Automation Anywhere Version A2019

Legal Notices

Content

Explore

Welcome to the Explore pages for Automation Anywhere Enterprise A2019. This collection of topics is designed to introduce you to our latest RPA and Intelligent Automation platform.

Overview

Enterprise A2019 is the RPA industry's first purely web-based Intelligent Automation platform that is cloud-native. Delivered in the Cloud or On-Premises, Enterprise A2019 is designed for ease of use by all types of users across technical skill levels. The platform enables businesses of all sizes to achieve unprecedented scale with enterprise-class security, data privacy, and reduced time to value and costs of ownership. With Enterprise A2019, businesses can also leverage built-in artificial intelligence (AI) capabilities and easily integrate third-party AI solutions, such as computer vision, natural language processing, and predictive modeling—all with the simplicity of drag-and-drop AI into any automation workflow.

The Enterprise A2019 platform also includes attended automation and plug-ins that enable business users to automate tasks from within their business applications such as Microsoft Excel and Salesforce. This capability makes automation of front-office processes easier, faster, and more cost-efficient.

Enterprise A2019 is available globally and in 10 languages, including English, French, German, Japanese, Korean, Italian, Portuguese, Spanish, Simplified Chinese, and Traditional Chinese.

Resources

For a hands-on introduction to Enterprise A2019, see Training - What's New in A2019. This is a free Automation Anywhere University course that provides an overview of core capabilities and features.

Note: To access this course, you must first be registered and logged in to your Automation Anywhere University or A-People account.

Available products

The Enterprise A2019 platform includes the following offerings:

- Enterprise A2019 delivered in the cloud, hosted by Automation Anywhere with no client installation or additional infrastructure required
- Enterprise A2019, the full platform delivered On-Premises
- Enterprise A2019 Free Trial, with 30 days to try the cloud-based offering with full tech support included during the trial period
- Community Edition, a free web-based option for users to experience a wide-range of Enterprise A2019 bot creation capabilities

Discover more about Automation Anywhere Enterprise by browsing these topics:

- Enterprise A2019 Release Notes
  This topic describes new capabilities, changed features, fixed features (resolved issues), security fixes, deprecated features, and known behavior or limitations.

- Enterprise A2019 feature comparison matrix
  Use the feature comparison matrix to compare the Enterprise A2019 features with the Automation Anywhere Enterprise Version 11.3.x features.
- Enterprise A2019 FAQ
  For details and questions on the latest Automation Anywhere platform, Enterprise A2019, review this FAQ.
- Automation Anywhere Enterprise Overview
  The Automation Anywhere Enterprise Digital Workforce platform is the foundation to deliver the automation of complex business work, securely, and at scale.
- Attended automation
  Automation Anywhere provides a robust RPA platform for attended automation that enables humans to collaborate with bots for completing tasks efficiently.
- Security architecture
  Many of the largest financial organizations in the world rely on Automation Anywhere's secure digital workforce platform to automate security-sensitive operations.
- General Data Protection Regulation guidelines
  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).

Related concepts
Enterprise A2019 Release Notes
Automation Anywhere Enterprise Overview
Security architecture

Enterprise A2019 Release Notes

This topic describes new capabilities, changed features, fixed features (resolved issues), security fixes, deprecated features, and known behavior or limitations.

Follow the links to view the release note updates for the respective release.

- Enterprise A2019.12 Release Notes
  Review the new features, supported packages, changed features, fixed features, and known limitations in the Enterprise A2019.12 (Build 4105) release. There are no security fixes in this release.
- Enterprise A2019.11 Release Notes
  Review the new features, supported packages, changed features, fixed features, and known limitations in the Enterprise A2019.11 (Build 3337) release. There are no security fixes in this release.
- Enterprise A2019.10 Release Notes
  Review the new features, supported packages, changed features, fixed features, and known limitations in Enterprise A2019.10 (Build 2545). There are no security fixes in this release.
- Enterprise Version A2019 (Build 2094) Release Notes
  These release notes describe new features, changed features, fixed features, security fixes, deprecated features, and known limitations in Enterprise Version A2019 (Build 2094).
- Enterprise Version A2019 (Builds 1598 and 1610) Release Notes
  These release notes describe new features, changed features, fixed features, security fixes, deprecated features, and known limitations in Enterprise Version A2019 (Builds 1598 and 1610).
- Enterprise Version A2019 (Builds 1082 and 1089) Release Notes
  These release notes describe new features, changed features, fixed features, security fixes, deprecated features, and known limitations in Enterprise Version A2019.

- Enterprise A2019 (Build 550) Release Notes
  These release notes describe new features, changed features, fixed features, security fixes, deprecated features, and known limitations in Enterprise A2019 (Build 550).
- Enterprise A2019 (Build 543) Release Notes
  These release notes describe new features, changed features, fixed features, security fixes, deprecated features, and known limitations in Enterprise A2019 (Build 543).

Related reference
Enterprise A2019 feature comparison matrix
Enterprise A2019 FAQ

Enterprise A2019.12 Release Notes

Release date: 11 May 2020

Review the new features, supported packages, changed features, fixed features, and known limitations in the Enterprise A2019.12 (Build 4105) release. There are no security fixes in this release.

- Enterprise A2019
- IQ Bot A2019
- Bot Insight A2019

Enterprise A2019

New features
Migration from 11.x and 10.x TaskBots and MetaBots to A2019 (currently available only to those in the Migration Early Adopter Program)   Enterprise A2019   Migration to Enterprise A2019 is currently only available to select customers through our Migration Early Adopter Program. If you are interested in learning more about this program and requirements, please contact your Automation Anywhere representative.   • Migrate TaskBots and MetaBots created in 10.x to Enterprise A2019.   Migrate Enterprise bots   • The summary report generated by the Bot Scanner now provides information about the number of bots that can or cannot be migrated to A2019.   Analyze reports   • (11.x only) Additional support is provided for packages and variables.   Package mapping for migration | Variable mapping for migration   • (11.x only) Migration APIs enable you to migrate a single 11.x bot or entire folders of bots to A2019. Use the Repository Management API to identify bots and folders for migration.

New features
Migration APIs	Repository Management API
Integrate Enterprise Control Room with a remote Git repository Enterprise A2019 Integrate the Enterprise Control Room with remote Git repositories to manage bot version controls, and back up and restore bots and the dependent files. The integration ensures one-to-one mapping of bots between the Enterprise Control Room and the remote Git file structure. When you perform a bot check-in, a Git commit is performed at the remote Git host. Integrating Enterprise Control Room with Git repositories
Additional actions in the Interactive forms package Enterprise A2019 and Community Edition The Interactive forms package includes the following actions: • Set focus: Sets the focus on the selected form element. • Highlight: Highlights the selected element of a form. • Unhighlight: Removes the highlight from the selected element of a form. Interactive forms package
Form builder enhancements for interactive forms Enterprise A2019 and Community Edition The form builder includes the following elements: • Document: Use this element to render an image (.jpg) or PDF file along with the form. • Password: Use this element for a field that requires masking of the input data. Create a form
Run Task Bot option for attended Bot Runner (Service Cloud case ID: 00453797) Enterprise A2019 and Community Edition If the default device is mapped to the Bot agent, a user with an attended Bot Runner license in the Enterprise Control Room can now use the Run Task Bot option from the bot context menu (vertical ellipsis) to run the bot. Run a bot
New features in Universal Recorder and actions that use the recorder feature

New features

Enterprise A2019 and Community Edition
 	
• Secure recording mode ensures that sensitive data is not stored in the bots. When secure recording mode is enabled, the bots do not capture application images or values.
 	
   Actions in the Image Recognition, Mouse, OCR, Screen, and Recorder packages support this feature.
 	
• JRE 6 is supported on both 32-bit and 64-bit systems.
• After you capture an object, you are returned to the window containing the Bot editor.
 	
   Actions in the Image Recognition, Mouse, OCR, Screen, and Recorder packages support this feature.
 	
Recording tasks in applications that run on JRE 6 | Secure recording mode

Insert a work item action Enterprise A2019 and Community Edition The Insert work item action provides you the flexibility to insert a work item from an existing queue to another queue as part of the bot execution. You can orchestrate multiple bots, enabling optimal device utilization through the queueing mechanism of workload management. Workload package
View error details of a work item Enterprise A2019 and Community Edition You can view the reason for a workload automation failure in the new Error section on the View work item details page. View work items
Extract text from windows Enterprise A2019 and Community Edition Use the Capture text of window action to extract text from a window and save it to a string variable. You can capture text from UNIX shells and Windows applications. App Integration package
Store string values securely in a credential variable Enterprise A2019 and Community Edition Configure a credential variable to hold a user-provided value or a credential from the Credential Vault. A credential variable cannot be converted to another data type, and the value cannot be displayed in a message box or written to a file.

New features
User-defined variables: Credential
Preload packages for improved bot performance Enterprise A2019 and Community Edition Preload packages on your local device to shorten the bot runtime. When you preload packages used in a bot, the system skips the package download process at bot runtime, thereby improving the bot performance. Preload packages
New features in the If and Loop packages Enterprise A2019 and Community Edition   - Execute actions based on whether the value of the source datetime variable is Equal to or Not Equal to, or is Greater than or Equal to, or is Lesser than or Equal to the value of the target datetime variable.   - Execute actions on migrated bots based on whether Web control exists or is active.   - Configure a Loop action with multiple conditions.   Specify whether all or either of the conditions must be met. If package | Loop package
Run a bot by inserting a file variable in the Run action Enterprise A2019 and Community Edition The Task Bot > Run action now supports a file variable input in the Task Bot to run field.
Configure a table variable using the Assign action in Data Table package Enterprise A2019 and Community Edition You can use this action to manually enter values, assign column names, specify the column data type (string, number, datetime, or Boolean), and move columns and rows. Data Table package
Configure Wait package actions to terminate a running bot if a condition is unsatisfied Enterprise A2019 and Community Edition Select the Throw an exception option in the Wait for screen change and Wait for window actions to show an error message and terminate a bot if the screen does not change or the window does not open or close within the specified amount of time. Using Wait for screen change action | Using Wait for window action

New features
Email trigger for new emails Enterprise A2019 and Community Edition Use email triggers to start a bot when a new email message is received in the specified email service. Supported email services are: • Microsoft Outlook • Email Server • EWS Server Add an email trigger
Generate a random integer from a user-specified range and assign it to a number variable Enterprise A2019 and Community Edition Use the Random action from the Number package to generate an integer in the range of -9,223,372,036,854,775,808 through 9,223,372,036,854,775,807. Random number action
Enterprise A2019 Bot agent OS support Enterprise A2019 Enterprise A2019 Bot agent is now supported for single users on Windows Server 2019, Windows Server 2016, Windows Server 2012, Windows 8, and Windows 7 SP1. Bot agent compatibility
Return the Bot agent installation path using the system variable AAInstallationPath Enterprise A2019 and Community Edition
Copy and paste actions and triggers between bots (Service Cloud case ID: 00455116) Enterprise A2019 and Community Edition Use the Copy to shared clipboard and Paste from shared clipboard icons at the top of the Bot editor to duplicate actions, triggers, and metadata at a time.
GDPR self-reporting Enterprise A2019 and Community Edition General Data Protection Regulation self-reporting enables the Enterprise Control Room administrator to run reports that include the following data elements (sensitive data will be masked in the output):

Automation Anywhere Version A2019 - 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).

New features
• User Bot Runner device access. • User data in associated credential vault. • Devices registered by the user. • All documents (artifacts) uploaded or updated to public or private repositories by the user. • All bots associated to the user. • Bot Insight dashboard report includes a list of all dashboards associated to this user ID.

Supported packages	
Package	Version
Node Manager	6.5.4738
Application	2.0.0-20200418-005328
App Integration	1.0.0-20200418-005326
Analyze	2.2.1-20200314-193039
Boolean	2.0.0-20200418-005329
Bot Migration	2.3.0-20200424-015945
Browser	2.0.0-20200418-005330
Clipboard	2.0.0-20200418-005342
Comment	2.0.0-20200418-005342
CSV/TXT	2.0.0-20200418-005342
Database	2.0.0-20200418-005345
Data Table	2.0.0-20200418-005637
Datetime	2.0.0-20200418-005348
Delay	2.1.0-20200418-005348
Dictionary	2.0.0-20200418-005349
Run DLL	2.0.0-20200418-005620
Email	2.0.0-20200418-005352
Error handler	2.0.0-20200418-005357
Excel basic	2.0.0-20200422-000204
Excel advanced	2.0.0-20200422-000103
File	2.0.0-20200418-005358
File & folders	2.0.0-20200317-030352
Folder	2.0.0-20200418-005400
FTP / SFTP	2.0.0-20200418-005404
IF/ELSE	2.0.0-20200418-005406

Supported packages	
Package	Version
Image Recognition	2.0.0-20200420-104210
Interactive forms	2.12.0-20200420-084203
IQ Bot	2.0.0-20191031-150538
JavaScript	2.0.0-20200418-005413
Simulate keystrokes	2.0.0-20200418-005415
Legacy Support	1.0.0-20200422-075546 1.0.0-20200422-075549
List	2.0.0-20200418-005422
Log To File	2.0.0-20200418-005423
Loop	2.0.0-20200418-005424
Message Box	2.0.0-20200418-005424
Mouse	2.0.0-20200418-005428
Number	2.0.0-20200418-005433
OCR	2.1.0-20200418-005434
Office 365 Excel	2.0.0-20200418-005517
Office 365 Calendar	2.0.0-20200418-005338
Office 365 OneDrive	2.0.0-20200418-005523
PDF	2.1.0-20200418-005526
PGP	2.1.0-20200418-005528
Ping	2.0.0-20200418-005529
Printer	2.0.0-20200418-005535
Play Sound	2.0.0-20200418-005530
Prompt	2.0.0-20200418-005536
Python Script	2.0.0-20200418-005537
Recorder	2.0.0-20200318-020414
REST Web Service	2.0.0-20200418-005619
SAP	2.1.0-20200418-005622
Screen	2.0.0-20200418-005625
SNMP	2.0.0-20200418-005627
SOAP Web Service	3.0.0-20200418-005630

Supported packages	
Package	Version
String	3.0.0-20200418-005635
System	2.0.0-20200418-005636
Task	2.0.0-20200417.230104-1256
Terminal Emulator	2.0.0-20200418-005641
Trigger Email	1.1.0-20200418-005652
VBScript	2.0.0-20200418-005643
Wait	3.0.0-20200418-005645
Window	2.0.0-20200418-005700
Workload	2.0.0-20200422-054201
XML	2.0.0-20200418-005650

Changed features
Build 4088 replaced with Build 4105 Build 4088 has been deprecated and replaced with Build 4105. If you have installed build 4088, perform a regular upgrade to get the new build. After you are on Build 4105, an update of the Bot agent is also required. Update Enterprise A2019
User interface changes in Excel basic and Excel advanced packages The text field titled Cell name is now Cell address in the actions from the Excel basic and Excel advanced packages.
Specify the column title in the Get cell address action in the Excel advanced package The Specific cell option is now the Based on header option, which accepts the column title as either the column heading or the default column title. Using the Get cell address action
Edit a work item without changing its status You no longer have to change the status of a new work item for editing. You can now edit work items that are in New status. Previously, you were allowed to edit the work item attribute values after changing the state of the attributes so that the edits to the work item could be saved. Edit work items
Mark work items for reprocessing

Changed features
The Ready to run action is now updated to Re-process so that you can mark work items that are in Failed, Data error, or On hold state to New status for reprocessing. View work items | Edit queues

Fixed features	
Service Cloud case ID	Description
00530388	Multiple bot updates and check-ins succeed irrespective of the Enterprise A2019 version used to import the bot. Bot check-in on Cloud deployments used to fail when the bot was imported multiple times and overwritten. This issue is now fixed.
00521691	After Excel files are extracted from a .zip file, common tasks such as renaming and deleting the Excel files failed. This issue is now fixed.
00519528	Bot Scanner version 2.0.0 now works as expected. The crash issue is now fixed.
00517040	When the Email package is used in Exchange Web Services, the action loop exited after processing 10 emails. This early exit is fixed. Now all specified emails are processed before the loop exits.
00504163	When bots are run using the Open and Close actions from the DLL package in a loop, the Bot agent window now functions correctly. The Bot agent service does not require a manual restart after a bot is run.
00494267	Actions from the DLL package can now be run inside and outside a loop.
00494273	The Create worksheet action in the Excel advanced package now supports default sheet names for all the supported languages in Enterprise A2019.
00492554	The Sort table action in the Excel advanced package now supports OS setting for the Swedish region.
00446956	The Open action in the CSV/TXT package can now read values from files encoded with UTF-8.
00503230	The SOAP Web Service action now supports responses with non-English characters.
00522147	The $StringVar.String:trim$ shorthand now trims leading and trailing spaces in a string when used in the Message box package.
--	You can now deploy bots on selected Bot Runner devices with the Run as option from the My bots page in an Enterprise Control Room configured on Microsoft Azure.
--	Scheduled bots now run as expected and do not get stuck in the queue in an Enterprise Control Room configured on Microsoft Azure.

Fixed features	
Service Cloud case ID	Description
--	After you capture an object in a browser or application window, the browser window containing the Bot editor is now reactivated. Previously, users had to manually return to the Bot editor. Actions in the Image Recognition, Mouse, OCR, Screen, and Recorder packages support this feature.
00475070	Exporting a report to CSV from Activity > Historical now correctly outputs the data.
00516331	You can now build a bot that contains more than one Database > Read from action that is followed by a Loop action, within the same database session. Each time the bot runs the Read from action, the query results are refreshed, and the loop will only iterate on the current results.
00509735	Auto Login now works when you deploy a bot as an unattended Bot Runner on a Horizon Virtual Desktop Infrastructure (VDI) session.
00509831	Prompt package actions now support long inputs. The user interface displays up to 512 characters. If the input is longer than 512 characters, the rest appear as a tooltip when the user hovers over the prompt box.
00518566	You can now use the recorder feature within actions to select window titles and file paths on a device that has proxy authentication enabled. Previously, users had to manually enter this information because they could not access the device through actions while building a bot.
00475107	The Japanese language now supports column names when using CSV-related actions.
00532894 00532253 00539241	When you reimport a bot using exported files from a different Enterprise Control Room of the same version (from version A2019.12 onward) and choose to overwrite the bot, you can now check-in that bot. The error generated when you choose the overwrite option that prevented check-in of the reimported bot is now fixed only for version A2019.12 onward. Reimporting bots on A2019.11 and older releases are not supported at this time.
00521222, 00525635, 00529274, 00526613, 00526489, 00530609, 00530787, 00533445, 00535366, 00530900, 00538070	The progress of a TaskBot is not stalled at line 0 and does not remain in queue to run when you deploy the bot on a Bot Runner. The status of the device reflects `Yet to Be Determined` until the device is available to process the items.
00421195	You can now create a work queue by providing details such as the queue name, queue owners, participants, consumers, and work item structure. This feature is available from Workload > Queues > Create Queue.

Known limitations
Folders created using the Folder > Create action cannot have names that contain system actions or device references such as AUX, CON, LPT, NUL, and PRN.

Known limitations
Mouse click with key combo for preset triggers in SAP application is currently not supported.
The following are known limitations in the form builder: • If the character limit is set to 0 and the field is marked necessary for the Password element in a form, an error message is displayed when you run the bot. • An invalid file path associated with the Document element in a form displays an error message when the Get and Set actions of the interactive forms are used. • A blank page is displayed on the form builder when you paste content into any of the existing form elements. • A form that is linked to a bot through the Display action of interactive forms is displayed in front of all other windows, even when the Always display form window in front option is not selected.
Cloud-enabled deployments only support local authentication.
Linux is not supported for Cloud-enabled On-Premises installations.
• Work items might be queued on the View queues page as the number of devices in the device pool increase. This should not affect the bot execution because the queues are cleared when the work items are processed. • You cannot simultaneously insert work items from multiple devices in a queue. • You cannot create a draft queue. • When you insert a number value using the Insert work item to a queue, the system shows an incorrect value. For example, if you insert 023456789, the system shows 2.3456789E7. • When you add more devices to a device pool that is processing WLM automations, the newly added devices might not immediately pick up the pending work items. Workaround: Pause and resume the WLM automation.
If a device goes idle while processing workload management work items in a device pool, it will not process the work items. However, those work items can be processed by other devices in the pool.

