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 recommended approach for enterprise deployments. Furthermore, Active Directory can be used to provide inter-component message security.

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 configured with appropriate domain trusts, communication message security is enabled by default for the necessary inter-component communication.
  Further information on securing connections by enabling message security is provided within the *Securing Network Connectivity Data Sheet*.
- **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 validate users' access to 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 use 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 to the platform.

Single sign-on enables Active Directory to automatically validate the logged-in user with their account within the domain with which Blue Prism is associated 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.

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.

Single sign-on for Blue Prism requires users' Active Directory accounts, Blue Prism server(s), and all Blue Prism devices that will be accessed by users (i.e. the interactive clients, and possibly the runtime resources) to be in domains that directly reside within a single or multiple Active Directory forests.

Benefits of Runtime Resources authenticating via domain accounts

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 such as 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.

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 such as Development, Test, and Production.

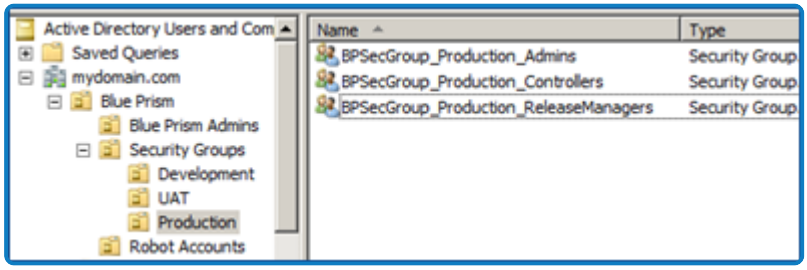
Blue Prism provides two environments for managing Active Directory authentication to the platform:

- **Single-authentication environment** – Supports Active Directory accounts where roles are mapped to Active Directory security groups. In single-authentication environments, Active Directory users can be contained within multiple domains but only a single forest.
- **Multi-authentication environment** – Supports Active Directory accounts where roles are mapped to individual users in Blue Prism. In multi-authentication environments, Active Directory users can be contained in multiple domains and multiple forests. This environment type also supports Blue Prism native authentication (see the Authentication in Blue Prism topic in the online help for more details). This is the latest and recommended environment for enterprise deployments.

Active Directory configuration in a single-authentication Blue Prism environment

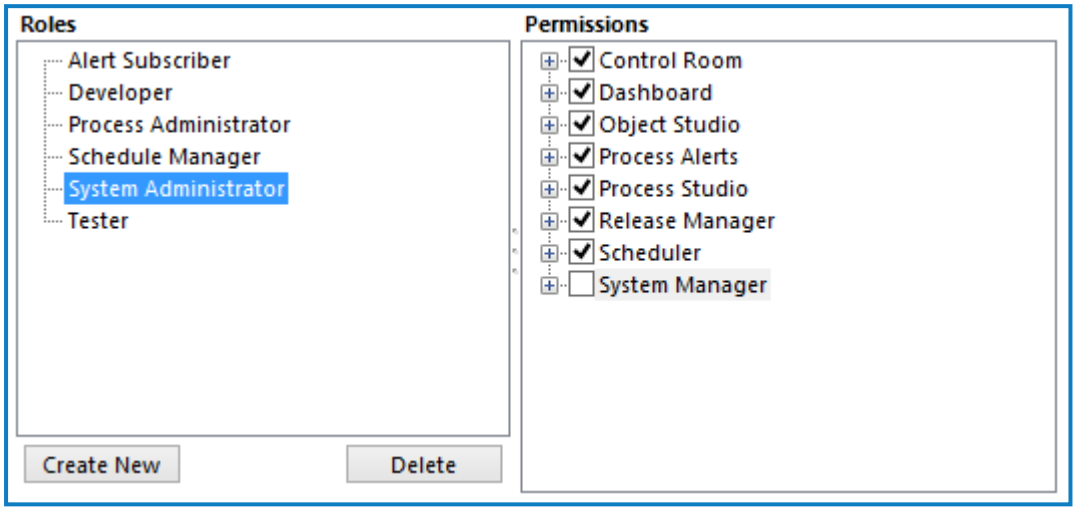
The following steps are required for managing user access to Blue Prism with single-authentication Active Directory:

1. **Configure Active Directory security groups** – Security groups should be set up in Active Directory to reflect each user role in a Blue Prism environment. The users within the domain should then be added to the relevant security group.



2. **Specify the domain that hosts the Active Directory security groups** – Blue Prism will be configured with the domain where the Active Directory security groups will reside. Only security groups in the specified domain can be associated with a Blue Prism user role, however users from any domain within the common Active Directory forest can be assigned to these security groups. They can either be direct members of this group, or be granted membership via a nested group. As part of the configuration it is necessary to select which Active Directory security group users should be members of in order to grant them System Administrator rights.

