
# AUTOMATION ANYWHERE ENTERPRISE

## THROUGH THE LENS OF FISMA

COALFIRE

North America | Europe
877.224.8077 | info@coalfire.com | Coalfire.com

# TABLE OF CONTENTS

# INTRODUCTION

Automation Anywhere Enterprise (AAE), the solution provided by Automation Anywhere, offers Federal Agencies and government entities the ability to automate complex workflows within their IT systems to drive efficiency, standardization, and cost reductions. For these Federal Agencies, AAE is architected to meet security control requirements for the Federal Information Security Management Act (FISMA) when deployed in an on-premise IT system.

The intent of this white paper is to provide information to IT professionals implementing AAE within a FISMA-authorized on-premise IT system to ensure that AAE adheres to the control requirements and overall security posture. This white paper assumes that IT professionals will integrate AAE with an already existing FISMA-compliant environment and that supporting controls such as centralized authentication (e.g., Active Directory (AD), centralized log management, analysis and reporting capabilities through a Security Information and Event Management (SIEM), and network partitioning and network access control through virtual local area networks (VLANs) and firewalls) are in place and may be integrated with AAE where appropriate.

For FISMA, IT professionals must develop and maintain a System Security Plan (SSP) that addresses the implementation for each selected control. This white paper outlines AAE's ability to support the implementation of applicable security controls, enabling IT professionals to update an IT system's SSP to address the secure deployment and use of AAE. AAE's features and core capabilities were compared with FISMA Moderate selected controls from NIST SP 800-53 rev. 4 and analyzed for impacting or supporting control requirements.

This white paper only addresses control requirements that were relevant to the deployment, configuration, and maintenance of AAE, with other control requirements being omitted as these will be addressed by underlying IT infrastructure. Lastly, control requirements were not independently tested by Coalfire. The opinions in this white paper represent Coalfire's judgement of documented AAE features and controls from interviews with key Automation Anywhere personnel, product demonstrations, and published information sources supplied by Automation Anywhere.

# AUTOMATION ANYWHERE ENTERPRISE

AAE is a robotic process automation (RPA) platform that enables customers to increase productivity and lower operating costs. When integrated with a customer's enterprise environment, AAE can automate business processes with configurable software called "bots". Bots are application agnostic and can interact with any system or application the same way that human users do. With AAE, customers can harness the power of a digital workforce that is agile and scales on-demand based on business need.