IQ Bot A2019

The IQ Bot On-Premises version supports all the features and functionality available in IQ Bot Version 6.5.2.

[IQ Bot feature comparison matrix](#)

Review the compatibility of the IQ Bot A2019 On-Premises version with the corresponding Automation Anywhere Enterprise Control Room On-Premises version.

[IQ Bot version compatibility matrix](#)

The IQ Bot Cloud version is available for this release and supports all features and functionality available in IQ Bot Version 6.5.2. This version provides users with automatic provisioning for up to three environments such as Development, Test, and Production. Users can migrate learning instances between environments using APIs.

The IQ Bot Community Edition and the free trial version are available for this release. Both versions have feature parity and are based on IQ Bot Version 6.5.2.

Known limitations
IQ Bot On-Premises IQ Bot registration is not supported for Cloud-enabled On-Premises installations.

Bot Insight

New features
View filtered data of the dashboard widgets Enterprise A2019 and Community Edition The Bot Insight dashboard widget filter enables you to apply filters across the widgets in the dashboard to display filtered data. While the dashboard filters enable you to view different combinations of information from a single dashboard, the widget filters enable you to drill down to information from the already filtered data. You can also save and publish the custom dashboards with the preset widget filters. Bot Insight dashboard filter
Retrieve information from the Bot Insight API, and generate and visualize data analytics on Microsoft Power BI Enterprise A2019 and Community Edition The Automation Anywhere custom connector enables you to establish a secure connection to Microsoft Power BI, and generate and visualize data analytics. You can select the Bot Insight APIs in Microsoft Power BI and apply specific parameters for each of the APIs. The custom connector transforms the Bot Insight API responses to data model visualizations in Microsoft Power BI. Data connector for Power BI
Preview and analyze business information in the default business dashboard Enterprise A2019 and Community Edition The Data Preview menu in the Bot Insight default business dashboard displays information that is logged for multiple Analyze Open and Close commands used in the bot. The Preview Data menu does not appear when you perform a comparison between the default dashboards.
API enhancements Enterprise A2019 The deletetasklogdata API is updated to include the `runId` parameter. The getbotrundata API retrieves information about the vital statistics of the bot. The getaudittraildata API retrieves information about the audit data that is logged for all users.

New features
Bot Insight API details

Related tasks
Upgrade to Enterprise A2019
Update Enterprise A2019
Upgrading IQ Bot A2019

Enterprise A2019.11 Release Notes

Review the new features, supported packages, changed features, fixed features, and known limitations in the Enterprise A2019.11 (Build 3337) release. There are no security fixes in this release.

- Enterprise A2019
- IQ Bot A2019
- Bot Insight A2019

Enterprise A2019

Bot agent update: Enterprise A2019.11 includes a required update to your Bot agent. Ensure that you complete the update to continue with your automation activities. Update the Bot agent

New features

Migrate 11.x TaskBots and MetaBots to A2019
 	
Enterprise A2019
 	
  • Additional support is provided for packages and variables.
 	
     Package mapping for migration | Variable mapping for migration
 	
  • You can now migrate MetaBots (with DLLs) and their components from 11.x to A2019. You cannot migrate screen-based MetaBots.
 	
     How MetaBots are migrated
 	
  • Use the Bot Scanner to analyze MetaBots to determine if they can be migrated to A2019.
  • Verify the list of certified 11.x bot versions available for migration: Understanding Enterprise A2019 migration

Bot Store integration with the Enterprise Control Room Enterprise A2019 You can now access the Bot Store from within the Enterprise Control Room. You can install, configure, and run the Bot Store bots within the Enterprise Control Room. As a registered user, you can log in to the Bot Store from the Enterprise Control Room and access all your downloads. You can install bots and packages from your downloads to the Enterprise Control Room private

New features
repository. You can also submit your existing bots and packages from the Enterprise Control Room to the Bot Store. Bot Store
Use interactive forms in a bot Enterprise A2019 Interactive forms provide a form builder experience for users to build interfaces for submitting and regrouping data being used to send and receive data from various applications within their attended automation process. Users with Bot Creator and Bot Runner license can use the interactive forms package to control and manage the form flow within a bot during runtime. Actions performed by users on the interactive forms can be monitored to execute logic using subtasks. Interactive forms are first-class citizens within the bot repository and have the same workflows for moving forms between public and private workspaces, and for export or import actions. No additional licenses or permission are required to use interactive forms. Action items in the interactive forms can be used to manage various forms within a bot. Using interactive forms
Reuse an identical value between bots by configuring a global value in the Enterprise Control Room Enterprise A2019 and Community Edition A global value enables users to reuse an identical value between bots instead of creating a new variable for each bot. Global values remain constant for all users and bots in an Enterprise Control Room instance. A user with the `AAE_admin` role can configure a global value with a default value and enable non-admin users to overwrite the value to use in their bots. Global values | Create a global value | Overwrite the default value
Workload enhancements Enterprise A2019 and Community Edition • Monitor the progress of ongoing workload automations. You can also pause, resume, or stop the automations as required. • Configure and edit workload automations to ensure that the automations are deployed seamlessly to unattended Bot Runner devices. Execute the workload automations with priority or round-robin mode from the Devices > Edit Device pool page. • Set the output status of the work item processed in the Enterprise Control Room on the Queues and Work item details page using the $workItemResult$ variable in a TaskBot. • Edit work items that are in Ready to run, On hold, Data error, or Failed state. • Set the individual work item status to Mark complete, Defer, or Re-process from the Edit work item page or in bulk from the View queues page.

New features
View automation of a queue | Edit device pools | Edit work items | Use Work Item variables

Download a file from the Enterprise Control Room to your device

Enterprise A2019 and Community Edition

Use the Download CR file action from the File package to download a file from the Enterprise Control Room to your device.
Note: You cannot use this action to download a bot or a file from the My Scripts folder.

File package

Clone a bot or files

Enterprise A2019 and Community Edition

Create a read-only copy of a selected bot or file from the public repository to the private repository. The clone is a local copy for the same user and will not be updated with the public repository copy automatically. This provides a testing environment experience for Bot Creators to make and validate changes locally and take advantage of reusable TaskBots in concurrent developments by reusing an existing bot or file as a dependency.

- Cloned bots and files cannot be edited, renamed, or moved.
- Cloned bots and files can be deleted from a private repository.
- Users can create a copy of the cloned bot.
- A cloned bot can be used in Run Task action in another bot.
- Cloned bots and files can be added as a manual dependency for another bot.

New features in the If package
Enterprise A2019 and Community Edition

- Configure an If action with multiple conditions.

  Specify whether all or either of the conditions must be met.

- Verify whether JavaScript, Task, or VBScript ran successfully or not.
- Verify whether a string variable is empty or not.
- Execute actions only if two strings have matching uppercase and lowercase letters.

If package \| Perform an action based on cell value

Universal Recorder enhancements

Enterprise A2019 and Community Edition

Universal Recorder now enables you to:

- Automate in Java applications that run using Java Runtime Environment (JRE) 9, 10, and 11.
- Capture objects in tables in Oracle EBS applications.

New features

• Automate interactions with user interface objects in the taskbar, desktop, or currently active window. This option is available in the window selection drop-down list in the following packages:
  • Image Recognition
  • Mouse
  • Recorder
  • Screen
  • Simulate keystrokes
  • Window
 	
Universal Recorder overview

New features in the Excel advanced package
Enterprise A2019 and Community Edition
 	
  • In the Replace action, you can choose to replace cell values with an empty character.
  • In the Get cell address action, you can choose to save the retrieved cell address to a string variable.
 	
Using the Replace action | Using the Get cell address action

Add DLL dependencies Enterprise A2019 and Community Edition As a bot creator, you can use a DLL that refers to a child DLL. Bot dependencies
Licensing server failover Enterprise A2019 HA failover from a primary cluster to a secondary cluster applies to all the servers, including the licensing server, and is handled by the data center high availability tools. Distributed architecture with HA/DR support | HA cluster configuration overview
Automate locking, logging off, restarting, or shutting down the computer Enterprise A2019 and Community Edition Use actions from the System package at the end of tasks to automate locking, logging off, restarting, or shutting down the computer.
Manage running bots with the Pause and Stop actions from the Task Bot package Enterprise A2019 and Community Edition   • Insert a Pause action to temporarily pause the running bot.

New features
• Insert a Stop action to terminate the running bot. Task Bot package
Automate printer settings Enterprise A2019 and Community Edition Use actions from the Printer package to automate retrieving and setting the default printer.
Return the path and name of the currently running TaskBot using the system variable AATaskName Enterprise A2019 and Community Edition System variables
Run JavaScript, Python, or VBScript from a file selected from your desktop Enterprise A2019 and Community Edition You can select the file containing the script as part of configuring the action. Note: The file and any dependencies must be in a standalone folder. When you select a file for upload, all files and folders at the same folder level are uploaded. JavaScript package | Python Script package | VBScript package

Supported packages

Package	Version
Node Manager	6.0.4015
Application	2.0.0-20200302-135910
Analyze	2.2.1-20200314-193039
Boolean	2.0.0-20200302-135912
Browser	2.0.0-20200302-135913
Clipboard	2.0.0-20200302-135922
Comment	2.0.0-20200302-135922
CSV/TXT	2.0.0-20200312-122802
Database	2.0.0-20200302-135926
Data Table	2.0.0-20200302-140308
Datetime	2.0.0-20200302-135930

Package	Version
Delay	2.1.0-20200302-135931
Dictionary	2.0.0-20200302-135932
Run DLL	2.0.0-20200313-170350
Email	2.0.0-20200302-135934
Error handler	2.0.0-20200302-135940
Excel basic	2.0.0-20200302-140133
Excel advanced	2.0.0-20200302-140020
File	2.0.0-20200316-045955
File & folders	2.0.0-20200317-030352
Folder	2.0.0-20200302-135945
FTP / SFTP	2.0.0-20200302-135948
IF/ELSE	2.0.0-20200302-135950
Image Recognition	2.0.0-20200302-135953
IQ Bot	2.0.0-20191031-150538
JavaScript	2.0.0-20200313-170107
Simulate keystrokes	2.0.0-20200313-170111
Legacy Support	1.0.0-20200317-220124 1.0.0-20200317-220128
List	2.0.0-20200302-140013
Log To File	2.0.0-20200302-140014
Loop	2.0.0-20200302-140015
Message Box	2.0.0-20200302-140016
Migration	2.0.0-20200317-220133
Mouse	2.0.0-20200302-140016
Number	2.0.0-20200302-140023
OCR	2.1.0-20200302-140025
Office 365 Excel	2.0.0-20200309-140138
Office 365 Calendar	2.0.0-20200305-124125
Office 365 OneDrive	2.0.0-20200309-110128
PDF	2.1.0-20200302-140126
PGP	2.1.0-20200309-110135

Package	Version
Ping	2.0.0-20200302-140130
Printer	2.0.0-20200311-100204
Play Sound	2.0.0-20200309-110137
Prompt	2.0.0-20200302-140148
Python Script	2.0.0-20200313-170254
Recorder	2.0.0-20200318-020414
REST Web Service	2.0.0-20200312-090358
SAP	2.1.0-20200302-140250
Screen	2.0.0-20200302-140254
SNMP	2.0.0-20200302-140257
SOAP Web Service	2.0.0-20200312-110311
String	2.0.0-20200302-140306
System	2.0.0-20200309-140321
Task	2.0.0-20200317-030340
Terminal Emulator	2.0.0-20200302-140313
VBScript	2.0.0-20200313-170417
Wait	2.0.0-20200302-140319
Window	2.0.0-20200302-140348
XML	2.0.0-20200302-140321

Changed features
Change in the Dictionary > Remove action The Dictionary > Remove action offers the option to assign the removed value to a variable. Dictionary package
The Update migration status permission name has been changed to Allow a bot-runner user to run migrations. All functionalities remain the same.
When multiple bots are scheduled to run on the same user or device, the bots are now queued and run whenever the previous bots completes its run. Service Cloud case ID: 00440072

Changed features
Schedule	Workload management

Fixed features

Service Cloud case ID	Description
00483976	When the copy function is used, nested subfolders were not visible when users clicked browse to search through directories. This issue has been fixed.
00457550	When a user checks out a bot that uses the Run action to run child bots, the child bots are now cloned from the public repository to the private.
00492706	When a user exports a bot from another Enterprise Control Room and imports that same bot to a new Enterprise Control Room, the imported bot and enabled packages now show all required actions.
00482934	Bot deployments and website launches are now optimized for quicker process.
00421864	When a user is viewing historical activity details in Historical activity, the run option is no longer displayed.
00505120	When bots fail the check-in process, the contents are now restored in the Private repository.
00488504	Bots with more than 100 dependencies are now exported successfully without an error, even if the parent bots are in the list of those 100 dependencies.
00444902	When the Enterprise Control Room is used in Internet Explorer 11, the Bot agent is now compatible and the UI is rendered properly.
00454079	When the Capture action in the Recorder package is used, content in the browser is captured successfully.
00460530	In a developer Enterprise Control Room, a user can now successfully import a bot with cyclic dependency.
00493605	In the Run action in the TaskBot package, the Assign the output to variable (optional) option now functions properly when an assigned variable is removed.
00486734	When the Set cell action in the Excel advanced or Excel basic package is used with multiple Microsoft Excel files, the values of the Active cell operation now activate and set the cells accordingly in the respective Microsoft Excel file.
00530915	Migration is not advisable for 11.x customers using Workload Management (WLM) due to known issues.
--	You can now add date variables in the Vertical Bar Graph widget in the Bot Insight Business dashboard.

Service Cloud case ID	Description
00475173	All fields of the Recorder > Capture action have been translated into Enterprise A2019 supported languages.

Known limitations
MetaBot logic that uses a DLL function call with one or more parameters migrates successfully. However, when you run the migrated bot, an error is shown.
Global values of the Date time data type cannot be used in actions.
The A2019 On-Premises Enterprise Control Room installation does not support the semicolon (;) special character in the Windows user password. The installation fails if you use this special character.
When data is exported into a CSV file from User Management, Audit Logs, and Roles Management for all locales except English, the respective language is not displayed correctly.   Workaround: Export to a CSV file and access a Microsoft Excel file. Import and save that CSV file as a CSV with UTF-8 encoding.
Users must explicitly enable the feature flag for the forms feature in the On-Premises build.   Note: Contact support for further assistance.
Forms with many radio buttons and check boxes in the same row are not rendered correctly.
Only the Form Events and UI Triggers event types are supported by event loop as the file or folder triggers and hot keys have issues.

IQ Bot A2019

The IQ Bot On-Premises version is available for this release with additional features or updates since the last release. This IQ Bot version supports all the features and functionality available in IQ Bot Version 6.5.2.

IQ Bot feature comparison matrix

Review the compatibility of the IQ Bot A2019 On-Premises version with the corresponding Automation Anywhere Enterprise Control Room On-Premises version.

IQ Bot version compatibility matrix

The IQ Bot Cloud version is available for this release and supports all features and functionality available in IQ Bot Version 6.5.2. This version provides users with automatic provisioning for up to three environments such as Development, Test, and Production. Users can migrate learning instances between environments using APIs.

The IQ Bot Community Edition and the free trial version are available for this release. Both versions have feature parity and are based on IQ Bot Version 6.5.2 .

New features
Upgrade from earlier versions of IQ Bot to the latest IQ Bot A2019 On-Premises

New features
IQ Bot A2019 On-Premises If you are using any of the earlier versions of IQ Bot (5.3.x or 6.5.x), you can upgrade to IQ Bot A2019 Build 3337 On-Premises. Upgrading IQ Bot A2019
Use API to migrate learning instances between environments You can use an API to migrate learning instances in IQ Bot A2019 On-Premises.
Access IQ Bot A2019 from the Enterprise Control Room dashboard Enterprise A2019 and Community Edition You can access IQ Bot from the Enterprise Control Room through a link, provided you have registered IQ Bot in the Enterprise Control Room. Otherwise, the IQ Bot section remains hidden.

Known limitations
IQ Bot On-Premises IQ Bot A2019 installation fails if the user password contains any of these special characters: single quotation mark ('), quotation mark ("), or semicolon (;).
IQ Bot Cloud • ABBYY FineReader Engine is the default OCR for data extraction in IQ Bot Cloud. • Data validation using Python script is not supported. • IQ Bot extensions for custom extraction are not available.

Bot Insight

New features
View filtered data of Bot Insight dashboards Enterprise A2019 The Bot Insight dashboard filter enables you to apply filters across dashboards to display filtered data on the dashboard widgets. The filter enables you to view different combinations of information from a single dashboard, thereby eliminating the need to maintain separate dashboards for different sets of users. Bot Insight dashboard filter

New features
View business analytics for multiple transactions simultaneously Enterprise A2019 The Multiple Transaction Names menu displays transactional information about bots with multiple Analyze- Open and Close commands. Each Analyze- Open and Close command is considered as a transaction, and each transaction is displayed as a unique block in the data preview section. The number of rows for each unique transaction block is limited to 100. Business dashboard

Enterprise A2019.10 Release Notes

Review the new features, supported packages, changed features, fixed features, and known limitations in Enterprise A2019.10 (Build 2545). There are no security fixes in this release.

- Enterprise A2019
- IQ Bot A2019
- Bot Insight A2019

Enterprise A2019

New features

Migrate 11.3.x TaskBots to A2019
 	
Enterprise A2019
 	
  • Analyze whether you can migrate bots created in Enterprise client version 10.x using the Bot Scanner.
 	
    Analyze reports
 	
  • Additional support is provided for packages and variables.
 	
    Package mapping for migration | Variable mapping for migration
 	
  • Multiple Bot Runner users are supported for bot migration.
 	
    Migrate Enterprise bots

AISense Recorder to capture objects from remote applications This is a Beta release on Enterprise A2019 (Cloud deployment only) and Community Edition Record a task and capture objects using the AISense Recorder from applications that are usually accessed remotely and with a complex user interface (UI).

