AUTOMATION ANYWHERE ENTERPRISE 11 LTS

Release Notes

Product Version	11.1.0.0
Document Version	1.3
Date of Publication	11-05-2018
Update(s) to Document Edition	Sec. 7 – Known Behaviour - The installer does not verify the port number corresponding to its SQL Server named instance in Database Configuration during installation.

Table of Contents

1   Document Purpose

This release note document for Automation Anywhere Enterprise (AAE) 11 LTS describes new features, enhancements, and issues resolved in this major version release.

Refer the Version Comparison Matrix to get an enumerated list of new features for AAE 11 LTS vis-à-vis 10.x.

2 Installation and Upgrade Notes

2.1 Installation Pre-requisites

- Refer to the AAE 11 LTS Client and Control Room Installation Guide that is shipped with the product.
- Note that AAE 11 LTS Client will ONLY work with AAE 11 LTS Control Room. For Client-Control Room compatibility, please refer: Control Room-Client compatibility matrix.

2.2 Installing AAE Client

Refer *AAE 11 LTS Client Installation Guide* for steps to install AAE Client.

Follow the below mentioned steps to install AAE 11 LTS Client, if installing on an earlier version:

Install the AAE 11 LTS Client with the set-up file provided.
The installer will automatically uninstall the old version and install the new version.
The AAE 11 LTS Client will point to the same repository path; thus, ensuring access to the Bots.

IMPORTANT: With AAE 11 LTS, the Bots, when saved, will be obfuscated with AES 256-bit obfuscation. Therefore, bots saved in AAE 11 LTS cannot be opened/played in earlier versions.

2.3 Installing AAE Control Room

Refer AAE 11 LTS Control Room Installation Guide for steps to install Control Room.

Follow the below mentioned steps to install AAE 11 LTS Control Room, if installing on an earlier version:

1. Uninstall the existing version of Control Room.
2. Install the AAE 11 Control Room with the set-up file provided.

2.4 Upgrading from earlier versions of AAE

AAE 11 LTS Control Room provides a built-in migration tool that allows existing customers to migrate their data from earlier versions of AAE (viz. 10 SP2, 10 LTS) to AAE 11 LTS. For versions prior to 10 LTS (10.3), customers will have to undergo a two-step migration process – first upgrading to 10 LTS and then to 11 LTS.

For more details, refer article on [Migration](#)

2.5 Version Compatibility

- TaskBot(s) created in earlier releases are compatible with this release.
- TaskBot(s) and MetaBots created/saved in this release shall not work if the product is downgraded to earlier versions.
- **For Example**: TaskBot(s) created in the current version of AAE 11 LTS shall not work in AAE 10 LTS. This is because of change in the bot obfuscation algorithm. Refer [here](#) for more details.
- MetaBot(s) created in earlier versions are compatible with this version; please check the [Control Room – Client Compatibility Matrix](#) for more details.

2.5.1 Control Room – Client Compatibility Matrix

Client Version ↓	Control Room Version →									
	10.0.0	10.0.1	10.0.2	10.1.0	10.2.0	10.2.1	10.3.x	10 SP2	11.0	11.1
10.0.0	√	√	√	√	√	√	√*	√*	X	X
10.0.1	√	√	√	√	√	√	√*	√*	X	X
10.0.2	√	√	√	√	√	√	√*	√*	X	X
10.1.0	X	X	X	√	√	√	√*	√*	X	X
10.2.0	X	X	X	X	√	√	√*	√*	X	X
10.2.1	X	X	X	X	√	√	√*	√*	X	X
10.3.x	X	X	X	X	X	X	√**	√	X	X
10 SP2	X	X	X	X	X	X	X	√	X	X
11.0	X	X	X	X	X	X	X	X	√	√
11.1	X	X	X	X	X	X	X	X	X	√

√* - From version **10.3 (i.e. 10 LTS**) onwards, MetaBots are stored as **Single File Format**, as opposed to the old folder based structure. Therefore, **MetaBots** created in **earlier versions cannot be directly used** with the 10.3.0 Control Room. They must be converted to Single File Format first and then used in 10.3.0 version.

√** - The Control Room version must be **equal or higher** than the Client version.

2.5.2 Products Compatibility Matrix for Upgrade

Following matrix shows products compatibility of Control Room, Bot Insight, IQBot, and BotFarm versions for upgrading to Control Room 11 LTS:

Control Room Version	Upgrade to 11 LTS	Bot Insight Version	Upgrade to 11 LTS	IQBot Version	Upgrade to 11 LTS	BotFarm Version	Upgrade to 11 LTS
8.x, 9.x	×	-	-	-	-	-	-
10.0.x -10.2.x	×	-	-	-	-	1.2	-
10.3.x	√	1.5.2	√	-	-	1.3	-
10.5.x	√	2.1	√	5.x	-	1.4	-
11.0.0	×	11.0.0	×	-	-	2.0	-

NOTE: "-" indicates not available, "×" indicates not supported, and "√" indicates supported version.

3 Automation Anywhere Enterprise - Version Comparison Matrix

Control Room	Version 10	Version 11
Type	Web	Web
Hosting Technology	IIS	Java
Data Storage	SQL Database	SQL Database
User Interface	Standard Web UI	Rich and responsive UI Controls
Dashboard	Basic	Graphical, drilldown UI
Centralized Bot Deployment	√	√
Roles and permissions	√	√
Role based access control	√	√
Centralized licensing	√	√
Centralized Scheduling	Basic	Advanced with Repeat option
Credential Vault	Standard	Advanced with RBAC, Lockers
Operations Room	Standard	Detailed
Audit	Basic	Detailed with changes
Mode of Authentication	AD, non-AD	SSO, AD (with Kerberos), non-AD
Data Migration	Desktop Utility	Web-based tool
API based deployment	√	√
Load Balancing	√	√
High Availability mode	√	√
Version Control Integration	√	√
Multi Domain Support	√	√
Email notifications	√	√
Customizable help links	√	√
Bot Runner Session on Control room	√	√
Bot Deployment API	√	√
Workload Management		√
Bot Lifecycle Management		√
Bot Runner health check		√
Bot Login Credentials API		√
Configurable Password Policy		√
Support for SQL 2016		√
Create/Rename Folders in Control Room		√

Bot Insight	Version 2.1	Version 11
Installer	Separate Installer	Integrated Installer
High Availability	√	√
Multi-Domain Support	√	√
Double byte data visualizations	√	√
Fluid Visualization Engine		√
Denser Dashboards		√
Better data caching		√

AAE Client (Bot Creator / Bot Runner)	Version 10	Version 11
Number of Commands	480+	480+
Ease of Use (drag and drop)	√	√
Recorders	Smart Recorder, Web Recorder, Screen Recorder	Smart Recorder, Web Recorder, Screen Recorder
MetaBot	√	√
IQBot	√ (Basic training)	√ (Centralized platform)
Online help	√	√
Packaging bot dependencies	√	√
Multi User support (Citrix/Terminal server)	√	√
Secure Recording	√	√
Integrated OCR engine	√	√
Bot Obfuscation	Basic 3DES	AES-256 algorithm
Dynamic Java Automation	√	√
AISense		√
Integrated Workbench		√
Quick command replication		√
Support for Windows 10		√
Support for Edge browser		√
Command-line Login to Client		√
Disaster Recovery of Bot Runners		√
Support for Windows Server 2016		√
Microsoft logo certification		√
Support for Japanese language		√
Folder support for MetaBots		√
Resolution independent IR		√
Auto mode in OCR		√

4   What's New

Automation Anywhere Enterprise 11 LTS (v11.1) is a full production release with support for following new capabilities in addition to 11.0 features.

