AUTOMATION ANYWHERE ENTERPRISE 10 SP2

TECHNICAL SPECIFICATIONS DOCUMENT

Document Version	1.0
Date of Publication	28-06-2017
Update(s) to Document Edition	-

Table of Contents

Email: support@automationanywhere.com

1 Introduction

This document contains following technical details for the Automation Anywhere Enterprise 10.5.0 product.

- Deployment
- Protocols
- Ports
- Encryption and credentials
- Sensitive user information

2 System Requirements

The below section contains recommended software and hardware requirements for the Automation Anywhere Enterprise product.

2.1 Control Room

2.1.1 Express and Custom Standalone Installation

2.1.1.1 Software Requirements

Operating Systems	Microsoft Windows 7.0 SP1 (Minimum) Microsoft Windows Server 2012 R2 (Recommended)
Web Server/IIS	Internet Information Services 7.5 onward
.NET Framework	**For Windows 8.1 and Window Server 2012 R2:** Microsoft .NET 4.6.1 **For other** Supported Operating Systems**:** Microsoft .NET 4.6
Data Management System	**For Express:** Microsoft SQL Server 2014 Express Service Pack 1 (SP1)
	For Custom Standalone: Microsoft SQL Server 2012 Express/Standard/Enterprise or higher

2.1.1.2 Hardware Requirements

Processor	x64 Server Based CPU with 8 Cores *Hyper-threading recommended (if applicable)*
RAM	8 GB (Recommended)
Disk Space	100 GB (Depends upon Repository size)

2.1.2 Distributed Installation

Applicable for Custom-Distributed mode of installation

2.1.2.1 Application Server - Software Requirements

Operating System	Microsoft Windows 7.0 SP1 (Minimum) Microsoft Windows Server 2012 R2 (Recommended)
Web Server/IIS	Internet Information Services 7.5 onward
.NET Framework	**For Windows 8.1 and Window Server 2012 R2:** Microsoft .NET 4.6.1 **For other** Supported Operating Systems**:** Microsoft .NET 4.6
Data Management System	Microsoft SQL Server 2012 Express/Standard/Enterprise or higher
Java Framework	JRE 1.6 onward

2.1.2.2 Application Server - Hardware Requirements

Processor	x64 Server Based CPU with Minimum 4 Cores *Hyper-threading recommended (if applicable)*
RAM	8 GB
Disk Space	20 GB (Depends upon repository size)

2.1.2.3 Shared Data Server - Software Requirements

Operating System	Microsoft Windows Server 2012 R2

2.1.2.4 Shared Data Server - Hardware Requirements

Processor	x64 Server Based CPU with Minimum 8 Cores *Hyper-threading recommended (if applicable)*
RAM	8 GB
Disk Space	100 GB (Depends upon repository size)
Shared Drive	-

2.1.3 Supported Operating Systems

Operating System	Edition
Microsoft Windows 10	Pro, Enterprise
Microsoft Windows Server 2012 R2	Standard, Datacenter
Microsoft Windows Server 2012	Standard, Datacenter
Microsoft Windows 8.1	Pro, Enterprise
Microsoft Windows 8	Pro, Enterprise
Microsoft Windows Server 2008 R2	Standard
Microsoft Windows 7 SP1	Professional, Enterprise

2.2 Client

Processor	Intel Core i5 2.6 GHz
RAM	8 GB
Disk Space	32 GB (Depends on repository size)
Operating System	Microsoft Windows 7 SP1 (Minimum) Microsoft Windows 8.1 Pro 64-bit (Recommended)
.NET Framework	Microsoft .NET 4.6

2.3 WebSocket Server

CPU	x64 Server based machine to handle large requests.
Processor	x64 Server Based CPU with Minimum 4 Cores *Hyper-threading recommended (if applicable)*
RAM	16 GB Though the Socket service will consume a MAX 2 GB RAM in normal conditions, it can be increased up to 16 GB. For details refer: https://msdn.microsoft.com/en-us/library/aa366778.aspx#memory_limits
Disk Space	100 GB Though the web-socket service has a small install foot-print, the disk will be required for other applications (including OS files).
Operating System	Microsoft Windows Server 2012 R2
Certificates	PFX files. Details of other certificate types and conversion can be referred from the AAE 10 LTS – Installation Guide. You can also refer https://helpdesk.ssls.com/hc/en-us/articles/204093372-What-are-certificate-formats-and-what-is-the-difference-between-them

3 Architecture Diagram

The following diagram describes Automation Anywhere Enterprise product architecture.

