



Robotic Process Automation Software

Login Agent

USER GUIDE

Version: 5.0.29

For more information please contact:

info@blueprism.com | UK: +44 (0) 870 879 3000 | US: +1 888 757 7476

www.blueprism.com

Contents

Introduction	3
Editions of Login Agent	3
Distributable Files	3
Mandatory Security Policies.....	4
Installation	5
Using Login Agent	6
Overview	6
Automation Examples	7
Advanced Installation and Configuration	8
Updating or customising the Login Agent configuration.....	8
Troubleshooting.....	11
Identifying Login Agent Runtime Resources in Control Room	11
Common Issues	11
Enable Logging for Login Agent.....	11
Resource stuck on error message: "Incorrect password or username"	11
Anonymous resourcepc logins are disabled.....	12
Frequently Asked Questions	13

The information contained in this document is the proprietary and confidential information of Blue Prism Limited and should not be disclosed to a third party without the written consent of an authorised Blue Prism representative. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying without the written permission of Blue Prism Limited.

© Blue Prism Limited, 2001 – 2016

®Blue Prism is a registered trademark of Blue Prism Limited

All trademarks are hereby acknowledged and are used to the benefit of their respective owners.

Blue Prism is not responsible for the content of external websites referenced by this document.

Blue Prism Limited, Centrix House, Crow Lane East, Newton-le-Willows, WA12 9UY, United Kingdom
Registered in England: Reg. No. 4260035. Tel: +44 870 879 3000. Web: www.blueprism.com

Introduction

The Login Agent software provides a mechanism for securely logging into a Windows desktop device for the purposes of executing Blue Prism processes.

This document guides the new user through the process of installing the Blue Prism Login Agent software, and provides some guidance on its use.

Editions of Login Agent

The correct version of Login Agent to use will be dependent on the version of Blue Prism that is installed.

- Blue Prism Versions 4.1.25 to 5.0.21
Download a compatible version of Login Agent from the user portal.
At the time of publication the latest compatible version is Login Agent 2.0.0.
- Blue Prism Version 5.0.23
Download a compatible version of Login Agent from the user portal.
At the time of publication the latest compatible version is Login Agent 5.0.23.
- Versions 5.0.24 and above
Login Agent is provided within the Blue Prism installer. Following the install of Blue Prism on a given device, the Login Agent installation executable can be found within the **Installers** in the Blue Prism install location.

	Login Agent 2.0.0 (from Portal)	Login Agent 5.0.23 (from Portal)	Login Agent (Embedded)
Location of installer	Download from User Portal	Download from User Portal	Within install directory of Blue Prism versions 5.0.24+.
Supported Blue Prism versions	4.1.25 – 5.0.21	5.0.23+	Version of Blue Prism that the installer was provided with.
Supported Operating Systems	Windows XP, Windows Vista, Windows 7, Windows 8.1, Windows 10 Includes 32-bit and 64-bit architectures.	Windows XP, Windows Vista, Windows 7, Windows 8.1, Windows 10, Windows Server 2008, Windows Server 2012 Includes 32-bit and 64-bit architectures and R2 editions.	Windows XP, Windows Vista, Windows 7, Windows 8.1, Windows 10, Windows Server 2008, Windows Server 2012 Includes 32-bit and 64-bit architectures and R2 editions.
Prerequisites	An appropriate version of Blue Prism must be installed and configured prior to installing Login Agent. When installing onto a virtual device, the host virtualization technology must support third-party credential providers		
User access	Administrator access is required on the target system		

Distributable Files

There are two installers available for each version of Login Agent:

- For 32-bit operating systems: LoginAgentSetup32.msi or LoginAgent_x86.msi
- For 64-bit operating systems: LoginAgentSetup64.msi or LoginAgent_x64.msi

