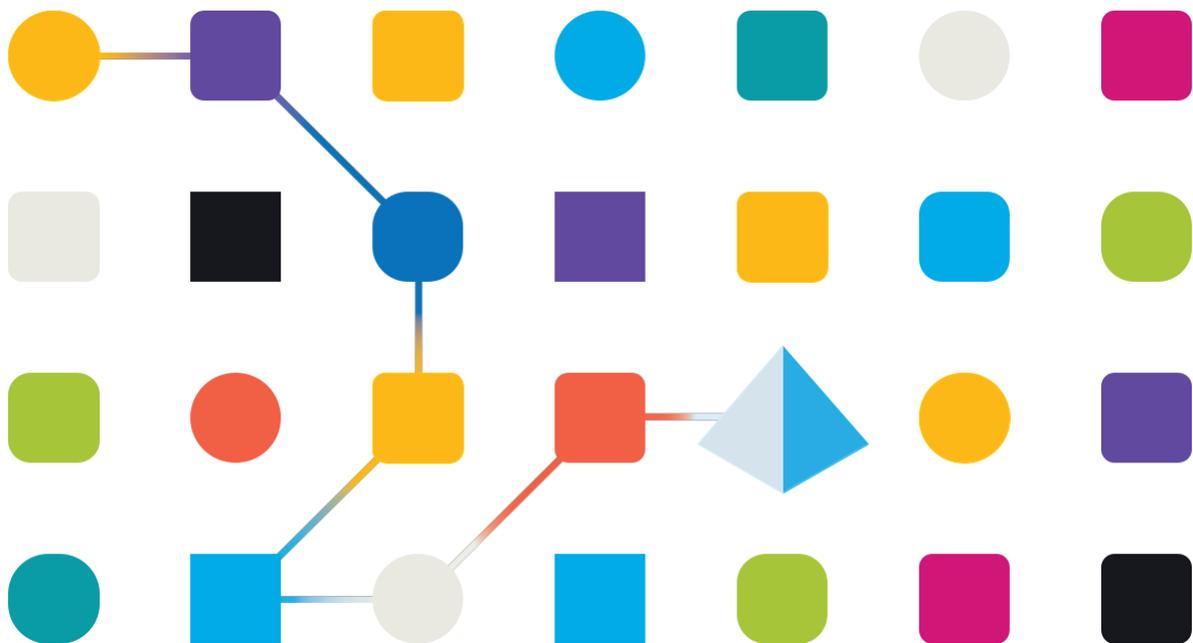


blueprism[®]

Blue Prism 7.0 Login Agent User Guide

Document Revision: 1.0



Trademarks and Copyright

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 authorized 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 – 2021**

© “Blue Prism”, the “Blue Prism” logo and Prism device are either trademarks or registered trademarks of Blue Prism Limited and its affiliates. All Rights Reserved.

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, 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

Login Agent	1
Security policies	2
Ctrl + Alt + Del – Secure Attention Sequence	2
On-screen pre-login message	3
Display lock screen	3
Install Login Agent	4
Editions of Login Agent	4
Distributable files	4
Prerequisites	4
Install Blue Prism Login Agent	5
Command line installation	7
Advanced installation and configuration	8
Update or customize the Login Agent configuration	8
Set the Blue Prism connection used by the Login Agent runtime resource	8
Update the port that the Login Agent runtime resource listens on	9
Configure the Login Agent runtime resource with certificate-based encryption	9
Configuring the Login Agent runtime resource to authenticate against Blue Prism	10
Adding parameters to the start-up command	10
Setting up Windows login credentials	11
Using the Login Agent	12
Example processes	12
Example actions	13
Troubleshooting Login Agent	14
Login Agent – Frequently Asked Questions	16

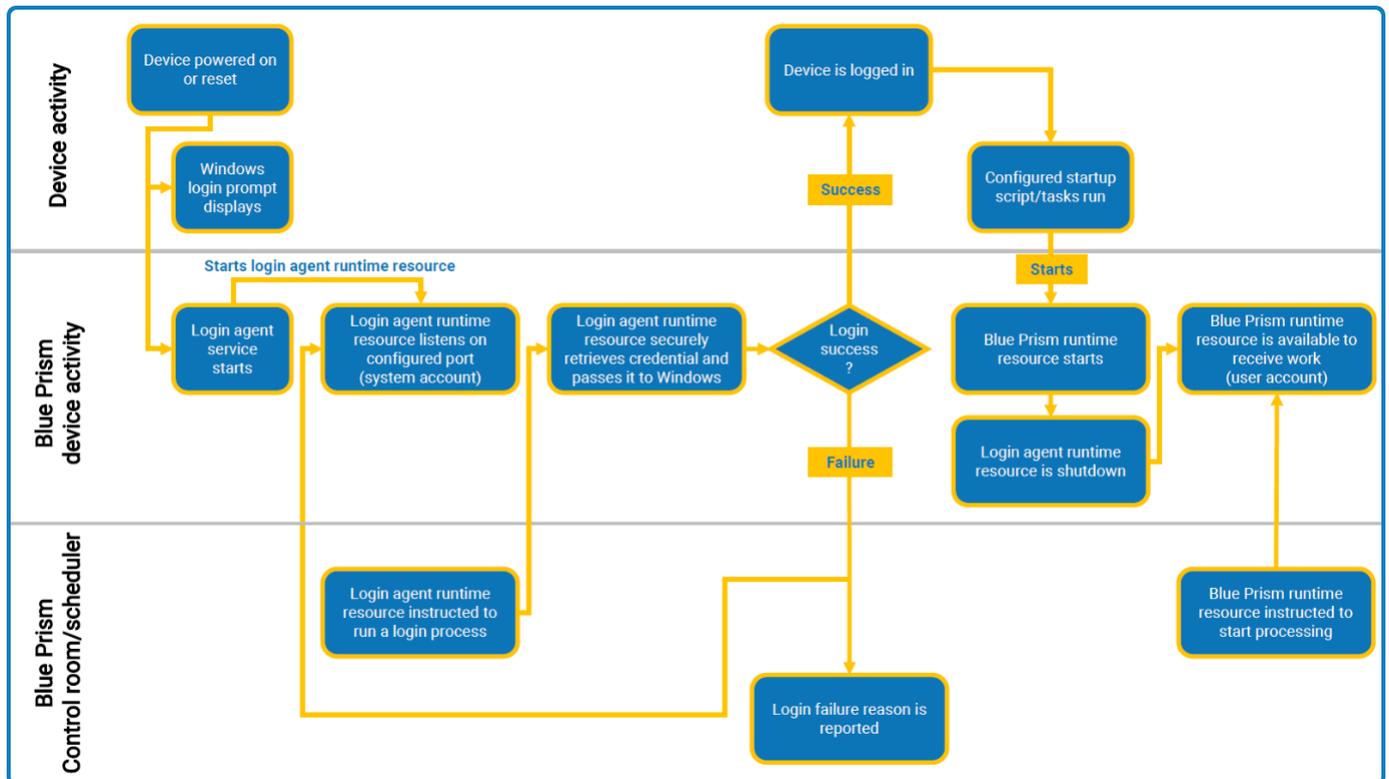
Login Agent

Blue Prism 런타임 리소스에서 자동화된 프로세스를 실행할 때 런타임 리소스가 로그인되어 있고 잠겨 있지 않은 장치에서 실행되고 있어야 합니다. 이렇게 하면 프로세스가 해당 사용자의 컨텍스트에서 작동할 수 있으며 필요한 모든 로컬 응용 프로그램 및 네트워크 리소스에 액세스할 수 있습니다.

Blue Prism 로그인 에이전트는 Blue Prism 런타임 리소스가 시작될 수 있도록 Windows 시스템의 로그인 프로세스를 자동화하는 메커니즘을 제공합니다. 다음과 같은 내용이 포함됩니다.

- 로그인 에이전트 런타임 리소스를 실행하기 위해서는 적절한 정보로 로그인 에이전트 서비스를 구성합니다.
- 로그인 에이전트 런타임 리소스는 적절한 Blue Prism 환경에 연결되는 장치의 전원이 켜지거나 재부팅될 때 자동으로 시작됩니다.
- 로그인 에이전트 런타임 리소스는 수동으로 또는 일정을 통해 로그인하도록 지시를 받습니다.
- 로그인 에이전트는 데이터베이스에서 적절한 자격 증명을 안전하게 검색하고 이를 사용하여 Windows 에서 인증합니다.

아래 다이어그램은 장치의 전원이 켜진 상태에서 로그인되어 프로세스 자동화 명령을 수신할 수 있는 상태까지 발생하는 이벤트의 흐름을 보여줍니다.



Security policies

장치가 네트워크에 로그인할 때마다 적용되는 보안 정책이 구성되는 것이 일반적입니다. 로그인 에이전트는 런타임 리소스를 호스트하는 장치를 네트워크에 자동으로 로그인하는 데 사용됩니다. 사람의 개입이 필요한 보안 정책이 이러한 장치에 적용되면 로그인 에이전트가 작동하지 않을 수 있습니다. 따라서 장치에서 이러한 정책을 비활성화하거나 프로그래밍 방식으로 통과할 수 있도록 하는 정책을 적용해야 합니다.

- SAS 서비스를 활성화하지도 않고 구성도 하지 않고 사람의 개입이 필요한 정책이 없는 장치의 경우, 로그인 에이전트가 자동으로 로그인할 수 있습니다. 사람의 개입이 필요한 정책이 있는 장치의 경우, SAS 서비스를 사용하여 프로그래밍 방식으로 Ctrl + Alt + Del 을 보낼 수 있고, 일부 정책을 일시적으로 비활성화할 수 있는 지원되지 않는 기능도 제공합니다만, 권장되는 접근 방식은 아닙니다.

- SAS 서비스는 로컬 시스템 또는 로컬 관리자 계정으로 실행해야 합니다.

다음 섹션에서는 공통 보안 정책을 통과하기 위한 권장 솔루션과 대안 솔루션을 제공합니다.