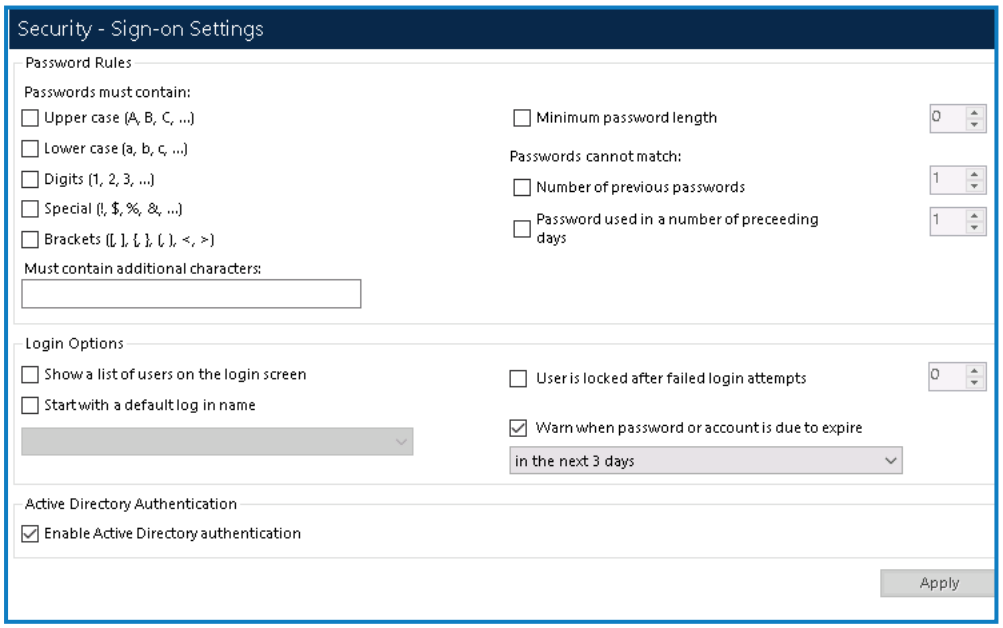
3. **Configure and map the Blue Prism roles to Active Directory security groups** – The pre-configured Blue Prism user roles can then be edited or amended, and new roles can also be added. Each active role in a given Blue Prism environment will then be mapped to an existing Active Directory security group within the configured domain.



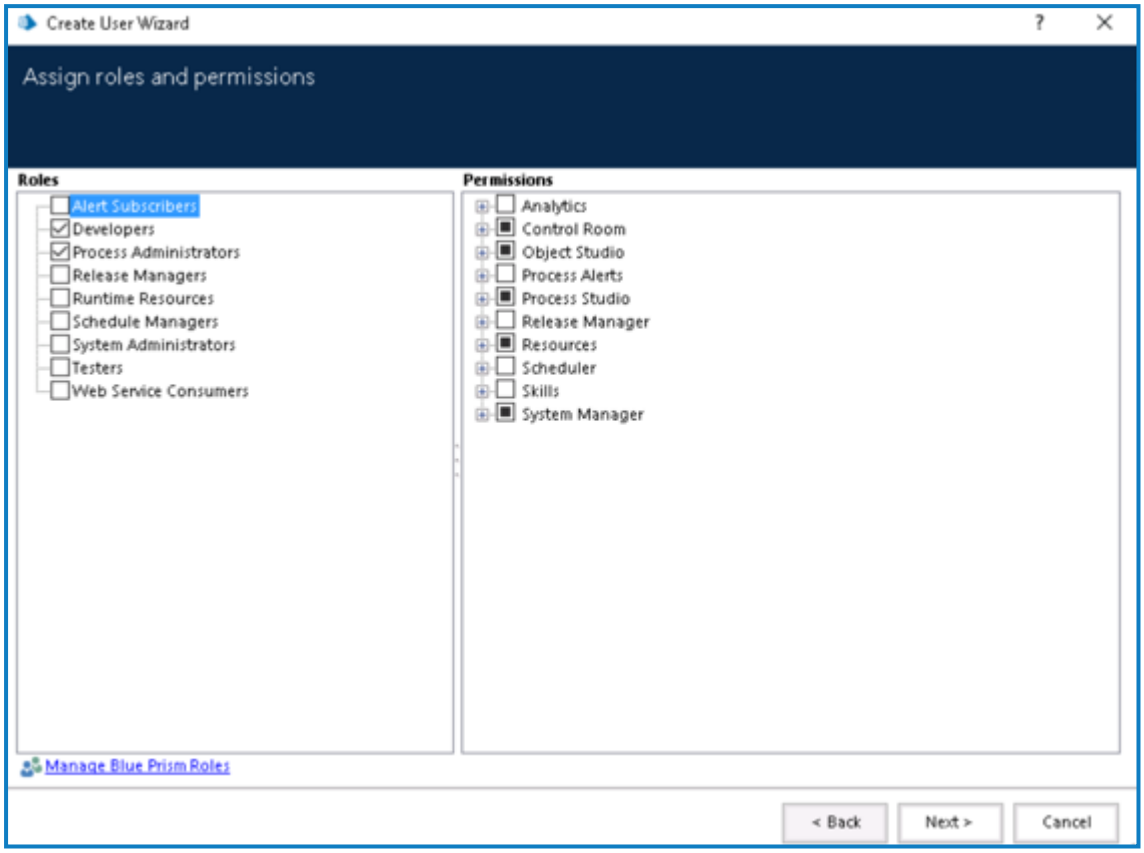
Active Directory configuration in a multi-authentication Blue Prism environment

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

1. **Enable Active Directory authentication in Blue Prism** – Blue Prism administrators who are members of an Active Directory domain must enable Active Directory authentication in Blue Prism before mapping Active Directory users to Blue Prism roles.



2. **Map Active Directory users to Blue Prism roles** – Active Directory users are retrieved from the Active Directory domains and forests and mapped individually to Blue Prism roles via the Create new user wizard in Blue Prism.



For further details, see Single Sign-on.