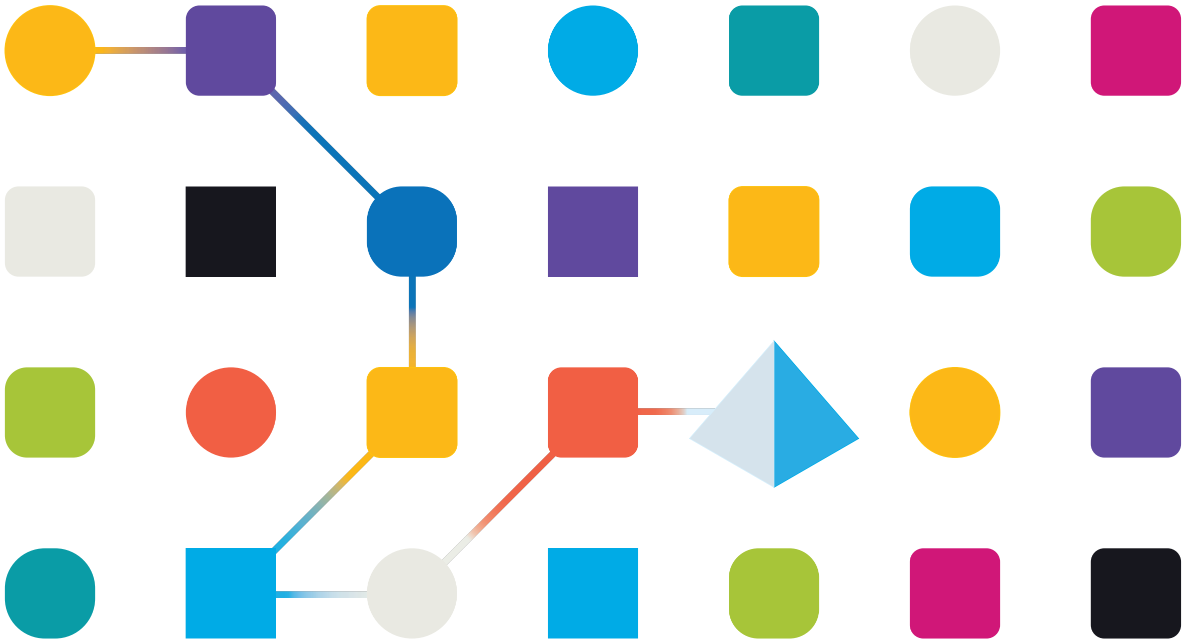
Blue Prism 7.2

Active Directory Integration

Document Revision: 1.0



Trademarks and Copyright

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

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

Supported Active Directory infrastructure 6

- Single forest trust 7
- Two-way forest trust 7
- One-way outgoing forest trust 7
- Two-way external trust 8
- One-way outgoing external trust 9

Configure Active Directory integration for Single Sign-on 10

- Active Directory user authentication 10
- Runtime resource authentication 11
- Supported connection modes 11
- Synchronize users with Active Directory 12

Configure Active Directory domains 13

- Prerequisites 13
- Add a domain 13
- Edit a domain 14
- Delete domains 14
- Trust relationships between domains 15

Troubleshooting – Single sign-on 16

- Users can't sign in or performance issues occur during login 16
- Windows credentials are required 19
- Error messages display 19

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 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.

Supported Active Directory infrastructure

Blue Prism supports authentication/authorization for multiple Active Directory domains within a single forest or across multiple forests, provided the correct forest trusts and domain trusts are established. The following diagrams provide examples of some of the different trusts that are supported:

- Single forest trust on the next page
- Two-way forest trust on the next page
- One-way outgoing forest trust on the next page
- Two-way external trust on page 8
- One-way outgoing external trust

The diagrams show the Active Directory domains that could be used as part of the authentication/authorization process, for example, domains which:

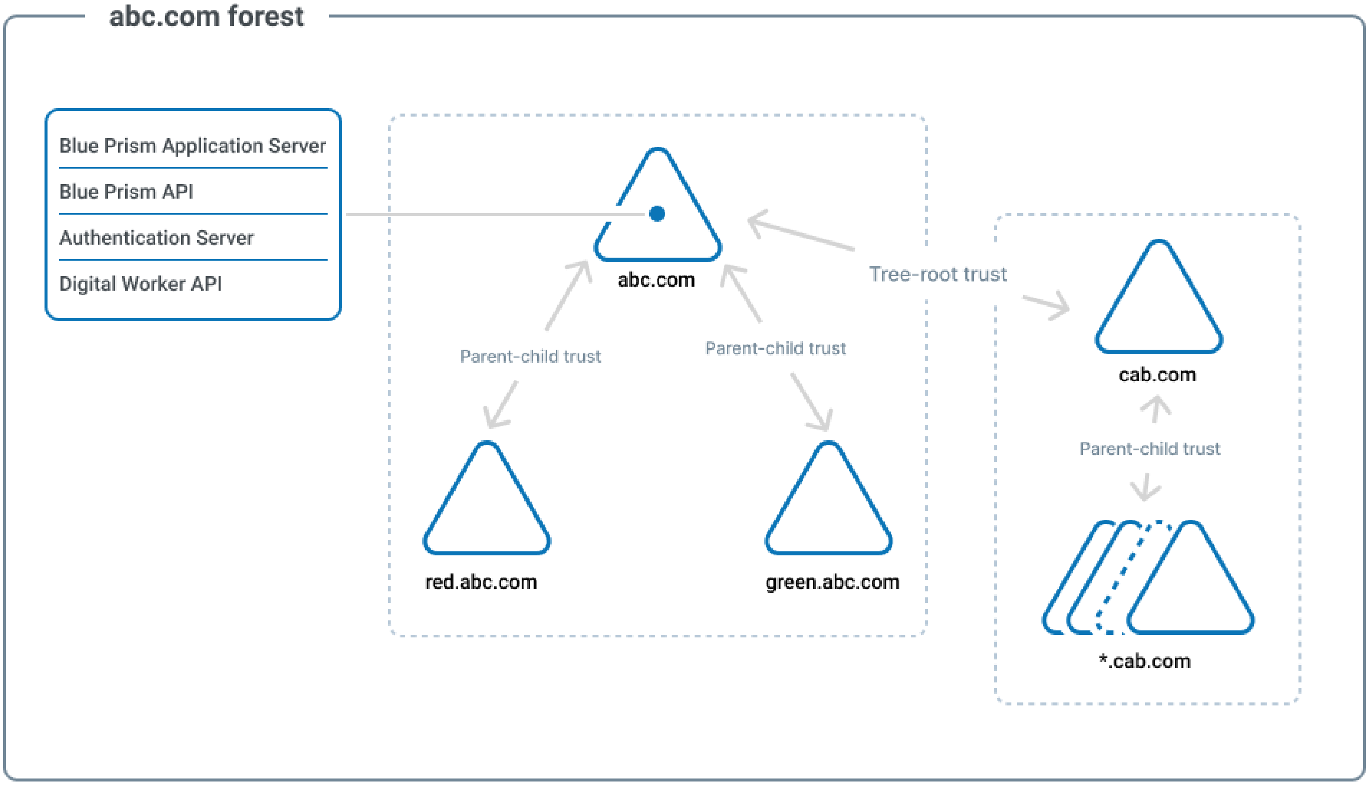
- Contain Active Directory users that need to authenticate in Blue Prism.
- Contain security groups that are assigned directly to roles in Blue Prism.
- Contain any parent security groups which include security groups directly assigned to roles in Blue Prism.

By default, the Blue Prism applications requiring authentication/authorization will discover the available domains by traversing the forest trusts and domain trusts. However, it is also possible to explicitly configure which of the trusted domains you want to include in your authentication/authorization process. For more information, see Check if you need to manually configure Active Directory domains that will be queried during the login process.

> The blue dot in all diagrams represents the Active Directory domain where Blue Prism applications are installed, for example, Blue Prism Application Server, Blue Prism API, Authentication Server, or Digital Worker API.