New features
Record a task with AISense Recorder
Manage your automation as Work Items for resource optimization and workload automation Enterprise A2019 and Community Edition Divide your automation into small, logical modules called Work Items using the new feature. Process these Work Items simultaneously using queues to ensure that your organization's automation goals are achieved with optimum resource utilization. Use the workload module to create and manage workload queues and run bots on unattended Bot Runners through the workload queues. Also, pass the Work Item attributes or values to the bot from the Enterprise Control Room when you Run bot with queue with the help of Work Item variables. Workload management
Install Enterprise Control Room on Red Hat Enterprise Linux 7.7 and Linux CentOS 7.7 Enterprise A2019 Use the command line to install your Enterprise Control Room on your Linux servers in the datacenter. Installing Enterprise Control Room on Linux
Use wildcard characters in folder and file path fields in the Encrypt and Decrypt actions Enterprise A2019 and Community Edition Substitute an asterisk (*) for one or more unknown alphanumeric characters or symbols. This maximizes the search results by returning all folders and files that contain the string that you have specified. Encrypt | Decrypt
Use system variables to return data from the computer that is connected to the running Bot agent Enterprise A2019 and Community Edition You can use the following system variables: • AAControlRoom: Returns the URL of the Enterprise Control Room. • CPUUsage: Returns the percentage utilization of the CPU. • RAMUsage: Returns the RAM usage in megabytes. • OSName: Returns the operating system. • TotalRAM: Returns the total amount of RAM available.
Automate tasks in Oracle EBS and Forms with the Universal Recorder Enterprise A2019 and Community Edition

New features
Open Oracle EBS applications in a browser as Java Web Start applications or as a thick client. The Universal Recorder can capture the following objects: • Window/Tab • Button • Text box • Label (read-only) • Radio button • Check box • Table/Grid • Scroll bar • Menu • Combo-box/Drop-down list

Supported packages

Package	Version
Node Manager	2.0.2885
Application	2.0.0-20200131-085947
Analyze	2.1.0-20200204-154550
Boolean	2.0.0-20200131-085949
Browser	2.0.0-20200127-180439
Clipboard	2.0.0-20200131-085958
Comment	2.0.0-20200130-183435
CSV/TXT	2.0.0-20200205-175938
Database	2.0.0-20200205-175940
Data Table	2.0.0-20200131-200235
Datetime	2.0.0-20200131-090006
Delay	2.1.0-20200131-090007
Dictionary	2.0.0-20200205-175946
Run DLL	2.0.0-20200205-230300
Email	2.0.0-20200206-135926
Error handler	2.0.0-20200130-183452
Excel basic	2.0.0-20200205-110122
Excel advanced	2.0.0-20200205-110012
File	2.0.0-20200131-090018
Folder	2.0.0-20200131-090021

Package	Version
FTP / SFTP	2.0.0-20200206-110020
IF/ELSE	2.0.0-20200131-090025
Image Recognition	2.0.0-20200131-090028
IQ Bot	2.0.0-20191031-150538
JavaScript	2.0.0-20200205-180013
Simulate keystrokes	2.0.0-20200205-105955
List	2.0.0-20200131-090039
Log To File	2.0.0-20200131-090040
Loop	2.0.0-20200131-090041
Message Box	2.0.0-20200131-090041
Migration	1.1.0-20200206-180601
Mouse	2.0.0-20200131-090044
Number	2.0.0-20200205-110015
OCR	2.1.0-20200131-090053
Office 365 Excel	2.0.0-20200205-180122
Office 365 Calendar	2.0.0-20200206-105949
Office 365 OneDrive	2.0.0-20200127
PDF	2.1.0-20200131-090152
PGP	2.1.0-20200205-110117
Ping	2.0.0-20200131-090156
Play Sound	2.0.0-20200127-180654
Prompt	2.0.0-20200127-180707
Python Script	2.0.0-20200205-180148
Recorder	2.0.0-20200212
REST Web Service	2.0.0-20200206-110309
SAP	2.1.0-20200205-180245
Screen	2.0.0-20200131-090311
SNMP	2.0.0-20200207-090446
SOAP Web Service	2.0.0-20200127-180819
String	2.0.0-20200131-090323
System	2.0.0-20200205-110240
Terminal Emulator	2.0.0-20200131-090330

Package	Version
VBScript	2.0.0-20200205-180309
Wait	2.0.0-20200131-090335
Window	2.0.0-20200131-090337
XML	2.0.0-20200131-090339

Changed features
Updated layout for the summary report generated by Bot Scanner The layout of the summary report is updated to provide information about the number of bots scanned, and the commands and variables used in the scanned bots that are supported in A2019. Analyze reports
Python script and VBScript packages return output without quotation marks The actions in the Python script and VBScript packages now return output without any quotation marks. For example, if the action previously returned `"ABC"` as the output, now the action returns only `ABC`.
Use Microsoft SQL Server address as alias for database Service Cloud case ID: 00401484 The Enterprise Control Room now supports using a Microsoft SQL Server address as alias for a database during installation. KB article: Change database server after A2019 Control Room installation (Apeople login required)

Fixed features

Service Cloud case ID	Description
00463210	In a virtual machine using Remote Desktop Protocol, the Keystrokes action now functions properly without prompting a special characters error.
00455359, 00466407, 00475122	When the Enterprise Control Room is used in Google Chrome, renaming a folder in the My bots section no longer causes the browser to crash.
00440659	In the Data Table package, the Create folders/files if it doesn't exist option in the Write to file action now functions properly and does not create a file when the option is not selected.
00377861, 00466104	When you install Enterprise A2019 On-Premises with Amazon Relation Database Service (RDS) and there is no internet connectivity, the installation now completes successfully.

Service Cloud case ID	Description
00472738, 00496476	In the Enterprise Control Room, the bot now runs successfully without prompting an interactive bot error message in any circumstance.
00472655	In the Loop action, selecting the Cell range in the Loop through option now functions properly with the For each row in worksheet in the Iterator option.
00475040	When a bot is developed in Google Chrome, the pause and resume options now function correctly.
00445671	The time taken to connect to the Enterprise Control Room is now less than 2 minutes after you restart the Enterprise Control Room services.
00421864	You can now configure your Bot agent using the Google Chrome browser. The following error message is no longer displayed: `Please use Chrome to configure your bot agent.`
00462095	Bot compilation time has decreased, so it takes less time for the bot to run. Previously, some bots took up to 40 seconds in pre-processing mode.

IQ Bot A2019

The IQ Bot On-Premises version is available for this release with additional features or updates since the last release. This IQ Bot version supports all the features and functionality available in IQ Bot Version 6.5.2.

IQ Bot feature comparison matrix

Review the compatibility of the IQ Bot A2019 On-Premises version with the corresponding Automation Anywhere Enterprise Control Room On-Premises version.

IQ Bot version compatibility matrix

New features
IQ Bot On-Premises unified database IQ Bot Build 2545 On-Premises now supports a unified database. You have to run a migration script to migrate the databases of Builds 1089, 1598, and 2079 to Build 2545. Run IQ Bot On-Premises database migration script

Note: The version number in the IQ Bot installer is incorrect and will be fixed in the next release.

Bot Insight A2019

New features
New Bot Insight homepage

New features
The new homepage displays all the available dashboards in a single page and enables you to directly access the dashboard of your choice. The smart search functionality enables you to search for dashboards in the Search text field. The homepage also enables you to bookmark your favorite dashboards and to sort the dashboards based on the following parameters: • Dashboard Name • Type • Total Views • Last Refreshed Bot Insight dashboards
Operations dashboard View information about the bots that are deployed on different Bot Runner machines and their statistics based on the performance from the Bot Insight Operations dashboard. You can use this information to enhance productivity and take measures based on real-time information for RPA deployments. You can directly access the Bots and Audit dashboards from the hyperlinks in the Operations dashboard. Operations dashboard
Transaction data View data that is aggregated and logged by the bots when they are deployed in the Bot Runner machines by using the Transaction data feature in the Profile menu. You can access this feature from the Business dashboard. Business dashboard
Exporting data from widgets Export data that is generated by the various smart widgets to comma-separated value (CSV) files on your local drive from the Custom Business dashboard. The export file for all the widgets, except the Data Table Chart and the US Map, contains the following headers: • Group • Subgroup • Metric • Volume The Data Table Chart export file contains all the headers that are present in the Data Table Chart. The US Map export file contains the state codes, metric values, and the volume headers. Exporting data from a dashboard widget
Visualization updates

New features
Customize the widgets on the Bot Insight dashboards to gain insights for specific scenarios. The following widgets are added to Bot Insight: • Heat Map   • Data Table Chart   Bot Insight Visualizations

Known limitations

Using the Universal Recorder in Oracle EBS applications:

- The Select item by text action does not retrieve the value of a selected ListView object.
  Workaround: Manually enter the item value after capturing the object control or use the Select item by index action.
  Note: Item index count starts at 1.
- At runtime, the Select item by text and Select item by index actions do not appear to select the item specified in a PageTab object, but the bot successfully executes the action.
- At runtime, the Select item by text and Select item by index actions do not appear to select the item specified in a ComboBox object, but the bot successfully executes the action.

In Enterprise A2019 On-Premises, the following activities are currently not logged in the workload logs:

- Create a queue
- Create a device pool
- Create a bot
- Run a bot with a queue

You can access the logs from the C:\ProgramData\AutomationAnywhere\Logs folder.
Related information
https://www.automationanywhere.com/in/lp/rpa-editions-comparison

Enterprise Version A2019 (Build 2094) Release Notes

These release notes describe new features, changed features, fixed features, security fixes, deprecated features, and known limitations in Enterprise Version A2019 (Build 2094).

Version A2019 Build 2094

Build 2094 contains updates for the following:

- Enterprise Community Edition
- Bot Insight A2019
- IQ Bot A2019
- On-Premises (Build 2079)

New features in Version A2019 Build 2094

Feature	Description
Migration	Migrate 11.3.x TaskBots to A2019. • Run the Bot Scanner (previously called the pre-migration utility) to analyze if your 11.x bot (currently only 11.3.1, 11.3.2, and 11.3.2.x versions are supported) can be migrated to A2019. The utility generates a summary report in HTML format and a separate report for each bot in XML format. Bot Scanner overview • Migrate multiple TaskBots with dependent TaskBots using a single Run-as user. Migrate Enterprise bots • As part of the bot migration process, you can identify previously migrated TaskBots on the bot selection page and preview a list of the dependent TaskBots before finalizing the migration. Migrate Enterprise bots • Analyze the status of individual bot migrations and identify any unsupported commands or attributes associated with the migrated bot and its dependencies. Migration reports • Additional support is provided for packages and variables. Package mapping for migration
SAML 2.0	Switch an authenticated environment Enterprise Control Room database to a SAML identity provider (IDP). Set up SAML authentication
Bot Deploy API	The Bot Deploy API now includes `/automations/ deploy` and is introduced to support the `runAs user` feature for Bot deployment. • The Bot Deploy API works only in Enterprise public accounts, and not in Community Edition.

Feature	Description
	• The API supports callback URL for environments that have both the Enterprise Control Room and callback server on the same network.
Geo Presence	The Geo Presence feature is a multi-tenant, secure, scalable, Cloud Control Room enhancement to securely communicate with users and Bot Runners over a customer network.
Exchange Web Services support	Actions in the Email package enable users to automate email-related operations using Exchange Web Services (EWS). Email package
Variables in place of an index or key value	Data table, dictionary, list, and record type variables can express index and key values as variables. Simple variable types
Copy bot	The copy bot functionality retains the metadata of the original bot, including captured images, recorded objects, called files, and child bots. Copy a bot
Excel actions to retrieve cell, column, or row location	The following actions enable users to retrieve location information from an Excel sheet and save it to a variable. • Get cell address • Get column • Get row
Recorder enhancements	Users can discard the most recently captured object while the Recorder is running.

Supported packages

Package	Version
Node Manager	1.0.1891
Application	2.0.0-20191223-210256
Boolean	2.0.0-20191223-210258
Browser	2.0.0-20191223-210259

Package	Version
Clipboard	2.0.0-20191223-210308
Comment	2.0.0-20191223-210309
CSV/TXT	2.0.0-20191223-210310
Database	2.0.0-20191223-210312
DataTable	2.0.0-20191223-210802
DateTime	2.0.0-20191223-210316
Delay	2.1.0-20191223-210318
Dictionary	2.0.0-20191223-210318
DLL	2.0.0-20191223-210742
Email	2.0.0-20200114-060001
Error Handler	2.0.0-20191223-210326
Excel	2.0.0-20200107-140225
Excel_MS	2.0.0-20200107-140116
File	2.0.0-20200114-060009
Folder	2.0.0-20200114-060012
FTP/SFTP	2.0.0-20191223-210334
If/Else	2.0.0-20191223-210336
IR	2.0.0-20191223-210339
IQ Bot	2.0.0-20191031-150538
JavaScript	2.0.0-20191223-210345
Keystrokes	2.0.0-20191223-210348
List	2.0.0-20191223-210350
LogToFile	2.0.0-20191223-210350
Loop	2.0.0-20191223-210352
MessageBox	2.0.0-20191223-210352
Migration	1.1.0-20200111-070201
Mouse	2.0.0-20191223-210355
Number	2.0.0-20191223-210402
OCR	2.1.0-20191223-210525
Office 365 Excel	2.0.0-20191231-170605
Office 365 Calendar	2.0.0-20191231-170422
Office 365 OneDrive	2.0.0-20191231-170612

Package	Version
PDF	2.1.0-20191223-210631
PGP	2.1.0-20191223-190649
Ping	2.0.0-20191223-210634
PlaySound	2.0.0-20191223-210636
Prompt	2.0.0-20191231-130717
Python	2.0.0-20191223-210644
Recorder	2.0.1-20200111-070529
Rest	2.0.0-20191231-120639
SAP	2.1.0-20191223-210745
Screen	2.0.0-20191223-210748
SNMP	2.0.0-20191223-210752
SOAP	2.0.0-20191210-081952
String	2.0.0-20200114-110316
System	2.0.0-20191223-210800
Terminal Emulator	2.0.0-20191223-210806
VBScript	2.0.0-20191223-210809
Wait	2.0.0-20191223-210812
Window	2.0.0-20191223-210814
XML	2.0.0-20191223-210815

Changed features

Feature	Description
Office 365 packages authorization	Authorize each Office 365 package separately through the Connect package in each package. Using the Connect action

Fixed features

Feature	Description
Bot agent	In the Enterprise Control Room, upgrading to the latest Bot agent version now successfully executes the bot without any prompted error messages. See Manually switch the Bot agent.

Feature	Description
Excel advanced package	In the Excel advanced package, the Close action now terminates only a specific open session as defined by the session name.
Keystrokes	The Keystrokes command now functions properly with the Japanese keyboard layout.

Security fixes

The security fixes in this release have not changed since the previous release. For a list of these fixes, see Enterprise Version A2019 (Builds 1598 and 1610) Release Notes.

Deprecated features

The deprecated features in this release have not changed since the previous release. For a list of these deprecations, see Enterprise Version A2019 (Builds 1598 and 1610) Release Notes.

Known limitations in Build 2094

Migration

- When selecting a bot for migration, values for the Last Migrated and Migrated By columns might differ for the same bot in the Available Files and Selected tables.
- The "System" value in the Migrated By column indicates that the bot has not been migrated previously.
- When viewing commands and variables associated with each migrated bot, you should only see the unsupported commands and variables. Currently, all commands and variables are shown.

IQ Bot A2019 Build 2079

IQ Bot On-Premises version is available for this release with no additional features or updates since the last release. This version is based on IQ Bot Version 6.5.2 feature and functionality.

IQ Bot feature comparison matrix

IQ Bot A2019 On-Premises version is compatible with the corresponding Automation Anywhere Enterprise Control Room On-Premises version.

IQ Bot version compatibility matrix

For a fresh Enterprise Control Room installation, the user has to upload the IQ Bot package manually. See Add packages to the Enterprise Control Room for details.

The package can be downloaded from https://apeople.automationanywhere.com/s/downloads.

IQ Bot fixed features

The fixed features in this release have not changed since the previous release.

IQ Bot security fixes

The security fixes in this release have not changed since the previous release.

IQ Bot deprecated features

The deprecated features in this release have not changed since the previous release.

IQ Bot known limitations

There are no new known limitations in this release.

Bot Insight new features in Build 2094

Feature	Description
Visualizations	The Visualization widget in the Bot Insight dashboard provides a host of highly customizable widgets that you can use to gain insights on specific scenarios. Vertical and horizontal Clustered and Stacked bars are added. Adding a dashboard widget

Bot Insight changed features

The changed features in this release have not changed since the previous release.

Bot Insight fixed features

The fixed features in this release have not changed since the previous release.

Bot Insight deprecated features

The deprecated features in this release have not changed since the previous release.

Bot Insight known limitations

The known limitations in this release have not changed since the previous release.

Enterprise Version A2019 (Builds 1598 and 1610) Release Notes

These release notes describe new features, changed features, fixed features, security fixes, deprecated features, and known limitations in Enterprise Version A2019 (Builds 1598 and 1610).

Version A2019 Builds 1598 and 1610

Build 1598 contains updates for the following:

- Enterprise Community Edition
- Bot Insight
- IQ Bot A2019

Build 1610 contains updates for the following:

- On-Premises
- Bot Insight
- IQ Bot A2019

New features in Version A2019 Builds 1598 and 1610

Feature	Description
Pre-migration utility for On-Premises	The Automation Anywhere pre-migration utility evaluates your 11.x bots for migration to A2019. Run the pre-migration utility to verify whether your existing 11.x bots can be migrated to A2019. Use the summary report generated by the utility to identify the bots that can and cannot be migrated and decide if you want to start the migration. Note: This is an initial version of the pre-migration utility. We plan to include updates to the utility in upcoming releases to help migrate most of your bots.
On-Premises Windows installer	A2019 On-Premises Windows installer is certified for Azure.
Bot Creator and Bot Runner on Azure Cloud	Users can create and execute bots for devices on Azure Cloud.
Action localization	Labels, buttons, and tooltips are localized to the supported language set.
Updated action packages	- Additional REST Web Service error codes for better troubleshooting of API calls - PGP package for encrypting and decrypting files - Improvements to SAP actions
Control Room to a SAML-based, SSO-authenticated Control Room	A2019 integrates with SAML identity providers (IDPs). Post installation, administrators can switch the Control Room to a SAML-based, SSO-authenticated Control Room.
Move email messages to different folder	The Move message command enables the user to move all the filter-matched emails to a different folder.

Supported packages

Package	Version
Node Manager	1.0.2110
Application	2.0.0-20191128-060339
Boolean	2.0.0-20191128-060340
Browser	2.0.0-20191128-060342
Clipboard	2.0.0-20191128-060350
Comment	2.0.0-20191128-060351
CSV/TXT	2.0.0-20191128-060352
Database	2.0.0-20191128-060354
DataTable	2.0.0-20191128-060707
DateTime	2.0.0-20191128-060358
Delay	2.1.0-20191128-060359
Dictionary	2.0.0-20191128-060400
DLL	2.0.0-20191128-060648
Email	2.0.0-20191205-100336
Error Handler	2.0.0-20191128-060404
Excel	2.0.0-20191128-060547
Excel_MS	2.0.0-20191128-060434
File	2.0.0-20191128-060407
Folder	2.0.0-20191128-060409
FTP/SFTP	2.0.0-20191128-060412
If/Else	2.0.0-20191128-060414
IR	2.0.0-20191121-100240
IQ Bot	2.0.0-20191031-150538
JavaScript	2.0.0-20191128-060423
Keystrokes	2.0.0-20191128-060426
List	2.0.0-20191128-060427
LogToFile	2.0.0-20191128-060428
Loop	2.0.0-20191128-060429
MessageBox	2.0.0-20191128-060429
Mouse	2.0.0-20191128-060430

Package	Version
Number	2.0.0-20191128-060437
OCR	2.1.0-20191121-100301
PDF	2.1.0-20191128-060540
PGP	2.1.0-20191129-100500
Ping	2.0.0-20191128-060544
PlaySound	2.0.0-20191128-060545
Prompt	2.0.0-20191128-150505
Python	2.0.0-20191128-060553
Recorder	1.0.45-20190904-210340
Rest	2.0.0-20191128-060646
SAP	2.1.0-20191128.003143-259
Screen	2.0.0-20191121-100518
SNMP	2.0.0-20191128-060656
String	2.0.0-20191128-060704
System	2.0.0-20191128-150557
Terminal Emulator	2.0.0-20191128-060711
VBScript	2.0.0-20191121-110553
Wait	2.0.0-20191128-060716
Window	2.0.0-20191128-060718
XML	2.0.0-20191017-030831

Fixed features

The fixed features in this release have not changed since the previous release. For a list of these features, see Enterprise Version A2019 (Builds 1082 and 1089) Release Notes.

Security fixes

The security fixes in this release have not changed since the previous release. For a list of these fixes, see Enterprise Version A2019 (Builds 1082 and 1089) Release Notes.

Deprecated features

The deprecated features in this release have not changed since the previous release. For a list of these deprecations, see Enterprise Version A2019 (Builds 1082 and 1089) Release Notes.