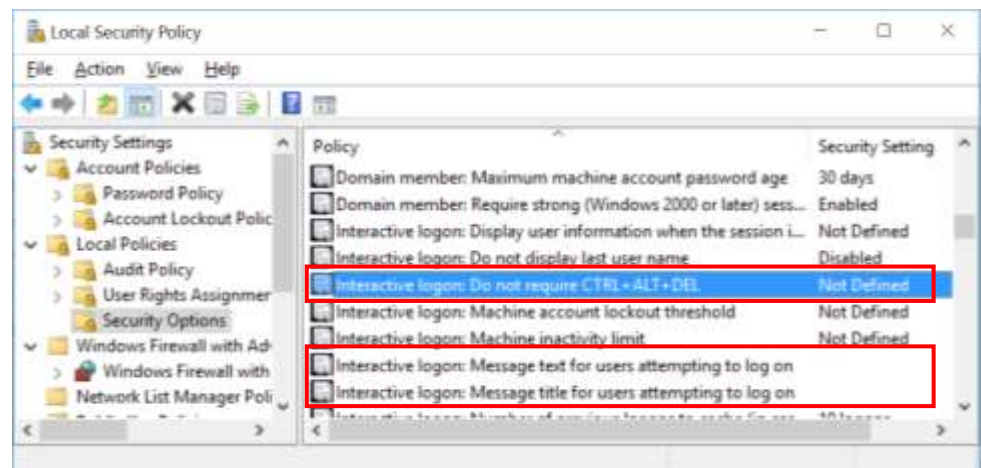
Mandatory Security Policies

In order for Login Agent to be able to function it is essential that the following security policies are be configured on each target device. These are to ensure that when the device is first started the Windows username and password fields are presented without requiring any user input. Explicitly:

- There must not be a requirement to press ctrl + alt + del prior to the user name and password fields being presented.
[Local Security Policy: Interactive Login: *Do not require ctrl + alt + del*: **Enabled**]
- There must not be a requirement to traverse an on-screen message such as a usage acceptance policy as part of the login process.
[Local Security Policy: Interactive Login: *Message title for users attempted to log on*: **Empty**]
[Local Security Policy: Interactive Login: *Message text for users attempted to log on*: **Empty**]
- There must not be a requirement to traverse a lock screen (Windows 8.1 and Windows 10).
[Local Group Policy Editor: *Do not display the lock screen*: **Enabled**]

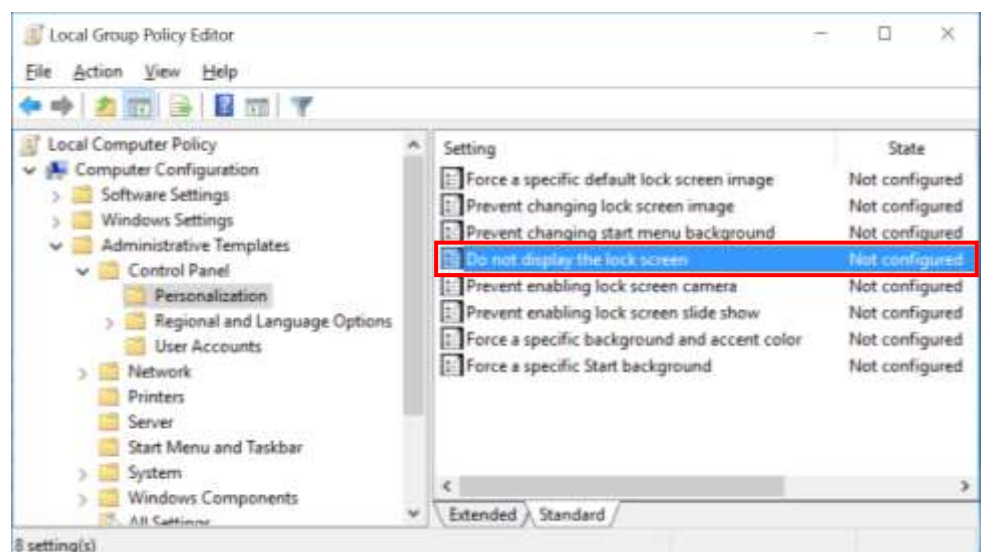
These policies will be automatically set for the local machine when Login Agent is installed, but commonly these settings are overwritten by global settings on the network.

Local Security Policy settings can be found within Local Security Policy, beneath Security Settings -> Local Policies -> Security Options.



Local Group Policy Editor settings can be found within the Local Group Policy Editor beneath Computer Configuration -> Administrative Templates -> Control Panel -> Personalization.

[Windows 8.1 and 10 only]



Where security policies are applied globally, such as by Active Directory Group Policy, these changes will need to be applied centrally to affect all intended target devices.

Installation

The steps below illustrate those required to perform an initial installation of Login Agent.

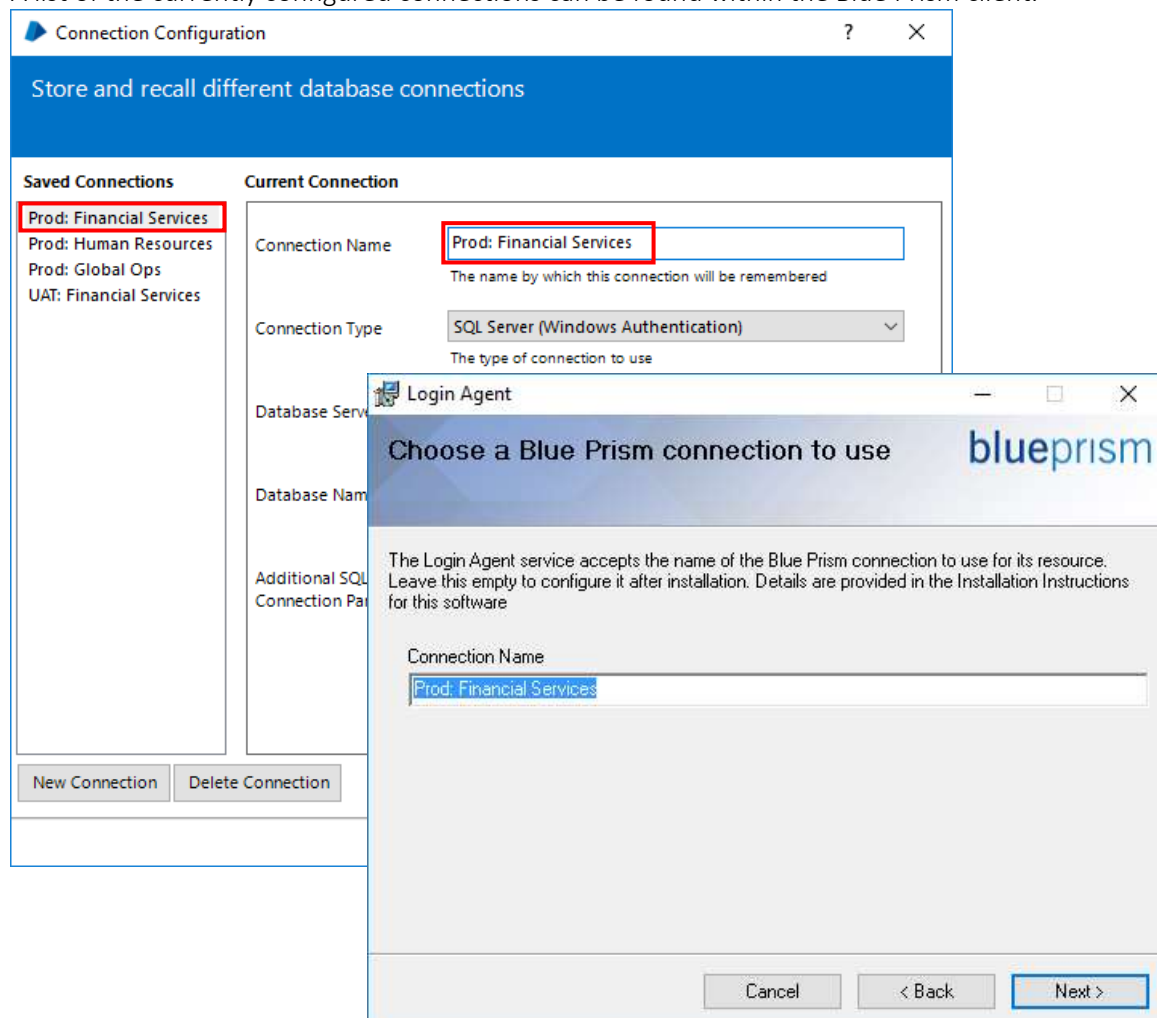
Login Agent should only be installed on a device where Blue Prism has been installed and at least one Blue Prism connection has been configured.

When installing on virtualized devices, it is necessary for the virtualization host technology to support third party credential providers.