Bot Creator is a Client component which creates bots. Bot Runner runs the bots with/without supervision of Control Room.

In a typical scenario, all the communication between Client and Control Room pass through a Network Firewall and a Load Balancer.

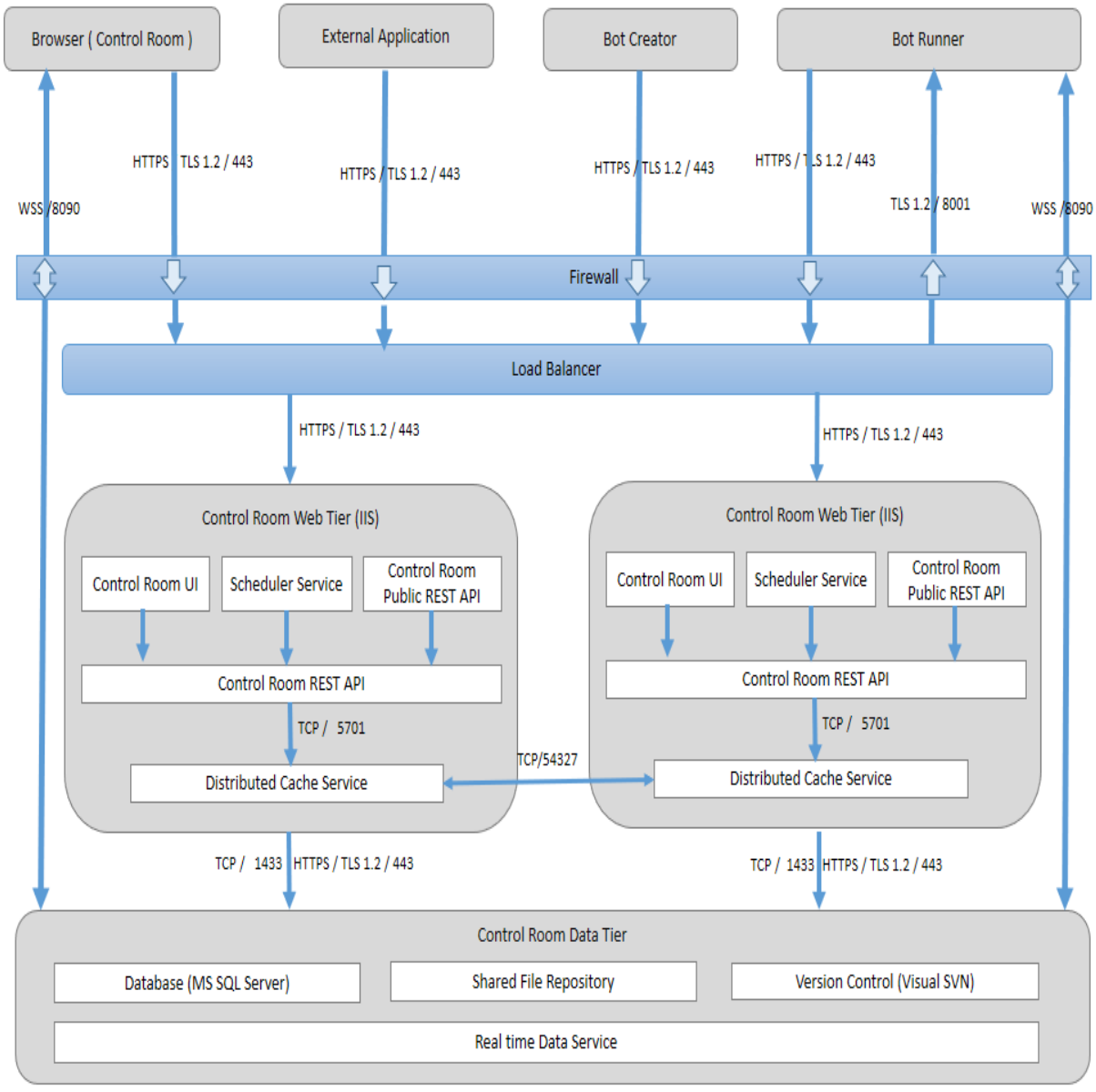

Figure 1

Various secure protocols are used to communicate between different modules of Client and Control Room. Two Application Servers with Data tier are represented in above diagram to describe how load balancing and synchronization take place between servers.