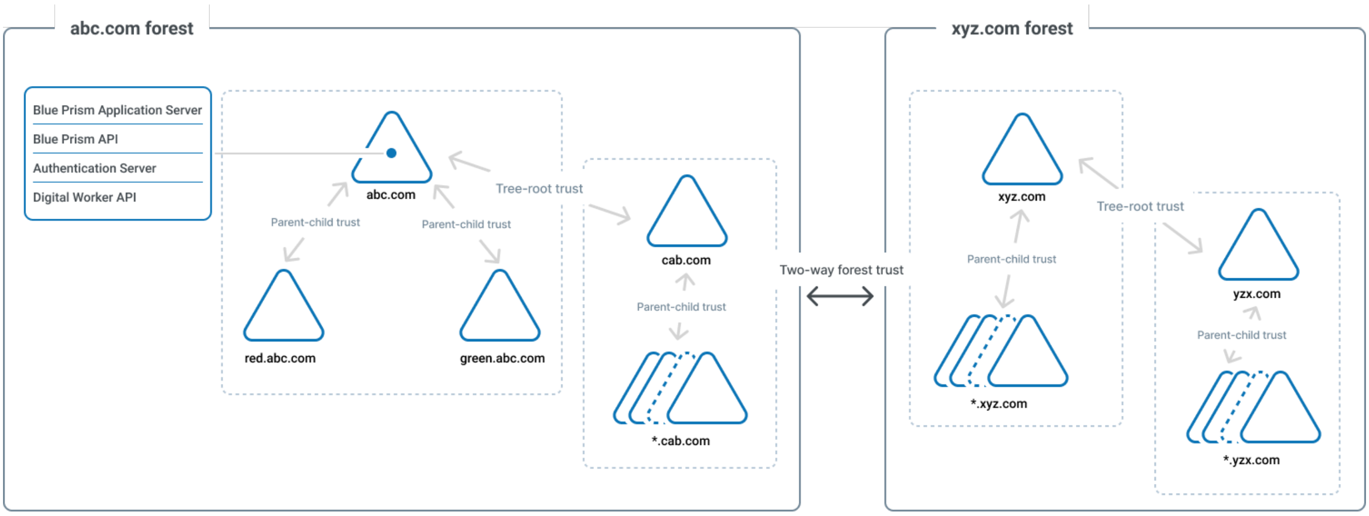
Single forest trust

Within a single forest, all trusts are two-way transitive trusts. As a result, all the domains within the forest can be used as part of the authentication/authorization process.



Two-way forest trust

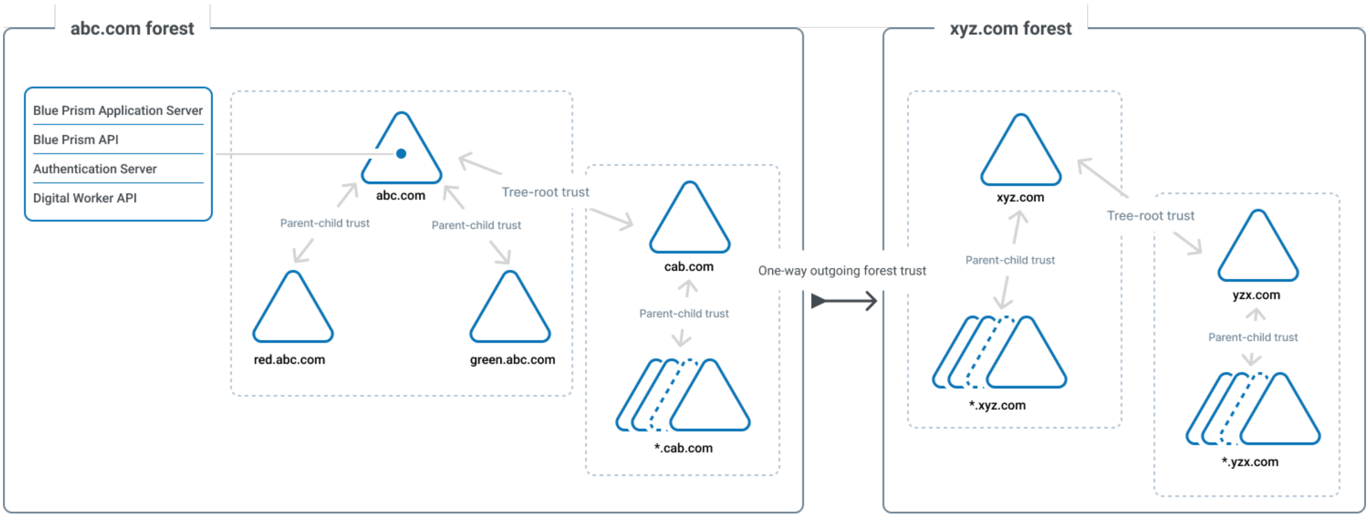
Two-way forest trusts are transitive as well. As a result, all of the domains within the trusted forest can be used as part of the authentication/authorization process.