Known limitations in Builds 1598 and 1610

- IQ Bot is not supported in Automation Anywhere Cloud and users cannot register any IQ Bot instance with the Cloud Control Room.
- If a bot is deployed on a device, no other bots can be deployed on that device until the first bot has completed the deployed task.
- When deploying a bot using Unattended Bot Runner on a virtual machine with Windows 10 desktop, users have to enable remote access to the device (Control Panel > System Properties > Allow Remote Access).
- Deploying a bot with Bot Runner on a locked device will leave that device in an unlocked state.
- A Bot Creator is not able to view devices as assigned by the Control Room administrator. With this release, changes to the basic role has removed the View and manage all devices permission so that unless this permission is expressly granted by the Control Room administrator, the Bot Creator will no longer be able to see other devices in the Control Room. Bot Creators can register their devices directly; however, they will not be able to see the other devices in the Control Room.
- Unable to deploy bots from a private workspace using the wizard. Bot Creators can deploy bots from the editor.
- If users have set up Active Directory for Control Room authentication, changing to SAML or Control Room Database is not supported.
- Device pool administrators can delete a device pool after automation is scheduled and assigned to the pool.
- Users without SMTP can still import bots and packages.
- When users delete a bot from the Public workspace, the same bot is deleted from the Private workspace as well.
- Elastic Search Disaster Recovery backup is not supported.
- Using the Run Task action with the child task using triggers is not supported.
- User cannot export a bot with dependencies if that user does not have access to any of the related dependencies.
- Users cannot check out bots if they are linked through circular dependencies.
- Minimizing the window for some Microsoft Active Accessibility apps, such as Notepad, Calculator, or Remote Desktop Applications, can cause the operation to fail.
- UI Automation, such as Snagit Editor Window for example, will not work in the background unless expressly minimized.
- UI Triggers are not generating events with Snagit Editor or Inflow app.
- Applications such as calculator use different technologies on Windows 10 vs. Windows 2012 or other servers. In these cases, when a bot is created in one server configuration, the bot cannot be carried to another server. User triggers in these cases will not trigger bot deployment and there are no errors in the trigger listener or node manager logs.
- UI Triggers that are configured with multiple triggers are taking as much as 25 seconds to complete.
- UI Triggers with a single capture and a filter do not work with files larger than 2 MB.
- Button events where a user is switched from one window to a new window of an application fail to deploy a bot when listening for UI Triggers.
- For Automation Anywhere Elastic Search Service users, the C:\ProgramData\AutomationAnywhere folder has to be removed before installing A2019.
- Users cannot enable SMTP with TLS for the On-Premises version of the Enterprise Control Room (On-Premises only).
- User credentials are not editable (On-Premises only).
- Even when a newly added device is registered correctly, the indication icon does not turn green.
- Activity - In Progress table is not cleaning event records until the user performs a hard refresh (F5) of the browser.
- Domains are not shown for the Device/Run as tab when creating a role. This option is also missing when running a bot.
- Node manager is not able to establish a handshake SSL connection to the Control Room running on SSL certificate (On-Premises only).
- Repository Management API is incomplete; there is only one URL in the Swagger file.
- Device pools display completed automations, not scheduled automations.

- If a user is not the device pool administrator, the devices are not correctly displayed when editing a device pool.
- For an Unattended Bot Runner, with a device assigned and auto-login credentials set, and Run as self selected, the Run now option is disabled.
- When a user is running a bot from the Run Wizard and the Bot agent requires an update, after the user has updated the agent from the pop-up box, the user cannot deploy the bot until the user navigates back to the previous page and returns to the workflow to run the wizard.
- Folder triggers do not deploy bots when a folder change event occurs.

IQ Bot A2019 Builds 1598 and 1610

IQ Bot On-Premises version is available for this release with no additional features or updates since the last release.

IQ Bot changed features

IQ Bot is compatible with A2019 Builds 1598 and 1610.

IQ Bot fixed features

The fixed features in this release have not changed since the previous release.

IQ Bot security fixes

The security fixes in this release have not changed since the previous release.

IQ Bot deprecated features

The deprecated features in this release have not changed since the previous release.

IQ Bot known limitations

There are no new known limitations in this release.

Bot Insight new features in Builds 1598 and 1610

Feature	Description
Operation dashboard	The Operation dashboard in Bot Insight displays the Audit dashboard. You can search for the dashboards using the Search text box. You can also customize the dashboards based on your requirements. Role-based access control and permissions are applied to the dashboards so that the dashboard shows data only a specific user is authorized to view. See Operations dashboard.
Analytic visualization widgets	The following new widgets are added:

Feature	Description
	• Stacked Bar Chart • Clustered Bar Chart See Adding a dashboard widget.

Bot Insight changed features

The changed features in this release have not changed since the previous release.

Bot Insight fixed features

The fixed features in this release have not changed since the previous release.

Bot Insight deprecated features

The deprecated features in this release have not changed since the previous release.

Bot Insight known limitations

The deprecated features in this release have not changed since the previous release.

Enterprise Version A2019 (Builds 1082 and 1089) Release Notes

These release notes describe new features, changed features, fixed features, security fixes, deprecated features, and known limitations in Enterprise Version A2019.

Version A2019 Builds 1082 and 1089

Build 1082 contains updates for the following:

- Enterprise Community Edition
- Bot Insight

Build 1089 contains updates for the following:

- On-Premises
- IQ Bot A2019
- Bot Insight

New features in Version A2019 Builds 1082 and 1089

Feature	Description
Universal recorder support for SAP	The universal recorder now supports the SAP graphical interface for fast and accurate control and ease of editing generated scripts.
Citrix support	Citrix agent enables remote application recording for object cloning on Citrix servers and leverages ICA to create user sessions.
Enhanced code editing	Select multiple lines of code in editor to copy, move, disable, enable, as well as disable/enable a line of an action in a bot script. Users can run bots from a particular line of code or action inside the bot.
Bot import and export	Users can export bots with dependencies into a common zip file, including all actions. Users can manually exclude packages from the export process. All imported action packages will be automatically installed into the target Cloud Control Room and the bots placed inside the user private workspace.
Background processing	Background processing for Citrix Virtual Apps and Windows native applications. Excel packages inherently support background processes.
REST package	Support for GET, POST (text, XML, and HTML), PUT, and DELETE methods. Authentication types supported include Basic, Logged-in AD user, and NTLM.
OCR Action	Users can capture window and capture image by path.
Active Directory integration for On-Premises	Allowing auto-discovery of sites and domains, Automation Anywhere Enterprise Version A2019 On-Premises integrates Active Directory to support multi-domain as well as multi-forest deployments.

Supported packages

Package	Version
Node Manager	1.0.1745
Application	2.0.0-20191016.213334-22
Boolean	2.0.0-20191017-030403
Browser	2.0.0-20191017-030404

Package	Version
Clipboard	2.0.0-20191016.213334-16
Comment	2.0.0-20191017-030408
CSV/TXT	2.0.0-20191017-030409
Database	2.0.0-20191017-030411
DataTable	2.0.0-20191029.062940-3
DateTime	2.0.0-20191017-030416
Delay	2.1.0-20191017-030417
Dictionary	2.0.0-20191017-140648
DLL	2.0.0-20191031-100332
Email	2.0.0-20191024-120209
Error Handler	2.0.0-20191031-100110
Excel	2.0.0-20191024-160417
Excel_MS	2.0.0-20191101-120011
File	2.0.0-20191017-140654
Folder	2.0.0-20191017-140657
FTP/SFTP	2.0.0-20191023-181858
If/Else	2.0.0-20191017-030432
IR	1.0.0-20190923-115359
IQ Bot	2.0.0-20191031-150538
JavaScript	2.0.0-20191031-100128
Keystrokes	2.0.0-20191018-100419
List	2.0.0-20191017-030447
LogToFile	2.0.0-20191017-030447
Loop	2.0.0-20191017-030449
MessageBox	2.0.0-20191017-030449
Mouse	2.0.0-20191017-030450
Number	2.0.0-20191029-100152
OCR	2.1.0-20191017-030626
PDF	2.1.0-20191017-030713
Ping	2.0.0-20191017-030715
PlaySound	2.0.0-20191024-160415
Prompt	2.0.0-20191024-160423

Package	Version
Python	2.0.0-20191031-100238
Recorder	1.0.45-20190904-210340
Rest	2.0.0-20191024-090501
SAP	2.1.0-20191031-100334
Screen	2.0.0-20191017-030809
SNMP	2.0.0-20191023-181621
String	2.0.0-20191025-221016
Terminal Emulator	2.0.0-20191023-181907
VBScript	2.0.0-20191031-100352
Wait	2.0.0-20191017-030828
Window	2.0.0-20191017-030829
XML	2.0.0-20191017-030831

Changed features

Changed features	
TaskBot	All rich features of MetaBot, such as DLL and code protection using execute permission, are now part of a standard TaskBot. This also includes inline scripting using Python, VBScripts, and more to help reduce the learning curve for new users and provides a uniform bot development experience.

Fixed features

The fixed features in this release have not changed since the previous release. For a list of these features, see Enterprise A2019 (Build 550) Release Notes.

Security fixes

The security fixes in this release have not changed since the previous release. For a list of these fixes, see Enterprise A2019 (Build 550) Release Notes.

Deprecated features

The deprecated features in this release have not changed since the previous release. For a list of these deprecations, see Enterprise A2019 (Build 550) Release Notes.

Known limitations in Builds 1082 and 1089

- IQ Bot is not supported in Automation Anywhere Cloud and users cannot register any IQ Bot instance with Cloud Control Room.
- To create database tables in Cloud Control Room where internet access is restricted and deploying Liquibase, users are required to unblock the Java process to connect to www.liquibase.org in order to download the schema and allow java.exe to have internet access.
- The Folder trigger has the following event options: create, modify, and delete. The File trigger only has the modify and delete event options.
- A bot cannot have duplicate Triggers that point to the same directory.
- Using the action Run Task with the child task using triggers is not supported.
- Activity - In Progress is not cleaning the event record until user does hard refresh (F5) of the browser.
- User cannot export a bot with dependencies if that user does not have access to any of the related dependencies.
- Users cannot checkout bots if they are linked via circular dependencies.
- Minimizing the window for some Microsoft Active Accessibility apps, such as Notepad, Calculator, or Remote Desktop Applications, can cause the operation to fail.
- UI Automation, such as Snagit Editor Window for example, will not work in the background unless expressly minimized.
- If the system Citrix plugin is not updated, the Recorder will not launch.
- If the user renames a previously saved recorder bot, a download error is generated and results in loss of images.
- For Elasticsearch users, remove the C:\ProgramData\AutomationAnywhere folder prior to installing A2019.
- Users cannot enable SMTP with TLS for the on-premises version of the Enterprise Control Room (On-Premises only).
- User credentials are not editable (On-Premises only).
- Installer fails to create credentials using Windows Authentication. Use SQL Authentication service credentials (On-Premises only).
- In an On-Premises environment, creating credentials with the Credential Vault is not supported in this release.
- When using the Recorder with Citrix in an On-Premises deployment, the Citrix Agent could generate an internal server error during the recording process.

IQ Bot A2019 Builds 1082 and 1089

IQ Bot Community Edition is available for this release. IQ Bot is not yet available on Automation Anywhere Enterprise Cloud.

See IQ Bot Community Edition quick start guide .

IQ Bot changed features

IQ Bot is compatible with A2019 Build 1089.

IQ Bot fixed features

The fixed features in this release have not changed since the previous release.

IQ Bot security fixes

The security fixes in this release have not changed since the previous release.

IQ Bot deprecated features

The deprecated features in this release have not changed since the previous release.

IQ Bot known limitations

For On-Premises, if IQ Bot and Enterprise Control Room are installed on the same machine, on restarting the machine, IQ Bot does not work, and displays an error message.
Note: We recommend restarting Automation Anywhere Control Room Reverse Proxy service to resolve the issue.

Bot Insight new features in Builds 1082 and 1089

Feature	Description
Smart data profiling for country, state, and zip codes	Bot Insight analyzes information provided in the variables to automatically identify information based on the country, state, and zip or postal code. You can use this information to create the World and US Map widgets. See Editing a data profile.
Business data delete API	Use this API to delete logged data from either the production mode or the development mode for a particular Enterprise Control Room instance. See Bot Insight API details.
Business data profile API	Use this API to extract the business data profile logged in Bot Insight. See Bot Insight API details.
Business data API	Use this API to extract the business data logged in Bot Insight. See Bot Insight API details.
Resize dashboard widgets	You can resize and save the widgets in the Bot Insight dashboard based on your requirements. When you resize a dashboard widget, other widgets in the dashboard are automatically adjusted to fill in the available layout. See Editing a dashboard widget.
US map widget	The US Map widget enables you to visualize and analyze information about Country, State, City, and Zip Code. See Adding a dashboard widget.

Feature	Description
World map widget	The World Map widget enables you to visualize and analyze information about Country, State, Zip Code, Latitude, and Longitude. See Adding a dashboard widget.
Parent child dashboard	When you create a new bot, Bot Insight automatically creates a default dashboard. If you have a parent bot and a child bot, Bot Insight creates a separate dashboard for each of the bots. See Bot Insight dashboards.
Notification of variable updates in the standard dashboard	Data profile updates are highlighted with a red dot in the standard dashboard. See Customizing a dashboard.
Data logging	When you deploy and run a bot on the Bot Runner machine, Bot Insight aggregates all the information about that bot. The published dashboard for that bot displays the aggregated bot information. See Bot Insight dashboards.
Bot Insight	The Analyze package provides the following functions to enable business analytics in the Bot Insight dashboard: • Analyze Open • Analyze Close

Bot Insight changed features

The changed features in this release have not changed since the previous release.

Bot Insight fixed features

The fixed features in this release have not changed since the previous release.

Bot Insight deprecated features

The deprecated features in this release have not changed since the previous release.

Bot Insight known limitations

The known limitations in this release have not changed since the previous release.

Enterprise A2019 (Build 550) Release Notes

These release notes describe new features, changed features, fixed features, security fixes, deprecated features, and known limitations in Enterprise A2019 (Build 550).

New features in A2019 Build 550

Feature	Description
On-premises installer	The on-premises installation application for Enterprise A2019.
IQ Bot supports IE11	IQ Bot A2019 (Build 550) supports Internet Explorer version 11 (IE11).
Download all documents action	Use the Download all documents action to download the extracted results from an IQ Bot server that was created by running a TaskBot, using the Upload Document action.

Supported packages in Build 550

The supported packages in this release have not changed since the previous release. For a list of these packages, see Enterprise A2019 (Build 543) Release Notes.

Changed features

IQ Bot A2019 (Build 550) Changed Features	
Issue	Description
Language toggle UI redesigned	On the IQ Bot landing page, user can click the language toggle at the top right corner, to select a language from the drop-down list. The UI displays in the selected language. User can select a language from either the Enterprise Control Room or IQ Bot language toggle icon. Note: After logging out of the system, the system performs a reset. This requires the user to select the language again at login.
Upload document action	The Upload document action lets you to upload documents for processing with IQ Bot, using a TaskBot.

Fixed features

IQ Bot A2019 (Build 550) fixed features:

- Japanese documents using Microsoft Azure Computer Vision OCR engine get classified correctly.
- In the Designer window, during document training, user is able to move from one page to the other successfully along with mapping of form and table fields.
- Download API can download successfully processed documents after moving the bot and learning instance to production.

Security fixes

No security features are introduced in this build.

Deprecated features

No deprecated features are introduced in this build.

Known limitations

IQ Bot A2019 (Build 550) known limitations:

- When using Internet Explorer (IE) 11, icons disappear after a page refresh. A hard refresh (Ctrl plus F5) helps fix the issue.
- When using Internet Explorer (IE) 11, if user imports a domain, the system shows an error message. However, the feature works as expected.
- User is unable to migrate IQBA files from other versions of IQ Bot.
- IQ Bot portal does not launch after a machine restart. User has to restart Automation Anywhere Control Room Reverse Proxy Service as well.

Enterprise A2019 (Build 543) Release Notes

These release notes describe new features, changed features, fixed features, security fixes, deprecated features, and known limitations in Enterprise A2019 (Build 543).

New features in A2019 Build 543

Feature	Description
Next generation bot workbench	Create bots from any device, from anywhere through a web browser. The intuitive new design for applying multiple personas with varying bot building skills and a redesigned work area for simple assembly and deployment. These include: • A universal recorder to simplify capturing processes • List and Flow views for TaskBot creation • Powerful bot code management capabilities

Feature	Description
	• Rich variable passing with no cross-language mapping required
Bot Runner	Access and run bots from the cloud. When bots are deployed to Bot Runners, any dependent actions are also deployed. When updates to Actions are available, the updates are also automatically pushed.
Package manager	The package manager centralizes control over bundled actions to enable users to deploy and upgrade only those targeted actions being used.
Advanced variable types	Access expanded variables and array types for enhanced action implementation, including DateTime, numbers, list, Boolean, dictionary, multi-dimension arrays for reading Microsoft Excel documents, and file data column for .CSV files.
Inline scripting	Native support for Python and VBScript inline scripting languages enables simple data passing between scripts and bots.
New UX	The new user experience provides assistance for users who are getting started and includes step-by-step guidance for common tasks.
Excel automation	Configure Microsoft Excel TaskBot automation without installing Microsoft Office on the Bot Runner machine.
Recording of automation	Record automation, even from a remote device.
IQ Bot	Enterprise A2019 will fully support IQ Bot, the only AI-driven solution for users to automate processing of complex documents.
Bot Insight	The Analyze package provides the following functions to enable business analytics in the Bot Insight dashboard: • Analyze Open • Analyze Close

Table 1. Supported packages in Build 543

Package	Version
Node Manager	1.0.1221
Application	1.0.0-20190919.040305-1231
Boolean	1.0.0-20190919.040305-1435
Browser	1.0.0-20190919.040305-1287
Clipboard	1.1.0-20190919.040305-1492
Comment	1.0.0-20190919.040305-633
CSV/TXT	1.2.0-20190919.040305-1349

Package	Version
Database	1.1.0-20190919.040305-1287
DateTime	1.0.0-20190919.040305-1189
Delay	1.1.0-20190919.040305-1492
Dictionary	1.0.0-20190919.040305-1337
DLL	1.0.0-20190920.070246-677
Email	1.0.0-20190919.040305
Error Handler	1.0.0-20190919.040305-1333
Excel	1.1.0-20190921.042722-1353
Excel_MS	1.0.0-20190921.042722-1309
File	1.0.0-20190919.040305-1382
Folder	1.0.0-20190919.040305-1337
FTP/SFTP	1.0.0-20190919.040305-660
If/Else	1.0.0-20190919.040305-1375
IR	1.0.0-20190923.062209-1140
IQ Bot	2.0.0-20191031-150538
JavaScript	1.0.1-20190919.040305-989
Keystroke	1.1.0-20190919.040305-1492
List	1.0.0-20190919.040305-1466
Log to File	1.1.0-20190919.040305-1456
Loop	1.0.0-20190919.040305-1466
Message Box	1.1.0-20190919.040305-1492
Mouse	1.1.0-20190919.040305-1492
Number	1.0.0-20190919.040305-1148
PDF	1.1.0-20190919.040305-1492
Ping	1.0.0-20190919.040305-1319
PlaySound	1.0.0-20190919.054049-118
Prompt	1.1.0-20190919.040305-1180
Python	1.0.3-20190919.040305-1287
Recorder	1.0.45-20190904.153347-191
RunTask	1.1.0-20190701.181500-763
SAP	1.1.0-20190923.152217-493
Screen	1.0.0-20190919.040305-1105

Package	Version
SNMP	1.0.0-20190919.040305-359
Step	1.0.0-20190701.181442-695
String	1.1.0-20190919.040305-1469
Table	1.0.0-20190919.040305-719
VBScript	1.0.1-20190919.040305-1334
Wait	1.0.0-20190919.040305-1287
Window	1.0.0-20190919.040305-1333
XML	1.0.0-20190919.040305-717

Changed features

This build does not include any changed features.

Fixed features

No fixed features are introduced in this build.

Security fixes

No security fixes are introduced in this build.

Deprecated features

No deprecated features are introduced in this build.

Known limitations

Feature	Limitation description
Recorder	.NET Framework 4.6.1 is required for the Recorder package.
Bot agent	Users of build 543 are required to download and install the latest agent.
Bot Insight	Bot Insight has the following limitations: • Bot Insight dashboard does not support Drag and Drop to move and arrange the dashboard widgets within the dashboard. • The Date widget in the dashboard displays the Unix time stamp.

Feature	Limitation description
	• Bot Insight does not support the Aggregate By feature in the Table widget, if the table contains a Timestamp. • Once the bots run successfully, the default dashboard is generated after 5 to 10 seconds.

Enterprise A2019 feature comparison matrix

Use the feature comparison matrix to compare the Enterprise A2019 features with the Automation Anywhere Enterprise Version 11.3.x features.