Distributed Cache Service is introduced from Control Room 10.3.0 version. It holds application specific data and shares with REST Service as well as the other instances of Cache Service. Internally it uses Hazelcast Distributed Cache mechanism.

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 listens on WSS protocol. It plays a mediator role between browser where 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.

Version Control System (VCS) and MS SQL Server are external software applications. They may or may not be on the Data tier depending upon the need.

Data tier can be configured for failover cases separately if high availability is concerned. Refer the AAE Control Room 10.5.0 High Availability Configuration Guide for detailed information.

4 Deployment

This section provides high-level deployment environment for the Automation Anywhere Enterprise products.

4.1 Control Room

Control Room supports two different installation modes:

1. Distributed mode
2. Standalone mode

Figure 2 describes high-level deployment of the Automation Anywhere Enterprise Control Room components in case of distributed mode installation.

MS SQL Server and SVN server are not bundled with installer. They are external components as illustrated separately in the diagram.

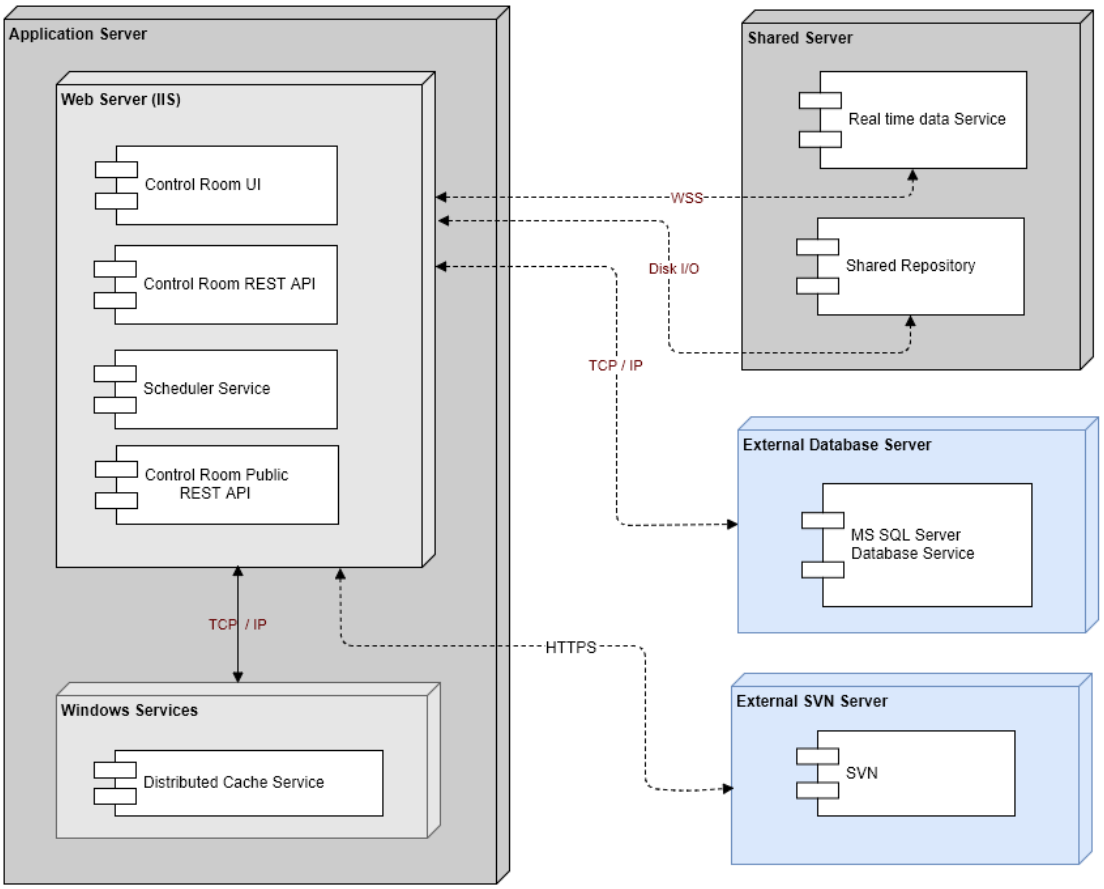

Figure 2. Automation Anywhere Enterprise Control Room 10.5.0 Deployment Diagram Distributed mode Installation

In standalone installation mode, all the components are installed in a single machine. MS SQL Server Express edition is bundled with the installer. SVN Server is an external component as illustrated separately in the diagram.