One-way outgoing forest trust

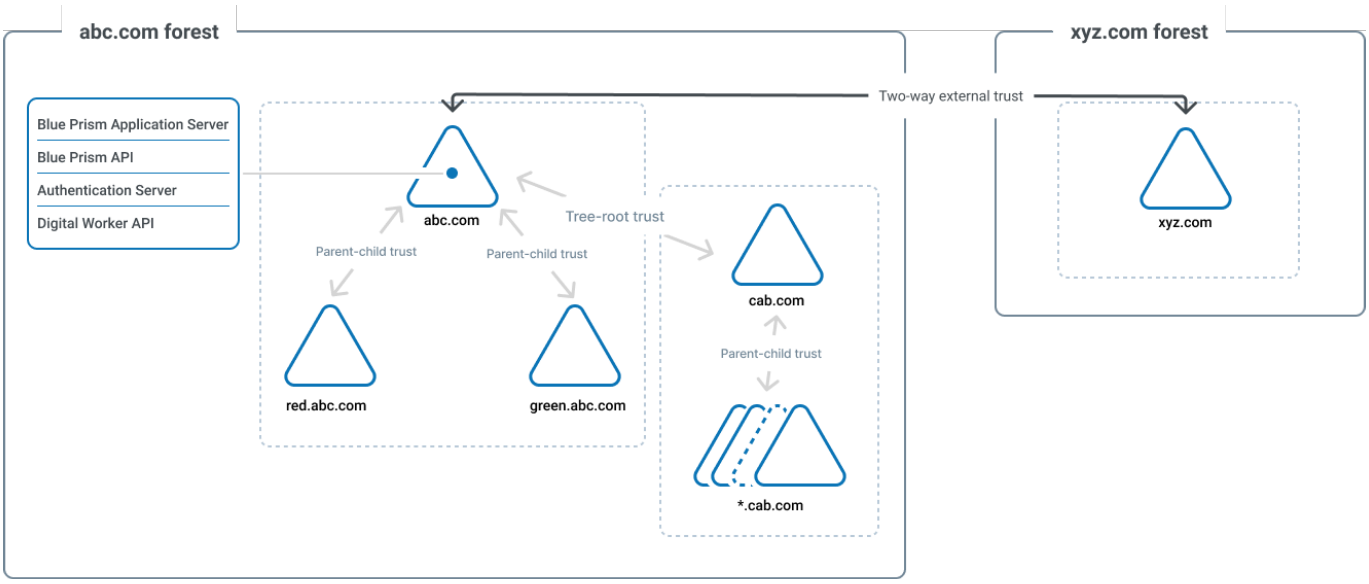
If the forest where the Blue Prism applications are installed has an outgoing transitive trust to another forest, all domains in the trusted forest can be used as part of the authentication/authorization process.

However, domain credentials must be provided for each of the domains in the trusted forest so that the Blue Prism applications can query those domains. For more information, see Configure Active Directory domains on page 13.