4.1   Control Room

1. Built-in Migration within Control Room for existing customers to migrate data from 10.x to 11 LTS
2. Single Sign-On (SAML 2.0) authentication in addition to Windows and Database authentications
3. New User Interface for BLM to manage movement of bots across different environments
4. Enhanced Dashboards view for Work Load Management and Audit Log
5. Service Level Agreement (SLA) calculator for Work Load Management
6. Historical activities with detailed view of historical automations
7. Run or Schedule Master Bot with missing dependency
8. Enhanced User Experience with
   a. Pagination, Sorting, and Filtering across all pages
   b. Bulk Activate or Deactivate Schedules
   c. Create or Rename Folders in Control Room Repository
   d. Description for Control Room Users
   e. Differentiated display of deleted Users
   f. Copy existing Roles
9. Introduced new permissions to provide Role-based access to
   a. View, Manage and Install Licenses
   b. Run or Schedule a bot
   c. Play or Pause an automation
   d. View and Manage Schedules
   e. View Devices
   f. API Usage
10. Silent Installation of Control Room

4.2   Bot Insight

1. Upgraded Visualization Engine
   a. Quick & easy dashboard construction
   b. Denser dashboards with more widgets
2. Security Improvements
   a. Ports for Track & Trace methods disabled
   b. Integrated Login
   c. HTTPS with self-signed certificate built-in with the installer
   d. Installer checks for certificate validity before going further
3. Operations Analytics
   a. New Home, Audit & Workload Dashboards inside Control Room
   b. Graphical and drill-down widgets to analyze operational data
4. Bot Insight Admin Role
   a. Introduced a Bot Insight Admin role. This user has full access to the Bot Insight Application including the Bot Insight APIs.

4.3   Client

1. Resolution independent Image Recognition with enhanced accuracy
2. Single Sign-On (SAML 2.0) authentication in addition to Windows and Database authentications
3. Microsoft Windows Edge browser support
4. Disaster Recovery of production Bot Runners
5. Windows Server 2016 certification

6. Microsoft logo certification
7. Support for Japanese language
8. Folder support to store MetaBots
9. Auto-naming and filters for objects in MetaBots
10. MetaBot Logics and Parameters description
11. New automation commands in MetaBot Logics
12. Enhanced reliability of OCR automation
13. Upload Bot Dependency
14. Support for Command Line login
15. Linking Bot to Queue Category
16. Enable debug logging through UI
17. Password Policy Enforcement
18. Restriction of passing credential variable from TaskBot to MetaBot

5   Control Room

5.1   New Features and Enhancements

5.1.1   Data Migration

A **web-based data migration** tool is built-in within the Control Room that allows existing customers to seamlessly migrate their Automation environment from **10 LTS (10.3) or higher to 11 LTS (11.1).**

- Enterprise customers currently running on 10 LTS or higher can migrate their data **phase-wise** without disrupting their production environment.
    - For each migration run, a Control Room Admin can
    - select 10.x users or roles to be migrated,
    - review the data and its dependencies selected for migration,
    - visualize the data being migrated,
    - analyse the history of the data that was migrated.
- This mechanism helps the user to ensure that there is a parity between the existing and new systems at any point in time during the migration process.

For more information click here

NOTE: For customers currently running on version prior to 10 LTS, a direct migration to 11 LTS is not supported. They will have to undergo a two-step migration process by first upgrading to 10 LTS and then to 11 LTS.

5.1.2   Workload Management

(**NOTE:** Bots are tasks; these two terms have been interchangeably used in this document depending on the reference.)

With Workload Management, AAE users can configure the RPA platform for effective auto-distribution of workload to workload processors (bot runners or human) to achieve best optimization of resources, performance, and productivity levels to meet the Corporate SLAs. *(Zendesk # 54765)*
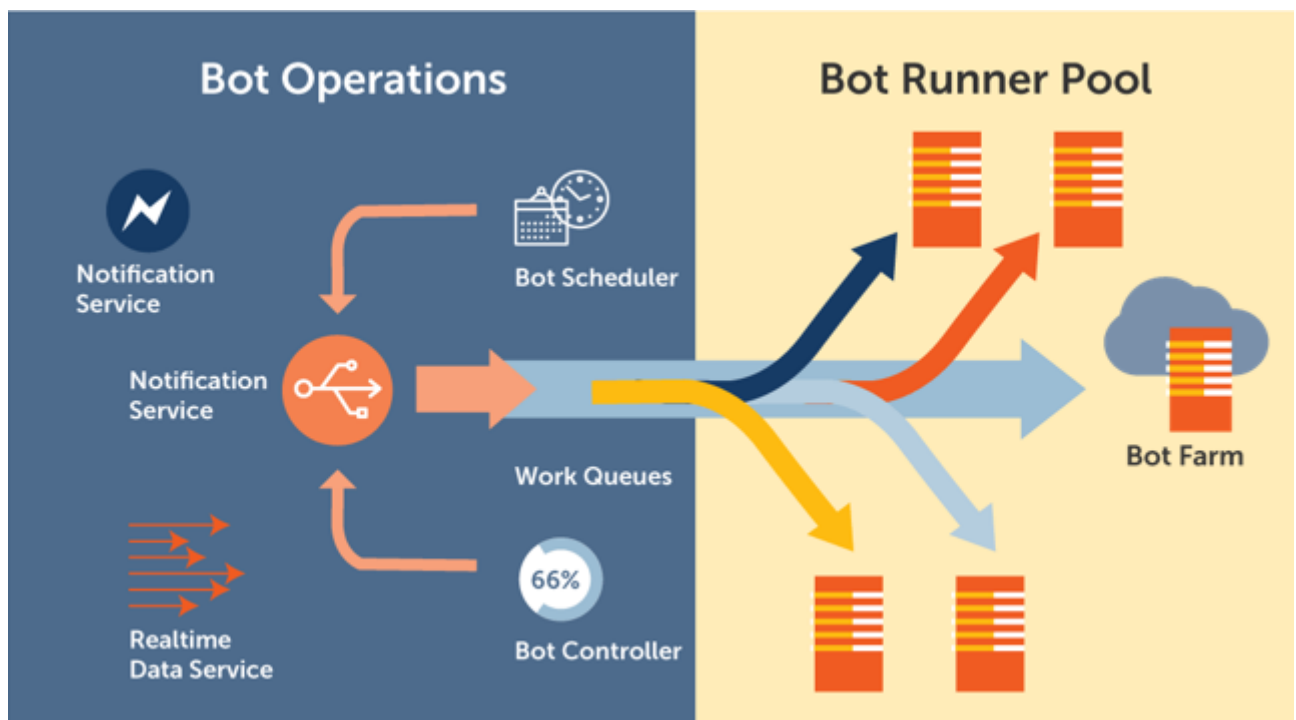
Figure 1: Workload Management in AAE v.11.0

Key Features & Business Benefits:

- SLA driven workload management.
- Centralized Workload queues to decrease wait time and increase processing volume.
- Prioritize a specific queue among other queues within Device pools to achieve SLA goals.
- Multi-Channel input from files, bots, APIs, emails, and database for increased flexibility.
- Agent assisted automation to handle human intervention in the automation workflow.
- End-to-end data encryption using AES 256 for information security.
- Support for complex workflow at ease with Queue orchestration.
- SLA calculator to get recommendations on pool size or SLA based on given input load
- API support to export or import queue meta data from/to the control room

For more information: click here

5.1.3 Credential Vault 2.0

Credential Vault 2.0 brings in granular, Role based access and ownership to Credentials used in the Bots, thus ensuring absolute data safety.