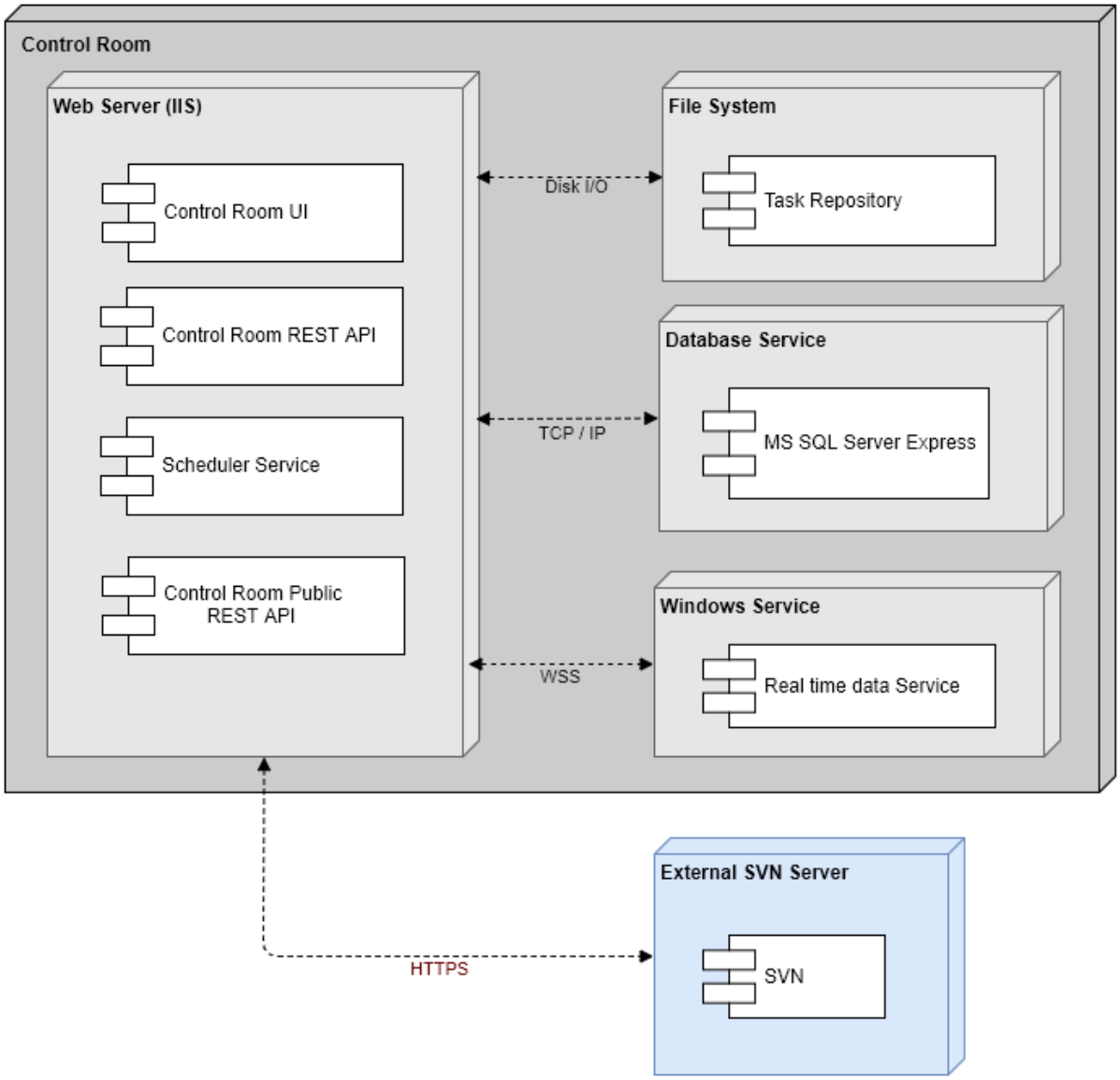

Figure 3. Automation Anywhere Enterprise Control Room 10.5.0 Deployment Diagram Standalone mode Installation

4.2 Client

Figure 4 describes deployment of Enterprise Client Core Components. The illustrated components are installed by Automation Anywhere Enterprise Client setup.