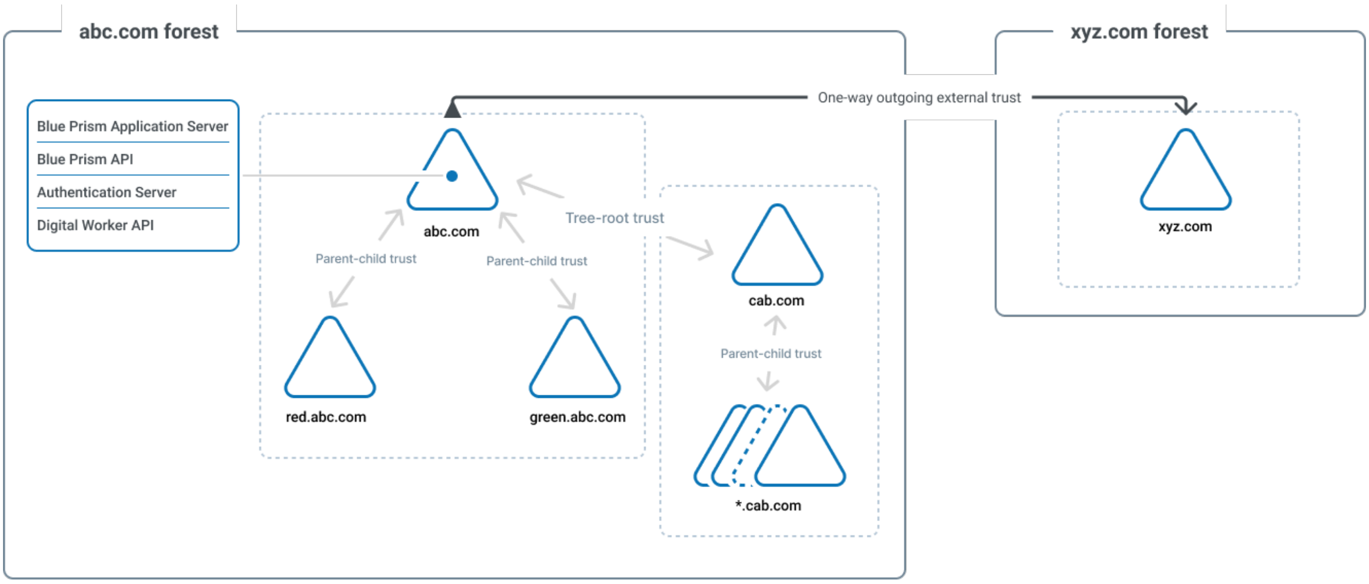
Two-way external trust

A non-transitive external trust can be set up between domains in different forests. This trust only allows the specific domain from that forest to be used as part of the authentication/authorization process.



One-way outgoing external trust

The one-way outgoing external trust behaves the same way as the two-way external trust, however, domain credentials must be provided for the external domain so that the Blue Prism applications can query those domains. For more information, see Configure Active Directory domains on page 13.



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.

When using Active Directory single sign-on in Blue Prism, it is possible to configure the system to support users from across multiple forests within a common Active Directory network infrastructure with options for role management either in Blue Prism or Active Directory, or both.

This applies to the following scenarios:

- Active Directory users logging into the interactive client via Authentication Server.
- Active Directory users logging into the interactive client using built-in authentication.
- Authentication of AutomateC commands, runtime resources, and process alerts via the `/sso` command line parameter.
- Authentication of telnet commands and web service requests.

Active Directory user authentication

The following prerequisites must be met before configuring Active Directory authentication in Blue Prism:

- The local machine on which the Blue Prism interactive client is installed and on which the Blue Prism administrator is logged on must be a member of an Active Directory domain.
- All devices must be connected via a Blue Prism application server with a secure connection mode.
- If using multiple Active Directory domains, the appropriate credentials for each relevant . Active Directory domain must be configured in Blue Prism.

The following configuration must be carried out to enable Active Directory user authentication in Blue Prism:

- The Blue Prism administrator must enable **Active Directory authentication** and select at least one of the role management options for Active Directory users on the System > Security - Sign-on Settings screen in the Blue Prism interactive client:
  - **Manage role membership in Blue Prism** – Active Directory users are directly assigned to Blue Prism roles.
  - **Manage role membership in Active Directory** – Active Directory security groups are mapped to Blue Prism roles. Users are assigned the relevant Blue Prism roles based on their Active Directory security group membership when they log in.
- Depending on the role management option(s) selected on the Security - Sign-on Settings screen, Active Directory users must be created in Blue Prism by:
  - Manually creating users and directly assigning them roles and permissions via the Create user wizard, and/or
  - Assigning Active Directory security groups to Blue Prism roles via the Role Membership dialog. Blue Prism user accounts for users belonging to Active Directory security groups are created either when they log into Blue Prism for the first time, or when administrators manually synchronize users with Active Directory on the Security - Users screen.

> Active Directory authentication in Blue Prism does not support built-in security groups or those with derived membership such as domain users or authenticated users.

Active Directory can be integrated with both Blue Prism and Authentication Server. Authentication Server users configured to use Active Directory authentication in Hub can also be added to Blue Prism based on their Active Directory security group membership. For more details, see Add Active Directory users to Blue Prism based on their security group membership and the Hub administrator guide.

Runtime resource authentication

Runtime resources can authenticate via Active Directory 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. The runtime resource inherits the Blue Prism user roles mapped to the currently logged-in Windows user.

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.

Synchronize users with Active Directory

Clicking **Synchronize users with Active Directory** 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) and to reflect any changes made to existing users in Active Directory. An Active Directory's user details are refreshed in Blue Prism from Active Directory every time they log into Blue Prism, however administrators can refresh the details of all Active Directory users in the user list by selecting this option.

