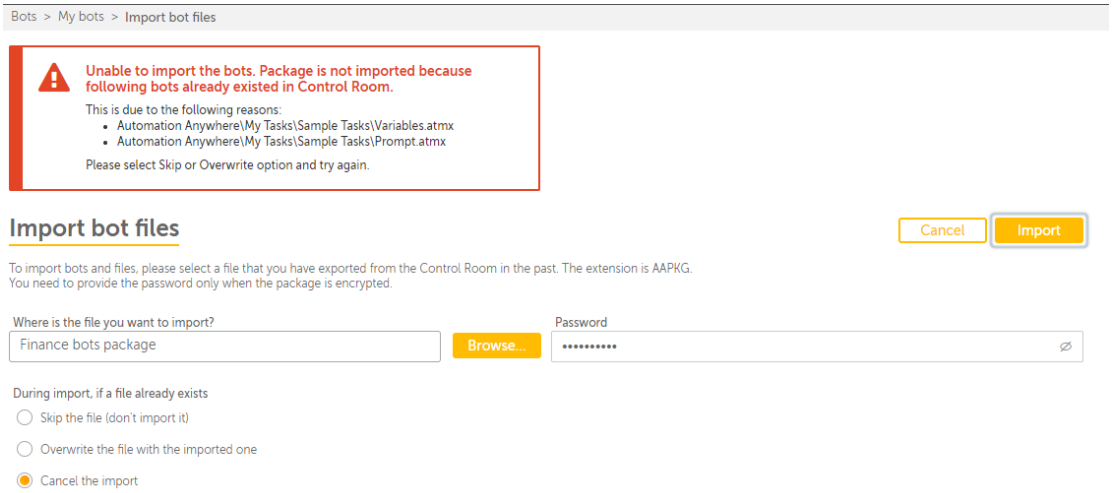
To import bot files:

1. Go to Bots > My Bots page
2. Click Import Bot Files.
3. This launches the Import bot wizard page wherein you must select the package file that was exported by another Enterprise Control Room user:



4. To select the file, click Browse.
5. Go to the source folder where the exported package was stored and shared by the Enterprise Control Room user with Export Bots privileges.
6. Select the required package - it has an AAPKG extension.
7. If encrypted, provide the same password that was used for export from source Enterprise Control Room.
8. If some of the files that are being imported from the package are already available in the Enterprise Control Room, you can choose to,
    - Skip the file(s) and not import the duplicate files
    - Overwrite the existing files with the imported ones
    - Cancel the import action.
      Note: When you use this option, the entire import operation is canceled and if at least one file already exists in Enterprise Control Room. In this case, no bots will be imported into Enterprise Control Room.
        - When you select Skip or Overwrite options, and click Import the files are successfully imported.
        - However, when you select Cancel and click Import, you are prompted to select either of the above options.

©2020 Automation Anywhere. All rights reserved.

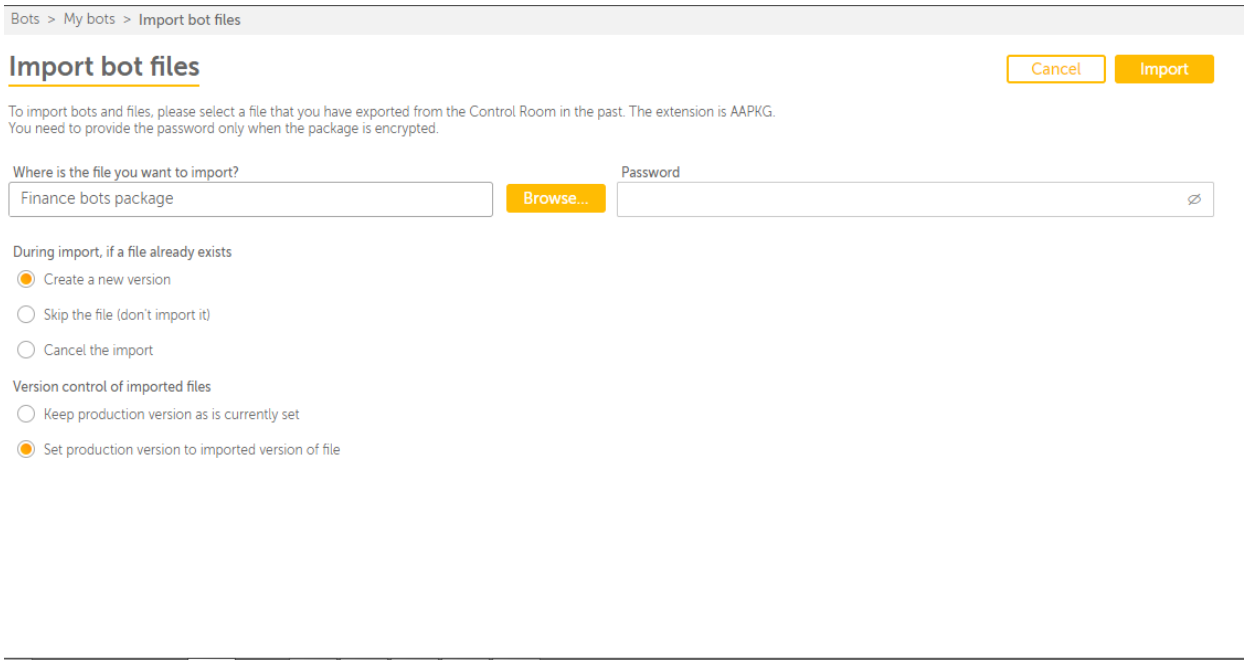


9. After the bots are imported successfully, you return to the My Bots page.

Import bot files - version control enabled

To import bot files:

1. Go to Bots > My Bots page
2. Click Import Bot Files.
3. This launches the Import bot files wizard page wherein you must select the file that was exported by another Enterprise Control Room user:



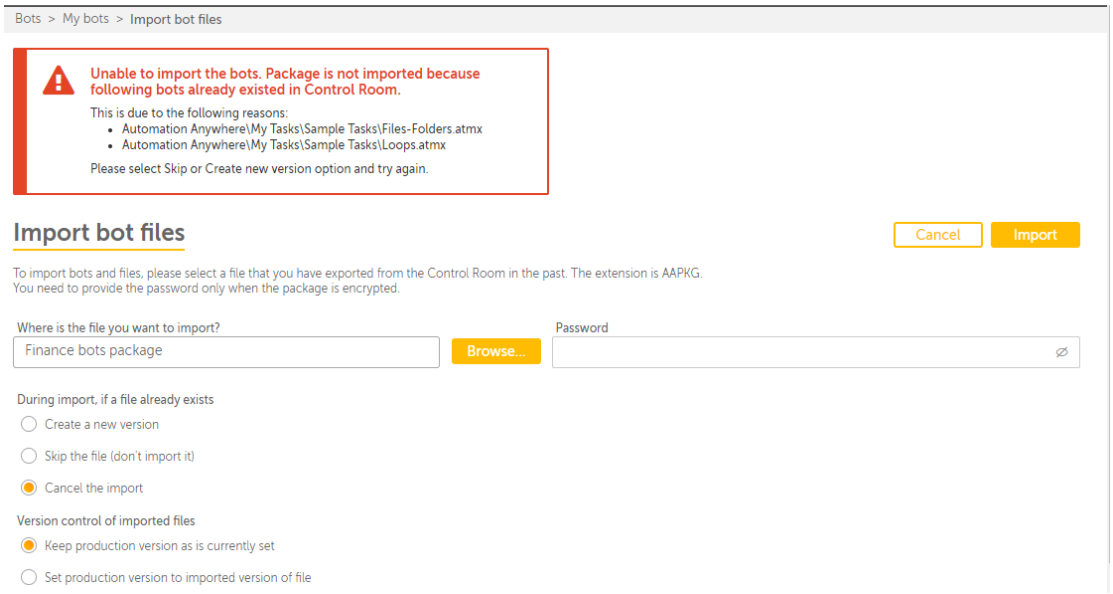
4. To select the file, click Browse.
5. Go to the source folder where the package was exported and shared by the Enterprise Control Room user with Export Bots privileges.

©2020 Automation Anywhere. All rights reserved.

6. Select the required package - it has an AAPKG extension.
7. If encrypted, provide the same password that was used for export from source Enterprise Control Room.
8. If some of the files that are being imported from the package are already available in the Enterprise Control Room, you can choose to,
   - Create a new version of files. A new version is created in the destination Enterprise Control Room irrespective of version control - whether enabled or not in the source Enterprise Control Room. Note: If the bot being imported is already present in the destination Enterprise Control Room and does not have any updates, a new version of the bot will not be created.
   - Skip the file and do not import the file. This means that there will be no change in the file of the destination Enterprise Control Room.
   - Cancel the import action.
     Note: When you use this option, the entire import operation is canceled and if at least one file already exists in Enterprise Control Room. In this case, no bots will be imported into Enterprise Control Room.
9. You must choose the production version type,
   - Keep production version as is currently set - The system will not make any change in the production versions of the imported bots and dependencies.
   - Set production version to imported version of file - The latest (imported) versions are set as production versions for all the imported bots and dependencies.

     - When you select Skip or Create options, and click Import the files are successfully imported:

     - However, when you select Cancel and click Import, you are prompted to select either of the above options:



10. After the bots are imported successfully, you return to the My Bots page.

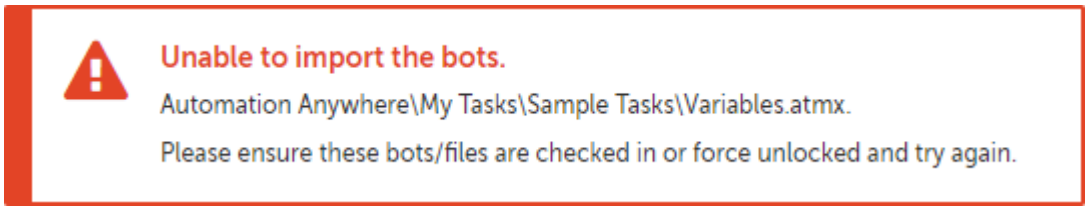
Note: If the Email settings are enabled for Export and Import operations of a BLM package, an email notification is sent to the user who performs import whether the action succeeded or failed.

©2020 Automation Anywhere. All rights reserved.

Import bots - Validations

When you import bot files, the system checks for following validations during import:

- Whether bot or dependent file already exists in Enterprise Control Room
- Whether a file is locked if version control is enabled. If this validation fails, you are shown:



You can fix this issue from the Enterprise Control Room using Unlock bot or from the Client using Checkin option.

Audit Logs

An audit entry is logged in the Enterprise Control Room Audit Log page when you import bots.

The audit details are divided in two parts - Action Details and Import Bot Details:

- The Import Bot Details include the Source Enterprise Control Room name, Package Name, Package Encryption if password has been set while exporting the bot, Imported Bot name with filepath, and Imported Dependency name with file path.

  11.3.1 If a file already exists and the user has selected the option - Create a new version, Skip or Overwrite, the status is displayed followed by the name and number of bots or files Imported, Skipped or Overwritten as per the requirement. The following illustrates the audit log details when files are skipped:

©2020 Automation Anywhere. All rights reserved.

11.3.1

IMPORT BOTS DETAILS

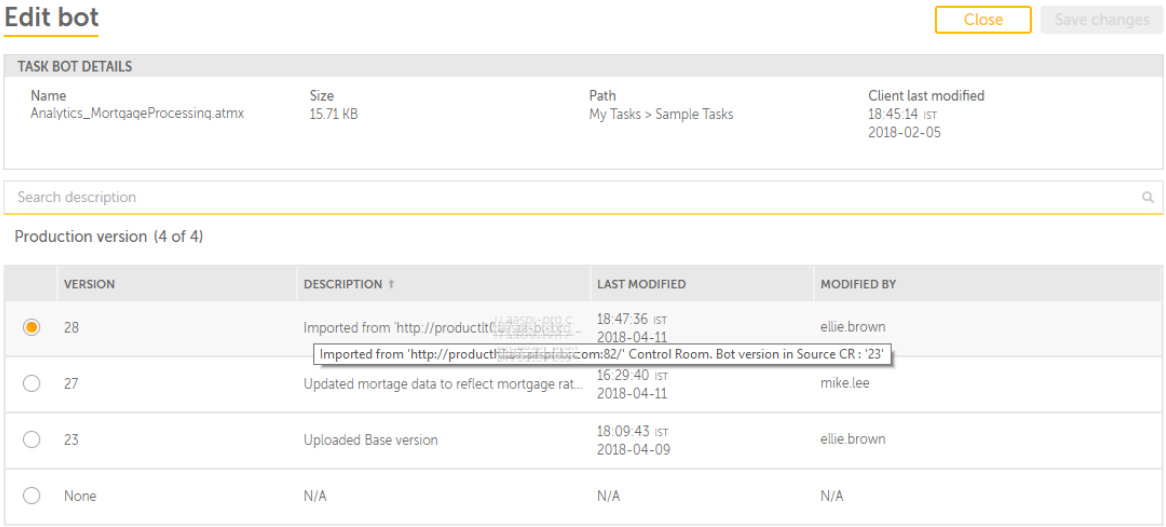
ATTRIBUTE	VALUE
Source Control Room	http://ec2-54-203-20-232.us-west-2.com...
Package Encryption	No
If a file already exists	Skip the file
Skipped File(1)	Automation Anywhere\My Scripts\Sample S...
Skipped Bot(2)	Automation Anywhere\My Tasks\Active Dire...
Imported Bot(1)	Automation Anywhere\My Tasks\Sample Ta...
Imported File(2)	Automation Anywhere\My Scripts\Sample S...
Imported Bot Dependency(1)	Automation Anywhere\My Tasks\Sample Ta...
Imported Bot Dependency(2)	Automation Anywhere\My MetaBots\Invent...

Automation Anywhere\My Scripts\Sample Scripts\CheckFolderExists.vbs

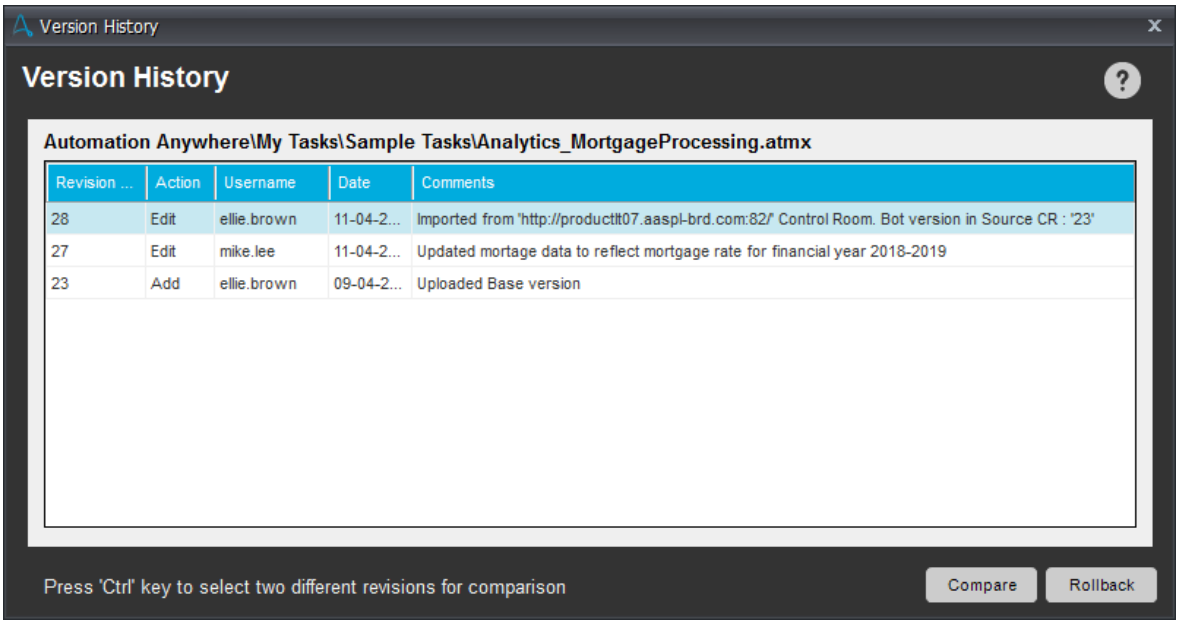
- The bots/files entries are displayed in the Attributes column in the following sequence - Skipped/ Overwritten, Imported , and Imported Dependency. The number inside the bracket indicates the bot/ file number skipped/overwritten or imported.
- The filepath of the imported entity can be viewed by hovering over the filepath in the Value column.
- When Version Control is enabled, the source Enterprise Control Room version of each item in the list are displayed and the version number is appended towards the end of the file.

    - If you want to know from which Enterprise Control Room a bot was imported with its version number, you can track it through version history in the Edit bot page

©2020 Automation Anywhere. All rights reserved.



- Alternatively, if you want to know from which Enterprise Control Room a bot was imported with its version number, you can also track it through the Version History in the Automation Anywhere Enterprise Client:



Activity overview

Use the Activity management page to view activities that are scheduled and are in progress. Also view a historical chronology of activities performed on a bot.

To view the information in the Activity section of the Enterprise Control Room, ensure you have View everyone's In progress activity, View my scheduled bots, and View my bots privileges with appropriate folder level permissions.

©2020 Automation Anywhere. All rights reserved.

See Bot Permissions for a Role.

Manage activities

Monitor in progress activity
: Monitor the ongoing automation activities, which you have triggered or scheduled from the In progress activity page of the Enterprise Control Room. Manage one or more automation activities using the pause, stop, or resume operation.

View and manage activities
: View and manage activities that are scheduled from the Scheduled Activity page. Access the Scheduled activity page by logging in to the Enterprise Control Room and clicking Activity > Scheduled.

Manage historical activity
: The Historical activity page captures and chronologically lists the automations that have occurred. Use this page to run the activity again and perform other tasks, such as export the data in the table in CSV format, customize columns, or refresh the list in the table.

Perform actions

Run a Bot
: The bots must be checked into a Control Room repository so that they are available for production deployment. Users with Run my Bots privileges might then deploy and execute the bots from the In progress, Scheduled, or My Bots page.

Run bot with queue
: Collectively process all work items of a queue across all the Bot Runners present in one or more device pools.

Schedule a bot
: To run a bot at a later point in time, on a periodic basis, or at a specific point in time, use the Schedule bot page.

Monitor in progress activity

Monitor the ongoing automation activities, which you have triggered or scheduled from the In progress activity page of the Enterprise Control Room. Manage one or more automation activities using the pause, stop, or resume operation.

Prerequisites

The following permissions are required:

- View my In progress activity to monitor and manage all ongoing automations on the bots for which you have either Upload, Download, or Delete permission.
- View everyone's In progress activity along with View my bots and Run my bots activity permissions to monitor and manage all ongoing automations on the bots with corresponding folder permissions.
- 11.3.4 View All in progress activity to see all ongoing automations, irrespective of the Bot folder permission.

©2020 Automation Anywhere. All rights reserved.

Procedure

1. View the progress of the bots being downloaded from the Bot Store.
2. View the in progress automations on Bot Runner machines that have the Run Time window hidden from view.
3. Apply search parameters to Status, Activity Type, Bot, Queue, Device, and Item Name columns for ease of access.
   Tip: When you specify search parameters for the same column, the system searches using the OR operator. When you specify search parameters for different columns, the system searches using the AND operator.
4. Perform the following actions on a column for efficiency:
   a) Click a column to sort it in ascending and descending order.
   You can sort up to three columns by holding the Shift key when you click two or more columns. This gives you the option of sorting two additional columns. This way, the sorting is done on the entire table and not just on the data that is currently visible to you. The last sorting is stored in the memory applied by a user per session.
   b) Use a drag-and-drop operation to move the column left or right.
   c) Move your mouse cursor at the end of the column and drag it to resize it.
5. Monitor the following in the Activity table:
   a) Check whether the Status of the activity is:
   Active (In progress) for a bot running on Bot Runner machines.
   Paused for a bot that is paused either from the Enterprise Control Room or a device.
   Unknown for a bot that fails to run for unknown reasons.
   Waiting for user input for a bot that is paused and requires an input from a user.
   Note: 11.3.3 Only Active status is applicable to the bots and Digital Workers downloaded from the Bot Store.
   b) View the Progress of the activity, in percentage.
   c) Check whether the Activity Type is:
   Run Bot
   Import queue files
   Run bot with queue
   11.3.3 Bot Store - Download bots
   d) View the time when the activity was Started On.
   This is in the format HH:MM:SS YYYY-MM-DD.
   e) View the name of the bot.
   f) 11.3.3 View the name of the bot package being downloaded from the Bot Store.
   g) View the Queue name.
   Note: 11.3.3 This column is not applicable for the bots and Digital Workers downloaded from the Bot Store.
   h) Check the Device on which the activity is running.
   Note: 11.3.3 This column is not applicable for the bots and Digital Workers downloaded from the Bot Store.
   i) Check the Username, which is an Enterprise Control Room user account used for running the automation on a remote Bot Runner.
   j) Check the name of the automation in Item Name.
6. Perform the following table-level actions for a set of multiple activities:
   a) Refresh the list of activities listed in the table.
   b) Pause in progress activities that are being performed on the bot.
   c) Resume in progress activities that were paused.
   d) Stop in progress activities regardless of the activity stage of a bot.

©2020 Automation Anywhere. All rights reserved.

e) Export in progress activities list to a csv file.
f) Move to History the selected activities.
g) Click the Customize columns icon to show the list of available columns. Select to add a column.

7. Perform the following tasks on an activity:
   a) Select View in progress activity to view activity details.

   Note: 11.3.3 This option is not applicable to the bots and Digital Workers downloaded from the Bot Store.
   b) Select Pause in progress activity to pause an activity.
   c) Select Resume in progress activity to resume an activity that was paused.
   This is visible only when you pause the activity.
   d) Select Stop in progress activity to stop the progress of an activity.
   e) Select Move in progress activity to move the activity to Historical Activity page.

Related tasks
View in progress activity details
Manage historical activity

View in progress activity details

You can view in real time, monitor, and manage all ongoing automations on bots in the Enterprise Control Room.

Prerequisites

The following permissions are required:

- View everyone's In progress activity
- View my In progress activity
- Run my bots with corresponding folder permissions

Procedure

1. Click Activity > In Progress
2. Select an ongoing automation.
3. Click the view icon.
   The View activity in progress page is launched, which shows the following details:

Area	Description
BOT + DEPENDENCIES	The name of the bot and dependencies for the scheduled bot.
DEVICES	The name of the device connected to the bot.
NAME + DESCRIPTION	The name and description for the activity. By default, this displays the bot name, and the date, time, and name of the user who ran the bot.
RUN DETAILS	The run details for the bot, which include: • Progress: The bot progress in percentage • Status: Active, Paused, Unknown or Waiting for user input • Started on: The date and time when the bot was executed

©2020 Automation Anywhere. All rights reserved.

Area	Description
	• Line + Command: The current line number and command name of that line Note: 11.3.3 The details of the command are not displayed for the protected bots that are downloaded from the Bot Store.
GENERAL DETAILS	The details for the bot execution, including: • Last modified: The date and time when the bot was last modified. • Modified by: The name of the user who last made changes to the bot. Note: 11.3.4 You must have the View user basic permission to view information about the user who last modified the folder. • Object type: The type of object of the bot, such as Run Bot.

4. Choose to pause, play, stop, or move the activity to the historical activity page.
   a) Click Play to run a bot that is `Paused`.
   b) Click Pause to interrupt a bot that is `Active` (In progress).
   c) Click Stop to stop the in-progress bot.
   A message is displayed asking you to confirm the action:
   - d) Click Yes, stop to return to the In progress page.
   - e) Click No, Cancel to return to the View activity in progress details page.

   f) Click Move to history to move the activity that is in `Unknown` status from the In progress activity page to the Historical activity page.

   Note: You cannot pause/resume or stop an automation that has queues from the View activity in progress page. You can do those activities from the Workload → Queues page by using the View Automation option. See Manage Work Items.

Related concepts
Audit log overview
Manage Work Items

Manage historical activity

The Historical activity page captures and chronologically lists the automations that have occurred. Use this page to run the activity again and perform other tasks, such as export the data in the table in CSV format, customize columns, or refresh the list in the table.

Prerequisites

The following permissions are required:

- View my in-progress activity permission to see all the completed automations that you deployed or scheduled.
- View everyone's in-progress activity to see all the automations run or scheduled by other users.

  Note: To view the activities in the Historical activity page, the Run/Schedule permission on the corresponding Bot is required.

©2020 Automation Anywhere. All rights reserved.

11.3.5 You can view the history of a deleted bot if you previously had the permission. However, you cannot run the deleted bot from the Historical activity landing page and the View historical activity page.

Procedure

1. View the list of all the activities, which have finished running - successfully or unsuccessfully. For example, if in some cases where an activity failed to run, use this page to verify the status of such an activity.
   Remember: The information is captured in the Historical activity page only if the bot is uploaded by the Bot Creator to the Enterprise Control Room repository.
2. Apply search parameters to the Status, Device Name, Automation Name, User, and Bot Name columns in the search bar.
   Tip: When you specify search parameters for the same column, the system searches using the OR operator. When you specify search parameters for different columns, the system searches using the AND operator.
3. Perform the following actions on a column for efficiency:
4. View the following in the Activity table:
   - Status of the activity such as Unknown, Completed, Failed, Stopped, or Time Out.
   - Name of the Bot Runner (Device name) machine on which the automation was being run.
   - Name of the automation.
   - Name of the Bot.
   - Name of the User under whose account that particular activity/automation was running on the device.
   - Date and time on which the activity was started and completed.
5. Perform the following table-level actions for a set of multiple activities. These actions can be performed only at a table-level and not on individual items.
   a) Refresh the table.
   b) Export the selected activities in CSV format.
   c) Customize selected columns.
6. Perform the following tasks on an individual item in the Historical activity page:
   - View details of the activity.
   - Run the bot.
     Tip: Move your mouse over the Actions icon and click the Run icon to run the activity again. When you click the Run icon, it opens the Run bot now page with all the values of the bot populated. You can then make changes to the bot and run the bot again.
   - Export data from the table to a CSV file.

     Export data to CSV

   Note: 11.3.3 When a bot is run locally on an Unattended or Attended Bot Runner or Bot Creator machine, the View and Run bot actions are not available for that particular activity.

Related tasks
Create a role
View details of selected activity from history
Run a Bot

Export data to CSV

You can export data to a CSV file. You can export selected records, all records, or filtered records.

©2020 Automation Anywhere. All rights reserved.

You can use any of the following options from the Export items to CSV menu to export the data:

- Export checked items: Exports the records you have selected from the table.
- 11.3.4 Export filtered items: Exports the records available after applying filters from the table.
- 11.3.4 Export ALL items: Exports all the records available in the table.
  Note: You can export a maximum of 100,000 records at a time.

Notes:

- 11.3.4 You must have the View user basic permission in order to export the basic information about other users to the CSV file.
- 11.3.5 The historical data of a deleted bot is also exported in the CSV file.

The time required to export data to a CSV file might vary based on the number of records being exported. A message appears on the screen if the time required to export the data is more than 2 seconds. The CSV file is available for download after it is generated.

The Export items to CSV option is disabled when exporting the data. However, you can perform other operations in the Enterprise Control Room. The system creates an audit entry only if the export process fails.

CAUTION: If you refresh the Enterprise Control Room while the export is in progress, the export process fails.

View details of selected activity from history

View the execution details of a selected bot in the View historical activity page. The page shows details based on activity type such as Run bot or Schedule a bot. You can also run the bot again from this page.

Prerequisites

The following permissions are required:

- View my in-progress activity
- View everyone's in-progress activity
- Run/Schedule permission on the corresponding Bot.

Note: 11.3.5 You can view the details of the run history of a deleted bot for audit and compliance purposes. However, you cannot run a deleted bot from this page.

Procedure

1. In the Historical activity page, select a bot.
2. Click the View icon for that activity.

   The View historical activity page opens, showing the following details:

©2020 Automation Anywhere. All rights reserved.

Area	Description
Bot + Dependencies	Displays the bot name and name of its dependent bots or files.
Device	Displays the device name of the source Enterprise Control Room from which the bot was deployed.

Run Details	• Progress: Displays color-coded progress in the automation:
	  • Red: When automation fails or is stopped with an error message
	  • Green: when the automation is completed
	• Percentage of automation completed, stopped, or failed.

Schedule Details	This tab is visible only if the bot is deployed using the Schedule a bot operation. • Schedule type: Displays the type of schedule used to deploy the bot. For example, Run once. • Next occurrence: Displays the next schedule run date + time. • Start/End date: Displays the schedule start and end date + time.
General details	Displays the following details: • Last Modified: Displays the date and time when changes were last made to the folder. • Modified by: Displays the name of the user who last made changes to the folder in date and time. Note: 11.3.4 You must have the View user basic permission to view information about the user who last modified the folder. • Object type: Displays the activity type - Run Bot or Schedule Bot.

Related tasks
Run a Bot

Schedule a bot

To run a bot at a later point in time, on a periodic basis, or at a specific point in time, use the Schedule bot page.

Prerequisites

Following permissions are required:

- View everyone's In progress activity
- View my scheduled bots
- View my bots

Note:

- You can access only those folders for which you have the Run and Schedule permission.

©2020 Automation Anywhere. All rights reserved.

- You cannot schedule Attended Bots from the Enterprise Control Room. Only Unattended Bots are available for the Schedule operation.

You can schedule a bot from any of the following Enterprise Control Room pages:

- Activity > In progress
- Activity > Scheduled
- Bots > My bots
- Devices > Bot runners and bot creators

To schedule a bot, do the following:

Procedure

1. Click the Schedule bot... link on the appropriate page, such as In progress, Scheduled, My bots, or Bot runners and bot creators page.
   The Schedule bot page is launched.
2. From the Select a TaskBot area, click one of the folders depending on your requirements.
   The Type and name of the available bots are shown on the right hand side in a tabular format.
3. Click a bot to select a TaskBot depending on your requirements.
   The Select button is enabled.
4. Click the Select button.
   The bot is ready to be scheduled. You can view the dependencies of the selected bot in the Review dependencies for <bot name> section.
   Note: When you click the Select button, the label of the button changes to Replace. This gives you an option of selecting another bot and replacing the selected bot.
   Although, you will be able to schedule a bot, automation fails in the following cases:
   - If any of the bot dependencies are missing
   - If you do not have the folder privileges on the dependencies
   - If you do not have the Run and Schedule permission (the one that shows a red dependency icon –)
5. Click the Next link.
   The Schedule and Devices tab is shown. You have two options of scheduling a bot – Run once and Run repeatedly.
   - Run once: Use this option to run the bot once on a given day at X hour. When you select this option, set the Start date and Start time.
   - Run repeatedly: Use this option to schedule your bot to run every X minutes per hours on a given day. When you select this option, select the Start date, End date, and Start time.
     - Enter the Start date either manually in MM/DD/YYYY format or by using the pop-up calendar. The default value of the Start date field is set to the current day of your local system.
       Enter the End date if you are using the Run repeatedly option. The default value of the End date field is blank.
       Note: If the value selected in the Start date field is the current day, the scheduled time has to be greater than the current time. Also, the value of the End date field has to be later than or equal to the value in the Start date field.
     - 11.3.3 Enter the Start time using the drop-down list to quickly set the time value. The list contains pre-defined time values in the 12-hour format at intervals of 15 minutes. You can also manually set the time value in the 12-hour format. However, this is not available for the selection in the drop-down list. The default value of the Start Time field is rounded off to the closest half-hour that is 15 minutes away. For example, if the current time is 11:22 AM, it will display 12:00 PM.

©2020 Automation Anywhere. All rights reserved.

- Time Zone: While creating and editing a schedule, you can select the Time Zone with the start time. The default value of the Time Zone is set to the current location your system.

Note: A schedule is run based on the Time Zone selected when creating or editing a schedule. For more information about selection of time in schedules by considering Day Light Saving Time (DST) switch over, see Day Light Saving and Time Zone Selection in Schedules.

6. After selecting the Run once or Run repeatedly options, click a device of your choice from the Available devices area and use the arrow button to move it to the Selected devices area.
   The list shows the devices connected and disconnected to the Enterprise Control Room.
   Note: You can select only bot runner devices that are connected. If a device is not connected, it is not enabled. Also, if the device does not appear in the list, ensure that an active bot runner session is running on the device.
7. Optional: Select the Run bot runner session on control room to view the progress of the bot run in the Activity > In Progress page.
   Note: On selecting this option, a separate Audit logs for run bot deployment and bot runner session is logged in the Enterprise Control Room.
   After the device is added to the list of selected devices, the Upcoming schedules for that device are shown. This helps to decide whether to deploy another schedule or not.
8. Click the Next link.
   The Name and Description tab appears.
9. Enter a name and description in the General area and click the Schedule bot button.
   The bot is added to the Activity table of the Scheduled activity page.
   Note: The Schedule bot button remains disabled until all the required items, such as bots, schedule details, and devices are not selected.

Day Light Saving and Time Zone Selection in Schedules

Day Light Saving Time (DST) switchover and selection of Time Zone in Schedules.

When the Day Light Saving Time (DST) switchover occurs, the clock is set forward or backward during this time interval. When DST starts, the time is set forward from 2 am to 3 am When DST ends, the clock is set back by 1 hour between 2 am and 1 am If your schedules are set to trigger during this time interval, then verify whether your schedules run as expected when the DST switchover occurs.

Note:

- All the application servers must be in the same time zone in the distributed mode for the Enterprise Control Room login to work.
- If you have existing schedules, we recommend that you edit the time in the schedule to ensure that the schedule does not fall in between DST switchover time.
- If you create schedules during the DST switchover, they are automatically created an hour later.

For other default schedule behavior, see table.

11.3.2

Schedule behavior during DST switchover

The table describes the default schedule behavior when bots are scheduled during DST switchover

Schedule type	Schedule behavior
Run once	The schedule will run only once. For example, if a schedule is set to run on the Day Light Savings day and falls in the switchover time say 2:30, it will run at 3:30 0nly.
Run repeatedly > Monthly	The schedule will be skipped. For example, if a schedule is set to run on the Day Light Saving day and falls in the switch over time, it will not run at all. In this case, it is recommended that you either pre pone or post pone the schedule time.
Run repeatedly > Weekly	The schedule will be either pushed by an hour or skipped based on the schedule day and time. For example: • If the first instance of the weekly schedule is set to run on the Day Light Saving day and falls in the switch over time, it will be pushed by an hour. Note: Here first instance refers to the first day of the Start date • However, if the subsequent instance of the weekly schedule is set to run on the Day Light Saving day and falls in the switch over time, it will be skipped.
Run repeatedly > Repeats Daily > Repeat every n hour or minute	The schedule will be either pushed by an hour or skipped based on the schedule day and time. For example: • If the first instance of the daily schedule is set to run on the Day Light Saving day and falls in the switch over time, it will be pushed by an hour. Note: Here first instance refers to the first day of the Start date • However, if the subsequent instance of the daily schedule is set to run on the Day Light Saving day and falls in the switch over time, it will be skipped.

View and manage activities

View and manage activities that are scheduled from the Scheduled Activity page. Access the Scheduled activity page by logging in to the Enterprise Control Room and clicking Activity > Scheduled.

©2020 Automation Anywhere. All rights reserved.

Prerequisites

The following permissions are required for tasks such as edit, view, activate, deactivate, or delete the schedule:

- View my scheduled bots
- View my bots

See Create a role.

Procedure

1. Schedule a bot.
2. Apply search parameters to the Activity Name column in the search bar.
   Tip: When you specify search parameters for the same column, the system searches using the OR operator. When you specify search parameters for different columns, the system searches using the AND operator.
3. Monitor the following in the Activity table:
   a) The schedule Type: For example, One time or Recurring.
   b) Next occurrence of the scheduled bot to run.
   c) Activity name: For example, list files in a folder, loops.
   d) Bot name: For example, monthly-payroll.atmx.
   e) Schedule description: For example, every Monday at 3 PM.
   f) Devices on which the bot will run at the scheduled time.
   g) Status of the scheduled activity: For example, active or inactive.
   h) The name of the user who last modified the activity in Modified by.
   Note: You must have the View user basic permission to view information about the user who last modified the activity.
   i) The date and time when the activity was Last modified.
4. Perform the following table-level actions for a set of multiple activities:
   a) Refresh the Schedules page.
   b) Activate or Deactivate the schedules.
   c) Delete the schedules.
   d) Export the selected schedules to a csv file.
   e) Select the columns to show or hide in the Activity table by using Customize columns.
5. Perform the following tasks on an individual schedule:
   a) Edit the scheduled bot.
   b) View details of the scheduled bot.
   c) Activate or Deactivate the scheduled bot.
   d) Delete the scheduled bot.

Related tasks
View scheduled bot details
Edit a schedule
Delete a schedule
Activate or deactivate a schedule

View scheduled bot details

Use the View scheduled bot page to view details of a bot after it is scheduled to run.

©2020 Automation Anywhere. All rights reserved.

Prerequisites

The following permissions are required:

- View everyone's In progress activity
- View my scheduled bots
- View my bots

The following table describes the different areas of the View scheduled bot page.

Area	Description
BOT + DEPENDENCIES	The name of the bot and dependencies for the scheduled bot.
SCHEDULE + DEVICES	The date and time at which the bot has been scheduled with the name of the device connected to the bot.
NAME + DESCRIPTION	The name and description for the bot.
RUN DETAILS	The run details for the bot. For example, when the bot last ran.
SCHEDULED DETAILS	The following details for the schedule are displayed: • Schedule type: Whether the schedule runs once or repeatedly. • Next occurrence: When the schedule runs again. • Start date: The date when the schedule runs for the first time. • End date: The date when the schedule stops running.
GENERAL DETAILS	The following details for the schedule are displayed: • Last modified: The date and time the bot was last modified. • Object type: The object type of the bot, such as scheduled bot. • Modified by: The name of the user who last made changes to the scheduled bot. Note: 11.3.4 You must have the View user basic permission to view information about the user who last modified the folder.

Procedure

1. Click Edit to update the bot schedule.
2. Click Activate or Deactivate to activate or deactivate the schedule.

Edit a schedule

You can edit a bot schedule from the Scheduled activity page to ensure that the automation is not skipped because of a change in the schedule type, date, or time, when Bot Runners are added or removed, or when the settings are updated.

©2020 Automation Anywhere. All rights reserved.

Prerequisites

You require the following permissions:

- Delete my scheduled activity
- View and manage all scheduled activity from my folders
- View and manage all scheduled activity

Procedure

1. Select a schedule in the Activity tab.
2. Click the Edit icon.
3. In the Edit scheduled bot page, make changes to the bot depending on your requirements.
   Important: Select the bots and devices because these are required to Save your changes.
4. Click Schedule bot.

Delete a schedule

Delete schedules of a bot from the Scheduled Activity page.

Prerequisites

The following permissions are required:

- Delete my scheduled activity
- View and manage all scheduled activity from my Folders
- View and manage all scheduled activity

Procedure

1. Select a schedule in the Activity table.
2. Click the Delete icon.
3. Confirm the delete action by clicking Yes, delete.

Activate or deactivate a schedule

Use the Scheduled Activity page to activate or deactivate schedules individually or in bulk.

Prerequisites

The following permissions are required:

- View and manage all scheduled activity.
- View and manage all scheduled activity from my Folders.

For example, you can choose to activate schedules that are inactive to run the automation in bulk. Or you can deactivate multiple schedules during downtime.

©2020 Automation Anywhere. All rights reserved.

Procedure

1. Go to Activity > Scheduled
2. In the Scheduled activity page, select a schedule that is in active status.
   You can also activate multiple schedules by clicking the Activate option above the Activity table.
   Note: The Deactivate or Activate option appears based on the greater number of active or deactivated schedule status.
   - When the number of schedules with Active status is more than the Inactive ones, the Deactivate option is shown.
   - When the number of schedules with Inactive status is more than the Active ones, the Activate option is shown.
3. Click Deactivate.
   By default, all schedules on this page are in active state. Therefore, the default action is Deactivate. This changes to Activate for a schedule that is deactivated.
   The schedule is deactivated. The status in the Next Occurrence column is displayed as NA and the Status changes to Inactive.

Devices overview

A device is an Automation Anywhere Enterprise client machine that connects you to the Enterprise Control Room to create or run bots.

Users connected to the Enterprise Control Room as a Bot Creator or a Bot Runner can be managed from the Enterprise Control Room.

What are My Devices and why use them?

My Devices is a list of devices registered and connected to your current Enterprise Control Room instance.

Use My devices with the manage devices privileges to view and manage the registered devices and identify the devices' status (connected or disconnected) from the Enterprise Control Room instance. See Manage devices.

What are Device Pools and why use them?

Device pools are a logical grouping of similar Bot Runners on which you can run bots with the work item from a queue. For example, you can group devices of a specific department or unit and create a device pool for it.

Use My Device Pool to create and view a list of device pools that are available from the current Enterprise Control Roominstance. A Device Pool admin can view all the devices that can be used for work items in workload management. You can also create device pools comprising Bot Runners. See Manage device pools.

- Manage devices
  As an Enterprise Control Room admin or a user with manage devices privileges, you can view the devices that are registered to your Enterprise Control Room instance.
- Manage device pools
  A device pool is a logical grouping of similar type of devices on which bots are run as work items from

©2020 Automation Anywhere. All rights reserved.

their respective queues. For example, you can group devices of a particular department/unit and create a device pool for it.

Manage devices

As an Enterprise Control Room admin or a user with manage devices privileges, you can view the devices that are registered to your Enterprise Control Room instance.

Device privileges include viewing and managing Bot Runners, Bot Creators, and creating and managing device pools.

Only an admin user has access to see all the devices (Bot Runners and Bot Creators) in the Enterprise Control Room. A non-admin user will not have access to view the Bot Creators.

View device details

You can view the following details of the device:

- Status – View the combined status of the user and the device used by that user. The Connected and Disconnected statuses indicate whether the bot is logged in or logged out of the Enterprise Control Room respectively. An Offline status indicates that the device user is unregistered or disabled by the Enterprise Control Room admin.
- Device name – View the device's fully qualified server name.
- Username – View the name of the user connected with the device.
- Device pool – View the name of the device pool that includes the device. N/A indicates that the device cannot be a part of any device pool and - - indicates that the device is not a part of any device pool.

  Manage device pools

- Type – View the type of license assigned by the Enterprise Control Room admin.
- 11.3.5 Work item ID – View the ID of the Work Item that is currently processed by the device. This column is hidden by default.
- 11.3.5 Queue name – View the name of the queue that is currently processed by the device. This column is hidden by default.

Manage devices with a task

You can perform a task on an individual device or on multiple devices by selecting the required devices from the table. Perform the following tasks to manage the devices:

- Run bot - Run one or more bots for the production deployment with the Run my Bots privileges.

  Run a Bot

- Schedule bot - Schedule one or more bots to run on a periodic basis or at a specific point of time.

  Schedule a bot

You can also perform the following actions on the selected devices:

©2020 Automation Anywhere. All rights reserved.

- Export data to a CSV file based on month, filters, or selection to save the data for future analysis.
- Refresh table to view the latest device status.
- Customize columns to show or hide specific columns. By default, all the columns are shown.

Work efficiently with device entries

You can perform the following actions on a column in the My Devices table to help you work efficiently:

- Click a column to sort it in an ascending or descending order. You can sort up to three columns using the Shift key, enabling you to sort two additional columns. The entire table is sorted rather than just the data that is currently visible to you. The last sorting done by the user is saved for that session.
- Drag and drop to move the column to the left or right.
- Move your mouse pointer at the end of the column and drag it to resize the column.

- Run a Bot
  The bots must be checked into a Control Room repository so that they are available for production deployment. Users with Run my Bots privileges might then deploy and execute the bots from the In progress, Scheduled, or My Bots page.
- Schedule a bot
  To run a bot at a later point in time, on a periodic basis, or at a specific point in time, use the Schedule bot page.

Related concepts
Roles overview
Related tasks
Schedule a bot
Run a Bot

Run a Bot

The bots must be checked into a Control Room repository so that they are available for production deployment. Users with Run my Bots privileges might then deploy and execute the bots from the In progress, Scheduled, or My Bots page.

Prerequisites

- Ensure you have Run my bots privilege.
- Ensure a client with Bot Runner license is connected to the Enterprise Control Room.

Procedure

1. Login to Enterprise Control Room.
2. Click Bots > My bots.
   My bots page that has only the bots created by users with Unattended Bot Runner license is displayed.
   Note: You cannot run bots created by users with attended Bot Runners license.
3. Click Run bot > Run bot now.
   Run bot now page is displayed.
4. Under Select a TaskBot tab, select a folder that contains bots.

   The TYPE and NAME of the bot are displayed.

©2020 Automation Anywhere. All rights reserved.

Note: You can only access the folders for which you have Run Schedule privileges.

5. Select a TaskBot.
6. Click the → icon.

   The bot is added to the Review dependencies for Files-Folders section.

   Note: When you run a bot, automation can fail if:
   - Any of the bot dependencies are missing.
   - You do not have folder privileges for the dependencies.
   - You do not have Run Schedule privileges (icon appears).
7. Click Next.

   Available devices and bot runners in the Enterprise Control Room are displayed.

8. (Optional) Select Run Bot Runner Session on Control Room.

   This allows the Enterprise Control Room to take Remote Desktop Protocol (RDP) of the Bot Runner machine to run a scheduled task, if it is in locked or logged off state. This method is recommended when Bots are deployed on virtual machines and terminal servers. See Guidelines for RDP-based bot deployment.

9. Select any bot under the Available bot runners section, and click the → icon.
   Note: You can only select a connected Bot Runner devices, as disconnected devices are not enabled. Also, if a device is not displayed, ensure the device has an active Bot Runner session.
10. Click Next.
11. (Optional) Under the General tab, update the Name and Description.
    The [bot name].[DD.MM.YY][HH.MM.SS].[USERNAME] format is available by default, which you can change as per your preference.
12. Click Run Now.
    The selected bot is initiated and you can view the progress under the In Progress activity page.
    Note: Run now is disabled if the device is disconnected or the required fields are not filled.

- Guidelines for RDP-based bot deployment
  When you deploy a bot from the Enterprise Control Room to any Bot Runner, it attempts an auto-login (if the Bot Runner is locked or logged off). However, auto-login is prone to security policies set on the machine. Therefore, certain policies might have to be relaxed for the auto-login function.

Related reference
Guidelines for RDP-based bot deployment

Schedule a bot

To run a bot at a later point in time, on a periodic basis, or at a specific point in time, use the Schedule bot page.

Prerequisites

Following permissions are required:

- View everyone's In progress activity
- View my scheduled bots

©2020 Automation Anywhere. All rights reserved.

- View my bots

Note:

- You can access only those folders for which you have the Run and Schedule permission.
- You cannot schedule Attended Bots from the Enterprise Control Room. Only Unattended Bots are available for the Schedule operation.

You can schedule a bot from any of the following Enterprise Control Room pages:

- Activity > In progress
- Activity > Scheduled
- Bots > My bots
- Devices > Bot runners and bot creators

To schedule a bot, do the following:

Procedure

1. Click the Schedule bot... link on the appropriate page, such as In progress, Scheduled, My bots, or Bot runners and bot creators page.
   The Schedule bot page is launched.
2. From the Select a TaskBot area, click one of the folders depending on your requirements.
   The Type and name of the available bots are shown on the right hand side in a tabular format.
3. Click a bot to select a TaskBot depending on your requirements.
   The Select button is enabled.
4. Click the Select button.
   The bot is ready to be scheduled. You can view the dependencies of the selected bot in the Review dependencies for <bot name> section.
   Note: When you click the Select button, the label of the button changes to Replace. This gives you an option of selecting another bot and replacing the selected bot.
   Although, you will be able to schedule a bot, automation fails in the following cases:
   - If any of the bot dependencies are missing
   - If you do not have the folder privileges on the dependencies
   - If you do not have the Run and Schedule permission (the one that shows a red dependency icon –)
5. Click the Next link.
   The Schedule and Devices tab is shown. You have two options of scheduling a bot – Run once and Run repeatedly.
   - Run once: Use this option to run the bot once on a given day at X hour. When you select this option, set the Start date and Start time.
   - Run repeatedly: Use this option to schedule your bot to run every X minutes per hours on a given day. When you select this option, select the Start date, End date, and Start time.
     - Enter the Start date either manually in MM/DD/YYYY format or by using the pop-up calendar. The default value of the Start date field is set to the current day of your local system.
       Enter the End date if you are using the Run repeatedly option. The default value of the End date field is blank.
       Note: If the value selected in the Start date field is the current day, the scheduled time has to be greater than the current time. Also, the value of the End date field has to be later than or equal to the value in the Start date field.

©2020 Automation Anywhere. All rights reserved.

- 11.3.3 Enter the Start time using the drop-down list to quickly set the time value. The list contains pre-defined time values in the 12-hour format at intervals of 15 minutes. You can also manually set the time value in the 12-hour format. However, this is not available for the selection in the drop-down list. The default value of the Start Time field is rounded off to the closest half-hour that is 15 minutes away. For example, if the current time is 11:22 AM, it will display 12:00 PM.
- Time Zone: While creating and editing a schedule, you can select the Time Zone with the start time. The default value of the Time Zone is set to the current location your system.

Note: A schedule is run based on the Time Zone selected when creating or editing a schedule. For more information about selection of time in schedules by considering Day Light Saving Time (DST) switch over, see Day Light Saving and Time Zone Selection in Schedules.

6. After selecting the Run once or Run repeatedly options, click a device of your choice from the Available devices area and use the arrow button to move it to the Selected devices area.
   The list shows the devices connected and disconnected to the Enterprise Control Room.
   Note: You can select only bot runner devices that are connected. If a device is not connected, it is not enabled. Also, if the device does not appear in the list, ensure that an active bot runner session is running on the device.
7. Optional: Select the Run bot runner session on control room to view the progress of the bot run in the Activity > In Progress page.
   Note: On selecting this option, a separate Audit logs for run bot deployment and bot runner session is logged in the Enterprise Control Room.
   After the device is added to the list of selected devices, the Upcoming schedules for that device are shown. This helps to decide whether to deploy another schedule or not.
8. Click the Next link.
   The Name and Description tab appears.
9. Enter a name and description in the General area and click the Schedule bot button.
   The bot is added to the Activity table of the Scheduled activity page.
   Note: The Schedule bot button remains disabled until all the required items, such as bots, schedule details, and devices are not selected.

Manage device pools

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

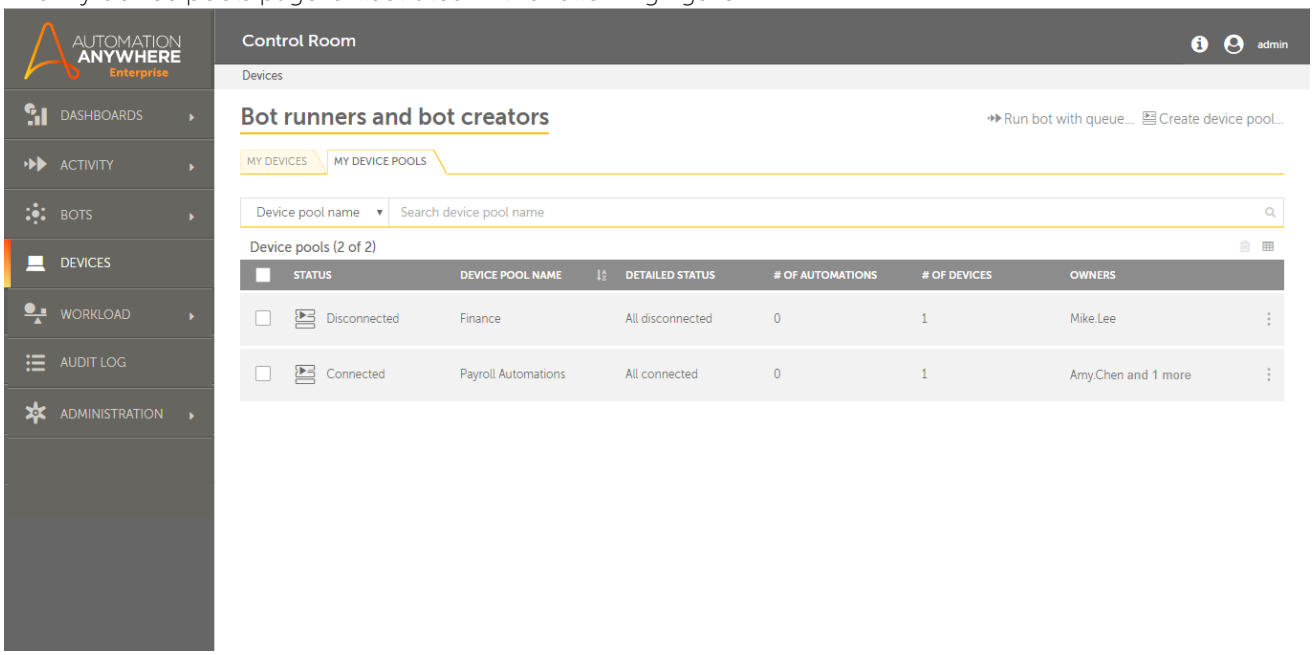
Introduction

You can manage all device pools that can be used for work items in Workload Management if you are a device Pool Admin. You can view only those device pools for which you have device Pool Owner, Pool Consumer or both privileges.