(Zendesk # 47518, 47880, 61522, 47474, 48249, 54767, 70168, 71057, 49972, 52685)

Key Features & Business Benefits:

- Locker based ownership and sharing of Credentials.
- Separation of duties with fine grained RBAC on Credential Management and Consumption.
- Stronger encryption of Credentials using AES-256 and RSA-2048 algorithms.
- Support for standard and user specific credential type.

For more information: click here
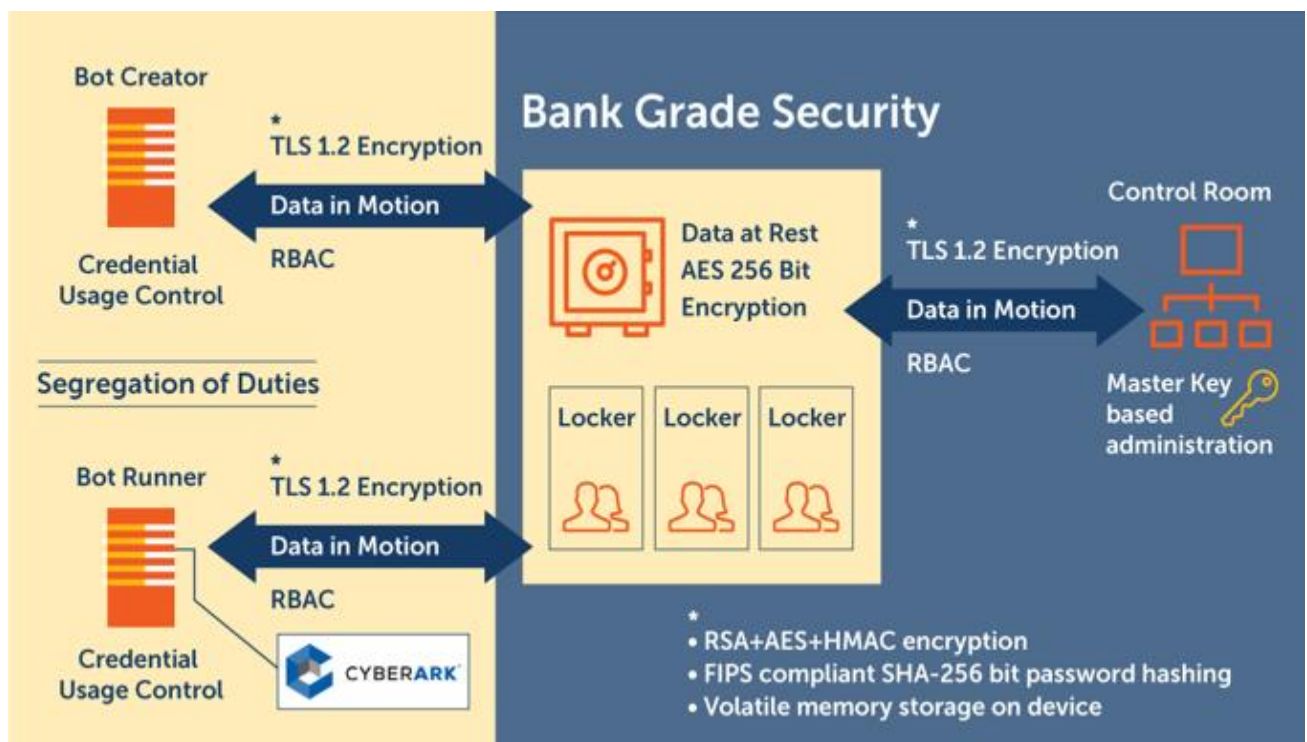

Figure 2: Locker based Credential Vault 2.0

5.1.4 Bot Lifecycle Management

Bot Lifecycle Management (BLM) enables organizations to have separate automation environments like Development, Testing, Acceptance, and Production (DTAP) and allows bot(s) graduate through its lifecycle stages (as defined by the organization) before they are deployed in production. *(Zendesk # 41412,47465)*
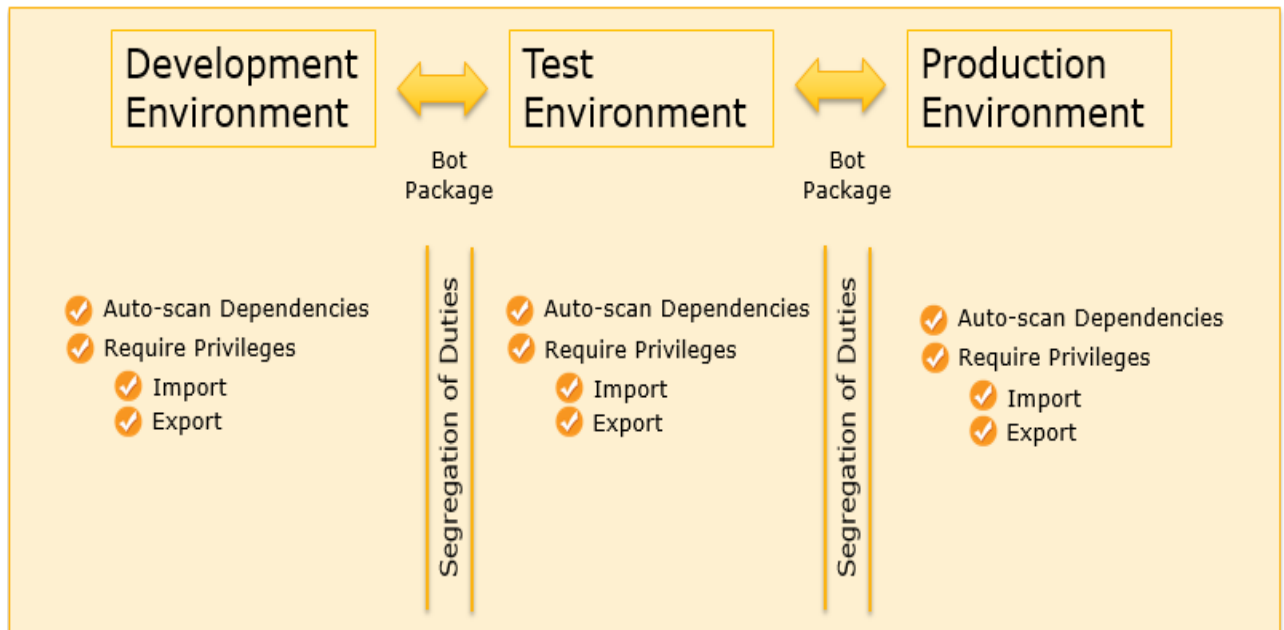
Figure 3: Migrating Bots using BLM (Bot Lifecycle Management)

AAE 11 LTS enables promotion of bots from one environment to another from Control Room UI.

Key Features & Business Benefits:

- Move multiple bots, their dependent bots, and files between Control Rooms.
- Granular Role based access control on BLM export and import
- AES-256 bits encryption of the exported package
- BLM APIs to export/import bots and dependencies

For more information: click here

5.1.5   Modern UX and Micro-Services Driven Architecture

AAE 11 LTS brings in a fully revamped UX of Control Room built for enhanced user experience and usability. The User Interface has various modern controls built-in to facilitate quick search, sort, filter to bring up the right data, and customization controls such as show/hide/move columns/widgets.