## SUMMARY OF CORE FUNCTIONALITY

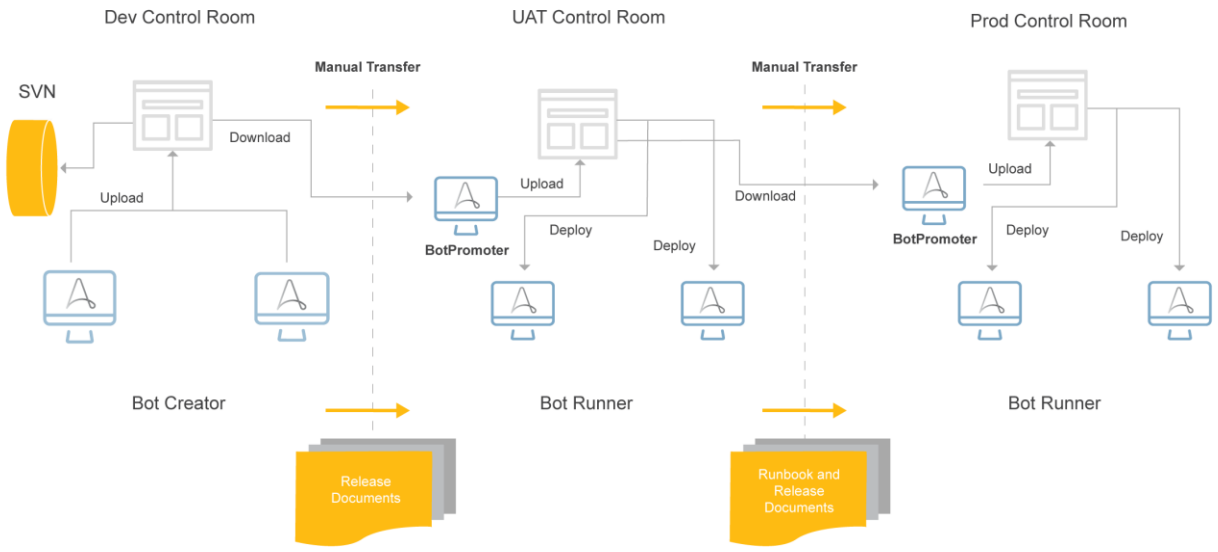


Figure 1 - Automation Anywhere Enterprise (AAE) Deployment Architecture

### Control Room

Control Room (CR) is a web-based central interface that provides customers with the ability to monitor and manage all bots in a customer's environment. CR capabilities include:

- Automation Deployment
- Access Control and Collaboration
- Digital Workforce Management

CR is a customer's single point of access and control for bot deployment and execution. All Bot Creators and Bot Runners must be synchronized with CR for bots to be uploaded to CR from Bot Creators and deployed to Bot Runners. Bots may be deployed to Bot Runners manually or through automated scheduling for execution, supporting both attended and unattended automations. CR also maintains bot integrity through built-in version control features.

Customers can manage access to CR, Bot Creators, and Bot Runners through a management interface in CR. Pre-defined roles and permission sets that follow separation of duties and least privilege principles are available for customers to provision based on proper authorization. Customers also have the option to integrate their existing identity and access management solution to provide a centralized mechanism for controlling access to their overall production environment.

Overall AAE system health, audit records, and other Key Performance Indicators (KPIs) can be viewed through customizable dashboards in CR. Customers can receive real-time heartbeat and telemetry information of AAE and their bots. Customers also have the capability to export audit records in CSV format for ingestion into their existing SIEM solution.

### Bot Creator and Bot Runner

Bot Creator is a software application used for the development of bots. Customers can build two types of bots: TaskBots and MetaBots. TaskBots are used to automate rule-based business processes that use

structured data. Depending on the type of business process, TaskBots can be built for object-based, image-based, or coordinate-based automation. MetaBots are multi-use automation building blocks that can be leveraged across many TaskBots. Bot Runner is a software application used for executing bots deployed from a customer's CR. Bot Creators and Bot Runners are required to authenticate with a customer's CR.

### IQ Bot

IQ Bots are cognitive bots that use machine learning to understand unstructured and semi-structured data from images (i.e., business documents in the form of images, PDFs, visual media). IQ Bot can learn how to extract the right information to apply to specific business processes based on how customers perform these tasks daily.

### Bot Insight

Bot Insight is an analytics platform integrated with CR. Customers can use Bot Insight to tag any data variable or attribute in a TaskBot or MetaBot for analysis in near-real-time. Bot Insight includes dashboards based on advanced algorithms specific to each bot.

## ARCHITECTURE

### Core System Components

CR runs on a Jetty webserver running Windows 2012 R2 and uses an integrated Microsoft SQL Server 2012 database. An additional PostgreSQL database is used for metadata analytics. CR generates logs for all automation actions, which can be accessed through CR Audit Logs. CR may also optionally be connected with an Apache Subversion (SVN) server. Information communicated between CR and other modules is done with secure protocols (TLS 1.2, HTTPS, WSS). Bots are deployed only from CR; depending on the scale on which AAE is operating, this can occur locally from a desktop or from virtual or cloud-based infrastructure.

Bot Creators are Windows-based development systems used to author and tailor automations. Bot Creators run on Windows and must authenticate against an active CR. Bot Runners also operate on Windows and are deployed on individual machines, either physical or virtual.

BotFarm utilizes cloud platforms such as Amazon Web Services (AWS) public cloud or internal virtual infrastructure (e.g. Citrix, VMware) to automatically provision Bot Runners based on scheduled workloads. This is an optional feature that supports dynamic scale up and scale down of the digital workforce.

### Supported Application Integrations

Bot Runners must authorize against AD, via credentials from the centralized Credential Vault (CV), and then again against an available CR. AAE uses FIPS 140-2-validated cryptographic modules to encrypt the credentials stored at-rest in CV with AES-256 and uses FIPS 140-2-compliant algorithms to encrypt the credentials in-transit when transmitted over HTTPS with TLS 1.2.

By default, AAE produces and captures logs with native Windows tools. Should a more complex solution be required, AAE can integrate with Splunk as a centralized log repository and management tool. Splunk's enterprise-grade Universal Forwarders monitor logs and forward them to the Splunk Indexing Server in real-time. These Universal Forwarders are designed to be compatible with most operating systems and networking environments, including those utilized by AAE.

### Minimum Hardware and Software Requirements

| | BOT RUNNER | BOT CREATOR | CONTROL ROOM | SQL SERVER | POSTGRESQL SERVER |
|---|---|---|---|---|---|
| **OPERATING SYSTEM** | Windows 7 SP1 | Windows 7 SP1 | Windows Server 2012 | Windows Server 2008 R2 | Windows Server 2008 R2 |
| **PROCESSOR** | Intel Core i5 2.6 GHz | Intel Core i5 2.6 GHz | 8 core Intel Xeon Processor | 4 core Intel Xeon Processor | 2 core Intel Xeon Processor |
| **RAM** | 8 GB | 8 GB | 16 GB | 8 GB | 4 GB |
| **STORAGE** | 32 GB | 32 GB | 500 GB | 500 GB | 10 GB |
| **OTHER** | .NET Framework 4.6 (Windows 8.1 and Windows Server 2012 R2: 4.6.1) | .NET Framework 4.6 (Windows 8.1 and Windows Server 2012 R2: 4.6.1) | .NET Framework 4.6 (Windows 8.1 and Windows Server 2012 R2: 4.6.1) | SQL Server 2012 or later | PostgreSQL 9.5 |

# FISMA COMPLIANCE WITH AUTOMATION ANYWHERE ENTERPRISE

## OVERVIEW

Automation Anywhere has implemented select FISMA Moderate security controls in AAE. The following tables provide AAE's implementation description of select FISMA Moderate security controls from NIST SP 800-53 rev. 4. Customers can leverage this information to properly implement AAE within their existing FISMA-authorized solution in accordance with FISMA requirements and security best practices. Each table will have the following information:

### Control ID

The control ID is a unique identifier of a control such as 'AC-2 (1)' or 'SA-8'. Customers can use the control ID to correlate the information provided in this white paper to their SSP.

### Control Name

The control name is the name of the control according to NIST SP 800-53 rev. 4. Customers can use the control name to gain a high-level understanding of what the intent/purpose of the control is.

### Implementation Description

The implementation description is a brief description of how AAE supports a customer's ability to implement a control. Customers can use this information to document the security controls natively provided by AAE or AAE integration capabilities in the implementation description in their SSP for the IT system where AAE is deployed.

### Supports/Impacts

**Support:** Customers who deploy AAE within their environment can leverage native AAE security controls or integration capabilities to implement a control.

**Impact:** Customers who deploy AAE within their existing FISMA-authorized environment will meet the control requirements by proper integration with existing control capabilities (processes, procedures, configurations, etc.).