- Core components
- Bot development
- Bot extensibility and code reuse
- Integration capabilities
- Device utilization capabilities
- Recorder capabilities
- Bot actions

Core components

	Enterprise A2019	Enterprise Version 11.3.x
Target user	• Citizen Developer • Specialist/RPA Developer • IT	• RPA Developer • IT
Delivery model	• Software as a Service (SaaS) • On-Premises	• On-Premises • Hybrid Cloud
Operating system	• Microsoft Windows • Linux (Linux CentOS 7.7, Red Hat Enterprise Linux 7.7)	• Microsoft Windows
Microsoft Active Directory support	Available (On-Premises)	Available
SAML 2.0	Available	Available
Authenticated proxy support	Available	Not available
Localized user interface (UI)	10 plus languages	3 languages
Bot Insight support	Available	Available

	Enterprise A2019	Enterprise Version 11.3.x
IQ Bot support	Available	Available
Interactive forms (attended automation) support	Not available	Available
Bot Creator platform	Web-based	Thick client
Bot Runner platform	Web-deployed	Thick client
Attended bots	Available	Available
Unattended bots	Available	Available
Upgrade to use new actions or commands	• No upgrade required for Cloud • Upgrade required for On-Premises	Upgrade required
Automate queuing	Available	Available

Bot development

Feature	Enterprise A2019	Enterprise Version 11.3.x
In-product learning	Available	Not available
Bot Creator Flow view	Available	Not available
Bot Creator Dual view	Available	Not available
Bot Creator Code view	Available	Available
Actions search	Available	Not available
Variable types	11	4
Advanced expressions	Available	Limited availability
Remote device testing	Available (Develop on one device and test on another device)	Not available
Localized actions	Available	Not available
Collaborative development	Available	Not available
Email triggers	Not available	Available
File and folder triggers	Available	Available
Interface triggers	Available	Not available
MetaBot Logic	Available through TaskBot	Available

Feature	Enterprise A2019	Enterprise Version 11.3.x
MetaBot DLL	Available through DLL: Run function action	Available
MetaBot Screen recalibration	Not available	Available
Import and export bots	Available	Available
Bot Lifecycle Management (BLM)	Available	Available
Global values	Available	Not available
Bot cloning	Available	Not available

Bot extensibility and code reuse

Feature	Enterprise A2019	Enterprise Version 11.3.x
Custom actions in palette	Available (build using Package Development Kit)	Not available
Inline scripting	Available in Python, VBScript, and JavaScript	Not available
Code reuse	Available for TaskBots, custom actions, and DLLs	Limited availability for MetaBots and DLLs

Integration capabilities

Feature	Enterprise A2019	Enterprise Version 11.3.x
Callouts using inline scripting	Available for Python, VBScript, and JavaScript	Not available
Enterprise Control Room APIs	Available	Available
REST Web Service	Available	Available
SOAP Web Service	Available	Available

Device utilization capabilities

Feature	Enterprise A2019	Enterprise Version 11.3.x
Workload management (WLM)	Available	Available
Device pools	Available for scheduling and WLM	Available in WLM only
Run-as users pool for automations	Available Set up multiple run-as users for device pools to provide effective license and device utilization	Not available

Feature	Enterprise A2019	Enterprise Version 11.3.x
Background processing	Available	Not available

Recorder capabilities

Feature	Enterprise A2019	Enterprise Version 11.3.x
Unified Recorder	Available	Not available
Recorder for Web/Windows	Available	Available
Recorder for SAP	Available for 64-bit Version 750 Patch 9 or later	Available
Recorder for Citrix	Available - ICA Agent-based	Available
Recorder for Oracle	Available	Available

Bot actions

Feature	Enterprise A2019 actions	Enterprise Version 11.3.x commands
Active Directory	Not available	Available
Analyze	Available	Not available
Application	Available	Available
Boolean	Available	Not available
Bot migration	Available	Not available
Browser	Available	Not available
Clipboard	Available	Available
Comment	Available	Available
Credential Vault	Available	Available
CSV/TXT	Available	Available
Data Table	Available	Not available
Database	Available	Available
Datetime	Available	Not available
Delay	Available	Available
Dictionary	Available	Not available
DLL	Available	Limited availability through MetaBot
Download a file from Enterprise Control Room	Available	Not available

Automation Anywhere Version A2019 - 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).

Feature	Enterprise A2019 actions	Enterprise Version 11.3.x commands
Email	Available (SMTP, EWS, and Outlook)	Available (SMTP, EWS)
Error handler	Available (Advanced - Try, Catch, Finally, Throw)	Available (Basic)
Excel advanced	Available	Limited availability
Excel basic (without Excel)	Available	Not available
File operations	Available	Available
Folder operations	Available	Available
FTP / SFTP	Available	Available
If	Available	Available
Image Recognition	Available	Available
Interactive form operations	Available	Not available
JavaScript	Available	Available through Run Script
List operations	Available	Not available
Log To File	Available	Available
Loop	Available	Available
Message Box	Available	Available
Mouse	Available	Available
Number	Available	Not available
OCR	Available	Available
Office 365 Calendar	Available	Not available
Office 365 Excel	Available	Not available
Office 365 OneDrive	Available	Not available
One Drive	Available	Not available
PDF	Available	Available
PGP	Available	Available
Play Sound	Available	Available
Printer	Available	Available
Prompt	Available	Available
Python Script (Inline)	Available	Not available
Recorder	Available	Available
REST Web Service	Available	Available

Feature	Enterprise A2019 actions	Enterprise Version 11.3.x commands
SAP support	Available (Native)	Limited availability through MetaBot
SAP BAPI	Not available	Available
Screen	Available	Available
Simulate keystrokes	Available	Available
SNMP	Available	Available
SOAP Web Service	Available	Available
Step	Available	Not available
String	Available	Available
System	Available	Available
TaskBot	Available	Available
Terminal Emulator	Available	Available
VBScript (Inline)	Available	Not available
Wait	Available	Available
Window	Available	Available
Workload	Available	Available
XML	Available	Available

Related concepts
Enterprise A2019 Release Notes
Package Software Development Kit (SDK)
Related reference
Enterprise Control Room operating system compatibility
Enterprise A2019 FAQ

Enterprise A2019 FAQ

For details and questions on the latest Automation Anywhere platform, Enterprise A2019, review this FAQ.

What is Enterprise A2019?
　　Enterprise A2019 delivers a browser-based, intuitive experience for business users to easily automate tasks and powerful tools for developers to build process automation, delivering security, governance, and control on a scalable infrastructure for IT.
What is included in Enterprise A2019?
　　Everything to build the bots you need to automate your business processes: Control Room cluster, Bot editor, Bot Runner, Universal Recorder, Enterprise-grade security certifications, support, access to the Bot Store, and courses on Automation Anywhere University.

How is Enterprise A2019 deployed?

Enterprise A2019 can be deployed On-Premises as well as in the Cloud.

For Enterprise A2019 On-Premises deployment, the installation is on the customer's servers. With the web-based nature of the Bot Creator, there is no installation or deployment required on the user machines, resulting in a significant reduction in total cost of ownership (TCO).

For Enterprise A2019 deployed in the Cloud, the platform is available as a true software-as-a service (SaaS) experience. Automation Anywhere offers this SaaS experience as a turnkey solution where the buyers do not have to worry about choosing the cloud provider, or any other infrastructure elements– Automation Anywhere takes care of it all. Admins get the complete set of features for user management, security, governance, and control that they also access through a web browser. The end users can then access the platform using their browser, log in, and start creating their bots.

What additional cloud hosting options are available?

Enterprise A2019 can be hosted on AWS, Microsoft Azure, Google Cloud, IBM, and any public, private, or hybrid cloud service.

What scripting languages does Enterprise A2019 support?

Enterprise A2019 supports JavaScript, Python, and VBScript.

Is Enterprise A2019 available in languages other than English?

Yes, Enterprise A2019 is available in 10 languages: English, French, German, Italian, Japanese, Korean, Portuguese, Spanish, Simplified Chinese, and Traditional Chinese.

How is Enterprise A2019 updated?

For Cloud deployed Enterprise A2019, customers are always on the latest version with updates rolled out by Automation Anywhere on a regular basis. For features such as action packages, admins and users have the ability to test the latest packages before choosing to accept the update.

For On-Premises customers, regular updates are made available through the customer portal, providing admins an opportunity to keep their business-wide installation on the version of their choice.

What are some of the data privacy and security aspects of Enterprise A2019?

Enterprise A2019 (Cloud deployed and On-Premises) includes enterprise-class security and data privacy out of the box. All the process and personally identifiable information (PII) data resides in the on-prem Bot agent on the customers' infrastructure behind its own firewall. This data is never exchanged with the cloud unless the bot is explicitly told to share it.

Data privacy includes AES 256-bit encryption for data at rest and TLS/1.2 for network/data in motion, as well as Kerberos-based active directory (AD) authentication. Its microservices architecture leverages the latest in web-scale security methods keeping bots, data, and users secure. No personal data is goes outside of the environment–unless you tell it to; it remains completely under the control of the IT manager.

Enterprise A2019 meets the following regulatory requirements for security: PCI, GLBA, GDPR, FISMA, OWASP, and SOC2. Enterprise A2019 deployed in the Cloud also employs industry best practices for security including L7 load balancing, Web Application Firewall, and private networking to control access.

Related concepts
Enterprise A2019 Release Notes

Automation Anywhere Enterprise Overview

The Automation Anywhere Enterprise Digital Workforce platform is the foundation to deliver the automation of complex business work, securely, and at scale.

Automation Anywhere leads the industry with the largest installed base of bots (automation tasks are called bots) – a bot install base that is many times larger than its closest competitor. This large install base, and corresponding product maturity, translates into a more robust and resilient product with a depth and breadth of features unparalleled in the Robotic Process Automation (RPA) space. Automation Anywhere's bots have proven capable of automating thousands of applications across varying infrastructures and industries, including some of the world's largest Banks and Telecommunication companies. This is the reason seventeen of the top twenty Business Process Outsourcers (BPOs) have chosen Automation Anywhere to deliver their Enterprise-class Digital Workforce.

Automation Anywhere Enterprise has been designed to gradually scale up to match each step of the RPA journey. It avoids imposing complexity in the early stages to ensure short time-to-benefit and reduced up-front expense. No heavy workflow methodologies or burdensome infrastructure requirements are there during the initial phases. Once initial pilots are ready to scale up, the centralized Enterprise Control Room delivers the automated provisioning, orchestration and controls required for large scale deployments. From desktops to datacenter and cloud-based scale-ups, Automation Anywhere distinguishes itself by delivering Enterprise-class management and control, without diminishing rapid time to value, across any infrastructure.

- Enterprise Control Room overview
  The Enterprise Control Room manages, schedules, executes, and configures various capabilities of bots and Bot Runners using a collection of specialized web services.
- Distributed Architecture
  Automation Anywhere platform is deployed using a distributed architecture.
- Network Architecture and Boundary Controls
  Communication between authorized and authenticated Bot Creators, Bot Runners, and the Enterprise Control Room use secure protocols and pass through a network firewall and a load balancer.

Enterprise Control Room overview

The Enterprise Control Room manages, schedules, executes, and configures various capabilities of bots and Bot Runners using a collection of specialized web services.

Components

The Enterprise Control Room is a centralized management point for all bots. A reverse proxy is responsible for listening for remote connection requests and forwarding those requests to the correct specialized service. The following figure shows the Enterprise Control Room components and general data center interaction.
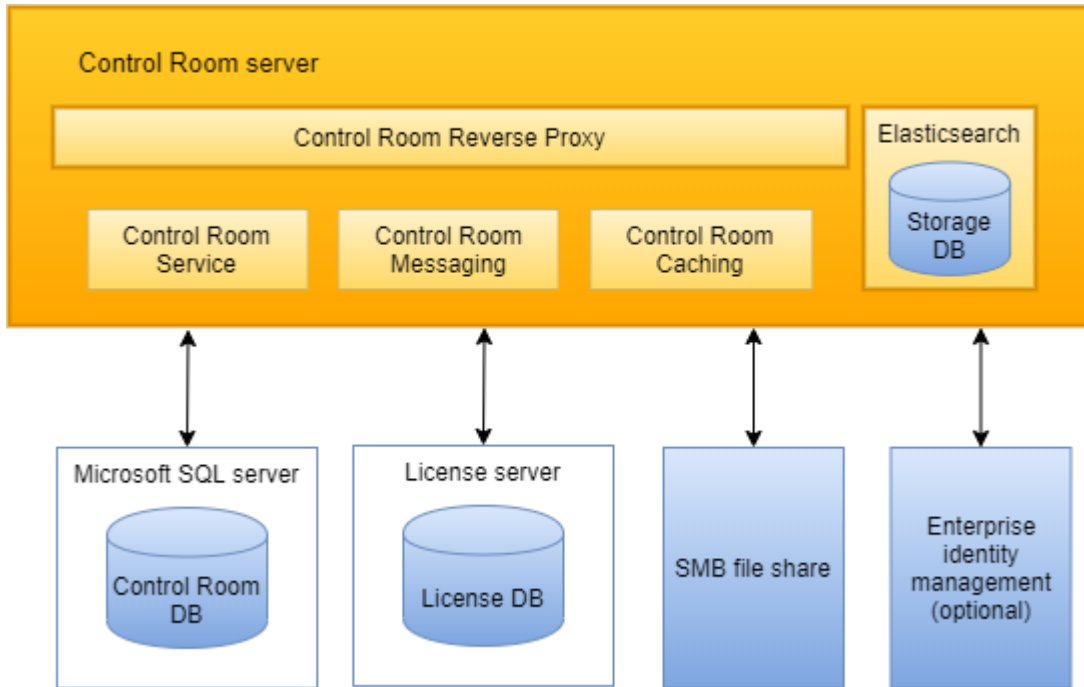
In the data center, Enterprise Control Room is installed on a server and configured to interact with the other data center components.

The Enterprise Control Room includes objects that performs the following:

- Enterprise Control Room reverse proxy is managed through the following functions:

    - Enterprise Control Room services

    - Enterprise Control Room messaging

    - Enterprise Control Room caching

- Elasticsearch

The Enterprise Control Room required data center components include:

- An SQL server with an Enterprise Control Room database.

- A Server Message Block (SMB) file share

Centralized Automation Deployment

- Enterprise Control Room acts as the single point of access and control for bot execution.
- Enterprise Control Room provides bot upload and download features to facilitate seamless collaboration for end to end business process automation by multiple users.
- All scheduling is managed by the Enterprise Control Room. Bots are deployed on the Bot Runners either ad hoc or on pre-defined schedules. Once the schedules are created, Enterprise Control Room automatically and intelligently picks up the subsequent updates to bots, without any need to alter automation schedules.

Centralized Access Control

- Least Privilege and Access controls user access. They are implemented in the Enterprise Control Room through Role Based Access Control (RBAC).
- All Users and Roles are created and managed from the Enterprise Control Room.

Collaboration Centralized Workforce Management

- Enterprise Control Room dashboards provide a single view of the entire automation infrastructure.
- Enterprise Control Room receives real time heartbeat and telemetry from automations with events, exceptions and alerts.
- Unauthorized users cannot pause, resume or stop any of the ongoing automations on any Bot Runner.
- All historical automation data is logged in and available through Enterprise Control Room Audit Logs.

Distributed Architecture

Automation Anywhere platform is deployed using a distributed architecture.

Centralized management is accomplished via a web-based server, called the Enterprise Control Room, to manage all development and execution of the digital workforce. The Enterprise Control Room is connected to Bot Creators and Bot Runners. Bot Creators are development systems used for authoring and tailoring of automations. Bot Runners execute the automations; they are run-time systems installed on machines. Bot Runners can be deployed on desktops, on virtual machines in data centers or cloud.
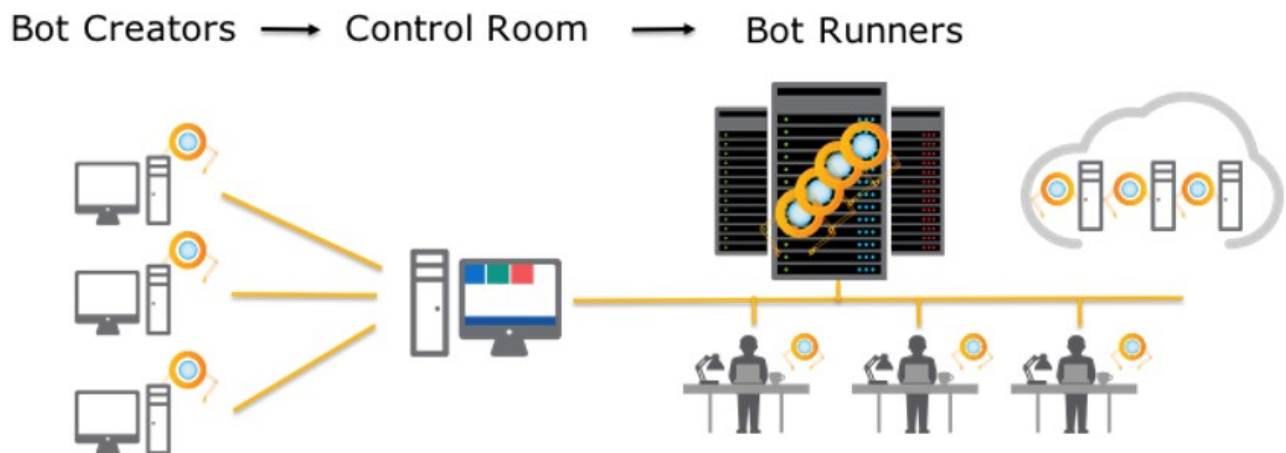
- Distributed architecture with HA/DR support
  The Automation Anywhere Enterprise self-contained platform within the customer environment mitigates the risk of "cross-contamination" from an unlikely event of a security breach from another network.

Distributed architecture with HA/DR support

The Automation Anywhere Enterprise self-contained platform within the customer environment mitigates the risk of "cross-contamination" from an unlikely event of a security breach from another network.

Automation Anywhere Enterprise supports distributed architecture to deliver the optimal performance and security. Following are the main distributable components of Enterprise Control Room which can be clustered to achieve High Availability (HA):

- Automation Anywhere Web Socket Server Service
- Microsoft SQL Server 2012 and higher

Figure 1. Distributed Mode
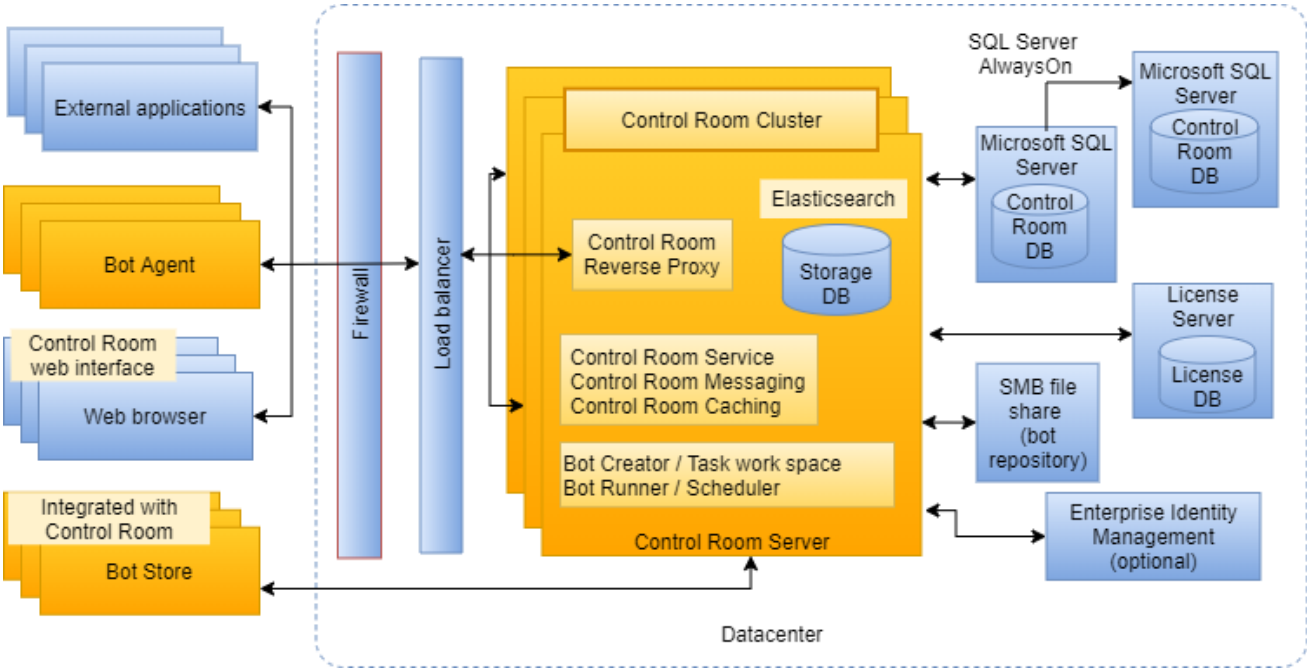
Distributed Cache

Enterprise Control Room architecture uses distributed cache to update all other nodes as soon as any information is updated in one of the nodes. This ensures fastest data synchronization across all the nodes and delivers seamless user experience. Automation Anywhere Enterprise platform uses clustering mechanism to implement distributed cache, to synchronize all data operations. For example, when the Credential Vault is opened from one node, it is automatically opened for all other nodes too.