When this option is selected:

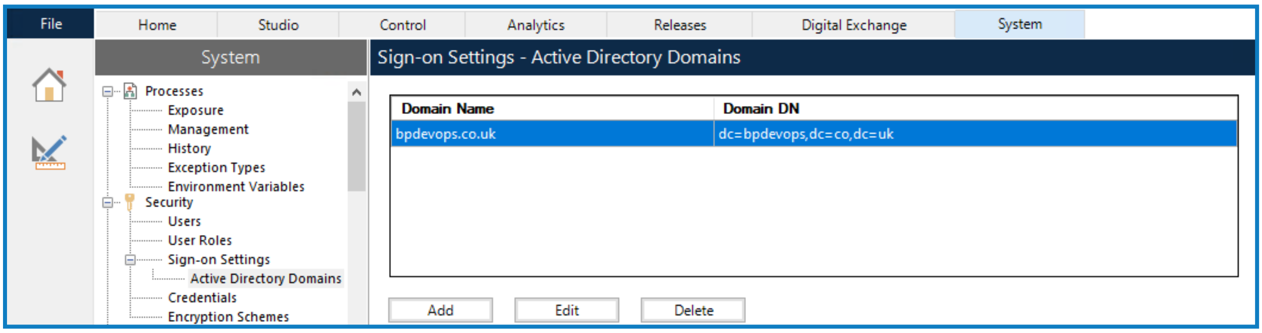
- Any new Active Directory user accounts assigned to a security group which is mapped to a Blue Prism role will display in the Blue Prism user list.
- Any user accounts disabled in Active Directory will be marked as deleted in Blue Prism. If a previously disabled account has been re-enabled in Active Directory, it will display in the Blue Prism user list again.
- Any user accounts deleted from Active Directory will be marked as deleted in Blue Prism, but they can no longer be reinstated.
- Any updates to a user’s Distinguished Name or UPN in Active Directory will display in Blue Prism. If the UPN is updated, the user’s username will be updated accordingly.

A dialog displays the progress of the synchronization process. Administrators are prevented from closing the dialog until the process completes. Once the process has completed, a summary displays the total number of synchronized accounts and the associated actions.

Configure Active Directory domains

Blue Prism administrators are able to view, add, edit, and delete Active Directory domains and associated credentials stored in the Blue Prism database.

To access and manage Active Directory domains in Blue Prism, navigate to **System** > **Security** > **Sign-on Settings** > **Active Directory Domains**.



Sign-on Settings - Active Directory Domains

Domain Name	Domain DN
bpdevops.co.uk	dc=bpdevops,dc=co,dc=uk

> You only need to add new Active Directory domains in multi-forest environments with a one-way trust relationship. For more details, see Trust relationships between domains on page 15.

Prerequisites

The following prerequisites must be met before adding Active Directory domains:

- **Ensure the encryption scheme is configured** – Active Directory domain credentials are encrypted in the Blue Prim database using the default encryption scheme, so an encryption scheme must be configured before adding domains. It is recommended to store the encryption key on the application server. For more details, see Encryption schemes.
- **Ensure the encryption key is accessible to the Blue Prism API** – If the encryption key is stored on the application server, additional steps must be taken to make the encryption keys available to the Blue Prism API. This is to ensure that Active Directory users across multiple domains are able to use the browser-based Control Room. To allow this, the Blue Prism API must be able to decrypt the domain credentials using the encryption scheme stored on the application server. For more details, see API configuration.

Add a domain

1. On the Sign-on Settings - Active Directory Domains screen, click **Add**.

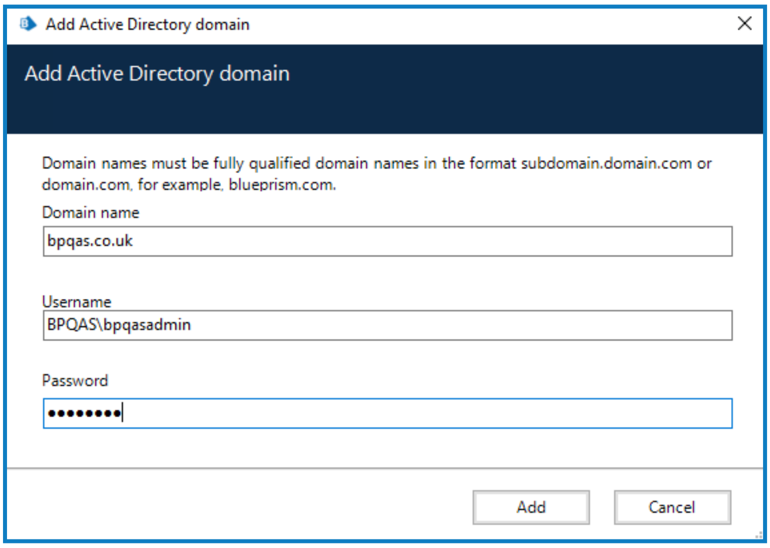
   The Add Active Directory domain screen displays.