Ctrl + Alt + Del – Secure Attention Sequence

사용자가 로그인의 일부로 Ctrl + Alt + Del(SAS, 보안 주의 시퀀스)을 눌러야 하는 요구 사항이 있는 경우:

<p>Recommended(권장) 소프트웨어 SAS 가 모든 런타임 리소스에 제출될 수 있도록 하는 로컬 보안 정책을 적용합니다. 로그인 작업의 일부로 프로그래밍 방식으로 SAS 를 보내도록 SAS Service 에 요청하도록 Blue Prism 자동화 프로세스를 구성합니다.</p>	<p>Policy setting Local Group Policy > Administrative Templates > Windows Components > Windows Logon Options > Disable or enable software Secure Attention Service 값: Enabled for either <i>Services</i> or <i>Services and Ease of Access applications</i>. Login Agent install options</p> <ul style="list-style-type: none"> SAS Service 를 설치하고 SAS 프록시를 활성화합니다. 소프트웨어 SAS 를 보내도록 지시하는 로그인 프로세스 구성
<p>Alternative(대안) 사용자가 로그인 작업의 일부로 SAS 를 통과해야 하는 요구 사항을 비활성화합니다. (런타임 리소스로 사용될 기기에만 적용하면 됩니다.)</p>	<p>Policy setting Local Security Policy > Interactive Login > Do not require Ctrl + Alt + Del 값: Enabled</p>
<p>Alternative (unsupported) 필요에 따라 즉석에서 정책 설정을 비활성화하도록 Blue Prism SAS 서비스를 구성합니다.</p>	<p>Login Agent install options</p> <ul style="list-style-type: none"> SAS 서비스 설치하고 로컬 SAS 프록시 설정 로그인 프로세스에서 소프트웨어 SAS 를 보낼 필요가 없습니다.

On-screen pre-login message

사용자가 로그인 시 일부로 화면 메시지를 통과해야 하는 요구 사항이 있는 경우:

<p>Recommended(권장) 사용자가 로그인 작업의 일부로 로그인 메시지를 통과해야 하는 요구 사항을 비활성화합니다. (런타임 리소스로 사용될 기기에만 적용하면 됩니다.).</p>	<p>Policy setting Local Security Policy > Interactive Login > Message text for users attempted to log on 값: [Blank] Local Security Policy > Interactive Login > Message title for users attempted to log on 값: [Blank]</p>
<p>Alternative (unsupported) 필요에 따라 즉석에서 정책 설정을 비활성화하도록 Blue Prism SAS 서비스를 구성합니다.</p>	<p>Login Agent install options</p> <ul style="list-style-type: none"> • SAS 서비스 설치하고 로컬 법적 메시지 정책을 설정합니다.

Display lock screen

로그인 에이전트를 사용하여 잠긴 런타임 리소스를 잠금 해제할 수 있도록 잠금 화면을 통과할 필요가 없어야 합니다. 이렇게 하면 장치를 더 쉽게 잠그고 잠금 해제할 수 있으므로 장치의 안전한 작동을 보장하는 데 도움이 됩니다.

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

값: Enabled.

Install Login Agent

Editions of Login Agent

이 가이드는 Blue Prism 6.5 이상에서 로그인 에이전트를 사용하는 방법에 대한 정보를 제공합니다. 이전 버전의 경우 Blue Prism Portal 에서 해당 가이드를 다운로드하십시오.

Location of installer	Blue Prism 설치 위치의 Installers 디렉토리에 포함됩니다.
Supported Blue Prism versions	설치 프로그램과 함께 제공된 Blue Prism 의 버전입니다.
Supported Operating Systems	설치 프로그램과 함께 제공된 Blue Prism 버전과 동일합니다.
Prerequisites	로그인 에이전트를 설치하기 전에 적절한 버전의 Blue Prism 을 설치하고 구성해야 합니다. 가상 장치에 설치할 때 호스트 가상화 기술은 타사 자격 증명 공급자를 지원해야 합니다.
User access	대상 시스템에 관리자 액세스 권한이 필요합니다.

Distributable files

로그인 에이전트의 각 버전에 사용할 수 있는 두 가지 설치 프로그램이 있습니다.

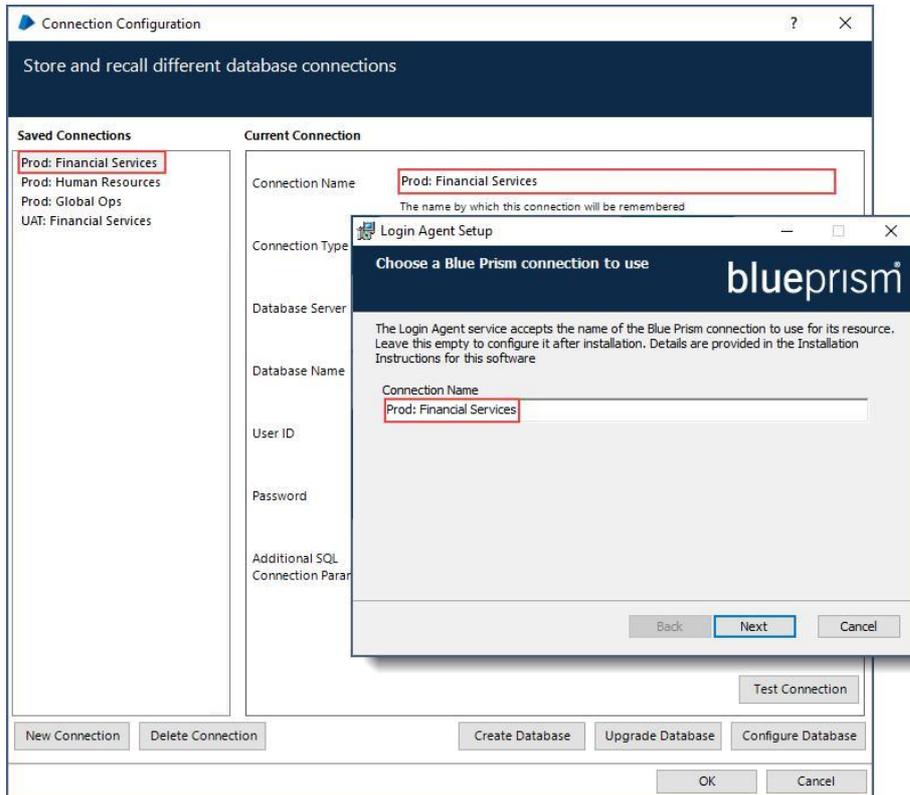
- LoginAgent_x86.msi
- LoginAgent_x64.msi