Network Architecture and Boundary Controls

Communication between authorized and authenticated Bot Creators, Bot Runners, and the Enterprise Control Room use secure protocols and pass through a network firewall and a load balancer.

All communication between authorized and authenticated Bot Creators, Bot Runners, and the Enterprise Control Room use secure protocols and pass through a network firewall and a load balancer, based on customer deployment topology consistent with best practices as defined by NIST SC-7 Boundary Protections that require connections to networks only through managed interfaces using devices such as firewalls and load balancers.

All communications are denied by default and only allowed through specific services:

- Secure protocols, such as TLS 1.2, HTTPS, are used to communicate between different registered devices and Enterprise Control Room servers.
- Real time Data Service is a common service for all Application Servers. It receives and broadcasts real time task progress data coming from each running Bot Runner. It plays a mediator role between browser where Enterprise Control Room is opened and a Bot Runner where task is running.
- Shared File Repository is a file system location where all the bots reside physically. It is shared across all the Application Servers, so that same repository view and operations become possible.
- Data tier can be configured for failover cases separately if high availability is concerned.
- All network connections are terminated at the conclusion of each session or within a specified time period.
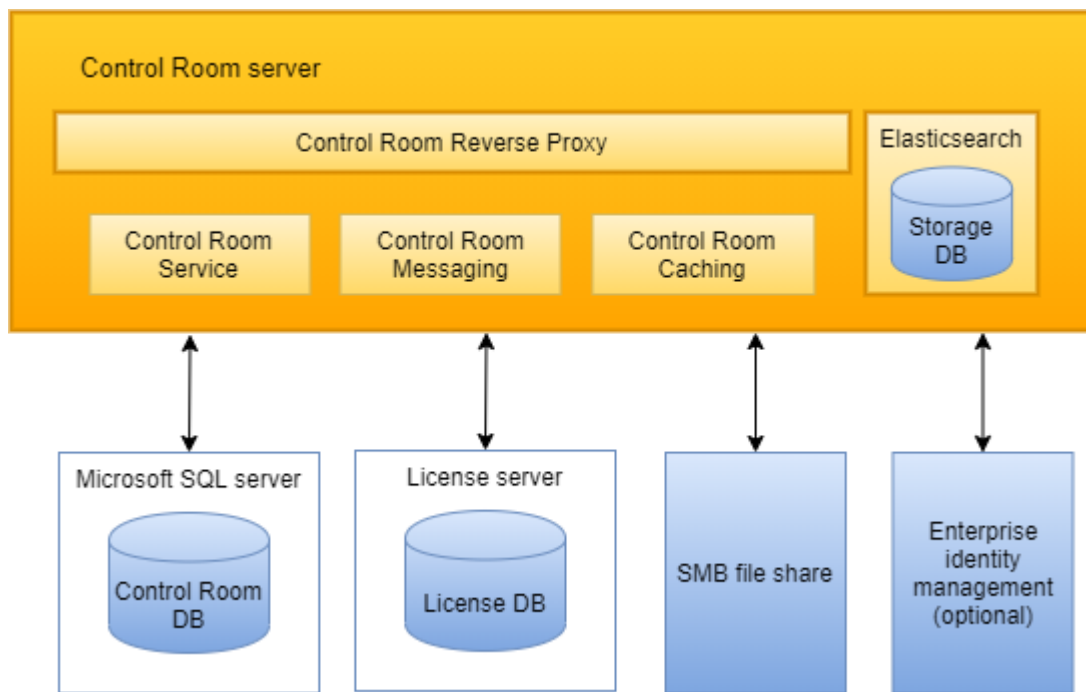
Attended automation

Automation Anywhere provides a robust RPA platform for attended automation that enables humans to collaborate with bots for completing tasks efficiently.

With attended automation, users can focus on critical inputs that require manual overview or approval, while the bots manage the repetitive tasks such as gathering information across databases, validating data or responding to chats. An attended process can be initiated in a variety of ways, including hot keys (like CTRL-SHIFT), a mouse-click in an application, or by clicking on the process in the system tray. The bots can then take over and perform those tasks faster, which can eliminate the possibility of human errors.

As attended automation is triggered by specific events or actions that users engage in across multiple platforms, it must be deployed as an agile and user friendly solution. When combined with unattended automation, a hybrid RPA model is formed that offers the following benefits:

- Reduction in possible errors caused by manual user updates or entries.
- Automated integration between multiple applications or databases occur in the background.
- User expertise is leveraged for higher-value work, repetitive tasks are consistently addressed.
- API integration not required.
- Training bots for continuous improvements can greatly reduce both time and business cost.

Attended automation is useful when all the tasks within a business process cannot be completely automated. When some of such tasks are used to trigger other bots with very little or no user intervention, it is called unattended automation. Unattended automation deploys bots that can be scheduled or triggered by events, which execute tasks and interact with applications without human involvement. Although attended and unattended bots are not mutually exclusive, a combination of attended and unattended automation provides for a complete RPA solution.

The following table provides a comparison between attended and unattended automation:

Attended automation	Unattended automation
Typically targeted at front-office activities where an entire process cannot be automated	Completely automated to execute back-end tasks and actions
Must be triggered by a user to start or complete certain tasks	Rules that are provisioned into the process can trigger and complete the tasks automatically
Can be triggered when required	Predetermined schedules start and complete the business tasks
Works best when integrated with service desk processes or environments	With back-end operations addressed, process compliance is always adhered to at very low costs
Visual workflow that is easy to comprehend for a first-time user	Time-consuming task allocations are automated to help front-end users focus on customer experience

Sample scenarios

Consider a typical scenario where an existing customer of an insurance firm has dialed in to review a claim status and a support executive is handling this call. The executive might have to spend a lot of time to retrieve customer information such as historical data, insurance type, and personal information, which might be in multiple applications or databases. With attended automation, the executive can just trigger a bot that collates data across various applications or databases and present it in a single user-readable format. This can reduce manual efforts and the executive can now focus on the critical task of addressing the customer's issue.

The following image illustrates the attended automation scenario:
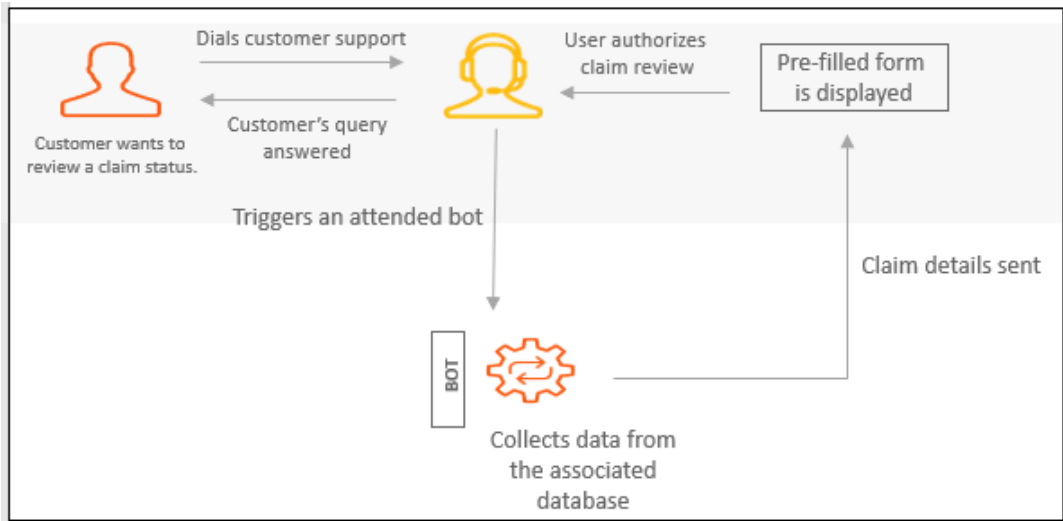
Consider another scenario where a new client's information must be updated across multiple resources. This can be a laborious process if an executive has to manually perform these updates every time for a new application. With unattended automation, the executive has to record only the necessary information on a single spreadsheet and trigger a bot with preset conditions. This unattended bot then allocates the new client data across multiple applications or databases in the background, without any further intervention or supervision the executive.

The following image illustrates the unattended automation scenario:
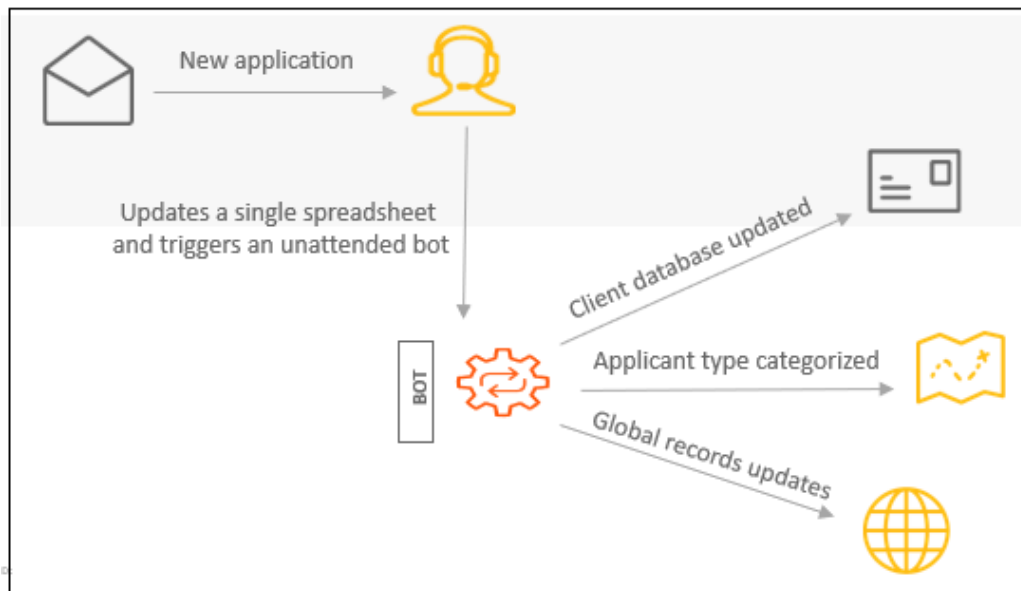
Related concepts
Attended automation using Enterprise A2019

Security architecture

Many of the largest financial organizations in the world rely on Automation Anywhere's secure digital workforce platform to automate security-sensitive operations.

The platform's security architecture is founded on Least Privilege principles and a strict Separation of Duty model with 41 technical controls implemented across seven NIST 800-53r4 Control Families. Controls are applied across three components: the Enterprise Control Room, Bot Creators (development systems), and Bot Runners (bot execution run times) through the bot life cycle from creation through decommissioning. This security architecture and the underlying controls are mapped to industry best practices as defined by NIST and can be readily mapped to other frameworks, for example, CoBIT (SOX) and ISO 27002.

Access Controls. Automation Anywhere Enterprise (AAE)

Access Controls. Automation Anywhere Enterprise (AAE) limits and controls human and bot access to logical resources across components.

- Two independent control planes enforce least privilege. Only developers are enabled to read or write, only authorized Enterprise Control Room users to execute automations, (Enterprise Control Room authorizes and executes) subject to fine-grained Role Based Access Controls (RBAC) down to individual automations (bot), Bot Runners and domains.
- Bot-level Separation of Duty is enforced. Each bot is obfuscated and executed by its corresponding authorized Bot Runners.
- Bot execution is controlled via RBAC. Domain privileges are defined across groups of bot and Bot Runners.
- Security at-rest and in-transit. All access credentials are secured at-rest via a central credential vault with support for third-party credential stores, for example, CyberArk. All communications are secured in-transit via SSL and TLS.

Configuration management

Configuration management is controlled at both bots and Bot Runner levels.

- The Enterprise Control Room authorizes, enforces, and logs changes to all Bot Creators and Bot Runners.
- Bot change control on execution is enforced through encryption and authentication.

Identification and authentication

Identification and authentication is controlled through Microsoft Windows authentication services.

- Bot Creators use for authentication
- Bot Runners have two levels of authentication, one for autologin authentication of the runner and the other for execution of bots.
- Credentials are secured at-rest and in-motion through the Credential Vault or integration with third-party products.

Risk assessment

Risk assessment is undertaken on Static, Dynamic, and Network-based Vulnerability Assessments. Audit and Accountability are established through event capture, logging and auditing on all three components with granular event capture at the bot level and nonrepudiation. Bot Insight embedded analytics provides near-real-time Incident Response and integration with Security Event and Information Management systems.

- Security architecture model
  Automation Anywhere Cognitive security architecture is founded on Least Privilege principles and a strict Separation of Duty model with 41 technical controls implemented across seven NIST Control families.
- Securing the RPA environment with external controls
  The Automation Anywhere architecture consists of a standard desktop and server class infrastructure for the registered devices and the Enterprise Control Room.
- Independent categories for Bot Creators and Bot Runners
  For logical separation of duties, Enterprise Control Room divides automation users into two broad categories: Bot Creators (development) users and Bot Runners (run-time) users.
- Role-Based Access Control
  Enterprise Control Room implements Least Privileges and Separation of Duties through a configurable Role-Based Access Control (RBAC) capability that conforms to requirements in NIST AC 2, 3, 5, and 6.
- Bot execution access by dynamic access token
  The Enterprise Control Room implements and enforces a Trusted Path for registration and authentication of Bot Creators and Bot Runners in accordance with NIST SC-11 to protect against any attempt to execute unauthorized bots.
- Secure credential store Credential Vault
  The Automation Anywhere platform provides a centralized Credential Vault to securely store all credentials and provision them to bots on an on-demand basis.
- Authentication with Enterprise Control Room
  When a Bot Creator or Bot Runner tries to connect to Enterprise Control Room, the credentials are encrypted using AES (256 bits key length) and RSA (2048 bits key length) and then transmitted on top of the existing layer of Transport Layer Security (TLS).
- Support for secure protocols
  The Automation Anywhere platform supports secure protocols, for example, TLS 1.2 and HTTPS data transfer.
- Network security overview
  All communication between the Enterprise Control Room, Bot Creators and Bot Runners is done using outbound WCF TLS 1.2 communications and inbound HTTPS TLS 1.2.
- Change management
  Access restrictions for configuration management.
- Identity and authentication
  All automation actions, for example, create, view, update, deploy, and delete, across the Automation Anywhere Enterprise are done only after Enterprise Control Room authentication is successfully completed.
- Defenses against common vulnerabilities
  The Automation Anywhere Enterprise platform provides some defenses against common attacks on applications.
- Compliance and vulnerability scanning
- Audit logs
  The Automation Anywhere Enterprise platform provides a comprehensive and centralized audit logging of all automation activities to authorized users. Role-based access control to Audit Log is managed through the Enterprise Control Room. More than 60 audit actions are logged.
- Additional security controls
  Automation Anywhere Enterprise Control Room restricts the database connection configuration with the system administrator account.

Security architecture model

Automation Anywhere Cognitive security architecture is founded on Least Privilege principles and a strict Separation of Duty model with 41 technical controls implemented across seven NIST Control families.

The NIST framework was selected as a foundation for best practices as a way to enumerate the controls implemented throughout. Translations from NIST to other control frameworks are widely available, resources are provided at the end of this topic.

The product security architecture is maintained by the Automation Anywhere's Product Management team and forms part of a formal policy model as an integral part of the Automation Anywhere Development Roadmap. The following table lists the Control families and the corresponding features and security impacts. Details on each Control family and how the security architecture is implemented in Automation Anywhere products are in the corresponding topics.

Control Family	Control Code	Enterprise Control Room Feature	Security Impact
Access controls	AC-3, 6, 7, 9, 10, 12	Central policy control	Enforce access restrictions for change control and least privileges on system components: • Fine grained access to bots and Bot Runners is controlled via RBAC, • Bot and Bot Runner domains can be assigned to roles via RBAC • RBAC roles are fully audited
	AC-2, 3, 5, 6	Role-based access control (RBAC)	Enable user access, restricts operational privileges, enforces least privilege principles
	AC-17	Bot repository	Bot versioning system with access restrictions
	AC-3, 7, 9, 10, 11	Bot and Bot Runner encryption	Encryption and obfuscation of sensitive information at bot level through credential vault and integration with key management systems
Configuration (change) management	CM-2, 5, 6, 7, 9	Centralized Bot Runner control	Restrict functionality based on roles, domains, implement deny-all and allow-by exception
	CM-10	Centralized licensing	Centralized provisioning, tracking and enforcement of Bot Creator and Bot Runner licensing
	CM-2, 5, 6, 8	Bot operations room	
	CM-8	Inventory control	Maintains centralized inventory control of all bots and runtimes

Control Family	Control Code	Enterprise Control Room Feature	Security Impact
Bot Creator configuration management	SA-10	Bot Creator management, bot check-in, check-out	Enterprise Control Room applies software life cycle management to bots from development, test, and production. Bot versioning enables change control of automations.
Audit and accountability	AU-1 through 15	Audit trail	Automated event logs captured on three levels: Enterprise Control Room, Bot Runners, and Bot Creators. Non-repudiation is assured through read-only logs, all user identities are bound to actions.
Identification and authentication	IA-1 through 5	Active Directory integration, Bot Runner ID and Attestation	Implements Windows platform security including cryptographic bidirectional authentication, Bot Runner identification and attestation, and password management policies. Credential vault with integration with key management systems, protects the integrity of credentials.
Incident response	IR-4, 6	Incident response	Bot Insight embedded analytics capabilities can monitor events and generate alerts to SIEM systems for response.
Controlled maintenance	MA-2	Automated maintenance	Enterprise Control Room versioning system provides an automated mechanism to roll out updates to bots, historical information is maintained.

(1) Resources: ISACA provides guides that map NIST SP800-53 to other security frameworks such as CoBIT (SOX), SANS Top20 (http://www.counciloncybersecurity.org/critical-controls/tools/) and ISO27002 (http://www.bankinfosecurity.in/mapping-nist-controls-to-iso-standards-a-7251).

Securing the RPA environment with external controls

The Automation Anywhere architecture consists of a standard desktop and server class infrastructure for the registered devices and the Enterprise Control Room.

