blueprism®

6.5 User Guide

Login Agent

Document Revision: 1.0

Trademarks and copyrights

Blue Prism Limited, 2 Cinnamon Park, Crab Lane, Warrington, WA2 0XP, United Kingdom.

Registered in England: Reg. No. 4260035. Tel: +44 870 879 3000. Web: www.blueprism.com

Contents

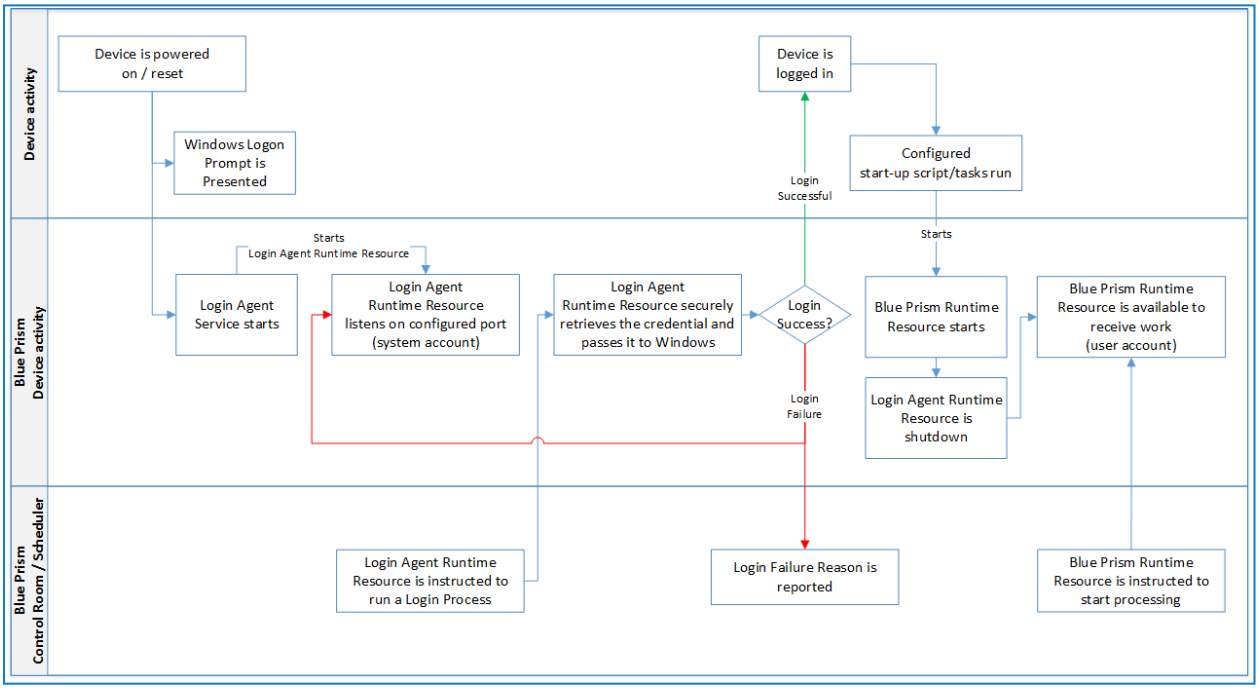
Introduction

When executing an automated process on a Blue Prism Runtime Resource, it is necessary for the runtime resource to be running 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 it may need.

Blue Prism Login Agent provides a mechanism for automating the login process for a Windows machine so that a 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 to log in manually or via a schedule.
- The Login Agent securely retrieving the appropriate credential from the database and using this to authenticate with Windows.

The diagram below shows the flow of events that occur to take a device from being powered on to being logged in and able to receive process automation instructions.



Security Policies

It is common for security policies to have been configured so that they apply each time a device is logged onto the network. The Login Agent is used to automatically log devices that host runtime resources onto the network. If security policies that require human intervention are applied to these devices, this can prevent the Login Agent from working. Therefore, it is necessary for these policies to be disabled on the devices or policy needs to be applied that allows them to be programmatically traversed.