## ACCESS CONTROL

| CONTROL ID | CONTROL NAME | IMPLEMENTATION DESCRIPTION |
|---|---|---|
| AC-2 (1) | Account Management \| Automated System Account Management | AAE provides automated mechanisms for customers to support the management of AAE accounts. Additionally, AAE supports integration with various identity and access management solutions. |
| AC-2 (2) | Account Management \| Removal of Temporary/Emergency Accounts | AAE uses role-based access control (RBAC) to restrict access to AAE system components. Customers can define unique roles and permission sets used for accounts that a customer defines as temporary and/or emergency. |
| AC-3 | Access Enforcement | AAE uses RBAC to restrict access to AAE system components. Customers will have to provide proper authorizations for users to gain logical access to AAE and provision AAE access accordingly. |
| AC-4 | Information Flow Enforcement | AAE system components are configured to only provide essential capabilities for AAE to perform its intended functions. All information flows between AAE system components have been authorized by Automation Anywhere through its Software Development Lifecycle (SDLC). Customers will have to authorize all information flows between AAE and other system components. Additional information flows can be created by the customer based on customer authorization. |
| AC-5 | Separation of Duties | AAE uses RBAC to restrict access to AAE system components. Customers will have to follow separation of duties principles when administering role-based access to AAE. |
| AC-6 | Least Privilege | AAE uses RBAC to restrict access to AAE system components. Customers will have to follow privilege principles when administering role-based access to AAE. |
| AC-6 (2) | Least Privilege \| Non-Privileged Access for Nonsecurity Functions | Customers can leverage pre-defined privileged and non-privileged role definitions and use AAE RBAC to restrict access to AAE system components. |
| AC-6 (5) | Least Privilege \| Privileged Accounts | AAE uses RBAC to restrict access to AAE system components. Customers will have to define which personnel are authorized to use privileged AAE accounts. |
| AC-6 (9) | Least Privilege \| Auditing Use of Privileged Functions | AAE audits privileged functions and allows customers to export those audit records in CSV format for upload to a SIEM tool. |
| AC-6 (10) | Least Privilege \| Prohibit Non-Privileged Users from Executing Privileged Functions | AAE uses RBAC to restrict access to AAE system components. Roles are assigned specific permissions that allow user accounts with assigned roles to only execute permissions assigned to those specific roles. |
| AC-7 | Unsuccessful Logon Attempts | AAE provides the capability for the customer to configure the enforcing account lockout after unsuccessful logon attempts. AAE can enforce a configurable limit of consecutive invalid logon attempts by a user during a configurable time-period. User accounts that exceed this limit are locked and will require unlocking by the customer administrator. |

| CONTROL ID | CONTROL NAME | IMPLEMENTATION DESCRIPTION |
|---|---|---|
| AC-11 (1) | Session Lock \| Pattern-Hiding Displays | AAE displays a publicly consumable login page whenever a user has been idle long enough to trigger its appearance. |
| AC-12 | Session Termination | AAE automatically terminates user sessions after twenty (20) minutes of inactivity. |

## AUDIT AND ACCOUNTABILITY

| CONTROL ID | CONTROL NAME | IMPLEMENTATION DESCRIPTION |
|---|---|---|
| AU-2 | Audit Events | AAE generates audit records for the following types of auditable events:<br>• Successful and unsuccessful account logon events<br>• Account management events<br>• Object access<br>• Policy change<br>• Privilege functions<br>• Process tracking<br>• System events<br>• For Web applications:<br>– All administrator activity<br>– Authentication checks<br>– Authorization checks<br>– Data deletions<br>– Data access<br>– Data changes<br>– Permission changes |
| AU-2 (3) | Audit Events \| Reviews and Updates | Automation Anywhere provides customers with a list of auditable events that AAE produces for auditing and review. |
| AU-3 | Content of Audit Records | AAE audit records contain the following information:<br>• What type of event occurred<br>• When the event occurred<br>• Where the event occurred<br>• Source of the event<br>• Outcome of the event<br>• Identity of any individuals or subjects associated with the event |
| AU-9 | Protection of Audit Information | AAE uses RBAC to restrict access to AAE system components. |
| AU-9 (2) | Protection of Audit Information \| Audit Backup on Separate Physical Systems/Components | AAE database backups for audit information can be configured to support a customer's database backup strategy such as weekly full backups. Customers will have to ensure backups are stored on a separate physical system. |
| AU-12 | Audit Generation | AAE generates audit records for the following types of auditable events:<br>• Successful and unsuccessful account logon events<br>• Account management events<br>• Object access<br>• Policy change |

| CONTROL ID | CONTROL NAME | IMPLEMENTATION DESCRIPTION |
|---|---|---|
| | | • Privilege functions<br>• Process tracking<br>• System events<br>• For Web applications:<br>– All administrator activity<br>– Authentication checks<br>– Authorization checks<br>– Data deletions<br>– Data access<br>– Data changes<br>– Permission changes |

## CONFIGURATION MANAGEMENT

| CONTROL ID | CONTROL NAME | IMPLEMENTATION DESCRIPTION |
|---|---|---|
| CM-6 | Configuration Settings | AAE was designed to only require specific ports and protocols to function as intended. Customers can refer to AAE 11.0 Security Architecture when defining and documenting configuration settings for their IT system. |
| CM-7 | Least Functionality | AAE requires specific ports and protocols enabled to function as intended. Customers can refer to AAE 11.0 Security Architecture when defining and documenting least functionality requirements. |