Login Agent must be used with the version of the VBO that is provided within the associated Blue Prism release file.

1. Locate and run the appropriate installer depending on the CPU architecture of the target device (e.g. whether it is 32-bit or 64-bit device).
2. On the screen that prompts for a Connection Name, a name that exactly matches an existing Blue Prism connection on the local device must be provided.

A list of the currently configured connections can be found within the Blue Prism client.



3. Optionally select a custom installation location and complete the installation.
4. If using Login Agent with a Blue Prism environment that is configured for Single Sign On, the services console should be used to configure the Login Agent service to logon with a Blue Prism domain account.
5. Once the installation has completed, reboot the device.

Using Login Agent

Overview

When executing an automated process on a Blue Prism Runtime Resource, it is necessary for the Runtime Resource to be listening on a device which is logged in and not locked. This allows the process to operate under the context of that user and provides access to all of the local applications and network resources that it may need.

Login Agent provides a mechanism that is intended to assist with automating the logging of a device into Windows such that the main Blue Prism Runtime Resource can be started. This includes:

- Configuring the Login Agent service with appropriate information to launch a Login Agent Runtime Resource.
- A Login Agent Runtime Resource being started automatically when a device is powered on (or rebooted) that connects to the appropriate Blue Prism environment.
- The Login Agent Runtime Resource being instructed (manually or via a schedule) to Log in.
- The Login Agent securely retrieving the appropriate credential from the database and using this to authenticate with Windows.

When appropriately configured a conceptual representation of the flow of events that will occur to take device from being powered on to being logged in and able to receive process automation instructions is shown below.

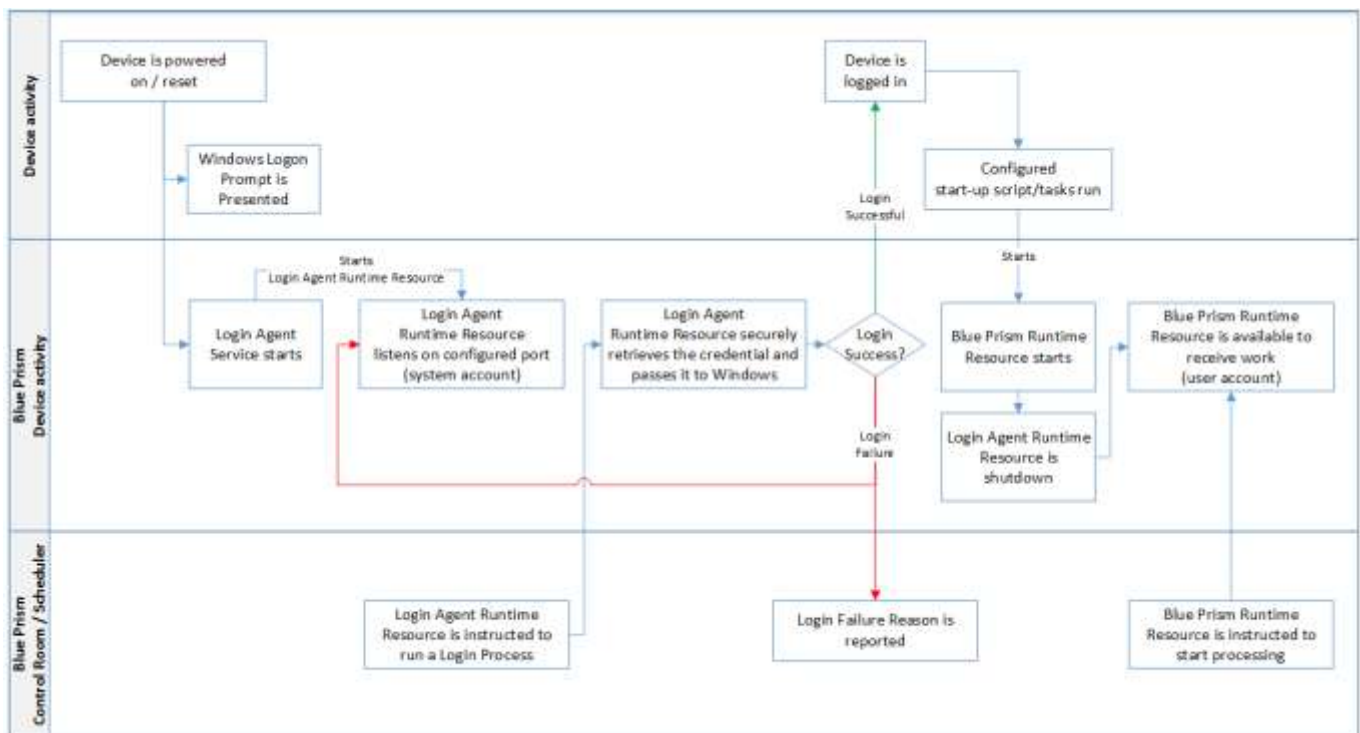


Figure 1: Conceptual flow of events for Login Agent 5.0.23+

Automation Examples

Once Login Agent has been deployed on the required devices, the Login Agent Release Package can be imported into the environment. This package includes a number of components that can be used to illustrate how to interact with a device that has been configured with Login Agent.

The package file (Login Agent Release.bprelease) is located within the Login Agent install Directory and can be imported using the **File -> Import** menu option on any single device. The data is copied into the database so it only needs to be completed once for each relevant Blue Prism environment.

The default **Login** and **Change Password** processes require that a Credential record is created for each device where the process will be run. These credential records need to be created using the default naming format:

Windows Login: [MachineName].

E.g. if the Runtime Resource is configured on robot0001 on port 8190, the default credential name should be *Windows Login: robot0001*.

Example Processes

A number of example Blue Prism processes are provided within the release package:

- Login:** Instructs a Login Agent Runtime Resource to retrieve a credential (based on a default static naming format) and execute a login. Supports both local account and network account logins.
 Intended for Login Agent Runtime Resource?: **Yes**
 Intended for Blue Prism Runtime Resource?: **No**
- Logout:** Instructs a Blue Prism Runtime resource to close all programs in the user session and log out of Windows. An optional delay can be passed in as the parameter 'Delay' which will hold off from logging out for the time specified. The process will still complete immediately, and the session will logout after the delay has passed.
 Intended for Login Agent Runtime Resource?: **No**
 Intended for Blue Prism Runtime Resource?: **Yes**

Specifying a Delay of 1 second (or greater) can help when troubleshooting.

- Check Logged In:** Checks the current logged in state of the device where the Runtime Resource is running.
 Intended for Login Agent Runtime Resource?: **Yes**
 Intended for Blue Prism Runtime Resource?: **Yes**
- Change Password:** Resets the password for the currently logged on user and overwrites the password associated with the credential record. Provides support for configuring the complexity of the password that will be generated.
 Intended for Login Agent Runtime Resource?: **No** – process terminates immediately
 Intended for Blue Prism Runtime Resource?: **Yes**

Example Actions

A Business Object, leveraged by the above processes, is provided that provides a set of example actions that can be used to achieve common authentication actions with the operating system such as **Log In, Is Logged In, Log Out, Change Password, Lock Screen, Unlock Screen**.

Information regarding the Login Agent VBO and its actions can be found in the API documentation under Help > API Documentation.

When overwriting existing versions of the Login Agent VBO, it is necessary to re-verify any processes that use the provided functionality.

Advanced Installation and Configuration

Updating or customising the Login Agent configuration

The configuration of Blue Prism Login Agent service which is responsible for initialising the Login Agent Runtime Resource is stored within a local configuration file:

```
C:\ProgramData\Blue Prism Limited\Automate V3\LoginAgentService.config
```

The `workingdirectory` element points to the installation directory for the Blue Prism software.

The `startuparguments` element gives the arguments that will be used when launching the Login Agent Runtime Resource.

Common start-up argument configuration changes include:

- Updating the Blue Prism connection that the Login Agent Runtime Resource will use
- Updating the port number that Login Agent Runtime Resource will listen on
- Configuring the Login Agent Runtime Resource to apply certificate-based encryption
- Adding custom parameters to be included in the start-up process of the Login Agent Runtime Resource

Updating the Blue Prism connection that is used

The value of the connection name must be an exact match of the name of an existing Blue Prism connection on the local device.

```
<startuparguments>
  <argument name="resourcepc" />
  <argument name="public" />
  <argument name="port">
    <value>8181</value>
  </argument>
  <argument name="dbconname">
    <value>Prod: Financial Services</value>
  </argument>
```

If no connection is specified in the configuration file the first connection specified in Blue Prism client connection list on the local device will be used.