2. Enter a domain name.

   This must be the fully qualified domain name (FQDN) using the format subdomain.domain.com or domain.com.

3. Enter the username and password for the domain. Usernames must be in the format username@domain.co.uk or DOMAIN\username. The credentials must be requested from a system administrator beforehand.

> Active Directory domain credentials are stored in the database and are encrypted before storage. The credentials stored for each domain must be that of an Active Directory service account. The service account password must not expire, the service account must not be a user account, and should follow Active Directory service account best practices.You only need to enter domain credentials in a multi-forest environment with a one-way trust.



Add Active Directory domain

Domain names must be fully qualified domain names in the format subdomain.domain.com or domain.com, for example, blueprism.com.

Domain name: bpqas.co.uk

Username: BPQAS\bpqasadmin

Password: ••••••••

4. Click **Add**.

   The domain name and credentials are validated against the Active Directory domain controller and the added domain displays in the domains list.

Edit a domain

1. On the Sign-on Settings - Active Directory Domains screen, select a domain and click **Edit**.

   You can only edit one domain at the time.

2. Change the information as required. You will have to re-enter your password.

> You cannot edit domain names.

3. Click **Save** to apply your changes.

Delete domains

1. On the Sign-on Settings - Active Directory Domains screen, select the required domain(s) and click **Delete**.

   A message displays asking you to confirm the deletion.

2. Click **Delete** to delete the selected domain(s).

Trust relationships between domains

For multi-forest environments, trust relationships must be configured between domains. These can be two-way or one-way to the domain that should be trusted.

For example:

- In a one-way trust between Domain A and Domain B, users in Domain A can access resources in Domain B. However, users in Domain B cannot access resources in Domain A.
- In a two-way trust, Domain A trusts Domain B and Domain B trusts Domain A. This means that authentication requests can be passed between the two domains in both directions.

Two-way trusts do not require the user to provide domain credentials if the user running the Blue Prism application server has relevant read access to the domain that the user belongs to. In these examples, the Blue Prism application server would reside in Domain B. Two-way trusts require credentials to be provided when the user needs to query a trusted domain using an account different to the account running the Blue Prism application server. One-way trusts require a domain with credentials to be created.

The following trust types are supported:

- External
- Parent-child
- Tree-root
- Forest

For more information, see Supported Active Directory infrastructure.

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 or performance issues occur during login

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.

> Some additional database scripts may be required for troubleshooting. These can be downloaded from the Blue Prism Portal as required. Where required, the appropriate database script is named in the scenarios below.

- **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 single sign-on settings, they should be able to sign in.

  If a user is attempting to sign in following a product upgrade and they receive the error message "Login failed. This user has no roles assigned in Blue Prism", download the database script **BP-9497-ConfigureTrustedDomain.sql** from the Blue Prism Portal and follow the steps outlined in this Knowledge Base article.

  Check that the user account has been created and has been assigned at least one Blue Prism role, either directly or via security group membership.

  You should first synchronize users with Active Directory on the Security - Users screen. If the user account does not display in the user list, this means it has not been created yet:

  - If user roles are managed in Blue Prism, you should create the user account and assign the required roles to it.
  - If user roles are managed in Active Directory, you should check which Active Directory groups are mapped to Blue Prism roles under **System** > **Security** > **User Roles**. The user should be a member of at least one of these groups. If not, your network administrator should add the account to the appropriate security group before you synchronize the user list with Active Directory again to check that the account displays in the user list.
  - If roles are managed both in Blue Prism and Active Directory, you should create the user account and assign the required roles to it directly and/or via security group membership, as required.
- **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.

- **Check if you need to configure the Active Directory timeout limit** – If a user either cannot sign in using Active Directory or is experiencing performance issues during the login process, and the logs show several instances of *System.TimeoutException: Timeout after 5 seconds*, you can set an Active Directory timeout limit in the database. The database script **BP-9268-SetActiveDirectoryQueryTimeout.sql** is available for download from the Blue Prism Portal for this purpose. This will alter the timeout settings for the application server(s) and all API instances pointing to the Blue Prism database. Back up your database before running this script against your Blue Prism database.
- **Check if you need to manually configure the Active Directory domains that will be queried during the login process** – To reduce the time taken for the Active Directory cache to populate, system administrators can manually configure the trusted Active Directory domains that will be queried during the login process. If at least one Active Directory domain is manually configured, these settings will be used during the login process to query only the configured domain(s), rather than programmatically identifying which domains can be queried. The database script **BP-9497-ConfigureTrustedDomain.sql** is available for download from the Blue Prism Portal for this purpose.

