



Automation Anywhere Enterprise

Auto-Login Best Practices & Troubleshooting Guide

Specifications and Strategies Covered in this document are subject to change

Contents

Auto-Login Best Practices & Troubleshooting Guide	1
Contents	2
Overview	3
1. Best Practices to setup Auto Login Feature	4
1.1 Fully qualified name	4
1.2 Legal disclaimer enabled	4
1.3 One user per machine	4
1.4 Running Services	5
1.5 Application Path on Local Machine	5
2. Best Practices to use Auto Login Feature	6
2.1 Scenario 1: Auto login with Log Off status of BOT runner machine (Most preferred)	6
2.2 Scenario 2: Auto login with lock status of BOT runner machine	6
3. Auto Login Troubleshooting	6
3.1 Diagnosis Utility	6
3.2 Running Diagnosis Utility	7
3.3 Verify Auto-Login Utility	9
3.4 Verify Auto-Login Utility	9
3.5 Running Instance WinLogon.exe	9
3.6 DLLs	10
4. Capability Matrix	10

Overview

Automation Anywhere Enterprise provides the Auto-Login functionality by which a bot can automatically login into a machine, run the scheduled automation task and then restore the machine to its original locked/logged off state once the task is finished.

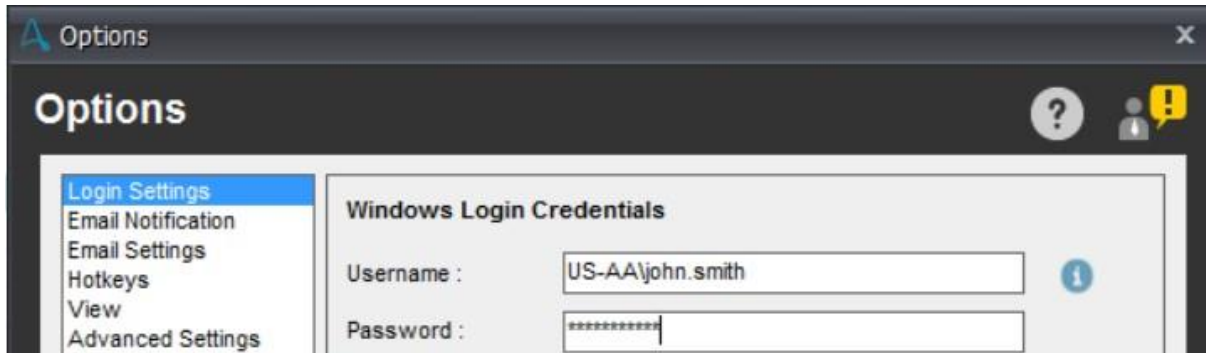
The Auto-Login functionality thus enables unattended Robotic Process Automation; which ensures high Bot-Runner utilization and less idle time.

This document provides information regarding best practices and steps to troubleshoot the Auto-Login feature when it fails to work as expected.

1. Best Practices to setup Auto Login Feature

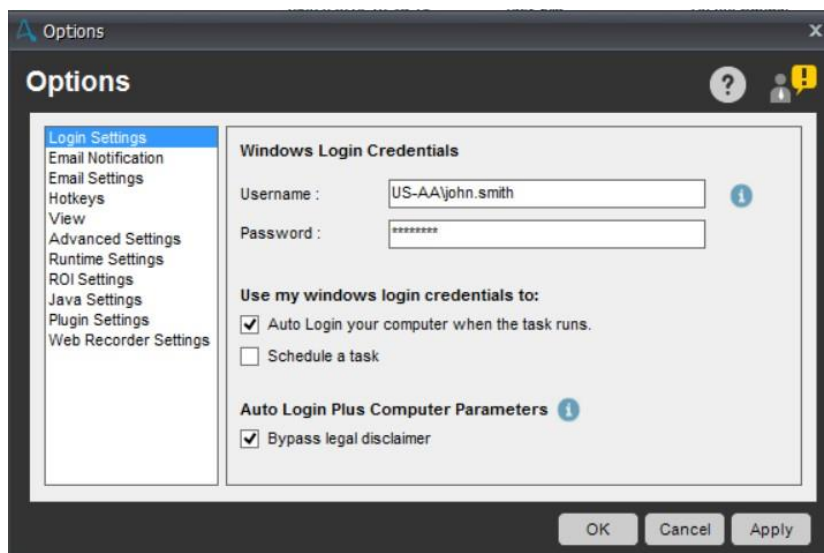
1.1 Fully qualified name

When providing the credentials in the **Login Settings** of **Tools -> Options** of AAE Client, ensure that you provide the fully qualified name (DOMAIN\UserName) in the Username field. For e.g. US-AA\john.smith



1.2 Legal disclaimer enabled

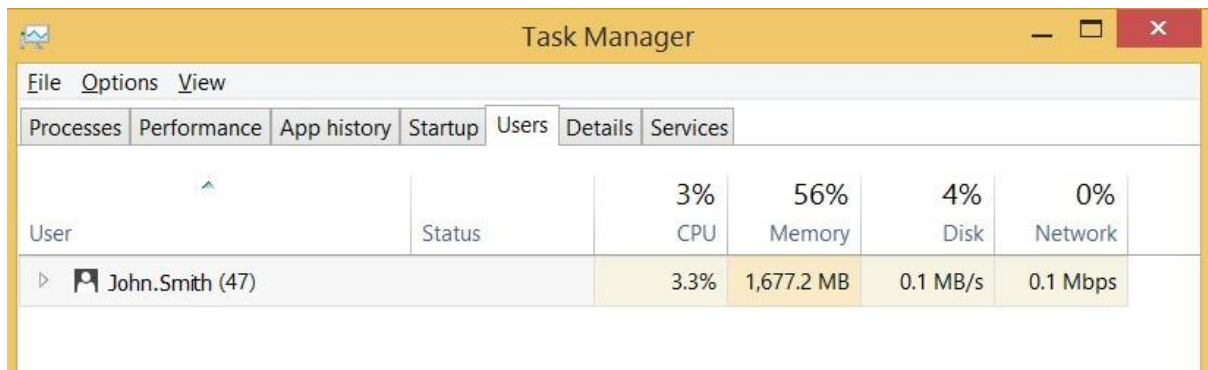
If the Bot-Runner machine shows up a legal disclaimer every time when the user logs in, ensure that the 'Bypass legal disclaimer' is ticked in the Login **Settings** of **Tools -> Options** of AAE Client



1.3 One user per machine

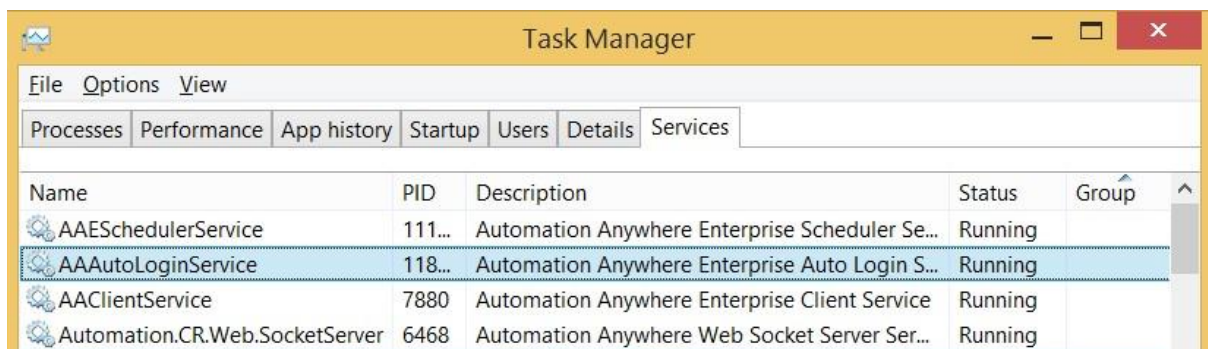
Ensure that the Bot-Runner machine has only one user logged in when the scheduled task is supposed to run.