(Zendesk # 62931, 47874, 47456, 59003)

For more information: click here

The AAE 11 LTS application architecture is Micro-Services based to promote faster innovation and flexibility.
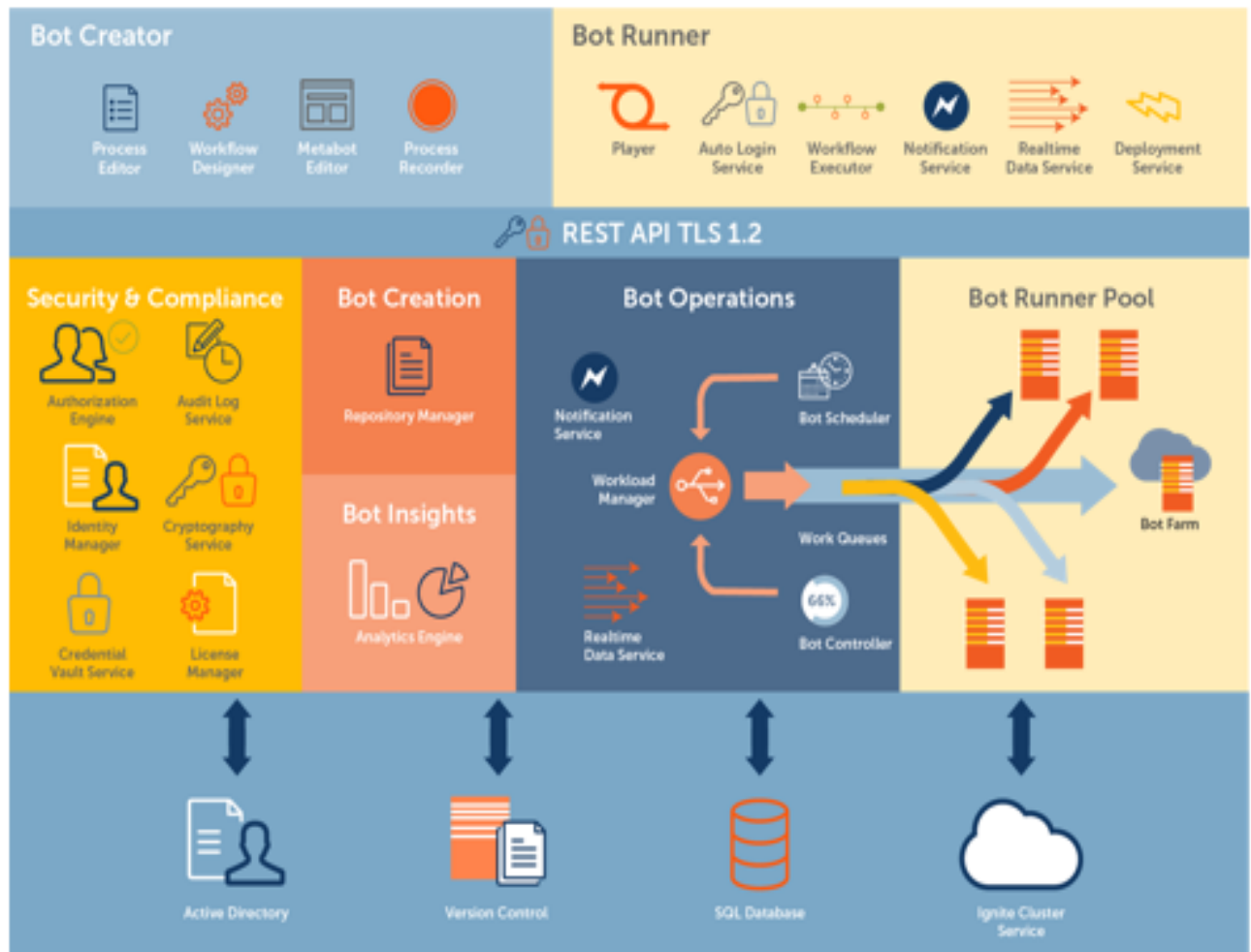
Figure 4: Micro Services based Architecture

5.1.6 Pagination, Sorting, and Filtering

If the number of items in Control Room landing page tables are greater than 200, rest of the items are displayed on subsequent pages in the same table. This delivers faster loading of Control Room tables since Control Room fetches only top 200 records at any time, even if total number of records are higher than that. User can also traverse through different pages of the table.

User can also reach the desired information faster by Sorting and Filtering available in Control Room tables. Sorting and filtering render the latest and most relevant data since that is performed on the entire data in the Control Room database, and not just on the visible data in Control Room UI.

5.1.7 Bot Insight Driven Centralized Monitoring Dashboards

AAE 11 LTS brings in round-the-clock real time KPIs and visual dashboards providing RPA users ability to monitor any current and anticipated issues.

Multiple RPA aspects such as Bot Heartbeat, Bot Status, Top Bot Failure Reasons could be visualized on a single page at a central location.

For more information: click here
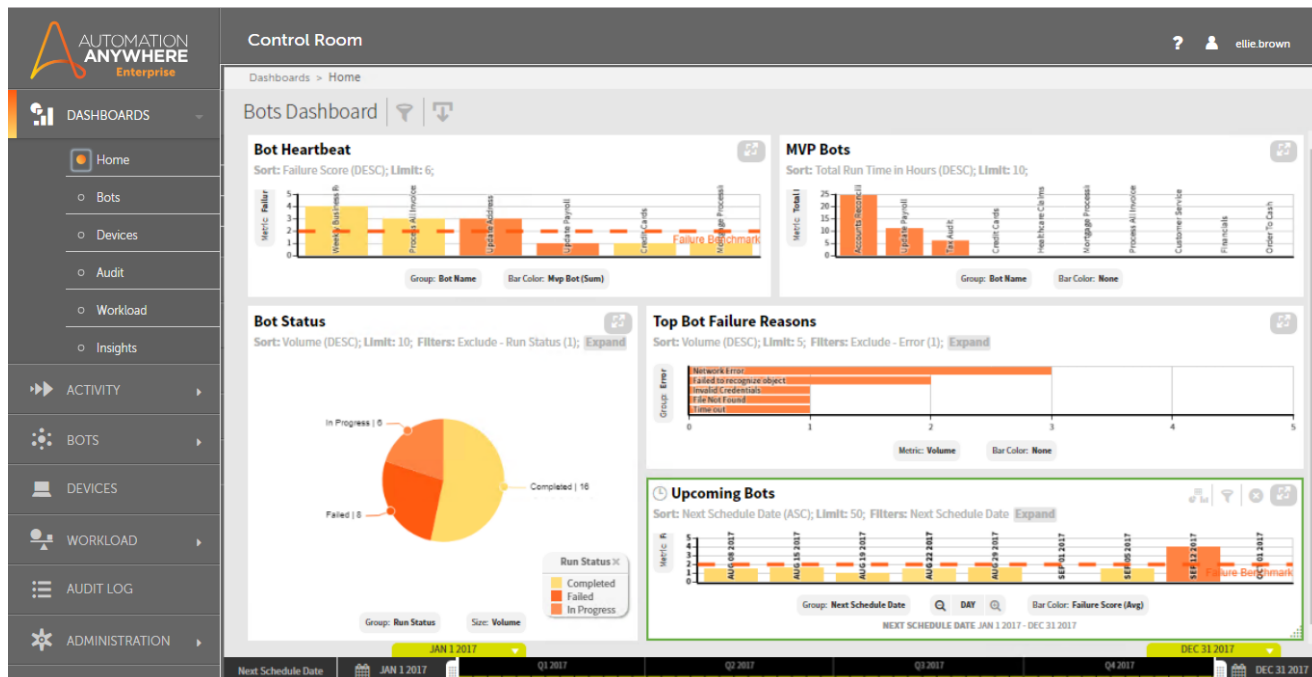
Figure 5: Control Room v.11 Dashboard

5.1.8 Advance Schedule and Run from Control Room

- AAE 11 LTS enables quick bot run from multiple places within the Control Room thus, enhancing usability.
- Explicit permissions to provide granular control over who can manage schedules.
- The Centralized Scheduler has been improved as well to include a 'Repeat' option for cases where the bot run must be triggered at regular intervals.
- The Schedules can also be activated/deactivated in bulk to facilitate system upgrades and pre-planned downtimes.