  > When a new domain is added to Active Directory, it must also be added to the configuration, otherwise it will be ignored, and users belonging to this domain will not be able to log in until the configuration has been updated.

  Before running the script, please ensure that:

  - You have backed up your Blue Prism database.
  - Any Active Directory domains that meet one or more of the following criteria are manually configured (if using Blue Prism versions 7.1.0 or 7.1.1):
    - Contain users that must be able to log in.
    - Contain security groups that are assigned directly to Blue Prism roles.
    - Contain parent security groups which include security groups that are directly assigned to Blue Prism roles.
  - Any Active Directory domains that meet one or more of the following criteria are manually configured (if using Blue Prism version 7.1.2 or later):
    - Contain users that need to log in using telnet commands or processes exposed as web services using a User Logon Name (Pre-Windows 2000) username format. For example, john as opposed to DOMAIN\john or john@domain.com.
    - Contain users that have an alias User Principal Name (UPN) suffix that is different to the Domain Name System (DNS) name of the Active Directory domain. For example, corp.dir.company.com (DNS name) and company.com (alias suffix), where john@company.com is the UPN. An optional database script to configure alias suffixes (BP-10681-ConfigureUpnSuffixes.sql) is available for download from the Blue Prism Portal.
  - The domain host name, security identifier (SID), and the name of the forest in which the domain resides has been provided for each domain that needs to be queried.

- **Check if you need to configure domain cache settings** – To further improve performance during login, the behavior of the cache that stores the discovered domains can be configured by setting a refresh interval and a maximum cache duration. The database script **BP-9654-SetCacheDurationAndRefreshInterval.sql** is available for download from the Blue Prism Portal for this purpose. Back up your database before running this script against your Blue Prism database.
  - The refresh interval is the interval in minutes at which the cached data will be updated from Active Directory. The value can be set between 5 and 1440 minutes. The default value is 5.
  - The maximum cache duration is the amount of time in minutes that the data will be held in the cache before it is invalidated. The value can be set between 5 and 1440 minutes. The default value is set to 30 if using Blue Prism versions 7.1.0 or 7.1.1, and to 1440 if using Blue Prism version 7.1.2 or later.

    > These two settings must be configured as a pair, and the maximum cache duration must be set higher than the refresh interval. If one or both settings are not configured, the default values will be used.

  - This cache is populated in Blue Prism when:
    - Establishing a direct database connection.

      > If logging in using a direct database connection, users may be unable to successfully log in while the cache is being populated. The time required to populate the cache can vary, but you can manually configure trusted Active Directory domains that will be queried during the login process to reduce the wait time.

    - Starting a Blue Prism application server.
    - Enabling Active Directory authentication in System > Security > Sign-on Settings.

  > The cache is not populated in Blue Prism unless Active Directory authentication has been enabled.

  For more details on the Active Directory domain cache, see this Knowledge Base article.

- **Check if you need to configure Domain Controller name mappings** – You might need to configure Domain Controller name mappings in the database if the following error message and log displays when searching for Active Directory users or security groups, and when adding or editing Active Directory domains:
    - Error message: *The domain record could not be saved: Invalid credentials. Please check your credentials.*
    - Error log: *The user name or password is incorrect. If the domain credentials for dc=example,dc=com are valid, please provide a domain controller mapping record.*

      This could occur if the domain of interest is on a different network from the network on which the Blue Prism application server is running. If you are certain that the provided credentials are correct, you need to add domainName and domainControllerName parameters to the database so Active Directory queries for the domain specified in domainName are directed to the endpoint defined in domainControllerName.

      To do this:

      1. Back up your Blue Prism database.
      2. Download the BP-9420-AddDomainNamePreferences.sql script from the Blue Prism Portal and open it in a suitable editor.
      3. Update the placeholder values for the domainName and domainControllerName parameters for each required domain with your own values, for example:
          - domainName – The name of your Active Directory domain or the DNS name of the domain, for example, company.com.
          - domainControllerName – The DNS name of the domain, for example, company.com or the FQDN of a Domain Controller in the domain, for example, server-id.company.com.
      4. Execute the script against your Blue Prism database.

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 and a Kerberos realm for each BP Server connection in the Blue Prism interactive client. 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, 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.

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.