The device pool owner privilege allows you to create device pools comprising Bot Runners.

©2020 Automation Anywhere. All rights reserved.

The My device pools page is illustrated in the following figure:



Note: You need to create device pools to view those in the list. To get started, click the create a device pool here link.

For ease of access, you can search by device pool name.

The following describes the list of items that can be viewed in the table:

Table Item	Description
Status	Shows device's status. Here, status refers to the status of both User and Device from which the user is connects. • Connected when the user and device are connected to the Control Room from selected Bot Runner • Disconnected when the user and device are not connected to the Enterprise Control Room from selected Bot Runner • Offline when the user is deactivated by the Enterprise Control Room admin
Device Pool Name	Shows name of the device pool
Detailed Status	Shows status of the devices that are part of that particular device pool • All Connected when all users and devices are connected to the Enterprise Control Room • All Disconnected when one or more user and device are disconnected from the Enterprise Control Room

©2020 Automation Anywhere. All rights reserved.

Table Item	Description
# of Automations	Shows the number of automation that are currently deployed on that particular device pool
# of Devices	Shows the number of devices that are included in the device pool
Owners	Shows the owner name(s) of the device pool

You can do the following actions on a table column:

- Click a column to sort it in ascending and descending order. You can sort up to three columns by holding the Shift key when you click two more columns. This gives you the option of sorting two additional columns. This way the sorting is done on the entire table and not just the data that is currently visible to you. The last sorting is stored in memory applied by a user per session.
- Use a drag-and-drop operation to move the column left or right
- Move your mouse cursor at the end of the column and drag to re-size

The following describes the tasks that you can do on an individual device pool:

Table Item	Description
Run	Allows you to run a Bot on the device pool immediately
View	Allows you to Create device pools
Edit	Allows you to Edit device pool
Delete	Allows you to Deleting device pools

Alternatively, you can select all device pools and do the following actions. Note that these actions can be doed only at a table level and not on individual items.

Table Item	Description
Delete	Allows you to delete one or more device pools
Customize column	Allows you to show or hide columns other than Device Pool Name

When you want to do actions such as Run bot with queue or Create a device pool quickly without switching your current location, you can use the following options:

Table Item	Description
Run bot with queue	Allows you to run bot with a queue for workload management
Create device pool	Allows you to Create device pools for workload management

Audit Log

All the Create, Update, Delete actions are tracked in audit log for record keeping and future use. You can refer those entries in the Audit Log page.

©2020 Automation Anywhere. All rights reserved.

To view details of the audit entry, click View which is visible when you mouse over ⋮.

- Create device pools
  Create a device pool with a unique name and add Unattended Bot Runners to the device pool. To create device pools, an Enterprise Control Room administrator grants the Create device pools feature permission and assigns the AAE_Pool Admin role.
- View device pool
  As a Enterprise Control Room user with device pool management privileges or as a device pool owner, you can view device pool details to ensure the information provided is correct and if required customize as per your workload requirement.
- Edit device pool
  As a Enterprise Control Room user with device pool management privileges or as a device pool owner, you can edit device pool details to customize as per your workload requirement.
- Deleting device pools
  You can delete a device pool comprising of unattended Bot Runners after your entity's SLAs are achieved and the device pools are no longer required.

Related tasks
Edit device pool
Deleting device pools
Related reference
View device pool

Create device pools

Create a device pool with a unique name and add Unattended Bot Runners to the device pool. To create device pools, an Enterprise Control Room administrator grants the Create device pools feature permission and assigns the AAE_Pool Admin role.

Prerequisites

- You can add only those Unattended Bot Runners that are not part of any other pool and are not associated with any role.
- If the device associated with the Unattended Bot Runner is added to the device pool, you can only use the Run bot with queue option to run bots on that device. You cannot create a device pool comprising of Attended Bot Runners.
- You can add Enterprise Control Room user roles as consumers. Only users with these roles can use the pool for any automation.

Procedure

To create a device pool, do the following:

1. Click Devices.
2. Click Create device pool on the top right of the Devices page.
   Tip: If no device pools are available, click the create a device pool link in the My Device Pool page.
   The Create device pool page appears.
3. Enter a valid device pool name.
   For example, you can create a Finance Automation pool that can run all finance-related automations on Unattended Bot Runners from the finance department.
4. Select Unattended Bot Runners from the list.

©2020 Automation Anywhere. All rights reserved.

This list shows only the devices with Unattended Bot Runner licenses.
Restriction: Unattended Bot Runners that are a part of other device pools are disabled for selection.

5. Add the Unattended Bot Runner(s) to the Selected devices list.
   Tip: Click the left arrow button to remove the Bot Runner from the Selected devices list.
6. Subsequently, grant permissions to view, edit, and delete the device pool to the other Enterprise Control Room users:
   a) Click Next to select the Device Pool Owners.
   b) Select user(s) from the Available users list.
   Tip: Search the list of users based on their Username, First name, or Last name.
   Note: 11.3.4 You must have the View user basic permission to view information about other users in order to add them as Device Pool Owners.
   c) Click the right arrow button
   The user appears in the Selected users list.
   Note: The device pool creator is listed as the default owner of the pool.
   d) Click the left arrow button to remove the user from the Selected users list.
   Restriction: You cannot remove the device pool creator.
7. Click Next to select the Device Pool Consumers.
   Do this step so that the device pool consumers can view the device pool when they run the automation.
   a) Select a Role from the Available roles list.
   Tip: Search for a role name.
   b) Click the right arrow button.
   The user appears in the Selected roles list.
   Tip: Click the left arrow button to remove the user from the Selected roles list.
8. Click Create Device Pool.
   The device pools for which you have consumer privileges are listed in the My Device Pools page.

Next steps

Create queues
Related concepts
Run bot with queue

View device pool

As a Enterprise Control Room user with device pool management privileges or as a device pool owner, you can view device pool details to ensure the information provided is correct and if required customize as per your workload requirement.

1. Go to Devices > My Device Pools.
2. For the device pool that you need to view, mouse over ⋮.
3. Click View device pool.

   The Device Pool Details page is launched in view mode. The page provides details of the device pool in two sections:

   - Device Pool Details such as the Name, Description, Status, and Detailed Status.
   - Device Pool contents in tabs such as Automations, Unattended Bot Runners, Device Pool Owners, and Device Pool Consumers.

©2020 Automation Anywhere. All rights reserved.

Note: 11.3.4 You must have the View user basic permission to view information about other users added as Device Pool Owners.

Select each tab to view its details.

The following provides details for each of the following tabs:

- Automations- Shows the automations that are using the device pool and the order that is chosen to run those. This is shown as the default view. To find an automation quickly, use the search option using Status, Automation name, Queue, or Activity type.
  You can perform the following actions on a table column:
  1. Click a column to sort it in ascending and descending order. You can sort up to three columns by holding the Shift key when you click two more columns. This gives you the option of sorting two additional columns. This way the sorting is done on the entire table and not just the data that is currently visible to you. The last sorting is stored in memory applied by a user per session.
  2. Use a drag-and-drop operation to move the column left or right.
  3. Move your mouse cursor at the end of the column and drag to re-size
- Bot Runners- Shows list of Unattended Bots that are part of the device pool.
- Device Pool Owners- Shows list of Device Pool Owners that are granted permission to view, edit, and delete the device pool. See Create device pools.
- Device Pool Consumers- Shows the list of Device Pool Consumers who are granted permission to view the device pool as an option while running automations. See Create device pools.
- General Details- Shows the last modified date and time, name of the user who modified device pool details, and the Object Type which is the component on which modification was done.

When you view a device pool, apart from updating the Bot Runner, Device Pool Owner, and Consumer details, you can additionally choose to:

- Run Bot with queue
- Edit device pool
- Create device pools

Edit device pool

As a Enterprise Control Room user with device pool management privileges or as a device pool owner, you can edit device pool details to customize as per your workload requirement.

When you open the device pool in edit mode, you have to first define the priority or the order in which the automations will run in the Automations tab. This is visible only when you edit a device pool and is not available when you create a device pool. Apart from this you can update the Bot Runner, Device Pool Owner, and Consumer details.

To edit a device pool,

Procedure

1. Go to Devices > My Device Pools.
   Tip: You can also edit device pool details when in view mode. See View device pool to learn more.
2. For the device pool that needs to be updated, mouse over the actions icon.
3. Click the edit icon.
   The Device Pool Details page is launched in edit mode.
4. Select the order in which your automations will run.

©2020 Automation Anywhere. All rights reserved.

Select either Round robin or Priority as shown in table.

- Round robin- Use this when you want to run your automations at equal time intervals termed as Time slice. A Time slice unit can be defined in seconds, minutes, and hours. You can calculate or estimate the time for each automation and then provide this number.

  This means that the automations are executed for only 5 minutes first, then system checks for other automations in queue for execution, If yes, that automation is paused and next automation is executed. This will continue till all automations in the queue are executed.
  Note:
  - The default Time Slice is set to 5 minutes.
  - The Time slice should be more than zero.

- Priority as shown in table- Use this when you want to run your automations on priority defined in the Priority table. This method allows you to run automations in order of priority. Automations are processed till all are consumed from the specified automation queue.

  The following details are shown in the priority table:

Table Item	Description
Priority	Shows the priority number allotted to that queue. • The Priority column is editable. You can set/re-set automation implementation priority. Ensure that you provide unique priority value to two different work items as same values will not be allowed. • You can also view the Priority list in ascending or descending order by clicking the ordering arrows in the Priority header.
Status	Shows the automation status - Active or Inactive
Automation Name	Shows the automation that is selected to run on the device pool
Started On	Shows the run date and time of the automation
bot	Shows the bot name that will run using this device pool
Queue	Shows the Queue name that will be used to run automation using this device pool
Activity Type	Shows the Activity type used to run the automation using this device pool - Run bot with queue.

  You can perform the following actions on a table column:
  - Click a column to sort it in ascending and descending order. You can sort up to three columns by holding the Shift key when you click two more columns. This gives you the option of sorting two additional columns. This way the sorting is done on the entire table and not just the data that is currently visible to you. The last sorting is stored in memory applied by a user per session.
  - Use a drag-and-drop operation to move the column left or right.
  - Move your mouse cursor at the end of the column and drag to resize.
  - Search on Status, Automation Name, Queue, and Activity Type headers in the table if the data available is large.

5. Update the list of Bot Runners that will be included in the device pool. See Create device pools for details.

©2020 Automation Anywhere. All rights reserved.

6. Update the list of Device Pool Owners who are granted permission to view, edit, and delete the device pool. See Create device pools for details.

   Note: 11.3.4 You must have View user basic permission to view information about other users in order to add them as Device Pool Owners.
7. Update the list of Device Pool Consumers who are granted permission to view the device pool as an option when running TaskBot. See Create device pools for details.
8. Click Save changes.

Deleting device pools

You can delete a device pool comprising of unattended Bot Runners after your entity's SLAs are achieved and the device pools are no longer required.

You can choose to delete your device pools in either of two ways:

- Delete one device pool
  1. To delete one device pool, mouse over the actions icon-
  2. Click .

     If the device pool is being used for workload automation, you will not be allowed to delete it.

  3. Confirm or cancel as required.
- Delete multiple or all device pools
  1. Select the device pools to delete.
  2. Optional: Select all device pools by selecting the Select All check box in the header.
  3. Click given at the top of the device pools table.
  4. Confirm or cancel as required.

Based on your selection, the devices are deleted.

Workload overview

Use the Workload Management page to divide your automations into small, yet logical work items. Process them simultaneously to ensure that time-based Service Level Agreements (SLAs) are met with optimum resource utilization. Additionally, integrate with a chat application to share the outcome of workload automation with your organization's customers.

Prerequisite

Before you begin, ensure you have the AAE_Admin, AAE_Queue_Admin, and AAE_Pool_Admin privileges to create and manage workload queues, manage workload SLAs, work with workload APIs, and retrieve workload outcome details using your organization's chat application.

For workload automation, do the following:

©2020 Automation Anywhere. All rights reserved.

Step 1: Create and manage workload queues
A queue is one of the main building blocks of Workload Management (WLM). A queue holds data known as work items for further processing. The system distributes these work items to individual Unattended Bot Runners in a device pool for processing.

Step 2: Manage workload SLAs
Estimate the device pool size or time required to process a given queue size from the Workload Service Level Agreement (SLA) page.

Step 3: Add work items using APIs (optional)
Use the Workload Management (WLM) API to add or insert data for work items in an existing queue in your Enterprise Control Room.

Step 4: List all work items in a queue (optional)
Automation Anywhere provides a REST API that enables you to retrieve a list of work items in a given queue.

Related tasks
Create a work item in a queue
List all work items in a queue
Related reference
Workload command
Sample Workload Management properties file
Workload Management guidelines

Workload Management guidelines

To make optimal use of the Enterprise Control Room Workload module, you can choose to follow guidelines provided by Automation Anywhere.

Do

1. Ensure that the queue has at least 2 owners so that there is no dead-lock if an owner is deleted or disabled.
2. If Work Item are added frequently to a queue, set the reactivation threshold to 1 so that as soon as a Work Item is added, the same will be picked up.
3. There could be upto 10 Work Item columns displayed in Control Room. Make generous use of that so that you have maximum visibility of your Work Item data.
4. You can also make generous use of the Work Item values which can accept upto 1000 characters, especially for Work Item result value.
5. To prioritize certain Work Items, ensure that you sort the Work Item data when you create queues.
6. For adding work items to queue, use CSV as XLS format is not currently fully supported - for example the date-time format.
7. To insert Work Items in a loop, use the v2/wlm/workitems API as this API accepts list of work items in JSON format
8. Ensure that the time/clocks of all the machines in a Cluster are synchronized. This is important for proper functioning of the Apache Ignite cache server.
9. Persistent and continual database connectivity is critical to the functioning of Workload Management. Hence ensure that you have a periodic network scan or use tools that can detect/avoid network blips.
10. Apply the pagination filter to retrieve more than 200 Work Items when you retrieve it using the Work Item API.

©2020 Automation Anywhere. All rights reserved.

```
"page":
{
"offset":0,
"length":1000
}
```

Do not

1. To ensure the system does not clog, do not use the v2/WLM/Work Item API in a loop to insert Work Items in bulk.
2. If the Bot Runner is part of a device pool, do not create local schedules on that Bot Runner so that the Bot Runner runs only the WLM Work Items.
3. If a user has a queue in use, then do not remove the the Run bot permission from that user (role).
4. If a Work Item is in progress, do not shut down a Bot Runner. To take a Bot Runner down for maintenance, ensure that you pause the queue and no Work Item is in progress on the Bot Runner.
5. If a Work Item queue is being processed, do not Stop or Restart the Automation Anywhere Control Room Services. Instead, Pause the queue automation, and then Restart the services.

Manage workload queues

A queue is one of the main building blocks of Workload Management (WLM). A queue holds data known as work items for further processing. The system distributes these work items to individual Unattended Bot Runners in a device pool for processing.

Create device pools, add Bot Runners to the pool, create queues, add queue owners/participants/consumers, define the work item structure, insert work items, and finally run the automation with the queue.

Create and manage queues

To create and manage queues, do the following:

Step 1: Create device pools and add bot runners to the pool
: Create a device pool with a unique name and add Unattended Bot Runners to the device pool. To create device pools, an Enterprise Control Room administrator grants the Create device pools feature permission and assigns the AAE_Pool Admin role.

Step 2: Create queues
: Create queues that hold specific sets of data your bot is expecting for automation. To create queues, an Enterprise Control Room administrator grants the Create queues feature permission and assigns the AAE_Queue Admin role.

Step 3: Add names of queue owners
: Add queue owners who can create, edit, and view queues. The queue creator is the default queue owner and is able to add other users as queue owners, if required.

Step 4: Add names of queue participants (optional)
: Add queue participants from different roles defined in the Enterprise Control Room. This is an optional step.

©2020 Automation Anywhere. All rights reserved.

Step 5: Add names of queue consumers (optional)
Add queue consumers from different roles defined in the Enterprise Control Room. This is an optional step.

Step 6: Define the work item structure
Define the work item structure for processing in a queue. This enables you to manually upload the work items from the system in the absence of ready data in a file.

Step 7: Insert work items using multiple methods
Add work items from an Excel or CSV file to the queue.

Step 8: Run automation using Run bot with queue option
Collectively process all work items of a queue across all the Bot Runners present in one or more device pools.

Create queues

Create queues that hold specific sets of data your bot is expecting for automation. To create queues, an Enterprise Control Room administrator grants the Create queues feature permission and assigns the AAE_Queue Admin role.

Prerequisites

Create a queue by providing details such as the queue name, queue owners, participants, consumers, and by defining the work item structure.
Tip: A summary of these details is available in the tab on the left side. Open any tab to edit the details.

Procedure

1. Go to Workload > Queues.
2. Click Create queue.
   The Create queue page appears.
3. Configure the following General Settings:
   a) Queue Name: Enter a name for the queue that reflects its purpose.
   For example, Payroll Queue for work items that are designed to manage a payroll system.
   b) Optional: Description: Enter a description that reflects what the queue will achieve.
   For example, the Payroll Queue will process automations that are designed to manage the payroll system.
   c) Reactivation Threshold: Select the minimum number of new work items with a Ready to Run status required in the queue to resume the queue processing after all the work items in the queue are processed.
   By default, this is 1 (one).
   d) Optional: Time required for a person to complete one work item: Select the average time that a person would need to complete one work item in seconds, minutes, hours, or days.
4. Click Next to Add queue owners
   Note: You can choose to Create draft of queue and add the remaining information later.

Related tasks
Edit queues
Delete queues

©2020 Automation Anywhere. All rights reserved.

Add queue owners

Add queue owners who can create, edit, and view queues. The queue creator is the default queue owner and is able to add other users as queue owners, if required.

Prerequisites

Queue owners are allowed to edit the queue and add new work items to the queue.

Procedure

1. Select user(s) from the Available Users list in the Owners tab.
   Note: 11.3.4 You must have the View user basic permission to view information about other users in order to add them as queue owners.
2. Click the left arrow key.
   The users are added as Queue Owners in the Selected Users list.
3. Click Next to Add queue participants.

Add participants to queue

Add queue participants from different roles defined in the Enterprise Control Room. This is an optional step.

Prerequisites

Participant roles can add new work items and view the queue. However, they are not allowed to edit other queue properties.

Procedure

1. Select role(s) from the Available Roles list in the Participants tab.
2. Click the right arrow button.
   The roles are added as Participants in the Selected Roles list.
3. Click Next to Add consumers of queues.

Add consumers of queues

Add queue consumers from different roles defined in the Enterprise Control Room. This is an optional step.

Prerequisites

Queue consumers can view the queue and all the work items in the queue. In addition, they can use this queue for running bots on Unattended Bot Runners.

Procedure

1. Select role(s) from the Available Roles list in the Consumers tab.
2. Click the right arrow button.

©2020 Automation Anywhere. All rights reserved.

The roles are added as Consumers in the Selected Roleslist.

3. Click Next to Define work item structure.

Define work item structure

Define the work item structure for processing in a queue. This enables you to manually upload the work items from the system in the absence of ready data in a file.

Prerequisites

To consume the work items in the structure, first orchestrate the queue using the Insert Work Item command from the Enterprise client and use the system variable $Workitem (attribute name). See Workload command.

Define a work item structure using any one of the following methods:

- Using an Excel/CSV file.
- Using an existing queue category.
- Manually
  Remember: The work flow to process work items differs for a queue based on the method that you choose in the Define Work Item Structure.

Procedure

1. Select a method to add header columns for work item processing:
   - Excel/CSV file: Add the header columns from an existing Excel or CSV file.

     a) Enter a unique name for the work item structure in the Queue Category field.

     For example, if the queue contains employee information, you can specify the Queue Category as Employee Data.

     b) Select a column for inclusion in the work item structure from the list of column names. The columns are defined based on the header rows of the selected Excel or CSV file. A maximum of five (5) columns are allowed for selection and viewing in the Enterprise Control Room.

     11.3.3 However, if you upgrade to Version 11.3.3, you are allowed to select/view maximum ten (10) columns.

     For example, you can select column headers Employee Name, Employee ID, and Designation. You can then select the Data Type - Text, Number, or Date for that column. You can also choose to view these columns being processed in the Activity page.

     Note:
     - c) The system allows you to filter/sort work items on the columns for viewing the work item data in the Enterprise Control Room.

       Actions (sort, filter, search) for queues

©2020 Automation Anywhere. All rights reserved.

- d) When you upload work items from an xls or xlsx file with data type as text, the Excel file column populated with a date in any format (for example, 8/6/2019) is converted to its corresponding WLM date format (for example, Sat Jun 08 00:00:00) in the Enterprise Control Room Work Item. However, the same is not applicable to a csv file.

e) Select up to three columns for sorting in an ascending or descending order.

When the system processes the work items from the queue, it uses the sort criteria specified to retrieve the work items in that order. For example, to process payslips with first Employee ID followed by Employee Name from 1 to n and A to Z, specify Employee ID and Employee Name in an ascending order.

- Use queue category: Add header columns by searching for an Existing queue category or a list or from the Available queue categories.
  Tip: Search for an existing queue category when there are a large number of categories available for selection.
- Manually: Define the work item structure manually. You do not have to select from an existing structure.

  a) Enter a name for the work item structure in the Queue Category field.

  For example, if the queue contains employee information, enter the Queue Category as 'Employee Data'

  b) Add column header names for the work item and select the data type for each column - Text, Number, or Date
  c) Select the display and sorting for the columns in the Enterprise Control Room.

  When the system processes the work items from the queue, it uses the sort criteria specified to retrieve the work items in that order. For example, to process payslips with first Employee ID followed by Employee Name from 1 to n and A to Z, specify Employee ID and Employee Name in an ascending order.

2. Click Next to Add work items.

Add work items

Add work items from an Excel or CSV file to the queue.

Tip: You can also add work items later by editing the queue. See Edit queues.

When adding work items, ensure that the work item values are valid and non-empty. For example, if the work item column data type is Number, then the work item value for that column must have a numeric value. Similarly, for the Date type of the data type. If the values for Number or Date data types are invalid or empty, then the corresponding work item is marked as Data Error.

WLM work item life cycle

However, if the work item column data type is Text and if you have not provided any value, the work item is still marked as Ready to run. You can edit the work item and provide appropriate values. The Edit work item page also allows you to change the work item status.

Edit work items

©2020 Automation Anywhere. All rights reserved.

Procedure

1. Click Browse to select an Excel or CSV file.
   The file is added as a work item in the queue.
2. Click Create Queue.

The queue is successfully added at the top of the Queues list. You can choose to apply the column sorting to view as required.
Note: When you upload work items from an .xls or .xlsx file with data type as text, the Excel file column populated with a date in any format (for example, 8/6/2019) is converted to its corresponding WLM date format (for example, Sat Jun 08 00:00:00) in the Enterprise Control Room Work Item. However, the same is not applicable to a .csv file.

Next steps

1. Run bot with queue

   After you have created a queue, it is ready for deployment from a bot

2. Manage Work Items

   Manage work items of a queue to fix the discrepancies before queue processing and reduce your automation-related errors.

Run bot with queue

Collectively process all work items of a queue across all the Bot Runners present in one or more device pools.

To run a bot with queue, the following feature permissions are required:

- Run my bots
- Schedule my bots to run

Use Run a bot with queue from:

1. Activity > Scheduled, Bots > My Bots page.
2. Workload > Queues page.

The procedure for running a bot with a queue is the same in all these pages.

To process the work items using the Bot Runners, choose the bot to run, select a queue and a device pool, and give it a name with an appropriate description.

To run a bot with queue, do the following:

Step 1: Add bots and dependent files
Add bots and dependent files to the automation using Run bot with queue.
Step 2: Select a queue and device pools
Add queues and device pools to the automation using Run bot with queue.

©2020 Automation Anywhere. All rights reserved.

Step 3: Add name and description (optional)
Add a name and description for the automation using Run bot with queue.

Related tasks
View automation of a queue
Related reference
Sample Workload Management properties file

Add queues and device pools

Add queues and device pools to the automation using Run bot with queue.

Prerequisites

You can select only those queues that are not in use and for which you have consumer access privileges. The In use queues appear disabled in the Available queues list. This means that you cannot use multiple queues to add Bot Runners.

Procedure

1. Select a Queue from the Available queues list.
   Tip: Use Search to quickly find the required queue and device pool.
2. Click Add.
3. Select a Device Pool from the Available device pools list.
4. Click Add.
   The queue and device pool are added to the run bot with the queue list.
5. Optional: Select Run bot runner session on Control Room for devices that are in a locked state
6. Optional: Click Remove to replace the queue or device.
7. Click Save (Run?).

Add bots and dependencies

Add bots and dependent files to the automation using Run bot with queue.

Prerequisites

You can run only Unattended Bots. You cannot run Attended Bots from the .

Procedure

1. Go to Activity > Scheduled, Bots > My Bots, or Workload > Queues page.
   You are taken to the Bots > My bots page.
2. Click Run bot with queue.
   Note: If version control is enabled, you can choose either the latest version or the production version of the Bots.
3. Select a TaskBot to process in the queue from the Folders list.
   By default, the My Tasks folder is selected.
   Tip: Use Search to find a file quickly.
4. Go to the folder that contains the required TaskBot.

©2020 Automation Anywhere. All rights reserved.

5. Click Add.
   If the TaskBot has any dependent files, they are shown in the Bot + Dependencies tab above the file selection.
6. Optional: Review the list of dependent files, if available.
7. Optional: Click Replace to select another bot instead of the selected one.
8. Click Next to Add queues and device pools.

Add name and description

Add a name and description for the automation using Run bot with queue.

Prerequisites

The system assigns the automation Name that contains the filename, date, time, and username by default. This is automatically generated and can be changed based on your requirement.

Procedure

1. Name: Enter a name for the automation.
2. Enter a Description.
   Tip: This could describe the purpose of running the bot with a queue.
3. Click Run now.
   The status of the queue changes from Not in use to In use in the Queues list on the Queues page.

   Note that this queue will not be available for any other automation. This means that only one queue can be used by one bot.

Next steps

1. Estimate the device pool size or time required to process a given queue size. See Manage workload SLAs.
2. 11.3.1.2 If required, update the wlm.properties file to configure the time interval required to trigger an automation. See Sample Workload Management properties file.

Workload

For workload maintenance tasks such as view the details of queues to pause, stop, or resume its automation, edit the queues, manage the work items in the queue, and delete the obsolete queues.

Workload maintenance tasks

For workload automation maintenance, do the following (in any order):

- Manage Work Items: Manage work items of a queue to fix the discrepancies before queue processing and reduce your automation-related errors.
- View queue details: Use the View queues details page to view the details of a particular queue.

©2020 Automation Anywhere. All rights reserved.

- View automation of a queue: Use the View activity in progress page to Pause, Resume, or Stop an in-progress automation.
- Edit queues: Edit a queue using two methods - from the Queues list, or from the View queue page.
- Delete queues: Delete any selected or all the available queues.

Related concepts
Manage workload queues
Related tasks
Manage workload SLAs

View queue details

Use the View queues details page to view the details of a particular queue.

Prerequisites

Permissions required:

1. Queue Creator or Queue Participant rights
2. View and manage my Queues feature permission

Procedure

1. Go to Workload > Queues
2. Hover over a queue to view
3. Click the vertical ellipsis button
4. Click the view details button
   This launches the View queues page which shows details of the queue in two sections:
   a) Name, Description, My access status, and queue Status such as:
   - b) Active when work item is currently being processed or staged for processing
   - c) Complete when work item successfully processed by a Bot Runner or marked Complete
   - d) Unsuccessful when work item processing failed on Bot Runner
   - e) Ready to run when work item is successfully processed for execution does not have any data errors and can be staged for processing
   - f) On hold when work item is deferred from processing by a Bot Runner
   - g) Data error when there is an error in loading data from the file

   h) Queue contents in different tabs such as:
   - i) Work Items: This is the default view. This allows you to view all work items in a list form. Use this to edit, delete or modify the column view and change the status of all or selected work items.
   - j) General: View the Reactivation Threshold and Time required to complete one work item.
   - k) Owners: View the user names of queue owners who can edit the queue and add new work items.
     Note: You must have the View user basic permission to view information about other users that are added as queue owners.
   - l) Participants: View the user names of queue participants who can add new work items and view the queue.
   - m) Consumers: View the user names of consumers who can view the queue and all the work items in the queue. In addition, they can use this queue when running bots.
   - n) Work Item Structure: View the work item structure that you defined when creating the queue.

©2020 Automation Anywhere. All rights reserved.

Tip: Edit any of these details by either clicking the edit this queue link or the Edit button. Also delete the queue by clicking the Delete button.

Next steps

View automation of a queue
Related concepts
Manage Work Items
Related tasks
Create queues
Edit queues
Delete queues
Related reference
Actions allowed on view queue page

Actions allowed on view queue page

Use different actions such as sorting, searching, or filtering on the table view of the queues.

Searching and filtering

For ease of access, apply search parameters to Status, My Access, Queue Name, Work Item Result, ID, and Start Time columns.

- Specify the search parameters in the search bar for Queue Name. When you specify search parameters for the same column, the system searches using OR operator. When you specify search parameters for different columns, the system searches using AND operator.
- Choose the search parameters from a list in the search bar for Work Item Status.
- 11.3.3 Apply filters to Work Item Result to quickly track the final status of the Work Item. For example if the Work Item was completed or skipped.
- 11.3.4.1 Use the Work Item ID to search for specific Work Items and combine with the Start Time to monitor the progress of the Work Items that you search based on the ID. The Start Time filters the list of all Work Items that start between two given Start Date and Start Times. For example, all Work Items started between 01/12/2019 13:00 hrs. and 31/12/2019 15:00 hrs.
  Note: Use a hyphen (-) as separator between IDs as any other symbol gives an error. For example, 100-250.

Table items

The following describes the list of items that can be viewed in the table:

Table Item	Description
ID	Shows the system generated id for a work item. When a work item is added to a queue, system generates an id for that work item.
Status	Shows Work item status:

©2020 Automation Anywhere. All rights reserved.

Table Item	Description
	• Active when work item is currently being processed. This means the bots corresponding to that work item are running. • Complete when work item successfully processed by a Bot Runner or marked Complete. • Unsuccessful when work item processing failed on Bot Runner. • Ready to run when work item is successfully processed for execution does not have any data errors and can be staged for processing. • On hold when work item is deferred from processing by a Bot Runner • Data error when there is an error in loading data from the file
11.3.3 Work Item Result	Shows the value that you set in the Set work-item result command. See Set work item result command.
Start Time and End Time	Shows the Work Items processing start/end time and date.
Modified by	Shows the name of the user who had modified the Work Item last.
Last Modified	Shows the time and date when the Work Item was modified last.

Note: Apart from the above system generated columns, the fields that you define in your work item are also displayed as columns.

Actions on table column

Use the following actions on a table column:

- Click a column to sort it in ascending and descending order. You can sort up to three columns by holding the Shift key when you click two more columns. This gives you the option of sorting two additional columns. This way the sorting is done on the entire table and not just the data that is currently visible to you. The last sorting is stored in memory applied by a user per session.
- Drag a column to the left or right
- Move your mouse cursor at the end of the column and drag to re-size

Actions on Work Items

Use the following tasks on specific Work Items:

Table Item	Description
Refresh	Allows you to refresh the table contents so that you can view the latest Work Item status
Delete	Allows you to delete one or multiple Work Items.
Mark complete	Allows you to mark one or more Work Items as Complete whose status is On hold, Data Error, or Ready to run.
Ready to run	Allows you to mark one or more Work Items as Ready to run whose status is On hold, or Data Error

©2020 Automation Anywhere. All rights reserved.

Table Item	Description
On hold	Allows you to mark one or more Work Items as On hold whose status is Ready to run
Customize columns	Allows you to show or hide specific columns. By default, all columns are displayed including the ones defined in the Work Item.

Alternately, select Work Items and use the following actions. Note that these actions can be performed only at a table level and not on individual Work Items.

Table Item	Description
View	Allows you to view details of selected Work Item.
Edit	Allows you to edit details of selected Work Item. You can see this icon only if you are the Queue Owner or Participant or Consumer and the status of the Work Item is Unsuccessful, On hold, or Data error
Delete	Allows you to delete the selected Work Item. Note that if a Work Item is in Active state, you are not allowed to delete it.
11.3.4.1 Export items to CSV	Allows you to export the selected Work Items to a CSV file. You can export a maximum of 100,000 Work Item entries at a time. To export, use the following options: • Export selected Work Items. • Export filtered Work Items based on the search parameters such as date and time filters - for last 24 hours, or 7, 30, 60, and 90 days, or custom date and time. • Export all Work Items. Note: The CSV file naming convention includes the browser time instead of UTC when you use the option Export checked items.

Related tasks
Define work item structure

Edit queues

Edit a queue using two methods - from the Queues list, or from the View queue page.

Prerequisites

Permissions required:

1. AAE_Queue Admin role
2. Queue Owner rights to edit queues that you created
3. Queue Participant rights to edit queues that are created by other queue owners

©2020 Automation Anywhere. All rights reserved.

Procedure

1. Go to Workload > Queues
2. Edit a queue from the View queue page or from the Queues list
3. Hover over a queue to edit
4. Click the vertical ellipsis button
5. Click the View button
   The View queue page is launched.
6. Click either of the following to launch the Edit Queue page
   - edit this queue link
   - Edit button
7. Edit the queue details such as the queue name (applicable only if in draft), description, work items, threshold and time values, owners, participants, and consumers.
   Note:
   - The Work Item structure cannot be edited after it is defined.
   - 11.3.4 You must have the View user basic permission to view information about other users that are added as queue owners.
8. Upload a file for the work item that will be used for processing in this queue
   The Work Items tab is shown by default.
   Tip: You can search for a work item quickly based either on Status or Status details using the search option.
9. Click Browse
10. Select the file to upload
    Note: You can upload only an Excel or CSV file.
11. Click Save changes
    If you provide a duplicate name, an error is displayed.
12. Edit the name and save the changes made to the queue
    An edit successful message appears.

Next steps

Delete queues
Related concepts
Manage Work Items
Related tasks
Create queues
View queue details
Delete queues

View automation of a queue

Use the View activity in progress page to Pause, Resume, or Stop an in-progress automation.

Prerequisites

Permissions required:

1. AAE_Queue Admin role
2. Queue Consumer or Queue Participant rights
3. Manage everyone's In progress activity feature permission

©2020 Automation Anywhere. All rights reserved.

Procedure

1. Go to Workload → Queues
2. Hover over a queue with status In use
3. Click the vertical ellipsis button
   This launches the In progress → View activity in progress page where you can Pause/Resume or Stop the automation.
   Note: Although this page is accessible from the Workload module, the page is launched from Activity module. However, you cannot Pause/Resume or Stop actions directly from the Activity > In progress page. For these actions, the Workload > Queues > View automation action is used.
   - Click the Pause button
     The system will pause distributing work items from this queue to available bot runners in the device pool.
     Note: Until you resume this automation, any work items with Ready to Run status from this queue are not sent for processing.
   - Click the Resume button.

     The system will start distributing the work items from this queue.

   - Click the Stop button

     The system stops distributing the work items from the queue associated with this automation.

4. Select any of the following option in the message
   - Click Accept to return to the Queues page.
   - Click Cancel to return to the In progress page.

Next steps

Edit queues
Related tasks
Delete queues
View queue details

Delete queues

Delete any selected or all the available queues.

Prerequisites

Permissions required:

1. AAE_Queue Admin role
2. Queue Owner rights

Procedure

1. Go to Workload > Queues.
2. Delete selected or all queues
   - Delete selected queue

a) Hover over a queue to delete
b) Click the vertical ellipsis button
c) Click the Delete button
d) A confirmation message to permanently delete the selected queue appears.
e) Click Yes, delete to confirm or No, cancel to discard the action.
f) A confirmation message appears after you delete the queue

- Delete multiple selected or all queues
  a) Select the check box of required queues or select the check-box given in the header to select all queues
  b) Click the Delete button above the table header.
  c) A confirmation message to permanently delete multiple queues appears.
  d) Click Yes, delete to confirm or No, cancel to discard the action.
  e) A confirmation message appears.
  Note: A queue will not be deleted if it is being used for processing a work item. An error message appears for that particular queue.

Next steps

Manage workload SLAs
Related tasks
View queue details
View automation of a queue
Edit queues

Manage Work Items

Manage work items of a queue to fix the discrepancies before queue processing and reduce your automation-related errors.

To mange work items, do the following:

Step 1: View work items
View work items with a status of Completed, Unsuccessful, On hold, Active, or Data Error in the View work item page.
Step 2: Edit work items
Use the Queues page or the Work item page to edit the work items of a queue if their status is Unsuccessful, On hold, or Data Error.
Step 3: Delete work items
Delete work items one at a time or in bulk in the View work item page. You cannot delete any work item with Active status.

Related tasks
View queue details

View work items

View work items with a status of Completed, Unsuccessful, On hold, Active, or Data Error in the View work item page.

©2020 Automation Anywhere. All rights reserved.

Prerequisites

Permissions required:

1. AAE_Queue Admin role.
2. View and manage my Queues feature permission.
3. Queue Owner, Queue Consumer, or Queue Participant

Procedure

1. Go to Workload > Queues.
2. Select and open a queue in view or edit mode.
3. Hover over a work item to view it.
4. Click the vertical ellipsis button.
5. Click View.
   The View work item page appears. The page provides details of the work item in four sections- Work Item Details, Work Item, Automation, and Work Item Results.
6. In the Work Item Details section, view the following:
   a) Status
      a) Successful or Unsuccessful for work items that have failed, are in unknown state or stopped.
      b) Pending for work items that are deferred, new or paused.
      c) Active for work items that are already processed in the queue and are running.
      d) Data error for work items that are being uploaded from the file.
      e) 11.3.3 Ready to run for work items that are being processed in the queue.
   b) Status Details
      a) Successful for work item with a status of NA.
      b) Unsuccessful for work items with one or more errors has an Unknown status or is stopped.
      c) Active for work item with a status of NA.
      d) Pending for a work item that is new, deferred, or paused.
      e) Data Error for work items with one or more errors.
   c) Start time and End time: This is shown when the work item is being processed.
   d) Queue Name: View the name of the queue of this work item.
7. In the Work Item section, view the following:
   a) Attributes of the selected work item.
   b) Audit log comments (if any) that were added when editing the work item.
8. In the Automation section, view the name of the automation, bot name, and device pool under which this work item was processed.
9. In the Work Item Results section, view the output status of the work item processed in the Enterprise Control Room
   Tip: If a chat bot is integrated with the Enterprise Control Room, the work item status can be shown to a customer by retrieving the result with the help of a REST API. See List all work items in a queue
10. In the General Details section, view the Last modified date and time, Modified by, and Object type.

Next steps

1. Edit work items
2. Delete work items

Related reference

©2020 Automation Anywhere. All rights reserved.

Work item status and actions

Edit work items

Use the Queues page or the Work item page to edit the work items of a queue if their status is Unsuccessful, On hold, or Data Error.

Prerequisites

Permissions required:

1. AAE_Queue Admin role
2. View and manage my Queues feature permission
3. Queue Owner, Queue Consumer, or Queue Participant

Procedure

1. To edit a work item, use any of the following methods based on where you are in the Workload page:
   - Queues page:
     a) Hover over a work item to edit it.
     b) Click the vertical ellipse button.
     c) Click Edit.
   - Work Item page > Edit button > .

   The work item page appears in edit mode.
2. Change the work item status to Mark complete, Defer, or Re-process in the Work item attributes and automation details section.
   The system will set the status to Data Error during the data load if there is any issue with the data. For example, if a user types a text value for a number field, or an invalid date string for an attribute of date type, the status is displayed as Data Error.
   Work item status and actions.
3. Click Save changes.

Next steps

Delete work items

Delete work items

Delete work items one at a time or in bulk in the View work item page. You cannot delete any work item with Active status.

Prerequisites

Permissions required:

1. AAE_Queue Admin role
2. View and manage my Queues feature permission

©2020 Automation Anywhere. All rights reserved.

3. Queue Owner, Queue Consumer, or Queue Participant

Procedure

1. Go to Workload > Queues.
2. Select and open the queue in view or edit mode.
3. Hover over a work item to view it.
4. Click the vertical ellipsis button.
5. Click Delete.
   The selected work item is deleted successfully.
   Note: You can also delete a work item one at a time or in bulk using the Delete option provided above the Work items table.

Related tasks
Manage workload SLAs
Related reference
Sample Workload Management properties file
Work item status and actions

Work item status and actions

Based on the work item status, only certain work item actions allowed.

Work item- status and actions

The following table provides a description of each work item status and the action you can do on a work item having that status:

Work Item Status	Description	Actions
Active	Work item is currently being processed	View
Completed	Work item successfully processed by a Bot Runner	View and Delete
Unsuccessful	Work item processing failed on Bot Runner	View, Edit, and Delete
Ready to run	Work item is successfully processed for execution	View, Edit, and Delete
On hold	Work item is deferred for use by the Queue admin	View, Edit, and Delete
Data Error	Error in loading data from the file	View, Edit, and Delete
Paused	Work item processing was paused by the Queue admin	View, Edit, and Delete

Related tasks
Edit work items

©2020 Automation Anywhere. All rights reserved.

Manage workload SLAs

Estimate the device pool size or time required to process a given queue size from the Workload Service Level Agreement (SLA) page.

Prerequisites

Permissions required to orchestrate Workload Management to meet your organizations' target SLA:

1. Enterprise Control Room admin or a user with the SLA Calculator feature permission
2. AAE_Queue_Admin role
3. Queue Owner, Participant, or Consumer privilege

Tip: You can see only those automations with queues for which you are either the owner /participant / consumer. However, the Queue Admin can see all the queues in the system.

Procedure

1. Select an active automation to arrive at the targeted SLA.
   You can also directly enter the parameters for calculation if you do not have an existing automation. If specified, the data from this is used to calculate the SLA in the Calculation tab.
2. Click the right arrow button to add the automation for the SLA calculation.
3. Click Next.
   The Calculation tab appears.
4. If you have selected an existing automation, the system populates the number of work items processed and the average processing time of a work item for that automation.
5. Enter the following:
   a) Number of work items processed. The maximum number of work items allowed are up to 999999999999 (ninety-nine billion, nine hundred ninety-nine million, nine hundred ninety-nine thousand, nine hundred ninety-nine). For example, enter 67890.
   b) Average processing time per work item either in days, hours, minutes, or seconds. For example, 2000 seconds or 33 minutes and 20 seconds.
   c) The number of devices in your device pool in The processing time with this number of devices field to calculate the time it takes to process the number of work items specified with the given average processing time of each work item. For example, the number of devices for processing time is 120.
6. Click Calculate
   The system shows the result based on the specified parameters. For example, your SLA will be 8 hours and 20 minutes if the above example is considered.
7. Enter The number of devices with this total processing time field to calculate the device pool size.
8. Click Back to return to the previous tab if required.

Next steps

- Add or insert data for work items in a given queue in the Enterprise Control Room.
- Fetch the list of work items in a given queue and share the result with customers using a chat application.

©2020 Automation Anywhere. All rights reserved.

Sample Workload Management properties file

The Workload Management configuration file wlm.properties enables an Enterprise Control Room administrator to customize the workload-related properties based on the organization's automation requirements. For example, users can configure the time interval required to trigger an automation.

11.3.1.2

Sample code

Use the following sample code to configure the Workload Management-related properties:

```
wlm.db.staging.size=100
wlm.db.staging.low.water.mark=70
wlm.staging.upper.water.mark=50
wlm.staging.low.water.mark=35
wlm.ignite.low.water.mark=5

wlm.file.upload.encrypt.lines.count=100
wlm.file.upload.batch.size=100

workOrder.concurrent.execution.count=5
workOrder.max.execute.lines=1000

workOrder.execution.job.interval.seconds=30
allowed.workItem.processing.deviation=2
wlm.device.timeout.minutes=30
wlm.minimum.seconds.between.deploy=10
wlm.deploy.compensation.seconds=20
wlm.priority.pool.redeploy.minutes=30

wlm.automation.trigger.interval.millis=900000
```

1. Copy the code to a file and save it as a wlm.properties file in the config folder of the Enterprise Control Room application path.

   For example C:\Program Files\Automation Anywhere\Enterprise\config

2. You can change the properties based on the organization's workload automation requirements.

©2020 Automation Anywhere. All rights reserved.

For example, change the automation trigger interval. The default time is set to 15 minutes or 900000 milliseconds.

3. Restart the Automation Anywhere Enterprise Control Room Service for the changes to apply.
   Note: The wlm.properties file is available in the config folder by default from Version 11.3.3.

Related reference
Workload Management properties configuration description

Workload Management properties configuration description

11.3.1.2 Use the list of Workload Management properties as a reference to view the configurations in the wlm.properties file.

Configuration description with default values

Configuration	Default value	Description	Remarks
wlm.db.staging.size	100	Determines the number of Work Items that can be moved from new to draft state for staging to the messaging queue cache in a single instance. The state is marked internally. These are staged in order. For example, if you use 5 devices, the staging will start from 500 (100 x 5) Work Items. Note that Work Item refers to a row or line in a CSV file being processed.	This is an internal parameter and hence to be changed.
wlm.db.staging.low.water.mark	70	Determines the minimum number of staged Work Items that can be pushed to the messaging queue cache. When the number of staged Work Items are less than this value, the next batch of Work Items are moved to staging. For example, if you use 5 devices, the queue will include 350 (70 x 5) Work Items as the low water mark.	This is an internal parameter and hence to be changed.

©2020 Automation Anywhere. All rights reserved.

Configuration	Default value	Description	Remarks
wlm.staging.upper.water.mark	50	Determines the maximum number of staged Work Items that can be pushed to the Apache Ignite queue cache. For example, if you use 5 devices, 250 (50 x 5) work items can be queued.	This is an internal parameter and hence n to be changed.
wlm.staging.low.water.mark	35	Determines the number of Work Items that can be pushed from staging to queue to the Apache Ignite queue cache when the Work Items are less than the number given in this property. Note that the queue processing is continuous and this count keeps decreasing. Use this to maintain the level of Work Items that can be pushed from staging to queuing stage. For example, if you use 5 devices the Work Items are to be queued when the number is below 175 (35 x 5).	This is an internal parameter and hence n to be changed.
wlm.ignite.low.water.mark	5	Not Applicable from Version 11.3.3.	For users on versions l than 11.3.3 - This is an internal parameter and hence not to be changed.
wlm.file.upload.encrypt.lines.count	100	Determines the number of Work Items that can be encrypted.	This is an internal parameter and hence n to be changed.
wlm.file.upload.batch.size	100	Not Applicable from Version 11.3.3	For users on versions l than 11.3.3 - This is an internal parameter and hence not to be changed.
workOrder.concurrent.execution.count	5	Determines the maximum number of work orders that can be processed at a time. For example, you can concurrently process a	This is an internal parameter and hence n to be changed.

©2020 Automation Anywhere. All rights reserved.

Configuration	Default value	Description	Remarks
		maximum of 5 work orders when the property value is set to 5. Note that a work order is a background job that ingests set of Work Items for processing. For example, a work order can contain 100 Work Items.	
workOrder.max.execute.lines	1000	Determines the maximum number of Work Items in a work order that can be processed at a time. This is useful when data with large volumes are uploaded.	This is an internal parameter and hence n to be changed.
workOrder.execution.job.interval.seconds	30	Determines the default time interval between the processing of pending work orders.	This is an internal parameter and hence n to be changed.
allowed.workItem.processing.deviation	2	Not Applicable	Not applicable
wlm.minimum.seconds.between.deploy	10	Determines the minimum time between two concurrent Work Item deployments. This is not applicable from Version 11.3.3	For users on versions l than 11.3.3 - If you upload two Work Item in a Queue and there a two Devices then the f item will be processed 30 seconds and the second one will be processed 10 seconds after that.
wlm.priority.pool.redeploy.minutes	30	Determines the time interval specified in priority mode after which the Work Items are to be redeployed to all Bot Runner devices.	This parameter is deprecated from Versi 11.3.3 For users on versions l than 11.3.3 - If a Device stuck for any Work Iter then WLM will wait for minutes and then redeploy the next Wor Item to all other Devic

©2020 Automation Anywhere. All rights reserved.

Configuration	Default value	Description	Remarks
wlm.automation.trigger.interval.millis	900000	Determines the time interval (in milliseconds) for processing staged or queued Work Items. For example, when you create a new automation at 10:00, it will process the work item for queuing at 10:10.	This parameter is used the backend to refresh the Devices. If the 1st WLM automation fails, takes 15 minutes to redeploy. You can change this to a lower value - for example, 60000, which is 1 minute. After setting th value, restart the Automation Anywhere Control Room Service
11.3.3 wlm.workitems.columns.subcrub	False	Determines whether to truncate the characters of a data in a column when processing the Work Items. It is recommended that you keep this turned off as it runs on each field and affects data ingestion.	This is an internal parameter and hence to be changed.

Related reference
Sample Workload Management properties file

Bot Store integration overview

11.3.3 The seamless integration of the Bot Store enables you to access Bot Store directly from the Enterprise Control Room. In the Enterprise Control Room, you can download bots and Digital Workers from Bot Store or create and package Digital Workers and bots to be uploaded to Bot Store.

Benefits of Bot Store integration

- Discover and download pre-built, ready-to-use Digital Workersand bot packages from Bot Store to the Enterprise client.
- Leverage the 'one-stop-shop' solution to configure and run the downloaded bot in the Enterprise Control Room.

What are Digital Workers and protected bots

Digital Workers

Digital Workers are a set of role-related automation tasks that are performed in a sequence.

Digital Workers automate entire processes, do multiple tasks in a set of sequences, and are ready-to-deploy and download from the Automation Anywhere Bot Store.

©2020 Automation Anywhere. All rights reserved.

For example, an Accounts Payable Digital Worker can be used to automate invoice processing, payment processing, and record management.

Protected bots
The Bot Store offers developers, who build Digital Workers or bot packages, a monetization opportunity by protecting the business logic contained within the bots. When you run a protected bot, the commands that are executed are not displayed in the In progress activity page.

- Accessing Bot Store
  All Enterprise Control Room users can access Bot Store from the Home tab within the Bot Store tab.
- Downloaded bots from Bot Store
  The My Downloads page displays information about all the bots and Digital Workers that you have downloaded from the Bot Store.
- Running protected bots
  When you run a bot from the Enterprise Control Room, you can view its status, progress, activity being performed, and other information on the In progress activity page.

Related tasks
Accessing Bot Store
Downloading bots to Enterprise Control Room repository
Related reference
Downloaded bots from Bot Store
Folder structure of downloaded bots
Running protected bots

Accessing Bot Store

11.3.3 All Enterprise Control Room users can access Bot Store from the Home tab within the Bot Store tab.

Prerequisites

You must have valid Bot Store credentials and an Internet connection to access the Bot Store from the Enterprise Control Room. If you do not have valid Bot Store credentials, you must register with the Bot Store before accessing it from the Enterprise Control Room.
Note: You cannot use your Enterprise Control Room credentials to access the Bot Store.
To access the Bot Store, do the following:

Procedure

1. Navigate to Bot Store > Home.
2. Click Open Bot Store.
   Automation Anywhere opens the Bot Store in a separate tab.
3. Log in using your Bot Store credentials.

©2020 Automation Anywhere. All rights reserved.

Downloaded bots from Bot Store

11.3.3 The My Downloads page displays information about all the bots and Digital Workers that you have downloaded from the Bot Store.

When you access the page for the first time, you are required to log in using your Bot Store credentials. The system keeps you logged in for seven days. After seven days, you are required to log in to the Bot Store again.
Note: If you do not have valid Bot Store credentials, you must register with the Bot Store. After you have registered with the Bot Store, you can use the registered email ID and password to log in to the Bot Store from Enterprise Control Room. See Accessing Bot Store.

The list of bots or Digital Workers available on this page is the same as the list on the My Downloads page in the Bot Store. The list displays the bots and Digital Workers downloaded by you (the user that has logged in to the Bot Store from the Enterprise Control Room).

The My Downloads page provides the following information:

- TYPE: Specifies whether it is a bot or Digital Worker.
- NAME: Specifies the name of the bot or Digital Worker.
- ORDER DATE: Specifies the date and time the bot or Digital Worker was purchased or downloaded.
- OWNER NAME: Specifies the name of the person or organization that owns the bot or Digital Worker.
- PURCHASE TYPE: Specifies whether the bot or Digital Worker is available for free or must be purchased.
  Note: This column is hidden by default, you must unhide the column to display it on the page.

You can perform the following operations on this page:

- Use the Refresh table icon to refresh the list of downloaded bots and Digital Workers.
- Show or hide columns that are displayed in the table.
- Sort and filter the list based on the TYPE, NAME, OWNER NAME, and PURCHASE TYPE attributes. You can use the same attributes to search for a bot or Digital Worker.
- Download a bot or Digital Worker available on this page to the Enterprise Control Room repository. See Downloading bots to Enterprise Control Room repository.