(Zendesk # 47468,23294,42854,53154,65582,67065)

For more information: click here

Figure 6: Advanced Scheduler option in AAE 11 LTS

5.1.9 Run + Schedule privileges

A new permission 'Run + Schedule' has been introduced at folder level for Control Room repository.

- When creating roles, a user can explicitly grant **Run** or **Schedule** or **Run + Schedule** permission on specific folders to allow users to run or schedule a bot from these folders only.
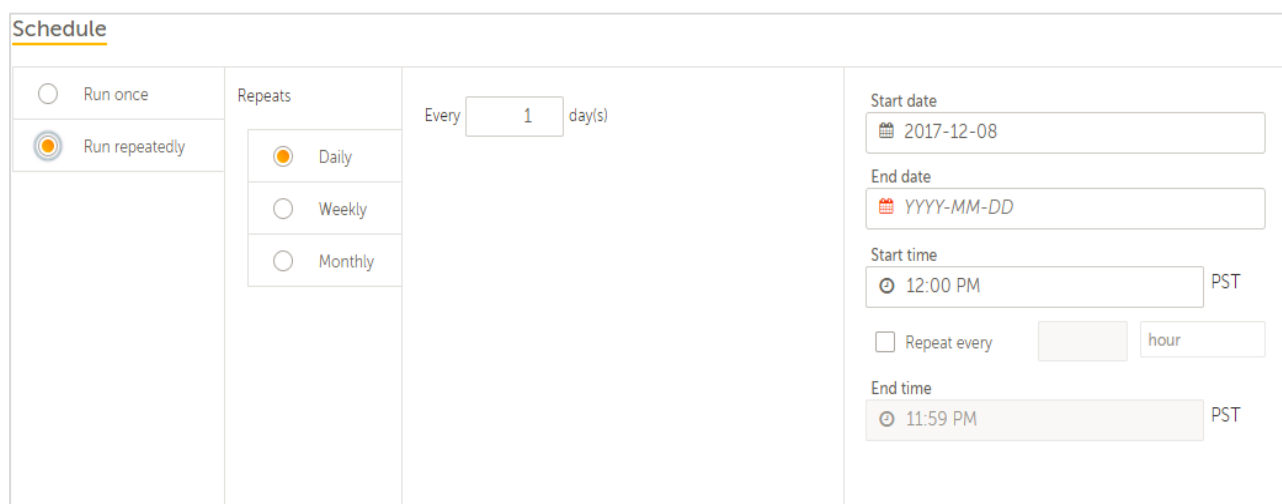- This feature enables users to provide granular control on bots which can be run or scheduled by the user from Control Room.

NOTE: The **Run + Schedule** folder permission substitutes the earlier behaviour of allowing user to run or schedule a bot if (s)he has a **Download** permission on a folder to which the bot belongs.

5.1.10 Run or Schedule Master Bot with missing dependency

A Master Bot can now be run or scheduled from Control Room even if one or more of its dependencies are found missing. This ensures that Master Bot can still be executed on Bot Runners where the missing dependency may not be executed under an IF condition or the dependent file is found on the local machine at run-time.

5.1.11 Role based access to Play/Pause automation

The Play/Pause actions on a running automation is now controlled via specific permission. A user having view activity permission cannot play/pause the running automation however a user having manage activity permission can play/pause the running automation.

5.1.12 Role based access to Bot Runner Devices

In Devices page of Control Room, user can see only those Bot Runner devices which are tagged to user's role(s). Also, at the time of creating or updating roles in the system, authorized users with "View and manage roles" will allocate the devices only from the list of devices which are tagged to such users' role(s). This ensures that if a user is not authorized to access some Bot Runner devices, s/he will not be able to authorize other users to access such devices.

Note - 11.x "Devices" are same as 10.x "Clients".

5.1.13 Improved Audit

With AAE 11 LTS, not only all the actions (creating user, deploying bot and more) are thoroughly audited, but the changes done in the Control Room (e.g. updating user details, settings, schedules and more) are tabled out to get the exact details that have been modified. This ensures complete compliance with the Audit policies.

So also, users can choose the time-frame for which Audit details are to be displayed and exported (to csv) for granular use. *(Zendesk # 47471, 45599, 51910, 46596, 47930)*

For more information: [click here](#)

Figure 7: Audit entry with extensive details

5.1.14 Password Policy for non-AD Users

AAE 11 LTS introduces a configurable password policy for non-AD users wherein Control Room Administrators can enforce password compliance parameters such as minimum and maximum password length and password mix (alphabets, numbers, capital letters, special characters).

To avoid brute force login attack, Admins can also make use of the Account Lock-out feature by specifying the maximum number of consecutive unsuccessful login attempts after which a user's account gets disabled. *(Zendesk # 42341, 49378, 70435)*

For more information: click here

5.1.15 API to synchronize AD credentials with CV

With more and more corporate policies asking for password rotation, AAE's Credential vault can automatically be synched with the new password set by the user in the Active Directory (AD) via REST APIs. These APIs can also be made use by 3rd party Credential Vaults (e.g. CyberArk) to add/update the Bot's auto-login password. *(Zendesk # 57453, 61786)*

For more information: click here

5.1.16 New permissions for API usage

The usage of APIs is now controlled by role permissions.

5.1.17 Separate permission for View, Manage and Install Licenses

The Control Room license management is now made more granular and controlled via separate permissions.

- A '**View License'** permission allows user to view license details from the License page.
- A '**Manage user device license'** permission allows user to allocate/deallocate/release license
- A '**Install license'** permission allows user to install a new Control Room license

5.1.18 Create/Rename Folders in Control Room

A Control Room Admin can now create or rename folders in Control Room Repository. This helps the user in organizing and managing the folder structure in the Repository and avoids dependency on the Bot Creator to upload at-least one task to create a folder in Control Room Repository. User can manage the folder permissions for each role instead of first granting every role a 'My Task' folder permission and then later changing to specific folder when it gets created via Bot Creator.

5.1.19 Copy Roles

When creating roles which are slightly different from each other, it makes sense to have a master Role template and spin roles from that. The 'Copy Roles' option in the Control Room facilitates this with a single click.

5.1.20 Description of Control Room users

Control Room users can now be tagged with their corresponding identifiers in external systems. At the time of creation of Users in Control Room, an optional "Description" field is available. Authorized users can use it to tag any type of associated business information with the Control Room user entity.

5.1.21 Differentiated display of deleted users

If a Control Room user has left the organization or is no longer working on the project, his/her username is preceded with "(inactive)" in Control Room UI, upon account deletion in Control Room. This helps in communicating the real-time status of any given Control Room user. If any corrective action needs to be taken regarding any Control Room data created/modified/owned by such *inactive* user, other Control Room users may contact the Admin, instead of unsuccessfully connecting with such *inactive* user.