Prerequisites

- 로그인 에이전트는 Blue Prism 이 설치되고 하나 이상의 Blue Prism 연결이 구성된 장치에만 설치해야 합니다.
- 가상화된 장치에 설치할 때 가상화 호스트 기술이 타사 자격 증명 공급자를 지원해야 합니다.
- 로그인 에이전트는 연결된 Blue Prism 릴리스 파일 내에서 제공되는 VBO 버전과 함께 사용해야 합니다.

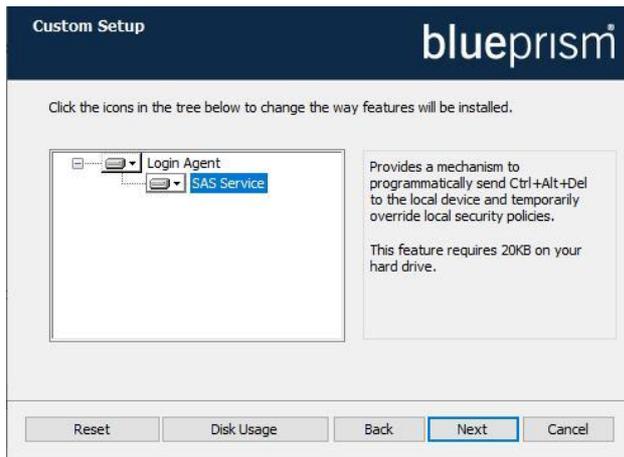
Install Blue Prism Login Agent

1. Blue Prism 설치의 Installers 디렉토리로 이동하여 시스템에 적합한 로그인 에이전트 MSI 파일을 실행하십시오.
2. 연결 이름(Connection Name)을 입력합니다. 이름은 로컬 장치의 기존 Blue Prism 연결과 정확히 일치해야 합니다.
현재 구성된 연결을 보려면 Blue Prism 로그인 화면에서 구성(**Configure**)을 클릭합니다.



3. 사용자 지정 설치 위치(custom installation location)를 선택하거나 기본 위치(default location)를 사용합니다.

4. SAS 서비스가 로그인 에이전트와 함께 설치되는지 여부를 선택합니다.



SAS 서비스는 프로그래밍 방식으로 Ctrl + Alt + Del 명령을 보내는 메커니즘을 제공합니다.

SAS 서비스를 선택하면 추가 옵션을 사용할 수 있습니다.

- **Enable SAS proxy** – Blue Prism SAS 서비스가 Ctrl + Alt + Del 명령을 리소스에 보내도록 지시할 수 있습니다.
- **Set local SAS proxy** – SAS 명령을 프로그래밍 방식으로 수신할 수 있도록 로컬 리소스에 대한 로컬 정책을 즉시 재정의하려고 시도합니다. 로그인 시 SAS가 필요하고 정책을 중앙에서 재정의할 수 없는 경우 이 옵션을 선택합니다. 이는 Windows 업그레이드 또는 업데이트로 인해 중단될 수 있는 지원되지 않는 기능을 제공하므로 권장되지 않습니다.
- **Set local legal message policy** – 로그인 시 법적 메시지가 표시되지 않도록 로컬 리소스에 대한 로컬 정책을 즉시 재정의하려고 시도합니다. 로그인 시 법적 메시지가 표시되고 정책을 중앙에서 재정의할 수 없는 경우 이 옵션을 선택합니다. 이는 Windows 업그레이드 또는 업데이트로 인해 중단될 수 있는 지원되지 않는 기능을 제공하므로 권장되지 않습니다.

이러한 옵션 구성에 대한 자세한 내용은 보안 정책([Security Policies](#))을 참조하십시오.

5. 설치가 완료되면 장치를 재부팅하십시오.



로그인 에이전트는 콜백 연결이 필요하지 않으므로 선택한 연결이 블루프리즘 서버 연결(권장)인 경우 콜백 연결이 설정되지 않습니다.

Command line installation

SAS 서비스 없이 로그인 에이전트를 설치하려면 다음 명령을 사용하십시오.

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

사용자 지정 설치 옵션 설정하십시오.

SAS 서비스와 함께 로그인 에이전트를 설치하려면 ADDLOCAL 매개변수를 사용하십시오.

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

SAS 서비스 구성 설정을 지정하려면:

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

필요에 따라 필수 true/false 값을 적용합니다. 설정 이름과 값은 대소문자를 구분하지 않습니다.

Advanced installation and configuration

Update or customize the Login Agent configuration

로그인 에이전트 런타임 리소스 초기화를 담당하는 Blue Prism 로그인 에이전트 서비스의 구성은 로컬 구성 파일에 저장됩니다.

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

작업 디렉토리 요소(workingdirectory element)는 Blue Prism 소프트웨어의 설치 디렉토리를 가리킵니다. 시작 인수 요소(startuparguments element)는 로그인 에이전트 런타임 리소스를 시작할 때 사용할 인수를 제공합니다.

공통 시작 인수 구성 변경 사항은 다음과 같습니다.

- 로그인 에이전트 런타임 리소스가 사용할 Blue Prism 연결 업데이트
- 로그인 에이전트 런타임 리소스가 수신 대기할 포트 번호 업데이트
- 인증서 기반 암호화를 적용하도록 로그인 에이전트 런타임 리소스 구성
- 로그인 에이전트 런타임 리소스의 시작 프로세스에 포함될 사용자 정의 매개변수 추가

Set the Blue Prism connection used by the Login Agent runtime resource

로그인 에이전트 런타임 리소스는 기본 Blue Prism 연결을 사용하여 Blue Prism 환경에 대한 연결을 설정합니다. 또는 dbconname 매개변수를 사용하여 사용할 연결을 강제 실행할 수 있습니다.

연결 이름(connection name) 값은 로컬 장치의 기존 Blue Prism 연결 이름과 정확히 일치해야 합니다.

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

구성 파일에 연결이 지정되지 않은 경우 로컬 장치의 Blue Prism 클라이언트 연결 목록에 지정된 첫 번째 연결이 사용됩니다.

Update the port that the Login Agent runtime resource listens on

로그인 에이전트 런타임 리소스에서 사용하는 수신 포트는 장치가 로그인한 후 사용되는 런타임 리소스에서 사용할 수신 포트와 별도로 구성됩니다. 로그인 에이전트 런타임 리소스와 Blue Prism 런타임 리소스가 동일한 포트를 사용할 필요는 없습니다.

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

Configure the Login Agent runtime resource with certificate-based encryption

기존 런타임 리소스가 지정된 인증서를 사용하여 들어오는 연결을 강제로 암호화하도록 구성된 경우(예: 런타임이 /sslcert 스위치를 사용하여 시작되는 경우) 로그인 에이전트 런타임 리소스에 적절한 구성을 수동으로 적용해야 합니다.

구성 파일 내의 startuparguments 요소는 적절한 정보를 포함하도록 업데이트될 수 있습니다.

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

예를 들어:

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

 인증서 기반 암호화는 수신 포트에서 수신된 트래픽에만 적용됩니다. 암호화는 로그인 프로세스의 일부로 사용될 자격 증명을 검색하는 연결에 별도로 적용됩니다. 인증서 기반 암호화는 인증서가 적용되고 Blue Prism 런타임 리소스로 테스트된 후에만 로그인 에이전트 런타임 리소스에 적용되어야 합니다.

Configuring the Login Agent runtime resource to authenticate against Blue Prism

로그인 에이전트 런타임 리소스는 Blue Prism 환경에서 인증하도록 구성할 수 있습니다.

기본 인증으로 구성된 Blue Prism 환경 – 시작 매개변수에는 /user [username] [password]가 포함되어야 합니다.

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

Single Sign-on 용으로 구성된 Blue Prism 환경 – 시작 매개변수는 현재 로그인한 사용자의 컨텍스트를 전달하기 위해 /sso 를 포함해야 합니다.

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



로그인 에이전트는 로그인 에이전트 Windows 서비스의 로그온 컨텍스트에서 시작됩니다. 싱글 사인온을 사용하는 경우 로그인 에이전트 서비스는 Blue Prism 에 대한 적절한 액세스 권한이 있는 서비스 계정으로 시작하도록 구성해야 합니다.

Adding parameters to the start-up command

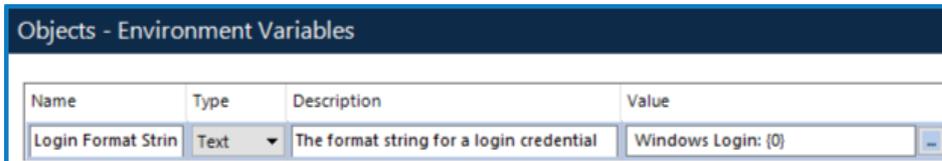
로그인 에이전트 런타임 자원에 추가 시작 명령 매개변수를 추가해야 하는 경우 유사한 방식으로 추가할 수 있습니다. 예를 들어, SQL Server 인증 데이터베이스에 대한 DB 암호를 추가하려면 `</startuparguments>` 태그 앞에 아래 XML 을 추가합니다.

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

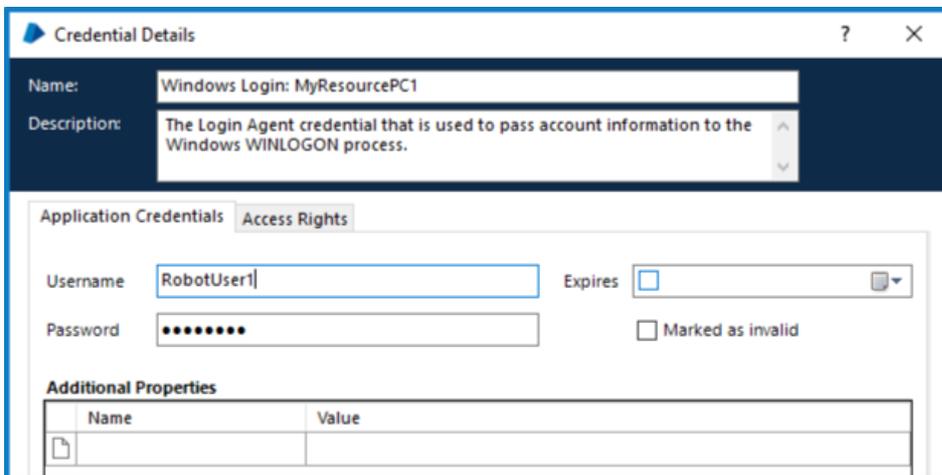
Setting up Windows login credentials

로그인 자격 증명은 지정된 컴퓨터에 로그인하는 데 사용되는 Windows 사용자 계정 및 암호입니다. 환경 변수는 시스템에 로그인하는 데 사용되는 자격 증명 이름의 형식을 정의합니다. 다음 프로세스에서는 환경 변수를 만들고 로그인 에이전트에 대한 자격 증명을 추가하는 방법을 설명합니다.

