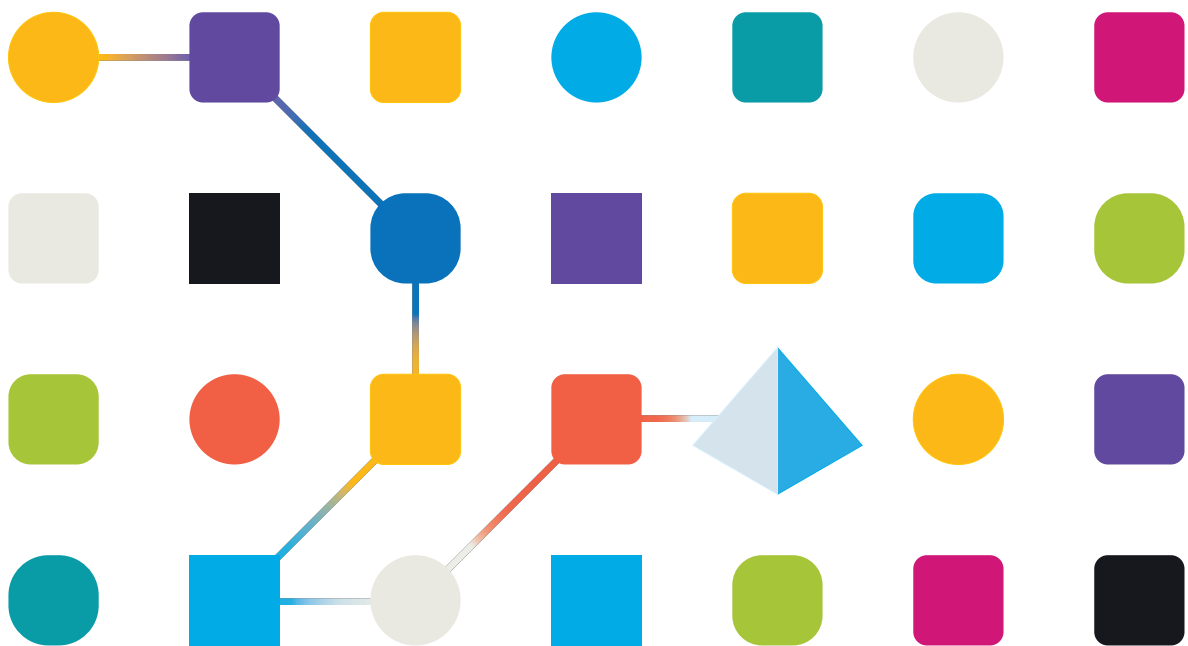




# Blue Prism 7.0

## Active Directory Integration

Document Revision: 3.0



## Trademarks and Copyright

The information contained in this document is the proprietary and confidential information of Blue Prism Limited and should not be disclosed to a third-party without the written consent of an authorized Blue Prism representative. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying without the written permission of Blue Prism Limited.

### © Blue Prism Limited, 2001 – 2023

“Blue Prism”, the “Blue Prism” logo and Prism device are either trademarks or registered trademarks of Blue Prism Limited and its affiliates. All Rights Reserved.

All trademarks are hereby acknowledged and are used to the benefit of their respective owners. Blue Prism is not responsible for the content of external websites referenced by this document.

Blue Prism Limited, 2 Cinnamon Park, Crab Lane, Warrington, WA2 0XP, United Kingdom.  
Registered in England: Reg. No. 4260035. Tel: +44 370 879 3000. Web: [www.blueprism.com](http://www.blueprism.com)

# Contents

- Active Directory integration** ..... 4
- Benefits of Single Sign-on for the Blue Prism platform** ..... 5
  - Benefits of runtime resources authenticating via domain accounts ..... 5
- Configure Active Directory integration for Single Sign-on** ..... 6
  - Active Directory configuration in a single-authentication environment ..... 7
  - Active Directory configuration in a multi-authentication environment ..... 9
  - Database conversion ..... 10
  - Runtime resource authentication ..... 11
  - Supported connection modes ..... 11
  - User refresh ..... 12
- Troubleshooting – Single sign-on** ..... 13
  - Users can't sign in ..... 13
  - Windows credentials are required ..... 13
  - Error messages display ..... 13

# 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 in the [Blue Prism Network Connectivity](#) 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 validate users' access to the platform. This approach not only simplifies the login 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.

Additionally, using centralized authorization 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

Blue Prism runtime resources 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.

## Configure Active Directory integration for Single Sign-on

Blue Prism supports single sign-on using Microsoft Active Directory Domain Services, which allows 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. 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 types of environments for managing Active Directory authentication to the platform:

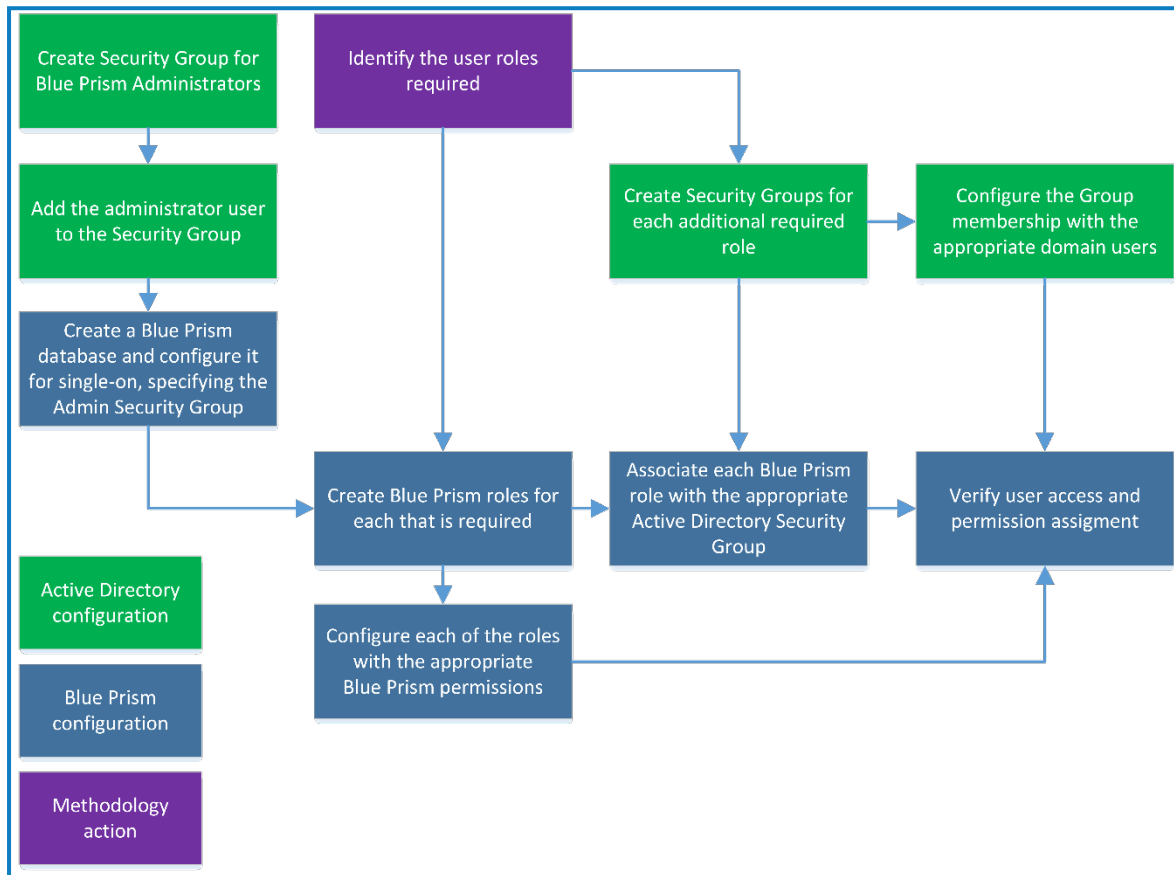
- **Multi-authentication environment** – supports Active Directory accounts where roles are mapped to individual users in Blue Prism. In multi-authentication environments, Active Directory users can be contained in multiple domains and multiple forests.
- **Single-authentication environment** – referred to as *Active Directory Single Sign-On* authentication in previous versions of Blue Prism, it 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.