Updating the port that the Login Agent Runtime Resource will listen on

The listening port used by the Login Agent Runtime Resource is configured separately to the listening port that will be used by the Runtime Resource is used once the device has been logged on. There is no requirement for the Login Agent Runtime Resource and the Blue Prism Runtime Resource to use the same port.

```
<startuparguments>
  <argument name="resourcepc" />
  <argument name="public" />
  <argument name="port">
    <value>8181</value>
  </argument>
  <argument name="dbconname">
    <value>Prod: Financial Services</value>
  </argument>
```


Configuring the Login Agent Runtime Resource with certificate-based encryption

Where the conventional Runtime Resources are configured to force encryption of incoming connections using a specified certificate (e.g. where the Runtimes are started using the `/sslcert` switch), it is necessary to manually apply the appropriate configuration to the Login Agent Runtime Resource.

The `startuparguments` element within the configuration file can be updated to include the appropriate information:

```
<argument name="dbconname">
  <value>Prod: Financial Services</value>
</argument>
<argument name="SSLCert">
  <value>[Certificate Thumbprint]</value>
</argument>
```

E.g.

```
<argument name="dbconname">
  <value>Prod: Financial Services</value>
</argument>
<argument name="SSLCert">
  <value>fee449ee0e3965a5246f000e89fde2a065fd89d4</value>
</argument>
```

Certificate-based encryption is only applied to the traffic received on the listening port. Encryption is applied separately to the connection that retrieves the credentials that will be used as part of the login process.

Certificate-based encryption should only be applied to Login Agent Runtime Resources once the certificate has been applied and tested with a Blue Prism Runtime Resource

Configuring the Login Agent Runtime Resource to authenticate against Blue Prism

The Login Agent Runtime Resource can be configured to authenticate with the Blue Prism environment.

- Blue Prism environments configured with native authentication
Start-up parameters will need to include `/user [username] [password]`

```
<argument name="user">
  <value>[username]</value>
  <value>[password]</value>
</argument>
```

```
<argument name="user">
  <value>jbloggs</value>
  <value>pa55w0rd</value>
</argument>
```

- Blue Prism environments configured for Single Sign-on
Start-up parameters will need to include `/SSO` to pass the context of the currently logged in user.

```
<argument name="SSO" />
```

Login Agent starts under the logon context of the Login Agent windows service. When using single sign-on, the Login Agent service will need to be configured to start with a service account that has appropriate access to Blue Prism.

Adding custom parameters to the start-up command

Where it is necessary to add additional start-up command parameters to the Login Agent Runtime resource, they can be added in a similar fashion. For example, to add a DB password for a SQL Server authenticated database add the XML below before the closing `</startuparguments>` tag:

```
<argument name="setdbpassword">  
  <value>Password$123</value>  
</argument>
```






Troubleshooting

Identifying Login Agent Runtime Resources in Control Room

Applies to Login Agent 5.0.23 and above

Login Agent Runtime Resources are shown using a dedicated icon within Control Room.

When appropriately configured, the Login Agent Runtime Resource is started whenever the machine is in a pre-logged in state, and remains active until the device has been logged on and a conventional Blue Prism Runtime Resource has been started. The Login Agent Runtime Resource is automatically shut-down by the start-up of a Blue Prism Runtime Resource.

Available Resources		
Name		State
 WIN10CLIENT		Connected
 WIN7CLIENT		Connected
 WIN81CLIENT		Offline
 WIN-DG3LMS9017D		Connected
 WIN-DG3LMS9017D:8182		Connected

Common Issues

Common issues when trying to work with Login Agent include:

- Incorrect configuration of security policies on the local device**
 It is essential that the specified security policies have been disabled. These include disabling lock screens, disabling the requirement to press ctrl + alt + del prior to logging in; and disabling log-on messages such as usage access policy messages.