1. 시스템 탭에서 **Objects > Environment Variables** 를 선택합니다.
2. 옵션 메뉴에서 **Add Variable** 를 클릭합니다.
3. 환경 변수의 이름은 환경 변수 *Login Format String* 에 따라 형식이 지정되어야 합니다.
*Windows Login: {0}*을 기본값으로 사용하는 것을 권장합니다. 괄호 안의 숫자는 로그인하려는 런타임 리소스의 시스템 이름에 대한 자리 표시자입니다. 이 값은 로그인 프로세스가 실행될 때 시스템 이름으로 대체되며 기존 자격 증명과 일치합니다.



4. 시스템 탭에서 **Security > Credentials** 을 선택합니다.
자격 증명은 Blue Prism 서버와 동일한 연결 유형을 사용하여 생성해야 합니다. 예를 들어, 직접 데이터베이스 연결에 로그인한 상태에서 자격 증명을 생성했지만 로그인 에이전트 클라이언트 시스템이 Blue Prism 서버 유형 연결을 지정하는 경우 자격 증명을 찾을 수 없습니다.
5. 옵션 메뉴에서 **New** 를 클릭합니다. 자격 증명 세부 정보 대화 상자가 표시됩니다.
6. 환경 변수 이름을 자격 증명 이름으로 입력하고 지정된 시스템의 사용자 이름과 암호를 입력합니다.



7. **OK** 를 클릭하여 자격 증명을 저장합니다.

Using the Login Agent

로그인 에이전트가 필요한 장치에 배포되면 로그인 에이전트 릴리스 패키지를 환경으로 가져올 수 있습니다. 이 패키지에는 로그인 에이전트로 구성된 장치와 상호 작용하는 방법을 설명하는 데 사용할 수 있는 여러 구성 요소가 포함되어 있습니다.

패키지를 가져오려면 **File > Import** 를 선택하고 Blue Prism 설치의 Blue Prism 로그인 에이전트 디렉터리로 이동한 다음 로그인 에이전트 Release.bprelease 파일을 선택합니다. 데이터는 데이터베이스에 복사되므로 각 관련 Blue Prism 환경에 대해 한 번만 완료하면 됩니다.

기본 로그인 및 비밀번호 변경 프로세스에서는 프로세스가 실행될 각 장치에 대해 자격 증명 레코드가 생성되어야 합니다. 이러한 자격 증명 레코드는 기본 명명 형식인 Windows Login: [MachineName]을 사용하여 생성해야 합니다. 예를 들어 런타임 리소스가 포트 8190 의 robots0001 에 구성된 경우 기본 자격 증명 이름은 Windows Login: robot0001 이어야 합니다.

자세한 내용은 [Setting up Windows login credentials](#) 을 참조하십시오.

Example processes

릴리스 패키지에는 다음과 같은 Blue Prism 프로세스의 예가 제공됩니다.

- Change Password** – 현재 로그인한 사용자의 암호를 재설정하고 자격 증명 레코드와 연결된 암호를 덮어씁니다. 생성될 암호의 복잡성을 구성하기 위한 지원을 제공합니다.
 로그인 에이전트 런타임 리소스를 위한 것입니까? No – 프로세스가 즉시 종료됩니다.
 Blue Prism 런타임 리소스를 위한 것입니까? Yes
- Check Logged In** – 런타임 리소스가 실행 중인 장치의 현재 로그인 상태를 확인합니다.
 로그인 에이전트 런타임 리소스를 위한 것입니까? Yes
 Blue Prism 런타임 리소스를 위한 것입니까? Yes
- Login** – 로그인 에이전트 런타임 리소스에 자격 증명(기본 정적 명명 형식 기반)을 검색하고 로그인을 실행하도록 지시합니다. 로컬 계정 및 네트워크 계정 로그인을 모두 지원합니다. 로그인 에이전트 런타임 리소스를 위한 것입니까? Yes
 Blue Prism 런타임 리소스를 위한 것입니까? No
- Logout** – Blue Prism 런타임 리소스에 사용자 세션의 모든 프로그램을 닫고 Windows 에서 로그아웃하도록 지시합니다. 선택적 지연은 지정된 시간 동안 로그아웃을 보류하는 매개변수 'Delay'로 전달할 수 있습니다. 프로세스는 여전히 즉시 완료되며 지연 시간이 지나면 세션이 로그아웃됩니다.
 로그인 에이전트 런타임 리소스를 위한 것입니까? No
 Blue Prism 런타임 리소스를 위한 것입니까? Yes
 1 초(또는 그 이상)의 지연을 지정하면 문제 해결에 도움이 될 수 있습니다.

Example actions

위의 프로세스에 의해 활용되는 비즈니스 개체는 운영 체제와 공통 인증 작업을 달성하는 데 사용할 수 있는 일련의 예제 작업을 제공합니다. 예제는 Log In, Is Logged In, Log Out, Change Password, Lock Screen, Unlock Screen 등입니다.