RPA platform

This topic details the best practices for securing the RPA platform with external security controls. Network-based firewalls, Intrusion Detection Systems, anti-malware, and external log servers are all standard security controls that are relevant to RPA deployment and the other infrastructure in your environment. The following figure shows logically where these components are deployed in the RPA deployment:
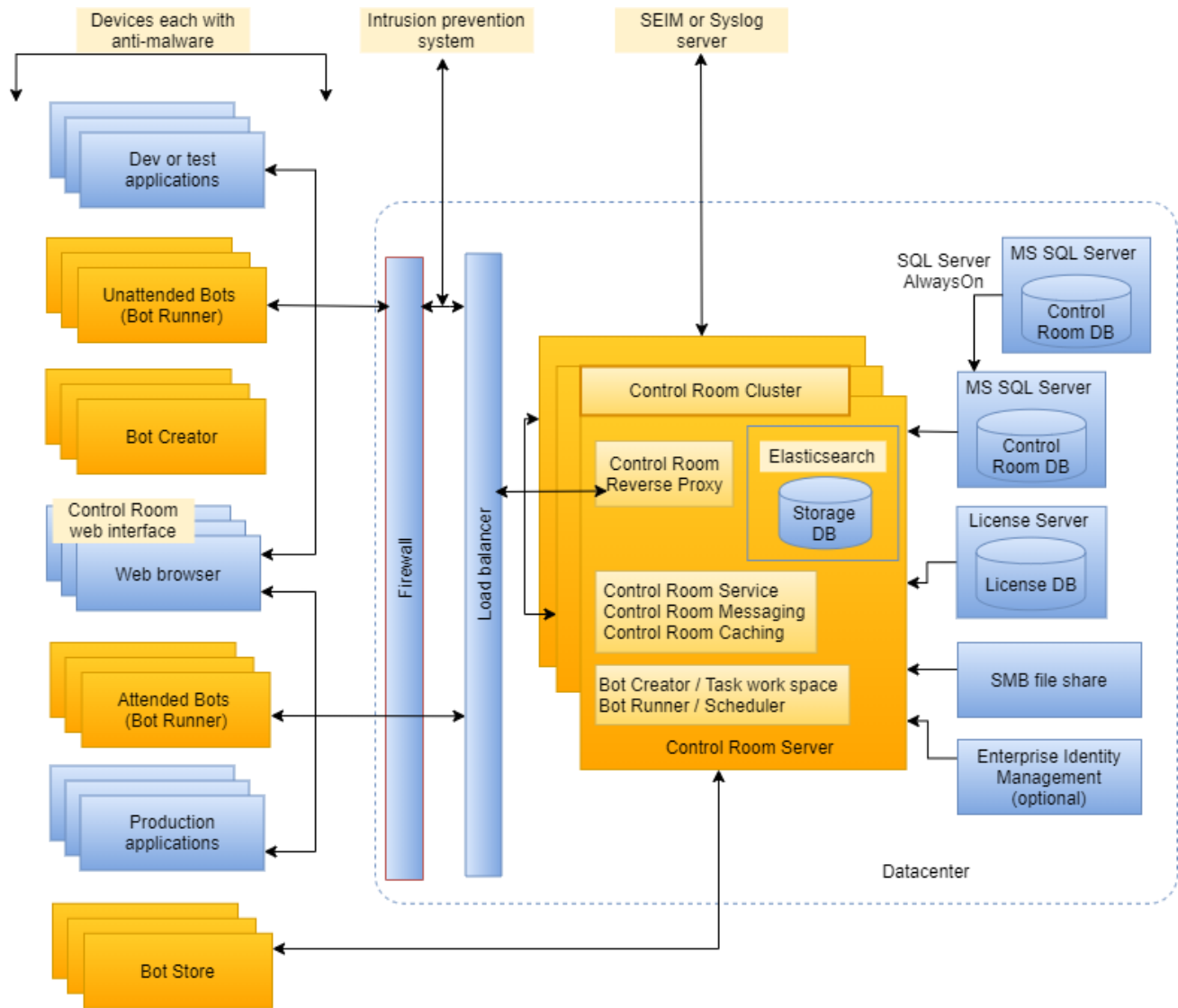
Each external security control is discussed in detail in the following sections, in terms of placement and configuration. Supporting network services such as Active Directory, SMB File Share, Microsoft SQL Server, and production applications, and are accessed through network firewalls or directly, depending on their placement relative to the RPA components.

Network-based access control to protect RPA with firewalls

Network-based firewalls and local server-based firewall are used to protect the Enterprise Control Room or all nodes in a Enterprise Control Room cluster. By default, required protocols on the Enterprise Control Room are permitted

from the corporate network. Additionally, all clustering protocols are permitted only between the nodes in the Enterprise Control Room cluster. Network-based firewalls are used to isolate Development, Test, and Production RPA environments from the corporate network and from each other.

For unattended automation environments, the Bot Runners are placed in a specific isolated network and protected by a network-based firewall. Attended automations run from corporate workstations with the Bot Runner Bot agent installed and are protected via the corporate perimeter firewalls or internal firewalls protecting the corporate desktop infrastructure, like any desktop.

Anti-malware to protect RPA from viruses and malware

The Automation Anywhere Bot agent runs on desktop class infrastructure and is considered a corporate desktop. Anti-malware or anti-virus software is used to protect the registered device environment from malicious software in the form of viruses and malware.

Intrusion detection systems to protect RPA from direct attacks

Intrusion Detection and Prevention Systems (IPS) protect the corporate network by detecting network-based attack through network traffic analysis. Like any other critical section of the data center, an IPS protects the RPA platform at the egress point, behind the network-based firewall.

Security Event Incident Management to protect RPA with external auditing

All Automation Anywhere Enterprise Control Room logs can be forwarded to a Security Event Incident Management (SEIM) system for external storage, processing, and alerting. Integration with SEIM or any Syslog-based audit consolidation and reduction system greatly enhances the security posture and governance compliance. Configure the Enterprise Control Room to forward audit logs to the appropriate Syslog collection server in the environment.

Independent categories for Bot Creators and Bot Runners

For logical separation of duties, Enterprise Control Room divides automation users into two broad categories: Bot Creators (development) users and Bot Runners (run-time) users.

Bot Creators exist on a separate Microsoft Windows system with its own credentialing system to create, update, and unit test the bots on the Bot Creator. Bot Creators only upload and download bots to and from the Enterprise Control Room. Users on the Enterprise Control Room users have privileges to execute bots on Bot Runners but have no access to the Bot Creators. This separation of duty constitutes a dual authorization by requiring both the developer and the business user to create and execute the bot in conformance with NIST AC-3 best practices.

Role-Based Access Control

Enterprise Control Room implements Least Privileges and Separation of Duties through a configurable Role-Based Access Control (RBAC) capability that conforms to requirements in NIST AC 2, 3, 5, and 6.

All Enterprise Control Room users are assigned one or more roles. Access are available based on the usage conditions assigned to each role when users are a member. Authorized users can temporarily or permanently suspend other users when needed. RBAC enforces session handling to prevent unauthorized access. If an unauthorized user

attempts to view session details or gain access, the Control Room cluster will prevent this progress and immediately terminates the unauthorized session. The unauthorized user will be prompted to log in with valid credentials. Inactive accounts can be disabled.

The administrator controls are responsible for all security functions, consistent with best practices in NIST SC-3: Security Function Isolation.

The Enterprise Control Room includes segmented administrator roles by default. Many permissions are supported for creating new roles.

Controls are implemented at the Enterprise Control Room, Bot Creators, and Bot Runners layers, for NIST Access Controls (AC) and Change Management (CM) guidelines. The following technical controls are implemented to ensure access is governed through NIST Least Privileges.

- RBAC on bots
- RBAC on Bot Runners
  RBAC on Bot Runners facilitates complete isolation of one department Bot Runner seamlessly from the remaining departments' Bot Runners.
- RBAC for Credential Vault credentials management
  Credentials created in the Enterprise Control Room are used across Bot Creators and Bot Runners.
- Role-based processing domains
  The Enterprise Control Room RBAC applies the least privilege principles to domains by implementing Processing Domains, specifying role-based privileges and permissions at the bots and Bot Runners level.
- RBAC on Audit Log
  Audit is automated for all privileged and nonprivileged roles to conform to best practices, as defined in NIST AC-6.
- RBAC on viewing bot activity
  The Enterprise Control Room Activity menu provides options shows the status of the Automation Anywhere Enterprise automations. These options are: In Progress, Scheduled, and Historical.
- RBAC on User Management
  Access is deny all and allow by exception based on roles, domains as defined in RBAC. Only those users with access to User Management can manage other users in system.
- RBAC on roles and permissions management
  Access is deny all and allow by exception based on roles, domains as defined in RBAC.
- RBAC on bot schedules
  Access is deny all and allow by exception based on roles and domains as defined in RBAC.
- RBAC on license management
  Access to license management is deny all and allow by exception based on roles and domains as defined in RBAC.

RBAC on bots

Access is deny all and allow by exception based on roles, except for admin roles. Addressing NIST AC-17 (access control), NIST configuration managments for NIST CM-2 (base line configurations), access restrictions for NIST CM-5, NIST CM-6, and NIST CM-7 (least functionality), and monitoring NIST CM-9 for bot activity across the development, test, and production environment.

RBAC on Bot Runners

RBAC on Bot Runners facilitates complete isolation of one department Bot Runner seamlessly from the remaining departments' Bot Runners.

Bots are executed from the Control Room cluster. Local bot executions are protected through multiple layered security, and are designed to prevent fraud as a result from escalation of privileges on Microsoft Windows. The Bot Runner are executed by Windows, addressing access control enforcement in accordance with NIST AC-3 Access Enforcement and AC-6 Least Privilege for Code Execution.

If user roles does not have access to sets of Bot Runners, as a result, these users are unable to view the Bot Runners' executions or remote scheduling automation. See (Role-based processing domains).

RBAC for Credential Vault credentials management

Credentials created in the Enterprise Control Room are used across Bot Creators and Bot Runners.

These credentials are securely stored in the centralized Credential Vault to facilitate access control, and to divide in logical groups called lockers. These lockers enable complete separation between the credentials of one department from another.

Permissions for credential management-related roles include the following:

Manage my credentials and lockers
    By default, all users can manage their own credentials and interact with lockers if granted permissions.
Manage my lockers
    Allows the user to create and manage their own lockers.
Administer ALL lockers
    User has limited actions on all lockers.

Each locker has the following permissions:

Table 1. Locker permissions

	View locker	Edit locker	Delete locker	Add participant/ owner	Remove participant/ owner	View credential	Assign credential	Remove credential	User-specific value	Common value
Consume						✓			✓	
Participate						✓	✓			
Own	✓	✓	✓		✓	✓	✓	✓		✓
Share	✓	✓	✓	✓	✓	✓	✓	✓		✓
Admin	✓	✓	✓	✓	✓	✓	✓	✓		✓

Role-based processing domains

The Enterprise Control Room RBAC applies the least privilege principles to domains by implementing Processing Domains, specifying role-based privileges and permissions at the bots and Bot Runners level.

RBAC is applied at a folder level to completely and seamlessly isolate one department bot from the remaining department bots. If the user role does not have access to a set of bots, those bots do not exist, thereby enabling the separation of duties across different domains. For example, finance and accounting roles can access only the bots that automate their respective functions, and specific Bot Runners can execute these bots. This is consistent to best practices as defined by NIST AC-4 Processing Domains.

This permission is further divided into the following sub permissions:

Run
> Only those users who have this permission can run bots from the Enterprise Control Room to remote Bot Runners.

Authorized users assign various permutation and combinations of these accesses to different sets of users and roles based on the business need.

RBAC on Audit Log

Audit is automated for all privileged and nonprivileged roles to conform to best practices, as defined in NIST AC-6.

Access is view-only based on a deny all and allow by exception based on roles and domains as defined in the Audit section 7 addressing Audit and Accountability (NIST AU 1 through 15) and as required by NIST AC-2 Automated System Account Management. If a role does not have permission to view Audit Logs, then the Audit Trail tab is not visible to all members of that role. Audit automatically captures all events related to creation, modification, enablement, disablement, and removal of users, bots, Bot Creators, and Bot Runners.

RBAC on viewing bot activity

The Enterprise Control Room Activity menu provides options shows the status of the Automation Anywhere Enterprise automations. These options are: In Progress, Scheduled, and Historical.

Access to bot Activity status is deny all and allow by exception based on roles and domains as defined in RBAC. Two levels of checks are applied to access the bot Activity data. The user is required to be a member of a role that has access to view the Enterprise Control Room. Users with Enterprise Control Room access that can view only the bots belonging to their departments, as applied through RBAC on bots.

RBAC on User Management

Access is deny all and allow by exception based on roles, domains as defined in RBAC. Only those users with access to User Management can manage other users in system.

This permission is further divided into the following sub permissions:

Create Users
> Only those users that create new users from the Enterprise Control Room.

Edit Users
> Only those users that edit existing users from the Enterprise Control Room.

Delete Users
> Only those users that delete existing users from the Enterprise Control Room.

Authorized users assign various combinations of these access permissions to different sets of users and roles based on the business requirements.

RBAC on roles and permissions management

Access is deny all and allow by exception based on roles, domains as defined in RBAC.

Users with access to roles and permissions management can create, edit, and delete roles in the system. This permission is typically assigned to administrators and power users from across enterprises.

RBAC on bot schedules

Access is deny all and allow by exception based on roles and domains as defined in RBAC.

This permission is further divided into the following sub permissions:

Schedule my bots to run
    Only those users that create new schedules.
Edit my scheduled activity
    Only those users that edit their schedules.
Delete my scheduled activity
    Only those users that delete their schedules.
View and manage ALL scheduled activity
    Only those users that manage (edit or delete) all the existing schedules created by any user.

Administrators assign various permutation and combinations of these accesses to different sets of users and roles based on the business requirements.

RBAC on license management

Access to license management is deny all and allow by exception based on roles and domains as defined in RBAC.

Only those users with access to license management permission are able to update the license from the Enterprise Control Room. A common license exists for all the users across the Automation Anywhere Enterprise, for a specific Enterprise Control Room. The updated license ia effective for all the Bot Creators and Bot Runners registered with the corresponding Enterprise Control Room.

Bot execution access by dynamic access token

The Enterprise Control Room implements and enforces a Trusted Path for registration and authentication of Bot Creators and Bot Runners in accordance with NIST SC-11 to protect against any attempt to execute unauthorized bots.

The Enterprise Control Room issues new client access tokens or identifiers through hashing, signed by the Enterprise Control Room and sent to Bot Creators and Bot Runners over HTTPS. Every subsequent communication between Enterprise Control Room and Bot Creator or Bot Runner is serviced by the Enterprise Control Room after validation of the signature of the latest access token sent by the Bot Creator or Bot Runner. Each access token is unique to every

Bot Creator or Bot Runner. This ensures that even if an unauthorized user could bypass enterprise security and access the system, the Enterprise Control Room security restricts any damage.

Secure credential store Credential Vault

The Automation Anywhere platform provides a centralized Credential Vault to securely store all credentials and provision them to bots on an on-demand basis.

Use the Credential Vault to store other information deemed confidential or sensitive. The credential store implements NIST controls IA-2 to uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users).

Sensitive information does not need to be stored in bots or on Bot Runner systems, the Credential Vault facilitates a logical separation of credentials from the bots.

Credential Vault variables are created from the Enterprise Control Room and are instantly available to all the Bot Creators and Bot Runners registered with the respective Enterprise Control Room. Credential Vault adds flexibility and dynamic character to bots because only the credential references are present in the bots, and not the credentials. When bots are moved from one environment to another environment, absolutely no change is required in the bots. Bots can seamlessly pick up the credentials values applicable for the new environment from the Enterprise Control Room of that environment. Additionally, the Enterprise Control Room automatically stores configuration-related sensitive data into the Credential Vault by default.

- Cryptographic providers
  Use only the listed supported cryptographic providers.
- Credential Vault encryption
  The Automation Anywhere Enterprise Control Room installation generates the Master key and Data encryption key.
- Credential storage
  All sensitive data is stored in the Credential Vault using AES-256 encryption.
- Credential provisioning to bots
  Credentials are provisioned only during the execution of automation.

Cryptographic providers

Use only the listed supported cryptographic providers.

Enterprise client

AES256
    Microsoft .NET AesCryptoServiceProvider
RSA2048
    Microsoft .NET RSACryptoServiceProvider
HMACSHA256
    Microsoft .NET HMACSHA256
PGP Encrypt/Decrypt action
    Bouncy Castle OpenPGP 1.8.1

Enterprise Control Room

AES256
> Bouncy Castle FIPS 1.0.0

RSA2048
> Bouncy Castle FIPS 1.0.0

HMACSHA256
> Bouncy Castle FIPS 1.0.0

PBKDF2 + HMACSHA512
> Bouncy Castle FIPS 1.0.0

Credential Vault encryption

The Automation Anywhere Enterprise Control Room installation generates the Master key and Data encryption key.

The Automation Anywhere Enterprise Control Room installation generates the following two keys:

Master key
> This RSA-2048 bit key is managed by an administrator outside of the system. This key unlocks the Credential Vault. The administrator types the Master key each time the Enterprise Control Room is started. When the vault is open, the master key is immediately erased from memory and it is not stored anywhere in the Automation Anywhere Enterprise product.

Data encryption key
> This AES-256 bit key is stored in the Enterprise Control Room database and is used to encrypt and decrypt the credentials at the time of storage or provisioning. This key is encrypted using the Master key. The Data encryption key does not leave the Credential Vault at any time. Credential encryption and decryption are done at the Credential Vault.

Credential storage

All sensitive data is stored in the Credential Vault using AES-256 encryption.

These credentials are encrypted by the Credential Vault service to conform to NIST SC-28 and to prevent unauthorized access or disclosure of credentials. Only encrypted credentials travel from the Enterprise Control Room to the Database server and are stored in the database in an encrypted form. The data encryption key encrypts all credentials using an AES 256-bit key generated by a FIPS 140-2 Level 1 validated module to meet the NIST IA-7, SC-12, and 13 requirements for implementation of mechanisms for authentication to a cryptographic module that meets the requirements of applicable federal laws.

The data for user credentials for autologin to Bot Runners is also encrypted and securely stored in the Credential Vault with the bot credentials.

Credential provisioning to bots

Credentials are provisioned only during the execution of automation.

Bot Runners or bots do not store credentials locally. Credentials are provisioned only during the execution of the automation. When the credentials are requested by Bot Runners, encoded (64 bit) credentials travel from the

Enterprise Control Room to Bot Runner over HTTPS protocol. When the bots finish execution, credentials are erased from the memory.

Authentication with Enterprise Control Room

When a Bot Creator or Bot Runner tries to connect to Enterprise Control Room, the credentials are encrypted using AES (256 bits key length) and RSA (2048 bits key length) and then transmitted on top of the existing layer of Transport Layer Security (TLS).

This extra layer of message level encryption provides protection against network stack issues (such as Heartbleed where OpenSSL was leaking sensitive data from memory) and also adds protection to the last hop of the connection when TLS is terminated at the load balancer. These credentials are decrypted by Enterprise Control Room and authenticated against the hashed (PBKDF2 and HMAC SHA512 algorithm) user passwords or against via Lightweight Directory Access Protocol (LDAP).

- Supported authentication methods for Enterprise A2019 On-Premises
  Review the authentication methods supported by Enterprise A2019 On-Premises.

Supported authentication methods for Enterprise A2019 On-Premises

Review the authentication methods supported by Enterprise A2019 On-Premises.

Supported authentication methods

- using LDAP
- Active Directory using Kerberos
- SAML
- Local authentication using a database

The benefits of integrating with Active Directory include the following:

Easier adoption
    Integrates with an existing authentication solution, compliant with the standards.
Maintenance
    All passwords and password policies are centrally administered.
Better user experience
    Fewer passwords to remember.

Kerberos provides additional benefits over NTLM pass-through authentication.

- Open standard versus closed proprietary standard
- Mutual authentication of client and server
- Integration with smart cards for 2FA

Local authentication manages user passwords through the Credential Vault. Passwords are hashed using the HMACSHA512 algorithm, which is keyed by the output of the Password-Based Key Derivation Function (PBKDF2). User passwords are encrypted in transit through TLS 1.2.

All authentication and session management is handled through the well-tested Spring Security framework. Kerberos integration is provided through the well-tested Waffle framework. SAML integration is provided through the well-tested OneLogin framework.

Active Directory integration for authentication

Automation Anywhere offers seamless integration with Microsoft Windows Active Directory for access to the Enterprise Control Room, Bot Creators, and Bot Runners. When Enterprise Control Room is integrated with the Active Directory, all the Active Directory users with basic details are directly available in the Enterprise Control Room without any extra configuration. For Active Directory integration, user passwords stay in only Active Directory and are not saved in the platform.

In addition to Active Directory authentication, the Enterprise Control Room has its own controls to prevent unauthorized access to anDynamic access token authentication of Bot Runnersy automation data.

Dynamic access token authentication of Bot Runners

Bot Runner users can also configure their credentials for Bot Runners machine autologin. These credentials are saved in the centralized Credential Vault.

Multi-domain Active Directory support

Automation Anywhere platform architecture supports single-forest multi-domain Active Directory integration. Enterprise A2019 On-Premises can be configured with Active Directory global catalog server in a way that the Enterprise Control Room, Bot Creators and Bot Runners can all be in the same or different Active Directory domains of a single forest. This gives added flexibility and control for large-scale complex deployment where users are spread across geographies.

Multi-domain support is provided out of the box and no additional configuration is required. The Enterprise A2019 On-Premises user provisioning from different Active Directory domains is also seamless. It enables the Enterprise A2019 On-Premises admin to centrally orchestrate the digital workforce running across the globe.

Support for secure protocols

The Automation Anywhere platform supports secure protocols, for example, TLS 1.2 and HTTPS data transfer.

- Deployment of bots from the Enterprise Control Room to remote Bot Runners is done over TCP and TLS 1.2.
- Upload and download of bots from the Bot Creator to the Enterprise Control Room is done over HTTPS.
- Transfer of any information from the Enterprise Control Room to the database and vice versa is done over TDS and TLS 1.2.
- Transfer of encoded credentials from the Enterprise Control Room to Bot Runners is done over HTTPS.
- WebSocket communication with the real-time data service in the Enterprise Control Room is done over HTTPS.