- Downloading bots to Enterprise Control Room repository
  You can download bots that are available on the My Downloads page to the My bots page.
- Folder structure of downloaded bots
  When you download a bot or Digital Worker from the Bot Store to the Enterprise Control Room repository, it creates various folders within the Bot Store folders. These folders contain dependent files that the bot or Digital Worker uses.

Downloading bots to Enterprise Control Room repository

11.3.3 You can download bots that are available on the My Downloads page to the My bots page.

Prerequisites

Ensure that you have the `AAE_Bot Store Consumer` role assigned to you. See System created roles.

You must have upload permission to the Bot Store folder available within the My Tasks folder. If the bot or Digital Worker you are downloading contains a MetaBot, you must also have upload permission to the My MetaBots folder.

Procedure

1. Navigate to Bot Store > My Downloads.
2. Search for the bot that you want to download.
   You can search for a bot or Digital Worker based on the TYPE, NAME, OWNER NAME, and PURCHASE TYPE attributes.
3. Hover your mouse over the ellipsis to display the Download to my bots icon.
   Note: The Download to my bots icon is available only if you have the `AAE_Bot Store Consumer` role assigned to you.

   This icon is not available for the bots and Digital Workers that are created in the Enterprise client version earlier than the Version 11.3.3.

4. Click the Download to my bots icon.
   The Download to my bots page appears.
5. Select any of the following options to specify the action to take if the bot package already exists in the Bot Store folder in the Enterprise Control Room:
   - Skip the file (don't download it): Does not download the bots from the Bot Store that are already available in the bot package.
   - Overwrite the file with the downloaded one: Overwrites the bot available in the Enterprise Control Room repository with the bot downloaded from the Bot Store.
   - Cancel the download: Cancels the download of the bot from the Bot Store.

   The following options are available if version control is enabled in the Enterprise Control Room:

   - Create a new version: Creates a new version of the bot that is downloaded from the Bot Store.
   - Skip the file (don't download it): Does not download the bots from the Bot Store that are already available in the bot package and are of the same version.
   - Cancel the download: Cancels the download of the bot from the Bot Store.
     a) Select an option to specify how to handle the production version of the bot if you have selected the Create a new version option:
     - b) Keep production version as is currently set: Select this option if you do not want to change the current production version of the bot.
     - c) Set production version to imported version of file: Select this option if you want to change the production version to the version of the downloaded bot.
6. Click Download to my bots.
   The system downloads the bot package or Digital Worker from the Bot Store, extracts the files from the package, and copies the files into the relevant folders. The system creates a folder with the same name as that of the downloaded bot or Digital Worker within the `Bot Store` folder. It also creates other relevant folders and copies the dependent bots and other files in those folders.
   Note: If the downloaded bots or Digital Workers contain a MetaBot, that MetaBot is stored in the `My MetaBots` folder.
   You can view the progress of the bot being downloaded from the In progress activity page. See Monitor in progress activity.
   Note:

   The system does not display an error message if the download fails. The reason for why the download failed is available on the Audit log page.

©2020 Automation Anywhere. All rights reserved.

If the bot or Digital Worker you have downloaded from the Bot Store uses any credential variables, these variables are not created in the Credential Vault.

11.3.5 An unprotected bot downloaded through the Bot Store can have a duplicate GUID. Enterprise Control Room will create a new unique GUID for the downloaded bot to avoid data conflict in the Bot Insight dashboard.

Folder structure of downloaded bots

11.3.3 When you download a bot or Digital Worker from the Bot Store to the Enterprise Control Room repository, it creates various folders within the Bot Store folders. These folders contain dependent files that the bot or Digital Worker uses.

All the bots and Digital Workers that are available on the Bot Store are submitted as a package, which contains different folders containing files that are used as input and to store the output generated by these bots and Digital Workers. The dependent files are available in specific folders in a specific directory structure under the Bot Store folder in the Enterprise Control Room.
Note: If the downloaded bots or Digital Workers contain a MetaBot, that MetaBot is stored in the `My MetaBots` folder.

Use the Bot Store sub-folder under the My Tasks folder to access the dependent files for a bot or Digital Worker. The folder structure is similar for all bots and Digital Workers that you download from the Bot Store. The following example shows the folders available for a bot and Digital Worker downloaded from the Bot Store.

Table 1. Sample Digital Worker or Bot Package Structure

Digital Worker Folder	Sub-folders
<Digital Worker or bot package name>	My Tasks: Can contain only the .atmx file type. Store the Master Bot and all the other sub-tasks referred by the Master Bot in this sub-folder.
	My Metabots: Can contain only the .mbot file type.
	Error Folder: Can contain all the file types except .atmx and .mbot files
	Input Folder: Can contain all the file types except .atmx and .mbot files

Running protected bots

11.3.3 When you run a bot from the Enterprise Control Room, you can view its status, progress, activity being performed, and other information on the In progress activity page.

To protect the intellectual property of the Bot Creators, information about the command and logic of the bot downloaded from the Bot Store is not exposed. When you run a protected bot, information about the

©2020 Automation Anywhere. All rights reserved.

command being executed is not shown on the In progress activity page. Similarly, for a protected bot, information about the last command executed is not displayed on the Historical activity page. See Run a Bot.

You can identify a protected bot based on the value available in the PROTECTION TYPE column on the My bots page. A bot is protected if the value is Protected for that bot in the PROTECTION TYPE column.
Note: This column is hidden by default, you must unhide the column to show it on the page.

A bot or Digital Worker that you have downloaded may contain dependent bots that are protected. To view information about the dependent bots and whether they are protected or not, you can click the View bot icon on the My bots page. However, information about the command being executed is not shown for the dependent bots that are protected.

Audit log overview

Comprehensive and continuous audit logging capabilities in the Enterprise Control Room ensures enterprise-level security and quality compliance.

Across the platform, event details along with the outcome are automatically captured for more than 60 types of entity actions, including creation, modification, enabling, disabling, and removal of users, bots, Bot Creators, and Bot Runners.

A Enterprise Control Room administrator or a user with Audit Log privileges can view logs and details of both successful and unsuccessful activities in the Audit log page.

Audit log actions

In the Audit log page you can do the following:

- Filter data:
  - Time filter: Enables you to filter data for a specific time period. By default, the option is Last 24 hours selected. You can select other options to filter data for that period or configure a custom time filter.
  - Additional filter: Apart from the time filter, you can apply filters based on the status, activity type, name of an item, user who perform the action, source device and so on.
- Search: Search for the entries from the table. To search the exact phrase, enclose the search phrase within double quotes. Combine Time and Search filters to refine your search. For example, you can filter the audit log to search for Status = Successful for Last 7 days.
- Export data: Export data from the table to a CSV file. See, Export data to CSV.
- View details: View details of an entry in the table. Hover over the entry for which you want to view details and click Audit details. Refresh the contents to view the updated status.
- Customize columns: Enables you to set display option for row-level toolbar and to show or hide specific columns.

How to work efficiently with audit log entries

You can perform the following actions on a column of the Audit log table to help you work efficiently:

- Sort data: Click a column header to sort the data in that column in ascending and descending order. Use the Shift key to sort data for more than one columns. You can sort data for up to three columns. This gives you the option of sorting two additional columns. This way the sorting is done on the entire

©2020 Automation Anywhere. All rights reserved.

table and not just on the data that is currently visible to you. The last sorting is stored in memory applied by a user per session.
- Rearrange columns: Drag the column header to rearrange the columns in the table.
- Resize columns: Adjust the column header to resize the width of that column.
- View details: Click the View ( ) icon to view details of a record. This icon is displayed when you hover over the Actions ( ) icon.

- Specify search parameters for the same column for the Enterprise Control Room to search using OR operator. Specify search parameters for different columns, for using the AND operator.

  Note: When you use special characters, hyphen (-) or underscore (_), the system lists all Item Names, Source Devices, and Request ID instead of these columns having these parameters.

- View audit details
  The Enterprise Control Room admin or a user with Audit Log privileges can track the activity details from the Audit Log page.
- Export data to CSV
  You can export data to a CSV file. You can export selected records, all records, or filtered records.
- Audit logs for run bot deployment and bot runner session
  As a Enterprise Control Room administrator or a user with "View everyone's audit log actions" privileges, you can view audit entries for Run Bot Deployment and Bot Runner Sessions in the Audit log page of the Enterprise Control Room.
- Audit logs for bots downloaded from the Bot Store
  Enterprise Control Room administrators or a user with "View everyone's audit log actions" privileges can view audit entries for the bots or Digital Workers downloaded from the Bot Store in the Audit log page of the Enterprise Control Room. Audit logs for the above include successful and unsuccessful entries.

View audit details

The Enterprise Control Room admin or a user with Audit Log privileges can track the activity details from the Audit Log page.

Procedure

1. Click Audit Log.
2. (Optional) Use the Time Filter drop-down to change the interval time for the activity log.

   The Time Filter is set to 24 hours by default.

3. (Optional) Use the All columns drop-down and the Search field to find a specific action item.

   The Actions table lists the various available 'Action' items.

4. To view the details of any 'Action', click the > icon.

   Action Details page is displayed with the following details:

   - Status

     Shows if the selected action was succeded or failed.

- Action taken by

  The user name who performed the action.

- Object type

  Type of object for the selected action.

- Source device

  The IP address of the source device.

- Request ID

  Details of the Request ID.

- Item name

  Name of the item (if available).

- Time

  The time stamp of the user login.

- Action type

  Details of the type of action performed.

- Source

  Name of the source.

  Note: Only those fields where updates are available can be viewed. Also, the information that is stored in the Credential Vault is displayed (encrypted).

Note: It is not recommended to restart only the Automation Anywhere Elastic Search Service as it results in an error on the Enterprise Control Room Audit log page.

Related concepts
Credentials- Overview

Export data to CSV

You can export data to a CSV file. You can export selected records, all records, or filtered records.

You can use any of the following options from the Export items to CSV menu to export the data:

- Export checked items: Exports the records you have selected from the table.
- 11.3.4 Export filtered items: Exports the records available after applying filters from the table.
- 11.3.4 Export ALL items: Exports all the records available in the table.
  Note: You can export a maximum of 100,000 records at a time.

Notes:

©2020 Automation Anywhere. All rights reserved.

- 11.3.4 You must have the View user basic permission in order to export the basic information about other users to the CSV file.
- 11.3.5 The historical data of a deleted bot is also exported in the CSV file.

The time required to export data to a CSV file might vary based on the number of records being exported. A message appears on the screen if the time required to export the data is more than 2 seconds. The CSV file is available for download after it is generated.

The Export items to CSV option is disabled when exporting the data. However, you can perform other operations in the Enterprise Control Room. The system creates an audit entry only if the export process fails.

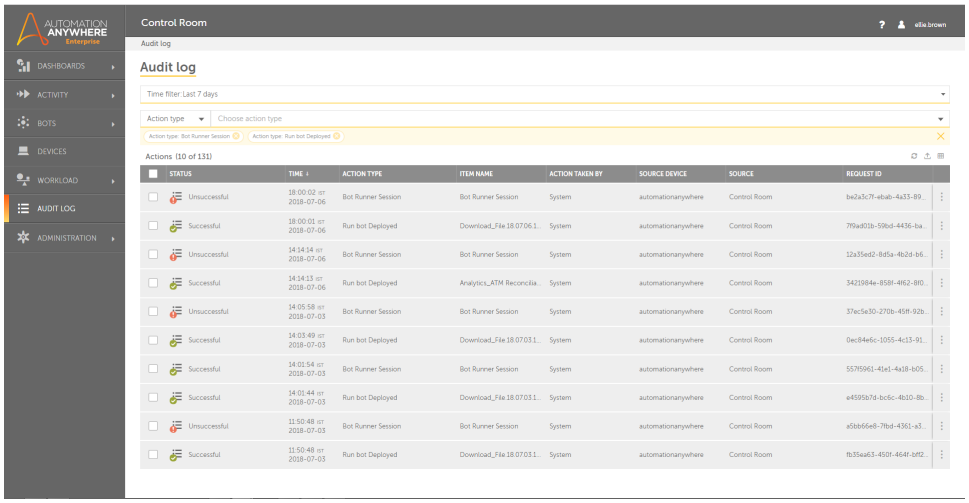
CAUTION: If you refresh the Enterprise Control Room while the export is in progress, the export process fails.

Audit logs for run bot deployment and bot runner session

As a Enterprise Control Room administrator or a user with "View everyone's audit log actions" privileges, you can view audit entries for Run Bot Deployment and Bot Runner Sessions in the Audit log page of the Enterprise Control Room.

Audit logs for the above include both entries - Successful and Unsuccessful.

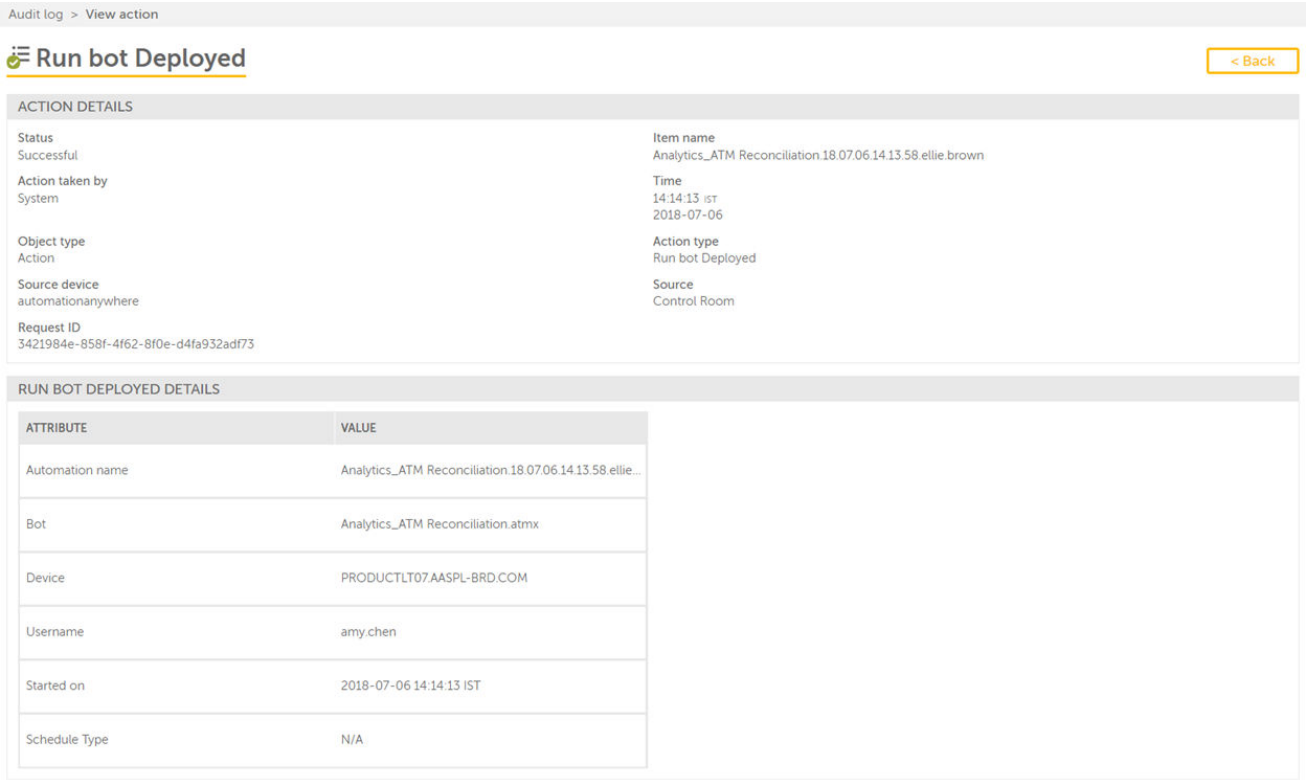
The following illustration shows entries relevant to Audit Log for Bot Deployment locally or through RDP:



Run bot deployment

Entries for a successful or unsuccessful bot deployment using the action Run now are logged in the Audit log page of the Enterprise Control Room. The following illustration shows successful deployment of a bot

on a Bot Runner machine:



Reasons for run bot deployment failure

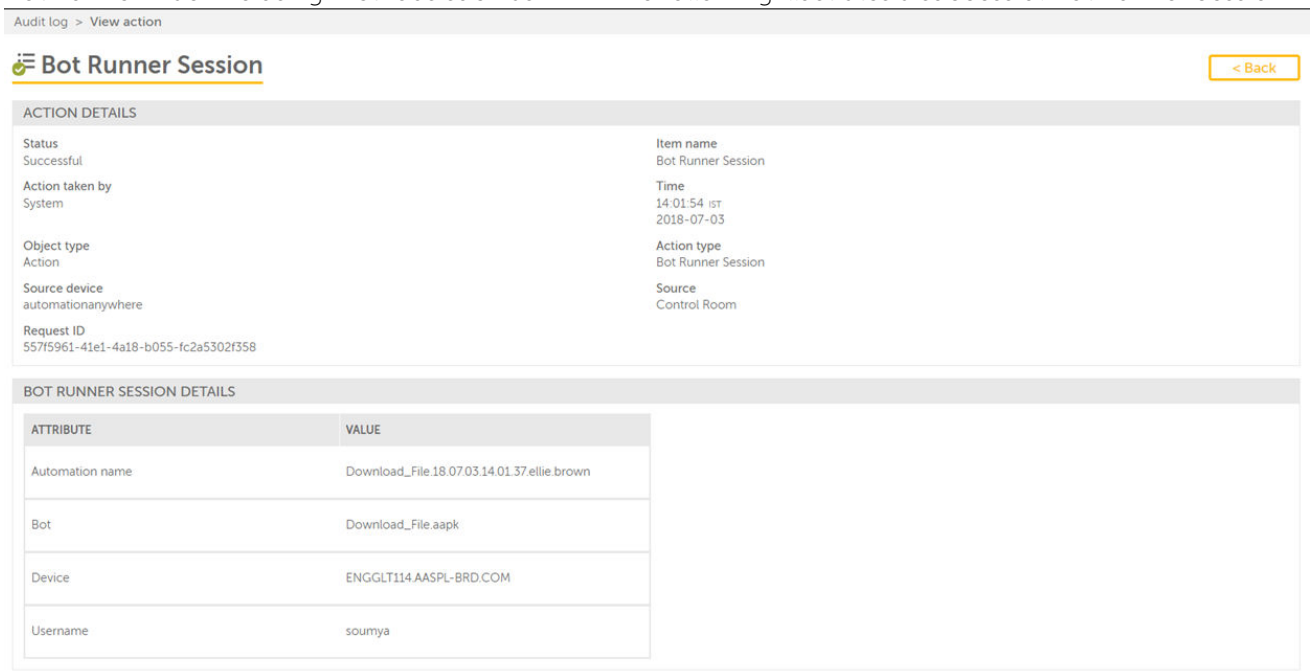
The reason for a run bot deployment failure is logged when,

1. Bot Runner could not be reached or shows disconnected, which could be due to:
    - The Enterprise client Service not running on the Bot Runner machine
    - Bot Runner machine is shut down
    - Network issues
    - Bot Runner user is not logged on to the Enterprise client
2. Bot Runner is disabled.
3. Bot Runner could not download the deployed package.

©2020 Automation Anywhere. All rights reserved.

Bot Runner Session

The audit entry for a Bot Runner Session is logged to indicate whether a bot was deployed successfully to a Bot Runner machine using methods such as RDP. The following illustrates a successful Bot Runner Session:



Similarly, when a Bot Runner Session fails, the audit details display the reasons in Results panel.

Reasons for Bot Runner Session failure

The reason for a Bot Runner session failure is logged when the Bot Runner's remote desktop session cannot be acquired in the following cases:

1. User has not set the Windows Login Credentials in the Tools > Options > Login > Settings of Enterprise client.
2. User has selected Bypass legal disclaimer in the Tools > Options > Login > Settings of Enterprise client.
3. Automation Anywhere Player is already running on the Bot Runner.
4. Remote Desktop Session to the Bot Runner is disabled.
5. Either the RDP port is blocked, there is a network error, or the Bot Runner host name was not resolved.

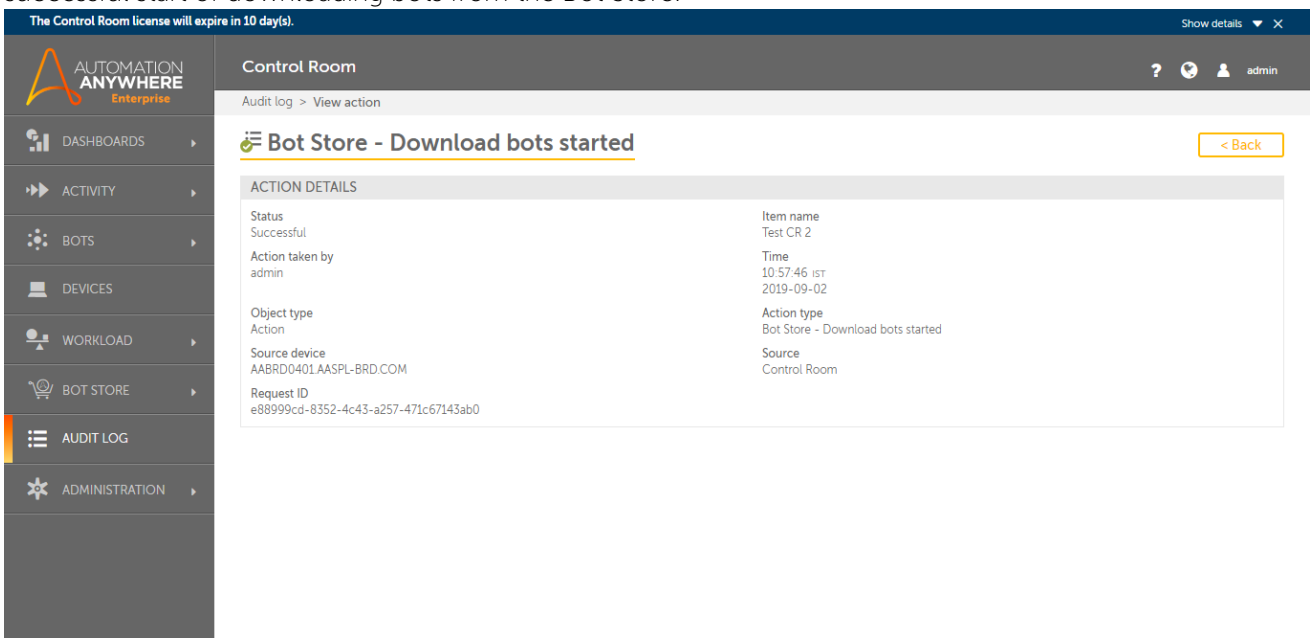
Audit logs for bots downloaded from the Bot Store

Enterprise Control Room administrators or a user with "View everyone's audit log actions" privileges can view audit entries for the bots or Digital Workers downloaded from the Bot Store in the Audit log page of the Enterprise Control Room. Audit logs for the above include successful and unsuccessful entries.

©2020 Automation Anywhere. All rights reserved.

Bot Store - Download bots started

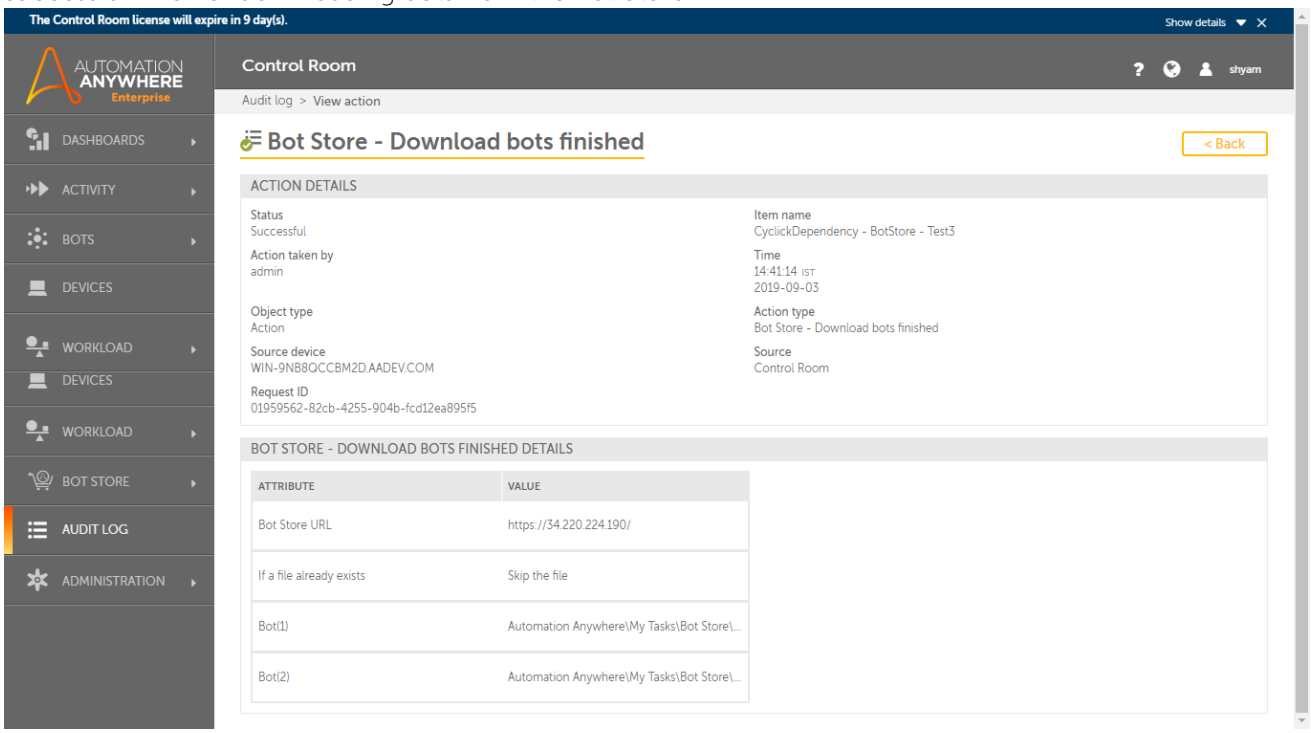
The entries for a successful or unsuccessful operation of starting the download process of a bot from the Bot Store to the Enterprise Control Room are logged in the Audit log page. The following illustrator shows successful start of downloading bots from the Bot Store:



Bot Store - Download bots finished

The entries for a successful or unsuccessful operation of finishing the download process of a bot from the Bot Store to the Enterprise Control Room are logged in the Audit log page. The following illustrator shows

successful finish of downloading bots from the Bot Store:



Note: The Bot Store - Download bots finished log appears before the Bot Store - Download bots started log for the bot packages or Digital Workers that are small in size.

Reasons for download bot failure

The process of downloading a bot from the Bot Store might fail because of the following reasons:

- The connection to the Bot Store is lost when the system is downloading a bot.
- The Enterprise client version of the bot or Digital Worker is not Version 11.3.3 or later.
- Lack of space in the Enterprise Control Room repository.
- The connection to the shared repository for Enterprise Control Room is lost when the system is downloading a bot.

Dashboards overview

The Enterprise Control Room dashboard provides graphical insight into your RPA infrastructure so that you can analyze, interpret, and make informed decisions for your bots.

The information about active users, registered clients, failed tasks, applications, bots, bot schedules, workflows, queues, and the overall status of devices (memory, CPU, and hard disk utilization) is dynamically updated on the dashboards.

Why use dashboards?

- Leverage real-time analytics to make business decisions.

©2020 Automation Anywhere. All rights reserved.

- Enforce corrective actions on resource allocations, configurations, and automation sequence based on operational details.
- Generate customizable dashboards specific to each entity using features, for example, filtering and sorting, to identify and alert abnormal activities.
- Get insight into all operational details of the bots as they are running.
- Ensure comprehensive insight into digital workforce performance by setting the time bar for each widget.

What you must know about operational and business analytics

Operational analytics

Monitor the performance of a bot, task status, past and upcoming schedules of tasks, audit information, utilization of various resources, workload status, and health of the machine on which the tasks are running.

The dashboards available for operational analytics are home, bots, devices, audit, and workload.

Business analytics

Leverage transactional analytics information to make business decisions, for example, the total sales in a month, invoicing and payment trends, insight about new customers, and quote to order ratio.

Access business analytics from the Insights dashboard in the Enterprise Control Room.

Related concepts
Dashboards - workload
Dashboards - audit
Dashboards - devices
Dashboards - bots
Dashboards - home
Related tasks
Dashboards - Insights
Related reference
How Business Analytics works

Dashboards - home

As an Enterprise Control Room user with View dashboards privileges, view data to which you have access permission presented in the form of widgets.

For more information, see Home dashboard.

Dashboards - bots

As an Enterprise Control Room user with View my bots and View my scheduled bots privileges, view the Bots page of the Dashboards module.

For more information, see Bots dashboard.

©2020 Automation Anywhere. All rights reserved.

Dashboards - devices

As an Enterprise Control Room user with Dashboard view privileges, view and analyze data related to devices (Bot Runner machines) when bots are deployed on them.

For more information, see Devices dashboard.

Dashboards - audit

A user with View everyone's audit log actions permission can view a snapshot of audit information as captured in the Enterprise Control Room.

For more information, see Audit dashboard.

Dashboards - workload

An Enterprise Control Room user with View Dashboard permissions can view the workload status of device pools, queues, and work items in the Executive or Operation Manager Dashboards.

Workload dashboard

The Workload dashboard provides information about the status of device pools, queues, and work items in the Executive dashboard tab and the Operation Manager's dashboard tab. The Executive dashboard tab enables you to monitor the progress of the queues for which you are an owner or a consumer. The Operation Manager's tab enables you to monitor the queues for which you are an owner, consumer, or participant.

EXECUTIVE DASHBOARD

Device pools by backlog: Provides information about the device pools by backlog. The device pool backlog is measured as the time required to complete the existing work item from all automation tasks in that pool. You can adjust the device pool size or reorder the automation tasks as per your requirement.

Queues by time to complete: Provides information about the list of queues ordered by time to complete. Time to complete is measured as the time required to complete the existing work items. You can pause or change the priority of an automation task. You can click an individual queue to view details such as queue name, number of open items, average processing time, and expected time to complete.

Queue status: Provides information about the queues that are processed in the last 7 days. The status for the work items of each queue is displayed and enables you to monitor the progress of your workload items.

Queue with average processing time: Provides information about the queues that were processed in the last 7 days with the average processing time. The queues listed are based on the average processing time for a work item compared to a daily average.

OPERATION MANAGER'S DASHBOARD

©2020 Automation Anywhere. All rights reserved.

Device pools by FTE: Enables you to view pools in descending order of Full Time Equivalent (FTE). This allows you to evaluate the value of each pool in the equivalent manual effort required to process the same work item.

Pools by decreasing error rate: Enables you to view pools ordered by decreasing error rate and enables you to identify the pools that require attention. The error rate is calculated as the number of work items with an error by the number of work items processed from that pool.

Device pools by backlog: Provides information about the device pools by backlog. The device pool backlog is measured as the time required to complete the existing work item from all automation tasks in that pool. You can adjust the device pool size or reorder the automation tasks as per your required.

Queues with average wait time: Enables you to view the list of queues that are processed in the last 7 days with the average wait time. This helps you to decide whether to increase the priority or pool size as per your business needs. The wait time is calculated by subtracting the processing start time from the automation start or resume time.

Queues by decreasing error rate: Enables you to view the list of queues ordered by decreasing error rate and helps you identify the queues that require attention. The error rate is calculated as the number of work items with error divided by the number of work items processed from that pool.

Dashboards - Insights

Bot Insight helps automation experts to access real-time business insights and digital workforce performance measurement by leveraging productivity data that the deployed bots generate and process. It helps the automation experts and consumers to interactively analyze task data using widgets.

Prerequisites

- To access the Bot Insight application from the Enterprise Control Room Insights dashboard, you must either be a Bot Creator or a Enterprise Control Room user with AAE_Bot Insight Admin, AAE_Bot Insight Consumer, or AAE_Bot Insight Expert privileges.
- To access Bot Insight, ensure the Bot Insights - Business Analytics license is enabled.

Procedure

1. Go to Enterprise Control Room > Dashboards > Insights.
2. Click Open Bot Insight.
   Automation Anywhere opens the Bot Insight dashboard in a separate tab.
3. Enter the Bot Insight login credentials.
   If you are already logged into the Enterprise Control Room, you do not need to login again into Bot Insights. For more information about the Single Sign-on feature into applications, see Log onto Bot Insights.
4. Click Go to Enterprise Control Room and re-login as a user with the appropriate permissions if you do not have the required Bot Insight permissions or if the Bot Insight license has expired.

Next steps

For more information, see Business Analytics.

©2020 Automation Anywhere. All rights reserved.

Enterprise Control Room APIs

The Automation Anywhere Enterprise Control Room provides various public APIs which allow you to customize your business automation for third-party applications.

These APIs enable the third-party applications to consume RPA, orchestrate bots and manage the RPA data based on events.

Filters in an API request body
: Filtering provides basic conditional queries and page control for processing web pages. There are 3 basic features related to filtering: filtering conditions, sorting columns, and pagination parameters.

Use these APIs to manage your business automation using third-party applications.

- Audit API
  Requests audit data for a given input combination of date filter, sorting mechanism, and pagination.
- Authentication API
  Use the Authentication API to generate, refresh, and manage JSON Web Tokens (JWT) that are required for authorization in all Enterprise Control Room APIs.
- Auto Login Credentials API overview
  Use the Auto Login Credentials API to automate the login process in order to remotely run bots on locked devices. Users with an AAE_Admin role can create, update, or delete the login credentials.
- Automation Management API
  Use the Enterprise Control Room bot Automations API to trigger deployment of bots from an external system or a third-party application.
- Bot Execution Orchestrator API
  As a Enterprise Control Room administrator or a user with View and Manage Scheduled Activity permission, deploy bots and monitor its progress using a set of Enterprise Control Room APIs.
- APIs to manage credential vault
  As an Enterprise Control Room user with Manage my credentials and lockers role permissions, use the Credential Vault API to manage your attributes, credentials, keys, lockers, and Credential Vault mode in the Enterprise Control Room.
- Bot Insight Data API
  Get bot process data for analytic analysis. Only users with Bot Insight administration role can access this API.
- API to export and import Bot Lifecycle Management
  Use the export and import bots APIs to customize the organization's Bot Lifecycle Management solution for an uninterrupted automation life-cycle.
- API data migration from 10.x to 11.x Enterprise Control Room
  As a Enterprise Control Room administrator with View and Manage Migration role permissions, use the Migration APIs to migrate data from 10.x to the latest 11.x Enterprise Control Room.
- API to add and remove manual dependencies
  Use the Manual Dependencies API to manually add and remove dependent files to/from a TaskBot from My Docs, My Exes, and My Scripts folders in the repository.
- License API
  Request detailed license information for your Enterprise Control Room installed licenses.
- Repository Management API overview
  Use the Repository Management API to programmatically delete a file, retrieve bot variables, return a list of files and folders in a folder, and search for files and folders in your Enterprise Control Room.
- User management API overview
  Use the User Management APIs to create, search, update, or delete roles and users in your .

©2020 Automation Anywhere. All rights reserved.

- Workload Management API overview
  Use the Workload Management (WLM) API to programmatically manage and create queues and work items in your Enterprise Control Room.
- Filters in an API request body
  Filtering provides basic conditional queries and page control for processing web pages. There are 3 basic features related to filtering: filtering conditions, sorting columns, and pagination parameters.

Audit API

Requests audit data for a given input combination of date filter, sorting mechanism, and pagination.

Prerequisites

JSON Web Token (JWT)
: All Enterprise Control Room APIs require a JSON Web Token (JWT) to access the APIs. Generate an authentication token using the Authentication API. A JWT is required to run all Enterprise Control Room APIs.

Roles and license
: Users with the AAE_Admin role or users with the View everyone's audit log actions permission are able to view audit logs for the Enterprise Control Room.

- URL: `http://<your_control_room_url>/v1/audit/messages/list`
- Method: POST

Note:

- Use the Swagger definition files installed with your Enterprise Control Room to test the APIs. View the available Swagger APIs at `http://<your_control_room_url>/swagger/`
- You can also use a REST client to complete this task.

Procedure

1. Add an authentication token to the request header.
   Note: Use the Authentication API to generate a JSON Web Token.
2. Select POST as the method.
   Note: Apply filters to perform basic conditional queries and pagination control for processing web pages. There are three basic features related to filtering: filtering conditions, sorting columns, and pagination parameters. Refer to the Filters in an API request body.

   The following example requests unsuccessful login attempts for the month of December.

   Request body:

```
{
  "sort": [
    {
```

```
      "field": "createdOn",
      "direction": "desc"
    }
  ],
  "filter": {
    "operator": "and",
    "operands": [
      {
        "operator": "gt",
        "field": "createdOn",
        "value": "2019-12-01T00:00:00.001Z"
      },
      {
        "operator": "lt",
        "field": "createdOn",
        "value": "2019-12-31T23:59:59.999Z"
      },
      {
        "operator": "eq",
        "field": "status",
        "value": "Unsuccessful"
      },
      {
        "operator": "substring",
        "field": "activityType",
        "value": "LOGIN"
      }
    ]
  },
  "fields": [],
  "page": {
    "length": "1000",
    "offset": "0"
  }
}
```

3. Send the request.

- In Swagger, click Execute.
- In a REST Client, click SEND.

The response for this example returned data for date filter, sorting, and pagination. When there is no filtering used in the request, a successful response returns all pages for the specified Enterprise Control Room.

Response body:


```
{
  "page": {
    "offset": 0,
    "total": 847,
    "totalFilter": 4
  },
  "list": [
    {
      "id": "aOhx024BVd_jtov73ujy",
      "eventDescription": "User does not exist in Control Room.",
      "activityType": "LOGIN",
      "environmentName": "",
      "hostName": "50.xxx.xxx.66",
      "userName": "string",
      "status": "Unsuccessful",
      "source": "Control Room",
      "objectName": "N/A",
      "detail": "",
      "createdOn": "2019-12-05T00:24:45Z",
      "requestId": "a5f69abd-766c-4eed-8d2f-79aff572538c",
      "createdBy": "0"
    },
    {
      "id": "Y-ht024BVd_jtov7Nej4",
      "eventDescription": "User provided incorrect password.",
      "activityType": "LOGIN",
      "environmentName": "",
      "hostName": "50.xxx.xxx.66",
      "userName": "docs-2fa",
      "status": "Unsuccessful",
```


©2020 Automation Anywhere. All rights reserved.

```
      "source": "Control Room",
      "objectName": "N/A",
      "detail": "",
      "createdOn": "2019-12-05T00:19:40Z",
      "requestId": "8995877f-a9ba-41cf-8d6a-a3cfe5a5d63a",
      "createdBy": "0"
    },
    {
      "id": "m46_yG4BGE7puvDMHe_6",
      "eventDescription": "User does not exist in Control Room.",
      "activityType": "LOGIN",
      "environmentName": "",
      "hostName": "50.xxx.xxx.66",
      "userName": "string",
      "status": "Unsuccessful",
      "source": "Control Room",
      "objectName": "N/A",
      "detail": "",
      "createdOn": "2019-12-02T22:33:18Z",
      "requestId": "e3e6387e-9cd9-45af-ac5c-9279c1a63f95",
      "createdBy": "0"
    },
    {
      "id": "mI6qyG4BGE7puvDMle-y",
      "eventDescription": "User does not exist in Control Room.",
      "activityType": "LOGIN",
      "environmentName": "",
      "hostName": "50.xxx.xxx.66",
      "userName": "System",
      "status": "Unsuccessful",
      "source": "Control Room",
      "objectName": "N/A",
      "detail": "",
      "createdOn": "2019-12-02T22:10:52Z",
      "requestId": "a1d5944e-f14e-4981-a65d-7d2a59ed0c44",
      "createdBy": "0"
```


©2020 Automation Anywhere. All rights reserved.

```
    }
  ]
}
```

Response headers:

```
cache-control: no-cache, no-store, max-age=0, must-revalidate
content-length: 1854
content-security-policy: default-src 'self'
content-type: application/json
date: Sun, 08 Dec 2019 04:58:53 GMT
expires: 0
pragma: no-cache
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
x-xss-protection: 1; mode=block
```

Note: You can also run REST requests from a command terminal. The following is a curl request example. This example is formatted for readability.

```
curl -X POST "http://ec2-34-210-185-177.us-west-2.compute.amazonaws.com/v1/audi
t/messages/list" -H "accept: application/json" -H "X-Authorization: eyJhbGciOiJ
SUzUxMiJ9.eyJzdWIiOiI0IiwiY2xpZW50VHlwZSI6IldFQiIsImxpY2Vuc2VzIjpbXSwiYW5hbHl0a
WNzTGljZW5zZXNQdXJjaGFzZWQiOnsiQW5hbHl0aWNzQ2xpZW50Ijp0cnVlLCJBbmFseXRpY3NBUEki
OnRydWV9LCJpYXQiOjE1NzU3ODExMTUsImV4cCI6MTU3NTc4MjMxNSwiaXNzIjoiQXV0b21hdGlvbkF
ueXdoZXJlIiwibmFub1RpbWUiOjU2MzI3OTk4MTE5ODEzMDAsImNzcmZUb2tlbiI6IjRmYWM1ODg1Zj
M0ZThkYmJhZGQ1ZTMwZDIxNGY3MDA3In0.sqyQ5DiAMqSqu4qpiALFxW0cJGZCJCT8u-oJ9AoUBSvQ7
gS5Ss0hszFR4zYIMG_8qQBcENnySnfeDpTysyclRKRx2TCjb2OVpPI8Y76g-6vlaZgJP-_iOloOBzso
1I0Q7EHkFE7UOaeWurLcltUXCnjZfYaPC4UJqQTNto0LqavlxsBC3HdxYLg4FiA0D7CKP_sb9CAVPVK
N9wlxU35gFzggiBYxifVXSAtB_wtWbJzHeirgx4fuAw8lTBIO0URjgRSR4mgMt0y6hOHIrGuLhtx13c
3YQnQ2n5xfWX2OzbdwOLreIu87mbCiA4KZ9X95q1TuI7r6jKecUlrv-RwkVw" -H "Content-Type
: application/json" -d "{ \"sort\": [ { \"field\": \"createdOn\", \"direction\"
: \"desc\" } ], \"filter\": { \"operator\": \"and\", \"operands\": [ { \"operat
or\": \"gt\", \"field\": \"createdOn\", \"value\": \"2019-12-01T00:00:00.001Z\
" }, { \"operator\": \"lt\", \"field\": \"createdOn\", \"value\": \"2019-12-31T
23:59:59.999Z\" }, { \"operator\": \"eq\", \"field\": \"status\", \"value\": \"
Unsuccessful\" }, { \"operator\": \"substring\", \"field\": \"activityType\", \
```

©2020 Automation Anywhere. All rights reserved.

```
"value\": \"LOGIN\" } ] }, \"fields\": [], \"page\": { \"length\": \"1000\", \"
offset\": \"0\" }}"
```

Related concepts
Audit API filter example with createdOn and userName fields

Authentication API

Use the Authentication API to generate, refresh, and manage JSON Web Tokens (JWT) that are required for authorization in all Enterprise Control Room APIs.

The JWT is a text string with 703 characters.


```
{
  "token": "eyJhbGciOiJSUzUxMiJ9.eyJzdWIiOiIxIiwiY2xpZW50VHlwZSI6IldFQiIsImxpY2
Vuc2VzIjpbXSwiYW5hbHl0aWNzTGljZW5zZXNQdXJjaGFzZWQiOnsiQW5hbHl0aWNzQ2xpZW50Ijp0c
nVlLCJBbmFseXRpY3NBUEkiOnRydWV9LCJpYXQiOjE1NzMxMDc4NzMsImV4cCI6MTU3MzEwOTA3Mywi
aXNzIjoiQXV0b21hdGlvbkFueXdoZXJlIiwibmFub1RpbWUiOjM2NTc1NjI0OTQ2MzE2MDAsImNzcmZ
Ub2tlbiI6ImNiZjgwZWNkZmU5YmUwYzViOGI2MDk3NmU0ZTI2MTNiIn0.rGYxbS5kKUTxtZhYtRSXpm
IHwbf3IwLBIKDEA7odG5uGVAjD55Tv05bYdARx_3-tl1CBg_cDGbwj5FvaBt9u5xKu5W5j3Nur6x3PF
62NeB3ZIdxiUPaFBU0Br84mPJMD4_EpwBfbeSVOMH6ngiLtJYhIOtJa0kp4pAAm3mvkuOUELtH8lf3p
Qf-2Ose2fUAaebDkqiH13SUF1TONAjUQv6Ef_uY0wgq9SjZwKHg9SKUhX3S8PXAJne_ih2QnN8nUE1S
XGlkC04eoIvyWpFkM963XEjptc2uvwtVn42MdA4Nd1opD5yijEl9VM92Fe1sPb6_T5-oV-U1Iw0JHiX
2-Ug",  . . .
}
```


auth

POST http://<your_control_room_url>/v1/authentication

Body parameters:

```
{
  "username": "string",
  "password": "string",
  "apiKey": "string",
  "mfaCode": 0
}
```

Make a post request to generate a JWT.

- The `username` of the Automation Anywhere user.

©2020 Automation Anywhere. All rights reserved.

- The `password` of the Automation Anywhere user.
- The `apiKey` is required to configure Single Sign On (SSO). It can also be used in place of a password for users that are assigned to the API key generation role.
- The `mfaCode` is required for user with a role that has been enabled for two-factor authentication (2FA). See, Enabling Two-factor authentication.
  Note: We recommend that you either disable 2FA in a role or create a separate role that does not use 2FA for use in scripts or other programmatic environments. You should use username and apiKey to authenticate when programmatically making API requests. Avoid using passwords in plain-text format to improve security.

Note: Authentication tokens have a default timeout of 20 minutes.
A JWT is required in the header of other Enterprise Control Room APIs. Not all parameters are required to generate an authentication token. Go to the examples listed here for detailed information.

- Authenticate with username and password
- Authenticate with username and apiKey
- Authenticate using two-factor authentication (2FA)

Note:

Simple and Protected Negotiation GSSAPI Mechanism (SPNEGO)

You can use SPNEGO, pronounced "spenay-go," when your Enterprise Control Room is configured properly with the following authentication features:

- Active Directory (AD) mode of authentication
- AD is Kerberos enabled

In an Enterprise Control Room with SPNEGO properly configured, users do not need to enter a username and password to generate a JWT.

SPNEGO Authentication API URL example:`https://<your_control_room_url/v1/authentication/SPNEGO`

GET http://<your_control_room_url>/v1/authentication/token/{token}
URL parameter:
The token you are validating.
Note: The token is passed as a parameter in the URL. There are no parameters for the request body.

Read Validate an authentication token for task details.

POST http://<your_control_room_url>/v1/authentication/token
Body parameter:
A refresh token allows you to get a new token without the need to collect and authenticate credentials every time a token expires.

```
{
  "token": "string"
}
```

Click Refresh an authentication token for a detailed example of this API.

©2020 Automation Anywhere. All rights reserved.

POST http://<your_control_room_url>/v1/authentication/logout

Header parameter:

Immediately expires the token that you add to the header of the request.

```
POST 'http://<your_control_room_url>/v1/authentication/logout'
-H 'X-Authorization: <access_token>
```

Click Immediately logout (expire) an authentication token for a detailed example of this API.

POST http://<your_control_room_url>/v1/authentication/app/login

The `.../authentication/app/login` API is a service to service authentication API used by Automation Anywhere internally supported applications. This API is not supported for use by external users.

Related tasks

Create and assign API key generation role

Authenticate with username and password

Make a POST request with a username and password to generate a JSON Web Token (JWT) to use for authentication in Enterprise Control Room APIs.

Prerequisites

- Valid username and password for your Enterprise Control Room
- REST client or access to Automation Anywhere Swagger for your Enterprise Control Room.

- URL: `http://<your_control_room_url>/v1/authentication`
- Method: POST

Procedure

1. Enter the following parameters in the request body.
   Request body:

```
{
"username": "jdoe",
"password": "mypassword@123"
}
```

Depending on how your Enterprise Control Room is configured, a domain could be require with the username.

```
{
"username": "your-domain\\jdoe",
```

```
"password": "mypassword@123"
}
```

2. Send the request.
   - In a REST Client, click SEND.
   - In the Swagger interface, click Execute.

   Response body:
   Note: The JWT is a 703 character string.


```
{
  "token": "eyJhbGciOiJSUzUxMiJ9.eyJzdWIiOiIxIiwiY2xpZW50VHlwZSI6IldFQiIsI
mxpY2Vuc2VzIjpbXSwiYW5hbHl0aWNzTGljZW5zZXNQdXJjaGFzZWQiOnsiQW5hbHl0aWNzQ2x
pZW50Ijp0cnVlLCJBbmFseXRpY3NBUEkiOnRydWV9LCJpYXQiOjE1NzMxMDc4NzMsImV4cCI6M
TU3MzEwOTA3MywiaXNzIjoiQXV0b21hdGlvbkFueXdoZXJlIiwibmFub1RpbWUiOjM2NTc1NjI
0OTQ2MzE2MDAsImNzcmZUb2tlbiI6ImNiZjgwZWNkZmU5YmUwYzViOGI2MDk3NmU0ZTI2MTNiI
n0.rGYxbS5kKUTxtZhYtRSXpmIHwbf3IwLBIKDEA7odG5uGVAjD55Tv05bYdARx_3-tl1CBg_c
DGbwj5FvaBt9u5xKu5W5j3Nur6x3PF62NeB3ZIdxiUPaFBU0Br84mPJMD4_EpwBfbeSVOMH6ng
iLtJYhIOtJa0kp4pAAm3mvkuOUELtH8lf3pQf-2Ose2fUAaebDkqiH13SUF1TONAjUQv6Ef_uY
0wgq9SjZwKHg9SKUhX3S8PXAJne_ih2QnN8nUE1SXGlkC04eoIvyWpFkM963XEjptc2uvwtVn4
2MdA4Nd1opD5yijEl9VM92Fe1sPb6_T5-oV-U1Iw0JHiX2-Ug",
  "user": {
    "id": 9,
    "email": "a@a.com",
    "username": "jdoe",
    "domain": null,
    "firstName": "",
    "lastName": "",
    "version": 9,
    "principalId": 9,
    "deleted": false,
    "roles": [
      {
        "name": "API_Key_Generation",
        "id": 23,
        "version": 0
      },
      {
        "name": "AAE_Basic",
```

```
        "id": 2,
        "version": 0
      },
      {
        "name": "Docrole1",
        "id": 18,
        "version": 0
      },
      {
        "name": "AAE_Meta Bot Designer",
        "id": 13,
        "version": 0
      }
    ],
    "sysAssignedRoles": [],
    "groupNames": [],
    "permissions": [

        . . .

    ],
    "licenseFeatures": [
      "RUNTIME"
    ],
    "emailVerified": true,
    "passwordSet": true,
    "questionsSet": true,
    "enableAutoLogin": false,
    "disabled": false,
    "clientRegistered": false,
    "description": "",
    "createdBy": 1,
    "createdOn": "2019-10-10T13:39:56-05:00",
    "updatedBy": 1,
    "updatedOn": "2019-10-13T02:09:38-05:00",
    "publicKey": null,
```


©2020 Automation Anywhere. All rights reserved.

```
    "appType": null,
    "routingName": null,
    "appUrl": null
  }
}
```

Related concepts
Authentication API

Authenticate with username and apiKey

Make a POST request with a username and API to generate a JSON Web Token (JWT) to use to authenticate in Enterprise Control Room APIs.

Prerequisites

- A user with the Generate API-Key role.
  Note: The Generate API-Key feature requires the creation of a custom role, see Create and assign API key generation role.
- Generate API-Key.
- Valid username and apiKey for your Enterprise Control Room
- REST client or access to Automation Anywhere Swagger files for your Enterprise Control Room.

- URL: `http://<your_control_room_url>/v1/authentication`
- Method: POST

Using a Generate API-Key enables users to create tokens without the need to gather user credentials.

Procedure

1. Enter the following parameters in the request body.
   Request body:
   Note: The API-Key is a 40 character string.

```
{
"username": "jdoe",
"apiKey":  "3/.Z)8:P`+yVJq . . . *fTk.i>|VOOl&:"
}
```

   Depending on how your Enterprise Control Room is configured, a domain could be require with the username.

```
{
"username": "your-domain\\jdoe",
```

```
"apiKey":  "3/.Z)8:P`+yVJq . . . *fTk.i>|VOOl&:"
}
```

Note: The API-Key Duration can be configured by an Admin user from the ADMINISTRATION > Settings > General tab.