- For devices on which there are no policies that require human intervention the Login Agent can automatically log in without having to enable and configure the SAS service.
- For devices on which there are policies that require human intervention, the SAS service can be used to programmatically send Ctrl + Alt + Del and, whilst not a recommended approach, it also provides unsupported functionality that can attempt to temporarily disable some policies.

> The SAS service must be run by a local system or local admin account.

The following sections provide recommended and alternative solutions for traversing common security policies.

Ctrl + Alt + Del – Secure Attention Sequence

If there is a requirement for users to press Ctrl + Alt + Del (Secure Attention Sequence) as part of the login:

Recommended Apply Local Security Policy that enables a software SAS to be submitted on all runtime resources. Configure the Blue Prism automated process to request the SAS service to programmatically send the SAS as part of the login operation.	**Policy setting** Local Group Policy > Administrative Templates > Windows Components > Windows Logon Options > Disable or enable software Secure Attention Service Value: Enabled for either *Services* or *Services and Ease of Access applications*. **Login Agent install options** • Install the SAS service and enable the SAS proxy. • Configure login process to instruct a software SAS to be sent.
Alternative Disable the requirement for users to traverse the SAS as part of the login operation. (Only needs applying on devices that will be used as runtime resources).	**Policy setting** Local Security Policy > Interactive Login > Do not require Ctrl + Alt + Del Value: Enabled
Alternative (unsupported) Configure the Blue Prism SAS service to attempt to disable the policy setting on the fly.	**Login Agent install options** • Install the SAS service and set the local SAS proxy. • Login process does not need to send a software SAS.

On-screen pre-login message

If there is a requirement for users to traverse an on-screen message as part of the login:

Recommended	**Policy setting**
Disable the requirement for users to traverse a login message as part of the login operation. (Only needs applying on devices that will be used as runtime resources).	Local Security Policy > Interactive Login > Message text for users attempted to log on Value: [Blank] Local Security Policy > Interactive Login > Message title for users attempted to log on Value: [Blank]
Alternative (Unsupported)	**Login Agent install options**
Configure the Blue Prism SAS service to attempt to disable the policy setting on the fly.	• Install the SAS service and set the local legal message policy.

Display lock screen

There should be no requirement to traverse a lock screen making it possible for the Login Agent to be used to unlock a locked runtime resource. This helps to ensure secure operation of devices as it makes it easier to lock and unlock devices.

Local Group Policy Editor: Do not display the lock screen.

Value: Enabled.

Using Login Agent

Once the 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.

To import the package, select **File** > **Import**, browse to the Blue Prism Login Agent directory of the Blue Prism installation, and select the *Login Agent Release.bprelease* file. 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]. For example, if the runtime resource is configured on robot0001 on port 8190, the default credential name should be Windows Login: robot0001.

For more information, see Setting up Windows login credentials.

Example Processes

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

- **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
- **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
- **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 log out 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.

Example Actions

A business object, leveraged by the above processes, 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.

Installation

Editions of Login Agent

This guide provides information on using Login Agent with Blue Prism 6.5 and above. For previous versions, download the appropriate guide from the Blue Prism Portal.

Location of installer	Contained within the Installers directory of the install location of Blue Prism.
Supported Blue Prism versions	The version of Blue Prism that the installer was provided with.
Supported Operating Systems	Same as the version of Blue Prism that the installer was provided with.
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:

- LoginAgent_x86.msi
- LoginAgent_x64.msi

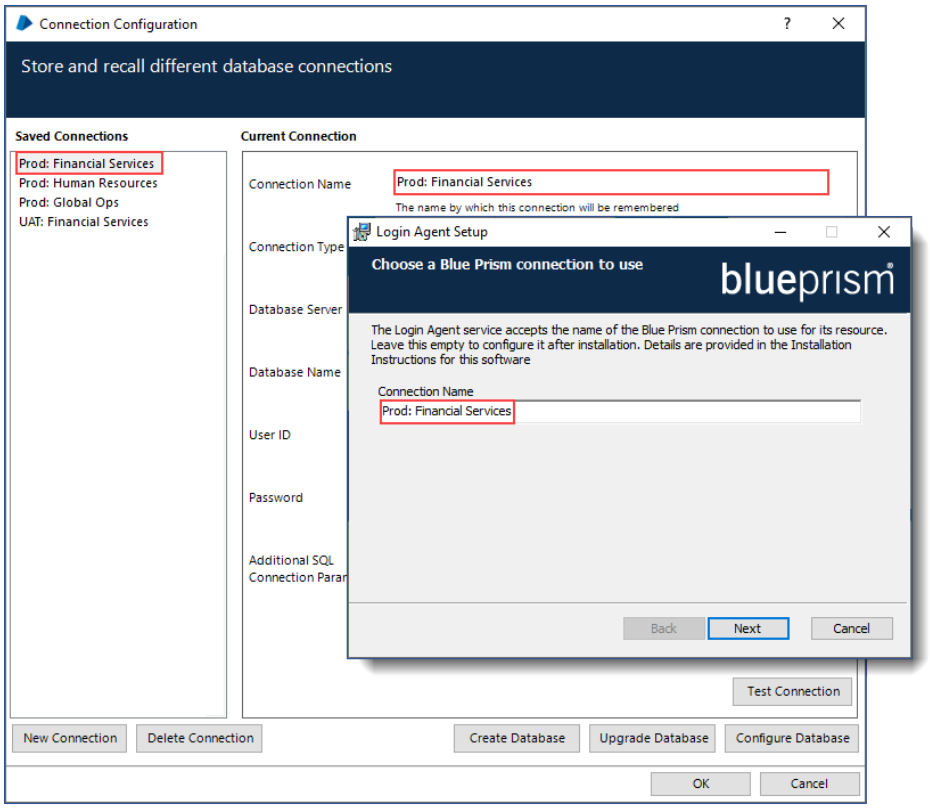
Prerequisites

- 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.

Install Blue Prism Login Agent

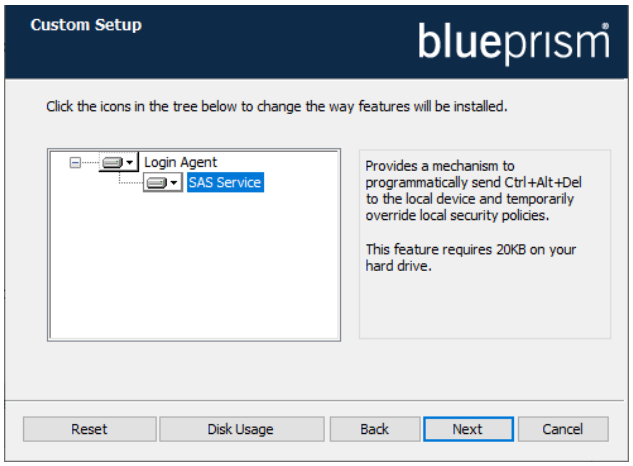
1. Navigate to the Installers directory of your Blue Prism installation and run the Login Agent MSI file appropriate to the machine.
2. Enter a Connection Name. The name must be an exact match for an existing Blue Prism connection on the local device.

   Click **Configure** from the Blue Prism sign in screen to view the currently configured connections.



3. Select a custom installation location or use the default location.

4. Select whether the SAS service is installed with the Login Agent.



The SAS service provides a mechanism to programatically send Ctrl + Alt + Del commands. If the SAS service is selected, further options are available:

- **Enable SAS proxy** - Allows the Blue Prism SAS service to be instructed to send the Ctrl + Alt + Del command to the resource.
- **Set local SAS proxy** - Attempts to override local policy on the local resource on the fly to allow SAS instructions to be received programatically. Select this option if SAS is required at login and if the policy cannot be overridden centrally. This is not a recommended approach as it provides unsupported functionality that could be broken by Windows upgrades or updates.
- **Set local legal message policy** - Attempts to override local policy on the local resource on the fly to prevent the legal message displaying at login. Select this option if a legal message displays at login and the policy cannot be overridden centrally. This is not a recommended approach as it provides unsupported functionality that could be broken by Windows upgrades or updates.