You can manage the users from the **Task Manager -> Users** tab of the Bot-Runner machine.



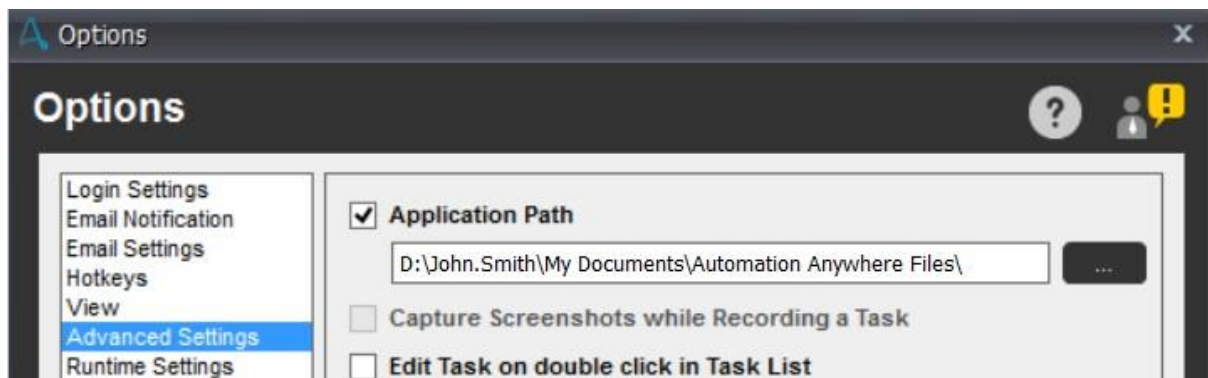
1.4 Running Services

Ensure that **AAESchedulerService** and **AAAAutoLoginService** are running on the Bot-Runner machine. You can check this from the **Task Manager** -> **Services** tab.



1.5 Application Path on Local Machine

Ensure that the AAE application path is on the local machine. AAE application path on network drive or share drive is not recommended. You can verify/change this from the Advanced Setting section of **Tools->Options** in AAE Client.



2. Best Practices to use Auto Login Feature

Automation Anywhere recommends 2 scenarios to use Auto Login feature as described below

2.1 Scenario 1: Auto login with Log Off status of BOT runner machine (Most preferred)

1. Connect to the BOT runner machine from BOT user machine.
2. Configure Auto Login settings as described in '**Best Practices to setup Auto Login Feature**' section.
3. **Log off** the BOT runner machine.
4. Open the control room from BOT user machine and then deploy or schedule a task to the BOT runner machine.

2.2 Scenario 2: Auto login with lock status of BOT runner machine

1. Connect to the BOT runner machine from BOT user machine.
2. Configure Auto Login settings as described in '**Best Practices to setup Auto Login Feature**' section.
3. **Lock** the BOT Runner machine. Please do not disconnect or minimize remote desktop session.
4. Open the control room from BOT user and then deploy or schedule a task to the BOT runner machine.

Note: User needs to perform Step 1 and step 2 only for first time of user of BOT runner machine. BOT user will also require to change a password in Auto login configuration as and when earlier configured password changes.

3. Auto Login Troubleshooting

3.1 Diagnosis Utility

We have built a utility which will identify the prerequisite needed for the Auto Login and will validate if all the needed access and rights are available.

The utility checks for the Auto-Login prerequisites, if they do not exist then corresponding action is performed.

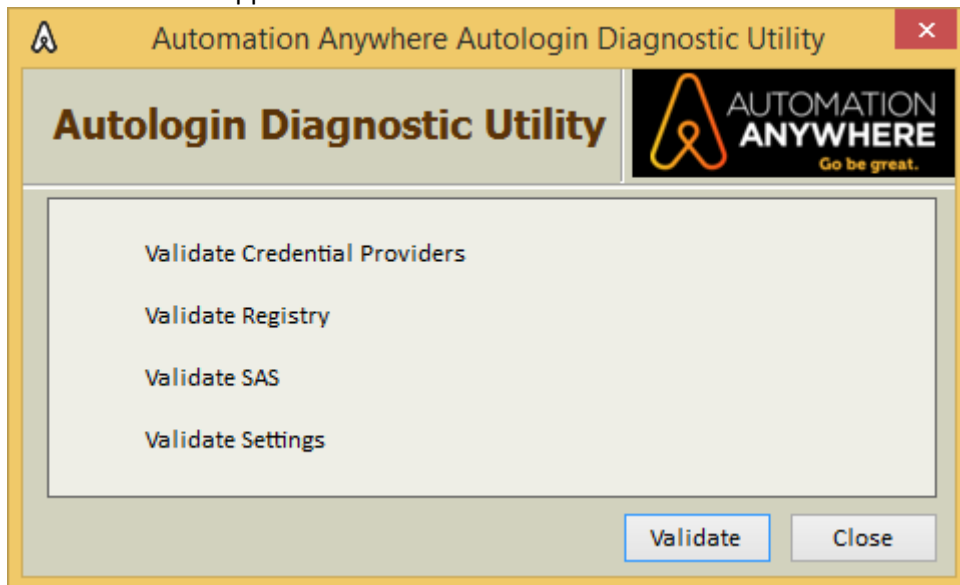
Use below link to download the utility.

http://www.automationanywhere.com/techsupport/Customers/Support/Utility/Autologin_Diagnose_Fix_Utility.zip

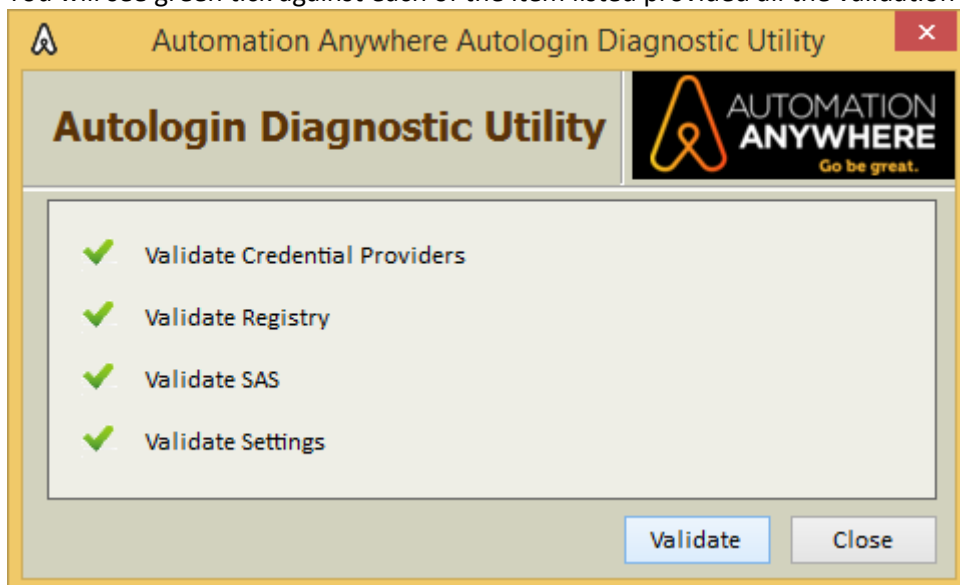
Once downloaded, unzip the utility and copy the files in the client folder at the installation path of AAE. (e.g. C:\Program Files (x86)\Automation Anywhere Enterprise x.x\Client)

3.2 Running Diagnosis Utility

- a. Double click to run the **AutologinDiagnoseUtility.exe**. You might be prompted with “User Access Control” dialog. Click **Yes** to continue.
- b. Below screen will appear with the details.