5.1.22 Changed behaviour of permissions

Unlike in 10.x, a user with 'View and Manage ALL scheduled activity' and 'View and Manage ALL scheduled activity from my folders' cannot schedule bots to run. To schedule bots, 'Schedule my bots to run' privilege should be granted.

5.1.23 Force Unlock multiple files

A user with 'Force Unlock' privileges can now unlock multiple files which are checked out by some user when version control is enabled.

5.1.24 Delete multiple files

A user with 'Manage Bot' privileges can now delete multiple files which are redundant when version control is disabled.

5.1.25 Integrated Installer

AAE 11 LTS Control Room installer packages in AAE's powerful Analytics Engine, out of the box Operation Analytics feature available at no additional cost. Separate license needed for Business Analytics where users can start tagging bots and variables for real-time RPA Analytics.

For more details, refer the 'AAE 11 LTS - Installation Guide'.

5.1.26 Silent Installation of Control Room

The silent installation of Control Room is possible by means of a PowerShell script.

5.1.27 Support for latest Operating Systems and SQL Versions

- AAE 11 LTS now supports Microsoft SQL Server 2016.
- AAE 11 LTS Client is now supported on Windows 10.

5.1.28 Additional Enhancements

1. It is now possible to reuse the deleted schedule names. (Zendesk # 60592, 64426, 47639)
2. Users can choose to provide a description to the Roles. (Zendesk # 45520)
3. Email notification will be sent to the Users when their accounts in AAE are deleted. (Zendesk # 38438)
4. Active Directory Users have the option to logoff from the Control Room. (Zendesk # 42315)
5. Users can edit their AAE account details in Control Room. (Zendesk # 44256, 45914)
6. An 'Auto-login' column is introduced in the Users landing page which helps to isolate users having auto-login enabled or not.
7. The Control Room repository now shows a 'Client Last Modified' column which helps to identify the date on which the file was last modified on the Client machine before it was uploaded to the Control Room.
8. The Help menu in Control Room now shows product build number in addition to the version number.

5.2   Security

5.2.1   Single Sign-On using SAML 2.0

- To meet the security and compliance of Enterprise organization, Control Room now supports a third (3rd) authentication mechanism Single Sign-On (built using SAML 2.0) apart from the Windows authentication and Database authentication types.
- Enterprise customers can leverage their IDP Server to authenticate any user attempting to login to Control Room using Single Sign-On option.

5.2.2   Kerberos Authentication Support

With AAE 11 LTS Active Directory Based deployment, the AAE users can be authenticated with the Industry Standard Kerberos Authentication Protocol.

Key Features & Business Benefits:

- Robust security as user credentials are never sent over the wire.
- Faster authentication based on the unique Kerberos ticket system.
- Cryptographic protection for authorization data carried in Kerberos tickets.

  For more information: click here

5.3   Bug Fixes

ZENDESK TICKETS#	DESCRIPTION
52940	Directory server unable to handle exception during Client login for AD Authentication
49379	Control Room allowed unidentified user to view/edit Admin tasks. Therefore, trespassing user information without credential mapping led to unauthorized access.

ZENDESK TICKETS#	DESCRIPTION
55124	When a user tried to deploy tasks with multiple dependencies from Control Room, the user received an error, "Object reference not set to an instance of the object."
51736	As a user attempted to install Control Room 10.3.0 on a server that had 10.3.5 setup, a message was displayed indicating that an "earlier version" of AAE was already installed.
41987	While installing Control Room 10 LTS (10.3.0) the installer pre-requisites screen displayed .Net Extensibility 4.5 to be already installed, although it was not.

6 Client

6.1 New Features and Enhancements

6.1.1 AISense driven Automation

With automations over virtual environments, Citrix, VDIs, VMs gaining market strength, AAE 11 LTS brings in AISense to automate applications running within virtual windows. AISense enables object type of automation for applications exposed as images, thus hugely widening the scope of RPA.

Key Features & Business Benefits:

- Cognitive powered automatic object creation of controls within the application window image.
- Smart linking between form fields and labels ensures position agnostic automation.
- Bulk extract and bulk data entry for rapid bot execution.

For more information: click here
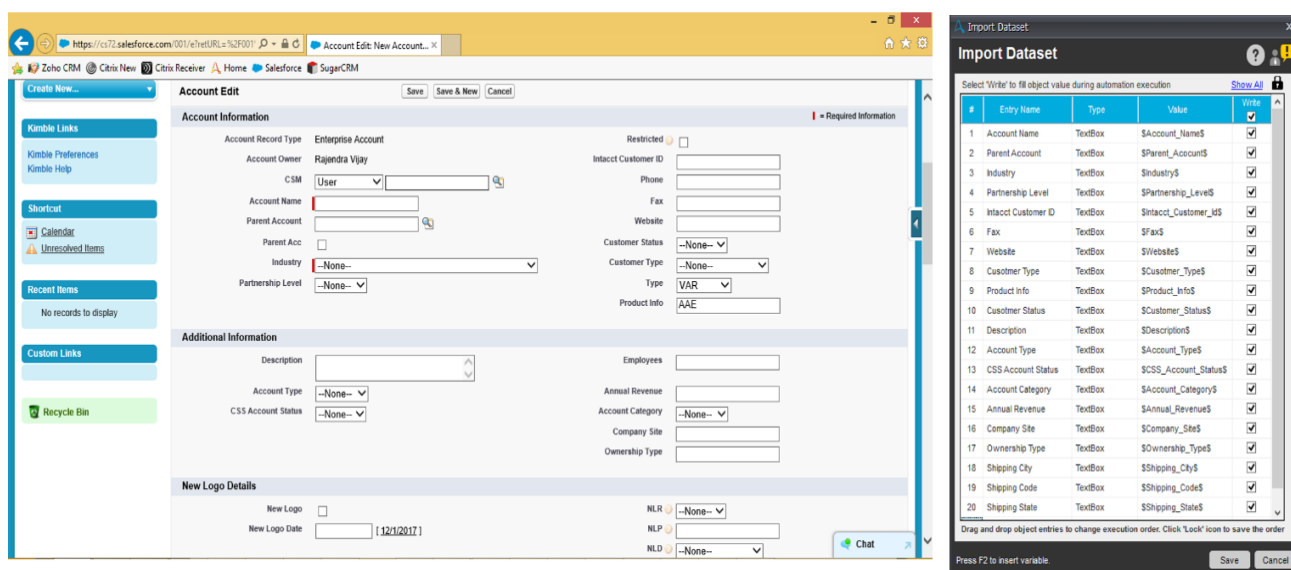
Figure 8: Bulk data entry with AISense

6.1.2 AES 256-Bit Obfuscation for Bots

RPA Data security has been made even more robust and Enterprise-Grade with the AES 256-bit obfuscation of bots (as opposed to the 3DES algorithm used in the earlier versions). *(Zendesk # 47891)*

Key Features & Business Benefits:

- Complements AAE's Credential Vault for Total RPA Data Security; in Rest and in Transit.
- AES 256-bit obfuscation of all AAE artifacts; TaskBots, MetaBots, Reports, Workflows.
- Up to 75% faster obfuscation; reduced bot saving time.

  IMPORANT: With AAE 11 LTS, the Bots when saved, will be obfuscated with AES 256-bit obfuscation. Therefore, bots saved in AAE 11 LTS cannot be opened/played in earlier versions.

6.1.3 Integrated Workbench for TaskBot- MetaBot

With AAE 11 LTS Client, there is no need to install a separate MetaBot Designer, as the MetaBot creator capability has been brought into a unified Editor aptly named Workbench.