For further information about configuring these options, see Security Policies.

5. Once the installation has completed, reboot the device.

Login Agent does not require a call back connection and therefore if the selected connection is a Blue Prism Server connection (recommended), a call back connection will not be established.

Command line installation

To install Login Agent without the SAS service, use the command:

```
msiexec /i LoginAgent_x64.msi /q
```

Custom install options

To install Login Agent with the SAS service, use the ADDLOCAL parameter:

```
msiexec /i LoginAgent_x64.msi /q ADDLOCAL=LoginAgent,SasService
```

To set the SAS service configuration settings:

```
msiexec /i LoginAgent_x64.msi /quiet EnableSASProxy=true AttemptOverrideSASGPO=false
AttemptOverrideLegalMsgGPO=true
```

Apply the required true/false values as required - the setting names and values are not case sensitive.

Advanced Installation and Configuration

Updating or customising the Login Agent configuration

The configuration of Blue Prism Login Agent, responsible for initializing 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.

Setting the Blue Prism connection used by the Login Agent Runtime Resource

The Login Agent Runtime Resource will use the default Blue Prism Connection to establish a connection into the Blue Prism environment. Alternatively, it is possible to use the dbconname parameter to force which connection will be used.

The value of the connection name must exactly match 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 the 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 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 runtime resources 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>
```

For example:

```
<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>
```

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 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 </startupparguments> tag:

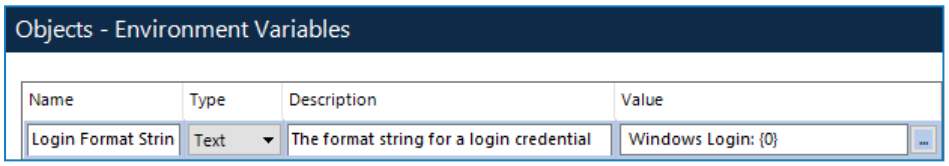
```
<argument name="setdbpassword">
      <value>Password$123</value>
</argument>
```

Setting up Windows login credentials

The login credential is a Windows user account and password used to log into a specified machine. An environment variable defines the format of the credential name that is used to log the machine in. The following process describes how to create the environment variable and add a credential for Login Agent.

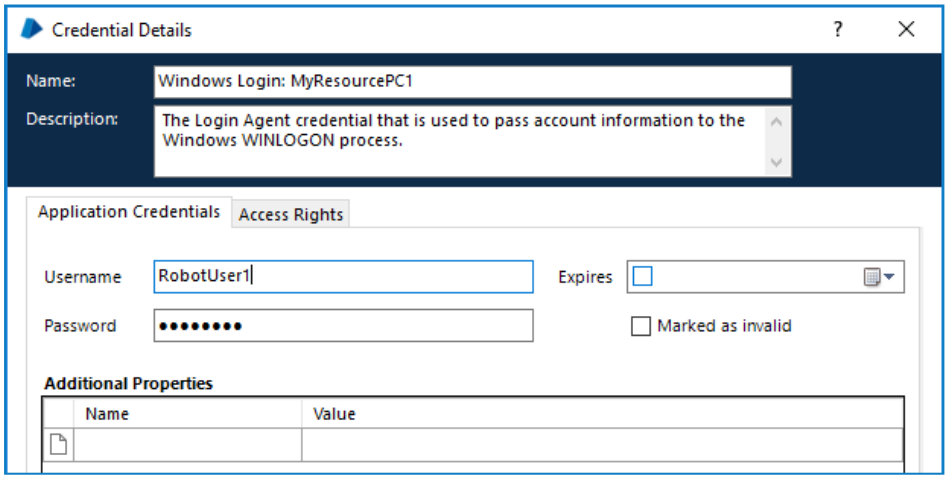
1. In the System tab, select **Objects** > **Environment Variables**.
2. Click **Add Variable** from the options menu.
3. The name of the environment variable must be formatted according to the environment variable *Login Format String*.

   It is recommended that *Windows Login: {0}* is used as the default value. The number in brackets is a placeholder for the machine name of the runtime resource that you want to log in to. The value is substituted with the machine name when the login process runs, and this is matched with an existing credential.



4. In the System tab, select **Security** > **Credentials**.

   The credential must be created using the same connection type as the Blue Prism server. For example, if you create the credential whilst logged into a direct database connection but the Login Agent client machine specifies a Blue Prism Server type connection, the credential will not be found.
5. Click **New** from the options menu. The Credential Details dialog displays.
6. Enter the environment variable name as the credential name and the username and password for the specified machine.



7. Click **OK** to save the credential.

Troubleshooting

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.

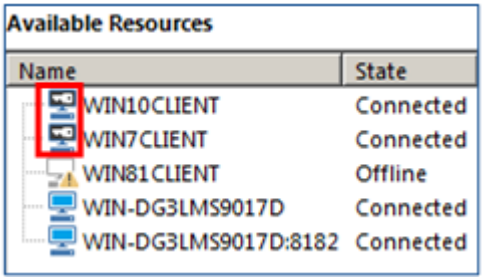
Security policies and settings can be inherited from different sources (e.g. local settings on the machine; and centrally via group policy) and the policies that are actually applied on the local device must be verified. It is advisable to watch the boot-up procedure to ensure the user is not prompted 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.

Identifying login agent runtime resources in Control Room

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.

Enable logging for Login Agent

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.

Anonymous resourcepc logins are disabled

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?

Disabling the Ctrl + Alt + Del makes it easier to get started with the Login Agent. However, if required, the Login Agent does provide a mechanism, via the Blue Prism SAS service, to programmatically traverse the Ctrl + Alt + Del screen if it is allowable on the device for software to submit the SAS.

Why do we require the security policy that allows software SAS to be submitted?

If there is a requirement to use Ctrl + Alt + Del as part of the login, this setting must be enabled to allow the instruction to be submitted programmatically by the Blue Prism SAS service.

What account context should the Login Agent services use?

- Login Agent server service - It is recommended that a domain user account is used - this is the context that Login Agent Runtime Resources will use. Additionally, if the runtime resource is configured to authenticate against the environment through the use of /sso startup parameter, it is this context that will be used to authenticate the runtime resource against the Blue Prism environment.
- Login Agent SAS service - A local admin right is required.

Why can't Login Agent traverse the login message?

There is no supported mechanism provided by Windows to do so, but a workaround is available using the Blue Prism SAS service that will attempt to disable the message on the fly. As this is a non-supported Windows approach, it may cease to be available following a Windows update and is provided without warranty.

For further information, see Mandatory security policies.

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 executed by a Login Agent Runtime Resource.

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

The login actions are performed by a separate runtime resource to the ongoing 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 *v6 Data Sheet – Credential Manager* contains additional information.

Can I modify the login process to select which credentials to use?

By creating a custom process which orchestrates the login, 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 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.

What happens if a conventional runtime resource does not shut down the Login Agent runtime resource?

When configured correctly, once a device running Login Agent has been logged in, a conventional runtime resource will start up and immediately instruct the Login Agent runtime resource to shut down. If however a conventional runtime resource does not start, the Login Agent service is configured to automatically shut down a Login Agent resource once the device has logged in. This prevents a Login Agent runtime resource from being available on a logged in device for a prolonged period of time.

How can the callback connection be disabled for the Login Agent connection to the Blue Prism Server?

If using a .NET Remoting connection (not recommended), Login Agent is automatically configured to instruct the Blue Prism Server not to establish a callback connection.

If using a WCF connection, callback ports are not used.