로그인 에이전트 VBO 및 해당 작업에 대한 정보는 **Help > API Documentation** 문서 아래의 API 문서에서 찾을 수 있습니다.

 로그인 에이전트 VBO의 기존 버전을 덮어쓸 때에는 제공된 기능을 사용하는 모든 프로세스를 다시 확인해야 합니다.

Troubleshooting Login Agent

로그인 에이전트로 작업할 때 일반적인 문제는 다음과 같습니다.

로컬 장치의 잘못된 보안 정책 구성

지정된 보안 정책을 비활성화해야 합니다. 여기에는 잠금 화면 비활성화, 로그인 전에 CTRL + ALT + DEL 을 눌러야 하는 요구 사항 비활성화가 포함되며; 사용법 접근 정책 메시지와 같은 로그온 메시지의 비활성화도 포함합니다.

보안 정책 및 설정은 다른 소스(예: 머신의 로컬 설정, 그룹 정책을 통한 중앙 집중식)에서 상속될 수 있으며 로컬 장치에 실제로 적용된 정책을 확인해야 합니다. 사용자에게 예기치 않거나 지원되지 않는 입력에 대한 프롬프트가 표시되지 않도록 부팅 절차를 관찰하는 것이 좋습니다.

로그인 에이전트 런타임 리소스의 잘못된 구성

로그인 에이전트 런타임 리소스의 구성은 기존 런타임 리소스에 사용되는 설정에 대해 유효성을 검사해야 합니다. 특히 사용된 연결이 Blue Prism 클라이언트 내에서 작동하는 연결인지 확인하십시오.

제어실에서 로그인 에이전트 런타임 리소스 식별

로그인 에이전트 런타임 리소스는 제어실 내 전용 아이콘을 사용하여 표시됩니다.

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

적절하게 구성된 경우 로그인 에이전트 런타임 리소스는 시스템이 사전 로그인 상태에 있을 때마다 시작되고 장치가 로그온되고 기존 Blue Prism 런타임 리소스가 시작될 때까지 활성 상태를 유지합니다. 로그인 에이전트 런타임 리소스는 Blue Prism 런타임 리소스의 시작에 의해 자동으로 종료됩니다.

로그인 에이전트에 대한 로깅 활성화

적절한 레지스트리 키 설정을 구성하여 특정 장치에서 진단 로그를 생성하도록 로그인 에이전트를 구성할 수 있습니다.

적절한 버전의 로그인 에이전트의 경우 다음 위치에 있는 레지스트리 내에서 키를 찾을 수 있습니다.

`HKEY_LOCAL_MACHINE\SOFTWARE\Blue Prism Limited>LoginAgent`

- **LogFileDir** – 로그 파일이 생성될 위치를 지정합니다.
- **LogLevel** – 로그 메시지의 세밀한 정도를 지정합니다. 0: 비활성화됨(기본값); 1: 오류 메시지; 2: 디버그 메시지; 4: 추적 메시지. 레벨 조합의 경우 값을 함께 추가할 수 있습니다. 예를 들어 값 7 은 오류 메시지, 디버그 메시지 및 추적 메시지를 제공합니다.



로깅은 문제 해결할 때에만 권장됩니다.

레지스트리 설정 변경 사항을 적용하려면 장치를 재부팅해야 합니다.

익명 resourcepc 로그인에 비활성화되었습니다.

Blue Prism 환경이 익명 공용 런타임 리소스를 방지하도록 구성된 경우 이 메시지는 런타임 리소스가 익명 연결을 설정하려고 시도하기 때문에 연결을 방지하고 있음을 나타냅니다.

이 솔루션에 대한 일반적인 접근 방식은 다음과 같습니다.

- 시작할 때 환경에 대해 인증하도록 런타임 리소스를 구성합니다. Blue Prism 에 대해 인증하도록 로그인 에이전트 런타임 리소스를 구성하는 방법에 대한 정보는 고급 설치(Advanced Installation) 섹션을 참조하십시오.
- 익명 공용 런타임 리소스를 허용하도록 환경을 재구성합니다(권장하지 않음).

Login Agent – Frequently Asked Questions

로그인 에이전트는 어떤 종류의 로그인을 조정합니까?

로그인 에이전트는 대상 장치에서 로컬 대화식 로그인을 조정합니다. 대화형 로그인이 성공하면 (예: 예약된 작업 또는 로그인 스크립트를 통해) 기존의 Blue Prism 런타임 리소스가 시작될 것이며 그것은 로컬로 설치된 응용 프로그램의 그래픽 사용자 인터페이스와 상호 작용하는 자동화된 프로세스를 실행할 책임을 집니다.

Ctrl + Alt + Del 을 비활성화해야 하는 이유는 무엇입니까?

Ctrl + Alt + Del 을 비활성화하면 로그인 에이전트를 더 쉽게 시작할 수 있습니다. 그러나 필요한 경우 로그인 에이전트는 소프트웨어가 SAS 를 제출하도록 장치에서 허용되는 경우 Blue Prism SAS 서비스를 통해 프로그래밍 방식으로 Ctrl + Alt + Del 화면을 가로지르는 메커니즘을 제공합니다.

소프트웨어 SAS 제출을 허용하는 보안 정책이 필요한 이유는 무엇입니까?

로그인의 일부로 Ctrl + Alt + Del 을 꼭 사용해야 하는 경우 Blue Prism SAS 서비스에서 프로그래밍 방식으로 명령을 제출할 수 있도록 이 설정을 활성화해야 합니다.

로그인 에이전트 서비스는 어떤 계정 컨텍스트를 사용해야 합니까?

- Login Agent server service – 도메인 사용자 계정을 사용하는 것이 좋습니다. 이는 로그인 에이전트 런타임 리소스가 사용할 컨텍스트입니다. 또한 런타임 리소스가 /sso 시작 매개변수를 사용하여 환경에 대해 인증하도록 구성된 경우 Blue Prism 환경에 대해 런타임 리소스를 인증하는데 사용되는 것은 이 컨텍스트입니다.
- Login Agent SAS service – 로컬 관리자 권한이 있는 서비스 계정이 필요합니다.

로그인 에이전트가 로그인 메시지를 건너갈 수 없는 이유는 무엇입니까?

이렇게 하기 위해 Windows 에서 제공하는 지원되는 메커니즘은 없습니다만, 임기응변으로 필요할 때 메시지를 즉시 비활성화하는 Blue Prism SAS 서비스를 사용할 수 있습니다. 이는 Windows 가 정식으로 지원하지 않는 접근 방식이므로 Windows 업데이트 이후 사용이 중단될 수 있으며 보증 없이 제공됩니다. 자세한 내용은 [Security policies](#) 을 참조하세요.

로그인 에이전트 런타임 리소스가 모든 프로세스를 실행할 수 있습니까?

기본적으로 로그인 에이전트 런타임 리소스는 운영 체제에 대한 액세스가 제한된 사용자 컨텍스트에서 작동하므로 로그인 에이전트 런타임 리소스에서는 제한된 작업 종류만 실행할 수 있습니다.

로그인한 다음 조합해서 처리를 시작하는 명령을 전달할 수 있습니까?

로그인 작업은 일반적인 처리와 같이 진행 중인 비즈니스에 대해 별도의 런타임 리소스에 의해 수행되므로 로그인에 대한 명령과 비즈니스 프로세스를 실행하는 명령은 적절한 유형의 런타임 리소스에 별도로 전송되어야 합니다.

로그인을 조정하는 데 사용되는 자격 증명은 어디에 저장됩니까?

로그인을 조정하는 데 사용되는 자격 증명의 위치는 프로세스 내에서 정의됩니다. Blue Prism 에서 제공하는 예제 프로세스는 Credential Manager 내에 저장된 자격 증명을 사용합니다.

이러한 방식으로 저장된 자격 증명을 사용하면 암호화되어 안전하게 저장되며 기본적으로 보안 연결을 통해 추가로 전송됩니다.

The *v6 Data Sheet – Credential Manager* 에는 추가 정보가 포함되어 있습니다.

로그인 프로세스를 수정하여 사용할 자격 증명을 선택할 수 있습니까?

로그인을 조정하는 사용자 지정 프로세스를 생성하여 사용할 자격 증명을 결정하는 논리를 정의할 수 있습니다. 이것은 예를 들어 로그인할 장치를 기반으로 사용할 자격 증명을 정의할 수 있습니다. 하루 중 시간; 요일; 어떤 자격 증명에 이미 사용 중인지; 하드 코딩된 자격 증명을 사용할지, Credential Manager 를 사용하여 저장된 자격 증명이나 타사 시스템에 저장된 자격 증명을 사용할 지 등입니다.

가상화된 런타임 리소스에서 로그인 에이전트를 사용할 수 있습니까?

런타임 리소스에서 로그인 에이전트를 활용하려면 기본 가상화 기술이 타사 자격 증명 공급자를 지원해야 합니다.

익명의 공개 런타임 리소스를 허용하지 않는 환경에서 로그인 에이전트를 사용할 수 있습니까?

예. 로그인 에이전트 런타임 리소스는 시작할 때 Blue Prism 환경에 대해 인증하도록 구성할 수 있습니다. 적절한 인증 정보를 전달하려면 로그인 에이전트 런타임 리소스의 시작 매개변수를 구성해야 합니다.

싱글 사인온을 위해 구성된 Blue Prism 환경에 연결할 때 로그인 에이전트 Windows 서비스가 Blue Prism 에 대한 적절한 액세스가 할당된 도메인 계정을 사용하여 시작하도록 설정되어 있는지 확인해야 합니다.

기존 런타임 리소스가 로그인 에이전트 런타임 리소스를 종료하지 않으면 어떻게 됩니까?

올바르게 구성된 경우 로그인 에이전트를 실행하는 장치가 로그인되면 기존 런타임 리소스가 시작되고 즉시 로그인 에이전트 런타임 리소스가 종료되도록 지시합니다. 그러나 기존 런타임 리소스가 시작되지 않으면 로그인 에이전트 서비스는 장치가 로그인되면 로그인 에이전트 리소스를 자동으로 종료하도록 구성됩니다. 이렇게 하면 로그인한 장치에서 로그인 에이전트 런타임 리소스를 장기간 사용할 수 없습니다.

Blue Prism 서버에 로그인 에이전트 연결을 위해 콜백 연결을 비활성화하려면 어떻게 해야 합니까?

.NET Remoting 연결을 사용하는 경우(권장하지 않음), 로그인 에이전트는 Blue Prism 서버에 콜백 연결을 설정하지 않도록 지시하도록 자동으로 구성됩니다.

WCF 연결을 사용하는 경우 콜백 포트가 사용되지 않습니다.