- c. Click on **Validate** button.
- d. You will see green tick against each of the item listed provided all the validation criterial are satisfied.



e. Following steps are performed by utility under **Validate Credential Providers**.

Sr No	Registry Key	Name	Type	Value
1	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\{75A22DF0-B81D-46ed-B119-CD30507BD614}	(Default)	String Value (REG_SZ)	Automation.CredentialProvider
2	HKEY_CLASSES_ROOT\CLSID\ {75A22DF0-B81D-46ed-B119-CD30507BD614}	(Default)	String Value (REG_SZ)	Automation.CredentialProvider
3	HKEY_CLASSES_ROOT\CLSID\ {75A22DF0-B81D-46ed-B119-CD30507BD614}	(Default)	String Value (REG_SZ)	Automation.CredentialProvider.dll
4	46edB119CD30507BD614} \InprocServer32	ThreadingModel	String Value (REG_SZ)	Apartment

Also ensures that Automation.CredentialProvider.dll is present in the system32 (e.g. C:\Windows\System32); if not, copies it from the installation path (e.g. C:\Program Files (x86)\Automation Anywhere Enterprise x.x\Client) from the appropriate folder (32 or 64 bit) depending on the machine config.

f. Following steps are performed under **Validate Credential Providers**.

Ensures that the Ctrl+Alt+Del registry is present, if not then creates them.

Sr No	Registry Key	Name	Type	Value
1	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\	SoftwareSASGeneration	DWORD (Hexadecimal)	3

g. Following steps are performed under **Validate SAS**.

Ensure that SAS.dll is present in the system32 (e.g. C:\Windows\System32) folder. If not, then copies the same from the product installation folder (e.g. C:\Program Files (x86)\Automation Anywhere Enterprise x.x\Client) from the appropriate folder (32 or 64 bit) depending on the machine config.

h. Following steps are performed under **Validate Settings**.

Ensures that the user has got administrative rights.

Ensures that the Auto-Login service is running, if not then starts it.

3.3 Verify Auto-Login Utility

- Click the below link to download the utility
<http://www.automationanywhere.com/techsupport/Customers/Support/Utility/AutoLoginDebugUtility.zip>
- Unzip the package and save it anywhere on the system.
- Enter the user name with domain and password and then click on Auto-Login button on the utility.
- Once you lock the machine, it should unlock itself immediately.
- If it does, then Auto-Login should work properly.
- If it does not, then the issue is with the Credential Provider dll.
- So, re-register the credential provider dll.
- To do so, navigate to the Client folder (e.g. C:\Program Files (x86)\Automation Anywhere Enterprise x.x\Client).
- Locate the Register.reg in client folder and double click the file to register the Auto-Login registry entries.
- The registry entries will be registered again.
- Restart the computer.

3.4 Verify Auto-Login Utility

Ensure that the **SoftwareSASGGeneration** key is present in the registry with the value as shown:

Sr No	Registry Key	Name	Type	Value
1	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\	SoftwareSASGeneration	DWORD (Hexadecimal)	3

If the above key is not there, create it manually and restart the machine. Ensure that there are no policies set on the system that will delete/modify this registry key.

3.5 Running Instance WinLogon.exe

Ensure that there is only 1 running instance of WinLogon.exe in the Task Manager. If there are more than one, restart the machine.



w3wp.exe	4232	Running	SYSTEM	00	115,152 K	IIS Worker P
wininit.exe	640	Running	SYSTEM	00	456 K	Windows St
winlogon.exe	676	Running	SYSTEM	00	692 K	Windows Lo
WINWORD.EXE	8360	Running	Deven.D...	00	122,876 K	Microsoft W

< >

^ Fewer details End task

3.6 DLLs

Ensure that the following dlls are present in the system32 folder (e.g. C:\Windows\system32). If not, copy them from the installation folder (e.g. C:\Program Files\Automation Anywhere X.X\Client\32Bit OR from 64-Bit; depending on OS) to system32 folder.