MetaBot plugin is bundled with Automation Anywhere Enterprise Client installer from 10.5.0 version.

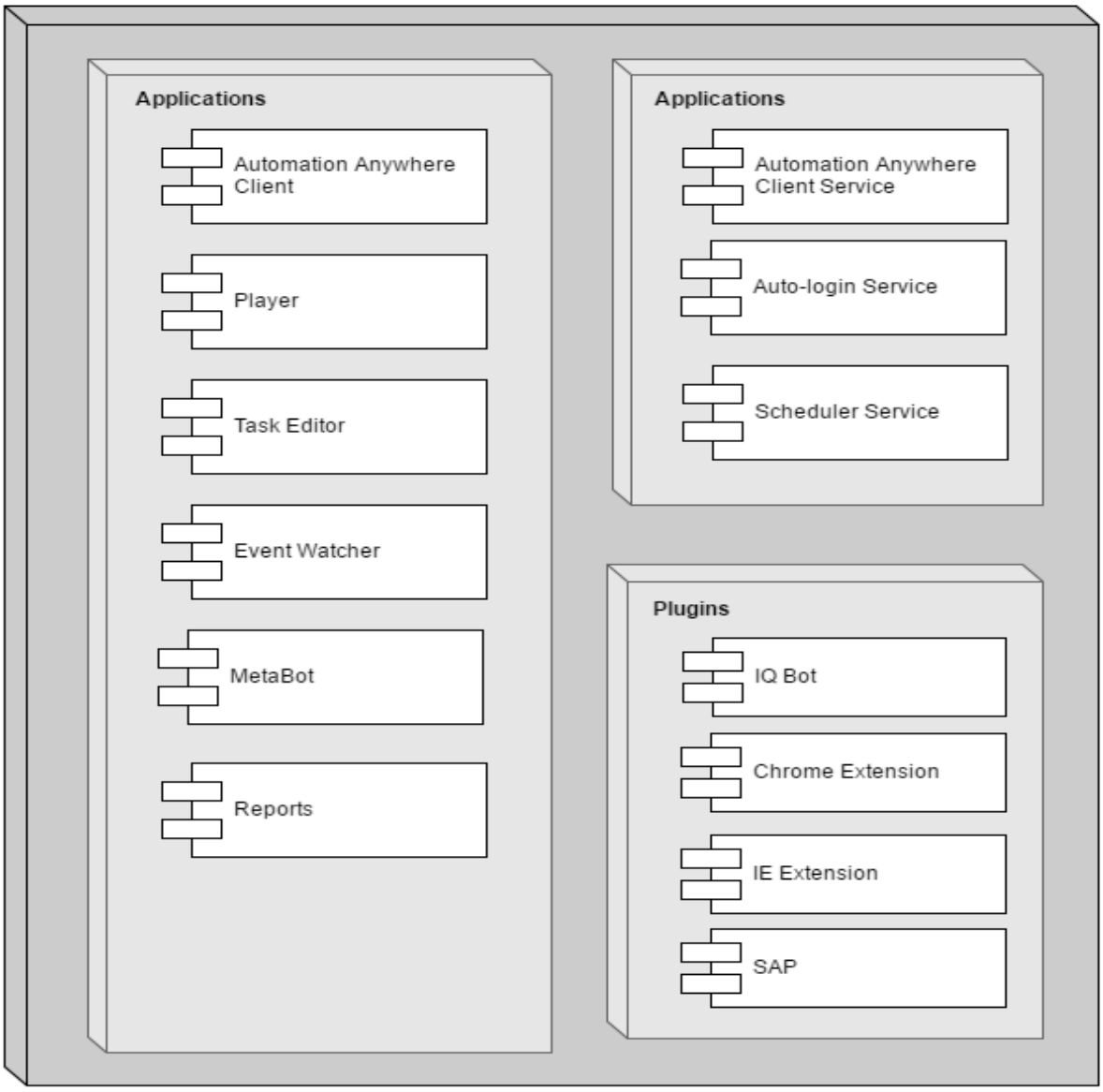

Figure 4. Automation Anywhere Enterprise Client 10.5.0 Deployment Diagram

Automation Anywhere Client provides launch points for various functionalities with a single interface. Primarily it validates a user account on Control Room and gives accessibility to authorized features.

