Active Directory integration with Blue Prism

Blue Prism supports single sign-on (SSO) using Microsoft Active Directory Domain Services. This enables users who have been authenticated by the operating system, and who are members of appropriate domains and forests, to log into Blue Prism without resubmitting their credentials.

Blue Prism provides two types of environments for managing Active Directory (AD) authentication to the Blue Prism Cloud platform:

- **Multi-authentication environment** – this option 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.
- **Single-authentication environment** – this option 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.

  In previous versions of Blue Prism, this option was referred to as Active Directory Single Sign-On authentication.

By default, Blue Prism Cloud platforms are configured as multi-authentication environments.

Prerequisites

- All virtual machines (VMs) on the Blue Prism Cloud platform must be domain joined to your organization's domain.
- Given the VMs are domain joined, the user that enables the AD authentication must be logged in with a domain account.

AD integration in a multi-authentication environment

For a high-level overview covering how to enable AD integration/SSO in a multi-authentication Blue Prism environment, see Multi-authentication Active Directory. More detailed steps are provided below:

1. Check that AD authentication is enabled under System > Security - Sign-on Settings. For information on how to do this, see Active Directory configuration in a multi-authentication Blue Prism environment.
2. Create and map your domain users using the Create User Wizard. For information on how to do this, see Create one or more Active Directory users in a multi-authentication environment.

3. Raise a request for the Blue Prism Cloud Operations team to change the connection mode on IO1 (Production App Server) and IO2 (Development App Server) Blue Prism Servers, in the Blue Prism client on Management Server, and in the Blue Prism client on the digital workers.

   Blue Prism Cloud Operations will carry out this change for you. For reference, the following information is available:

   - For information on changing the connection mode on the Blue Prism Servers, see Blue Prism server.

     There are three supported connection modes available. By default, **WCF: SOAP with Transport Encryption and Windows Authentication mode** is used.

   - For information on changing the connection mode on the Management Server and digital worker Blue Prism clients, see Connections.

4. Following the changes by the Blue Prism Cloud Operations team, you should validate that the Blue Prism login screen displays a **Sign in using Active Directory** button. If it does not, go back through the steps and ensure everything is setup correctly.

   For an example of the login screen with the button is shown below: