This document describes a method of providing secure, controlled windows authentication for virtual machines used for robotic automation. Blue Prism processes typically must operate within a logged on Windows session and, in order to facilitate this, the Blue Prism 'Login Agent' component uses documented Microsoft Windows APIs to:

* Generate, encrypt and regularly update random secure domain passwords for the robot VMs that are not known outside the system
* On Windows start-up, authenticate the resource, and programmatically login using the decrypted password
* On process initiation, programmatically unlock the Windows desktop
* On process completion, programmatically lock the Windows desktop

Login Agent provides this mechanism using either the GINA architecture for Windows XP and below, or the Credential Provider API for Windows Vista and above, for secure, autonomous process execution with a complete audit trail and without risk of unmanaged manual intervention.

## PasswordManagement_gif_1User and Password Management

For each robot resource, at regular intervals, the Windows password of the account being used by the VM should be regenerated. This is encapsulated into a process bundled with the Login Agent software; the basic flow of the process is as described on the right.

A strong, random password is generated and set into a credential, specific to the resource changing its password. Windows is then informed of the password change through the standard password change API, updating its local storage or the Active Directory domain controller as appropriate.

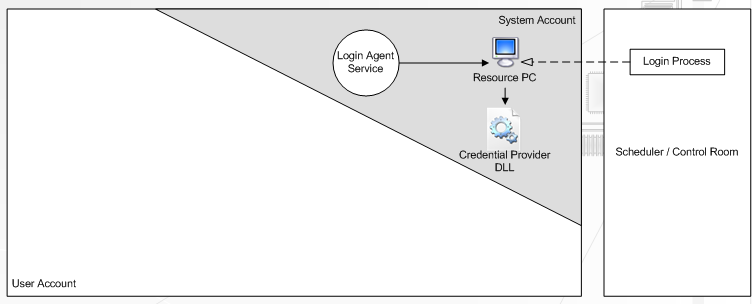
## AccountManagement_gif_1Resource Management

Each VM starts with a resource in its system account. On executing a 'Login' process, initiated by a Blue Prism schedule or Control Room request, it retrieves the VM's specific Windows login credential and passes it to the hosting Windows environment.

At this point the system resource relinquishes control to the resource running in the user account which is used to execute the business processes required of it. These processes can lock and unlock the desktop as appropriate, and can log out of the windows account when completed, passing control back to the resource in the system account, ready for the next login request.

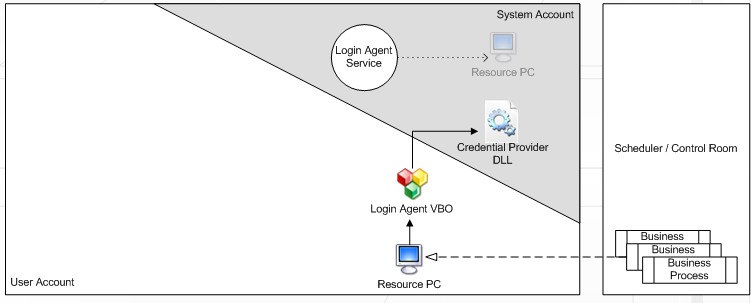
## Login Architecture

### Before Login

On boot, the login agent service starts and runs a Blue Prism resource in the system account. This has no access to user programs.

Using the Scheduler or Control Room within a Blue Prism client, a 'Login Process' is created and executed on the Blue Prism resource. This connects to the credential provider with the encrypted, authenticated login credentials and logs into Windows.

### After Login

****After a successful login, the system account resource is closed. The VM is configured to start a resource PC on login - this will operate within the user account and so will have access to the desktop and user programs to be automated. Sessions can be created and executed on it in the usual manner.

A pre-built 'Login Agent' Visual Business Object is provided with Blue Prism to enable the VM's screen to be locked and unlocked using the stored login credentials.

### Logging Out

A "Logout Process" is created and run on the user account resource while the VM is still logged in. This process will instruct Windows to log out. In doing so, the resource PC is closed down with all other user account applications.

The Login Agent service detects that the user has logged out and starts the resource PC in the system account to await the login process instructing the VM to login once more.