Task Editor allows to create tasks. It produces physical files for task. Player runs tasks which actually do a desired set of automation.

Event Watcher manages easy task execution facilities like hot key assigned to execute a task, various triggers defined to execute a task etc.

Meta Bots enable you to apply robotic process automation across environments. Meta Bots automate repeatable, complex, system-to-system processes using API-level integrations, then share them with Task Bots to get the job done.

Auto-login service is working in background and performs login process automatic on a given system. This applies specifically when Control Room administrator runs a task on a system and that system is logged off or locked state.

IQ Bot helps facilitate end-to-end process automation of both structured and unstructured data, extracting and digitizing key information within, acting on that data, and learning to manage exceptions as it goes. It has a self-directed process management capabilities.

Scheduler Service manages schedules defined at client side.

SAP plugin provides the integration capability to execute SAP BAPI APIs.

IE Extension is an IE browser extension. It acts like an agent between browser and task recorder module and helps in capturing objects with maximum possible information during task record. It also performs pre-defined actions on target objects during task play.

Chrome Extension is a Chrome browser extension. It acts like an agent and performs pre-defined actions on target objects during task play.

5 Protocols

A standard set of regulations and requirements that allow two electronic items to connect to and exchange information with one another.

The following table contains list of the protocols Automation Anywhere Enterprise products utilize to enable various task automation.

Sr. No	Protocol	Deployment
1	SNMP	Client
2	IMAP	Client
3	FTP / SFTP	Client
4	POP3	Client
5	HTTP/HTTPS	Client & Control Room
6	WS / WSS	Client & Control Room
7	TCP/IP	Client & Control Room
8	TLS	Control Room
9	SMTP	Client & Control Room
10	SOAP	Client
11	Named Pipes	Client
12	NTLM / NTLM v2	Control Room

6 Ports

Port is an endpoint of communication in an operating system. Automation Anywhere Enterprise uses below ports for internal and external communications.

Port	Description	Deployment	Used for
110 995	POP3	Client	"Email Automation" command to retrieve emails from mail server.
143 993	IMAP	Client	
21	FTP/SFTP	Client	"FTP/SFTP" command
25 465 587	SMTP	Client	Client: "Send email" command "Error handling" command "Email notification" feature Control Room: Send email when user created, password set/reset, role changed etc.
161	UDP	Client	"SNMP" command
22 23	Terminal Emulator	Client	"Terminal Emulator" command
80	HTTP	Client Control Room	Hosting of Control Room in IIS (Not recommended)
443	HTTPS	Client Control Room	Hosting Control Room in IIS (Recommended)
8001	TCP/IP	Client Control Room	Client Service to receive deploy/run/schedule requests from Control Room.
8090	WS / WSS	Client Control Room	Operation room data and pause/resume/stop actions.
1433	TCP/IP	MS SQL Server	Default port used by MS SQL Server
4530	TCP/IP	Client (AAProxyServer.exe)	It's used to communicate between client to respected plugins via TCP socket for AAE Client, Editor or Player
5701	TCP/IP	Control Room (Distributed Cache Service)	Control Room uses to connect to Cache Service.
54327	TCP/IP	Control Room (Distributed Cache Service)	Uses for distributing cache to other cache service instances.

Figure 5 explains component level communication channels with protocols and ports. Ports and protocols are same for standalone and distributed installations except the Cache service.