2. Send the request.
   - In a REST Client, click SEND.
   - In the Swagger interface, click Execute.

   Response body:
   Note:
   Note: The JWT is a 703 character string.


```
{
  "token": "eyJhbGciOiJSUzUxMiJ9.eyJzdWIiOiIxIiwiY2xpZW50VHlwZSI6IldFQiIsI
mxpY2Vuc2VzIjpbXSwiYW5hbHl0aWNzTGljZW5zZXNQdXJjaGFzZWQiOnsiQW5hbHl0aWNzQ2x
pZW50Ijp0cnVlLCJBbmFseXRpY3NBUEkiOnRydWV9LCJpYXQiOjE1NzMxMDc4NzMsImV4cCI6M
TU3MzEwOTA3MywiaXNzIjoiQXV0b21hdGlvbkFueXdoZXJlIiwibmFub1RpbWUiOjM2NTc1NjI
0OTQ2MzE2MDAsImNzcmZUb2tlbiI6ImNiZjgwZWNkZmU5YmUwYzViOGI2MDk3NmU0ZTI2MTNiI
n0.rGYxbS5kKUTxtZhYtRSXpmIHwbf3IwLBIKDEA7odG5uGVAjD55Tv05bYdARx_3-tl1CBg_c
DGbwj5FvaBt9u5xKu5W5j3Nur6x3PF62NeB3ZIdxiUPaFBU0Br84mPJMD4_EpwBfbeSVOMH6ng
iLtJYhIOtJa0kp4pAAm3mvkuOUELtH8lf3pQf-2Ose2fUAaebDkqiH13SUF1TONAjUQv6Ef_uY
0wgq9SjZwKHg9SKUhX3S8PXAJne_ih2QnN8nUE1SXGlkC04eoIvyWpFkM963XEjptc2uvwtVn4
2MdA4Nd1opD5yijEl9VM92Fe1sPb6_T5-oV-U1Iw0JHiX2-Ug",
  "user": {
    "id": 9,
    "email": "a@a.com",
    "username": "jdoe",
    "domain": null,
    "firstName": "",
    "lastName": "",
    "version": 9,
    "principalId": 9,
    "deleted": false,
    "roles": [
      {
        "name": "API_Key_Generation",
        "id": 23,
        "version": 0
      },
```

```
      {
        "name": "AAE_Basic",
        "id": 2,
        "version": 0
      },
      {
        "name": "Docrole1",
        "id": 18,
        "version": 0
      },
      {
        "name": "AAE_Meta Bot Designer",
        "id": 13,
        "version": 0
      }
    ],
    "sysAssignedRoles": [],
    "groupNames": [],
    "permissions": [

        . . .

    ],
    "licenseFeatures": [
      "RUNTIME"
    ],
    "emailVerified": true,
    "passwordSet": true,
    "questionsSet": true,
    "enableAutoLogin": false,
    "disabled": false,
    "clientRegistered": false,
    "description": "",
    "createdBy": 1,
    "createdOn": "2019-10-10T13:39:56-05:00",
    "updatedBy": 1,
```


©2020 Automation Anywhere. All rights reserved.

```
    "updatedOn": "2019-10-13T02:09:38-05:00",
    "publicKey": null,
    "appType": null,
    "routingName": null,
    "appUrl": null
  }
}
```

Related concepts
Authentication API
Related tasks
Authenticate with username and password

Authenticate using two-factor authentication (2FA)

Two-factor authentication (2FA) is a subset of multi-factor authentication (MFA). It provides an additional security layer that Automation Anywhere applies at the role level for users.

Prerequisites

- Valid username, password, and mfaCode for your Enterprise Control Room.
- REST client or access to Automation Anywhere Swagger for your Enterprise Control Room.

Note:

- The mfaCode is a Time-based One-Time Password (TOTP). We use two-factor authentication (2FA) which is a subset of the multi-factor authentication (MFA). Users need a 2FA code generator to create one-time codes or tokens.
- We recommend that you either disable 2FA in a role or create a separate role that does not use 2FA for use in scripts or other programmatic environments. You should use username and apiKey to authenticate when programmatically making API requests. Avoid using passwords in plain-text format to improve security.

- URL: `http://<your_control_room_url>/v1/authentication`
- Method: POST

Two-factor authentication is supported only in Active Directory and non-Active Directory user environments; it is not supported for an SSO environment.

Procedure

1. Enter the following parameters in the request body.
   Request body:

```
{
  "username": "docs-2fa-vm3",
```

©2020 Automation Anywhere. All rights reserved.

```
  "password": "mypassword@123",
  "mfaCode": 879179
}
```

2. Send the request.
   - In a REST Client, click SEND.
   - In the Swagger interface, click Execute.

   Response body:
   Note: The JWT is a 703 character string.


```
{
  "token": "eyJhbGciOiJSUzUxMiJ9.eyJzdWIiOiI3IiwiY2xpZW50VHlwZSI6IldFQiIsI
mxpY2Vuc2VzIjpbIkRFVkVMT1BNRU5UIl0sImFuYWx5dGljc0xpY2Vuc2VzUHVyY2hhc2VkIjp
7IkFuYWx5dGljc0NsaWVudCI6dHJ1ZSwiQW5hbHl0aWNzQVBJIjp0cnVlfSwiaWF0IjoxNTc1N
TY4MzU5LCJleHAiOjE1NzU1Njk1NTksImlzcyI6IkF1dG9tYXRpb25Bbnl3aGVyZSIsIm5hbm9
UaW1lIjo3NDYzMjI1Njc3MDE2MywiY3NyZlRva2VuIjoiMmY1ODZjYzFkNGNkM2RjOTBhNWI1M
WMwOTZlMmZmOTAifQ.juAhCYWz_mzAt_6WH5fTg3XzvmPWIM4LRTBDmh6_S7FRqfTBUWwquygN
Dek6EqLfXlvfaDp-3A5m0uYr7pJMdAjnYFMt29BSQTDtvb3ArqfVFQWvFB7a55N1zl_IvW-1Tn
fPxrGKqmK5tA2M4LKsaJ7EewBGWPEJAYKSlBgeo6-jtsioP6bOvFsSKLzn0CaFeFZ4lQthrKNH
5YdlwuOs01p1yOxuHUVzmOqYw8UeyOChh6A-fZjF2586ynLV4H-VFLK3YtxYRm1cwMi-d6RN3E
Hpu65Cqo0hBmTv0yF3p7edG3SmS9C1AZMk2Q3cksAcPzgoFKNvQ4tBUC2Mqd1kjQ",
  "user": {
    "id": 7,
    "email": "myemail@mycompany.com",
    "username": "docs-2fa-vm3",
    "domain": null,
    "firstName": "",
    "lastName": "",
    "version": 3,
    "principalId": 7,
    "deleted": false,
    "roles": [
      {
        "name": "APIKeyGenerator",
        "id": 18,
        "version": 0
      },
      {
```

```
        "name": "AAE_Meta Bot Designer",
        "id": 13,
        "version": 0
      },
      {
        "name": "docs-2fa-role",
        "id": 17,
        "version": 0
      }
    ],
    "sysAssignedRoles": [],
    "groupNames": [],
    "permissions": [
      {
        "id": 97,
        "action": "viewbotstore",
        "resourceId": null,
        "resourceType": "botstore"
      },
      {
        "id": 58,
        "action": "myschedule",
        "resourceId": null,
        "resourceType": "taskscheduling"
      },
      {
        "id": 59,
        "action": "managecredentials",
        "resourceId": null,
        "resourceType": "credentials"
      },
      {
        "id": 61,
        "action": "createstandard",
        "resourceId": null,
        "resourceType": "credentialattribute"
```

```
      },
      {
        "id": 91,
        "action": "generateapikey",
        "resourceId": null,
        "resourceType": "api"
      },
      {
        "id": 29,
        "action": "view",
        "resourceId": null,
        "resourceType": "repositorymanager"
      },
      {
        "id": 103,
        "action": "viewuserbasic",
        "resourceId": null,
        "resourceType": "usermanagement"
      },
      {
        "id": 62,
        "action": "metabotdesigner",
        "resourceId": null,
        "resourceType": "metabot"
      },
      {
        "id": 30,
        "action": "view",
        "resourceId": null,
        "resourceType": "devices"
      }
    ],
    "licenseFeatures": [
      "DEVELOPMENT"
    ],
    "emailVerified": true,
```


©2020 Automation Anywhere. All rights reserved.

```
    "passwordSet": true,
    "questionsSet": true,
    "enableAutoLogin": true,
    "disabled": false,
    "clientRegistered": false,
    "description": "",
    "createdBy": 4,
    "createdOn": "2019-12-04T20:45:05-08:00",
    "updatedBy": 4,
    "updatedOn": "2019-12-05T09:50:33-08:00",
    "publicKey": null,
    "appType": null,
    "routingName": null,
    "appUrl": null
  },
  "mfaSetupRequired": false
}
```


Next steps

Users with the role to generate API keys can use an apiKey in place of a passwordto generate and authentication token. See, Create and assign API key generation role.


```
{
  "username": "docs-2fa-vm3",
  "apiKey": "-Jc$z@p?'E`X!lCmds/6Yn<7_?3}XYjks#55Gl,K",
  "mfaCode": 879179
}
```


Related tasks
Create and assign API key generation role
Enabling Two-factor authentication

Validate an authentication token

Send a REST request to verify if a token is valid.

Prerequisites

- The token you are validating.

- REST client or access to Automation Anywhere Swagger files for your Enterprise Control Room.

- URL: `http://<your_control_room_url>/v1/authentication/token`
- Method: GET

Procedure

1. Enter the following parameters to the request URL.
   http://<your_control_room_url>/v1/authentication/token?token=<token>
2. Send the request.
   - In a REST Client, click SEND.
   - In the Swagger interface, click Execute.

   Response body:
   The token is valid.

```
{
  "valid": true
}
```

   The token is invalid.

```
{
  "valid": false
}
```

Related concepts
Authentication API

Refresh an authentication token

Refresh valid authenticatoin tokens without the need to collect user credentials.

Prerequisites

- The token you are refreshing.
- REST client or access to Automation Anywhere Swagger files for your Enterprise Control Room.

- URL: `http://<your_control_room_url>/v1/authentication/token`
- Method: POST

Procedure

1. Enter the following parameters in the request body.
   Request body:

```
{
    "token": "eyJhbGciOiJSUzUxMiJ9.eyJzdWIiOiIxIiwiY2xpZW50VHlwZSI6IldFQiI
sImxpY2Vuc2VzIjpbXSwiYW5hbHl0aWNzTGljZW5zZXNQdXJjaGFzZWQiOnsiQW5hbHl0aWNzQ
2xpZW50Ijp0cnVlLCJBbmFseXRpY3NBUEkiOnRydWV9LCJpYXQiOjE1NzMxMDgwNjEsImV4cCI
6MTU3MzEwOTI2MSwiaXNzIjoiQXV0b21hdGlvbkFueXdoZXJlIiwibmFub1RpbWUiOjM2NTc3N
TA4OTY5NzUxMDAsImNzcmZUb2tlbiI6ImJiNjgzMGJhMDY5MWYwYjZiM2M3MDE4NGY0OGM0MWY
1In0.f3kPRspfm0sei9DGHd9NoyLK-iCO-vs--8b_pLG9XSUR0186uvXFopB75eVAaG-1l_AZh
R78UE6Voi7_UggzHkLRrEpQ-szR7cmFDpLxZ28xLnFJYhaIuMNdw9dWDVquBWTQSpYGNJd56D-
tFFHBodwVdNamqWHxaQebq1zMyUyQV6Q-gKdgubpT5gwuXnp-BwScjHOYM3Fpj_nt0nEbJC5uW
pJNtLQBpVzhsRwwlRKNOHQVbo6X7zkvKBoij8ewa5FWQwX7T-760BeqfssR6mmMUo0zRaneUKA
YAskz0B-X5PcyCkrVJju2XqItQ9XMGNP7h_MaUDotU_CJyguPZA"
}
```


2. Send the request.
   - In a REST Client, click SEND.
   - In the Swagger interface, click Execute.

   Response body: A new token with an updated experation time.


```
{
  "token": "eyJhbGciOiJSUzUxMiJ9.eyJzdWIiOiIxIiwiY2xpZW50VHlwZSI6IldFQiIsI
mxpY2Vuc2VzIjpbXSwiYW5hbHl0aWNzTGljZW5zZXNQdXJjaGFzZWQiOnsiQW5hbHl0aWNzQ2x
pZW50Ijp0cnVlLCJBbmFseXRpY3NBUEkiOnRydWV9LCJpYXQiOjE1NzMxMTMxMTgsImV4cCI6M
TU3MzExNDMxOCwiaXNzIjoiQXV0b21hdGlvbkFueXdoZXJlIiwibmFub1RpbWUiOjM2NjI4MDc
1NDY4NjYzMDAsImNzcmZUb2tlbiI6ImUxODBiZjYxMzQyMjkwZTRlM2Q4M2ZlNTU3YWRmMmE5I
n0.mtR1RNDe3EPzlaLQ7mwF0yIk8G00wLKGmKTFhM2689rItXHjLLgv0iYaM1LPUtRv9GafjhX
fshcIm9lucyf8k8t3A7SVJFoiFY2TUNgeouPgHl7XlpzpmenDRoT4Otu9R1_FTpMi40HH81ARG
7WoLDPdOyhxgL9ZvoVtRgkMiNTn1vUJWGhzd6wMYzf70rJO_TcMKgLh3X6fpPkY_xD2ykrKsds
MO2lZnzDjzuf3BCdzGjMj1q99WKBgVwyMafv4WApUX5peRZlsiVJdZrM2x890yovW2Yy_fY3wd
P_57XRp1oA5vnm9FxJN9lKyxVic3Qvx8BGtXmR-GQ3T8fndjw",
  "user": {
    "id": 1,
    "email": "a@a.com",
    "username": "admin",
    "domain": null,
    "firstName": "",
    "lastName": "",
    "version": 1,
```

```
    "principalId": 1,
    "deleted": false,
    "roles": [
      {
        "name": "AAE_Admin",
        "id": 1,
        "version": 0
      }
    ],
    . . .
    ],
    "licenseFeatures": [],
    "emailVerified": true,
    "passwordSet": true,
    "questionsSet": true,
    "enableAutoLogin": false,
    "disabled": false,
    "clientRegistered": false,
    "description": "",
    "createdBy": 0,
    "createdOn": "2019-09-25T16:03:05-05:00",
    "updatedBy": 0,
    "updatedOn": "2019-09-25T16:03:05-05:00",
    "publicKey": null,
    "appType": null,
    "routingName": null,
    "appUrl": null
  }
}
```


Related concepts
Authentication API

Immediately logout (expire) an authentication token

Immediately invalidate an access token so that it cannot be used for authentication.

©2020 Automation Anywhere. All rights reserved.

Prerequisites

- The URL for the Enterprise Control Room in which the token was generated
- The token that you want to expire

Procedure

1. Enter the following parameters to the request URL.
   `http://<your_control_room_url>/v1/authentication/logout`
2. In a header for this request, enter the token that is to be expired.
   Note: There are no body parameters in this request.
3. Send the request.
   - In a REST Client, click SEND.
   - In the Swagger interface, click Execute.

   Response header:
   Note: A 204 response code indicates that the request was successful and that there is no additional content to be sent to the response body.

```
Status Code: 204 No Content
cache-control: no-cache, no-store, max-age=0, must-revalidate
content-security-policy: default-src 'self'
content-type: application/json
date: Thu, 31 Oct 2019 08:37:35 GMT
expires: 0
pragma: no-cache
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
x-xss-protection: 1; mode=block
```

Related concepts
Authentication API

Create and assign API key generation role

API key generation is available in Enterprise Control Room v11.3.2 and later. By default this parameter is not enabled for any of the System-created roles. An administrator is able to create a custom role for API key generation and assign that custom role to users.

This task describes how an administrator can create and assign a custom role for API key generation.

Procedure

1. Log in as an administrator to the Enterprise Control Room.
2. Go to Administration > Roles.

©2020 Automation Anywhere. All rights reserved.

3. Click Create role.
4. Scroll to the API section.
5. Select Generate API-Key.
6. Type a unique name in the Role name field.
7. Click Create role.
8. Go to Administration > Users, and assign the custom role you just created to non-admin users.
9. Log in as the user you assigned the Generate API-Key role to.
10. Under the user name, click Generate API-Key, and copy the API-Key to your clipboard.

Next steps

Use the API-Key to log into an Enterprise Control Rooms using SSO, or use the API-Key to log in a user without the user's password.
Related concepts
Authentication API
Related tasks
Authenticate with username and apiKey

Auto Login Credentials API overview

Use the Auto Login Credentials API to automate the login process in order to remotely run bots on locked devices. Users with an AAE_Admin role can create, update, or delete the login credentials.

Overview

When a bot is deployed from the Enterprise Control Room to the Bot Runner, the bot logs in to the Bot Runner using the credentials stored in the Credential Vault. These credentials are set by the user using the Tools > Options > Login Settings of the Enterprise client. Each time a user's Windows password is modified, the user must update the new password in the Enterprise client.

To automate this process, use the following URLs to create, update, or delete the login credentials that are stored in the Credential Vault.

Create auto login credential values

```
POST http://<your_control_room_url>/v1/credentialvault/external/credentials/log
insetting
```

Body parameters: The following parameters are required.

Field	Description
`Username`	The username of the Automation Anywhere user
`Windows_Username`	The Windows username for the computer
`Windows_Password`	The Windows password for the computer

Note: If the Enterprise Control Room is configured for Active Directory, use the following request body. Replace the text in the angle brackets with your credentials.

©2020 Automation Anywhere. All rights reserved.

```
{
"Username":"<domain\\username>",
"Windows_Username":"<domain\\your username>",
"Windows_Password":"<your password>"
}
```

Example: Create auto login credentials

Update auto login credential values

```
PUT http://<your_control_room_url>/v1/credentialvault/external/credentials/logi
nsetting
```

Example: Update auto login credentials

Delete auto login credential values

```
DELETE http://<your_control_room_url>/v1/credentialvault/external/credentials/l
oginsetting
```

Example: Delete auto login credentials

Create auto login credentials

Use the Create auto login credential values API to save a new instance of login credential values to the Credential Vault for the specified Automation Anywhere user and their device.

Prerequisites

Permissions
: You must have the `AAE_Admin` role.

JSON Web Token (JWT)
: All Enterprise Control Room APIs require a JSON Web Token (JWT) to access the APIs. Generate an authentication token using the Authentication API.

Note:

- Use the Swagger definition files installed with your Enterprise Control Room to test the APIs. View the available Swagger APIs at `http://<your_control_room_url>/swagger/`.
- You can also use a REST client to complete this task.

©2020 Automation Anywhere. All rights reserved.

Procedure

1. Add an authentication token to the request header.
   Note: Use the Authentication API to generate a JSON Web Token.
2. Specify the method and URL.
   - Method: POST
   - URL: `http://<your_control_room_url>/v1/credentialvault/external/credentials/loginsetting`
3. Provide the login details in the request body.

```
{
  "Username": "<Automation_Anywhere_username>",
  "Windows_Username": "<Windows_username>",
  "Windows_Password": "<Windows_password>"
}
```

4. Send the request.
   - In a REST client, click SEND.
   - In the Swagger interface, click Execute.

   Success Response:

```
201 Successful creation of credential.
```

Note: You can also run REST requests from a command terminal. The following is a curl request example, formatted for readability.

```
curl -X POST "<your_control_room_url>/v1/credentialvault/external/credentials/l
oginsetting" -H "accept: application/json"
                -H "X-Authorization: <authentication_token>" -H "Content-Type:
application/json"
                -d "{
                \"Username\": \"string\",
                \"Windows_Username\": \"string\",
                \"Windows_Password\": \"string\"
                }"
```

Update auto login credentials

Use the Update auto login credential values API to change and save login credential values to the Credential Vault for the specified Automation Anywhere user and their device.

©2020 Automation Anywhere. All rights reserved.

Prerequisites

Permissions
: You must have the `AAE_Admin` role.

JSON Web Token (JWT)
: All Enterprise Control Room APIs require a JSON Web Token (JWT) to access the APIs. Generate an authentication token using the Authentication API.

Note:

- Use the Swagger definition files installed with your Enterprise Control Room to test the APIs. View the available Swagger APIs at `http://<your_control_room_url>/swagger/`.
- You can also use a REST client to complete this task.

Procedure

1. Add an authentication token to the request header.
   Note: Use the Authentication API to generate a JSON Web Token.
2. Specify the method and URL.
   - Method: PUT
   - URL: `http://<your_control_room_url>/v1/credentialvault/external/credentials/loginsetting`
3. Provide the login details in the request body.

```
{
  "Username": "<Automation_Anywhere_username>",
  "Windows_Username": "<Windows_username>",
  "Windows_Password": "<Windows_password>"
}
```

4. Send the request.
   - In a REST client, click SEND.
   - In the Swagger interface, click Execute.

   Success Response:

```
200 Credentials were successfully updated.
```

Note: You can also run REST requests from a command terminal. The following is a curl request example, formatted for readability.

```
curl -X PUT "<your_control_room_url>/v1/credentialvault/external/credentials/loginsetting" -H "accept: application/json"
                -H "X-Authorization: <authentication_token>" -H "Content-Type: application/json"
```

©2020 Automation Anywhere. All rights reserved.

```
-d "{
\"Username\": \"string\",
\"Windows_Username\": \"string\",
\"Windows_Password\": \"string\"
}"
```

Delete auto login credentials

Use the Delete auto login credential values API to remove login credential values from the Credential Vault for the specified Automation Anywhere user and their device.

Prerequisites

Permissions
: You must have the `AAE_Admin` role.

JSON Web Token (JWT)
: All Enterprise Control Room APIs require a JSON Web Token (JWT) to access the APIs. Generate an authentication token using the Authentication API.

Note:

- Use the Swagger definition files installed with your Enterprise Control Room to test the APIs. View the available Swagger APIs at `http://<your_control_room_url>/swagger/`.
- You can also use a REST client to complete this task.

Procedure

1. Add an authentication token to the request header.
   Note: Use the Authentication API to generate a JSON Web Token.
2. Specify the method and URL.
   - Method: DELETE
   - URL: `http://<your_control_room_url>/v1/credentialvault/external/credentials/loginsetting`

   Create auto login credentials

3. Send the request.
   - In a REST client, click SEND.
   - In the Swagger interface, click Execute.

   Success Response:

   ```
   200 Credentials were successfully deleted.
   ```

Note: You can also run REST requests from a command terminal. The following is a curl request example, formatted for readability.

©2020 Automation Anywhere. All rights reserved.

```
curl -X DELETE "<your_control_room_url>/v1/credentialvault/external/credentials
/loginsetting" -H "accept: application/json"
                -H "X-Authorization: <authentication_token>" -H "Content-Type:
application/json"
                -d "{
                \"Username\": \"string\",
                \"Windows_Username\": \"string\",
                \"Windows_Password\": \"string\"
                }"
```

Automation Management API

Use the Enterprise Control Room bot Automations API to trigger deployment of bots from an external system or a third-party application.

Automation API

To deploy bots onto the Automation Environment, currently the user has to login to Enterprise Control Room, select the bot and the Bot Runners and then 'Run/Schedule' the task.

However, as the Automation scenarios scale up, there is an increasing need to deploy/trigger bots from an external third party application.

To meet this business requirement, Automation Anywhere has published Application Programming Interfaces (APIs) using which a bot can be triggered from an external system.

A Enterprise Control Room user can use these APIs to deploy bots (Tasks) to Bot Runners on commencement of events specified by a third-party/external application.

Note: You cannot deploy Attended bots from the Enterprise Control Room. Only Unattended bots are available for deployment from the Enterprise Control Room.

Key Features and Business Benefits of Enterprise Control Room APIs

- bots can be deployed from an external third party systems using Automation Anywhere APIs.
- The input and output of APIs is JSON based (industry standard data-interchange format).
- bot Deployment can be orchestrated from an External Application / Workflow using a combination of scripts and Automation Anywhere APIs.

Note: The bot deployment API can ONLY be invoked after the system/user has authenticated using the Authentication API

Also, the user will need to have the 'Run my bots' privileges and the privileges of the Bot Runners on which the bot is to be deployed.

Deployment endpoint

©2020 Automation Anywhere. All rights reserved.

The Deployment endpoint is used to deploy bots to Bot Runners.

API: `<Enterprise Control Room URL>/v1/schedule/automations/deploy`

The user can pass three parameters as JSON string.

1. bot name with relative path – This is mandatory.
2. List of Bot Runners and users in JSON format – This is mandatory.
3. Use RDP based approach – This is optional and set to false by default.

Deployment Scenario and corresponding JSON string:

1. For example, the name of the bot is Accountsbot.atmx and the bot is under 'My Tasks'
2. The bot is to be deployed on 2 machines
   - First machine hostname BR-1 with user U-1
   - Second machine hostname BR-2 with user U-2
3. The JSON string in the above scenario will be:

```
{
  "taskRelativePath": "My Tasks\\AccountsBot.atmx",
  "botRunners":
 [
    {
      "client": "BR-1",
      "user": "U-1"
    },
    {
      "client": "BR-2",
      "user": "U-2"
    }
  ]
}
```

Response Codes

Http(s) Status code	Response - Description
200	Successful creation of automaton.
400	Bad Request
401	Authentication Required
403	Unauthorized access
409	Conflict

©2020 Automation Anywhere. All rights reserved.

500	Internal Server error

Related concepts
Authentication API

Bot Execution Orchestrator API

As a Enterprise Control Room administrator or a user with View and Manage Scheduled Activity permission, deploy bots and monitor its progress using a set of Enterprise Control Room APIs.

Request details about files, folders and bots
: Request details about bots, folders, and files by searching by names, relative paths, and ids in the Enterprise Control Room where they are stored.

Request device details
: Use this API to retrieve a list of devices that are available for bot deployment.

Deploy a bot
: Deploy a bot on one or more devices using the bots id and the ids of the BOT_RUNNER devices.

Request bot progress
: Request bot status by specifying the id for a bot.

High-level process for monitoring and deploying bots

1. `.../v2/repository/file/list`: Retrieve the unique bot identification number used to deploy a bot.
2. `.../v2/activity/list`: Generate a list of devices (Bot Runners) available for running bots, including the status of the device.
3. `.../v2/automations/deploy`: Deploy a bot on multiple devices using the unique bot and device identification numbers.
4. `.../v2/activity/list`: Monitor the bot progress based on its unique identification number.

Searchable fields for devices:

- hostName: The host name of the device configured as a Bot Runner. If a naming convention is used for host names, searching on a unique substring in the host name is an effective way to identifies Bot Runner devices.
- userId: The unique numeric identification for a specific user also identifies the Bot Runner device. Unique user naming conventions can be used to identify users and devices that are licensed and configured as Bot Runners.

Searchable fields for bots:

- name: The unique name of a bot. You can search on the exact name (eq) or a text string (substring) that is contained in the bots name.
- path: The relative path of a folder in the Enterprise Control Room. You can search on a full path or a substring contained in the path.

Related concepts
Authentication API
Filters in an API request body
Related tasks

©2020 Automation Anywhere. All rights reserved.

Request details about files, folders and bots

Request details about bots, folders, and files by searching by names, relative paths, and ids in the Enterprise Control Room where they are stored.

Prerequisites

Use the bot names, folder paths and ids to retrieve detailed information.

Roles and license

You need to authenticate as a user that has a Bot runner (Run time with TaskBots and MetaBots) license.

- URL:

```
http://<your_control_room_url>/v2/repository/file/list
```

- Method: POST

Supported filterable fields:

path

This example searches for the string Finance in the path parameter. This search is not case sensitive. It finds Finance or finance.

- Field: path
- Type: string

```
{
  "filter": {
    "operator": "substring",
    "value": "Finance",
    "field": "path"
  }
}
```

name

Retrieve all the bots with 'HR' in their name. For example, Automation Anywhere\My Tasks\Bots\HR-daily.atmx

- Field: name
- Type: string

©2020 Automation Anywhere. All rights reserved.

```
{
  "filter": {
    "operator": "substring",
    "field": "name",
    "value": "HR"
  }
}
```

directory

The value false will get all files (and not directories); if the value is true, then it will return all the directories

- Field: directory
- Type: boolean

```
{
  "filter": {
    "operator": "eq",
    "field": "directory",
    "value": "false"
  }
}
```

parentId

This will get all the bots/files with parentid as 7

- Field: parentid
- Type: long

```
{
  "filter": {
    "operator": "eq",
    "field": "parentid",
    "value": "7"
  }
}
```

lastModified

This will get all the bots/files which were last modified at that date-time

- Field: lastModified

©2020 Automation Anywhere. All rights reserved.

- Type: date-time

```
{
  "filter": {
    "operator": "gt",
    "field": "lastModified",
    "value": "2020-01-07T18:00:00Z"
  }
}
```

Use the following fields to filter the response.

name: The partial or full name of a bot. You can search on the exact name (eq) or a text string (substring) that is contained in the bots name.

The following request returns a detailed list of all the bots that are in any folder that contains `Finance` in the folder path.

Procedure

1. Add an authentication token to the request header.
   Note: Use the Authentication API to generate a JSON Web Token.
2. Enter the URL for the API `http://<your_control_room_url>/v2/repository/file/list`.
3. Select the POST method.
4. In the request body, the substring "finance" is used to search for folder paths that contain the string.

```
{
  "filter": {
    "operator": "substring",
    "field": "path",
    "value": "finance"
  }
}
```

5. Send the request.
   - In a REST client, click SEND.
   - In the Swagger interface, click Execute.

   Response body:

   The id in the response below is the unique identifier for the bot. In this response there are two bots listed.

```
{
  "page": {
    "offset": 0,
    "total": 4,
    "totalFilter": 1
  },
  "list": [
    {
      "id": "12",
      "parentid": "11",
      "name": "FinanceHelloWorldGBG.atmx",
      "permission": {
        "delete": false,
        "download": true,
        "execute": false,
        "upload": true,
        "run": false
      },
      "lastModified": "2020-01-08T22:24:08.060Z",
      "lastModifiedBy": "10",
      "path": "Automation Anywhere\\My Tasks\\Finance\\FinanceHelloWorldGB
G.atmx",
      "directory": false,
      "size": 4578,
      "locked": false,
      "fileLastModified": "2020-01-08T22:21:58Z",
      "isProtected": false
    }
  ]
}
```


Next steps

To deploy a specific bot, use the numeric id of the bot. Here are some additional requests for retrieving detailed bot information.

©2020 Automation Anywhere. All rights reserved.

Request device details

Use this API to retrieve a list of devices that are available for bot deployment.

Prerequisites

Roles and license

You need to authenticate as a user with an Unattended bot runner license.

- URL:

```
http://<your_control_room_url>/v2/devices/list
```

- Method: POST

Supported filterable parameters:

id
: The numeric identifier for a device.

  - Field: id
  - Type: integer

```
{
  "filter": {
    "operator": "eq",
    "value": "7",
    "field": "id"
  }
}
```

hostName
: The name of the registered device.

  - Field: hostName
  - Type: string

```
{
  "filter": {
    "operator": "substring",
    "value": "AA",
    "field": "hostName"
```

©2020 Automation Anywhere. All rights reserved.

```
  }
}
```

userId
: A unique numeric identifier for the user associated with the registered device.

- Field: userId
- Type: long

```
{
  "filter": {
    "operator": "eq",
    "value": "13",
    "field": "userId"
  }
}
```

This task requests a list of all devices with a specific string in the name parameter and modified after a specific date. Use the list in the response to identify which devices are connected and available to run bots. All the devices in the list are registered Bot Runners.

Procedure

1. Add an authentication token to the request header.
   Note: Use the Authentication API to generate a JSON Web Token.
2. Select the POST method.
3. Enter the URL for the API `http://<your_control_room_url>/v2/devices/list`.
4. Enter a request filter to limit the number of registered devices listed in the response. By wrapping filters in the logical operator "and," you can build a detailed filter.

```
{
  "filter": {
    "operator": "and",
    "operands": [
      {
        "operator": "ne",
        "value": "7",
        "field": "id"
      },
      {
        "operator": "substring",
```

```
        "value": "ec",
        "field": "hostName"
      }
    ]
  }
}
```

5. Send the request.
   - In a REST client, click SEND.
   - In the Swagger interface, click Execute.

   Response body:

   The response includes 2 registered devices out of 8 that meet the filter criteria.

```
{
  "page": {
    "offset": 0,
    "total": 8,
    "totalFilter": 2
  },
  "list": [
    {
      "id": "1",
      "type": "BOT_CREATOR",
      "hostName": "EC2AMAZ-R8AC9KV",
      "userId": "2",
      "userName": "docbotcreator",
      "status": "DISCONNECTED",
      "poolName": "",
      "fullyQualifiedHostName": "EC2AMAZ-R8AC9KV"
    },
    {
      "id": "14",
      "type": "BOT_RUNNER",
      "hostName": "EC2AMAZ-R8AC9KV",
      "userId": "3",
      "userName": "docbotrunner",
      "status": "DISCONNECTED",
```

©2020 Automation Anywhere. All rights reserved.

```
      "poolName": "Finance Test Device Pool",
      "fullyQualifiedHostName": "EC2AMAZ-R8AC9KV"
    }
  ]
}
```

Next steps

Note the ids for devices with type of BOT_RUNNER and status of CONNECTED. Write down the device's id. The device id and bot id are used to deploy bots on Bot Runners.

Deploy a bot

Deploy a bot on one or more devices using the bots id and the ids of the BOT_RUNNER devices.

Prerequisites

Make sure that your Enterprise Control Room Deployment settings are enabled and there are Callback URLs listed. See, Callback URLs for bot deployment.

You need to identify the bot ids to be deployed and the device ids to deploy them to.

- Request details about files, folders and bots: Request details about bots, folders, and files by searching by names, relative paths, and ids in the Enterprise Control Room where they are stored.
- Request device details: Use this API to retrieve a list of devices that are available for bot deployment.

Roles and license

You need to authenticate as a user that has an Unattended bot runner license.

- URL: `http://<your_control_room_url>/v2/automations/deploy`
- Method: POST

Procedure

1. Add an authentication token to the request header.
   Note: Use the Authentication API to generate a JSON Web Token.
2. Enter the URL for the API `http://<your_control_room_url>/v2/automations/deploy`.
3. Select the POST method.
4. Enter the following parameters in the request body.

```
{
  "fileId": "12",
  "deviceIds": [
    "6",
```

```
    "7"
  ]
}
```

- fileId: The unique identifier for the bot.
- deviceIds: The unique identifiers of the device on which the bot is run.

Note: You can have only on fileId in the rquest, but you can have multipledeviceIds.

Response body:

A successful response returns the unique indentifier for the automation.

```
{
  "automationId": "8"
}
```

Related tasks
Request bot progress

Callback URLs for bot deployment

As an administrator, you can configure the Enterprise Control Room Deployment settings with known callback URLs.

Prerequisites

- Log in as an Admin user to view or configure Deployment settings.
- Identify a known callback URL.
- Role: AAE_Admin

Procedure

1. Navigate to ADMINISTRATION > Settings > General > CONTROL ROOM DATABASE & SOFTWARE. Find the Deployment settings section. Check whether Deployment settings are enabled and that there is at least on Callback URL.
2. To add or update Deployment settings, click the Edit icon for the Configuration settings page.
3. On the CONTROL ROOM DATEBASE & SOFTWARE tab, scroll to the Deployment settings section.
4. Enable Bot Runner deployment session on Control Room and add a known Callback URL.
   Note: The parent Callback URL must be white listed. You can append additional URL path parameters to a parent URL allowing you to have variable paths appended to the parent Callback URL.
   Example:
   - The white listed parent URL.

     ```
     https://<your_control_room_url>/dashboard
     ```

   - Additional appended callback path is valid because parent URL is white listed.

`https://<your_control_room_url>/dashboard/Finance`

5. Click Save changes.

Related tasks
Deploy a bot

Request bot progress

Request bot status by specifying the id for a bot.

Prerequisites

Bot id
The id of a specific bot to track its progress.
Roles and license

You need to authenticate as a user with an Unattended bot runner license.

Use this API to track the progress of a specific bot.

- URL: `http://<your_control_room_url>/v2/activity/list`
- Method: POST

Note:

- You can get a list of bot ids by using the Request details about files, folders and bots API.
- 11.3.4 outputVariables: A variable must be included as output before it can be returned in the API response.

Procedure

1. Add an authentication token to the request header.
   Note: Use the Authentication API to generate a JSON Web Token.
2. Enter the URL for the API `http://<your_control_room_url>/v2/activity/list`.
3. Select the POST method.
4. Enter the following parameters in the request body.

```
{
  "filter": {
    "operator": "and",
    "operands": [
      {
  "operator": "eq",
  "value": "6",
  "field": "deviceId"
  },
```

```
  {
  "operator": "eq",
  "value": "14",
  "field": "fileId"
  }
]
}
}
```

This request filters for all the activity for the bot with the fielld of 14 on the device with the deviceId of 6.

5. Send the request.
   - In a REST client, click SEND.
   - In the Swagger interface, click Execute.

   Response body:

```
{
  "page": {
    "offset": 0,
    "total": 33,
    "totalFilter": 3
  },
  "list": [
    {
      "id": "99f692c6-9ae4-4adb-8d27-0cd5b1b88de8",
      "automationName": "testHelloWorld_19.11.25.18.29.02_docs-admin_API",
      "fileName": "testHelloWorld.atmx",
      "filePath": "Automation Anywhere\\My Tasks\\testHelloWorld.atmx",
      "type": "TASK",
      "startDateTime": "2019-11-25T18:29:05Z",
      "endDateTime": "2019-11-25T18:29:21Z",
      "command": "Message Box",
      "status": "COMPLETED",
      "progress": 100,
      "automationId": "13",
      "userId": "21",
      "deviceId": "6",
      "currentLine": 1,
      "totalLines": 1,
```

©2020 Automation Anywhere. All rights reserved.

```
      "fileId": "14",
      "modifiedBy": "4",
      "createdBy": "4",
      "modifiedOn": "2019-11-25T18:29:21.637Z",
      "createdOn": "2019-11-25T18:29:02.541Z",
      "deploymentId": "93457151-7edd-4454-9dfd-35a3f1d96f25",
      "queueName": "",
      "queueId": "",
      "usingRdp": false,
      "message": "",
      "canManage": true,
      "deviceName": "AA-SJ-TerryMartin.AAI.AASPL-BRD.COM",
      "userName": "docs-bot",
      "isMigrated": false,
      "jobUniqueId": "99f692c6-9ae4-4adb-8d27-0cd5b1b88de8",
      "outputVariables": {
        "vMyHelloWorld": {
          "string": "Hello world from a variable"
        }
      }
    },
    {
      "id": "12e24bb7-7e37-4693-8e74-144ac3e6f566",
      "automationName": "testHelloWorld_19.11.25.18.30.33_docs-admin_API",
      "fileName": "testHelloWorld.atmx",
      "filePath": "Automation Anywhere\\My Tasks\\testHelloWorld.atmx",
      "type": "TASK",
      "startDateTime": "2019-11-25T18:30:36Z",
      "endDateTime": "2019-11-25T18:30:42Z",
      "command": "Message Box",
      "status": "COMPLETED",
      "progress": 100,
      "automationId": "14",
      "userId": "21",
      "deviceId": "6",
      "currentLine": 1,
```

```
      "totalLines": 1,
      "fileId": "14",
      "modifiedBy": "4",
      "createdBy": "4",
      "modifiedOn": "2019-11-25T18:30:42.260Z",
      "createdOn": "2019-11-25T18:30:33.615Z",
      "deploymentId": "137ed5b1-f573-4757-b890-fc93088e0c5f",
      "queueName": "",
      "queueId": "",
      "usingRdp": false,
      "message": "",
      "canManage": true,
      "deviceName": "AA-SJ-TerryMartin.AAI.AASPL-BRD.COM",
      "userName": "docs-bot",
      "isMigrated": false,
      "jobUniqueId": "12e24bb7-7e37-4693-8e74-144ac3e6f566",
      "outputVariables": {
        "vMyHelloWorld": {
          "string": "Hello world from a variable"
        }
      }
    },
    {
      "id": "9728beaf-6653-46a9-b053-b386b8333199",
      "automationName": "testHelloWorld_19.12.02.17.42.37_docs-admin_API",
      "fileName": "testHelloWorld.atmx",
      "filePath": "Automation Anywhere\\My Tasks\\testHelloWorld.atmx",
      "type": "TASK",
      "startDateTime": "2019-12-02T17:42:40Z",
      "endDateTime": "2019-12-02T17:42:44Z",
      "command": "Message Box",
      "status": "COMPLETED",
      "progress": 100,
      "automationId": "17",
      "userId": "21",
      "deviceId": "6",
```


©2020 Automation Anywhere. All rights reserved.

```
      "currentLine": 1,
      "totalLines": 1,
      "fileId": "14",
      "modifiedBy": "4",
      "createdBy": "4",
      "modifiedOn": "2019-12-02T17:42:45.072Z",
      "createdOn": "2019-12-02T17:42:37.591Z",
      "deploymentId": "ba70ed50-2a28-477b-9557-32283f5bba27",
      "queueName": "",
      "queueId": "",
      "usingRdp": false,
      "message": "",
      "canManage": true,
      "deviceName": "AA-SJ-TerryMartin.AAI.AASPL-BRD.COM",
      "userName": "docs-bot",
      "isMigrated": false,
      "jobUniqueId": "9728beaf-6653-46a9-b053-b386b8333199",
      "outputVariables": {
        "vMyHelloWorld": {
          "string": "Hello world from a variable"
        }
      }
    }
  ]
}
```


Related tasks
Create new variables

APIs to manage credential vault

As an Enterprise Control Room user with Manage my credentials and lockers role permissions, use the Credential Vault API to manage your attributes, credentials, keys, lockers, and Credential Vault mode in the Enterprise Control Room.

- Manage credentials
  Use the Credential Vault API to create, delete, search for, and update credentials.
- Manage credentials attributes
  Use the Credential Vault API to create, update, and delete attribute values.

©2020 Automation Anywhere. All rights reserved.

- Manage Credential Vault mode
  Use the Credential Vault API to manage the Credentail Vault mode. As a user with the `AAE_Admin` role, you can retrieve the mode or configure it after restarting the Enterprise Control Room.
- Manage keys
  As a user with the `AAE_Admin` role, you can use the Credential Vault API to generate, save, check the status of, and apply keys.
- Manage lockers
  Use the Credential Vault API to manage lockers, consumers, members, and credentials in the lockers.

Manage credentials

Use the Credential Vault API to create, delete, search for, and update credentials.

Permissions

By default, all users can create credentials. You are the Credential owner of any credentials that you created. As a Credential owner, you can update, delete, and transfer the ownership of your credentials.

Credential URLS

Create credential

Creates a new credential and configures one or more attributes.

```
POST http://<your_control_room_url>/v2/credentialvault/credentials
```

Body parameters:

Field	Required	Description
`name`	Required	New credential name; 50 characters maximum and cannot contain special characters
`description`	Optional	New credential description; 255 characters maximum
`attributes`		
`name`	Required	New attribute name; 50 characters maximum and cannot contain special characters
`description`	Optional	New attribute description; 255 characters maximum
`userProvided`	Required	Configures the input type with the following options: • If `userProvided: true`, the value is not preset during creation. Only consumers of the locker containing this credential can provide the value.

©2020 Automation Anywhere. All rights reserved.

Field	Required	Description
		• If `userProvided: false`, the credential owner enters the value. All consumers see the same attribute value set by the credential owner.
`masked`	Optional	Configures whether to mask the value. If `masked: false`, the value returns as an empty string when called.
`passwordFlag`	Optional	Flags the value as a password, which limits its use only to password-type fields. This ensures the value is not printed to plain text application. Commands that support Credential Variables

Response: This response contains information on the credential and its attributes.

```
{
  "id": "string",
  "name": "string",
  "description": "string",
  "lockerId": "string",
  "ownerId": "string",
  "attributes": [
    {
      "id": "string",
      "name": "string",
      "description": "string",
      "userProvided": true,
      "masked": true,
      "passwordFlag": true,
      "createdBy": "string",
      "createdOn": "string",
      "updatedBy": "string",
      "updatedOn": "string",
      "version": "string"
    }
  ],
  "createdBy": "string",
  "createdOn": "string",
```

©2020 Automation Anywhere. All rights reserved.

```
  "updatedBy": "string",
  "updatedOn": "string",
  "version": "string"
}
```

Create a new credential.
After you have created a credential, to add a standard value see Create a new value to a credential attribute.

Search for credentials

```
POST http://<your_control_room_url>/v2/credentialvault/credentials/list
```

Query parameter:

Field	Required	Description
consumed	Optional	Filters the returned values to only the credentials that being consumed by the current user.

Body parameters: This request body example includes filters, sorting, and page control to refine the response.

```
{
  "filter": {
    "operator": "NONE",
    "operands": [
      null
    ],
    "field": "string",
    "value": "string"
  },
  "sort": [
    {
      "field": "string",
      "direction": "asc"
    }
  ],
  "page": {
    "offset": 0,
    "length": 0
```

©2020 Automation Anywhere. All rights reserved.

```
  }
}
```

Filters allow you to refine what is returned in the response body. Read more about filters in Filters in an API request body.

Search for credentials using filters

Get credential by id

```
GET http://<your_control_room_url>/v2/credentialvault/credentials/{id}
```

Path parameter:

Field	Required	Description
`id`	Required	Identifies the credential

Response: This response contains information on the credential and its attributes.

```
{
  "id": "string",
  "name": "string",
  "description": "string",
  "lockerId": "string",
  "ownerId": "string",
  "attributes": [
    {
      "id": "string",
      "name": "string",
      "description": "string",
      "userProvided": true,
      "masked": true,
      "passwordFlag": true,
      "createdBy": "string",
      "createdOn": "string",
      "updatedBy": "string",
      "updatedOn": "string",
      "version": "string"
    }
  ],
  "createdBy": "string",
```

©2020 Automation Anywhere. All rights reserved.

```
  "createdOn": "string",
  "updatedBy": "string",
  "updatedOn": "string",
  "version": "string"
}
```

Update credential properties

As a credential owner, you can change the credential name or description, attribute name or description, input type, value masking, or password flagging.

Note: You cannot update a credential that is already assigned to a locker. You cannot change the credential id, credential owner, attribute value, or locker assignment with this API. Use the following APIs instead:

- Manage credentials attributes
- Manage lockers
- Update credential owner

```
PUT http://<your_control_room_url>/v2/credentialvault/credentials/{id}
```

Path parameter:

Field	Required	Description
`id`	Required	Identifies the credential

Body parameters:

Field	Required	Description
`name`	Required	New credential name; 50 characters maximum and cannot contain special characters
`description`	Optional	New credential description; 255 characters maximum
`attributes`		
`name`	Required	New attribute name; 50 characters maximum and cannot contain special characters
`description`	Optional	New attribute description; 255 characters maximum
`userProvided`	Required	Configures the input type with the following options: • If `userProvided: true`, the value is not preset during creation. Only consumers of the locker containing this credential can provide the value. • If `userProvided: false`, the credential owner enters the value. All

©2020 Automation Anywhere. All rights reserved.

Field	Required	Description
		consumers see the same attribute value set by the credential owner.
`masked`	Optional	Configures whether to mask the value. If `masked: false`, the value returns as an empty string when called.
`passwordFlag`	Optional	Flags the value as a password, which limits its use only to password-type fields. This ensures the value is not printed to plain text application. Commands that support Credential Variables

Response: This response contains information on the credential and its attributes.

```
{
  "id": "string",
  "name": "string",
  "description": "string",
  "lockerId": "string",
  "ownerId": "string",
  "attributes": [
    {
      "id": "string",
      "name": "string",
      "description": "string",
      "userProvided": true,
      "masked": true,
      "passwordFlag": true,
      "createdBy": "string",
      "createdOn": "string",
      "updatedBy": "string",
      "updatedOn": "string",
      "version": "string"
    }
  ],
  "createdBy": "string",
  "createdOn": "string",
  "updatedBy": "string",
```

©2020 Automation Anywhere. All rights reserved.

```
  "updatedOn": "string",
  "version": "string"
}
```

Update a credential.

Delete credential

```
DELETE http://<your_control_room_url>/v2/credentialvault/credentials/{id}
```

Path parameter:

Field	Required	Description
`id`	Required	Identifies the credential

Response:

```
Successful delete
```

Update credential owner

You can transfer any of your credentials to a new owner. If the credential is assigned to a locker, you can transfer the ownership to one of the locker members. If the credential is not assigned to a locker, you can transfer the ownership to any other user in the system. Users with the `AAE_Locker` role can update the credential owners for any credential in the system.

```
PUT http://<your_control_room_url>/v2/credentialvault/credentials/{id}/own
er/{credentialOwnerId}
```

URL parameter:

Field	Required	Description
`id`	Required	Identifies the credential
`credentialOwnerId`	Required	Specifies the new owner

Response:

```
Successful update of credential ownership
```

Create a new credential

Send a POST request to create a new credential.

©2020 Automation Anywhere. All rights reserved.

Prerequisites

JSON Web Token (JWT)

All Enterprise Control Room APIs require a JSON Web Token (JWT) to access the APIs. Generate an authentication token using the Authentication API.

Note:

- Use the Swagger definition files installed with your Enterprise Control Room to test the APIs. View the available Swagger APIs at `http://<your_control_room_url>/swagger/`.
- You can also use a REST client to complete this task.

Procedure

1. Add an authentication token to the request header.
   Note: Use the Authentication API to generate a JSON Web Token.
2. Specify the method and URL.
   - Method: POST
   - URL: `http://<your_control_room_url>/v2/credentialvault/credentials`
3. Add values to configure the credential.
   The example request includes the following options:
   - Credential name is Email.
   - Credential description (optional) is Used for email login and password.
   - Attribute name is Password.
   - The value is user-provided.

     Once this credential is saved to locker, the locker consumers will receive an email notification to provide the attribute value.

   - The value is masked. When called, the value returns as an empty string.
   - The value is flagged as a password.

     An attribute with this option selected will only be available for use in password-type fields. This ensures the attribute is not exposed and its value cannot be printed to a notepad or any other 'plain text' application. For more information, see Commands that support Credential Variables.

   Request body:

```
{
  "name": "Email",
  "description": "Used for email login and password",
  "attributes": [
    {
      "name": "Password",
      "userProvided": true,
      "masked": true,
      "passwordFlag": true
```

©2020 Automation Anywhere. All rights reserved.

```
    }
  ]
}
```

4. Send the request.
   - In a REST Client, click SEND.
   - In the Swagger interface, click Execute.

   The response for this example returns information on the new credential. The example response includes the following information:
   - Credential id is 17.
   - Owner id is 14.
   - Attribute id is 70.

   Response body:

```
{
"id": "17",
"name": "Email",
"description": "Used for email login and password",
"ownerId": "14",
"attributes":[
    {
        "id": "70",
        "name": "Password",
        "description": "",
        "userProvided": true,
        "masked": true,
        "createdBy": "14",
        "createdOn": "2019-12-23T19:01:13.449Z",
        "updatedBy": "14",
        "updatedOn": "2019-12-23T19:01:13.449Z",
        "version": "0",
        "passwordFlag": true
    }
],
"createdBy": "14",
"createdOn": "2019-12-23T17:42:43.802Z",
"updatedBy": "14",
"updatedOn": "2019-12-23T17:42:43.802Z",
```

©2020 Automation Anywhere. All rights reserved.

```
"version": "0"
}
```

Note: You can also run REST requests from a command terminal. The following is a curl request example. This example is formatted for readability. Replace the text inside the angle brackets, `<authentication_token>`, with your authentication token.

```
curl -X POST "<your_control_room_url>/v2/credentialvault/credentials" -H "accep
t: application/json"
        -H "X-Authorization: <authentication_token>" -H "Content-Type: applicat
ion/json"
        -d "{
             \"name\": \"Email\",
             \"description\": \"Used for email login and password\",
             \"attributes\":
              [
                { \"name\": \"Password\",
                  \"userProvided\": true,
                  \"masked\": true,
                  \"passwordFlag\": true }
               ]
            }"
```

Search for credentials using filters

Send a POST request with filters to return a list of credentials that belong to a particular locker.

Prerequisites

JSON Web Token (JWT)
: All Enterprise Control Room APIs require a JSON Web Token (JWT) to access the APIs. Generate an authentication token using the Authentication API.

Note:

- Use the Swagger definition files installed with your Enterprise Control Room to test the APIs. View the available Swagger APIs at `http://<your_control_room_url>/swagger/`.
- You can also use a REST client to complete this task.

Procedure

1. Add an authentication token to the request header.
   Note: Use the Authentication API to generate a JSON Web Token.
2. Specify the method and URL.
   - Method: POST
   - URL: `http://<your_control_room_url>/v2/credentialvault/credentials/list`
3. Optional: Add the query parameter to only return the credentials that were configured as userProvided and you have used.
   `http://<your_control_room_url>/v2/credentialvault/credentials/list?consumed=true`
4. Add filter parameters to the request body.
   The example request body contains the following parameters:
   - Searches for a locker with the Id of 2.
   - Sorts the results by credential Id.

   Request body:

```
{
  "fields": [],
  "filter": {
    "field": "lockerId",
    "value": "2"
  },
  "sort": [
    {
      "field": "id",
      "direction": "asc"
    }
  ],
  "page": {
    "offset": 0,
    "length": 0
  }
}
```

5. Send the request.
   - In a REST Client, click SEND.
   - In the Swagger interface, click Execute.

   Response body: The response for this example returns information on the three credentials that are assigned to locker 2.