Network security overview

All communication between the Enterprise Control Room, Bot Creators and Bot Runners is done using outbound WCF TLS 1.2 communications and inbound HTTPS TLS 1.2.

Bot deployment to remote bot runners, provisioning of credentials, automation scheduling, and event capture are done exclusively through the Enterprise Control Room. Use only HTTPS in the production environment.

- The REST APIs use Distributed Cache Service to get shared cached data required for specific functionality.
- The Scheduler Service makes REST API calls to run a task on a specific client machine at a specific time.
- Real-time Data Service makes REST API calls to authenticate incoming connection requests. It receives task execution progress updates by Bot Runners and sends that information to all connected browser clients using WebSocket Secure (WSS) protocol.
- The Enterprise Control Room makes REST calls for user authentication and repository operations, for example, upload a task, download a task, or compare two tasks.
- The Enterprise Control Room makes REST calls to the validate user session at regular intervals. The Enterprise Control Room deploys and runs a task on a specific device using Bot agent. It uses a TCP/IP channel.
- The Scheduler Service makes REST calls for autologin credentials. It also communicates to the Enterprise Control Room to get a license and user session-related information.
- The Enterprise Control Room makes REST calls to get autologin credentials for a logged-in device. It also communicates to the Enterprise Control Room to get the license and user session-related information.

Change management

Access restrictions for configuration management.

Baseline inventory controls for Bot Creators, Bot Runners and bots

The Enterprise Control Room provides a single-pane-of-glass on all automation operations and infrastructure, providing a way to baseline the configuration of the environment. Inventory controls are maintained through the application of RBAC and the use of the Bot Repository, Operations Room, and License Management to establish a single point of control for Base Line Configurations (NIST CM 2) access restrictions for configuration management (NI5T CM 5 and 6). Configure automated baseline reporting using the auditing and reporting systems in the Enterprise Control Room.

Change control and documentation RBAC

The Enterprise Control Room RBAC provides a point of access control and management for all changes to the Enterprise Control Room, Credential Vault, Bot Creators, bots, and Bot Runners with an automated mechanism to prohibit changes and report on any attempts to make unauthorized changes. The logging and auditing system on the Enterprise Control Room provides the reporting mechanism for change management to conform to best practices as described in NIST CM-3 through 5.

Software usage and license management

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

Dual authorization change management

Separation of duties is implemented at multiple levels. Dual authorization is achieved through separation of control planes for the Bot Creators and Bot Runners. Only bots created by an authorized Bot Creator can be executed by a separately authorized Bot Runner and only by a user who has been given the privileges to do so by an administrator.

Identity and authentication

All automation actions, for example, create, view, update, deploy, and delete, across the Automation Anywhere Enterprise are done only after Enterprise Control Room authentication is successfully completed.

After authentication is successful, the platform applies a second mandatory level of access control enforcement in the form of fine-grained Role-Based Access Control (RBAC).

The Enterprise Control Room has its own controls to prevent unauthorized access to any automation data.

Dynamic access token authentication of Bot Runners.

- Password hashing
  Password hashing does a one-way, permanent transformation of the passwords of the Enterprise Control Room users, inline with standard password management practices.
- Authentication failure messages
  If an authentication attempt fails, the Automation Anywhere Enterprise platform does not specifically state if the username or password is incorrect. It only states that the supplied credentials are incorrect.
- Auto logoff
  The Automation Anywhere Enterprise platform complies with information security guidelines regarding user session timeout because of inactivity.
- Authentication for Bot Runners
  Two layers of authentication are present for deploying the bots on remote Bot Runners.
- Dynamic access token authentication of Bot Runners
  The Enterprise Control Room implements and enforces a Trusted Path for registration and authentication of Bot Creators and Bot Runners in accordance with NIST SC-11.
- Integration with third-party identity and access management solutions
  The Automation Anywhere Enterprise platform supports seamless integration with privileged access management solutions, for example, CyberArk, TPAM, and Thycotic.

Password hashing

Password hashing does a one-way, permanent transformation of the passwords of the Enterprise Control Room users, inline with standard password management practices.

Enterprise Control Room passwords are concatenated with a salt and then hashed using the PBKDF2WithHmacSHA512 algorithm before being stored in the database.

- The salt is 256 bits in size and is randomly generated by a cryptographically secure PRNG.
- The HMAC SHA512 algorithm is used for hashing and provides additional security over traditional approaches.
  - A keyed hash provides protection against hash length extension attacks.
  - SHA 512 bit key is larger than the commonly used SHA 256 bit key.
- The key used for the HMAC is from the secure Password-Based Key Derivation Function (PBKDF2).
- Hashing is done for 100,000 rounds (based on NIST recommendations).

Every time a Bot Creator or Bot Runner authenticates against Enterprise Control Room, its credentials are authenticated against the hashed credentials.

Authentication failure messages

If an authentication attempt fails, the Automation Anywhere Enterprise platform does not specifically state if the username or password is incorrect. It only states that the supplied credentials are incorrect.

This is one critical information security requirement for Automation Anywhere Enterprise customers and defends the system against a brute force attack.

This authentication involves the following:

- Bot Creator, Bot Runner connection to Control Room
- User log in to the Control Room from the browser
- Connection from the Control Room to the SQL Server

All failed authentication attempts are logged. See Audit logs. Audit Log access is provided as per RBAC and audit logs are made available on a read-only basis for all users.

Auto logoff

The Automation Anywhere Enterprise platform complies with information security guidelines regarding user session timeout because of inactivity.

An active session with Enterprise Control Room is terminated after a predefined time interval when it is not being used. Users are automatically logged-off after an idle period of 20 minutes. Similarly, a Bot Creator session is terminated after 8 hours.

Authentication for Bot Runners

Two layers of authentication are present for deploying the bots on remote Bot Runners.

The logged off/disconnected/locked Bot Runner is logged on/connected/unlocked using the configured credentials. These credentials are fetched from the centralized Credential Vault over HTTPS. This first level of authentication is done against the domain automatically, on behalf of the user and is called Bot Runner autologin.

After being authenticated, Bot Runners can be authorized to execute bots independently and asynchronously.

Dynamic access token authentication of Bot Runners

The Enterprise Control Room implements and enforces a Trusted Path for registration and authentication of Bot Creators and Bot Runners in accordance with NIST SC-11.

The Automation Anywhere Enterprise platform protects the automation data against any attempt to subvert the path. The Enterprise Control Room issues new client access tokens, or identifiers, after a predefined time period. These tokens are protected to conform to NIST IA-5 by being signed by theEnterprise Control Room and sent to Bot Creators and Bot Runners over HTTPS. Every subsequent communication between the Enterprise Control Room and Bot Creator/Bot Runner is serviced by the Enterprise Control Room only after validation of the signature of the latest access token sent by the Bot Creator/Runner.

The access token is unique to every Bot Creator/Bot Runner. This protects the system from an unauthorized attempt to bypass security and execute an unauthorized bot, and is consistent with the best practices to conform to NIST IA-9 Service Identification and Authorization. These controls implement IA-3 for cryptographically based bidirectional authentication and attestation of Bot Runners and Bot Creators before establishing connections. This also addresses requirements around unique, automated, identifier management IA-4 for multiple forms of authorization and identification. Identifiers are dynamically managed for audit and control purposes. Identifiers are used as authenticators and managed for verification on initial deployment, revoke, and prevent reuse. There are no static, unencrypted, identifiers in use by Bot Creators or Bot Runners and cached tokens are cleared periodically.
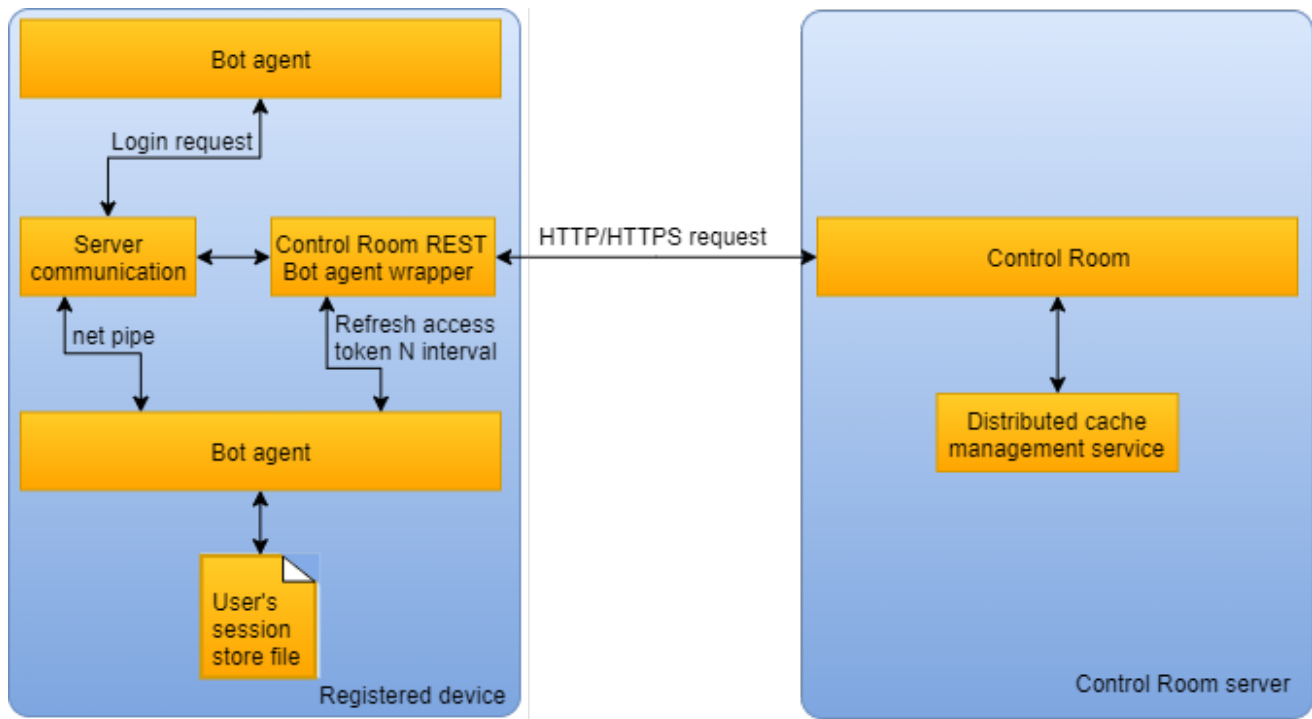
Integration with third-party identity and access management solutions

The Automation Anywhere Enterprise platform supports seamless integration with privileged access management solutions, for example, CyberArk, TPAM, and Thycotic.

CyberArk

Automation Anywhere provides integration with CyberArk, the leading privileged account security solution. Enterprises can decouple business applications' credential management from the platform. Bot Creators and Bot Runners can use the credentials stored in the CyberArk repository. Using CyberArk credentials, Automation Anywhere Enterprise bots authenticate against business applications.

Defenses against common vulnerabilities

The Automation Anywhere Enterprise platform provides some defenses against common attacks on applications.

The list below contains several examples of these attacks and the security controls in place to prevent them.

SQL Injection (SQLi)

SQL injection is a high-risk vulnerability that can seriously impact the confidentiality, integrity, and availability of a database. It enables an attacker to execute any SQL of his or her choosing inside the DB, thus allowing them to read sensitive data, modify/insert data, and execute various operations.

The Enterprise Control Room prevents SQL injection using query provided by the Hibernate framework.

Cross Site Scripting (XSS)

Cross-site scripting is a high-risk vulnerability that can seriously impact the confidentiality, integrity, and availability of any user web session. It enables an attacker to execute any JavaScript inside the victim's browser, allowing them to spy on the user's input/output or take unauthorized actions on behalf of the user. They could also redirect the user offsite to a malicious malware download or a credential phishing page.

The Enterprise Control Room prevents cross-site scripting using automatic output encoding provided by the ReactJS framework.

OWASP Top 10

Automation Anywhere Enterprise provides the following controls to protect against the OWASP Top 10:

Risk	Control
A1: Injection	All input is escaped before commands or queries are executed.
A2: Broken authentication and session management	See the identification and authentication section.
A3: Cross-site scripting	All output is encoded before being returned.
A4: Insecure direct object references	Centralized authorization via Spring Security.
A5: Security misconfiguration	No default passwords, stack traces hidden, secure server configuration
A6: Sensitive data exposure	See the Security at rest and Security in motion sections
A7: Missing function level access control	Centralized authorization via Spring Security
A8: Cross-site request forgery	Using authorization HTTP header
A9: Using components with known vulnerabilities	Black Duck software composition analysis tool
A10: Unvalidated redirects and forwards	N/A - No redirect functionality present

Compliance and vulnerability scanning

Secure software development life cycle (S-SDLC)

Automation Anywhere has implemented a development security plan and protocol that defines a specific depth of testing/evaluation to be done by the Engineering team on each release, conforming with best practices as defined by NIST SA-11 Developer Security Testing and Evaluation and NIST SA-15, Development Process, Standards, and Tools. This plan has been documented and shared with the Automation Anywhere Engineering teams.

Veracode vulnerability scanning for static and dynamic code analysis

On each weekly build, during the development process and before every release, all Automation Anywhere software is scanned for flaws using the Veracode tool. Automation Anywhere Enterprise meets the requirements for the strictest security policy available in the tool, Veracode Level 5, which is defined as no Very High, High, or Medium severity vulnerabilities. Analysis reports are available with each release.

Dependency analysis

On each weekly build during the development process and before every release, all of the third- party libraries and dependencies in Automation Anywhere's software are scanned for known vulnerabilities using the Black Duck tool. Automation Anywhere upgrades vulnerable libraries when new versions become available. Analysis reports are available with each release.

Penetration testing

Automation Anywhere does a penetration test via a third-party vendor before each major release. Additionally, Automation Anywhere incorporates the feedback from penetration tests conducted by customers, which includes some of the largest financial institutions in the world. Analysis reports are available with each release.

Audit logs

The Automation Anywhere Enterprise platform provides a comprehensive and centralized audit logging of all automation activities to authorized users. Role-based access control to Audit Log is managed through the Enterprise Control Room. More than 60 audit actions are logged.

All valid and invalid attempts of actions are logged. Events are logged by the following factors:

Doer of the action
> For example, a username.

Source of the action
> For example, Bot Runner or Enterprise Control Room

Type of event
> The description of the event.

When the event occurred
> For example, the date and the time of the event.

Where the event occurred
> The device.

Outcome of the event
> Description and status of the event.

Some key audit actions include the following:

- Log in and log out of the centralized Enterprise Control Room.
- Create, update, and delete Users.
- Activate and deactivate the Enterprise Control Room users.
- Any change of password for any user
- Create, update, and delete roles (helps in tracking changes to security policy, change in user access privileges)
- Create, update, and delete schedules
- Connection to the Credential Vault
- Create, update, and delete credentials
- Deploy the bots from the Enterprise Control Room to the remote Bot Runners.
- Pause, resume, and stop the ongoing automations.
- Any upload and download from Bot Creators and Bot Runners
- Any check-in, check-out of bots from Bot Creators and Bot Runners
- Update email and other settings
- Enable and disable secure recording.
- Change a license.

RBAC on audit log

Audit is automated for all privileged and nonprivileged roles to conform to best practices as defined in NIST AC-6. Access is view-only based on a deny-all and allow by exception based on roles and domains as defined in the Audit Section 7 addressing Audit and Accountability (NIST AU 1 through 15) and as required by NIST AC-2 Automated System Account Management.

If a role does not have permission to view Audit Logs, the Audit Trail tab is not visible to all members of those roles. Audit automatically captures all events related to creation, modification, enable, disable, user removals, bots, Bot Creators, and Bot Runners.

Enterprise Control Room Bot Creator and Bot Runner activity logging

For every Bot Creator and Bot Runner, the Automation Anywhere Enterprise platform does comprehensive activity logging for bots, workflows, and reports.

Some of the key activities logged include the following:

- Task creation, update, deletion (task is a type of bot).
- Task run
- Workflow creation, update, deletion
- Workflow run
- Report creation, update, deletion
- Report run
- Change in bot properties

Audit of Bot Runner operations

Bot Insight captures additional Bot Runner events for review and analysis of audit records for indications of inappropriate or unusual activity. The Bot Insight logs can be exported for further analysis. Automated dashboards and reports are available and can be customized to identify and alert on anomalous activity. These capabilities conform to best practices as defined in NIST AU-6 Audit Review Analysis and Reporting.

Audit log nonrepudiation

The logs are protected against an individual (or process acting on behalf of an individual) falsely denying having done authorized actions through read-only privileges, automated event capture, and binds the identity of the user to the actions, in conformance with best practices as defined in NISGT AU-10 Non-repudiation and AU-11 Association of Identities.

Export audit logs

All Enterprise Control Room and Bot Insight Bot Runner logs are exported to a Security Event Information Management Systems for further analysis to support the organizations incident response efforts in accordance with the NIST AU-6 and IR-5 requirements.

Additional security controls

Automation Anywhere Enterprise Control Room restricts the database connection configuration with the system administrator account.

Restrict installation from database system administrator account

All the database level transactions are done with a nonsystem administrator account. The Enterprise Control Room installer passes the SQL Server 2012 certification test.

Autolock the device

When Automation Anywhere Enterprise bots are deployed from the Enterprise Control Room to remote Bot Runners, they revert the Bot Runner system to its original state. For example, if the Bot Runner machine was logged off and our bot logged into the machine, it logs it off after the automation execution finishes. This ensures that system level security is not compromised.

Using SHgetKnownFolderPath function

Automation Anywhere software uses the SHGetKnownFolderPath function and Knownfolder_ID to determine the full path to the special folders. This is a recommended practice from Microsoft and use of this function ensures that system will never redirect automation data to any other folder, even if someone attempts to hack the function call. This is also one of the InfoSec requirements of Automation Anywhere Enterprise customers.

API level security

Automation Anywhere software does authentication and authorization level checks at the API level. API calls are serviced only for those users who have permission on the automation data. Unauthorized users cannot bypass system security through rogue API calls.

Clean uninstall

When Automation Anywhere Enterprise client software is uninstalled, it leaves no trailing files or folders behind. This clean uninstall of the Enterprise client software complies with InfoSec policies.

Store data in Program Data folder

Automation Anywhere Enterprise client software allows storing of automation data in the Program Data folder, for the files which must be edited by end users. Permissions are also set on the directory during the installation so that the user can edit the content of the folder. This complies with the InfoSec requirements of Automation Anywhere Enterprise customers.

Protected handling of MSVC DLL files

Automation Anywhere Enterprise client software uses MSVCxxx.dll files for automation purposes, but it does not install these files by itself. Client software directly uses the DLL files installed by only the Microsoft operating system. This ensures that client software does not overwrite the DLL files installed by Microsoft and our customers do not have to worry about doing one more cycle of checking for any introduced vulnerabilities.

Assembly manifest

All the executables (.exe file) of the Automation Anywhere Enterprise Control Room and Enterprise client software contain the manifest files which describe assembly metadata, for example, filename, version number, and culture. This makes our platform comply with organizational InfoSec policies.

Application path on network

Automation Anywhere Enterprise supports configuration of reading and writing automation data to a location on a network drive. This enables users to keep all automation data at one place.

Autologin without disabling legal disclaimer

When Automation Anywhere Enterprise bots are deployed from the Enterprise Control Room to remote Bot Runners, our customers do not need to change security settings, for example, disable login page, disable legal disclaimer, or disable screensaver. Automation deployment works seamlessly without disabling these settings.

Secure Java automation

The Automation Anywhere Enterprise platform can securely automate even those difficult-to-automate business applications which download the Java runtime environment (jre) during automation execution. Whenever these applications are started, an Automation Anywhere Enterprise agent gets associated with Java executable noninvasive and automates the business application. After the automation finishes, the Automation Anywhere Enterprise agent is automatically terminated.

Automation in nonEnglish languages

Users can securely use German, French, Italian, and Spanish language keyboard characters through the embedded automation commands in Bot Creators. This enables users to write data into these languages. Automation Anywhere customers do not need to depend on less secure third-party libraries for this automation.

General Data Protection Regulation guidelines

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).

For the most current description of Automation Anywhere GDPR compliance statement, see Master License Agreement and Cloud Security and Compliance with Data Privacy.