(Zendesk # 39855, 40454, 47886, 47885, 46720, 63041, 46985, 47475, 59519, 54396, 58920)

Key Features & Business Benefits:

- One stop Editor to create TaskBots and MetaBots.
- Almost all commands and features (e.g. debugging support) of TaskBots are now made available to MetaBots.
- Open more than one Logics simultaneously
- Debugging support for MetaBot Logics too
- Copy variables across TaskBots-MetaBots
- Use one logic into another Logic of the same MetaBot
- Support for all type of variables in MetaBot Logics
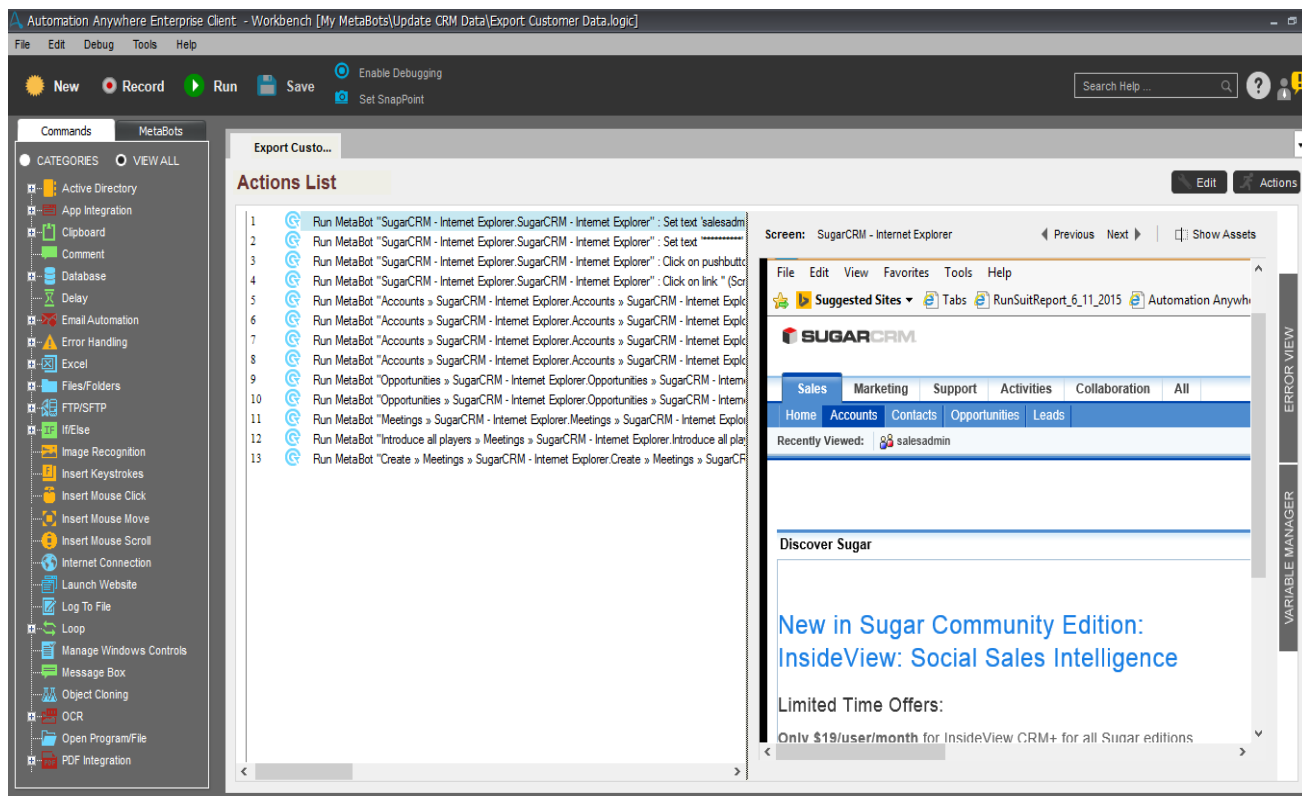
For more information: click here

Figure 9: Integrated TaskBot- MetaBot Workbench

6.1.4 Disaster Recovery support for Bot-Runners

Disaster Recovery (DR) support is introduced at the Bot Runners level also, in addition to already existing support for Control Room DR. In the event of disaster at primary deployment site, DR site Control Room and Bot Runners can be started, and all the automation schedules will seamlessly run on the DR site Bot Runners, without any need for configurations. Also, any data that is created on the DR site is automatically available on production site too when the operations are resumed from primary site.

6.1.5 Quick Command Replication between Bots

When commands are copied from one bot to another, AAE 11 LTS Workbench enables the user to copy the variables (used in those commands) as well. Thus, avoiding manual creation of variables in the new task and validating for missing variables; Bot creation made quicker. *(Zendesk # 47872)*

6.1.6 Enhanced Image Recognition

Image Recognition engine is revamped to deliver enhanced accuracy and change resilience. New image recognition method provides reliable image-based automation even when there are changes in Bot Runner's screen resolution, application browser zoom level or scaling. It also accurately identifies the desired image element when multiple

occurrences of the same image are present in the application screen. This is available for all image-based automation within TaskBots and MetaBots

6.1.7   Support for Edge browser

Windows 10 users can automate their business processes using Edge browser, with Object Cloning and Smart Recorder. This is done using Automation Anywhere Edge browser plug-in which can be installed using AAE Client installer, AAE Client UI or through command line.

NOTE: Edge browser automation is not yet available for **Silverlight and Flex** applications and MetaBot based automations.

6.1.8   Windows Server 2016 certification

AAE Client is now certified for automations using Windows Server 2016 operating system, for Datacenter" edition. With a single install of AAE Client on this OS, multiple users can create and run automations in their respective profiles.

6.1.9   Microsoft logo certification

AAE Client is now **Microsoft logo certified** for Windows 8.x and 10 OS's. This accreditation helps organization meet their governance and compliance requirements. This also enables easy sharing of AAE Client software within the organization, by uploading to customers' internal software store.

6.1.10 Support for Japanese language

More commands (such as Email Automation, zip/unzip Files/folders) of AAE Client have been enhanced to support Japanese language and Regional Settings.

6.1.11 Folder support to store MetaBots

MetaBots can now be organized inside a folder structure for easier navigation and management. This enables users to store similar MetaBots (e.g. from a department) in a common folder and then manage the access at the folder level instead of managing access at individual files level. When Version Control is enabled, users can also upload all the MetaBots of a folder, in a single attempt. For backward compatibility, all the old permissions assigned at MetaBot file level will be retained.

6.1.12 Auto-naming and filters for objects in MetaBots

For MetaBot screens, all the unidentified UI elements are given system generated names, based on their type (i.e. Text box, static text). This helps in uniquely identifying such objects at the time of creation of automation using those, without any need to configure the objects e.g. assign a unique name.

Two new filter types are also introduced to Textbox and Static text type objects. This enables user to quickly configure specific UI elements for any data entry (textbox) or data extraction (static text), wherever needed.

6.1.13 Enhanced reliability of OCR automation

In MetaBot, when performing an OCR based automation, system first tries to locate the given UI element using OCR. If system is not able to find the UI element using OCR due to any problem, it automatically tries to find the same object using image-based search. This enhances the automation reliability wherever OCR based automation is used.

6.1.14 MetaBot Logics and Parameters description

Automation Experts can see the description of Logic and all its variables, at the time of passing parameters from TaskBots to Logics. This acts as a platform for MetaBot users to communicate with TaskBot users with respect to acceptable values of parameters, best practices etc. For example, TaskBot users would know that a given variable expects input as a numeral or as a specific date format.