- 1) Automation.CredentialProvider.dll
- 2) msvcp100.dll
- 3) msvcp100d.dll
- 4) msvcp110.dll
- 5) msucr100.dll
- 6) msucr100d.dll
- 7) msucr110.dll
- 8) sas.dll

4. Capability Matrix

The following table provides the capability matrix of the Auto Login feature under various OSes and scenarios. Results are based on testing done on AAE 10.1.

OS Scenario	Win 7 (32 Bit)	Win 7 (64 Bit)	Win 8 (32 Bit)	Win 8 (64 Bit)	Win 10 (64 Bit)	Server 2008 (64 Bit)	Server 2012 (64 Bit)	Terminal Server	Citrix (Xen Desktop)
Local Schedule + Lock	Y	Y	Y	Y	Y	Y	Y	Y	Y
Local Schedule + LogOff	Y	Y	Y	Y	Y	Y*	Y*	N	N
Local Schedule + LogOff + Legal Disclaimer	Y	Y	Y	Y	Y	Y*	Y*	N	N
Lock + Deploy	Y	Y	Y	Y	Y	Y	Y	Y	Y
Lock + Disconnect + Deploy	NA	NA	NA	NA	NA	NA	NA	N	N
LogOff + Deploy	Y	Y	Y	Y	Y	Y	Y	N	N
RDP + Lock + Deploy	Y	Y	Y	Y	Y	Y	Y	Y	Y
RDP + Disconnect + Deploy	N	N	N	N	N	N	N	N	N
RDP + Lock + Disconnect + Deploy	N	N	N	N	N	N	N	N	N
RDP + LogOff + Deploy	Y	Y	Y	Y	Y	Y	Y	N	N

OS Scenario	Win 7 (32 Bit)	Win 7 (64 Bit)	Win 8 (32 Bit)	Win 8 (64 Bit)	Win 10 (64 Bit)	Server 2008 (64 Bit)	Server 2012 (64 Bit)	Terminal Server	Citrix (Xen Desktop)
RDP + Local Schedule + Lock	Y	Y	Y	Y	Y	Y	Y	Y	Y
RDP + Local Schedule + Lock + Disconnect	N	N	N	N	N	N	N	N	N
RDP + Local Schedule + Disconnect	N	N	N	N	N	N	N	N	N
RDP + Local Schedule + LogOff	Y*	Y*	Y*	Y*	Y*	Y*	Y*	N	N
VM + RDP + Lock + Deploy	Y	Y	Y	Y	Y	Y	Y	Y	Y
VM + RDP + Lock + Disconnect + Deploy	N	N	N	N	N	N	N	N	N
VM + RDP + Disconnect + Deploy	N	N	N	N	N	N	N	NA	NA
VM + RDP + LogOff + Deploy	Y	Y	Y	Y	Y	Y	Y	NA	NA
VM + Lock + Deploy	Y	Y	Y	Y	Y	Y	Y	NA	NA
VM + LogOff + Deploy	Y	Y	Y	Y	Y	Y	Y	NA	NA
VM + RDP + Local Schedule + Lock	Y	Y	Y	Y	Y	Y	Y	NA	NA
VM + RDP + Local Schedule + LogOff	Y	Y	Y	Y	Y	Y	Y	NA	NA
VM + RDP + Local Schedule + Lock + Disconnect	N	N	N	N	N	N	N	NA	NA
VM + RDP + Local Schedule + Disconnect	N	N	N	N	N	N	N	NA	NA

* - Issues faced inconsistently.

Known Limitations:

- 1) Auto login will not work in LOGOFF mode on cloud VMs (Azure, Amazon, Verizon etc)
- 2) Auto login will not work in LOGOFF mode in Citrix and Terminal Server (Multi-user session systems)
- 3) Auto login will not work in DISCONNECTED RDP systems.