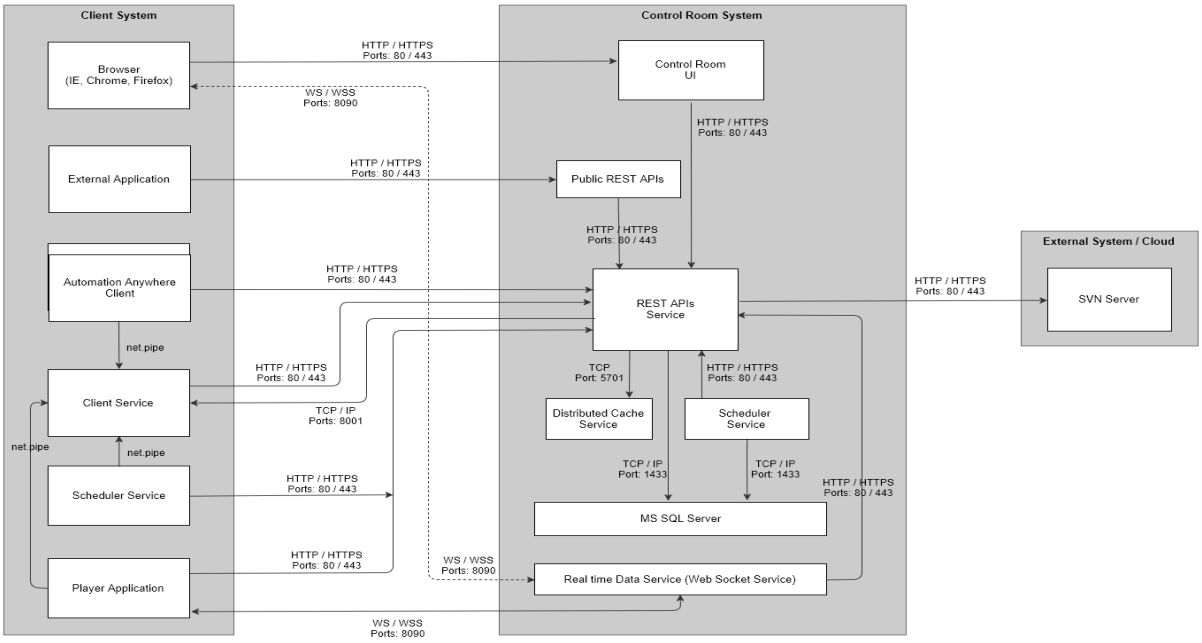

Figure 5

As presented on above figure, REST APIs uses Distributed Cache Service to get shared cached data which are required for specific functionality. It also accesses SVN server for various task versioning activities like check-in/out, get latest, rollback etc.

Scheduler Service makes REST API calls to run a task on specific client machine at specific time. It also uses database (MS SQL Server) to get details about task scheduled for clients.

Real time Data Service makes REST API calls to authenticate coming connection requests. It receives task execution progress updates by Bot Runners and sends that information to all connected browser clients using WSS protocol.

Automation Anywhere Client makes REST calls for user authentication and some repository operations like upload a task, download a task or compare two tasks.

Client Service makes REST calls to validate user session at some regular interval. Control Room deploys and runs a task on a specific client using Client Service. It uses TCP/IP channel.

Scheduler service makes REST call to get machine's credential to do auto-login to system. It also communicates to Client Service to get license and user session related information.

Player makes REST call to get auto-login credentials for logged in client. It also communicates to Client Service to get license and user session related information.

7 Credentials

- Password and other confidential information are encrypted while transferring over the wire. This is implemented using hybrid security using RSA+AES+HMAC (2048 bit key).
- Passwords entered in the application or any other sensitive information are not stored on the client machine, rather it is encrypted using AES (256 bits key length) and RSA (2048 bits key length) and stored into the database using SHA256 algorithm after salting.
- To perform auto-login to system when schedule occurs and machine is locked or logged off, user credentials are fetched from server.
- Passwords are protected in memory using system level Data Protection API (DPAPI), so that it cannot be discovered by memory mapping tools.

8 Sensitive User Information

- To remember a user on a specific machine, last logged in user information is saved on the local disk. However, this information does not contain any password. It is used to do application level auto-login on next application start up.
- Fields data which are used with Encrypt Keystroke & Encrypt Text options in commands are protected using machine level data protection APIs to avoid its direct visibility on the screen.
- To send notification emails and for user registration, control room requires SMTP email credentials. This can be provided during installation. It is optional from Automation Anywhere Enterprise 10.1.0 onwards
- To fulfil the end level automation, whatever information added by automation author at the command level are saved within task file, where same task file level encryption is applied.
- Client sessions are very much secured by JSON based token authentication mechanism. It includes management of session expiration and session renewal policies.
- Task files are obfuscated to protect against direct access of task contents. This includes all the information provided while recording or creating a task.

9 Encryption Algorithms

9.1 AES + RSA Algorithms

Before sending the password to Control Room for authentication, AES and RSA algorithms are used to secure the password entered by the user. These algorithms are used to secure the client sensitive data on Control Room.

9.2 SHA-256 (For hashing)

Control Room user passwords are stored in database after hashed using SHA-256 algorithm.