6.1.15 Upload Bot Dependency

When uploading a bot from AAE Client to Control Room, the Upload window now displays all the dependencies of the bot even if there is circular dependency. This ensures that dependency information is captured, and the selected dependencies are uploaded whenever the bot gets uploaded. Also, a bot can be deployed from Control Room even if there is a circular dependency.

6.1.16 Support for Command Line login

AAE Client Users can now login to Control Room using command line arguments. This is especially helpful in the event of machine reboot (for VM's) wherein a physical user is not present to login AAE Client to Control Room. In such case, customers can write a script to call the command line to login AAE Client to Control Room.

6.1.17 New automation commands in MetaBot Logics

"Insert Keystrokes", "Insert Mouse Click" and "Insert Mouse Move" commands are now available in MetaBot Logics also. These commands will help in creating keystrokes and mouse actions based automations through MetaBots.

Note that these commands were already available for automation through TaskBots.

6.1.18 Linking Bot to Queue Category

Queue category is a data template that specifies a work item structure (i.e. list of attributes and their data types). Every queue created in the Control Room is associated with a queue category. Hence all work items in a queue will have the same set of attributes specified in that queue category. If you want to use your bot for a WLM automation ("Run bot with queue"), it should be linked to a queue category from the Workbench. Once a bot is linked to a queue category, it can be used for a WLM automation with any queue created in the Control Room with that queue category.

6.1.19 Enable Debug Logging

Enabling debug logging for Bot Creators / Runners has been made even more easier by provision of an option in the User Interface. Also, when debug logging is enabled, and the log files are getting filled up, the users are intimated of the same on the status bar of AAE Client.

6.1.20 Additional Enhancements

1. AAE 11 LTS Client will not put the version number in the Installation path. *(Zendesk: # 42640,45915,48202)*
2. AAE 11 LTS Client is supported* on Windows 10. *(Zendesk: #45591,47248,49897,59786)*
3. Appropriate warning message provided when using local variables for 'Run Task' command. *(Zendesk: # 54465)*
4. MetaBot logic commands can call another MetaBot logic. *(Zendesk: # 47884,58921)*
5. MetaBots are updated instantaneously when their embedded logics are updated. *(Zendesk: # 47451)*

*With certain limitations, viz. Microsoft Edge Automation and triggers on Windows 10 Apps are not supported.

6.2   Security

6.2.1   Single Sign-On using SAML 2.0

- The authentication mechanism of AAE Client user to login to Control Room has been made more secure through the support for Single Sign-on using SAML 2.0.
- Upon Login with SSO option, AAE Client users are redirected to the IDP Server URL to provide the IDP credentials and on successful validation, the user can login Control Room.

6.2.2   Password Policy Enforcement

For any change in Password policy by Control Room Admin, the AAE Client user is forced to change his password from Control Room if the old password does not meet the current password requirements.

6.2.3   Restriction of passing credential variable from TaskBot to MetaBot

Credential variables are not allowed to be exchanged between TaskBots and MetaBots. This ensures there are no unintended usage of credential variables. If needed, credential variables can be independently accessed from centralized Credential Vault, from TaskBots or from MetaBot Logics.

6.3   Bug Fixes

ZENDESK TICKETS#	DESCRIPTION
68022	Email Automation command not erroring out for incorrect attachment save path.
48299	App Integration command dlls not getting registered
46810	PDF Command: Value of radio button in PDF Form Fields returns null/blank
49854	AAE Client Installation: Unable to customize installation folder
48737	Send Mail command failed to attach file from a network drive intermittently
43432	Email Automation: Attachment does not get saved if the filename has special characters
44174, 59714	Email subject variable removes blank
43432	When using the Email automation command, the attachments were not getting saved when they contained special characters.

6.4   Deprecated

- In AAE Client, the Define Tab (pointing to Process InVision) has been removed, but customers can keep using Process InVision as a standalone product as is.
- The Login to My App application from AAE Client has been deprecated.
- Migration of Schedules created in Windows from older versions (9.x or earlier) to Automation Scheduler has been deprecated.

7 Known Behavior

7.1 Control Room

1. Installer does not support installing a Certificate Authority Certificate (trust anchor) unless a secure database connection is selected. If you wish the Control Room to connect to other services securely via TLS, such as LDAPS and secure SMTP you must manually import your CA certificate into the CR after the Windows installer but prior to completion of web-based configuration.

2. The installer does not verify the port number corresponding to its SQL Server named instance in Database Configuration during installation. Ensure you provide a port number that corresponds with the appropriate SQL Server named instance.

3. When the Automation Anywhere Control Room Caching services is restarted, the Automation Anywhere Control Room Service should also be restarted.

4. When Automation Anywhere Control Room Services are restarted (Or) when Control Room is installed for the first time, it will take time (~5 minutes) for the Control Room UI to be shown in the browser.

5. When migrating from 10.x to 11.x; if the bot having the same name is present in 11.x repository, the same bot will not be migrated from 10.x.

6. Packages exported via User Interface in Bot Lifecycle Management cannot be used by APIs (and vice-versa).

7. The number of Bot runners in Device Pool may not be reflected correctly, if a device is removed from the pool.

8. There could be instances of multiple audit entries (for create locker, create queue scenarios).

9. It is critical that communication between the Control Room servers is sufficiently protected as it contains security sensitive information that is not encrypted. All network hosts, apart from Control Room servers, should be blocked from accessing the cluster communication ports listed in the Architecture and Implementation Guide.

10. Deployment may take longer than expected for a new Workload Management Device Pool when the Control Room is configured for Active Directory integration.

11. When configuring the LDAP(S) server for Active Directory integration it is necessary to specify a domain controller that is a Global Catalog server. The LDAP server connectivity test during web-based configuration only validates that the server is an LDAP server, it does not validate whether the server is a GC or not. If a non-GC LDAP server is specified searches for users will not return any results.

12. Filtering and Sorting is available on select few columns of Control Room tables and not on all columns.

7.2 Bot Insight

1. After migration from AAE 10 LTS to AAE 11 LTS, Dashboards that were marked as bookmarks don't show up in the bookmarks section of Bot Insight. Users will need to bookmark their favourite Dashboards manually.

2. Sometimes the KPI widget does not show data specifically in the Internet Explorer browser. To make this work, go to Internet options > Advanced tab and click on Reset Internet Explorer settings.

7.3 Client

1. While uninstalling AAE 11 LTS Client, user may come across the 'File in Use' page that displays random numbers instead of showing the open Automation Anywhere applications in use. User may ignore this as the product will be correctly uninstalled.
2. In certain operating systems having stringent security policies, while uninstalling AAE 11 LTS Client, the "Automation.CredentialProvider.dll" (in the System32 folder) does not get removed by the uninstaller. In such cases, the dll must be manually deleted or by using a batch script.
3. If the AAE 11 LTS Client remains offline (disconnected from Control Room) for more than 8 hours; the user must re-login to the AAE 11 LTS Client to renew the user session. This is in line with Industry Standard policies on token expiry.
4. Flex and Silverlight Automation is not supported in Windows 10 and MetaBots.
5. In certain scenarios, the Java plugin installation state may not be correctly reflected, even when Java plugin is installed.
6. Autologin in logoff case for Windows Server 2016 is inconsistent. We recommend use of 'Run bot runner session on Control Room' (RDP based deployment).
7. Object cloning is not supported for Oracle Forms.
8. Firefox browser is not supported in MetaBots.
9. For MetaBot recording, to record any web application, the application must be opened in Internet Explorer 8 and above in document mode.
10. Microsoft Edge automation is not supported in MetaBots.