The environment type is selected when the [database is created](#) and it can only be changed when [converting](#) a single-authentication Active Directory environment to a multi-authentication Active Directory environment.

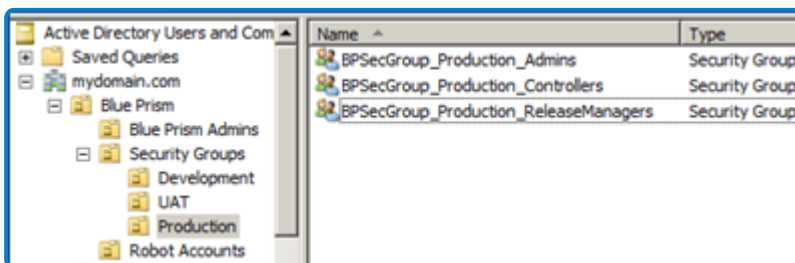
## Active Directory configuration in a single-authentication environment

Where Blue Prism is deployed within a single Active Directory forest, it can be configured to allow users to authenticate against the platform using single sign-on. It essentially requires an Active Directory security group to be mapped to each relevant Blue Prism role after which users will be granted access to the platform based on their Active Directory security group membership.

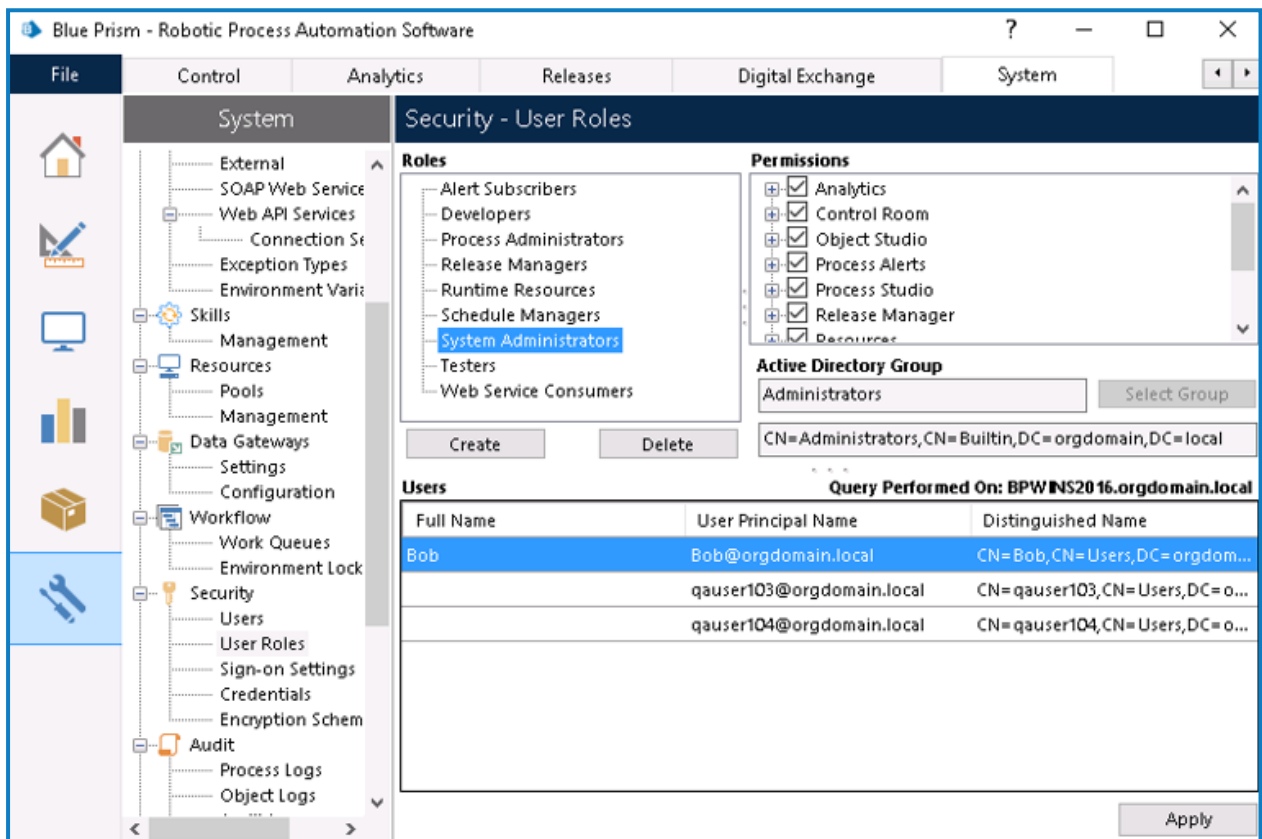
The steps required to configure Blue Prism integration with Active Directory for single sign-on in a single-authentication environment are illustrated in the diagram below:



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 must 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 before granting 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 be edited if required, and new roles can also be added. Each active role in a given Blue Prism environment must then be mapped to an existing Active Directory security group within the configured domain.



Blue Prism roles must be associated with security groups created in Active Directory. Single sign-on for Blue Prism does not support built-in groups or those with derived membership such as domain users or authenticated users. It is also recommended that the security groups used do not contain Foreign Security Principals.

Users who belong to the groups that have been configured should now be able to log into Blue Prism and perform the actions permitted by the corresponding Blue Prism role. Users may have to log out of Windows and log back in again for Active Directory changes to take effect.



## Active Directory configuration in a multi-authentication environment

The following steps are required for managing Active Directory user access to a multi-authentication environment:

1. **Enable Active Directory authentication in Blue Prism** – Blue Prism administrators who are members of an Active Directory domain must enable Active Directory authentication on the Security - Sign-on Settings screen in Blue Prism before mapping Active Directory users to Blue Prism roles.

**Security - Sign-on Settings**

**Password Rules**

Passwords must contain:

- Upper case (A, B, C, ...)
- Lower case (a, b, c, ...)
- Digits (1, 2, 3, ...)
- Special (!, \$, %, &, ...)
- Brackets ([, ], {, }, (, ), <, >)

Must contain additional characters:

Minimum password length:

Passwords cannot match:

- Number of previous passwords:
- Password used in a number of preceding days:

**Login Options**

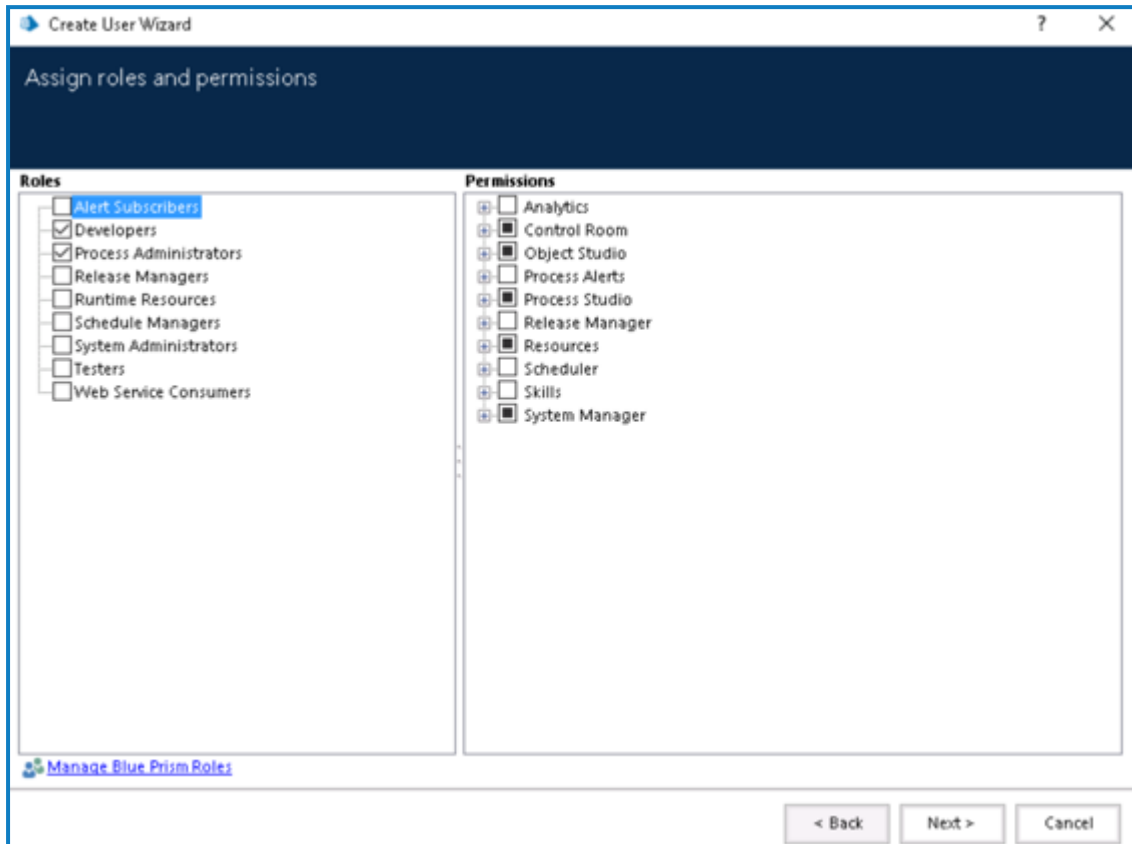
- Show a list of users on the login screen
- Start with a default log in name:
- User is locked after failed login attempts:
- Warn when password or account is due to expire:

**Active Directory Authentication**

- Enable Active Directory authentication

Apply

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 User Wizard](#) in Blue Prism.



## Database conversion

Blue Prism administrators can convert a single-authentication Active Directory database to a multi-authentication Active Directory environment. This is a one-way irreversible operation which converts all single-authentication accounts in a Blue Prism environment to multi-authentication accounts, automatically mapping roles to individual users based on their Active Directory security group membership (after which group membership is no longer relevant).

This feature is available in the [single sign-on settings](#) for administrators using the single-authentication environment.

Before starting the conversion please ensure:


- you are using one of the [supported connections](#) for Active Directory authentication.
- you have backed up your database.
- you have stopped all processes.
- all users and runtime resources are logged out of the environment.

After closing down any runtime resources the administrator will need to wait two minutes before they are able to perform the conversion, otherwise they will be reminded that all users must be logged out before they can proceed with the conversion.



Please be aware that depending on the number of users you are converting and any potential latency, the database conversion might take a few minutes.

When converting a single-authentication Active Directory environment to a multi-authentication Active Directory environment, administrators are prompted to create a recovery administrator user that uses Blue Prism native authentication. A native user with a secure password is required during the conversion process as Active Directory users in a multi-authentication environment cannot update an expired license using Active Directory credentials, since a Blue Prism server cannot be started with an expired license and Active Directory users cannot sign in to this environment using a direct SQL server database connection.

 This user can be removed once the database conversion has completed, however it is recommended to retain it for troubleshooting purposes, particularly in environments where all administrator accounts use multi-authentication Active Directory.

For more information on managing multi-authentication user accounts, see [Manage users](#).

## Runtime resource authentication

Runtime resources can authenticate via Active Directory either in a multi-authentication or single-authentication environment by passing the /sso switch in the command line at resource start-up. The `/sso` switch supports only the client/server [connection modes](#) mentioned above.