©2020 Automation Anywhere. All rights reserved.

```
{
  "page": {
    "offset": 0,
    "total": 2,
    "totalFilter": 2
  },
  "list": [
    {
      "id": "17",
      "name": "Database connection parameters",
      "description": "",
      "lockerId": "2",
      "ownerId": "14",
      "attributes": [
        {
          "id": "67",
          "name": "username",
          "description": "",
          "userProvided": true,
          "masked": false,
          "createdBy": "14",
          "createdOn": "2019-12-23T17:42:43.802Z",
          "updatedBy": "14",
          "updatedOn": "2020-01-24T21:40:56.048Z",
          "version": "3",
          "passwordFlag": false
        },
        {
          "id": "75",
          "name": "password",
          "description": "",
          "userProvided": true,
          "masked": false,
          "createdBy": "14",
          "createdOn": "2020-01-24T21:40:56.048Z",
          "updatedBy": "14",
```

```
          "updatedOn": "2020-01-24T21:40:56.048Z",
          "version": "0",
          "passwordFlag": false
        }
      ],
      "createdBy": "14",
      "createdOn": "2019-12-23T17:42:43.802Z",
      "updatedBy": "14",
      "updatedOn": "2020-01-27T18:08:39.416Z",
      "version": "4",
      "completed": false
    },
    {
      "id": "21",
      "name": "Email connection credentials",
      "description": "",
      "lockerId": "2",
      "ownerId": "14",
      "attributes": [
        {
          "id": "71",
          "name": "gmail password",
          "description": "",
          "userProvided": true,
          "masked": false,
          "createdBy": "14",
          "createdOn": "2020-01-24T18:18:44.132Z",
          "updatedBy": "14",
          "updatedOn": "2020-01-24T20:01:34.465Z",
          "version": "2",
          "passwordFlag": true
        }
      ],
      "createdBy": "14",
      "createdOn": "2020-01-24T18:18:44.132Z",
      "updatedBy": "14",
```

```
      "updatedOn": "2020-01-27T18:08:39.418Z",
      "version": "3",
      "completed": false
    }
  ]
}
```

Note: You can also run REST requests from a command terminal. The following is a curl request example. This example is formatted for readability. Replace the text inside the angle brackets, `<authentication_token>`, with your authentication token.

```
curl -X POST "<your_control_room_url>/v1/repository/filefolder/list" -H "accept
: application/json"
        -H "X-Authorization: <authentication_token>" -H "Content-Type: applicat
ion/json"
        -d "{
            \"fields\": [],
            \"filter\": {
                 \"field\": \"lockerId\",
                 \"value\": \"2\"
                 },
            \"sort\": [ {
                \"field\": \"id\",
                \"direction\": \"asc\"
                } ],
            \"page\": {
                \"offset\": 0,
                \"length\": 0
            }}"
```

Update a credential

Send a PUT request to update the credential name or description, attribute name or description, input type, value masking, or password flagging.

Prerequisites

JSON Web Token (JWT)
: All Enterprise Control Room APIs require a JSON Web Token (JWT) to access the APIs. Generate an authentication token using the Authentication API.

Permissions
: You must be the owner of a credential to update credential properties.

Note:

- Use the Swagger definition files installed with your Enterprise Control Room to test the APIs. View the available Swagger APIs at `http://<your_control_room_url>/swagger/`.
- You can also use a REST client to complete this task.

Procedure

1. Add an authentication token to the request header.
   Note: Use the Authentication API to generate a JSON Web Token.
2. Specify the method and URL.
   - Method: PUT
   - URL: `http://<your_control_room_url>/v2/credentialvault/credentials/{id}`
3. Add the fields and values to update.
   Request body:

```
{
"name": "Email connection parameters",
  "description": "",
  "ownerId": "14",
  "attributes": [
    {
      "id": "61",
      "name": "outlook password",
      "description": "",
      "userProvided": true,
      "masked": false,
      "createdBy": "14",
      "createdOn": "2020-01-27T19:07:12.363Z",
      "updatedBy": "14",
      "updatedOn": "2020-01-27T19:07:12.363Z",
      "version": "2",
      "passwordFlag": true
    }
  ],
```

©2020 Automation Anywhere. All rights reserved.

```
  "createdBy": "14",
  "createdOn": "2019-12-19T21:35:45.326Z",
  "updatedBy": "14",
  "updatedOn": "2020-01-27T19:07:12.364Z",
  "version": "4"
}
```


4. Send the request.
   - In a REST Client, click SEND.
   - In the Swagger interface, click Execute.

   The response for this example returns information on the new credential. The example response confirms the updated fields. It also contains the date and time of the update and the version. Each time the credential is updated, the version value increments by one.

   Response body:


```
{
  "id": "12",
  "name": "Email connection parameters",
  "description": "",
  "ownerId": "14",
  "attributes": [
    {
      "id": "61",
      "name": "outlook password",
      "description": "",
      "userProvided": true,
      "masked": false,
      "createdBy": "14",
      "createdOn": "2020-01-27T19:09:19.560Z",
      "updatedBy": "14",
      "updatedOn": "2020-01-27T19:09:19.560Z",
      "version": "3",
      "passwordFlag": true
    }
  ],
  "createdBy": "14",
  "createdOn": "2019-12-19T21:35:45.326Z",
  "updatedBy": "14",
```

```
  "updatedOn": "2020-01-27T19:09:19.560Z",
  "version": "5"
}
```

You can also run REST requests from a command terminal. Here is a Curl example of the request. This example is formatted for readability. Replace text inside the angel brackets with the appropriate values.

```
curl -X POST "<your_control_room_url>/v2/credentialvault/credentials"
                -H "accept: application/json" -H "X-Authorization: <authenticat
ion_token>"
                -H "Content-Type: application/json" -d "{ \"id\": \"<credential
_id>\",
                \"name\": \"<credential_name>\", \"description\": \"<credential
_description>\",
                \"ownerId\": \"<owner_id>\", \"attributes\": [], \"createdBy\"
: \"<user_id>\",
                \"createdOn\": \"<date_time>\", \"updatedBy\": \"<user_id>\",
                \"updatedOn\": \"<date_time>\", \"version\": \"<version_number>
\"}"
```

Manage credentials attributes

Use the Credential Vault API to create, update, and delete attribute values.

Permissions

By default, all users can create attributes with user-provided values. With additional permissions, a user can create attributes with standard values. See the BOTS section of Feature permissions for a role.

Credential attribute URLS

Retrieve all attributes of a specific credential

This URL returns the values of attributes that are configured as `"masked": false`.

```
GET http://<your_control_room_url>/v2/credentials/{id}/attributevalues
```

Path parameter:

Field	Required	Description
`id`	Required	Identifies the credential

©2020 Automation Anywhere. All rights reserved.

Query parameters:
Note: Query parameters can be used only by users with special permissions. See RBAC for Credential Vault credentials management.

Field	Required	Description
`credentialAttributeId`	Optional	Identifies the credential attribute
`userId`	Optional	Identifies the user; skip this field for credentials that are standard input.
`encryptionKey`	Optional	The RSA public key used to encrypt the value. See Retrieve RSA Public key encoded with Base64..

Response: The response lists all the attributes in the specified credential.

```
{
  "list": [
    {
      "id": "string",
      "credentialAttributeId": "string",
      "value": "string",
      "userId": "string",
      "createdBy": "string",
      "createdOn": "string",
      "updatedBy": "string",
      "updatedOn": "string",
      "version": "string"
    }
  ]
}
```

Create a new attribute value for a specific credential

Assign a value to an attribute for an existing credential. Use this URL after you have created a credential. See Create a new credential.
Note: You must either be a credential owner to provide a value for a standard credential, or have access to a credential through a locker.

```
POST http://<your_control_room_url>/v2/credentials/{id}/attributevalues
```

Path parameter:

©2020 Automation Anywhere. All rights reserved.

Field	Required	Description
`id`	Required	Identifies the credential

Query parameter:

Field	Required	Description
`encryptionKey`	Optional	The RSA public key used to encrypt the value. See Retrieve RSA Public key encoded with Base64..

Body parameters:

Field	Required	Description
`credentialAttributeId`	Required	Identifies the attribute
`value`	Required	Provides the standard input for the attribute

See Create a new value to a credential attribute.

Update credential attribute value of specific credential

```
PUT http://<your_control_room_url>/v2/credentials/{id}/attributevalues/{at
tributeValueId}
```

Path parameters:

Field	Required	Description
`id`	Required	Identifies the credential
`attributeValueId`	Required	Identifies the attribute

Body parameters:

Field	Required	Description
`value`	Required	Provides the standard input for the attribute
`version`	Optional	Provides the version number

Query parameter:

Field	Required	Description
`encryptionKey`	Optional	The RSA public key used to encrypt the value. See Retrieve RSA Public key encoded with Base64..

©2020 Automation Anywhere. All rights reserved.

Delete credential attribute value of specific credential

```
DELETE http://<your_control_room_url>/v2/credentials/{id}/attributevalues/
{attributeValueId}
```

Path parameters:

Field	Required	Description
`id`	Required	Identifies the credential
`attributeValueId`	Required	Identifies the attribute

Response:

```
Successful delete
```

Create a new value to a credential attribute

Send a POST request to assign a new value to an attribute for a specific credential.

Prerequisites

JSON Web Token (JWT)
: All Enterprise Control Room APIs require a JSON Web Token (JWT) to access the APIs. Generate an authentication token using the Authentication API.

Credential and attribute id
: Retrieve the credential and attribute ids from the credential that you created in Create a new credential. Use the ids to access and assign a value to the attribute.

Note:

- Use the Swagger definition files installed with your Enterprise Control Room to test the APIs. View the available Swagger APIs at `http://<your_control_room_url>/swagger/`.
- You can also use a REST client to complete this task.

Procedure

1. Add an authentication token to the request header.
   Note: Use the Authentication API to generate a JSON Web Token.
2. Specify the method and URL containing the credential id.
   - Method: POST
   - URL: `http://<your_control_room_url>/v2/credentialvault/credentials/17/attributevalues`
3. Provide attribute id and new value in the request body.
   Request body:

```
[
  {
    "credentialAttributeId": 84,
    "value": "john_smith"
  }
]
```

4. Send the request.
   - In a REST Client, click SEND.
   - In the Swagger interface, click Execute.

   The response for this example returns information on the new credential.

   Response body:

```
{
  "list": [
    {
      "id": "15",
      "credentialAttributeId": "84",
      "value": "Oy0hyrDwMeWF2dXLe00deQ==",
      "createdBy": "14",
      "createdOn": "2020-04-06T21:02:25.723Z",
      "updatedBy": "14",
      "updatedOn": "2020-04-06T21:02:25.723Z",
      "version": "0",
      "credentialAttribute": {
        "id": "84",
        "name": "password",
        "description": "",
        "userProvided": false,
        "masked": true,
        "createdBy": "14",
        "createdOn": "2020-04-06T21:00:40.476Z",
        "updatedBy": "14",
        "updatedOn": "2020-04-06T21:00:40.476Z",
        "version": "0",
        "passwordFlag": false
      }
```

©2020 Automation Anywhere. All rights reserved.

```
      }
    ]
  }
```

You can also run REST requests from a command terminal. Here is a Curl example of the request. This example is formatted for readability. Replace text inside the angle brackets with the appropriate values.

```
curl -X POST "<your_control_room_url>/v2/credentialvault/credentials"
                -H "accept: application/json" -H "X-Authorization: <authenticat
ion_token>"
                -H "Content-Type: application/json" -d
                {
                  "name": "name",
                  "description": "<credential_description>",
                  "attributes": [
                    {
                      "name": "<attribute_name>",
                      "userProvided": "<true_or_false>",
                      "masked": "<true_or_false>",
                      "passwordFlag": "<true_or_false>"
                    }
                  ]
                }
```

Manage Credential Vault mode

Use the Credential Vault API to manage the Credentail Vault mode. As a user with the `AAE_Admin` role, you can retrieve the mode or configure it after restarting the Enterprise Control Room.

Retrieve current Credential Vault mode

```
GET http://<your_control_room_url>/v2/credentialvault/mode
```

Response: The possible values are Express or Custom.

©2020 Automation Anywhere. All rights reserved.

```
{
  "name": "Express/Custom"
}
```

Update Credential Vault mode after Enterprise Control Room restart

`PUT http://<your_control_room_url>/v2/credentialvault/mode`

Body parameters: This request body example includes a field to update the Credential Vault mode and a field to provide the Private key if the connection mode is currently set to manual.

Field	Required	Description
`name`	Required	Updates the mode. Possible values: Express or Custom
`privateKey`	Required if current mode is custom	Unlocks the Credential Vault using the private key that was generated after Enterprise Control Room installation. See Generate Private/Public key pair

Response:

```
204 Mode has been successfully set
```

Manage keys

As a user with the `AAE_Admin` role, you can use the Credential Vault API to generate, save, check the status of, and apply keys.

Generate a Public/Private key pair after a fresh Enterprise Control Room installation

This URL can only be used after a fresh installation. After generating the key pair, use the following URL to save the keys. Once the keys are saved, no more keys can be generated for this Enterprise Control Room.

```
POST http://<your_control_room_url>/v2/credentialvault/keys
```

Response:

```
{
  "privateKey": "string",
```

©2020 Automation Anywhere. All rights reserved.

```
  "publicKey": "string"
}
```

Save a Public/Private key pair and mode after a Public/Private key pair is generated

Use the URL above to generate a Public/Private key pair, then use this endpoint to save the key pair. This URL generates a Data encryption key and opens the Credential Vault.
Note: New keys cannot be generated after a key pair is saved.

```
PUT http://<your_control_room_url>/v2/credentialvault/keys
```

Body parameters:

Field	Required	Description
`publicKey`	Required	Provides the Public key from the key pair generated with the URL above.
`privateKey`	Required	Provides the Private key from the key pair generated with the URL above.
`mode`	Required	Specifies the Credential Vault mode. Possible values: Express or Custom

Response:

```
204 Keys are saved
```

Check if Private key has been applied or not

Use this endpoint to check the Credential Vault status. If the Private key has been applied, the Credential Vault is unlocked.

```
GET http://<your_control_room_url>/v2/credentialvault/keys/private
```

Response: The response returns if the Private key has been applied or not.

```
{
  "applied": true/false
}
```

©2020 Automation Anywhere. All rights reserved.

Apply Private key to unlock the Credential Vault after restarting the Enterprise Control Room in manual mode

```
PUT http://<your_control_room_url>/v2/credentialvault/keys/private
```

Body parameters:

Field	Required	Description
`privateKey`	Required	Unlocks the Credential Vault using the private key that was generated after Enterprise Control Room installation. See Generate Private/Public key pair

Response:

```
Private key has been successfully applied
```

Retrieve RSA Public key encoded with Base64.

```
GET http://<your_control_room_url>/v2/credentialvault/keys/transport/public
```

Response:

```
{
  "publicKey": "string"
}
```

Manage lockers

Use the Credential Vault API to manage lockers, consumers, members, and credentials in the lockers.

Permissions

Users with an `AAE_Locker_Admin` role can view and manage all lockers. By default, non-admin users have permissions to create and manage their own lockers. Non-admin users can also be given permissions to access other lockers.
The roles and permissions related to locker management are:

- Locker Owner: A locker owner can edit, view, and delete a locker, and can add or remove other owners.

©2020 Automation Anywhere. All rights reserved.

- Locker Manager: A locker manager has access to all the functions of a locker owner, but does not have permission to add owners, managers, or participants to the locker.
- Locker Participants: A locker participant has access to view a locker and its participants, and can also add their own credentials to a locker. A locker participant can not access or view credentials created by other users.
- Locker Consumers: Locker consumers have access to view a locker and input a credential attribute value (if the attribute is configured for user-input). When you select one or more user-defined roles, the users who have these selected roles become consumers of the locker.

Lockers URLS

Create a new instance of a locker

```
POST http://<your_control_room_url>/v2/credentialvault/lockers
```

Body parameters:

Field	Required	Description	Notes
name	Required	New locker name	String (50 max); cannot contain special characters
description	Optional	New locker description	String (255 max)

Response body: This response body contains information on the new locker.

```
{
  "id": "lockerIdNumber",
  "name": "lockerName",
  "description": "lockerDescription",
  "createdBy": "userIdNumber",
  "createdOn": "dateTime",
  "updatedBy": "userIdNumber",
  "updatedOn": "dateTime",
  "version": "numberOfTimesUpdated"
}
```

Use the following URLs as part of creating a new locker:

- Add a credential to the locker.
- Add a member to the locker

©2020 Automation Anywhere. All rights reserved.

Search for lockers

Returns a list of lockers where the user is a member (owner, manager, or participant) or has usage permission (consumer). If the user has `AAE_Locker Admin` permission, this URL returns a list of all the lockers in the system.

```
POST http://<your_control_room_url>/v2/credentialvault/lockers/list
```

Body parameters: This request body example includes filters, sorting, and page control to refine the response.

```
{
  "filter": {
    "operator": "NONE",
    "operands": [
      null
    ],
    "field": "string",
    "value": "string"
  },
  "sort": [
    {
      "field": "string",
      "direction": "asc"
    }
  ],
  "page": {
    "offset": 0,
    "length": 0
  }
}
```

Filters allow you to refine what is returned in the response body. Read more about filters in Filters in an API request body.

Response body: This response body contains information on the lockers. It also returns the members, their permissions, and number of credentials for each locker.

```
{
  "page": {
    "offset": 0,
```

```
    "total": 0,
    "totalFilter": 0
  },
  "list": [
    {
      "id": "lockerIdNumber",
      "name": "lockerName",
      "description": "lockerDescription",
      "createdBy": "userIdNumber",
      "createdOn": "dateTime",
      "updatedBy": "userIdNumber",
      "updatedOn": "dateTime",
      "version": "numberOfTimesUpdated",
      "members": [
        {
          "id": "userIdNumber",
          "permissions": [
            "participate/own/manage/consume"
          ]
        }
      ],
      "countOfCredentials": numberOfCredentialsInLocker
    }
  ]
}
```

Search example:Search for lockers using filters

Retrieve a specific locker by id

```
GET http://<your_control_room_url>/v2/credentialvault/lockers/{id}
```

Path parameter:

Field	Required	Description	Notes
id	Required	Identifies the locker	String

Response body:

```
{
  "id": "lockerIdNumber",
  "name": "lockerName",
  "description": "lockerDescription",
  "createdBy": "userIdNumber",
  "createdOn": "dateTime",
  "updatedBy": "userIdNumber",
  "updatedOn": "dateTime",
  "version": "numberOfTimesUpdated"
}
```

Update an existing locker

```
PUT http://<your_control_room_url>/v2/credentialvault/lockers/{id}
```

Path parameter:

Field	Required	Description	Notes
id	Required	Identifies the locker	String

Body parameters: This request body includes all the possible fields to update.

Field	Required	Description	Notes
id	Required	Identifies the locker	String
name	Required	Confirms or updates the locker name	String
description	Optional	Describes the locker	String
createdBy	Optional	Identifies the creator by ID	String
createdOn	Optional	YYYY-MM-DD HH:MM:SS.MS	Date Time
updatedBy	Optional	Identifies the user who last modified the locker by ID	String
updatedOn	Optional	YYYY-MM-DD HH:MM:SS.MS	Date Time
version	Optional	Represents the number of times the locker was updated	Number

Response body: This response body contains information on the updated locker.

```
{
  "id": "lockerIdNumber",
```

©2020 Automation Anywhere. All rights reserved.

```
  "name": "lockerName",
  "description": "lockerDescription",
  "createdBy": "userIdNumber",
  "createdOn": "dateTime",
  "updatedBy": "userIdNumber",
  "updatedOn": "dateTime",
  "version": "numberOfTimesUpdated"
}
```

Delete locker

```
DELETE http://<your_control_room_url>/v2/credentialvault/lockers/{id}
```

Path parameter:

Field	Required	Description	Notes
id	Required	Identifies the locker	String

Locker consumers URLS

These URLs accept role not user IDs. Use the Role APIs to manage roles. See User management API overview.

Retrieve a list of consumers of a locker

```
GET http://<your_control_room_url>/v2/credentialvault/lockers/{id}/consume
rs
```

Path parameter:

Field	Required	Description	Notes
id	Required	Identifies the locker	String

Response body: This response contains a list of all the roles that can access the credentials inside the locker.

```
{
  "list": [
    {
      "id": "roleIdNumber"
    }
```

```
  ]
}
```

Add a consumer to a locker

```
POST http://<your_control_room_url>/v2/credentialvault/lockers/{id}/consum
ers
```

Path parameter:

Field	Required	Description	Notes
id	Required	Identifies the locker	String

Body parameters:

Field	Required	Description	Notes
id	Required	Identifies the role	String

Delete a consumer from a specific locker

```
DELETE http://<your_control_room_url>/v2/credentialvault/lockers/{id}/cons
umers/{roleId}
```

Path parameters:

Field	Required	Description	Notes
id	Required	Identifies the locker	String
roleId	Required	Identifies the role	String

Locker members URLS

Retrieve a list of locker members

```
GET http://<your_control_room_url>/v2/credentialvault/lockers/{id}/members
```

Path parameter:

Field	Required	Description	Notes
id	Required	Identifies the locker	String

Response body: The response contains a list of all the locker members and their permissions (participate, manage, or own).

```
{
  "list": [
    {
```

```
      "id": "userIdNumber",
      "permissions": [
        "participate/manage/own"
      ]
    }
  ]
}
```

Add or updates a member of a locker

```
PUT http://<your_control_room_url>/v2/credentialvault/lockers/{id}/members
/{userId}
```

Path parameters:

Field	Required	Description	Notes
id	Required	Identifies the locker	String
userId	Required	Identifies the user	String

Body parameters:

Field	Required	Description	Notes
permissions	Required	Possible values: participate, manage, own RBAC for Credential Vault credentials management.	String

Delete a member from a locker

```
DELETE http://<your_control_room_url>/v2/credentialvault/lockers/{id}/memb
ers/{userId}
```

Path parameters:

Field	Required	Description	Notes
id	Required	Identifies the locker	String
userId	Required	Identifies the user	String

©2020 Automation Anywhere. All rights reserved.

Locker credentials URLS

Retrieve a list of all credentials in a locker

```
GET http://<your_control_room_url>/v2/credentialvault/lockers/{id}/credent
ials
```

Path parameter:

Field	Required	Description	Notes
id	Required	Identifies the locker	String

Response body: The response contains a list of all credentials and their attributes that belong to the locker, based on the permissions for the current user.

```
{
  "list": [
    {
      "id": "credentialIdNumber",
      "name": "credentialName",
      "description": "credentialDescription",
      "completed": true/false,
      "lockerId": "lockerIdNumber",
      "ownerId": "userIdNumber",
      "attributes": [
        {
          "id": "attributeIdNumber",
          "name": "attributeName",
          "description": "attributeDescription",
          "userProvided": true/false,
          "masked": true/false,
          "passwordFlag": true/false,
          "createdBy": "userIdNumber",
          "createdOn": "dateTime",
          "updatedBy": "userIdNumber",
          "updatedOn": "dateTime",
          "version": "numberOfTimesUpdated"
        }
      ],
```

©2020 Automation Anywhere. All rights reserved.

```
      "createdBy": "userIdNumber",
      "createdOn": "dateTime",
      "updatedBy": "userIdNumber",
      "updatedOn": "dateTime",
      "version": "numberOfTimesUpdated"
    }
  ]
}
```

Add your credential to the locker

Note: You must be an owner, manager, or participant of the locker.

```
PUT http://<your_control_room_url>/v2/credentialvault/lockers/{id}/credent
ials/{credentialId}
```

Path parameter:

Field	Required	Description	Notes
id	Required	Identifies the locker	String
credentialId	Required	Identifies the credential	String

Delete a credential from the locker

Note: You must be an owner, manager, or participant of the locker.

```
DELETE http://<your_control_room_url>/v2/credentialvault/lockers/{id}/cred
entials/{credentialId}
```

Path parameter:

Field	Required	Description	Notes
id	Required	Identifies the locker	String
credentialId	Required	Identifies the credential	String

Search for lockers using filters

This example shows how to use this URL to return a list of lockers where the user has owner permission.

Prerequisites

Note:

©2020 Automation Anywhere. All rights reserved.

- Use the Swagger definition files installed with your Enterprise Control Room to test the APIs. View the available Swagger APIs at `http://<your_control_room_url>/swagger/`.
- You can also use a REST client to complete this task.

Procedure

1. Add an authentication token to the request header.
   Note: Use the Authentication API to generate a JSON Web Token.
2. Specify the method and URL.
   - Method: POST
   - URL: `http://<your_control_room_url>/v2/credentialvault/lockers/list`
3. Add filter parameters in the request body to return only the lockers where the user is an owner.
   Request body:

```
{
  "sort":[],
  "filter":{
    "value":"permissions",
    "field":"owner"
    },
  "fields":[],
  "page":{ }
}
```

4. Send the request.
   - In a REST Client, click SEND.
   - In the Swagger interface, click Execute.

   Response body: The response for this example returns information on two lockers.

```
{
  "page": {
    "offset": 0,
    "total": 2,
    "totalFilter": 2
  },
  "list": [
    {
      "id": "2",
      "name": "connection param",
      "description": "",
      "createdBy": "14",
```

```
      "createdOn": "2019-12-19T21:37:28.253Z",
      "updatedBy": "14",
      "updatedOn": "2020-02-03T19:35:37.419Z",
      "version": "3",
      "members": [
        {
          "id": "4",
          "permissions": [
            "participate"
          ]
        },
        {
          "id": "14",
          "permissions": [
            "participate",
            "own",
            "manage"
          ]
        }
      ],
      "countOfCredentials": 2
    },
    {
      "id": "4",
      "name": "AccountsNew",
      "description": "",
      "createdBy": "14",
      "createdOn": "2020-02-03T18:25:52.079Z",
      "updatedBy": "14",
      "updatedOn": "2020-02-21T20:46:59.045Z",
      "version": "2",
      "members": [
        {
          "id": "14",
          "permissions": [
            "participate",
```

```
            "own",
            "manage"
          ]
        }
      ],
      "countOfCredentials": 0
    }
  ]
}
```

Note: You can also run REST requests from a command terminal. The following is a curl request example. This example is formatted for readability. Replace the text inside the angle brackets, `<authentication_token>`, with your authentication token.

```
curl -X POST "<your_control_room_url>/v2/credentialvault/lockers/list" -H "acce
pt: application/json"
        -H "X-Authorization: <authentication_token>" -H "Content-Type: applicat
ion/json"
        -d "{
            \"fields\": [],
            \"filter\": {
                \"field\": \"permissions\",
                \"value\": \"owner\"
              },
            \"sort\": [],
            \"page\": {}
            }"
```

Bot Insight Data API

Get bot process data for analytic analysis. Only users with Bot Insight administration role can access this API.

The Bot Insight Data API endpoints are listed here. Click the request example to view detailed request and response information.

Bot Insight audit trail data

`/v1/botinsight/data/api/getauditraildata/0/${DateValue}`

Ensure that the GET request can retrieve all the Enterprise Control Room audit trail data.

©2020 Automation Anywhere. All rights reserved.

Bot Insight task meta data

```
/v1/botinsight/data/api/gettaskmetadata/Analytics_ATM Reconciliation
```

Ensure that the GET request can retrieve task meta data for the specified task.

Bot Insight task variable profile

```
/v1/botinsight/data/api/gettaskvariableprofile/${JobName}?from=$
{DateValue}&to=${DateValue}
```

Make a GET request to retrieve the Enterprise Control Room variable profile for the specified dates.

Bot Insight task log data

```
/v1/botinsight/data/api/gettasklogdata/${JobName}/0/${DateValue}
```

Make a GET request to retrieve detailed information on the specified task log.

Bot Insight bot run data

```
/v1/botinsight/data/api/getbotrundata/1/${DateValue}
```

Ensure that the GET request can retrieve bot data for a specific date or date range

Bot Insight audit trail data

Ensure that the GET request can retrieve all the Enterprise Control Room audit trail data.

Request

```
GET http://{{localhost}}/v1/botinsight/data/api/getauditttraildata/0/2019-02-05
```

```
Header: X-Authorization <<authentication token>>
```

All API calls must contain an authentication token in the request header. Generate a token with the Authentication API.

Response

```
{
"totalRecords": 567,
"auditTrailDataList": [
{
"activityType": "DELETE_BOT",
```

```
"createdBy": "0",
"createdOn": "2019-02-05T23:34:33.000Z",
"detail": "[{\"newValue\":\"My Tasks > Sample Tasks >
Analytics_TelecomOrderEntry.atmx\",\"attribute\":\"Path\",\"oldValue\":null},{\
"newValue\":\"
Bot\",\"attribute\":\"Object
type\",\"oldValue\":null},{\"newValue\":\"Taskbot\",\"attribute\":\"Bot
type\",\"oldValue\":null}]",
"environmentName": "",
"eventDescription": "",
"hostName": "50.225.245.66",
"id": "1bEDwGgBIjZXN_SOYNZJ",
"objectName": "Analytics_TelecomOrderEntry.atmx",
"requestId": "12f5a941-a77d-4950-b919-a91cd3ffc0b5",
"source": "Control Room",
"status": "Successful",
"userName": "DRTEST\\admin"
},
{
"activityType": "RUN_BOT_ENDED",
"createdBy": "0",
"createdOn": "2019-02-05T23:34:03.000Z",
"detail": "[{\"newValue\":\"Completed\",\"attribute\":\"Automation
status\",\"oldValue\":null},{\"newValue\":\"Task_05.19.02.05.15.32.15.admin\",\
"attribute\":\"A
utomation name\",\"oldValue\":null},{\"newValue\":\"--\",\"attribute\":\"Automa
tion
description\",\"oldValue\":null},{\"newValue\":\"Task_05.atmx\",\"attribute\":\
"Bot\",\"oldValue
\":null},{\"newValue\":\"abcdef.com\",\"attribute\":\"Device\",\"oldValue\":nul
l},{\"newValue\":
\"testrunneruser\",\"attribute\":\"Username\",\"oldValue\":null},{\"newValue\":
\"2019-02-05
15:34:03 PST\",\"attribute\":\"Started
on\",\"oldValue\":null},{\"newValue\":\"5\",\"attribute\":\"Line
number\",\"oldValue\":null},{\"newValue\":\"One time\",\"attribute\":\"Schedule
```


©2020 Automation Anywhere. All rights reserved.

```
Type\",\"oldValue\":null}]",
"environmentName": "",
"eventDescription": "",
"hostName": "abcdef.com",
"id": "1LECwGgBIjZXN_SO7dZi",
"objectName": "Task_05.19.02.05.15.32.15.admin",
"requestId": "a73eef1f-5aa9-4345-8ae8-e6f2e24ab41e",
"source": "Control Room",
"status": "Successful",
"userName": "System"
},
{
"activityType": "DEPLOYMENT_AUTOMATION",
"createdBy": "0",
"createdOn": "2019-02-05T23:34:00.000Z",
"detail": "[{\"newValue\":\"Task_05.19.02.05.15.32.15.admin\",\"attribute\":\"A
utomation
name\",\"oldValue\":null},{\"newValue\":\"Task_05.atmx\",\"attribute\":\"Bot\",
\"oldValue\":nul
l},{\"newValue\":\"abcdef.com\",\"attribute\":\"Device\",\"oldValue\":null},{\"
newValue\":\"test
runneruser\",\"attribute\":\"Username\",\"oldValue\":null},{\"newValue\":\"2019
-02-05 15:34:00
PST\",\"attribute\":\"Started on\",\"oldValue\":null},{\"newValue\":\"One
time\",\"attribute\":\"Schedule Type\",\"oldValue\":null}]",
"environmentName": "",
"eventDescription": "",
"hostName": "abcdef.com",
"id": "Gf4CwGgBv9m2c9mi4XaL",
"objectName": "Task_05.19.02.05.15.32.15.admin",
"requestId": "8927dc37-67eb-4f8f-8e13-3a60c6070fd3",
"source": "Control Room",
"status": "Successful",
"userName": "System"
},
.........................
```


©2020 Automation Anywhere. All rights reserved.

```
]
}
```

Bot Insight task meta data

Ensure that the GET request can retrieve task meta data for the specified task.

Request

```
GET http://{{localhost}}/v1/botinsight/data/api/gettaskmetadata/Analytics_ATM
Reconciliation
```

```
Header: X-Authorization <<authentication token>>
```

All API calls must contain an authentication token in the request header. Generate a token with the Authentication API.

Response

```
[
  {
    "attributeType": "STRING",
    "variableName": "amount",
    "displayName": "Amount",
    "isActive": "Y",
    "isAttributeTypeChanged": "N",
    "isInUse": "N",
    "mappedToColumn": 2,
    "dateModified": 1549490723370,
    "isEnabled": "Y",
    "newlyAdded": null,
    "taskId": null
  },
  {
    "attributeType": "STRING",
    "variableName": "bank_name",
    "displayName": "Bank Name",
```

©2020 Automation Anywhere. All rights reserved.

```
    "isActive": "Y",
    "isAttributeTypeChanged": "N",
    "isInUse": "N",
    "mappedToColumn": 3,
    "dateModified": 1549490723370,
    "isEnabled": "Y",
    "newlyAdded": null,
    "taskId": null
  },
  {
    "attributeType": "STRING",
    "variableName": "card_type",
    "displayName": "Card Type",
    "isActive": "Y",
    "isAttributeTypeChanged": "N",
    "isInUse": "N",
    "mappedToColumn": 4,
    "dateModified": 1549490723370,
    "isEnabled": "Y",
    "newlyAdded": null,
    "taskId": null
  },
  {
    "attributeType": "STRING",
    "variableName": "country_code",
    "displayName": "Country Code",
    "isActive": "Y",
    "isAttributeTypeChanged": "N",
    "isInUse": "N",
    "mappedToColumn": 5,
    "dateModified": 1549490723370,
    "isEnabled": "Y",
    "newlyAdded": null,
    "taskId": null
  },
  {
```


©2020 Automation Anywhere. All rights reserved.

```
    "attributeType": "STRING",
    "variableName": "reason",
    "displayName": "Reason",
    "isActive": "Y",
    "isAttributeTypeChanged": "N",
    "isInUse": "N",
    "mappedToColumn": 10,
    "dateModified": 1549490723370,
    "isEnabled": "Y",
    "newlyAdded": null,
    "taskId": null
  },
  {
    "attributeType": "STRING",
    "variableName": "state_code",
    "displayName": "State Code",
    "isActive": "Y",
    "isAttributeTypeChanged": "N",
    "isInUse": "N",
    "mappedToColumn": 6,
    "dateModified": 1549490723370,
    "isEnabled": "Y",
    "newlyAdded": null,
    "taskId": null
  },
  {
    "attributeType": "STRING",
    "variableName": "status",
    "displayName": "Status",
    "isActive": "Y",
    "isAttributeTypeChanged": "N",
    "isInUse": "N",
    "mappedToColumn": 7,
    "dateModified": 1549490723370,
    "isEnabled": "Y",
    "newlyAdded": null,
```


©2020 Automation Anywhere. All rights reserved.

```
    "taskId": null
  },
  {
    "attributeType": "STRING",
    "variableName": "transaction_date",
    "displayName": "Transaction Date",
    "isActive": "Y",
    "isAttributeTypeChanged": "N",
    "isInUse": "N",
    "mappedToColumn": 8,
    "dateModified": 1549490723370,
    "isEnabled": "Y",
    "newlyAdded": null,
    "taskId": null
  },
  {
    "attributeType": "STRING",
    "variableName": "transaction_type",
    "displayName": "Transaction Type",
    "isActive": "Y",
    "isAttributeTypeChanged": "N",
    "isInUse": "N",
    "mappedToColumn": 9,
    "dateModified": 1549490723370,
    "isEnabled": "Y",
    "newlyAdded": null,
    "taskId": null
  },
  {
    "attributeType": "NUMERIC",
    "variableName": "zip_code",
    "displayName": "Zip Code",
    "isActive": "Y",
    "isAttributeTypeChanged": "N",
    "isInUse": "N",
    "mappedToColumn": 1,
```


©2020 Automation Anywhere. All rights reserved.

```
    "dateModified": 1549490723370,
    "isEnabled": "Y",
    "newlyAdded": null,
    "taskId": null
  }
]
```

Bot Insight task variable profile

Make a GET request to retrieve the Enterprise Control Room variable profile for the specified dates.

Request

```
GET http://{{localhost}}/v1/botinsight/data/api/gettaskvariableprofile/Analytic
s_ATM
Reconciliation?from=2019-01-31&to2019-02-05
```

```
Header: X-Authorization <<authentication token>>
```

All API calls must contain an authentication token in the request header. Generate a token with the Authentication API.

Response

```
{
  "taskId": "94c23a0a-fe84-4f00-8cbc-28253acff30e",
  "taskName": "Analytics_ATM Reconciliation",
  "totalRecords": 1000,
  "profileVariables": [
    {
      "variableName": "amount",
      "displayName": "Amount",
      "mappedToColumnName": "string2",
      "attributeType": "STRING",
      "isAttributeTypeChanged": "N",
      "totalRecords": 1000,
      "totalNullRecords": 0,
```

©2020 Automation Anywhere. All rights reserved.

```
      "sumOfValue": 0,
      "averageOfValues": 0,
      "totalDistincts": 766,
      "newlyAdded": null,
      "enabled": null
    },
    {
      "variableName": "bank_name",
      "displayName": "Bank Name",
      "mappedToColumnName": "string3",
      "attributeType": "STRING",
      "isAttributeTypeChanged": "N",
      "totalRecords": 1000,
      "totalNullRecords": 0,
      "sumOfValue": 0,
      "averageOfValues": 0,
      "totalDistincts": 5,
      "newlyAdded": null,
      "enabled": null
    },
    {
      "variableName": "card_type",
      "displayName": "Card Type",
      "mappedToColumnName": "string4",
      "attributeType": "STRING",
      "isAttributeTypeChanged": "N",
      "totalRecords": 1000,
      "totalNullRecords": 0,
      "sumOfValue": 0,
      "averageOfValues": 0,
      "totalDistincts": 16,
      "newlyAdded": null,
      "enabled": null
    },
    {
      "variableName": "country_code",
```


©2020 Automation Anywhere. All rights reserved.

```
      "displayName": "Country Code",
      "mappedToColumnName": "string5",
      "attributeType": "STRING",
      "isAttributeTypeChanged": "N",
      "totalRecords": 1000,
      "totalNullRecords": 0,
      "sumOfValue": 0,
      "averageOfValues": 0,
      "totalDistincts": 1,
      "newlyAdded": null,
      "enabled": null
    },
    {
      "variableName": "reason",
      "displayName": "Reason",
      "mappedToColumnName": "string10",
      "attributeType": "STRING",
      "isAttributeTypeChanged": "N",
      "totalRecords": 1000,
      "totalNullRecords": 1,
      "sumOfValue": 0,
      "averageOfValues": 0,
      "totalDistincts": 4,
      "newlyAdded": null,
      "enabled": null
    },
    {
      "variableName": "state_code",
      "displayName": "State Code",
      "mappedToColumnName": "string6",
      "attributeType": "STRING",
      "isAttributeTypeChanged": "N",
      "totalRecords": 1000,
      "totalNullRecords": 0,
      "sumOfValue": 0,
      "averageOfValues": 0,
```

```
      "totalDistincts": 48,
      "newlyAdded": null,
      "enabled": null
    },
    {
      "variableName": "status",
      "displayName": "Status",
      "mappedToColumnName": "string7",
      "attributeType": "STRING",
      "isAttributeTypeChanged": "N",
      "totalRecords": 1000,
      "totalNullRecords": 0,
      "sumOfValue": 0,
      "averageOfValues": 0,
      "totalDistincts": 2,
      "newlyAdded": null,
      "enabled": null
    },
    {
      "variableName": "transaction_date",
      "displayName": "Transaction Date",
      "mappedToColumnName": "string8",
      "attributeType": "STRING",
      "isAttributeTypeChanged": "N",
      "totalRecords": 1000,
      "totalNullRecords": 0,
      "sumOfValue": 0,
      "averageOfValues": 0,
      "totalDistincts": 3,
      "newlyAdded": null,
      "enabled": null
    },
    {
      "variableName": "transaction_type",
      "displayName": "Transaction Type",
      "mappedToColumnName": "string9",
```


©2020 Automation Anywhere. All rights reserved.

```
      "attributeType": "STRING",
      "isAttributeTypeChanged": "N",
      "totalRecords": 1000,
      "totalNullRecords": 0,
      "sumOfValue": 0,
      "averageOfValues": 0,
      "totalDistincts": 240,
      "newlyAdded": null,
      "enabled": null
    },
    {
      "variableName": "zip_code",
      "displayName": "Zip Code",
      "mappedToColumnName": "string1",
      "attributeType": "NUMERIC",
      "isAttributeTypeChanged": "N",
      "totalRecords": 1000,
      "totalNullRecords": 0,
      "sumOfValue": 400979,
      "minimumValue": "10",
      "maximumValue": "800",
      "averageOfValues": 400.979,
      "totalDistincts": 575,
      "newlyAdded": null,
      "enabled": null
    }
  ],
  "standardDashboardName": null
}
```


Bot Insight task log data

Make a GET request to retrieve detailed information on the specified task log.

Request

```
GET http://{{localhost}}/v1/botinsight/data/api/gettasklogdata/Analytics_ATM
Reconciliation/0/2019-02-05
```

```
Header: X-Authorization <<authentication token>>
```

All API calls must contain an authentication token in the request header. Generate a token with the Authentication API.

Response


```
{
"totalRecords": 1,
"taskLogDataList": [
{
"machineName": "WIN-4MBO81V7Q7T",
"runStatus": "InProgress",
"userId": 1,
"dateLogged": 1549330489334,
"variables": "{\"amount\":\"65898\",\"bank_name\":\"Bank of
America\",\"card_type\":\"jcb\",\"country_code\":\"United
States\",\"reason\":\"\",\"state_code\":\"Missouri\",\"status\":\"Matched\",\"t
ransaction_date\":\"
Withdrawal\",\"transaction_type\":\"1499817600000\",\"zip_code\":\"10\" }"
},
{
"totalRecords": 1,
"taskLogDataList": [
{
"machineName": "WIN-4MBO81V7Q7T",
"runStatus": "CompletedSuccessfully",
"userId": 1,
"dateLogged": 1549330489334,
"variables": "{\"amount\":\"65898\",\"bank_name\":\"Bank of
America\",\"card_type\":\"jcb\",\"country_code\":\"United
States\",\"reason\":\"\",\"state_code\":\"Missouri\",\"status\":\"Matched\",\"t
```

```
ransaction_date\":\"
Withdrawal\",\"transaction_type\":\"1499817600000\",\"zip_code\":\"10\" }"
},
{
"totalRecords": 1,
"taskLogDataList": [
{
"machineName": "WIN-4MBO81V7Q7T",
"runStatus": "Aborted",
"userId": 1,
"dateLogged": 1549330489334,
"variables": "{\"amount\":\"65898\",\"bank_name\":\"Bank of
America\",\"card_type\":\"jcb\",\"country_code\":\"United
States\",\"reason\":\"\",\"state_code\":\"Missouri\",\"status\":\"Matched\",\"t
ransaction_date\":\"
Withdrawal\",\"transaction_type\":\"1499817600000\",\"zip_code\":\"10\" }"
},
{
"totalRecords": 1,
"taskLogDataList": [
{
"machineName": "WIN-4MBO81V7Q7T",
"runStatus": "Failed",
"userId": 1,
"dateLogged": 1549330489334,
"variables": "{\"amount\":\"65898\",\"bank_name\":\"Bank of
America\",\"card_type\":\"jcb\",\"country_code\":\"United
States\",\"reason\":\"\",\"state_code\":\"Missouri\",\"status\":\"Matched\",\"t
ransaction_date\":\"
Withdrawal\",\"transaction_type\":\"1499817600000\",\"zip_code\":\"10\" }"
},
{
"totalRecords": 1,
"taskLogDataList": [
{
"machineName": "WIN-4MBO81V7Q7T",
```

```
"runStatus": "TimedOut",
"userId": 1,
"dateLogged": 1549330489334,
"variables": "{\"amount\":\"65898\",\"bank_name\":\"Bank of
America\",\"card_type\":\"jcb\",\"country_code\":\"United
States\",\"reason\":\"\",\"state_code\":\"Missouri\",\"status\":\"Matched\",\"t
ransaction_date\":\"
Withdrawal\",\"transaction_type\":\"1499817600000\",\"zip_code\":\"10\" }"
}
```


Bot Insight bot run data

Ensure that the GET request can retrieve bot data for a specific date or date range.

Request

```
GET http://{{localhost}}/v1/botinsight/data/api/getbotrundata/0/2019-02-05
```

```
Header: X-Authorization <<authentication token>>
```

All API calls must contain an authentication token in the request header. Generate a token with the Authentication API.

Response


```
{
  "totalRecords": 367,
  "botRunDataList": [
    {
      "id": 1,
      "userName": "b2",
      "firstName": "b2",
      "lastName": null,
      "email": "a@a.com",
      "clientType": null,
      "hostName": "abcdef.com",
      "iPAddress": "fe80::c9a4:eecb:aeb5:58a1%Ethernet",
```

```
      "applicationPath": "C:\\Users\\chandank.DRTEST\\Documents\\Automation Any
where Files",
      "username_1": null,
      "fileName": "Analytics_ATM Reconciliation.atmx",
      "fileType": null,
      "startTime": "2019-02-05 00:35:30.0",
      "endTime": "2019-02-05 00:35:40.0",
      "status": "COMPLETED",
      "totalLines": "24",
      "timeTaken": "10",
      "successIndicator": "0"
    },
    {
      "id": 2,
      "userName": "b2",
      "firstName": "b2",
      "lastName": null,
      "email": "a@a.com",
      "clientType": null,
      "hostName": "QAVM01.drtest.com",
      "iPAddress": "fe80::c9a4:eecb:aeb5:58a1%Ethernet",
      "applicationPath": "C:\\Users\\chandank.DRTEST\\Documents\\Automation Any
where Files",
      "username_1": null,
      "fileName": "Analytics_MortgageProcessing.atmx",
      "fileType": null,
      "startTime": "2019-02-05 00:44:55.0",
      "endTime": "2019-02-05 00:45:07.0",
      "status": "COMPLETED",
      "totalLines": "34",
      "timeTaken": "12",
      "successIndicator": "0"
    },
    {
      "id": 3,
      "userName": "b2",
```

```
      "firstName": "b2",
      "lastName": null,
      "email": "a@a.com",
      "clientType": null,
      "hostName": "abcdef.com",
      "iPAddress": "fe80::c9a4:eecb:aeb5:58a1%Ethernet",
      "applicationPath": "C:\\Users\\chandank.DRTEST\\Documents\\Automation Any
where Files",
      "username_1": null,
      "fileName": "Analytics_ATM Reconciliation.atmx",
      "fileType": null,
      "startTime": "2019-02-05 01:17:02.0",
      "endTime": "2019-02-05 01:17:13.0",
      "status": "COMPLETED",
      "totalLines": "24",
      "timeTaken": "11",
      "successIndicator": "0"
    },
    {
      "id": 4,
      "userName": "b2",
      "firstName": "b2",
      "lastName": null,
      "email": "a@a.com",
      "clientType": null,
      "hostName": "abcdef.com",
      "iPAddress": "fe80::c9a4:eecb:aeb5:58a1%Ethernet",
      "applicationPath": "C:\\Users\\chandank.DRTEST\\Documents\\Automation Any
where Files",
      "username_1": null,
      "fileName": "Analytics_MortgageProcessing.atmx",
      "fileType": null,
      "startTime": "2019-02-05 01:17:13.0",
      "endTime": "2019-02-05 01:17:26.0",
      "status": "COMPLETED",
      "totalLines": "34",
```


©2020 Automation Anywhere. All rights reserved.

```
      "timeTaken": "13",
      "successIndicator": "0"
    },
    . . .
  ]
}
```

API to export and import Bot Lifecycle Management

Use the export and import bots APIs to customize the organization's Bot Lifecycle Management solution for an uninterrupted automation life-cycle.

Usually, the Enterprise Control Room user has to depend on means other than Enterprise Control Room (for example email) to deploy TaskBots from one environment to another. Using the Export-Import APIs, you can easily introduce a customized Bot Lifecycle Management (BLM) solution thus removing all external factors that could possibly disrupt your automation life cycle.

As a Enterprise Control Room user with Export bots and Download bots permission, you can export a bot and its dependent files. Similarly, as a user with Import bots and Upload bots permission, you can import that bot and its dependent files.

For example, you can move the bots that are verified as production ready from staging to production.

You can use the Enterprise Control Room Export Import REST API to manage your automation TaskBots including dependent files in different environments such as Development, Testing, Acceptance, and Production based on your organization's automation needs.

Refer Export bots and Import bots articles to use the functionality from your Enterprise Control Room user interface.

Features and benefits

- Role based access control on Bot Lifecycle Management
- Automatic export of dependencies (files and bots)
- Audit and traceability on source and target environment for compliance
- Email notification on successful execution or failure of export and import.

Export

- The Enterprise Control Room user whose credentials are used for authentication must have Export bots permission
- The Enterprise Control Room user whose credentials are used for authentication must have Download permission on the bots, minimum Execute permission on MetaBot, and dependencies that are being exported.
- If version control is enabled in the source Enterprise Control Room, the production version of all bots and dependencies which you want to export must be set.

©2020 Automation Anywhere. All rights reserved.

- User account that is used to run the Enterprise Control Room services must have access to the location where package is getting exported, for example, network location(shared drive) or on Enterprise Control Room server machine.

Import

- The Enterprise Control Room user whose credentials are used for authentication must have Import bots permission
- The Enterprise Control Room user whose credentials are used for authentication must have Upload permission on the bots and dependencies that are being imported.
- The Enterprise Control Room user who will execute the utility to import multiple bots must have access to the exported package file provided by Automation Anywhere.

API Endpoints

- Export- `<your_control_room_url>/v1/blm/export`

  For example,`https://crdevenv.com:81/v1/alm/export`

- Import- `<your_control_room_url>/v1/blm/import`

  For example, `https://crtestenv.com:82/v1/alm/import`

Using the above end points of the BLM Export Import API you can export and import a single bot and all of its dependencies.

Export Bot

Export a single bot with its dependent files using the Export API provided by Automation Anywhere:

1. Use the POST method to generate a token using the end point `http(s)://<hostname:port>/v1/authentication`. For this provide the Enterprise Control Room instance as `Server Name` / `Hostname` / `IP` and the `Port` number.

   For example, `https://crdevenv.com:81/v1/authentication`

2. Use the Post method and state the parameters for credentials in Body Data. Refer sample:

```
{
"username":"cradmin",
```

```
"password":"cr@admin"
}
```

3. Click Execute.
4. BLM Export API will make use of the authentication token that is obtained using the Authentication API. The authentication token has to be passed on as one of the header inputs to the BLM Export API.

5. Use the POST method and URL: `<your_control_room_url>/v1/blm/export`.

   Provide the following parameter for the request header:

   - `packageName:` Name of the package to be created.
   - `selectedFileIds:` This is a numeric value. Enter one or more selected file IDs you want to export.
   - `fileIds:` This is a numeric value. Enter one or more file IDs you want to export.
   - `excludeMetabots:` This is a Boolean value. Enter either `true` or `false`. Enter `true` if the dependent MetaBots are to be excluded in package
   - `password:` This is a string and is optional. Enter the export password.
     For example:

```
{
  "packageName": "doc-test",
  "selectedFileIds": [12
  ],
  "fileIds": [
    12
  ],
  "excludeMetaBots": true,
  "password": ""
}
```

6. Click Execute.
7. Response body returns a download link that can be used to download the exported file in aapkg format.

Import Bot

After the bot is successfully exported to a network drive or Enterprise Control Room machine path, another authorized user can import that package to a different Enterprise Control Room using the Import API:

1. Use the Post method to generate a token using the end point `http(s)://<hostname:port>/v1/authentication`. Provide the Enterprise Control Room instance as
   `Server Name`
   /
   `Hostname`
   /

©2020 Automation Anywhere. All rights reserved.

`IP`
and the
`Port`
number.

For example, `https://crtestenv.com:82/v1/authentication`

2. Use the Post method and state the parameters for credentials in Body Data.

   For example:

```
 {
"username":"cradmin2",
"password":"cr@admin"
}
```

3. Click Execute.
4. BLM Import API will make use of the authentication token that is obtained using the Authentication API. The authentication token has to be passed on as one of the header inputs to the BLM Import API.
5. Use the POST method and URL: `<your_control_room_url>/v1/blm/import`.

   Provide the following parameter for the request header:

   - `file:` Choose the file that you want to import in your Enterprise Control Room.
   - `overwriteOption:` Select either the `skip`, `overwrite`, or `abort` option if the file you are importing already exists.
   - `productionversionOption:` Select either the `current` or `imported` option. Set the production version as imported with the package or keep the current version as is.
   - `Password:` Enter the password to import protected package. You must not keep this field empty otherwise keep the default value as the password

   For example:

   Request Body:

```
"file": "doc-test_6488adfd-5989-46d8-a38a-7009876f2612.aapkg"
"overwriteOption": "skip"
"productionVersionOption": "current"
"password": "********"
```

6. Click Execute
7. The bot is imported in your Enterprise Control Room.

   For example: Because the file already exists in the folder, it is skipped as per the `overWrite` parameter value is defined as `skip`.