 Security policies and settings can be inherited from different sources (e.g. local settings on the machine; and centrally via group policy) and the policies that are actually applied on the local device must be verified. It is advisable to watch the boot-up procedure to ensure the user is not prompted for unexpected or unsupported input.
- Incorrect configuration of the Login Agent Runtime Resource**
 The configuration of the Login Agent Runtime Resource must be validated against the settings used for the conventional Runtime Resources. In particular, verify that the connection used is one that works within the Blue Prism client.

Enable Logging for Login Agent

Applies to Login Agent 5.0.23 and above

Login Agent can be configured to generate diagnostic logs on a specific device by configuring the appropriate Registry key settings.

For appropriate versions of Login Agent, the keys can be found within the Registry at the following location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Blue Prism Limited\LoginAgent
```

- LogFileDir:** specifies the location where the log file will be generated.
- LogLevel:** specifies the granularity of logs. 0: Disabled (default); 1: Error messages; 2: Debug messages; 4: Trace messages. For a combination of levels, the values can be added together. E.g. a value of 7 will provide error messages, debug messages and trace messages.

Logging is only recommend while troubleshooting.
It is necessary to reboot the device to apply registry setting changes.

Resource stuck on error message: "Incorrect password or username"

Applies to Login Agent versions prior to 5.0.23

When incorrect credential details are used as part of the log in process, the process can enter into a loop whereby it continually retries and receives a duplicate error message. In order to exit the loop, the target device should be restarted.

Anonymous resourcepc logins are disabled

Applies to Login Agent versions prior to 5.0.27 and above

When the Blue Prism environment is configured to prevent anonymous public Runtime Resources this message indicates that the Runtime Resource is preventing from connecting because it is trying to establish an anonymous connection.

Common approaches to this solution are:

- Configure the Runtime Resource to authenticate against the environment when it starts up.
See the Advanced Installation section for information on configuring Login Agent Runtime Resources to authenticate against Blue Prism.
- Re-configure the environment to allow Anonymous Public Runtime Resources (*not recommended*)

Frequently Asked Questions

What kind of Login does Login Agent orchestrate?

Login Agent orchestrates a local interactive login on the target device. Once the interactive login has succeeded, it is expected that a conventional Blue Prism Runtime Resource will then be started (such as via a scheduled task or logon script) which will then be responsible for executing the automated processes which interact with the graphical user interface of locally installed applications.

Why does ctrl + alt + del need to be disabled?

Security policy controls such as requiring users to press ctrl + alt + del prior to providing login credentials, are specifically designed to require user input and to prevent programmatic logins onto a local device. It is therefore essential the listed security policies are appropriately disabled.

Can the Login Agent Runtime Resource run any process?

By default the Login Agent Runtime Resource operates under the context of a user with limited access to the operating system and therefore only a limited set of actions that can be executed by a Login Agent Runtime Resource.

Can an instruction be passed that orchestrates and login and then starts processing?

The Log in actions are performed by a separate Runtime Resource to the on-going business as usual processing and therefore the instruction to Log in versus the instruction to execute business processes need to be sent separately to a Runtime Resource of an appropriate type.

Where are the credentials used to orchestrate a login stored?

The location of the credentials that are used to orchestrate a login will be defined within the process. The example processes provided by Blue Prism use credentials that are stored within Credential Manager. When using credentials stored in this way, they are encrypted and stored securely, and additionally transmitted over a secure connection by default.

The **Blue Prism Data Sheet – Credential Manager** contains additional information.

Can I modify the Log in process to select which credentials to use?

By creating a custom process which orchestrates the log in, logic can be defined that will determine which credential to use. This could for example define which credential to use based on the device which is to be logged in; the time of day; the day of the week; which credentials are already in use; whether to use hard coded credentials, those stored using Credential Manager, or those stored in a third party system etc.

Can Login Agent be used on virtualized Runtime Resources?

In order to leverage Login Agent on Runtime Resources it is essential that the underlying virtualization technology supports third-party credential providers.

Can Login Agent be used with environments that do not allow anonymous public Runtime Resources?

Yes. Login Agent Runtime Resources can be configured to authenticate against the Blue Prism environment when they start up. It is necessary to configure the start-up parameters of the Login Agent Runtime Resource to pass the appropriate authentication information.

When connecting to a Blue Prism environment that is configured for single sign-on it is necessary to ensure that the Login Agent windows service is set to start using a domain account that has been assigned appropriate access to Blue Prism.