Active Directory Integration

Blue Prism can leverage Active Directory (AD) Domain Services to provide a range of enterprise-strength capabilities including the capability to integrate Blue Prism to use Active Directory for user authentication. In this scenario Active Directory is used to manage and control user access to the Blue Prism platform in line with existing security policies – this is the preferred approach for enterprise deployments. Furthermore Active Directory can be used to provide inter-component message security.

Overview

The Blue Prism Platform should be deployed within an Active Directory Network Infrastructure to enable a number of enterprise-strength capabilities:

- **Message content security and integrity**
  When the Blue Prism components are deployed within an Active Directory Network Infrastructure, and the appropriate domain trusts are in place, communication message security is easily enabled for the necessary inter-component communication.
  Further information on securing connections by enabling message security is provided within the Installation Guide.

- **Single sign-on for the Blue Prism Platform (provided by Active Directory Domain Services)**
  Integrating Blue Prism with Active Directory for single sign-on (SSO) leverages the functionality of Active Directory to authenticate users of the platform. This approach not only simplifies the logon process but also aligns user access controls with existing network security policies.

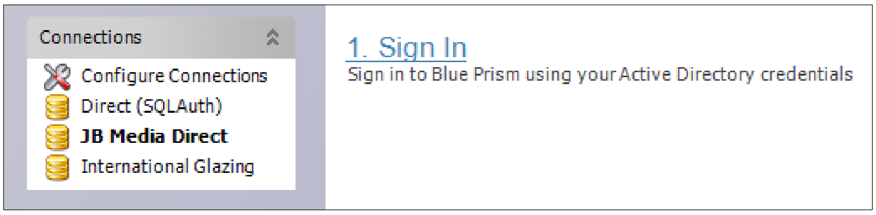
- **Runtime Resources authenticate using a domain account**
  Where the Blue Prism Runtime Resources are configured to authenticate using a domain account, they are able to utilize single sign-on methods to authenticate with the business applications and systems used as part of a process automation.

Benefits of Single Sign-on for the Blue Prism Platform

Blue Prism integration with Active Directory Domain Services for single sign-on is enabled as part of the installation procedure. It leverages the open standard Lightweight Directory Access Protocol (LDAP) to negotiate access to directory services and provide user authentication for the platform.

Single sign-on enables Active Directory to automatically validate the logged in user and establish if they have been granted the appropriate rights to access the Blue Prism platform.

Configuring Blue Prism to use Active Directory for single sign-on simplifies the administration and maintenance associated with managing large numbers of users across multiple environments whilst also ensuring that existing security policies are applied.



Sign in to Blue Prism using your Active Directory credentials

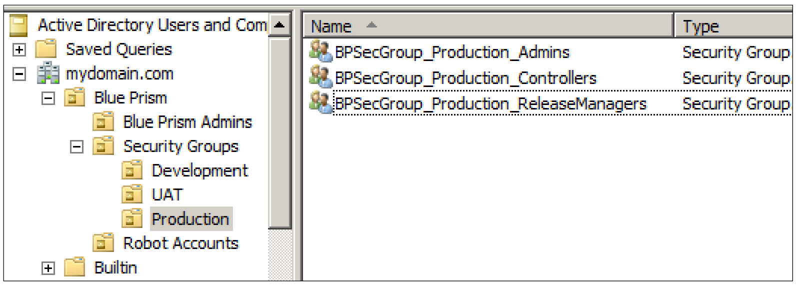
Using centralized authentication allows access rights to be managed, maintained and audited within a central function and adds an additional layer of security that is independent of the platform. This places Blue Prism access control in the hands of the network administrators and provides a familiar and trusted mechanism for restricting access to important software.

Configuring Active Directory Integration for Single Sign--on

Integration with Active Directory is configured for specified instances of Blue Prism allowing full segregation of roles across multiple environments (e.g. Development, Test and Production).

The following steps are required for managing user access to Blue Prism with Active Directory:

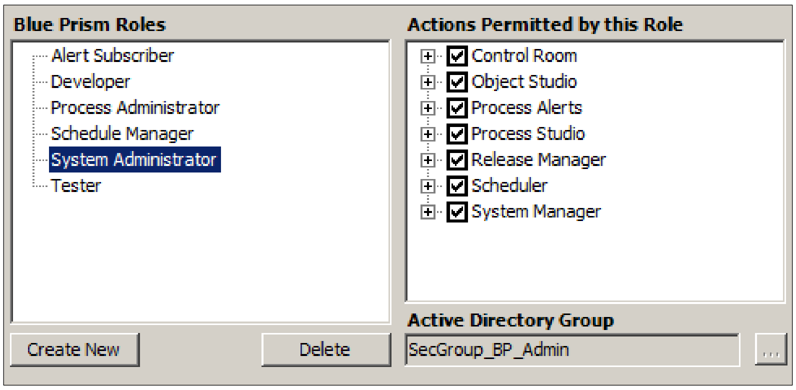
- **Configure Active Directory Security Groups**
  Activity Directory Security Groups are required to represent the user roles that will be available within the Blue Prism environment. The domain users that require access to the Blue Prism platform should then be added to the respective groups.



Active Directory Users and Com
⊞ Saved Queries
⊟ mydomain.com
  ⊟ Blue Prism
    Blue Prism Admins
    ⊟ Security Groups
      Development
      UAT
      Production
    Robot Accounts
  ⊞ Builtin

Name	Type
BPSecGroup_Production_Admins	Security Group
BPSecGroup_Production_Controllers	Security Group
BPSecGroup_Production_ReleaseManagers	Security Group

- **Configure and map the Blue Prism Roles with AD Security Groups**
  A number of pre-configured security roles are provided within Blue Prism - there is also the option to customize or add new custom roles to suit the organization. Within Blue Prism each role is aligned with the appropriate Active Directory Security Group to provide the members of the respective group with the related permissions.



Blue Prism Roles

- Alert Subscriber
- Developer
- Process Administrator
- Schedule Manager
- System Administrator
- Tester

Actions Permitted by this Role

- ⊞ ☑ Control Room
- ⊞ ☑ Object Studio
- ⊞ ☑ Process Alerts
- ⊞ ☑ Process Studio
- ⊞ ☑ Release Manager
- ⊞ ☑ Scheduler
- ⊞ ☑ System Manager

Active Directory Group: SecGroup_BP_Admin

Benefits of Runtime Resources authenticating using a domain account

The Blue Prism Runtime Resources (often referred to as robots) are responsible for executing the processes designed and configured within the platform. Typically processes will require interaction with various applications and systems, some of which may be integrated with Active Directory for single sign-on (SSO). Using a domain account to authenticate the Runtime Resources against the network allows a process to authenticate with relevant target systems using single sign-on. This simplifies the security model and accelerates development.

Additional benefits of using a domain account to authenticate a Runtime Resource include:

- Enforces existing security policies for the Runtime Resources (e.g. password reset and complexity requirements).
- Allows Active Directory Group Policy Objects (GPO) to be used to enforce user specific settings.
- Provides auditability and control of the accounts via Active Directory.
- Simplifies access to network resources such as shared drives, mailboxes, printers etc.