   Response body:

```
{
  "alreadyExistFiles": [
    "Automation Anywhere\\My Tasks\\Task_C.atmx"
  ],
  "checkoutFiles": [],
  "filesHasNoPermission": [],
  "addedOrUpdatedFiles": [],
  "overwrittenFiles": [],
  "skippedFiles": [
    "Automation Anywhere\\My Tasks\\Task_C.atmx"
  ]
}
```

API Response Codes

Http(s) Status code	Response- Description	Corrective Action
200	Package created successfully	NA
400	Bad request parameter	Retry with valid parameters
404	File not found	Ensure that the file/bot is present in Enterprise Control Room
501	Permission error	Ensure that you have the Export/Import bots or Upload/Download permission

Related concepts
Audit log overview
Related reference
Bot Lifecycle Management (BLM) - an overview
Export bots
Import bots

API data migration from 10.x to 11.x Enterprise Control Room

As a Enterprise Control Room administrator with View and Manage Migration role permissions, use the Migration APIs to migrate data from 10.x to the latest 11.x Enterprise Control Room.

The Migration APIs allow you to,

1. Save / update connection configuration to the 10.x Enterprise Control Room database
2. Save / update connection configuration to the 2.x Bot Insight database, if available

©2020 Automation Anywhere. All rights reserved.

3. Specify option to migrate data based on Roles, Users or Bots
4. Fetch list of data based on option specified for migration that is, Roles, Users, or Bots
5. View the migration progress summary
6. View migration statistics of number of entities that succeeded / failed per migration
7. Fetch list of new and updated bots from 10.x Enterprise Control Room post migration
8. Migrate files in bulk from the 10.x Enterprise Control Room My docs folder post migration

Alternately, you can use the Migration wizard given in Administration > Migration module to migrate the data from the Enterprise Control Room user interface. Refer Migration Overview for details.

Note: The examples provided in this article are for reference only.

API End Point

Use the following end points to access the API:

1. For migration process use <Enterprise Control Room URL>/v2/migration
2. For migrating files from the My Docs folder of source 10.x Enterprise Control Room after the migration process has completed use <Enterprise Control Room URL>/v1/migration

For example,

https://crdevenv.com:81/v2/migration

Migration Process APIs

The Migration APIs allow you to migrate 10.x Enterprise Control Room data to 11.x Enterprise Control Room using the end point mentioned earlier.

Before accessing the Migration API's you must first use the authentication API and pass it as a token to use a particular Migration API.

1. Use the POST method to generate a token using the end point http(s)://<hostname:port>/v1/authentication. For this provide the Enterprise Control Room instance as Server Name /Hostname /IP and the Port number.

   For example,https://crdevenv.com:81/v1/authentication

2. Provide the following request payload in Headers

   "X-Authorization" : "Authorization token"

   "Content-Type" : "application/json"

3. Provide the following request payload in Body:

   {

   "username": "<Username>",

   "password": "<Password>"

   }

For example,

```
{

"usename": "Ellie.Brown",

"password": "12345678"

}
```

1. Connect to source Enterprise Control Room database

This API allows you to save and update the connection configuration to the source 10.x Enterprise Control Room database.

1. Provide the "X-Authorization" and "Content Type" parameters in Headers.
2. Provide credential parameters in Body
3. Use the POST method to connect to the 10.x Enterprise Control Room database using the end point http(s)://<hostname:port>/v2/migration/connection

   For example,https://crdevenv.com:81/v2/migration/connection

4. Provide the following request parameters in Body:

   ```
   {

   "host": "string", "port": 0, "databaseName": "string", "username": "string", "password": "string", "integratedSecurity": true, "encrypt": true, "privateKey": "string", "repoPath": "string"

   }
   ```

   For example,

   ```
   {

   "host": "PRODUCTLT",

   "port": 1433,

   "databaseName": "CR104MIG",

   "username": "Ellie.Brown",

   "password": "12345678",

   "integratedSecurity": true,

   "encrypt": true,

   "privateKey": "ABC123",

   "repoPath": "D:\\Data\Automation Anywhere Server Files"

   }
   ```

©2020 Automation Anywhere. All rights reserved.

5. Click Send.

Parameter Description

Parameter	Description
host	Source Enterprise Control Room database host name
port	Source Enterprise Control Room database port number
databaseName	Source Enterprise Control Room database name
username	Username to connect to database
password	Password to connect to database
integratedSecurity	An indicator whether to use Windows authentication when connecting to source database. Set this to true if you want use Windows authentication. The default value is false
encrypt	An indicator whether to use secure connection to source database. Set this to true if you want to use a secure connection. The default value is false
privateKey	The private key to decrypt credential values in source database. This is available for configuration during the initial Enterprise Control Room setup.
repoPath	The shared repository path where Enterprise Control Room 10.x repository is stored

2. Get stored connection details

This API allows you to fetch the stored connection details of source 10.x Enterprise Control Room database from where the data can be migrated.

1. Provide the "X-Authorization" and "Content Type" parameters in Headers.
2. Provide credential parameters in Body
3. Use the GET method to fetch the connection configuration of 10.x Enterprise Control Room database using the end point http(s)://<hostname:port>/v2/migration/connection

   For example, https://crdevenv.com:81/v2/migration/connection

4. Click Send
5. You can view the result in Body data:

   {

   "host": "productlt",

   "port": 1433,

   "databaseName": "CR104MIG",

   "username": "",

   "password": "",

"integratedSecurity": true,

"encrypt": false,

"privateKey": "",

"repoPath": "D:\\DATA\AUTOMATION ANYWHERE SERVER FILES"

}

Parameter Description

Parameter	Description
host	Source database host
port	Source database port
databaseName	Source database name
username	Username to connect to source database
password	Password to connect to source database
integratedSecurity	An indicator whether to use Windows authentication when connecting to source database, default value is false
encrypt	An indicator whether to use secure connection to source database, default value is false
privateKey	Private key to decrypt credential values in source database
repoPath	The shared repository path where Enterprise Control Room 10.x repository is stored

3. Connect to 2.x Bot Insight database, if available

This API allows you to connect to the source 2.x Bot Insight database if available, to migrate analytics data.

1. Provide the "X-Authorization" and "Content Type" parameters in Headers.
2. Provide credential parameters in Body.
3. Use the POST method to connect to the Bot Insight database using the end point http(s)://<hostname:port>/v2/migration/connection /botinsight

   For example, https://crdevenv.com:81/v2/migration/connection/botinsight

4. Provide following request parameters in Body:

   {

   "host": "string",

   "port": 0,

   "databaseName": "string",

"username": "string",

"password": "string",

"integratedSecurity": true,

"encrypt": true,

"serverUrl": "string"

}

For example,

{

"host": "ProductIt",

"port": 8091,

"databaseName": "BotInsight",

"username": "Ellie.Brown",

"password": "12345678",

"integratedSecurity": true,

"encrypt": true,

"serverUrl": "https://productlt.example.com:82/analytics"

}

5. Click Send
6. The connection parameters are successfully saved when the response status is 200 Successful operation .

Parameter Description

Parameter	Description
host	Source Bot Insight database host name
port	Source Bot Insight database port number
databaseName	Source Bot Insight database name
username	Username to connect to database
password	Password to connect to database
integratedSecurity	An indicator whether to use Windows authentication when connecting to source database. Set this to true if you want use Windows authentication. The default value is false

©2020 Automation Anywhere. All rights reserved.

Parameter	Description
encrypt	An indicator whether to use secure connection to source database. Set this to true if you want to use a secure connection. The default value is false
serverUrl	Server url where the Bot Insight Visualization ServerPort

4. Get stored connection details

This API allows you to fetch the stored connection details of source 2.x Bot Insight database from where the data can be migrated.

1. Provide the "X-Authorization" and "Content Type" parameters in Headers.
2. Provide credential parameters in Body
3. Use the GET method to fetch the connection configuration of 10.x Enterprise Control Room database using the end point http(s)://<hostname:port>/v2/migration/connection/botinsight

   For example,https://crdevenv.com:81/v2/migration/connection/botinsight

4. Click Send
5. The connection parameters are successfully saved when the response status is 200 Migration config .
6. You can view the result in Body data:


```
{

"host": "ProductIt",

"port": 8091,

"databaseName": "BotInsight",

"username": "Ellie.Brown",

"password": "12345678",

"integratedSecurity": true,

"encrypt": true,

"serverUrl": "https://productIt.example.com:82/analytics"

}
```


Parameter description

Parameter	Description
host	Source Bot Insight database host name
port	Source Bot Insight database port number
databaseName	Source Bot Insight database name
username	Username to connect to database

©2020 Automation Anywhere. All rights reserved.

Parameter	Description
password	Password to connect to database
integratedSecurity	An indicator whether to use Windows authentication when connecting to source database. Set this to true if you want use Windows authentication. The default value is false
encrypt	An indicator whether to use secure connection to source database. Set this to true if you want to use a secure connection. The default value is false
serverUrl	Server url where the Bot Insight Visualization ServerPort

5. List of entities of TYPE available for migration in source database

This API returns list of entities available for migration in source database by TYPE parameter. Using the either of the options - Role, User, Bot, or Schedule, you can migrate all data that is associated with the parameter chosen.

1. Provide the "X-Authorization" parameters in Headers.
2. Use the GET method to connect to the Enterprise Control Room database using the end point http(s)://<hostname:port>/v2/migration/connection /entities followed by TYPE parameter that could include any one of the option - Roles, Users, Bots, or Schedules

   For example,https://crdevenv.com:81/v2/migration/connection/entities?Type=ROLE

3. Click Send
4. The data is returned when the response status is 200
5. The list of entities based on TYPE parameter are displayed in Body.

{

"entities":

[

{ "id": "0", "type": "ROLE", "sourceId": "1", "targetId": "0", "name": "Admin", "status": "SUCCESS", "reason": "" },

{ "id": "0", "type": "ROLE", "sourceId": "2", "targetId": "0", "name": "Basic", "status": "SUCCESS", "reason": "" },

{ "id": "0", "type": "ROLE", "sourceId": "3", "targetId": "0", "name": "IQBotValidator", "status": "SUCCESS", "reason": "" },

{ "id": "0", "type": "ROLE", "sourceId": "4", "targetId": "0", "name": "AnalyticsExperts", "status": "SUCCESS", "reason": "" },

{ "id": "0", "type": "ROLE", "sourceId": "5", "targetId": "0", "name": "AnalyticsConsumers", "status": "SUCCESS", "reason": "" },

{ "id": "0", "type": "ROLE", "sourceId": "6", "targetId": "0", "name": "BotAgentUser", "status": "SUCCESS", "reason": "" },

©2020 Automation Anywhere. All rights reserved.

{ "id": "0", "type": "ROLE", "sourceId": "7", "targetId": "0", "name": "BotFarmAdmin", "status": "SUCCESS", "reason": "" },

{ "id": "0", "type": "ROLE", "sourceId": "8", "targetId": "0", "name": "IQBotServices", "status": "SUCCESS", "reason": "" },

{ "id": "0", "type": "ROLE", "sourceId": "9", "targetId": "0", "name": "Bot Creator 10x", "status": "SUCCESS", "reason": "" },

{ "id": "0", "type": "ROLE", "sourceId": "10", "targetId": "0", "name": "Bot Runner 10x", "status": "SUCCESS", "reason": "" },

{ "id": "0", "type": "ROLE", "sourceId": "11", "targetId": "0", "name": "Bot Scheduler 10x", "status": "SUCCESS", "reason": "" }

]

}

Parameter description

Parameter	Description
id	Migration ID
type	Type of entity selected for migration - Role, User or Bot
sourceId	Id of entity in the source database
targetId	Id of entity after Migration in the target database
name	Name of the entity in the source database
status	The migration status for that particular entity
reason	The reason for migration failure for that particular entity

6. Prepare migration data based on User input

This API allows you to migrate entities with associated data based on the sub-section of the entity type specified for migration.

1. Provide the "X-Authorization" and "Content Type" parameters in Headers.
2. Use the POST method to migrate the data using the endpoint http(s)://<hostname:port>/v2/migration/prepare

   For example,https://crdevenv.com:81/v2/migration/prepare

3. Provide following request payload in Body:

   {

   "selected":

   [

{ "type": "<enitity type>",

"sourceId": "string" }

],

"excludes": ["<entity type>"

]

}

For example,

{ "selected": [{ "type": "ROLE", "sourceId": "12" }], "excludes": ["BOT"] }

4. Click Send
5. The data is listed successfully for migration when the response status is 200
6. The result is displayed in the Body

{ "selected":

[

{ "type": "ROLE", "sourceId": "12" }],

"excludes": ["BOT"]

}

Parameter description

Parameter	Description
type	Type of entity selected for migration - Role, User or Bot and Schedules
sourceId	The id of the entity in the source database
excludes	The entity name that is excluded from migration. The options are available based on the entity type selected. When you select Role or User, you can Exclude Bots and Schedules. When you select Bots and Schedules, you can Exclude MetaBots), or Overwrite existing Bots.

7. Start Migration

This API allows you to launch the migration process.

1. Provide the "X-Authorization" parameters in Headers.
2. Use the POST method to migrate the data using the endpoint http(s)://<hostname:port>/v2/migration/start/async

©2020 Automation Anywhere. All rights reserved.

For example, https://crdevenv.com:81/v2/migration/start/async

3. Click Send
4. The data migration starts successfully when the response status is 200 Successful operation
5. The result is displayed in the Body data

{

"id": 1,

"name": "2018.07.17.16.13.48.ellie.brown",

"createdBy": 1,

"migrationType": "ROLE_EXCLUDE_BOT_SCHEDULE"

}

Parameter description

Parameter	Description
id	Migration ID
name	Name of the user who initiated the migration
createdBy	Id of the entity that started the migration. For example, the Enterprise Control Room administrator
migrationType	The migration type chosen - Role, User, or Bots and Schedules

8. Migration object by id

This API lists the migration object details based on the ID that is generated using the Start Migration API.

1. Provide the "X-Authorization" parameters in Headers.
2. Use the GET method to fetch object details by id using the endpoint http(s)://<hostname:port>/v2/migration/<id>

   For example, https://crdevenv.com:81/v2/migration/9

3. Click Send.
4. The object details are listed successfully when the response status is 200
5. The details are shown in the Body data:

{

"id": "9",

"name": "2018.07.17.16.13.48.ellie.brown",

"startTime": "2018-07-17T10:43:48.127Z",

"endTime": "2018-07-17T10:43:49.833Z",

"createdBy": "1",

"migrationType": "ROLE_EXCLUDE_BOT_SCHEDULE",

"entities": []

}

Parameter description

Parameter	Description
id	Migration ID
name	Name of the user who initiated the migration
startTime	The time when the migration was initiated
endTime	The time when the migration was complete
createdBy	Id of the entity that started the migration. For example, the Enterprise Control Room administrator
entities	List of entities migrated during migration process
migrationType	The migration type chosen - Role, User, or Bots and Schedules

9. Migration Progress

This API allows you to view the process of migration that is in progress.

1. Provide the "X-Authorization" and "Content Type" parameters in Headers.
2. Provide credential parameters in Body
3. Use the GET method to fetch object details by id using the endpoint http(s)://<hostname:port>/v2/migration/pogress

   For example, https://crdevenv.com:81/v2/migration/progress

4. Click Send.
5. The object details are listed successfully when the response status is 200
6. The details are shown in the Body data:

{

"migration":

{ "id": "10", "name": "2018.07.17.16.55.59.ellie.brown", "startTime": "2018-07-17T11:25:59.800Z", "endTime": "2018-07-17T11:26:16.002Z", "createdBy": "1", "migrationType": "BOT_EXCLUDE_MetaBot", "entities": [] },

"current": "SCHEDULE",

"progress":

{

"BOT": { "total": "10", "successful": "7", "failed": "0", "skipped": "3" },

"SCHEDULE": { "total": "8", "successful": "8", "failed": "0", "skipped": "0" }

}

}

Parameter description

Parameter	Description
id	Migration id
name	Migration name displayed
startTime	Timestamp when Migration process started
endTime	Timestamp when Migration process completed. Null when migration is in progress
createdBy	Id of the user who created/started the migration process
current	Type of entity currently being migrated - ROLE, USER, CREDENTIAL, BOT, or SCHEDULE]
progress	Progress of the entities - • total - total number of entities of specific type to be migrated • successful - number of entities out of total migrated successfully • failed - number of entities out of total failed to be migrated • skipped - number of entities out of total skipped during migration

10. Migration statistics - number of entities that succeeded / failed per migration

This API allows you to view the number of successful or failed entities per migration.

1. Provide the "X-Authorization" parameters in Headers.
2. Use the GET method to fetch object details by id using the endpoint http(s)://<hostname:port>/v2/migration/statistics

   For example, https://crdevenv.com:81/v2/migration/statistics

3. Click Send.
4. The object details are listed successfully when the response status is 200
5. The details are shown in the Body data:

   {

   "items": [

{ "id": "1", "name": "2018.07.13.11.14.59.ellie.brown", "startTime": "2018-07-13T05:44:59.787Z", "endTime": "2018-07-13T06:56:25.537Z", "createdBy": "1", "duration": "4285s", "numSuccess": 0, "numFailed": 0, "numSkipped": 0 },

{ "id": "2", "name": "2018.07.13.12.28.08.ellie.brown", "startTime": "2018-07-13T06:58:09.283Z", "endTime": "2018-07-13T06:58:12.910Z", "createdBy": "1", "duration": "3s", "numSuccess": 1, "numFailed": 1, "numSkipped": 0 },

{ "id": "3", "name": "2018.07.13.12.40.34.ellie.brown", "startTime": "2018-07-13T07:10:34.470Z", "endTime": "2018-07-13T07:10:40.060Z", "createdBy": "1", "duration": "5s", "numSuccess": 10, "numFailed": 0, "numSkipped": 0 },

{ "id": "4", "name": "2018.07.13.12.42.19.ellie.brown", "startTime": "2018-07-13T07:12:20.007Z", "endTime": "2018-07-13T07:12:23.107Z", "createdBy": "1", "duration": "3s", "numSuccess": 0, "numFailed": 0, "numSkipped": 6 },

{ "id": "5", "name": "2018.07.13.13.39.53.ellie.brown", "startTime": "2018-07-13T08:09:53.113Z", "endTime": "2018-07-13T08:10:02.673Z", "createdBy": "1", "duration": "9s", "numSuccess": 4, "numFailed": 0, "numSkipped": 0 }

]

}

Parameter description

Parameter	Description
id	migration id
name	Migration name displayed
startTime	Timestamp when Migration process started
endTime	Timestamp when Migration process completed. Null when migration is in progress
createdBy	Id of the user who created the object
duration	Duration of migration - seconds or nano seconds
numSuccess	Number of items successfully migrated
numFailed	Number of items that failed to migrate
numSkipped	Number of items that were skipped during migration

Post Migration process APIs

Use the Migration APIs after the process has completed to

1. Import files from the My Docs folder of 10.x Enterprise Control Room
2. Fetch the list of new or modified bots from 10.x Enterprise Control Room since last migration run
   Note: Before accessing the APIs you must first use the authentication API and pass it as a token to use a particular Migration API.

©2020 Automation Anywhere. All rights reserved.

3. Use the POST method to generate a token using the end point http(s)://<hostname:port>/v1/authentication. For this provide the Enterprise Control Room instance as Server Name /Hostname /IP and the Port number.

   For example,https://crdevenv.com:81/v1/authentication

4. Provide the following request payload in Headers

   "X-Authorization" : "Authorization token"

   "Content-Type" : "application/json"

5. Provide the following request payload in Body:

   {

   "username": "<Username>",

   "password": "<Password>"

   }

For example,

{

"usename": "Ellie.Brown",

"password": "12345678"

}

Important: When the error code 404 is shown while using any or all the post migration APIs, re-use the API to fetch the list of root folders from 10.x Enterprise Control Room i.e. http(s)://<hostname:port>/v1/migration/legacyrepository/rootDirectories.

A. Import files from My Docs folder

Use certain set of APIs to migrate files from the My Docs folder of the 10.x Enterprise Control Room. These APIs allow you to import large number of files that could either be used in bots as dependencies or though stand alone are useful for automation.

1. Fetch list of root folders from 10.x Enterprise Control Room

This API allows you to fetch the list of folders available in the 10.x Enterprise Control Room Repository. This will help you understand the folder structure that was available in the source Enterprise Control Room.

1. Provide the "X-Authorization" parameters in Headers.
2. Use the GET method to fetch object details by id using the endpoint http(s)://<hostname:port>/v1/migration/legacyrepository/rootDirectories followed by excludeMetaBot) parameter

   For example, https://crdevenv.com:81/v1/migration/legacyrepository/rootDirectories?excludeMetaBot=true

©2020 Automation Anywhere. All rights reserved.

3. Click Send
4. The object details are listed successfully when the response status is 200
5. The details are shown in the Body data:

[

{ "name": "My Docs", "path": "Automation Anywhere\\My Docs" },

{ "name": "My Exes", "path": "Automation Anywhere\\My Exes" },

{ "name": "My Reports", "path": "Automation Anywhere\\My Reports" },

{ "name": "My Scripts", "path": "Automation Anywhere\\My Scripts" },

{ "name": "My Tasks", "path": "Automation Anywhere\\My Tasks" },

{ "name": "My Workflow", "path": "Automation Anywhere\\My Workflow" }

]

Parameter description

Parameter	Description
name	Name of the directory/folder
path	Directory/folder path

2. Fetch list of sub-folders of a root-folder from 10.x Control Room

This API allows you to fetch the list of sub-folders for a given root-folder available in the 10.x Enterprise Control Room Repository. This will help you understand the folder structure of the source Enterprise Control Room.

1. Provide the "X-Authorization" parameters in Headers.
2. Use the GET method to fetch object details by id using the endpoint http(s)://<hostname:port>/v1/migration/legacyrepository/childDirectories followed by the path parameter

   For example, https://crdevenv.com:81/v1/migration/legacyrepository/childDirectories?path=Automation Anywhere\My Docs

3. Click Send.
4. The object details are listed successfully when the response status is 200
5. The details are shown in the Body data:

{

"folders":

[

{ "name": "Log-Files", "path": "Automation Anywhere\\My Docs\\Log-Files" }

]

}

Parameter Description

Parameter	Description
folders	List of sub directories
name	Name of the directory/folder
path	Directory/folder path

3. Fetch list of files in given folder

This API allows you to fetch the list of files available in a given folder in the source Enterprise Control Room repository.

1. Provide the "X-Authorization" parameters in Headers.
2. Use the GET method to fetch object details by id using the endpoint http(s)://<hostname:port>/v1/migration/legacyrepository/childFiles followed by the path) and excludeMetaBot) parameters

   For example, https://crdevenv.com:81/v1/migration/legacyrepository/childFiles?path=Automation Anywhere\My Docs\Log-Files&excludeMetaBot=false

3. Click Send
4. The object details are listed successfully when the response status is 200
5. The details are shown in the Body data:

{

"files":

[

{ "id": "280", "name": "ActiveMQServer-2018-Jul-17-2.log.zip", "path": "Automation Anywhere\\My Docs\\Log-Files\\ActiveMQServer-2018-Jul-17-2.log.zip" },

{ "id": "281", "name": "IgniteServer-2018-Jul-17-4.log.zip", "path": "Automation Anywhere\\My Docs\\Log-Files\\IgniteServer-2018-Jul-17-4.log.zip" },

{ "id": "283", "name": "WebCR_Ignite-2018-Jul-17-4.log.zip", "path": "Automation Anywhere\\My Docs\\Log-Files\\WebCR_Ignite-2018-Jul-17-4.log.zip" },

{ "id": "284", "name": "WebCR_License-2018-Jul-17-4.log.zip", "path": "Automation Anywhere\\My Docs\\Log-Files\\WebCR_License-2018-Jul-17-4.log.zip" },

{ "id": "292", "name": "WebCR_Migration-2018-Jul-17-4.log", "path": "Automation Anywhere\\My Docs\\Log-Files\\WebCR_Migration-2018-Jul-17-4.log" },

{ "id": "285", "name": "WebCR_Migration-2018-Jul-17-4.log.zip", "path": "Automation Anywhere\\My Docs\\Log-Files\\WebCR_Migration-2018-Jul-17-4.log.zip" },

©2020 Automation Anywhere. All rights reserved.

{ "id": "293", "name": "WebCR_Migration-2018-Jul-17-4.txt", "path": "Automation Anywhere\\My Docs\\Log-Files\\WebCR_Migration-2018-Jul-17-4.txt" }

]

}

Parameter Description

Parameter	Description
files	List of sub files
id	File id of the bot
name	Name of the directory/folder
path	Directory/folder path

4. Search for a folder by name in Enterprise Control Room 10.x

This API allows you to search for a folder by given name from the source Enterprise Control Room My Docs repository.

1. Provide the "X-Authorization" parameters in Headers.
2. Use the GET method to fetch object details by id using the endpoint http(s)://<hostname:port>/v1/migration/legacyrepository/folders followed by the taskName parameter

   For example, https://crdevenv.com:81/v1/migration/legacyrepository/folders?taskName=Import-Table

3. Click Send
4. The object details are listed successfully when the response status is 200
5. The details are shown in the Body data:

{

"paths":

["Automation Anywhere\\My Docs\\Import-Table"]

}

Parameter description

Parameter	Description
paths	List of Directory/folder path

5. Fetch list of files for a given folder in Enterprise Control Room 10.x

This API allows you to fetch a list of files from a given folder from the source Enterprise Control Room My Docs repository.

©2020 Automation Anywhere. All rights reserved.

1. Provide the "X-Authorization" parameters in Headers.
2. Use the POST method to fetch list of files for a given folder using the endpoint http(s)://<hostname:port>/v1/legacyrepository/files

   For example, https://crdevenv.com:81/v1/legacyrepository/files

3. Provide the list of folder paths as request payload in Body

   [

   "string"

   ]

   For example, the following lists the files available

   [

   "Automation Anywhere\\My Docs\\Import-Table"

   ]

4. Click Send
5. The object details are listed successfully when the response status is 200
6. The Response details are shown in the Body data:

   {

   "files":

   [

   { "id": 1281, "type": "BOT", "sourceId": "1281", "targetId": 0, "name": "Automation Anywhere\\My Docs\\Import-Table\\Import-Table.txt", "status": "SUCCESS", "reason": "" },

   { "id": 293, "type": "BOT", "sourceId": "293", "targetId": 0, "name": "Automation Anywhere\\My Docs\\Import-Table\\WebCR_Migration-2018-Jul-17-4.txt", "status": "SUCCESS", "reason": "" }

   ]

   }

Parameter Description

Parameter	Description
files	List of sub files
type	file type
sourceId	Id of entity in the source database
targetId	Id of entity after migration in the target database
name	Name of the directory/folder

©2020 Automation Anywhere. All rights reserved.

Parameter	Description
status	Status of response - SUCCESS, SKIPPED, or FAILED
reason	Description for the reason of status FAILED or SKIPPED

B. Migrate new or modified bots from 10.x since the last migration in 11.x

This API allows you to fetch list of bots that are new or modified in source Enterprise Control Room version 10.x after data has already been migrated to destination Enterprise Control Room version 11.x . Essentially, this API allows you the liberty to continue using your 10.x environment whilst the 11.x environment is ready to go into production.

1. Provide the "X-Authorization" parameters in Headers.
2. Use the POST method to fetch object details by id using the endpoint http(s)://<hostname:port>/v1/legacyrepository/changedfiles

   For example, https://crdevenv.com:81/v1/legacyrepository/changedfiles

3. Provide the list of folder paths as request payload in Body

   {

   "changeSince": "<last migration date and time>"

   }

   For example, the following lists the bot names that were update post migration

   {

   "changeSince":"2018-06-25T12:05:00+05:30"

   }

   Tip: Do not specify the changeSince parameter to consider the delta for last migration date and time.
4. Click Send.
5. The object details are listed successfully when the response status is 200
6. The Response details are shown in the Body data:

   {

   "changedfiles":

   [

   { "type": "BOT", "sourceId": "6", "name": "Automation Anywhere\\My Tasks\\Sample Tasks\\Import-Table.atmx" },

   { "type": "BOT", "sourceId": "7", "name": "Automation Anywhere\\My Tasks\\Sample Tasks\\List-Variable.atmx" }

   ]

©2020 Automation Anywhere. All rights reserved.

```
}
```

Parameter description

Parameter	Description
changedFiles	List of entities that were changed or are new since last migration run
type	entity type
sourceId	Id of entity in the source database
name	Name of the directory/folder

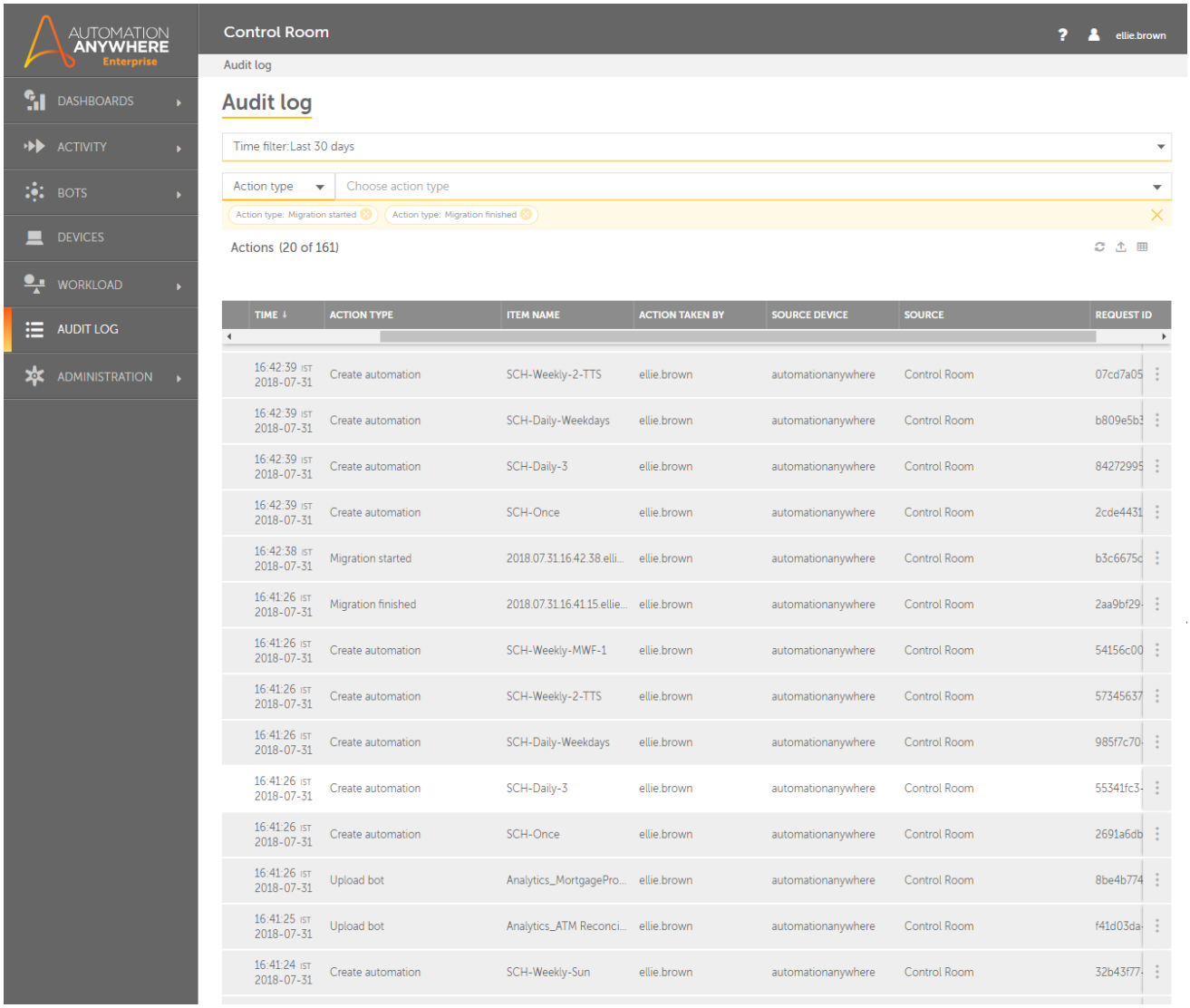
API Response Codes

Http(s) Status code	Response - Description	Corrective Action
200	Successful operation	NA
400	Bad request	Retry with valid parameters
401	Authentication required	Retry by providing authentication parameters
403	Unauthorized access	Ensure you have appropriate permissions to perform this operation
404	Not found	Ensure the requested data is present in Enterprise Control Room
409	Conflict	Ensure the parameters provided are correct
500	Internal server error	Ensure the server is up and running
501	Permission error	Ensure that you have the required permission

Audit Logs

The Audit Log displays individual entry for each entity that is migrated.

©2020 Automation Anywhere. All rights reserved.



When the migration process is initiated, a Migration started entry is logged in Audit log. Similarly when the migration process is completed, a Migration finished entry is logged. Between these two entries, migration entries are logged for each entity that is migrated such as Create, Update, or Upload operation.

Click to view details of the process.

API to add and remove manual dependencies

Use the Manual Dependencies API to manually add and remove dependent files to/from a TaskBot from My Docs, My Exes, and My Scripts folders in the repository.

As a Enterprise Control Room administrator or a user with View and Manage Scheduled Activity permission, you can manage dependencies manually. The Manual Dependencies APIs allow you to,

1. Add dependent files to a parent TaskBot
2. Remove dependent files from a parent TaskBot

©2020 Automation Anywhere. All rights reserved.

Note: The examples provided in this article are for reference only.

Before accessing the Dependencies API's you must first use the authentication API and pass it as a token to use a particular API.

1. Use the POST method to generate a token using the end point http(s)://<hostname:port>/v1/authentication. For this provide the Enterprise Control Room instance as Server Name /Hostname /IP and the Port number.

   For example, `https://crdevenv.com:81/v1/authentication`

2. Provide the following request payload in Headers

   "X-Authorization" : "Authorization token"

   "Content-Type" : "application/json"

3. Provide the following request payload in Body:

   {

   "username": "<Username>",

   "password": "<Password>"

   }

   For example,

   {

   "usename": "Ellie.Brown",

   "password": "12345678"

   }

API to add dependent files

Use this API to add files to a parent TaskBot for run and deploy automation successfully.

API end point

Use the following end point to access the APIs:

<Enterprise Control Room URL>/v1/files/manualdependencies/add

For example,

https://crdevenv.com:81/v1/files/manualdependencies/add

1. Provide the "X-Authorization" and "Content Type" parameters in Headers.

©2020 Automation Anywhere. All rights reserved.

2. Use the Deployment API to fetch the list of files available in the repository. See Bot Execution Orchestrator API.
3. Use the POST method to provide the file ids as request payload in Body:

```
{
"id": <parent file id>,
"child_ids": [ <dependent file id 1>, <dependent file id 2> ]
}
```

For example, the following adds the dependent files with ids <...> for the TaskBot with id <..>:

```
{
"id":10
"child_ids":[18, 19]
}
```

4. Click Send
5. The action is successful when the response status is 200.
6. You can view the response in the Body data.

Parameter Description

Parameter	Description
id	parent file id
child_ids	Collection of child manual dependency ids.

API to remove dependent files

Use this API to remove dependent files from a parent TaskBot.

API end point

Use the following end point to access the APIs:

<Enterprise Control Room URL>/v1/files/manualdependencies/remove

For example, https://crdevenv.com:81/manualdependencies/remove

1. Provide the "X-Authorization" and "Content Type" parameters in Headers.
2. Use the DELETE method to provide the following request payload in Body:

```
{
"id": 0,
```

```
  "child_ids": 0
  }
```

For example,the following removes/deletes the dependent files with ids <...> for the TaskBot with id <..>:

```
  {
  "id":
  "child_ids":
 }
```

3. Click Send
4. The action is successful when the response status is 200
5. You can view the response in the Body data.

Parameter Description

Parameter	Description
id	parent file id
child_ids	Collection of child manual dependency ids.

License API

Request detailed license information for your Enterprise Control Room installed licenses.

Prerequisites

JSON Web Token (JWT)
: All Enterprise Control Room APIs require a JSON Web Token (JWT) to access the APIs. Generate an authentication token using the Authentication API. Apply the token to each API you are going to execute.

Roles and licenses
: You need to authenticate with a user that has the following permissions:

  View licenses
  : Manage user's device licenses
  : Install licenses

  Note: Administrator users have these permissions by default. Create a custom role to assign to non-administrator users to allow them to be able to view license information.

- URL: `http://<your_control_room_url>/v2/license`
- Method: GET

©2020 Automation Anywhere. All rights reserved.

Procedure

1. Add an authentication token to the request header.
   Note: Use the Authentication API to generate a JSON Web Token (JWT). Authenticate with a user that has the required roles and licenses.
   In Swagger:
   a) Click Authorize and add the JWT to the Value field.
   b) Click Authorize then click Close

   In a REST client: Create a custom header named X-Authorization with the JWT as the Attribute Value.

2. Go to the License API URL. `.../v2/license`
   In Swagger:
   a) Click Try it out.
   b) Click Execute.
   In a REST client:
   a) Enter the License API URL in the URL field.

   ```
   http://<your_control_room_url>/v2/license
   ```

   b) Select the GET method.
   c) Click SEND.
   Response body:


```
{
  "licenseType": "PURCHASED",
  "installedBy": 1,
  "installationDate": "2019-11-12T07:18:17.247Z",
  "expirationDate": "2020-05-10T23:59:59.999999999Z",
  "products": [
    {
      "id": 1,
      "name": "CONTROLROOM",
      "version": "11.3.4.0",
      "features": [
        {
          "id": 2,
          "name": "UNATTENDED_BOTRUNNER",
          "enable": true,
          "purchasedCount": 5,
          "usedCount": 1,
          "licenseCountUnit": "NUMBER",
          "licenseModel": "FLOATING"
```

```
        },
        {
          "id": 1,
          "name": "BOT_CREATOR",
          "enable": true,
          "purchasedCount": 10,
          "usedCount": 0,
          "licenseCountUnit": "NUMBER",
          "licenseModel": "FLOATING"
        },
        {
          "id": 7,
          "name": "ATTENDED_BOTRUNNER",
          "enable": true,
          "purchasedCount": 0,
          "usedCount": 0,
          "licenseCountUnit": "NUMBER",
          "licenseModel": "FLOATING"
        }
      ]
    },
    {
      "id": 2,
      "name": "ANALYTICS",
      "version": "11.3.4.0",
      "features": [
        {
          "id": 5,
          "name": "ANALYTICS_API",
          "enable": false,
          "purchasedCount": 0,
          "usedCount": 0,
          "licenseCountUnit": "NUMBER",
          "licenseModel": "NONE"
        },
        {
```


©2020 Automation Anywhere. All rights reserved.

```
          "id": 4,
          "name": "ANALYTICS_CLIENT",
          "enable": false,
          "purchasedCount": 0,
          "usedCount": 0,
          "licenseCountUnit": "NUMBER",
          "licenseModel": "NONE"
        }
      ]
    },
    {
      "id": 4,
      "name": "COGNITIVE",
      "version": "",
      "features": [
        {
          "id": 3,
          "name": "IQBOT_RUNNER",
          "enable": false,
          "purchasedCount": 0,
          "usedCount": 0,
          "licenseCountUnit": "NUMBER",
          "licenseModel": "NONE"
        },
        {
          "id": 8,
          "name": "IQBOT_PAGES",
          "enable": false,
          "purchasedCount": 0,
          "usedCount": 0,
          "licenseCountUnit": "NUMBER",
          "licenseModel": "NONE"
        }
      ]
    },
    {
```


©2020 Automation Anywhere. All rights reserved.

```
      "id": 3,
      "name": "BOTFARM",
      "version": "",
      "features": [
        {
          "id": 6,
          "name": "BOTFARM_RUNNER",
          "enable": false,
          "purchasedCount": 0,
          "usedCount": 0,
          "licenseCountUnit": "SECONDS",
          "licenseModel": "HOURLY"
        }
      ]
    }
  ]
}
```


Response header:

```
cache-control: no-cache, no-store, max-age=0, must-revalidate
content-length: 1474
content-security-policy: default-src 'self'
content-type: application/json
date: Wed, 13 Nov 2019 10:33:56 GMT
expires: 0
pragma: no-cache
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
x-xss-protection: 1; mode=block
```

Next steps

You can also use c URL in a command or terminal window to make this API request.

```
curl -X GET "http://<your_control_room_url>/v2/license" -H "accept: application
/json" -H "X-Authorization: eyJhbGciOiJSUzUxMiJ9.eyJzdWIiOiIxOCIsImNsaWVudFR5cG
UiOiJXRUIiLCJsaWNlbnNlcyI6WyJERVZFTE9QTUVOVCJdLCJhbmFseXRpY3NMaWNlbnNlc1B1cmNoY
```

```
XNlZCI6eyJBbmFseXRpY3NDbGllbnQiOnRydWUsIkFuYWx5dGljc0FQSSI6dHJ1ZX0sImlhdCI6MTU3
MzY0MTIxOCwiZXhwIjoxNTczNjQyNDE4LCJpc3MiOiJBdXRvbWF0aW9uQW55d2hlcmUiLCJuYW5vVGl
tZSI6NDE5MDkwNzU3ODk4MjIwMCwiY3NyZlRva2VuIjoiN2YxNDJiODQ3OGRhY2MzYzUzNjFiNzQwNT
ljOTFjMmYifQ.b5FECqRdLb4tOWrScYSGwydJ2kHdx4XX_9LYQjKX-taOynEE0P1KozHrYEsqERMQFK
NTdUWnkKzHfXHWJ63IVzsSamSRLxWTWF0LiVkrrrdSA5mOtBJd3AdVC2Zxk828T2DGKX7O4U-kzSos-
LM9Hcx6gug86BWPubjuHbH5RZKUgXVYujcHIpw_2sPfQFHjHdvZWb2HwuTeTm_xxiTRS4LFOwoGh3lZ
dmOZ8ckmGQCkB-bX28a4dfyLCPBAB9XDYGKJ70IeQRgx4mhYVJ2g228iSe8GPWYcg2RiwedawP_vxy6
VLY6EDqUB7nbt5GuWf6W174S_AQei4LVYRQvsPQ"
```


Related concepts
Enterprise Control Room APIs

Repository Management API overview

Use the Repository Management API to programmatically delete a file, retrieve bot variables, return a list of files and folders in a folder, and search for files and folders in your Enterprise Control Room.

Repository URLs

Search for folders and files in your Enterprise Control Room repository

```
POST http://<your_control_room_url>/v1/repository/filefolder/list
```

Body parameters: This request body example includes filters, sorting, and page control to refine the response.

```
{
  "filter": {
    "operator": "NONE",
    "operands": [
      null
    ],
    "field": "string",
    "value": "string"
  },
  "sort": [
    {
      "field": "string",
      "direction": "asc"
    }
```

©2020 Automation Anywhere. All rights reserved.

```
  ],
  "page": {
    "offset": 0,
    "length": 0
  }
}
```

Filters allow you to refine what is returned in the response body. Read more about filters in Filters in an API request body.

Note: You can filter by the following fields: parentId, path, name, lastModified, and directory.
See Use filters to list specific files.

Return a list of folders and files in a directory

```
POST http://<your_control_room_url>/v1/repository/directories/{directoryid
}/files/list
```

URL parameter:

`.../directories/{directoryid}/files/list...`: The numeric value that identifies the directory position.

Body parameters: This request body example includes filters, sorting, and page control to refine the response.

```
{
  "filter": {
    "operator": "NONE",
    "operands": [
      null
    ],
    "field": "string",
    "value": "string"
  },
  "sort": [
    {
      "field": "string",
      "direction": "asc"
    }
  ],
  "page": {
```

```
    "offset": 0,
    "length": 0
  }
}
```

Filters allow you to refine what is returned in the response body. Read more about filters in Filters in an API request body.

Note: You can filter by the following fields: parentId, path, name, lastModified, and directory.
See Use filters to list bots from a specific folder.

Delete a repository file

```
DELETE http://<your_control_room_url>/v1/repository/files/{aafileid}
```

URL parameter:

`.../files/{aafileid}...`: The numeric value that identifies the file.

Note: You cannot delete folders with an ID less than 9.

See Delete a file from the repository.

Retrieve a list of bot variables

```
GET http://<your_control_room_url>/v1/repository/file/{fileId}/variables/{
fileVersion}
```

URL parameter:

`.../file/{fileId}/variables/{fileVersion}...`: The numeric value in `{fileId}` that identifies the file and the string in `{fileVersion}` that specifies the version. The file version can either be latest or production. The default value is latest.

Note: This endpoint can only retrieve string, list, and array variables.
See Retrieve a list of variables.

Delete a file from the repository

Send a Delete request to remove a file from the Enterprise Control Room repository.

Prerequisites

JSON Web Token (JWT)

All Enterprise Control Room APIs require a JSON Web Token (JWT) to access the APIs. Generate an authentication token using the Authentication API.

©2020 Automation Anywhere. All rights reserved.

Permissions
: You must have Delete permission for the folder you want to delete. If you can delete from the Enterprise Control Room interface, you can delete using this API.

  See Bot Permissions for a Role.

Note:

- Use the Swagger definition files installed with your Enterprise Control Room to test the APIs. View the available Swagger APIs at `http://<your_control_room_url>/swagger/`.
- You can also use a REST client to complete this task.

Procedure

1. Add an authentication token to the request header.
   Note: Use the Authentication API to generate a JSON Web Token.
2. Select Delete as the method.
3. In the URL, add the id for the file you are deleting.
   URL example:

   ```
   http://<your_control_room_url>/v1/repository/files/20
   ```

4. Send the request.
   - In a REST Client, click SEND.
   - In the Swagger interface, click Execute.

   Response body:

   ```
   OK
   ```

Retrieve a list of variables

Send a GET request to retrieve the string, list, and array variables used in a specific file.

Prerequisites

JSON Web Token (JWT)
: All Enterprise Control Room APIs require a JSON Web Token (JWT) to access the APIs. Generate an authentication token using the Authentication API.

Permissions
: You must have permission for the folder in which you want to perform operations. If you can view bot details in the Enterprise Control Room interface, then you can use this API.

  See Bot Permissions for a Role.

Note:

- Use the Swagger definition files installed with your Enterprise Control Room to test the APIs. View the available Swagger APIs at `http://<your_control_room_url>/swagger/`.
- You can also use a REST client to complete this task.

©2020 Automation Anywhere. All rights reserved.

Procedure

1. Add an authentication token to the request header.
   Note: Use the Authentication API to generate a JSON Web Token.
2. Select GET as the method.
3. In the URL, add the id and the File version for the file from which you are extracting variables.
   The File version can either be latest or production. The default value is latest.
   URL example:

   ```
   http://<your_control_room_url>/v1/repository/file/12/variables/latest
   ```

4. Send the request.
   - In a REST Client, click SEND.
   - In the Swagger interface, click Execute.

   Response body:

   ```
   {
     "botVariables": {
       "stringValue": {
         "string": "xyz"
       },
       "listValues": {
         "list": [a, b, c, d]
       }
     }
   }
   ```

Note: You can also run REST requests from a command terminal. The following is a curl request example. This example is formatted for readability. Replace the text inside the angle brackets, `<authentication_token>`, with your authentication token.

```
curl -X GET "http://<your_control_room_url>/v1/repository/file/12/variables/latest"
                    -H "accept: application/json" -H "X-Authorization: <authentication_token>"
```

Use filters to list specific files

This example shows how to send a POST request with filters to return all the bots from your repository that meet the search criteria. In this example, you have bots in several folders that contain the word `test`. Use the filters to return only the bots with `test` in the name.

©2020 Automation Anywhere. All rights reserved.

Prerequisites

JSON Web Token (JWT)
: All Enterprise Control Room APIs require a JSON Web Token (JWT) to access the APIs. Generate an authentication token using the Authentication API.

Permissions
: You must have permission for the folder in which you want to perform operations. If you can view files in the Enterprise Control Room interface, then you can use this API.

  See Bot Permissions for a Role.

Note:

- Use the Swagger definition files installed with your Enterprise Control Room to test the APIs. View the available Swagger APIs at `http://<your_control_room_url>/swagger/`.
- You can also use a REST client to complete this task.

Procedure

1. Add an authentication token to the request header.
   Note: Use the Authentication API to generate a JSON Web Token.
2. Specify the method and URL.
   - Method: POST
   - URL: `http://<your_control_room_url>/v1/repository/filefolder/list`
3. Add filter parameters in the request body.
   - Sort by `parentid` to return the results in order of the parent folder.
   - Filter by the "test" substring in the name field to return all bots containing the word `test` in the name.

   Request body:

```
{
  "sort":[{
    "field":"parentid",
    "direction":"asc"
  }],
  "filter":{
    "operator":"substring",
    "value":"test",
    "field":"name"
    },
  "fields":[],
  "page":{ }
}
```

4. Send the request.
   - In a REST Client, click SEND.

©2020 Automation Anywhere. All rights reserved.

- In the Swagger interface, click Execute.

Response body: The response for this example returns three bots from the repository: one from the My Tasks folder, and two from the Finance subfolder.


```
{
  "page": {
    "offset": 0,
    "total": 7,
    "totalFilter": 3
  },
  "list": [
    {
      "id": "14",
      "parentid": "7",
      "name": "testOnboarding.atmx",
      "permission": {
        "delete": false,
        "download": true,
        "execute": false,
        "upload": true,
        "run": false
      },
      "lastModified": "2019-12-02T17:39:05.339Z",
      "lastModifiedBy": "19",
      "path": "Automation Anywhere\\My Tasks\\testOnboarding.atmx",
      "directory": false,
      "size": 4602,
      "locked": false,
      "fileLastModified": "2019-12-02T17:38:56Z",
      "isProtected": false
    },
    {
      "id": "17",
      "parentid": "14",
      "name": "testInvoiceCompare.atmx",
      "permission": {
        "delete": false,
```

```
        "download": true,
        "execute": false,
        "upload": true,
        "run": false
      },
      "lastModified": "2019-12-02T17:39:05.339Z",
      "lastModifiedBy": "19",
      "path": "Automation Anywhere\\My Tasks\\Finance\\testInvoiceCompare.
atmx",
      "directory": false,
      "size": 4408,
      "locked": false,
      "fileLastModified": "2019-12-02T17:38:56Z",
      "isProtected": false
    },
    {
      "id": "18",
      "parentid": "14",
      "name": "testQuarterlyReport.atmx",
      "permission": {
        "delete": false,
        "download": true,
        "execute": false,
        "upload": true,
        "run": false
      },
      "lastModified": "2019-12-02T17:39:05.339Z",
      "lastModifiedBy": "19",
      "path": "Automation Anywhere\\My Tasks\\Finance\\testQuarterlyReport
.atmx",
      "directory": false,
      "size": 4408,
      "locked": false,
      "fileLastModified": "2019-12-02T17:38:56Z",
      "isProtected": false
    }
```


©2020 Automation Anywhere. All rights reserved.

```
  ]
}
```

Note: You can also run REST requests from a command terminal. The following is a curl request example. This example is formatted for readability. Replace the text inside the angle brackets, `<authentication_token>`, with your authentication token.

```
curl -X POST "<your_control_room_url>/v1/repository/filefolder/list" -H "accept
: application/json"
        -H "X-Authorization: <authentication_token>" -H "Content-Type: applicat
ion/json"
        -d "{
            \"sort\": [ {
                \"field\": \"parentid\",
                \"direction\": \"asc\"
            } ],
            \"filter\": {
                \"operator\": \"substring\",
                \"value\": \"test\",
                \"field\": \"name\" },
            \"fields\": [],
            \"page\": { }
            }"
```

Use filters to list bots from a specific folder

This example shows how to send a POST request with filters to list specific bots. In this example, you have a folder that contains bots from several departments. Use the filters to return only the bots with `finance` in the name.

Prerequisites

JSON Web Token (JWT)
: All Enterprise Control Room APIs require a JSON Web Token (JWT) to access the APIs. Generate an authentication token using the Authentication API.

Permissions
: You must have permission for the folder in which you want to perform operations. If you can view bots in the Enterprise Control Room interface, then you can use this API.

  See Bot Permissions for a Role.

Note:

- Use the Swagger definition files installed with your Enterprise Control Room to test the APIs. View the available Swagger APIs at `http://<your_control_room_url>/swagger/`.
- You can also use a REST client to complete this task.

Procedure

1. Add an authentication token to the request header.
   Note: Use the Authentication API to generate a JSON Web Token.
2. Specify the method and URL.
   - Method: POST
   - URL: `http://<your_control_room_url>/v1/repository/directories/14/files/list`

     The example URL specifies a subfolder of the My Tasks folder.
3. Add filter parameters in the request body.
   - Sort by name to return the results in alphabetical order.
   - Filter by the "finance" substring in the name field to return all bots containing `finance` in the name.

   Request body:

```
{
  "sort":[{
    "field":"name",
    "direction":"asc"
  }],
  "filter":{
    "operator":"substring",
    "value":"finance",
    "field":"name"
    },
  "fields":[],
  "page":{ }
}
```

4. Send the request.
   - In a REST Client, click SEND.
   - In the Swagger interface, click Execute.

   Response body: The response for this example returns information on the three bots that contain the word `finance` in their names.

```
{
  "page": {
```

```
    "offset": 0,
    "total": 6,
    "totalFilter": 3
  },
  "list": [
    {
      "id": "27",
      "parentId": "14",
      "name": "finance-new-vendor.atmx",
      "permission": {
        "delete": false,
        "download": true,
        "execute": false,
        "upload": true,
        "run": false
      },
      "lastModified": "2019-12-02T17:39:05.339Z",
      "lastModifiedBy": "19",
      "path": "Automation Anywhere\\My Tasks\\Q2\\finance-new-vendor.atmx"
,
      "directory": false,
      "size": "4602",
      "locked": false,
      "fileLastModified": "2019-12-02T17:38:56Z",
      "isProtected": false
    },
    {
      "id": "31",
      "parentId": "14",
      "name": "financeGenerateInvoice.atmx",
      "permission": {
        "delete": false,
        "download": true,
        "execute": false,
        "upload": true,
        "run": false
```

```
      },
      "lastModified": "2019-12-02T17:39:05.339Z",
      "lastModifiedBy": "19",
      "path": "Automation Anywhere\\My Tasks\\Q2\\financeGenerateInvoice.a
tmx",
      "directory": false,
      "size": "5060",
      "locked": false,
      "fileLastModified": "2019-12-02T17:38:56Z",
      "isProtected": false
    },
    {
      "id": "22",
      "parentId": "14",
      "name": "onboardingFinanceOrg.atmx",
      "permission": {
        "delete": false,
        "download": true,
        "execute": false,
        "upload": true,
        "run": false
      },
      "lastModified": "2019-12-02T17:39:05.339Z",
      "lastModifiedBy": "19",
      "path": "Automation Anywhere\\My Tasks\\Q2\\onboardingFinanceOrg.atm
x",
      "directory": false,
      "size": "3910",
      "locked": false,
      "fileLastModified": "2019-12-02T17:38:56Z",
      "isProtected": false
    }
  ]
}
```


©2020 Automation Anywhere. All rights reserved.

Note: You can also run REST requests from a command terminal. The following is a curl request example. This example is formatted for readability. Replace the text inside the angle brackets, `<authentication_token>`, with your authentication token.

```
curl -X POST "<your_control_room_url>/v1/repository/directories/14/files/list"
     -H "accept: application/json" -H "X-Authorization: <authentication_token>"
     -H "Content-Type: application/json" -d "{
     \"fields\": [ ],
     \"filter\": {
        \"operator\": \"substring\",
        \"field\": \"name\",
        \"value\": \"finance\"
        },
    \"sort\": [ {
        \"field\": \"name\",
        \"direction\": \"asc\"
    } ]
}"
```

User management API overview

Use the User Management APIs to create, search, update, or delete roles and users in your .

User Management Roles

The Role and User APIs are available to create and manage roles and users. Use the links in the following sections to compose an API request and receive a response. You can use the APIs in any order you want. The order that is presented below is as shown in the Automation Anywhere Swagger interface.

Role APIs

Use Role APIs to create a role, search for roles, retrieve a specific role using an object ID, update a role, or delete a role.

Create a new role

Creates a new role with a new role name.

```
POST http://<your_control_room_url>/v1/usermanagement/roles
```

See Create a new role.

©2020 Automation Anywhere. All rights reserved.

Search for roles
: Retrieves all roles based on search criteria, such as filtering, sorting, and pagination.

```
POST http://<your_control_room_url>/v1/usermanagement/roles/list
```

See Search for roles.

Retrieve a role
: Retrieves a specific role based on a unique role ID.

```
GET http://<your_control_room_url>/v1/usermanagement/roles/{id}
```

See Retrieve a specific role.

Update a role
: Modifies an existing role name based on a unique role ID.

```
PUT http://<your_control_room_url>/v1/usermanagement/roles/{id}
```

See Update an existing role.

Delete a role
: Deletes an existing role based on a unique role ID.

```
DELETE http://<your_control_room_url>/v1/usermanagement/roles/{id}
```

See Delete an existing role.

User APIs

Use User APIs to create a user, search for users, retrieve a user, update a user, or delete a user.

Create a new user
: Creates a user with a new user name.

```
POST http://<your_control_room_url>/v1/usermanagement/users
```

See Create a new user.

Search for users
: Retrieves current logged-in users based on search criteria, such as filtering, sorting, and pagination.

```
POST http://<your_control_room_url>/v1/usermanagement/users/list
```

See Search for users.

©2020 Automation Anywhere. All rights reserved.

Retrieve a user
: Retrieves user details based on a unique user ID.

```
GET http://<your_control_room_url>/v1/usermanagement/users/{id}
```

See Retrieve a specific user.

Update a user
: Modifies an existing user name based on a unique user ID.

```
PUT http://<your_control_room_url>/v1/usermanagement/users/{id}
```

See Update an existing user.

Delete a user
: Deletes an existing user based on a unique user ID.

```
DELETE http://<your_control_room_url>/v1/usermanagement/users/{id}
```

See Delete an existing user.

Related concepts
Roles overview
Related tasks
Search for users
Search for roles

Create a new role

Use Create New RoleAPI to create a new role with permissions in the Enterprise Control Room.

Prerequisites

View and Manage Roles
: Users who have `view and manage roles` permissions can view, create, and manage roles.

JSON Web Token (JWT)
: All Enterprise Control Room APIs require a JSON Web Token (JWT) to access the APIs. Generate an authentication token using the Authentication API. See Authentication API.

- URL: `http://<your_control_room_url>/v1/usermanagement/roles`

  Replace the content in the angle brackets with your Enterprise Control Room URL.

- Method: POST.
- Use the Swagger definition files installed with your Enterprise Control Room to test the APIs. View the available Swagger APIs at: `http://<your_control_room_url>/swagger/`.
- You can also use a REST client to complete this task.

©2020 Automation Anywhere. All rights reserved.

Procedure

1. Add an authentication token to the request header.
   Use the Authentication API to generate a JSON Web Token. See Authentication API.
2. Select POST as the method.
   `POST http://<your_control_room_url>/v1/usermanagement/roles`
3. In the request body, enter a new name for the role.
4. Send the request.

Parameter name	Mandatory	Type	Description
Name	Yes	String (255 max)	Role Name
Description	No	String (255 max)	Role description

The following request creates a new role with the following permissions: ID, action, and the resourceType.

Request body:

```
{
  "name": "User-Role-Management",
  "description": "",
  "permissions": [
    {
      "id": 58,
      "action": "myschedule",
      "resourceType": "taskscheduling",
      "resourceId": null
    },
    {
      "id": 59,
      "action": "managecredentials",
      "resourceType": "credentials",
      "resourceId": null
    },
    {
      "id": 30,
      "action": "view",
      "resourceType": "devices",
      "resourceId": null
    },
    {
```

©2020 Automation Anywhere. All rights reserved.

```
      "id": 97,
      "action": "viewbotstore",
      "resourceType": "botstore",
      "resourceId": null
    },
    {
      "id": 102,
      "action": "viewuserbasic",
      "resourceType": "usermanagement",
      "resourceId": null
    },
    {
      "id": 3,
      "action": "createuser",
      "resourceType": "usermanagement",
      "resourceId": null
    },
    {
      "id": 4,
      "action": "updateuser",
      "resourceType": "usermanagement",
      "resourceId": null
    },
    {
      "id": 2,
      "action": "deleteuser",
      "resourceType": "usermanagement",
      "resourceId": null
    },
    {
      "id": 1,
      "action": "usermanagement",
      "resourceType": "usermanagement",
      "resourceId": null
    },
    {
```


©2020 Automation Anywhere. All rights reserved.

```
      "id": 12,
      "action": "rolesmanagement",
      "resourceType": "rolesmanagement",
      "resourceId": null
    },
    {
      "id": 90,
      "action": "rolesview",
      "resourceType": "rolesmanagement",
      "resourceId": null
    }
  ],
  "principals": []
}
```


5. Send the request.
   - In Swagger, click Execute.
   - In a REST client, click SEND.

   Response body:


```
{
  "id": 42,
  "createdBy": 36,
  "createdOn": "2019-12-26T19:51:24Z",
  "updatedBy": 36,
  "updatedOn": "2019-12-26T19:51:24Z",
  "tenantId": 1,
  "version": 0,
  "status": "Active",
  "description": "",
  "name": "User-Role-Management",
  "accessRestriction": null,
  "permissions": [{
    "id": 1,
    "createdBy": 0,
    "createdOn": "2019-10-03T23:53:35Z",
    "updatedBy": 0,
    "updatedOn": "2019-10-03T23:53:35Z",
```


©2020 Automation Anywhere. All rights reserved.

```
    "tenantId": 1,
    "version": 0,
    "status": null,
    "action": "usermanagement",
    "resourceId": null,
    "resourceType": "usermanagement"
  }, {
    "id": 59,
    "createdBy": 0,
    "createdOn": "2019-10-03T23:53:47Z",
    "updatedBy": 0,
    "updatedOn": "2019-10-03T23:53:47Z",
    "tenantId": 1,
    "version": 0,
    "status": null,
    "action": "managecredentials",
    "resourceId": null,
    "resourceType": "credentials"
  }, {
    "id": 2,
    "createdBy": 0,
    "createdOn": "2019-10-03T23:53:35Z",
    "updatedBy": 0,
    "updatedOn": "2019-10-03T23:53:35Z",
    "tenantId": 1,
    "version": 0,
    "status": null,
    "action": "deleteuser",
    "resourceId": null,
    "resourceType": "usermanagement"
  }, {
    "id": 4,
    "createdBy": 0,
    "createdOn": "2019-10-03T23:53:35Z",
    "updatedBy": 0,
    "updatedOn": "2019-10-03T23:53:35Z",
```


©2020 Automation Anywhere. All rights reserved.

```
    "tenantId": 1,
    "version": 0,
    "status": null,
    "action": "updateuser",
    "resourceId": null,
    "resourceType": "usermanagement"
  }, {
    "id": 12,
    "createdBy": 0,
    "createdOn": "2019-10-03T23:53:35Z",
    "updatedBy": 0,
    "updatedOn": "2019-10-03T23:53:35Z",
    "tenantId": 1,
    "version": 0,
    "status": null,
    "action": "rolesmanagement",
    "resourceId": null,
    "resourceType": "rolesmanagement"
  }, {
    "id": 90,
    "createdBy": 0,
    "createdOn": "2019-10-03T23:54:11Z",
    "updatedBy": 0,
    "updatedOn": "2019-10-03T23:54:11Z",
    "tenantId": 1,
    "version": 0,
    "status": null,
    "action": "rolesview",
    "resourceId": null,
    "resourceType": "rolesmanagement"
  }, {
    "id": 58,
    "createdBy": 0,
    "createdOn": "2019-10-03T23:53:47Z",
    "updatedBy": 0,
    "updatedOn": "2019-10-03T23:53:47Z",
```


©2020 Automation Anywhere. All rights reserved.

```
    "tenantId": 1,
    "version": 0,
    "status": null,
    "action": "myschedule",
    "resourceId": null,
    "resourceType": "taskscheduling"
  }, {
    "id": 3,
    "createdBy": 0,
    "createdOn": "2019-10-03T23:53:35Z",
    "updatedBy": 0,
    "updatedOn": "2019-10-03T23:53:35Z",
    "tenantId": 1,
    "version": 0,
    "status": null,
    "action": "createuser",
    "resourceId": null,
    "resourceType": "usermanagement"
  }, {
    "id": 97,
    "createdBy": 0,
    "createdOn": "2019-10-03T23:54:12Z",
    "updatedBy": 0,
    "updatedOn": "2019-10-03T23:54:12Z",
    "tenantId": 1,
    "version": 0,
    "status": null,
    "action": "viewbotstore",
    "resourceId": null,
    "resourceType": "botstore"
  }, {
    "id": 30,
    "createdBy": 0,
    "createdOn": "2019-10-03T23:53:37Z",
    "updatedBy": 0,
    "updatedOn": "2019-10-03T23:53:37Z",
```


©2020 Automation Anywhere. All rights reserved.

```
      "tenantId": 1,
      "version": 0,
      "status": null,
      "action": "view",
      "resourceId": null,
      "resourceType": "devices"
    }, {
      "id": 102,
      "createdBy": 0,
      "createdOn": "2019-11-21T19:08:20Z",
      "updatedBy": 0,
      "updatedOn": "2019-11-21T19:08:20Z",
      "tenantId": 1,
      "version": 0,
      "status": "Active",
      "action": "runtimeclientsmanagement",
      "resourceId": "2",
      "resourceType": "runtimeclientsmanagement"
    }],
    "countPrincipals": 0,
    "principals": []
  }
```


Note: You can also run REST requests from a command terminal. The following is a curl request example. This example is formatted for readability. Replace the text inside the angle brackets, `<authentication_token>`, with your authentication token.

```
curl -X POST "http://<your_control_room_url>/v1/usermanagement/roles"
-H "accept: application/json"
-H "X-Authorization: <authentication_token>"
-H "Content-Type: application/json" -d '{
  "name": "User-Role-Management",
  "description": "",
  "permissions": [
    {
      "id": 58,
      "action": "myschedule",
```

```
      "resourceType": "taskscheduling",
      "resourceId": null
    },
    {
      "id": 59,
      "action": "managecredentials",
      "resourceType": "credentials",
      "resourceId": null
    },
    {
      "id": 30,
      "action": "view",
      "resourceType": "devices",
      "resourceId": null
    },
    {
      "id": 97,
      "action": "viewbotstore",
      "resourceType": "botstore",
      "resourceId": null
    },
    {
      "id": 102,
      "action": "viewuserbasic",
      "resourceType": "usermanagement",
      "resourceId": null
    },
    {
      "id": 3,
      "action": "createuser",
      "resourceType": "usermanagement",
      "resourceId": null
    },
    {
      "id": 4,
      "action": "updateuser",
```


©2020 Automation Anywhere. All rights reserved.

```
      "resourceType": "usermanagement",
      "resourceId": null
    },
    {
      "id": 2,
      "action": "deleteuser",
      "resourceType": "usermanagement",
      "resourceId": null
    },
    {
      "id": 1,
      "action": "usermanagement",
      "resourceType": "usermanagement",
      "resourceId": null
    },
    {
      "id": 12,
      "action": "rolesmanagement",
      "resourceType": "rolesmanagement",
      "resourceId": null
    },
    {
      "id": 90,
      "action": "rolesview",
      "resourceType": "rolesmanagement",
      "resourceId": null
    }
  ],
  "principals": []
}'
```


Related concepts
User management API overview
Related tasks
Search for roles
Search for users

©2020 Automation Anywhere. All rights reserved.

Search for roles

Use the Search for Roles API to search for roles based on a date filter, sorting, and pagination.

Prerequisites

View Roles
: Users who have `view roles` permissions can retrieve all roles.

JSON Web Token (JWT)
: All Enterprise Control Room APIs require a JSON Web Token (JWT) to access the APIs. Generate an authentication token using the Authentication API. See Authentication API.

- URL: `http://<your_control_room_url>/v1/usermanagement/roles/list`

  Replace the content in the angle brackets with your Enterprise Control Room URL.

- Method: POST

Procedure

1. Add an authentication token to the request header.
   Use the Authentication API to generate a JSON Web Token. See Authentication API.
2. Select POST as the method.
   `POST http://<your_control_room_url>/v1/usermanagement/roles/list`
   Apply filters to perform basic conditional queries and pagination control for processing web pages. There are three basic features related to filtering: filtering conditions, sorting columns, and pagination parameters. See the Filters in an API request body.

   The following request sets pagination filters, such as `page: offset` and `length`.

3. Send the request.
   - In a REST client, click SEND.
   - In the Swagger interface, click Execute.

   Request body:

```
{
"sort": [
  {
   "field": "name",
   "direction": "asc"
  }
],
"filter": {
  "operator": "substring",
  "value": "sample",
  "field": "name"
```

```
},
"fields": [],
"page": {
  "offset": 0,
  "total": 23,
  "totalFilter": 23,
  "length": 200
}
}
```


Response body:

The response in this example retrieves all roles which includes the word sample in the name field.


```
{
"page": {
  "offset": 0,
  "total": 37,
  "totalFilter": 3
},
"list": [
  {
   "id": 40,
   "name": "API_Roles_sample",
   "description": "",
   "countPrincipals": 0,
   "version": 0,
   "createdBy": 36,
   "createdOn": "2019-12-18T21:02:49.087Z",
   "updatedBy": 36,
   "updatedOn": "2019-12-18T21:02:49.087Z"
  },
  {
   "id": 39,
   "name": "API_sample",
   "description": "",
   "countPrincipals": 0,
```

```
    "version": 0,
    "createdBy": 36,
    "createdOn": "2019-12-18T21:01:58.383Z",
    "updatedBy": 36,
    "updatedOn": "2019-12-18T21:01:58.383Z"
   },
   {
    "id": 38,
    "name": "sample_1",
    "description": "",
    "countPrincipals": 0,
    "version": 0,
    "createdBy": 36,
    "createdOn": "2019-12-18T21:01:12.623Z",
    "updatedBy": 36,
    "updatedOn": "2019-12-18T21:01:12.623Z"
   }
  ]
  }
```


Note: You can also run REST requests from a command terminal. The following is a curl request example. This example is formatted for readability. Replace the text inside the angle brackets, `<authentication_token>`, with your authentication token.

```
curl -X POST "http://<your_control_room_url>/v1/usermanagment/roles/list"
-H "accept: application/json"
-H "X-Authorization: <authentication_token>"
-H "Content-Type: application/json" -d "{
  {
"sort": [
  {
   "field": "name",
   "direction": "asc"
  }
],
"filter": {
  "operator": "substring",
```

©2020 Automation Anywhere. All rights reserved.

```
  "value": "sample",
  "field": "name"
},
"fields": [],
"page": {
  "offset": 0,
  "total": 23,
  "totalFilter": 23,
  "length": 200
}
}'
```

Related concepts
User management API overview
Related tasks
Search for users

Retrieve a specific role

Use the Return Specific Role API to retrieve a specific role in the Enterprise Control Room.

Prerequisites

View Roles
: Users who have `view roles` permissions can retrieve details of a specific role.

JSON Web Token (JWT)
: All Enterprise Control Room APIs require a JSON Web Token (JWT) to access the APIs. Generate an authentication token using the Authentication API. See Authentication API.

- URL: `http://<your_control_room_url>/v1/usermanagement/roles/{ID}`.
- Method: GET.
- Use the Swagger definition files installed with your Enterprise Control Room to test the APIs. View the available Swagger APIs at: `http://<your_control_room_url>/swagger/`.
- You can also use a REST client to complete this task.

Procedure

1. Add an authentication token to the request header.
   Use the Authentication API to generate a JSON Web Token. See Authentication API.
2. Select GET as the method.
3. In the request URL, add a role ID you want to retrieve.
   `GET http://<your_control_room_url>/v1/usermanagement/roles/17`
   - In a REST client, click SEND.
   - In the Swagger interface, click Execute.

   Response body:

```
{
  "id": 17,
  "createdBy": 4,
  "createdOn": "2019-11-20T18:26:37Z",
  "updatedBy": 4,
  "updatedOn": "2019-11-20T18:26:37Z",
  "tenantId": 1,
  "version": 0,
  "status": "Active",
  "description": "Created a Role for Bot running",
  "name": "DocBotRoleMD1",
  "accessRestriction": null,
  "permissions": [{
    "id": 134,
    "createdBy": 0,
    "createdOn": "2019-12-05T00:03:05Z",
    "updatedBy": 0,
    "updatedOn": "2019-12-05T00:03:05Z",
    "tenantId": 1,
    "version": 0,
    "status": null,
    "action": "viewuserbasic",
    "resourceId": null,
    "resourceType": "usermanagement"
  }],
  "countPrincipals": 0,
  "principals": [{
    "id": 16,
    "createdBy": 4,
    "createdOn": "2019-11-22T20:52:35Z",
    "updatedBy": 4,
    "updatedOn": "2019-11-22T20:52:35Z",
    "tenantId": 1,
    "version": 0,
    "status": "Active",
    "username": "docs_md_admin",
```

```
    "description": "Created a user with admin rights",
    "deleted": false,
    "disabled": false,
    "email": "aamd@md.com",
    "firstName": "Docs_AAMD1",
    "lastName": "Docs_AAMD1",
    "autoLoginEnabled": true,
    "emailVerified": true,
    "clientRegistered": false,
    "passwordSet": false,
    "questionsSet": false,
    "activeDirectory": false
  }]
}
```

Parameter name	Description
id	System-generated role ID number.
createdBy	System-generated user ID of an admin user who created a role.
updatedBy	System-generated user ID of an admin user who updated a role.
tenantID	System-generated ID number of an active user.
version	System-generated version number for a new role. Each time a role is updated, the version number is incremented.
accessRestriction	Lists access restrictions for a specific role.
Permissions	Lists role permissions.
countPrincipals	Total number of active directory principal users.
principals	Lists active directory principal users.

Note: You can also run REST requests from a command terminal. The following is a curl request example. This example is formatted for readability. Replace the text inside the angle brackets, `<authentication_token>`, with your authentication token.

```
curl -X GET "http://<your_control_room_url>/v1/usermanagement/roles/31"
-H "accept: application/json"
-H "X-Authorization: <authentication_token>"
-H "Content-Type: application/json" -d "{17}"
```

Related concepts
User management API overview

Related tasks
Search for users

Update an existing role

Use the Update Existing Role API to update an existing role in the Enterprise Control Room.

Prerequisites

Edit Roles
: Users who have `edit roles` permissions can update a role.

JSON Web Token (JWT)
: All Enterprise Control Room APIs require a JSON Web Token (JWT) to access the APIs. Generate an authentication token using the Authentication API. See Authentication API.

- URL: `http://<your_control_room_url>/v1/usermanagement/roles/{ID}`.

  Replace the content in the angle brackets with your Enterprise Control Room URL.

- Method: PUT.
- Use the Swagger definition files installed with your Enterprise Control Room to test the APIs. View the available Swagger APIs at: `http://<your_control_room_url>/swagger/`.
- You can also use a REST client to complete this task.

Procedure

1. Add an authentication token to the request header.
   Use the Authentication API to generate a JSON Web Token. See Authentication API.
2. Select PUT as the method.
3. In the request URL, add a role ID you want to update.
   `PUT http://<your_control_room_url>/v1/usermanagement/roles/37`

   Request body:

```
{
 "id": null,
 "name": "viewRoles-Docs1",
 "accessRestriction": null,
 "permissions": [{
   "id": 59,
   "action": "ManageCredentials",
   "resourceId": null,
   "resourceType": "credentials"
 },  {
   "id": 134,
```

```
    "action": "ViewUserBasic",
    "resourceId": null,
    "resourceType": "UserManagement"
  }],
  "countPrincipals": 0,
  "principals": [{
    "id": 21
  }]
}
```


4. Send the request.
   - In Swagger, click Execute.
   - In a REST client, click SEND.

   Response body:


```
{
  "id": 37,
  "createdBy": 4,
  "createdOn": "2019-12-17T03:24:22Z",
  "updatedBy": 36,
  "updatedOn": "2019-12-18T00:13:27Z",
  "tenantId": 1,
  "version": 20,
  "status": "Active",
  "description": null,
  "name": "viewRoles-Docs1",
  "accessRestriction": null,
  "permissions": [{
    "id": 59,
    "createdBy": 0,
    "createdOn": "2019-10-03T23:53:47Z",
    "updatedBy": 0,
    "updatedOn": "2019-10-03T23:53:47Z",
    "tenantId": 1,
    "version": 0,
    "status": null,
    "action": "managecredentials",
```

```
    "resourceId": null,
    "resourceType": "credentials"
  }, {
    "id": 134,
    "createdBy": 0,
    "createdOn": "2019-12-05T00:03:05Z",
    "updatedBy": 0,
    "updatedOn": "2019-12-05T00:03:05Z",
    "tenantId": 1,
    "version": 0,
    "status": null,
    "action": "viewuserbasic",
    "resourceId": null,
    "resourceType": "usermanagement"
  }],
  "countPrincipals": 0,
  "principals": [{
    "id": 21,
    "createdBy": 4,
    "createdOn": "2019-11-24T17:41:37Z",
    "updatedBy": 4,
    "updatedOn": "2019-12-17T03:25:47Z",
    "tenantId": 1,
    "version": 11,
    "status": "Active",
    "username": "docs-bot",
    "description": "Basic bot and MetaBot designer",
    "deleted": false,
    "disabled": false,
    "email": "tm@aa.com",
    "firstName": "",
    "lastName": "",
    "autoLoginEnabled": false,
    "emailVerified": true,
    "clientRegistered": true,
    "passwordSet": true,
```


©2020 Automation Anywhere. All rights reserved.

```
    "questionsSet": true,
    "activeDirectory": false
  }]
}
```

Parameter name	Description
id	System-generated role ID number.
createdBy	System-generated role ID number of an admin user who created a role.
updatedBy	System-generated role ID number of an admin user who updated a role.
tenantID	System-generated ID number of an active user.
version	System-generated version number for a new role. Each time a role is updated, the version number is incremented.
status	An existing role state: active or disabled.
accessRestriction	Lists access restrictions for a specific role.
Permissions	Lists role permissions.
countPrincipals	The total number of the active directory principal users.
principals	Lists the active directory principal users.

Note: You can also run REST requests from a command terminal. The following is a curl request example. This example is formatted for readability. Replace the text inside the angle brackets, `<authentication_token>`, with your authentication token.

```
curl -X PUT "http://<your_control_room_url>/v1/usermanagement/roles/37"
-H "accept: application/json"
-H "X-Authorization: <authentication_token>"
-H "Content-Type: application/json" -d "'{
  "id": null,
  "name": "viewRoles-Docs1",
  "accessRestriction": null,
  "permissions": [{
    "id": 59,
    "action": "ManageCredentials",
    "resourceId": null,
    "resourceType": "credentials"
  },  {
    "id": 134,
    "action": "ViewUserBasic",
```

```
    "resourceId": null,
    "resourceType": "UserManagement"
  }],
  "countPrincipals": 0,
  "principals": [{
    "id": 21
  }]
}'
```

Related concepts
User management API overview
Related tasks
Search for roles

Delete an existing role

Use the Delete Existing Role API to delete an existing role in the Enterprise Control Room.

Prerequisites

Manage roles permission

Users who have `manage roles` permissions can delete roles. However, only custom roles can be deleted, the system-created roles, the first 16 roles with ID 1 to 16, cannot be deleted.

JSON Web Token (JWT)
All Enterprise Control Room APIs require a JSON Web Token (JWT) to access the APIs. Generate an authentication token using the Authentication API. See Authentication API.

- URL: `http://<your_control_room_url>/v1/usermanagement/roles/{ID}`

  Replace the content in the angle brackets with your Enterprise Control Room URL.

- Method: DELETE.
- Use the Swagger definition files installed with your Enterprise Control Room to test the APIs. View the available Swagger APIs at: `http://<your_control_room_url>/swagger/`.
- You can also use a REST client to complete this task.

Procedure

1. Add an authentication token to the request header.
   Use the Authentication API to generate a JSON Web Token. See Authentication API.
2. Select DELETE as the method.
3. In the request header, add a role ID you want to delete.
   `DELETE http://<your_control_room_url>/v1/usermanagement/roles/22`
4. Send the request.
   - In Swagger, click Execute.
   - In a REST client, click SEND.

©2020 Automation Anywhere. All rights reserved.

Response body:

```
"OK"
```

Note: You can also run REST requests from a command terminal. The following is a curl request example. This example is formatted for readability. Replace the text inside the angle brackets, `<authentication_token>`, with your authentication token.

```
curl -X DELETE "http://<your_control_room_url>/v1/usermanagement/roles/22"
-H "accept: application/json"
-H "X-Authorization: <authentication_token>"
-H "Content-Type: application/json" -d "{22}"
```

Create a new user

Use the Create New User API to create a new user in the Enterprise Control Room.

Prerequisites

View and Manage Users

Authenticate with a user that has the following ADMINISTRATION permissions:

- View users

  Users with these permissions are able to create and manage users. These are administrator permissions. It is recommended that non-administrator users be given limited permissions for creating and managing users. Learn how to create a role with limited permissions that can be assigned to users.

  - Create users
  - Edit users
  - Delete users
- View licenses

  Users with these permissions are able to view and manage device licenses. Device licenses are required to enable users to perform specific tasks. For example, Bot Creators require a DEVELOPMENT device license in order to create bots.

  Manage user's device license

JSON Web Token (JWT)

All Enterprise Control Room APIs require a JSON Web Token (JWT) to access the APIs. Generate an authentication token using the Authentication API. See Authentication API.

©2020 Automation Anywhere. All rights reserved.

Minimum required parameters

- Roles: Each user must have at least one role. The role id is required to create a role from the User Management API.

  Role based accessibility enables appropriate access to relevant data and actions.

  Note: For this example, we created a Bot Creator user. In the request body we assigned the following System created roles:
  - AAE_Basic (ID: 2)
  - AAE_Meta Bot Designer (ID: 13)
- username: String (255 max)
- email: Must conform to standard email format (username@domain.com)
- password: String: 8-15 characters in length. Allowable characters: a-z, A-Z, 0-9, @, -, _, !, #, $, %, &, and . (period)

Additional recommended parameters

- `"enableAutoLogin": true`
- `"username": "NumerOneUser"`
- `"firstName": "Doc"`
- `"lastName": "Writer"`
- `"email": "username@mydomain.com"`
- `"password": "changeme"`
- `"description": "Test user creation."`
- `"licenseFeatures": [ DEVELOPMENT, RUNTIME, IQBOTRUNTIME, ANALYTICSCLIENT, ANALYTICSAPI ]`

  Users can be created without an assigned device license. There are System default licenses that enable privileges for specific users and roles.

- Use the Swagger installed with your Enterprise Control Room to test the APIs. View the available APIs at: `http://<your_control_room_url>/swagger/`
- You can also use a REST client to complete this task.

Procedure

1. Add an authentication token to the request header.
   Use the Authentication API to generate a JSON Web Token. See Authentication API.
2. Select POST as the method.
   `POST http://<your_control_room_url>/v1/usermanagement/users`
3. In the request body, enter the mandatory parameters and recommend parameters.

   Request body :

```
{
  "roles": [
    {
      "id": 2
```

```
    },
    {
      "id": 13
    }
  ],
  "enableAutoLogin": true,
  "username": "BotCreatorUser",
  "firstName": "Robert",
  "lastName": "Developer",
  "email": "bob.dev@mydomain.com",
  "password": "changeme",
  "description": "Go create great bots.",
  "licenseFeatures": [
    "DEVELOPMENT"
  ]
}
```

4. Send the request.
   - In Swagger, click Execute.
   - In a REST client, click SEND.

   The response returns user details.

   Response body:

```
{
  "id": 61,
  "email": "bob.dev@mydomain.com",
  "username": "botcreatoruser",
  "domain": null,
  "firstName": "Robert",
  "lastName": "Developer",
  "version": 0,
  "principalId": 61,
  "deleted": false,
  "roles": [
    {
      "name": "AAE_Basic",
      "id": 2,
```

```
      "version": 0
    },
    {
      "name": "AAE_Meta Bot Designer",
      "id": 13,
      "version": 0
    }
  ],
  "sysAssignedRoles": [],
  "groupNames": [],
  "permissions": [
    {
      "id": 97,
      "action": "viewbotstore",
      "resourceId": null,
      "resourceType": "botstore"
    },
    {
      "id": 33,
      "action": "upload",
      "resourceId": "7",
      "resourceType": "repositorymanager"
    },
    {
      "id": 61,
      "action": "createstandard",
      "resourceId": null,
      "resourceType": "credentialattribute"
    },
    {
      "id": 93,
      "action": "download",
      "resourceId": "9",
      "resourceType": "repositorymanager"
    },
    {
```


©2020 Automation Anywhere. All rights reserved.

```
      "id": 134,
      "action": "viewuserbasic",
      "resourceId": null,
      "resourceType": "usermanagement"
    },
    {
      "id": 29,
      "action": "view",
      "resourceId": null,
      "resourceType": "repositorymanager"
    },
    {
      "id": 62,
      "action": "metabotdesigner",
      "resourceId": null,
      "resourceType": "metabot"
    },
    {
      "id": 34,
      "action": "download",
      "resourceId": "7",
      "resourceType": "repositorymanager"
    },
    {
      "id": 92,
      "action": "upload",
      "resourceId": "9",
      "resourceType": "repositorymanager"
    }
  ],
  "licenseFeatures": [
    "DEVELOPMENT"
  ],
  "emailVerified": true,
  "passwordSet": false,
  "questionsSet": false,
```


©2020 Automation Anywhere. All rights reserved.

```
    "enableAutoLogin": true,
    "disabled": false,
    "clientRegistered": false,
    "description": "Go create great bots.",
    "createdBy": 19,
    "createdOn": "2020-02-09T23:25:20Z",
    "updatedBy": 19,
    "updatedOn": "2020-02-09T23:25:20Z",
    "publicKey": null,
    "appType": null,
    "routingName": null,
    "appUrl": null
  }
```

Note: You can also run REST requests from a command terminal. The following is a curl request example. This example is formatted for readability. Replace the text inside the angle brackets, `<authentication_token>`, with your authentication token.

```
curl -X POST -H 'X-Authorization: <authentication_token>' -i '<your_control_roo
m_url>/v1/usermanagement/users' --data '{
  "roles": [
    {
      "id": 2
    },
    {
      "id": 13
    }
  ],
  "enableAutoLogin": true,
  "username": "BotCreatorUser",
  "firstName": "Robert",
  "lastName": "Developer",
  "email": "bob.dev@mydomain.com",
  "password": "changeme",
  "description": "Go create great bots.",
  "licenseFeatures": [
   "DEVELOPMENT"
```

```
  ]
}'
```

Next steps

- You can verify that the user was created by logging in to the Enterprise Control Room as the user that you created.
- System assigned roles, sysAssignedRoles, include a set of permissions that are required by the roles you assigned to the user and default roles that are assigned to all users.

Related concepts
User management API overview
Related tasks
Search for roles

Search for users

Use the Search for Users API to search for all users in the Enterprise Control Room.

Prerequisites

View Users
: Users who have `view users` permissions can retrieve all users.

JSON Web Token (JWT)
: All Enterprise Control Room APIs require a JSON Web Token (JWT) to access the APIs. Generate an authentication token using the Authentication API. See Authentication API.

- URL: `http://<your_control_room_url>/v1/usermanagement/users/list`.

  Replace the content in the angle brackets with your Enterprise Control Room URL.

- Method: POST.
- Use the Swagger definition files installed with your Enterprise Control Room to test the APIs. View the available Swagger APIs at: `http://<your_control_room_url>/swagger/`.
- You can also use a REST client to complete this task.

Procedure

1. Add an authentication token to the request header.
   Use the Authentication API to generate a JSON Web Token. See Authentication API.
2. Select POST as the method.
   Apply filters to perform basic conditional queries and pagination control for processing web pages. There are three basic features related to filtering: filtering conditions, sorting columns, and pagination parameters. See Filters in an API request body.
   `POST http://<your_control_room_url>/v1/usermanagement/users/list`
3. Send the request.
   - In a REST client, click SEND.
   - In the Swagger interface, click Execute.

©2020 Automation Anywhere. All rights reserved.

Request body:

The following request finds all users with a `username` that contains `doc` and who were created between December 1 and December 31, 2019.

```
{
  "fields": [],
  "filter": {
    "operator": "and",
    "operands": [
      {
        "operator": "substring",
        "field": "username",
        "value": "doc"
      },
      {
        "operator": "gt",
        "field": "createdOn",
        "value": "2019-12-01T00:00:00.989Z"
      },
      {
        "operator": "lt",
        "field": "createdOn",
        "value": "2019-12-06T23:00:00.123Z"
      }
    ]
  }
}
```

The response in this example returned data for the `doc` username.

Response body:

```
{
  "page": {
    "offset": 0,
    "total": 24,
    "totalFilter": 5
  },
```

©2020 Automation Anywhere. All rights reserved.

```
  "list": [{
    "id": 29,
    "username": "docs-2fa-vm1",
    "domain": "",
    "firstName": "",
    "lastName": "",
    "version": 2,
    "principalId": 29,
    "email": "tm@automationanywhere.com",
    "emailVerified": true,
    "passwordSet": true,
    "questionsSet": true,
    "enableAutoLogin": true,
    "disabled": false,
    "clientRegistered": true,
    "description": "",
    "createdBy": 4,
    "createdOn": "2019-12-05T05:24:49.330Z",
    "updatedBy": 0,
    "updatedOn": "2019-12-05T05:27:58.687Z",
    "licenseFeatures": ["DEVELOPMENT"],
    "roles": [{
      "id": 31,
      "name": "2fa-role-basic-bot-permission",
      "version": "0"
    }],
    "deleted": false
  }, {
    "id": 30,
    "username": "docs-test-02",
    "domain": "",
    "firstName": "",
    "lastName": "",
    "version": 0,
    "principalId": 30,
    "email": "a@a.com",
```


©2020 Automation Anywhere. All rights reserved.

```
    "emailVerified": true,
    "passwordSet": false,
    "questionsSet": false,
    "enableAutoLogin": true,
    "disabled": false,
    "clientRegistered": false,
    "description": "Docs resource",
    "createdBy": 4,
    "createdOn": "2019-12-05T23:15:53.907Z",
    "updatedBy": 4,
    "updatedOn": "2019-12-05T23:15:53.907Z",
    "licenseFeatures": ["RUNTIME", "IQBOTRUNTIME"],
    "roles": [{
      "id": 2,
      "name": "AAE_Basic",
      "version": "0"
    }, {
      "id": 13,
      "name": "AAE_Meta Bot Designer",
      "version": "0"
    }],
    "deleted": false
  }, {
    "id": 31,
    "username": "docs-test-04",
    "domain": "",
    "firstName": "",
    "lastName": "",
    "version": 0,
    "principalId": 31,
    "email": "a@a.com",
    "emailVerified": true,
    "passwordSet": false,
    "questionsSet": false,
    "enableAutoLogin": true,
    "disabled": false,
```


©2020 Automation Anywhere. All rights reserved.

```
    "clientRegistered": false,
    "description": "Docs resource",
    "createdBy": 4,
    "createdOn": "2019-12-05T23:16:26.543Z",
    "updatedBy": 4,
    "updatedOn": "2019-12-05T23:16:26.543Z",
    "licenseFeatures": ["RUNTIME", "IQBOTRUNTIME"],
    "roles": [{
      "id": 2,
      "name": "AAE_Basic",
      "version": "0"
    }, {
      "id": 13,
      "name": "AAE_Meta Bot Designer",
      "version": "0"
    }],
    "deleted": false
  }, {
    "id": 32,
    "username": "docs-user-md",
    "domain": "",
    "firstName": "",
    "lastName": "",
    "version": 0,
    "principalId": 32,
    "email": "a@a.com",
    "emailVerified": true,
    "passwordSet": false,
    "questionsSet": false,
    "enableAutoLogin": true,
    "disabled": false,
    "clientRegistered": false,
    "description": "Docs resource",
    "createdBy": 4,
    "createdOn": "2019-12-05T23:45:44.267Z",
    "updatedBy": 4,
```

```
    "updatedOn": "2019-12-05T23:45:44.267Z",
    "licenseFeatures": ["RUNTIME", "IQBOTRUNTIME"],
    "roles": [{
      "id": 2,
      "name": "AAE_Basic",
      "version": "0"
    }, {
      "id": 13,
      "name": "AAE_Meta Bot Designer",
      "version": "0"
    }],
    "deleted": false
  }, {
    "id": 33,
    "username": "docs-tm-admin",
    "domain": "",
    "firstName": "",
    "lastName": "",
    "version": 2,
    "principalId": 33,
    "email": "tr@automationanywhere.com",
    "emailVerified": true,
    "passwordSet": true,
    "questionsSet": true,
    "enableAutoLogin": false,
    "disabled": false,
    "clientRegistered": false,
    "description": "",
    "createdBy": 4,
    "createdOn": "2019-12-06T19:05:36.217Z",
    "updatedBy": 4,
    "updatedOn": "2019-12-06T19:07:21.097Z",
    "licenseFeatures": [],
    "roles": [{
      "id": 33,
      "name": "apiKey-Docs",
```


©2020 Automation Anywhere. All rights reserved.

```
      "version": "0"
    }, {
      "id": 1,
      "name": "AAE_Admin",
      "version": "0"
    }],
    "deleted": false
  }]
}
```

Response body parameters:

Parameter Name	Description
id	System-generated ID number who created a user.
username	User name for a new user.
domain	Active directory domain name.
version	System-generated version number for a new user.
email	New user email address.
passwordSet	String: 8-15 characters; a-z, A-Z, 0-9, @, -, _, !, #, $, %, &, and . (period). Set a password for a new user only.
PrincipalId	System-generated ID number of an active directory principal user who created a new user.
Permission	A specific permission ID.
licenseFeature	Automation Anywhere license associated with this role.
Roles: id	System-generated role ID number associated with this user. Not every user has an associated role.
createdBy	System-generated ID number of an admin user who created a new user.
updatedBy	System-generated ID number of an admin user who updated the user.

Note: You can also run REST requests from a command terminal. The following is a curl request example. This example is formatted for readability. Replace the text inside the angle brackets, `<authentication_token>`, with your authentication token.

```
curl -X POST "http://<your_control_room_url>/v1/usermanagment/users/list"
-H "accept: application/json"
-H "X-Authorization: <authentication_token>"
-H "Content-Type: application/json" -d "{
  "fields": [],
  "filter": {
```

```
    "operator": "and",
    "operands": [
      {
        "operator": "substring",
        "field": "username",
        "value": "doc"
      },
      {
        "operator": "gt",
        "field": "createdOn",
        "value": "2019-12-01T00:00:00.989Z"
      },
      {
        "operator": "lt",
        "field": "createdOn",
        "value": "2019-12-06T23:00:00.123Z"
      }
    ]
  }
}'
```

Related concepts
User management API overview

Retrieve a specific user

Use the Get Use Details API to retrieve a specific user in the Enterprise Control Room.

Prerequisites

View Users permission
: Users who have `view users` permissions can retrieve details of a specific user.

JSON Web Token (JWT)
: All Enterprise Control Room APIs require a JSON Web Token (JWT) to access the APIs. Generate an authentication token using the Authentication API. See Authentication API.

- URL: `http://<your_control_room_url>/v1/usermanagement/users/{ID}`.

  Replace the content in the angle brackets with your Enterprise Control Room URL.

- Method: GET.
- Use the Swagger definition files installed with your Enterprise Control Room to test the APIs. View the available Swagger APIs at: `http://<your_control_room_url>/swagger/`.

©2020 Automation Anywhere. All rights reserved.

- You can also use a REST client to complete this task

Procedure

1. Add an authentication token to the request header.
   Use the Authentication API to generate a JSON Web Token. See Authentication API.
2. Select GET as the method.
3. In the request header, add a specific user ID you want to retrieve.
   `GET http://<your_control_room_url>/v1/usermanagement/users/35`
4. Send the request.
   - In Swagger, click Execute.
   - In a REST client, click SEND.

   Response body:


```
{
  "id": 35,
  "email": "aa@aa.com",
  "username": "docbotusermd100",
  "domain": "ActiveDirectory (LDAP)",
  "firstName": "AAMHD4",
  "lastName": "AAMHD5",
  "version": 0,
  "principalId": 35,
  "deleted": false,
  "roles": [{
    "name": "DocBotRole03",
    "id": 18,
    "version": 0
  }],
  "sysAssignedRoles": [],
  "groupNames": [],
  "permissions": [{
    "id": 134,
    "action": "viewuserbasic",
    "resourceId": null,
    "resourceType": "usermanagement"
  }],
  "licenseFeatures": ["DEVELOPMENT"],
  "emailVerified": true,
  "passwordSet": false,
```

```
  "questionsSet": false,
  "enableAutoLogin": true,
  "disabled": false,
  "clientRegistered": false,
  "description": "Created a user for running bots",
  "createdBy": 4,
  "createdOn": "2019-12-16T23:00:58Z",
  "updatedBy": 4,
  "updatedOn": "2019-12-16T23:00:58Z",
  "publicKey": null,
  "appType": null,
  "routingName": null,
  "appUrl": null
}
```


Note: You can also run REST requests from a command terminal. The following is a curl request example. This example is formatted for readability. Replace the text inside the angle brackets, `<authentication_token>`, with your authentication token.

```
curl -X GET "http://<your_control_room_url>/v1/usermanagement/users/11"
-H "accept: application/json"
-H "X-Authorization: <authentication_token>"
-H "Content-Type: application/json" -d "{35}"
```

Related concepts
Roles overview
Related tasks
Search for users
Search for roles

Update an existing user

Use the Update User Details API to update an existing user information in the Enterprise Control Room.

Prerequisites

Edit Users permission
: Users who have `edit users` permission can update a specific user details.

JSON Web Token (JWT)
: All Enterprise Control Room APIs require a JSON Web Token (JWT) to access the APIs. Generate an authentication token using the Authentication API. See Authentication API.

- URL: `http://<your_control_room_url>/v1/usermanagement/users/{ID}`.

Replace the content in the angle brackets with your Enterprise Control Room URL.

- Method: PUT.
- Use the Swagger definition files installed with your Enterprise Control Room to test the APIs. View the available Swagger APIs at: `http://<your_control_room_url>/swagger/`.
- You can also use a REST client to complete this task.

Procedure

1. Add an authentication token to the request header.
   Use the Authentication API to generate a JSON Web Token. See Authentication API.
2. Select PUT as the method.
3. In the request header, add an existing user ID you want to update. To find a user ID you want to update, execute the Search Users API.
   `PUT http://<your_control_room_url>/v1/usermanagement/users/27`

   In the request body, add the mandatory parameters.

Parameter name	Mandatory parameters	Type	Description
Username	Yes	String (255 max)	New user name
Email	Yes	String; must include @ sign, such as a@a.com	New user email
Roles: name	Yes	String (255 max)	New name for the role

Request body

```
{
    "username": "docsusermd2",
    "domain": "",
    "firstName": "DocsUserMHD1",
    "lastName": "DocUserMHD2",
    "version": 2,
    "principalId": 27,
    "email": "aamd@aa.com",
    "description": "Created a user to create other roles and users",
    "createdOn": "2019-11-26T23:44:12.937Z",
    "updatedOn": "2019-11-26T23:51:39.163Z",
    "roles": [{
      "id": 27,
      "name": "RoleBotDocsMD6",
      "version": "0"
```

©2020 Automation Anywhere. All rights reserved.

```
    }],
    "deleted": false
  }
```

4. Send the request.
   - In Swagger, click Execute.
   - In a REST client, click SEND.

   Response body:

```
{
  "id": 27,
  "email": "aamd@aa.com",
  "username": "docsusermd",
  "domain": null,
  "firstName": "DocsUserMHD1",
  "lastName": "DocUserMHD2",
  "version": 6,
  "principalId": 27,
  "deleted": false,
  "roles": [{
    "name": "RoleBotDocsMD6",
    "id": 27,
    "version": 0
  }],
  "sysAssignedRoles": [],
  "groupNames": [],
  "permissions": [],
  "licenseFeatures": [],
  "emailVerified": true,
  "passwordSet": true,
  "questionsSet": true,
  "enableAutoLogin": false,
  "disabled": false,
  "clientRegistered": false,
  "description": "Created a user to create other roles and users",
  "createdBy": 4,
```

©2020 Automation Anywhere. All rights reserved.

```
  "createdOn": "2019-11-26T23:44:12Z",
  "updatedBy": 4,
  "updatedOn": "2019-12-02T23:31:25Z",
  "publicKey": null,
  "appType": null,
  "routingName": null,
  "appUrl": null
}
```

Note: You can also run REST requests from a command terminal. The following is a curl request example. This example is formatted for readability. Replace the text inside the angle brackets, `<authentication_token>`, with your authentication token.

```
curl -X PUT "http://<your_control_room_url>/v1/usermanagement/users/27"
-H "accept: application/json"
-H "X-Authorization: <authentication_token>"
-H "Content-Type: application/json" -d "'{
    "username": "docsusermd2",
    "domain": "",
    "firstName": "DocsUserMHD1",
    "lastName": "DocUserMHD2",
    "version": 2,
    "principalId": 27,
    "email": "aamd@aa.com",
    "description": "Created a user to create other roles and users",
    "createdOn": "2019-11-26T23:44:12.937Z",
    "updatedOn": "2019-11-26T23:51:39.163Z",
    "roles": [{
      "id": 27,
      "name": "RoleBotDocsMD6",
      "version": "0"
    }],
    "deleted": false
  }'
```

Related concepts
Roles overview
Related tasks
Search for users

©2020 Automation Anywhere. All rights reserved.

Delete an existing user

Use the Delete Existing User API to delete an existing user in the Enterprise Control Room.

Prerequisites

Edit Users
: Users who have `edit users` permissions can delete an existing user.

JSON Web Token (JWT)
: All Enterprise Control Room APIs require a JSON Web Token (JWT) to access the APIs. Generate an authentication token using the Authentication API. See Authentication API.

- URL: `http://<your_control_room_url>/v1/usermanagement/users/{ID}`

  Replace the content in the angle brackets with your Enterprise Control Room URL.

- Method: DELETE

Procedure

1. Add an authentication token to the request header.
   Use the Authentication API to generate a JSON Web Token. See Authentication API.
2. Select DELETE as the method.
3. In the request header, add an existing user ID you want to delete.
   `DELETE http://<your_control_room_url>/v1/usermanagement/users/15`
4. Send the request.
   - In Swagger, click Execute.
   - In a REST client, click SEND.

   Response body:

```
{
  "id": 15,
  "email": "aa@aa.com",
  "username": "docbotusermd4",
  "domain": "ActiveDirectory (LDAP)",
  "firstName": "AAMHD4",
  "lastName": "AAMHD5",
  "version": 0,
  "principalId": 15,
  "deleted": false,
  "roles": [],
  "sysAssignedRoles": [],
  "groupNames": [],
  "permissions": [],
```

©2020 Automation Anywhere. All rights reserved.

```
  "licenseFeatures": [],
  "emailVerified": true,
  "passwordSet": false,
  "questionsSet": false,
  "enableAutoLogin": true,
  "disabled": false,
  "clientRegistered": false,
  "description": "Created a user for running bots",
  "createdBy": 1,
  "createdOn": "2019-11-18T20:48:04Z",
  "updatedBy": 1,
  "updatedOn": "2019-11-18T20:48:04Z",
  "publicKey": null,
  "appType": null,
  "routingName": null,
  "appUrl": null
}
```


Note: You can also run REST requests from a command terminal. The following is a curl request example. This example is formatted for readability. Replace the text inside the angle brackets, `<authentication_token>`, with your authentication token.

```
curl -X DELETE "http://<your_control_room_url>/v1/usermanagement/users/15"
-H "accept: application/json"
-H "X-Authorization: <authentication_token>"
-H "Content-Type: application/json" -d "{15}"
```

Related concepts
User management API overview
Related tasks
Search for roles

Workload Management API overview

Use the Workload Management (WLM) API to programmatically manage and create queues and work items in your Enterprise Control Room.

WLM queues

WLM queues contain work items that are distributed for processing to unattended bot runners within a device pool.

©2020 Automation Anywhere. All rights reserved.

Filters allow you to refine what is returned in the response body. Read more about filters in Filters in an API request body.

List queues

```
POST http://<your_control_room_url>/v2/wlm/queues/list
```

Body parameters: This request body example includes filters, sorting, and page control to refine the response.

```
{
  "filter": {
    "operator": "NONE",
    "operands": [
      null
    ],
    "field": "string",
    "value": "string"
  },
  "sort": [
    {
      "field": "string",
      "direction": "asc"
    }
  ],
  "page": {
    "offset": 0,
    "length": 0
  }
}
```

Make a post request to return a list of all WLM queues, or use filters in the request body to refine the response results. Request and response examples:

Use filters to retrieve selected WLM queues

WLM work items

Create a work item in a queue

```
POST http://<your_control_room_url>/v2/wlm/queues/{id}/workitems
```

URL parameter:

`.../queues/{id}/...`: The numeric value that identifies a WLM queue that lists work items.

Body parameters: The generic request example does not identify the details of the JSON object.

```
{
  "workItems": [
    {
      "json": {}
    }
  ]
}
```

The following request body example includes a JSON object listing the mandatory key-value pairs that represent a WLM work item.

```
{
  "workItems": [],
  "json": {
    "Id": "string",
    "Customer Name": "string",
    "Amount": "number",
    "email": "string",
    "Invoice Date": "ISO 8601 date and time notation"
  }
}
```

A JSON object has key-value pairs that are required for specific WLM implementations. Make a post request to add a new work item to an existing queue.

