DATA SHEET

blueprism®
Software Robots - the Virtual Workforce

Secure Windows Authentication for Robots

Blue Prism® robots are securely located in the data center and carry out automated processes on their local device by interacting with the relevant target applications – often via the GUI (graphical user interface).

Robots executing automated business processes will require access to network resources such as file systems and printers, as well as a range of user applications. Unlike desktop-based automation tools, Blue Prism robots do not share a desktop with a human –they will need to be configured with appropriate user account(s) that provide the appropriate privileges to the resources that are used when following a business process.

When operating in this manner, particularly where there are large numbers of robots, it is essential that there is a mechanism for orchestrating secure authentication of these devices onto the network – Blue Prism Login Agent provides this capability.

> Blue Prism Login Agent provides a mechanism where by the credentials used by robots are 100% confidential.

Automated authentication

Blue Prism Login Agent provides a Runtime Resource that is able to receive a login instruction, securely locate the appropriate credential to use from the secure credential store, and instruct the local device to orchestrate an interactive login using official Microsoft Windows functionality.

This enables thousands of Runtime Resources to be instructed to log in to windows using either local or network credentials, to ensure that they are ready to receive work.

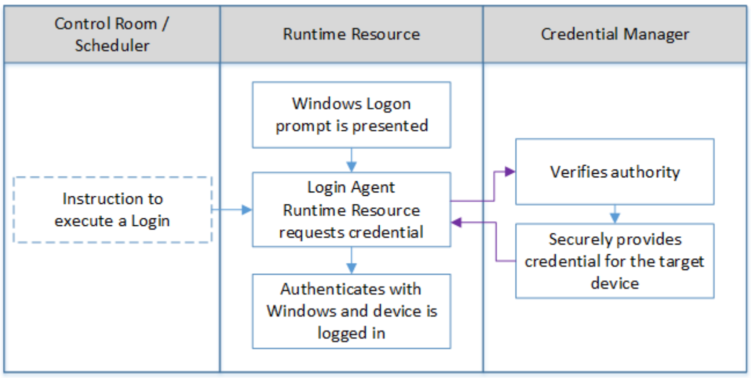
Control Room / Scheduler
Runtime Resource
Credential Manager
Windows Logon prompt is presented
Instruction to execute a Login
Login Agent Runtime Resource requests credential
Verifies authority
Securely provides credential for the target device
Authenticates with Windows and device is logged in

Figure 1: Conceptual representation of log in process

As you would expect, the credentials used by the robots are managed separately and encrypted securely using a customer-defined key. Further information is provided in the **Blue Prism Data Sheet – Credential Manager**.

Aligns with password security management

Many organizations enforce the use of strong passwords, and require users to periodically update them in line with agreed timeframes. Blue Prism Login Agent allows automated processes to be designed which can evaluate when passwords are due to expire, generate a suitably strong password and carry out the password reset.

Because these passwords are only used by robots, the password complexity can be incredibly high, and a situation can be created whereby no human is aware of the password used by any robot.

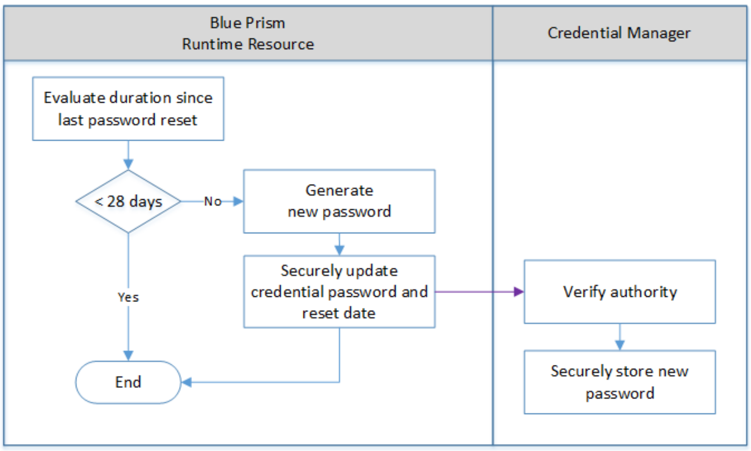
Blue Prism Runtime Resource
Credential Manager
Evaluate duration since last password reset
< 28 days
No
Generate new password
Yes
Securely update credential password and reset date
Verify authority
End
Securely store new password

Figure 2: Conceptual representation of password management

Additional capabilities

In addition to the capabilities outlined above, Blue Prism provides the ability to:

- Design potentially complex log on procedures which can selet which set of user credentials to use based on custom criteria (e.g. time of day, purpose of requesting the log on, machine name etc).
- Configure custom process logic to select the appropriate set of user credentials to use based on custom criteria (e.g. time of day, purpose of requesting the log on, machine name etc).
- Configure custom process logic to define password reset policies.
- Lock/Unlock the device.
- Recognise if the device is logged in.
- Define and retrieve additional memorable information (e.g. mother's maiden name).