Authentication occurs using the currently logged-in Windows user's credentials. In a multi-authentication environment, the runtime resource inherits the Blue Prism user roles mapped to the currently logged-in Windows user. In a single-authentication environment, the runtime resource inherits the Blue Prism roles mapped to the Active Directory security groups to which the currently logged-in Windows user has been assigned.

## Supported connection modes


Only the following client/server connection modes are supported for Active Directory authentication:

- WCF: SOAP with Message Encryption and Windows Authentication,
- WCF: SOAP with Transport Encryption and Windows Authentication
- .NET Remoting: Secure.

## User refresh

Clicking **Refresh User List** will update the list of Active Directory users under [Security - Users](#) to include any new users who are members of the appropriate Active Directory security groups (as configured in [Blue Prism roles](#)).

Any users who were previously registered with Blue Prism but have been deleted or deactivated in Active Directory will be marked as inactive. Inactive users do not initially appear in the user list but can be made visible by right-clicking the users list and selecting **Show All Users**.

 The user list is updated automatically so when a user attempts to log in, they are validated against the Active Directory in real-time regardless of whether the user list has been refreshed or not.

## Troubleshooting – Single sign-on

This page describes some common issues and suggested resolutions for system administrators using and managing [Single Sign-on](#) in Blue Prism.

### Users can't sign in

If login failures or performance issues are encountered during the login process via Active Directory, system administrators can check whether any of the scenarios below apply and perform the appropriate action.

#### If using Active Directory authentication in a single-authentication environment

- **Log out and back again** – If all user settings, including security groups are correct, try logging out and logging on again to the user's machine. When a user is added to an Active Directory group, the change takes effect the next time they log on.
- **Check the user's Blue Prism roles and their Active Directory security group membership** – If the user is a member of the Blue Prism Administrators group (as configured in the [single sign-on settings](#), they should be able to sign in.

Check that the user is a member of at least one of the Blue Prism security groups in Active Directory. Check which Active Directory groups are mapped to the [Blue Prism roles](#) in System Manager.

#### If using Active Directory authentication in a multi-authentication environment

- **Check the Blue Prism application server connection** – Make sure the user is connected to a Blue Prism application server with a valid and secure [connection mode](#) and that an Active Directory user record exists for the currently logged-in Windows user.

#### If converting a single-authentication Active Directory environment to a multi-authentication Active Directory environment

You should use a supported connection for Active Directory authentication before starting the conversion. If you haven't used a supported connection for Active Directory authentication before doing the conversion you will not see the Active Directory sign-in option on the Blue Prism login page and you will have to change your connection to a supported connection to be able to log back into the system.

### Windows credentials are required

If after signing in via Active Directory, you are prompted to enter Windows credentials, please check that you have configured a Service Principal Name (SPN) against the Active Directory account under which each Blue Prism Server service instance is running . For more details, see [SPN configuration](#).

### Error messages display

#### *The trust relationship between this workstation and the primary domain failed.*

This error indicates a problem with your network configuration. It can sometimes be a symptom of a disjointed namespace (a scenario in which a computer's primary domain name system (DNS) suffix doesn't match the DNS domain name where that computer resides).


*The specified domain does not exist or cannot be contacted.*

Sometimes a machine can appear to be a member of a domain, but badly configured. If this only happens from a specific machine, whereas other machines work without problems then this may be the problem. In this case, remove the machine from the domain and reattach it (a Domain administrator will need to carry out this action).

*The local machine is not a member of an Active Directory domain, or the domain cannot be contacted.*

If you receive this message when attempting to enable Active Directory authentication in a multi-authentication environment, this means that you need to request your Active Directory domain administrator to add you to an Active Directory domain before you can configure Active Directory authentication.

*Unable to retrieve the members of Security Group {Security Group Name} because it contains members which are either Foreign Security Principals or have unresolved SIDs.*

 This only applies to Active Directory authentication in a single-authentication environment.

Some Active Directory security groups (for example, some built-in groups) present querying difficulties and therefore such configurations are not recommended. Whilst users from these groups will be able to sign in with the correct permissions, some Blue Prism screens may not be able to accurately display membership information.