Update a work item in a queue

```
PUT http://<your_control_room_url>/v2/wlm/queues/{id}/workitems/{id}
```

URL parameters:

- `.../queues/{id}/...`: The numeric value that identifies a WLM queue that lists work items.
- `.../workitems/{id}`: The numeric value that identifies a WLM work item within a queue.

Body parameters:

```
{
  "version": 0,
  "status": "Enum",
  "result": "string",
  "json": {}
}
```

The following request body example includes a JSON object listing the mandatory key-value pairs that represent a WLM work item.

```
{
  "version": "0",
  "result": "",
  "status": "Enum",
  "json": {
    "Id": "string",
    "Customer Name": "string",
    "Amount": "number",
    "email": "string",
    "Invoice Date": "ISO 8601 date and time notation"
  }
}
```

Status enum array values:

```
Enum:
[ READY_TO_RUN, DATA_ERROR, UNKNOWN, STAGED, QUEUED, ACTIVE, UNSUCCESSFUL
, SUCCESSFUL, ON_HOLD ]
```

Click the link for a step by step example of how to update a work item Update work item data, results and status.

List work items in a queue

```
POST http://<your_control_room_url>/v2/wlm/queues/{id}/workitems/list
```

URL parameter:

`.../queues/{id}/...`: The numeric value that identifies a WLM queue that lists work items.

Body parameters: This request body example includes filters, sorting, and page control to refine the response.

```
{
  "filter": {
    "operator": "NONE",
    "operands": [
      null
    ],
    "field": "string",
    "value": "string"
  },
  "sort": [
    {
      "field": "string",
      "direction": "asc"
    }
  ],
  "page": {
    "offset": 0,
    "length": 0
  }
}
```

Delete work items from a queue

```
POST http://<your_control_room_url>/v2/wlm/queues/{id}/workitems/delete
```

URL parameter:

`.../queues/{id}/...`: The numeric value that identifies a WLM queue that lists work items.

Body parameters:

```
{
  "workitemIds": [
    0,
    1,
    2
```

```
  ]
}
```

Click the link for a step by step example of how to delete work items from a queue Delete work items in a queue.

Related concepts
WLM work item life cycle

Retrieve data on all available queues

Send a post request from the WLM API to retrieve all queues for your Enterprise Control Room.

Prerequisites

AAE_Queue Admin role
: You need a user account with the AAE_Queue Admin role to query and manage workload queues and work items in an Enterprise Control Room.

JSON Web Token (JWT)
: All Enterprise Control Room APIs require a JSON Web Token (JWT) to access the APIs. Generate an authentication token using the Authentication API.

- URL: `http://<your_control_room_url>/v2/wlm/queues/list`
- Method: POST

Note:

- Use the Swagger definition files installed with your Enterprise Control Room to test the APIs. View the available Swagger APIs at `http://<your_control_room_url>/swagger/`.
- You can also use a REST client to complete this task.

Procedure

1. Add an authentication token to the request header.
   Note: Use the Authentication API to generate a JSON Web Token.
2. Select POST as the method.
3. Leave the request body blank to request information on all available WLM queues.
   Request body:

   ```
   { }
   ```

4. Send the request.
   - In a REST Client, click SEND.
   - In the Swagger interface, click Execute.

   The response for this example returned data for 3 queues. When the there is no filtering used in the request, a successful responses returns all of the queues for the specified Enterprise Control Room.

   Response body:

```
"page": {
  "offset": 0,
  "total": 3,
  "totalFilter": 3
},
"list": [{
  "id": "5",
  "name": "q1",
  "status": "IN_USE",
  "description": "",
  "reactivationThreshold": "1",
  "manualProcessingTime": "0",
  "manualProcessingTimeUnit": "SECONDS",
  "workItemModelId": "1",
  "considerReactivationThreshold": false,
  "createdBy": "25",
  "createdOn": "2019-09-10T21:02:46.067Z",
  "updatedBy": "0",
  "updatedOn": "2019-09-10T23:31:16.681Z",
  "tenantId": "1",
  "version": "31"
}, {
  "id": "6",
  "name": "q2",
  "status": "IN_USE",
  "description": "",
  "reactivationThreshold": "1",
  "manualProcessingTime": "1",
  "manualProcessingTimeUnit": "HOURS",
  "workItemModelId": "2",
  "considerReactivationThreshold": false,
  "createdBy": "25",
  "createdOn": "2019-09-10T21:03:36.897Z",
  "updatedBy": "0",
  "updatedOn": "2019-09-10T23:31:17.004Z",
  "tenantId": "1",
```


©2020 Automation Anywhere. All rights reserved.

```
    "version": "22"
  }, {
    "id": "7",
    "name": "q3",
    "status": "IN_USE",
    "description": "",
    "reactivationThreshold": "1",
    "manualProcessingTime": "1",
    "manualProcessingTimeUnit": "DAYS",
    "workItemModelId": "3",
    "considerReactivationThreshold": true,
    "createdBy": "25",
    "createdOn": "2019-09-10T21:04:26.760Z",
    "updatedBy": "25",
    "updatedOn": "2019-09-26T20:54:33.658Z",
    "tenantId": "1",
    "version": "27"
  }]
}
```


Response headers

```
cache-control: no-cache, no-store, max-age=0, must-revalidate
connection: keep-alive
content-length: 1415
content-security-policy: default-src 'self'
content-type: application/json
date: Mon, 23 Sep 2019 17:17:28 GMT
expires: 0
pragma: no-cache
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
x-xss-protection: 1; mode=block
```

Note: You can also run REST requests from a command terminal. Here is a Curl example of the request. This example is formatted for readability. Replace text inside the angel brackets, <text>, with the appropriate values.

©2020 Automation Anywhere. All rights reserved.

```
curl -X POST "http://<your_control_room_url>/v2/wlm/queues/list"
-H "accept: application/json"
-H "X-Authorization: <authentication_token>"
-H "Content-Type: application/json" -d "{}"
```

Related concepts
Workload Management API overview

Use filters to retrieve selected WLM queues

Send a post request with filters to retrieve specific Workload Management (WLM) queues for your Enterprise Control Room.

Prerequisites

AAE_Queue Admin role
: You need a user account with the AAE_Queue Admin role to query and manage workload queues and work items in an Enterprise Control Room.

JSON Web Token (JWT)
: All Enterprise Control Room APIs require a JSON Web Token (JWT) to access the APIs. Generate an authentication token using the Authentication API.

- URL: `http://<your_control_room_url>/v2/wlm/queues/list`

  Replace the content in the angel brackets with information for your Enterprise Control Room.

- Method: POST

Procedure

1. Add an authentication token to the request header.
   Note: Use the Authentication API to generate a JSON Web Token.
2. Select POST as the method.
3. Add filter parameters in the request body to limit the information returned from all available WLM queues.

   This request is intended to return all WLM queues with a id value greater than 6.

```
{
  "filter": {
    "operator": "gt",
    "operands": [

    ],
    "field": "id",
```

```
      "value": "6"
    },
    "sort": [
      {
        "field": "id",
        "direction": "asc"
      }
    ],
    "page": {
      "offset": 0,
      "length": 100
    }
  }
```

4. Send the request.
   - In a REST Client, click SEND.
   - In Swagger interface, click Execute.

The response for this example returned only 1 queue that met the filter requirements.

Response body

```
{
  "page": {
    "offset": 0,
    "total": 3,
    "totalFilter": 1
  },
  "list": [
    {
      "id": "7",
      "name": "q3",
      "status": "IN_USE",
      "description": "",
      "reactivationThreshold": "1",
      "manualProcessingTime": "1",
      "manualProcessingTimeUnit": "DAYS",
      "workItemModelId": "3",
      "considerReactivationThreshold": false,
```

©2020 Automation Anywhere. All rights reserved.

```
      "createdBy": "25",
      "createdOn": "2019-09-10T21:04:26.760Z",
      "updatedBy": "0",
      "updatedOn": "2019-09-10T23:31:46.995Z",
      "tenantId": "1",
      "version": "24"
    }
  ]
}
```

Response headers

```
cache-control: no-cache, no-store, max-age=0, must-revalidate
connection: keep-alive
content-length: 527
content-security-policy: default-src 'self'
content-type: application/json
date: Mon, 23 Sep 2019 17:50:15 GMT
expires: 0
pragma: no-cache
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
x-xss-protection: 1; mode=block
```

Here is a Curl example of the same REST request. The example is formatted for readability.

```
curl -X POST "http://<your_control_room_url>/v2/wlm/queues/list"
-H "accept: application/json" -H "X-Authorization: <authentication_token>"
-H "Content-Type: application/json" -d "{ \"filter\": { \"operator\": \"gt\",
\"operands\": [ ], \"field\": \"id\", \"value\": \"6\" }, \"sort\": [ { \"field
\": \"id\",
\"direction\": \"asc\" } ], \"page\": { \"offset\": 0, \"length\": 100 }}"
```

Related concepts
Workload Management API overview

List all work items in a queue

Automation Anywhere provides a REST API that enables you to retrieve a list of work items in a given queue.

©2020 Automation Anywhere. All rights reserved.

Prerequisites

AAE_Queue Admin role
: You need a user account with the AAE_Queue Admin role to query and manage workload queues and work items in an Enterprise Control Room.

JSON Web Token (JWT)
: All Enterprise Control Room APIs require a JSON Web Token (JWT) to access the APIs. Generate an authentication token using the Authentication API.

- URL: `https://<your_control_room_url>/v2/wlm/queues/{id}/workitems/list`.
- Method: POST.

Procedure

1. Add an authentication token to the request header.
   Note: Use the Authentication API to generate a JSON Web Token.
2. Enter the following parameters in the request body.

   There are 2 inputs required for this request.

   Id

   ```
   7
   ```

   Request body:

   ```
   {
     "filter": {
       "operator": "and",
       "operands": [
         {
           "field": "id",
           "operator": "gt",
           "value": "30800"
         },
         {
           "field": "id",
           "operator": "lt",
           "value": "30900"
         }
       ]
     },
     "page": {
   ```

```
    "length": 3,
    "offset": 0
  }
}
```

3. Send the request.
   - In a REST Client, click SEND.
   - In the Swagger interface, click Execute.

   Response body:

```
{
  "page": {
    "offset": 0,
    "total": 229,
    "totalFilter": 12
  },
  "list": [
    {
      "id": "30888",
      "createdBy": "1",
      "createdOn": "2019-09-10T21:09:50.722Z",
      "updatedBy": "0",
      "updatedOn": "2019-09-10T21:13:46.304Z",
      "version": "5",
      "json": {
        "Invoice Id": "INV0004",
        "Customer Name": "APIName1",
        "Amount": 9007199254740991,
        "email": "API123@gmail.com",
        "Invoice Date": "2017-06-12T00:18:48Z"
      },
      "result": "",
      "deviceId": "3",
      "status": "SUCCESSFUL",
      "startTime": "2019-09-10T21:12:16.599Z",
      "endTime": "2019-09-10T21:13:17.062Z",
      "col1": "INV0004",
      "col2": "APIName1",
```

©2020 Automation Anywhere. All rights reserved.

```
      "col3": "9.007199254740991E15",
      "col4": "API123@gmail.com",
      "col5": "2017-06-12T00:18:48Z",
      "deviceUserId": "0",
      "queueId": "7",
      "comment": "",
      "automationId": "6",
      "totalPausedTime": "0",
      "error": "",
      "col6": "",
      "col7": "",
      "col8": "",
      "col9": "",
      "col10": ""
    },
    {
      "id": "30889",
      "createdBy": "1",
      "createdOn": "2019-09-10T21:09:51.383Z",
      "updatedBy": "0",
      "updatedOn": "2019-09-10T21:13:46.255Z",
      "version": "5",
      "json": {
        "Invoice Id": "INV0004",
        "Customer Name": "APIName1",
        "Amount": 9007199254740991,
        "email": "API123@gmail.com",
        "Invoice Date": "2017-06-12T00:18:48Z"
      },
      "result": "",
      "deviceId": "4",
      "status": "SUCCESSFUL",
      "startTime": "2019-09-10T21:12:23.841Z",
      "endTime": "2019-09-10T21:13:24.265Z",
      "col1": "INV0004",
      "col2": "APIName1",
```


©2020 Automation Anywhere. All rights reserved.

```
      "col3": "9.007199254740991E15",
      "col4": "API123@gmail.com",
      "col5": "2017-06-12T00:18:48Z",
      "deviceUserId": "0",
      "queueId": "7",
      "comment": "",
      "automationId": "6",
      "totalPausedTime": "0",
      "error": "",
      "col6": "",
      "col7": "",
      "col8": "",
      "col9": "",
      "col10": ""
    },
    {
      "id": "30890",
      "createdBy": "1",
      "createdOn": "2019-09-10T21:09:52.324Z",
      "updatedBy": "0",
      "updatedOn": "2019-09-10T21:13:46.347Z",
      "version": "5",
      "json": {
        "Invoice Id": "INV0004",
        "Customer Name": "APIName1",
        "Amount": 9007199254740991,
        "email": "API123@gmail.com",
        "Invoice Date": "2017-06-12T00:18:48Z"
      },
      "result": "",
      "deviceId": "5",
      "status": "SUCCESSFUL",
      "startTime": "2019-09-10T21:12:29.501Z",
      "endTime": "2019-09-10T21:13:30.102Z",
      "col1": "INV0004",
      "col2": "APIName1",
```


©2020 Automation Anywhere. All rights reserved.

```
      "col3": "9.007199254740991E15",
      "col4": "API123@gmail.com",
      "col5": "2017-06-12T00:18:48Z",
      "deviceUserId": "0",
      "queueId": "7",
      "comment": "",
      "automationId": "6",
      "totalPausedTime": "0",
      "error": "",
      "col6": "",
      "col7": "",
      "col8": "",
      "col9": "",
      "col10": ""
    }
  ]
}
```


Response header:

```
cache-control: no-cache, no-store, max-age=0, must-revalidate
connection: keep-alive
content-security-policy: default-src 'self'
content-type: application/json
date: Tue, 24 Sep 2019 19:40:09 GMT
expires: 0
pragma: no-cache
transfer-encoding: chunked
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
x-xss-protection: 1; mode=block
```

Related concepts
Workload Management API overview

Create a work item in a queue

Use the Workload Management (WLM) API to add or insert data for work items in an existing queue in your Enterprise Control Room.

Prerequisites

AAE_Queue Admin role
: You need a user account with the AAE_Queue Admin role to query and manage workload queues and work items in an Enterprise Control Room.

JSON Web Token (JWT)
: All Enterprise Control Room APIs require a JSON Web Token (JWT) to access the APIs. Generate an authentication token using the Authentication API.

- End point: `http://<your_control_room_url>/v2/wlm/queues/{id}/workitems`
- Method: POST

Procedure

1. Add an authentication token to the request header.
   Note: Use the Authentication API to generate a JSON Web Token.
2. Select the POST method.
3. In the URL, add the id for the queue you are adding the work item to.
   In this example you are adding a work item to the queue with id=7:

```
http://<your_control_room_url>/v2/wlm/queues/7/workitems
```

4. Enter the following parameters in the request body.
   Request body:

```
{
  "workItems": [
    {
      "json": {
           "Invoice Id": "INV909090",
        "Customer Name": "John Doe",
        "Amount": 100,
        "email": "jdoe@wunderground.com",
        "Invoice Date": "2019-01-10T00:18:48Z"
      }
    }
  ]
}
```

Response body:

```
{
  "list": [
```

©2020 Automation Anywhere. All rights reserved.

```
    {
      "id": "31363",
      "createdBy": "25",
      "createdOn": "2019-09-24T21:04:46.788Z",
      "updatedBy": "25",
      "updatedOn": "2019-09-24T21:04:46.788Z",
      "version": "0",
      "json": {
        "Invoice Id": "INV909090",
        "Customer Name": "John Doe",
        "Amount": 100,
        "email": "jdoe@wunderground.com",
        "Invoice Date": "2019-01-10T00:18:48Z"
      },
      "result": "",
      "deviceId": "0",
      "status": "READY_TO_RUN",
      "col1": "INV909090",
      "col2": "John Doe",
      "col3": "100.0",
      "col4": "jdoe@wunderground.com",
      "col5": "2019-01-10T00:18:48Z",
      "deviceUserId": "0",
      "queueId": "0",
      "comment": "",
      "automationId": "0",
      "totalPausedTime": "0",
      "error": "",
      "col6": "",
      "col7": "",
      "col8": "",
      "col9": "",
      "col10": ""
    }
  ]
}
```


©2020 Automation Anywhere. All rights reserved.

Response header:

```
cache-control: no-cache, no-store, max-age=0, must-revalidate
 connection: keep-alive
 content-length: 819
 content-security-policy: default-src 'self'
 content-type: application/json
 date: Tue, 24 Sep 2019 21:05:05 GMT
 expires: 0
 pragma: no-cache
 x-content-type-options: nosniff
 x-frame-options: SAMEORIGIN
 x-xss-protection: 1; mode=block
```

Related concepts
Workload Management API overview

Update work item data, results and status

Send a PUT request to update work item data, results and status.

Prerequisites

AAE_Queue Admin role
: You need a user account with the AAE_Queue Admin role to query and manage workload queues and work items in an Enterprise Control Room.

JSON Web Token (JWT)
: All Enterprise Control Room APIs require a JSON Web Token (JWT) to access the APIs. Generate an authentication token using the Authentication API.

Important: This API feature works in Enterprise Control Room Version 11.3.2 and later.

- URL: `http://<your_control_room_url>/v2/wlm/queues/{id}/workitems/{id}`
- Method: PUT

Status migration table

Existing Status	Can be moved to
Active	Unsuccessful
Data error	Deleted, Marked as complete, Ready to run
On hold	Deleted, Marked as complete, Ready to run
Ready to run Note: Queued workitems cannot be moved to any other state.	Deleted, On hold, Marked to complete

©2020 Automation Anywhere. All rights reserved.

Existing Status	Can be moved to
Complete	Deleted Note: Cannot be moved to Marked as complete or Ready to run.

Note:

- Use the Swagger definition files installed with your Enterprise Control Room to test the APIs. View the available Swagger APIs at `http://<your_control_room_url>/swagger/`.
- You can also use a REST client to complete this task.

Procedure

1. Add an authentication token to the request header.
   Note: Use the Authentication API to generate a JSON Web Token.
2. Select PUT as the method.
3. In the URL, add the id for the queue and the work item you are updating.
   URL example:

```
http://<your_control_room_url>/v2/wlm/queues/6/workitems/31365
```

4. Enter the following parameters in the request body.
   Request body:

```
{
  "version": "0",
  "json": {
        "Invoice Id": "INV909090",
        "Customer Name": "John Doe",
        "Amount": 100,
        "email": "jdoe@wunderground.com",
        "Invoice Date": "2019-01-10T00:00:01Z"
      },
  "result": "",
  "status": "ON_HOLD"
}
```

5. Send the request.
   - In a REST Client, click SEND.
   - In the Swagger interface, click Execute.

   Response body:

©2020 Automation Anywhere. All rights reserved.

```
{
  "id": 31365,
  "createdBy": 25,
  "createdOn": "2019-09-28T18:39:50.048Z",
  "updatedby": 25,
  "updatedOn": "2019-09-28T18:55:55.179Z",
  "version": 1,
  "json": {
    "Invoice Id": "INV909090",
    "Customer Name": "John Doe",
    "Amount": 100.0,
    "email": "jdoe@wunderground.com",
    "Invoice Date": "2019-01-10T00:00:01Z"
  },
  "result": "",
  "deviceId": 0,
  "status": "ON_HOLD",
  "col1": "INV909090",
  "col2": "John Doe",
  "col3": "100.0",
  "col4": "jdoe@wunderground.com",
  "col5": "2019-01-10T00:00:01Z",
  "col6": "",
  "col7": "",
  "col8": "",
  "col9": "",
  "col10": "",
  "deviceUserId": 0,
  "queueId": 5,
  "comment": "",
  "automationId": 0,
  "totalPausedTime": 0,
  "error": ""
}
```


- WLM work item life cycle
  Bulk processing of work items can be done from the WLM API or by uploading a CSV file of work items.

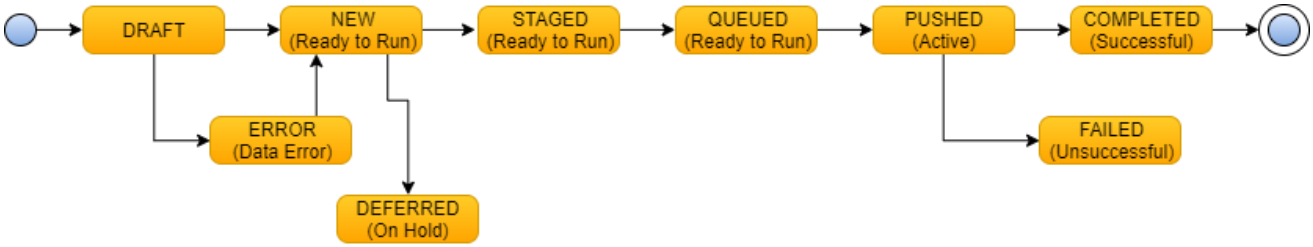
Related concepts
Workload Management API overview

WLM work item life cycle

Bulk processing of work items can be done from the WLM API or by uploading a CSV file of work items.

Work item life cycle

The following process flow table compares how the WLM API processes bulk work item uploads with how bulk work item uploads are processed from the UI. The UI hides or abstracts away a lot of the processing work flow. The diagram shows the work item status in all capital letters with the corresponding UI status in parenthesis.



Draft
: Work items are marked as DRAFT during ingestion of CSV file.

  Error (Data Error)
  : Work items failed in the validation phase are marked as ERROR.

New (Ready to Run)
: When ingestion process is completed, all work items are marked as NEW.

  Deferred (On Hold)
  : If initial processing of a work item is encounters, the work item is put into DEFERRED status.

    Move work items to On Hold state to suspend WLM processing until the work item is moved back to the Ready to run state

    .

Staged (Ready to Run)
: Work items are processed in predefined sorting order, Stager retrieves work items from the WORKITEMS table and adds them to the WORKITEMS_STAGING table that has a priority field. These prioritized work items are then marked as STAGED.

Queued (Ready to Run)
: Staged work items are then moved to IgniteMQ queue (blocking queue) where they can be pushed to the Bot Runners or devices for processing. Queued work items are marked as QUEUED.

Pushed (Active)
: When a work item is sent to a Bot Runner, the status is changed to PUSHED.

©2020 Automation Anywhere. All rights reserved.

Failed (Unsuccessful)
When a Bot Runner is unable to process a work item, the work item status is set to FAILED.

Completed (Successful)
Successfully processed work items are marked as COMPLETED.

Mapping of UI to API status for WLM work item processing

The following table shows the UI status and its corresponding API status.

UI	API
Complete	SUCCESSFUL
Unsuccessful	FAILED
Active	PUSHED
Error	DATA_ERROR
On hold	DEFFERED
Ready to run	NEW, QUEUED, or STAGED

Related tasks
Update work item data, results and status

Delete work items in a queue

Send a POST request from the WLM API to delete specific work items from specific queues.

Prerequisites

AAE_Queue Admin role
You need a user account with the AAE_Queue Admin role to query and manage workload queues and work items in an Enterprise Control Room.

JSON Web Token (JWT)
All Enterprise Control Room APIs require a JSON Web Token (JWT) to access the APIs. Generate an authentication token using the Authentication API.

- URL: `http://<your_control_room_url>/v2/wlm/queues/{id}/workitems/delete`
- Method: POST

Note:

- Use the Swagger definition files installed with your Enterprise Control Room to test the APIs. View the available Swagger APIs at `http://<your_control_room_url>/swagger/`.
- You can also use a REST client to complete this task.

Procedure

1. Add an authentication token to the request header.
   Note: Use the Authentication API to generate a JSON Web Token.
2. Select POST as the method.

©2020 Automation Anywhere. All rights reserved.

3. In the URL, add the id for the queue you are deleting work items from.
   URL example:

```
http://<your_control_room_url>/v2/wlm/queues/7/workitems/delete
```

4. Enter the following parameters in the request body.
   Request body:

```
{ "workitemId": [ 313665 ] }
```

5. Send the request.
   - In a REST Client, click SEND.
   - In the Swagger interface, click Execute.

   Response body:

```
OK
```

Related concepts
Workload Management API overview

Filters in an API request body

Filtering provides basic conditional queries and page control for processing web pages. There are 3 basic features related to filtering: filtering conditions, sorting columns, and pagination parameters.

Here is a representation of the JSON filtering structure used in the Automation Anywhere APIs.

```
{
  "filter": {
    "operator": "NONE",
    "operands": [
      null
    ],
    "field": "string",
    "value": "string"
  },
  "sort": [
    {
      "field": "string",
      "direction": "asc"
    }
```

©2020 Automation Anywhere. All rights reserved.

```
  ],
  "page": {
    "offset": 0,
    "length": 0
  }
}
```

The most basic part of this JSON object is the filter array.

Understanding filters

Basic filter

Filters can be used search for a single condition or they can be wrapped in logical operands AND and OR. Filtering can be a simple conditional evaluation of a single field. The operator, field, and value used in a filter are specific to the API they are used in.
Note: Values in the angle brackets < > include a list of all potential values. There should be only one value for each parameter.

Single parameter filter

```
{
  "filter": {
    "operator": "<NONE, lt, le, eq, ne, ge, gt, substring, and, or, no
t>",
    "field": "string",
    "value": "string"
  }
}
```

Two parameter filter

```
{
  "filter": {
    "operator": "<and, or>",
    "operands": [
      {
        "operator": "<NONE, lt, le, eq, ne, ge, gt, substring, and, or
, not>",
        "field": "string",
        "value": "string"
      },
```

©2020 Automation Anywhere. All rights reserved.

```
      {
        "operator": "<NONE, lt, le, eq, ne, ge, gt, substring, and, or
, not>",
        "field": "string",
        "value": "string"
      }
    ]
  }
}
```

Page

```
"page":{
    "offset":0,
    "length":0
}
```

Pagination rules parameters

- Offset:

  Type: integer

  The numeric value that indicates how many rows into a table that the filter starts evaluating.

- Length

  Type: integer

  The number of lines that are returned in a single page of results.

Sort

```
 "sort": [
    {
      "field": "string",
      "direction": "<asc, desc>"
    }
```

- Field: The field that you want the results to be filtered by. This must be a supported filterable field. Filterable fields vary depending on the API.
- Direction

©2020 Automation Anywhere. All rights reserved.

Type: Enum [desc, asc]

- asc = ascending (smallest to largest, 0 to 9, A to Z)
- desc = descending (largest to smallest, 9 to 0, Z to A)

API filter examples

Audit API filter example with createdOn and userName fields
: Create a filter that finds audit log entries for a specified date range for users with a specific string in their userName.

Audit API filter example with createdOn and userName fields

Create a filter that finds audit log entries for a specified date range for users with a specific string in their userName.

Request body

Finding the audit log entries you need is a formidable task. Use filtering to help narrow your results. The following example request identifies successful logins for users with the string "2fa" in their userName and that logged on to this Enterprise Control Room on December 5, 2019.

Example:

```
{
  "sort": [
    {
      "field": "createdOn",
      "direction": "desc"
    }
  ],
  "filter": {
    "operator": "and",
    "operands": [
      {
        "operator": "gt",
        "field": "createdOn",
        "value": "2019-12-05T00:00:00.001Z"
      },
      {
        "operator": "lt",
        "field": "createdOn",
```

©2020 Automation Anywhere. All rights reserved.

```
        "value": "2019-12-05T23:59:59.999Z"
      },
      {
        "operator": "eq",
        "field": "status",
        "value": "Successful"
      },
      {
        "operator": "substring",
        "field": "userName",
        "value": "2fa"
      }
    ]
  }
}
```

sort

- field: the name of the field used to sort the response.
- direction: the sort order. It can be asc, ascending, or desc, descending.

filter

Filter consists for an operator, value, and field. Filters are operands when used in conjunction with a boolean operator, such as and.

- operands: filters are used as operands when combined in a filter by using a boolean operator. There are two available boolean operators:
  - or: one of the conditions must be met.
  - and: all of the conditions must be met.
- operator: there are 11 operators `NONE, lt, le, eq, ne, ge, gt, substring, and, or, not`. And and or are used to evaluate multiple filters together. The other operators are used to evaluate values within individual filters. Not all operators work with all fields.
- field: the name of the field used in the filter.
- value: the value of the field to be evaluated.

Related concepts
Filters in an API request body
Related tasks
Audit API

User management example filter

This example filter is based on the User Management API fields and parameters. This filter searches for the username and the name of user.

This filter searches for the string bot-creator in the username field and the string Adweta in the firstName field.

```
{
  "sort": [
    {
      "field": "username",
      "direction": "asc"
    }
  ],
  "filter": {
    "operator": "and",
    "operands": [
      {
        "operator": "substring",
        "value": "bot-creator",
        "field": "username"
      },
      {
        "operator": "substring",
        "value": "Adweta",
        "field": "firstName"
      }
    ]
  }
}
```

sort

- field: the name of the field used to sort the response.
- direction: the sort order. It can be asc, ascending, or desc, descending.

filter

Filter consists for an operator, value, and field. Filters are operands when used in conjunction with a boolean operator, such as and.

- operands: filters are used as operands when combined in a filter by using a boolean operator. There are two available boolean operators:
  - or: one of the conditions must be met.
  - and: all of the conditions must be met.

©2020 Automation Anywhere. All rights reserved.

- operator: there are 11 operators `NONE, lt, le, eq, ne, ge, gt, substring, and, or, not`. And and or are used to evaluate multiple filters together. The other operators are used to evaluate values within individual filters. Not all operators work with all fields.
- field: the name of the field used in the filter.
- value: the value of the field to be evaluated.

Repository management filter with name and lastModified fields

This example filter is based on the Repository Management API fields and parameters. This filter example searches on the bot lastModified and name fields.

This filter searches for bots in the Enterprise Control Room repository with the string "finance" in the name of the files modified between January 7, 2020 and January 9, 2020.
Note: The Repository management API uses role based access. That means users can only see the files and folders to which they have access.

```
{
  "sort": [
    {
      "field": "directory",
      "direction": "desc"
    },
    {
      "field": "name",
      "direction": "asc"
    }
  ],
  "filter": {
    "operator": "and",
    "operands": [
      {
        "operator": "substring",
        "value": "finance",
        "field": "name"
      },
      {
        "operator": "gt",
        "value": "2020-01-07T00:00:00.001Z",
        "field": "lastModified"
      },
```

```
      {
        "operator": "lt",
        "value": "2020-01-09T00:00:00.001Z",
        "field": "lastModified"
      }
    ]
  }
}
```

sort

- field: the name of the field used to sort the response.
- direction: the sort order. It can be asc, ascending, or desc, descending.

filter

Filter consists for an operator, value, and field. Filters are operands when used in conjunction with a boolean operator, such as and.

- operands: filters are used as operands when combined in a filter by using a boolean operator. There are two available boolean operators:
  - or: one of the conditions must be met.
  - and: all of the conditions must be met.
- operator: there are 11 operators `NONE, lt, le, eq, ne, ge, gt, substring, and, or, not`. And and or are used to evaluate multiple filters together. The other operators are used to evaluate values within individual filters. Not all operators work with all fields.
- field: the name of the field used in the filter.
- value: the value of the field to be evaluated.

Whitelist file extensions to restrict upload of malicious files

As a Enterprise Control Room Administrator you can add file extensions to the configuration file that restricts the user from uploading files that have extensions other than the ones whitelisted in it.

Add a new file extension to the whitelist from the Enterprise Control Room UI:

Procedure

1. Log in to the Enterprise Control Room as an administrator.
2. Navigate to Administration > Settings > Client application.
3. Click the Edit option.
   The page opens in edit mode.
4. Select Only listed extensions option.
5. Enter the file extension to whitelist in the `Whitelisted file extensions` text box and click Add.
6. Scroll up and click Save changes.

©2020 Automation Anywhere. All rights reserved.

Control room troubleshooting issues

Known troublshooting issues and solutions related to the control room are documented here. Use the Send Feedback option at the bottom of every content page to provide constructive feedback and suggestions.

- Perform Enterprise Control Room health-check with Automation Anywhere diagnosis utility
  The Automation Anywhere Control Room Diagnostic Utility is an automated checkpoint verification tool that is used to view application relevant information and diagnose errors with the application for quick resolution. This feature is available in Enterprise Control Room Version 11.3.4 and later.
- Troubleshooting bot deployment
  Issue: I'm unable to deploy a bot because I get the following – Cannot run this interactive bot <bot name> at this time as another interactive bot is currently running.
- Property to schedule triggers efficiently
  The `org.quartz.scheduler.batchTriggerAcquisitionMaxCount` property enables you to define the maximum number of triggers that a scheduler node can acquire (for firing) at one time. The default value is 5.
- Troubleshooting Automation File Permissions
  Issue: When you upload an automation file from Enterprise client in a distributed environment, the following error message appears – Storage does not exists for job <job number>.

Perform Enterprise Control Room health-check with Automation Anywhere diagnosis utility

The Automation Anywhere Control Room Diagnostic Utility is an automated checkpoint verification tool that is used to view application relevant information and diagnose errors with the application for quick resolution. This feature is available in Enterprise Control Room Version 11.3.4 and later.

Prerequisites

Ensure that:

- The Enterprise Control Room is installed.
- PowerShell version 4.0 or above is installed.
- You run the utility with elevated acess privileges i.e.in administrative mode. For example:
  - For all Automation Anywhere Windows Services when you run the utility invoked in administrative mode, it fetches Status, Memory, and CPU usage of the service. But if the utility is not used with elevated access, then it can fetch only the Status of the service.
  - For Enterprise Control Room Ports, when you run the utility in administrative mode, it fetches the process name for respective Enterprise Control Room ports and the command line of the process. When you use it without elevated access it fetches only the process name for respective Enterprise Control Room ports.

The utility is bundled with the Automation Anywhere Enterprise Control Room setup and can be run as a diagnostic tool at any point in time to set check-points for verifying errors and issues.

©2020 Automation Anywhere. All rights reserved.

The diagnostic utility can be run from any of the file locations provided it is run on the machine on which the Enterprise Control Room application is installed. It does not necessarily have to be from the application installation path.

Procedure

1. Navigate to the path where the utility is stored.
   For example, <Application Installation Location>\Enterprise
2. Run the AA.DiagnosticUtility.CR.exe application file to launch the utility.
3. Click Yes in the Disclaimer window to include sensitive information such as IP address and Computer Name.
   After the utility completes execution, it generates an HTML report which opens in your default browser. The utility automatically captures checkpoints related to the System, Product, Automation Anywhere Windows Services, Enterprise Control Room Settings and Ports. It also captures errors and failure events in a log file.

Next steps

- Access the HTML report from <SystemDrive>:\ProgramData\AutomationAnywhere\CRLogs<YYYYMMDDHHMMSS>\DiagnosticUtilityCrReport<YYYYMMDDHHMMSS>.html.
- Use the automated checkpoint error messages and logs from the default logs folder to resolve the application issues. The log files are consolidated in a compressed file - <SystemDrive>:\ProgramData\AutomationAnywhere\CRLogs<YYMMDDHHMMSS>\Logs<YYMMDDHHMMSS>.zip.

Troubleshooting bot deployment

Issue: I'm unable to deploy a bot because I get the following – Cannot run this interactive bot <bot name> at this time as another interactive bot is currently running.

Cause:
Bots must be deployed one at a time. You cannot deploy more than one bot concurrently.
Solution:
Wait until the other bot finishes deploying then deploy your bot again. You can see bot deployment statuses from the In-progress activity page of the Enterprise Control Room.

Related tasks
Monitor in progress activity

Property to schedule triggers efficiently

11.3.3.1 The `org.quartz.scheduler.batchTriggerAcquisitionMaxCount` property enables you to define the maximum number of triggers that a scheduler node can acquire (for firing) at one time. The default value is 5.

The higher the number, the more efficient the firing is, when the number of triggers to fire at the same time increases. However, this can create an imbalance in the load between the cluster nodes. You need to modify the value of the `org.quartz.scheduler.batchTriggerAcquisitionMaxCountproperty` based on the number of schedule triggers configured to fire at the same time.

©2020 Automation Anywhere. All rights reserved.

Consider that the number of triggers the scheduler node needs to fire at a time is increased to 20. To trigger the schedules efficiently, do the following:

Procedure

1. Open the config folder from the Enterprise Control Room directory.

   For example, default location is:

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

2. Locate the `quartz.properties` file.

   If the file does not exist in your Enterprise Control Room directory, create it.

3. Open the `quartz.properties` file in the edit mode.
4. Add the following property option to the `quartz.properties` file.

```
org.quartz.scheduler.batchTriggerAcquisitionMaxCount=10
```

5. Save the `quartz.properties` file.
6. Restart the following services in this order:
   a) Automation Anywhere Control Room Caching
   b) Automation Anywhere Control Room Messaging
   c) Automation Anywhere Control Room Service

Troubleshooting Automation File Permissions

Issue: When you upload an automation file from Enterprise client in a distributed environment, the following error message appears – Storage does not exists for job <job number>.

Cause:

This issue is caused by one of fthe following reasons –

- The Enterprise Control Room installation wizard did not create the folder where the automation files will be uploaded.
- The folder where the automation files are to be uploaded does not have the required shared permission.

Solution:

1. Verify that the folder where the Automation Anywhere files are to be uploaded is created.

   For example, if you installed the client in the default location, you can open Windows Explorer and navigate to your C drive, Program Files. From here, you should see the Automation Anywhere folder.

2. Apply the Enable inheritance and shared permissions to the folder.
   a) Right-click the folder and click Properties.

©2020 Automation Anywhere. All rights reserved.

The Folder Properties dialog box appears.

b) Select the Security tab and then click Advanced.

The Advanced Security Settings dialog box appears.

c) Click Enable Inheritance, then click Apply.

- Enterprise Control Room : Files added to anti-virus exceptions list
  This article provides list of Automation Anywhere files that need to be added to the anti-virus list.
- Recover schedules post upgrade
  A user with scheduling permissions can recover the list of schedules that might have missing from the Schedules page after migrating to Automation Anywhere version 11.3 .
- Troubleshoot Active Directory multi-forest Control Room
  Use this topic as a reference to troubleshoot issues that you encounter in an Enterprise Control Room configured in Active Directory (AD) multi-forest environment.
- Update deployment settings file to maintain Remote Desktop session
  In case of network fluctuations, a system administrator is able to manage the continuity of the organization's Remote Desktop Protocol (RDP) session by customizing the Automation Anywhere Enterprise Control Room deployment properties file.

Enterprise Control Room : Files added to anti-virus exceptions list

This article provides list of Automation Anywhere files that need to be added to the anti-virus list.

All Enterprise Control Room binary files are digitally signed with Automation Anywhere company's certificate. This adds to security at binary level. This means that all the product files are not detected as a virus by your enterprise anti-virus.

However, if for some reason there are exceptions, you can add the following .exe files to the exceptions list of the anti-virus installed on your computer.

Table 1. Files for anti-virus exceptions list

Path/Location	Filename
<install location>\traefik For example, C:\Program Files\Automation Anywhere\Enterprise\traefik\	traefik.exe
<install location>\service For example, C:\Program Files\Automation Anywhere\Enterprise\service\	AutomationAnywhere.Controlroom.Service.exe
<install location>\rdp For example, C:\Program Files\Automation Anywhere\Enterprise\rdp\	AARemoteMachineConnector.exe

©2020 Automation Anywhere. All rights reserved.

Path/Location	Filename
<install location>\nssm For example, C:\Program Files\Automation Anywhere\Enterprise\nssm\	nssm.exe
<install location>\jre\bin For example, C:\Program Files\Automation Anywhere\Enterprise\jre\bin\	• jabswitch.exe x • java.exe x • java-rmi.exe x • javaw.exe x • jjs.exe x • keytool.exe x • kinit.exe • klist.exe • ktab.exe • orbd.exe • pack200.exe • unpack200.exe • policytool.exe • rmid.exe • rmiregistry.exe • servertool.exe • tnameserv.exe
<install location>\elasticsearch\jdk\bin For example, C:\Program Files\Automation Anywhere\Enterprise\elasticsearch\jdk\bin\	• jabswitch.exe x • java.exe x • javaw.exe x • jjs.exe x • keytool.exe x • kinit.exe • klist.exe • ktab.exe • pack200.exe • unpack200.exe • rmid.exe • rmiregistry.exe

Recover schedules post upgrade

A user with scheduling permissions can recover the list of schedules that might have missing from the Schedules page after migrating to Automation Anywhere version 11.3 .

©2020 Automation Anywhere. All rights reserved.

Prerequisites

Ensure the user who is performing the recovery has access to the Control Room database as a query to search the schedules should be executed. Also, if multiple schedules are involved, you need to use a REST API to perform a deactivate action.

How to recover schedules

Once you have migrated to Automation Anywhere Version 11.3, if you notice that your schedules are not listed in the Schedules page, you must follow certain steps to recover those so that your automation can continue without interruption.

To summarize, you must first search for the schedules that are missing, login to the Control Room, deactivate the schedules, and re-activate or delete the schedules.

Procedure

1. To search for missing schedules execute the following SQL query on the Control Room database,

```
SELECT
```

```
a_schedule.id
```

```
FROM
```

```
automation_schedule
                    a_schedule
```

```
JOIN automations automations ON
                        automations.id = a_schedule.id
```

```
WHERE
```

```
(
```

```
(a_schedule.next_run_datetime
                            < Sysutcdatetime() OR a_schedule.next_run_datetim
e is
                            null)
```

```
AND automations.status =
                                1
```

```
)
```

   Note: Upon execution, the SQL query returns the list of missing schedule ids. Use these schedule ids to perform steps shown below to recover your missing schedules.
2. You can now choose to deactivate the schedules one at a time using a URL or in bulk using a REST API.
   - Deactivate schedules one at a time using URL

     a) Login to Control Room -

     ```
     http(s)://<hostname>:<port>
     ```

b) Type the URL to view the Schedule details page -

```
http(s)://<hostname:port>/#/activity/scheduled/<missing_schedule_id>/
view
```

For example for the missing schedule with id 12, use -

```
https://localhost:8081/#/activity/scheduled/12/view
```

c) Click Deactivate button given at the top of the page.

d) Repeat steps b and c for other missing schedules.

- Deactivate schedules in bulk using REST API

  a) Use the Authentication API to logon to the Control Room.

  b) Use Put method -

  ```
  HTTP PUT
  ```

  c) Use Request URL -

  ```
  http(s)://<hostname>:<port>/v1/schedule/automations/deactivate
  ```

  For example,

  ```
  https://localhost:8081/v1/schedule/automations/deactivate
  ```

  d) Provide authorization token -

  ```
  Header: X-Authorization
                              token
  ```

  e) Specify content type -

  ```
  Content-Type:
                              application/json
  ```

  f) Provide schedule ids in body data -

  ```
  Body:
                              [<missing_schedule_id1,
                              missing_schedule_id2,..missing_schedule_i
  dn>]
  ```

  For example,

  ```
  Body: [12, 13, 14, 15, 16,
                                  20]
  ```

3. Go to Control Room to view the missing schedules in the Schedules page
4. Select the check box beside the required schedule to Activate or Delete multiple schedules .

Related tasks

Activate or deactivate a schedule

Delete a schedule

Troubleshoot Active Directory multi-forest Control Room

Use this topic as a reference to troubleshoot issues that you encounter in an Enterprise Control Room configured in Active Directory (AD) multi-forest environment.

Issues, possible causes and solution

Issue	Cause	Solution
KrbException: Server not found in Kerberos database (7)	The hostname used in the LDAP URL is pointing to the load balancer and not FQHN	Point the hostname used in the LDAP URL to FQHN
javax.security.auth.login.LoginException: Client not found in Kerberos database (6)	Username is incorrect	Type the username that is present in the Kerberos database
LDAP: error code 49 - 8009030C: LdapErr: DSID-0C09056D, comment: AcceptSecurityContext error, data 52e, v2580	Error code 52e - incorrect password could be due to many other issues such as DNS setup in the Active Directory (AD).	The AD admin can check the DNS settings
[Krb5LoginModule] authentication failed or javax.security.auth.login.LoginException: null (68)	Domain in the username is not in uppercase. For example, john@ENTERPRISECR.COM Domain name not being resolved can cause this as DNS is not able to find the KDC	Type the username in uppercase. For example, JOHN@ENTERPRISECR.COM
javax.security.auth.login.LoginException: Pre-authentication information was invalid (24)	Invalid password	Type the correct password
GSS start failed [Caused by GSSException: No valid credentials provided (Mechanism level: Fail to create credential. (63) - No service creds)]]	FQHN is not used in the LDAP URL	Use FQHN in the LDAP URL
javax.security.auth.login.LoginException: Clock skew too great (37)	The system clock between the Control Room host and AD host is not synchronized; by default it is 5 minutes.	The AD admin can check the attribute on the AD side
java.net.SocketException: Connection reset	Network connection issue between the Control Room host and AD host	The system admin can check the network connection between the Control Room host and AD host.

System Commands on AD host

Following system commands can be run on the AD host to:

- Check Kerberos Distribution Center (KDC) is running:

```
nslookup -type=srv _kerberos._tcp.ENTERPRISECR.COM
```

- Check GC is running:

```
nslookup -type=srv _gc._tcp.ENTERPRISECR.COM
```

©2020 Automation Anywhere. All rights reserved.

- Check LDAP is running:

```
nslookup -type=srv _ldap._tcp.ENTERPRISECR.COM
```

- Check domain trust:

```
nltest /domain_trusts
```

- Show details of a specific domain:

```
nltest /dsgetdc:ENTERPRISECR.COM
```

- Defining key distribution centers
  When one or more key distribution centers (KDCs) are inaccessible, resulting in delayed or no response and the domain list is shown as empty, an Enterprise Control Room administrator can define the KDCs in the um.properties file.
- Guidelines to set up service users for auto discovery mode
  Enable the Automation Anywhere Enterprise Control Room to discover and list domains and sites in an organization. Use this topic as reference to resolve issues that arise during creation of service users.

Related tasks
Defining key distribution centers
Related reference
Guidelines to set up service users for auto discovery mode

Defining key distribution centers

When one or more key distribution centers (KDCs) are inaccessible, resulting in delayed or no response and the domain list is shown as empty, an Enterprise Control Room administrator can define the KDCs in the um.properties file.

An Enterprise Control Room administrator is allowed to manually define KDCs in um.properties file so the request is forwarded only to the defined KDCs.

Procedure

1. Run the command to determine the KDCs for the domain:

```
nslookup -type=srv _kerberos._tcp.MYDOMAIN.COM where MYDOMAIN.COM is the d
omain.
```

   All the KDCs for the in_kerberos._tcp.EXAMPLE.MYDOMAIN.COM SRV service location are listed:

```
priority = 0
weight = 100
```

©2020 Automation Anywhere. All rights reserved.

```
port = 88
svr hostname = hostname2.example.mydomain.com
_kerberos._tcp.EXAMPLE.MYDOMAIN.COM SRV service location:
priority = 0
weight = 100port = 88
svr hostname = hostname2.example.mydomain.com
_kerberos._tcp.EXAMPLE.MYDOMAIN.COM SRV service location:
priority = 0
weight = 100
port = 88
svr hostname = hostname1.example.mydomain.com
svr hostname = hostname2.example.mydomain.com
```

2. Locate the um.properties file in the installation directory.
3. Append the following entry:

```
um.ldap.kdcs='EXAMPLE.MYDOMAIN.COM:sjcsrvbkp.example.mydomain.com:sjcsrv.e
xample.mydomain.com'
```

Tip:
- Domain has to be the first token, followed by one or more KDCs and separated by colons.
- Each domain is separated by commas. For example, the following has two domains: the first domain has three KDCs and the second domain has two KDCs:

```
um.ldap.kdcs='domain1.com:host1.domain1.com:host2.domain1.com:host3.do
main1.com,domain2.com:host1.domain2.com:host2.domain2.com'
```

This will force the request to be forwarded to either one of the two KDCs for this domain. If the domain in the LDAP URL is different than the username or more domains will need to be supported, all domains with the corresponding KDCs have to be defined in that entry.

If you have defined multiple KDCs in the um.properties file, you might experience a delayed response either in accessing the Enterprise Control Room or while changing the LDAP settings. In this case, define the KDCs one at a time so that the KDC contributing to the delay can be identified. Troubleshoot and resolve this KDC before defining it in the um.properties file.

4. Save the file and restart these services: Automation Anywhere Control Room Caching, Automation Anywhere Control Room Messaging, and Automation Anywhere Control Room Service.

Related reference
Guidelines to set up service users for auto discovery mode

Guidelines to set up service users for auto discovery mode

11.3.2 Enable the Automation Anywhere Enterprise Control Room to discover and list domains and sites in an organization. Use this topic as reference to resolve issues that arise during creation of service users.

Follow the below guidelines to resolve issues when you are creating service users:

- It is recommended to create a service user in a parent domain.
- If Key Distribution Centers (KDCs) are already defined in um.properties file, comment out the um.ldap.kdcs entry by putting a '#' in the front of the entry. This allows the auto discovery process to auto discover all the KDCs.
- If the above does not work, remove the comment for um.ldap.kdcs entry and define KDCs for all domains across all the forests. For this the AD admin has to be involved on the full list of domains in your AD system.
- If KDC is not defined in um.properties file, try to define one with all the KDCs for all domains across all forests.

  See Defining key distribution centers for details on setting up KDCs in um.properties file.

Related tasks
Defining key distribution centers

Update deployment settings file to maintain Remote Desktop session

In case of network fluctuations, a system administrator is able to manage the continuity of the organization's Remote Desktop Protocol (RDP) session by customizing the Automation Anywhere Enterprise Control Room deployment properties file.

To keep RDP sessions connected in case of network fluctuation for specific time period, customize the deployment.properties settings file that is stored in the <application path>/config folder.

Procedure

1. Go to the config folder in the application path. For example, C:\Program Files (x86)\Automation Anywhere\Enterprise\Control Room\config\
2. Open the deployment.propertie file in edit mode.
   The default properties are shown as:

   ```
   rdp.desktop.height=768
   rdp.desktop.width=1366
   rdp.port=3389
   ```

3. Add the following properties to customize your RDP sessions:

©2020 Automation Anywhere. All rights reserved.

```
rdp.status.timeout.interval=30
rdp.acquire.total.timeout.interval=120
wait.for.run.after.rdp.acquired=3
```

11.3.2

```
wait.for.seconds.to.close.rdp.after.device.disconnected=30
rdp.process.watcher.interval.seconds=30
rdp.close.on.bot.execution.complete=true
```

Note: The default values for status timeout, acquire total timeout interval, wait for run after rdp acquired are configured in the seconds time format. See Remote Desktop Protocol session settings description for more information on each setting.

- Remote Desktop Protocol session settings description
  Use this as a reference to customize the deployment.properties settings file that is used to maintain the Remote Desktop Protocol (RDP) session during bot deployment.

Related reference
Remote Desktop Protocol session settings description

Remote Desktop Protocol session settings description

Use this as a reference to customize the deployment.properties settings file that is used to maintain the Remote Desktop Protocol (RDP) session during bot deployment.

The table below describes each property for customizing your RDP sessions:

Property	Default value	Description
rdp.desktop.height	786	Desktop height of the remote desktop (screen resolution)
rdp.desktop.width	1366	Desktop width of the remote desktop (screen resolution)
rdp.port	3389	Remote Desktop Protocol (RDP) port. Update this if a different po used.
rdp.status.timeout.interval	30 seconds	The communication response ti between Enterprise Control Roo and Enterprise client to verify the machine status for which RDP session is to be launched.

©2020 Automation Anywhere. All rights reserved.

Property	Default value	Description
rdp.acquire.total.timeout.interval	120 seconds	The maximum time for which th server waits to begin the Bot Run session.
wait.for.run.after.rdp.acquired	3 seconds	The maximum time for which th server waits to begin the session (zero) before the user profile is invoked after which the actual us session begins.
11.3.2 wait.for.seconds.to.close.rdp.after.device.disconnected	30 seconds	The maximum time for which th server waits for a device to resun Bot Runner session after which t session is dropped.
11.3.2 rdp.process.watcher.interval.seconds	30 seconds	The time interval for which the R watcher keeps polling to check whether the Bot Runner session active or not. If the Bot Runner session is inactive, the RDP sessi dropped. Note: This property is enabled or rdp.close.on.bot.execution.comp is set to true.
11.3.2 rdp.close.on.bot.execution.complete	true	The setting allows the Enterprise client to communicate with the Enterprise Control Room to relea Bot Runner session after the play completes bot execution. If any changes are made to this proper the Enterprise Control Room ser need to be restarted for the char to take effect.

Related tasks
Update deployment settings file to maintain Remote Desktop session

Guidelines for General Data Protection Regulation

The General Data Protection Regulation (GDPR) is one of the strictest compliance frameworks for maintaining privacy of personal data. The GDPR defines personal data as any data that can be used to identify a natural person (Data Subject).

©2020 Automation Anywhere. All rights reserved.

For the most current description of Automation Anywhere GDPR compliance statement, see Master License Agreement and Cloud Security and Compliance with Data Privacy.

©2020 Automation Anywhere. All rights reserved.