## CONTINGENCY PLANNING

| CONTROL ID | CONTROL NAME | IMPLEMENTATION DESCRIPTION |
|---|---|---|
| CP-9 | Information System Backup | AAE database backups can be configured to support a customer's database backup strategy such as incremental and full backups at various intervals. |
| CP-10 | Information System Recovery and Reconstitution | Customers will have to consider recovery and reconstitution strategies for AAE as it relates to the customer's information system offering. Automation Anywhere provides disaster recovery and high-availability architecture documentation in AAE 11x Control Room User Guide. |
| CP-10 (2) | Information System Recovery and Reconstitution \| Transaction Recovery | AAE utilizes database technology that supports the ability for customers to implement transaction recovery. |

## IDENTIFICATION AND AUTHENTICATION

| CONTROL ID | CONTROL NAME | IMPLEMENTATION DESCRIPTION |
|---|---|---|
| IA-2 | Identification and Authentication (Organizational Users) | AAE supports the capability for an organization's information system to uniquely identify and authenticate organizational users and process acting on behalf of organizational users. Actions undertaken by AAE can be uniquely authenticated and identified to support after-the-fact reviews. |

| CONTROL ID | CONTROL NAME | IMPLEMENTATION DESCRIPTION |
|---|---|---|
| IA-2 (3) | Identification and Authentication \| Local Access to Privileged Accounts | AAE may be integrated with a customer's multi-factor authentication solution with SAML 2.0 to provide AAE with local access to privileged accounts. |
| IA-3 | Device Identification and Authentication | All instances of AAE are capable of being uniquely identified and authenticated before a connection to the customer's information system is established. |
| IA-4 (4) | Identifier Management \| Identify User Status | Customers can configure the identifiers used with AAE to uniquely identify individuals based internally-defined characteristics, criteria, and status. |
| IA-5 | Authenticator Management | AAE supports customers' authenticator-management efforts through AD integration or SAML 2.0. Customers can configure and deploy authenticators in ways that are compliant with all relevant FISMA standards, and said authenticators may be used in AAE. |
| IA-5 (1) | Authenticator Management \| Password-Based Authentication | AAE allows for customers to configure minimum password complexity settings (upper-case letters, lower-case letters, numbers, and special characters) within the application. Customers can also leverage AD to configure minimum password complexity settings and additional password complexity requirements such as:<br>• Minimum number of changed characters when a new password is created<br>• Storage and transmission encryption<br>• Minimum and maximum lifetime restrictions<br>• Minimum number of generations before password reuse is permitted<br>• Forcing an immediate change of a temporary password to a permanent password |
| IA-5 (4) | Authenticator Management \| Automated Support for Password Strength Determination | AAE can be integrated with a customer's AD to automatically determine if password authenticators are sufficiently strong to satisfy customer requirements. |
| IA-5 (6) | Authenticator Management \| Protection of Authenticators | Authenticators for AAE may be stored and transmitted in the same manner as other sensitive authenticators in the customer's environment. Authenticators may be securely stored in the AAE CV and authenticators may be securely transmitted with TLS. |
| IA-5 (7) | Authenticator Management \| No Embedded Unencrypted Static Authenticators | AAE CV provides customers the ability to securely store authenticators at-rest and have bots access credentials for use based on customer-defined workflows rather than embedding unencrypted static authenticators within bot workflows. |
| IA-6 | Authenticator Feedback | AAE is configured so that as credentials are entered into the application, the credentials are obscured. The characters of the password are represented with dots. |
| IA-8 | Identification and Authentication (Non-Organizational Users) | AAE allows customers to create unique usernames for their users based on customer-defined policy. |

| CONTROL ID | CONTROL NAME | IMPLEMENTATION DESCRIPTION |
|---|---|---|
| IA-2 | Identification and Authentication (Organizational Users) | AAE supports the capability for an organization's information system to uniquely identify and authenticate organizational users and processes acting on behalf of organizational users. Actions undertaken by AAE can be uniquely authenticated and identified to support after-the-fact reviews. |
| IA-2 (3) | Identification and Authentication \| Local Access to Privileged Accounts | AAE may be integrated with a customer's multi-factor authentication solution to provide AAE with local access to privileged accounts. |

## SYSTEM AND SERVICES ACQUISITION

| CONTROL ID | CONTROL NAME | IMPLEMENTATION DESCRIPTION |
|---|---|---|
| SA-8 | Security Engineering Principles | Automation Anywhere incorporates security engineering principles into all stages of the development of the AAE application. Security engineering principles are considered and applied to AAE during:<br>• Specification<br>• Design<br>• Development<br>• Implementation<br>• Modification |
| SA-11 | Developer Security Testing and Evaluation | Automation Anywhere carries out thorough testing on the AAE software and any changes made thereto prior to release, including but not limited to the following:<br>• Creating and implementing a security assessment plan<br>• Performing unit, integration, system, and regression testing<br>• Producing evidence that a security assessment has been carried out<br>• Implementing a verifiable flaw remediation program<br>• Correcting any flaws identified during the testing process |

## SYSTEM AND COMMUNICATIONS PROTECTION

| CONTROL ID | CONTROL NAME | IMPLEMENTATION DESCRIPTION |
|---|---|---|
| SC-2 | Application Partitioning | AAE has been designed to fully segregate user functionality from application management functionality. Users must access the application with different credentials to access different functionality within AAE. Any individual attempting to access management functionality in AAE must log in with credentials for that specific role. Users without such authorization are unable to access management functionality with only user credentials.<br><br>AAE also supports additional application partitioning safeguards with Stealth Mode and disabling user interfaces such as keyboard and mouse. Stealth Mode disables an AAE users's capability to view |

| CONTROL ID | CONTROL NAME | IMPLEMENTATION DESCRIPTION |
|---|---|---|
| | | application screens or program windows where AAE is performing automation activities. Disabling of user interfaces such as keyboard and mouse prevents users from executing unintended or unwarranted actions while AAE is performing automation activities. Together, Stealth Mode and disabling of keyboard and mouse provides AAE customers with additional controls to protect the confidentiality and integrity of customer information. |
| SC-8 | Transmission Confidentiality and Integrity | All transmissions within AAE are protected with TLS 1.2. |
| SC-18 | Mobile Code | Automation Anywhere maintains a definition of which mobile code technologies are permissible in which contexts. For the acceptable mobile code technologies, Automation Anywhere establishes usage restrictions and implementation guidelines. Any use of mobile code technologies in AAE or its development process is actively authorized, monitored, and controlled by Automation Anywhere.<br><br>Automation Anywhere also considers AAE bots to be mobile code. Adherence to best-practice SDLC processes such as the use of separate development, testing, and production environments supports the customer's ability to actively authorize, monitor, and control mobile code technologies. |
| SC-28 | Protection of Information at Rest | AAE produces an RSA key pair for each instance of the application. This key pair is the master key used at boot-up to decrypt an AES 256-bit key used to protect the confidentiality and integrity of sensitive data at-rest. It is the responsibility of the customer to ensure that the key pair is adequately protected and that appropriate processes are in place regarding distribution, storage, and access. |

### SYSTEM AND INFORMATION INTEGRITY

| CONTROL ID | CONTROL NAME | IMPLEMENTATION DESCRIPTION |
|---|---|---|
| SI-2 (2) | Flaw Remediation \| Automated Flaw Remediation Status | Automation Anywhere runs automated scans to detect flaws and vulnerabilities. Nessus scans are run monthly on Automation Anywhere's production environment. Weekly Vericode scans are carried out on a weekly basis on code for AAE to detect vulnerabilities. |
| SI-11 | Error Handling | When an error occurs in AAE, the message displayed to end users is generic and reveals no sensitive information. Only administrators can view detailed error information. |

## CONCLUSION

The AAE solution can be implemented in an existing FISMA-authorized environment in a manner that maintains the existing security posture and compliance assurance. Federal Agency IT professionals can deploy the solution into their environment, knowing the security controls detailed in this white paper support and meet FISMA compliance requirements. The built-in capabilities and mechanisms of AAE ensure that security and compliance requirements are maintained while offering cost-savings and efficiencies.

## ABOUT COALFIRE

Coalfire is the cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for more than 16 years and has offices throughout the United States and Europe. Coalfire.com

WP_AAE FISMA_201809