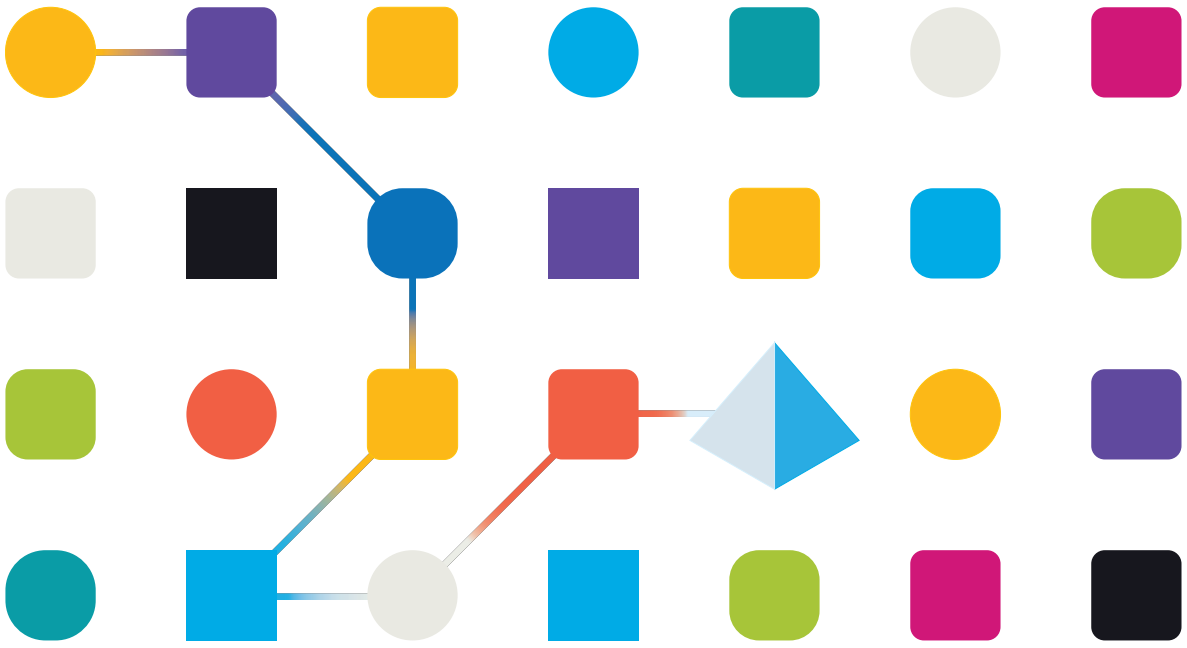
Blue Prism 7.1

Infrastructure Reference Guide

Document Revision: 2.0



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

Introduction

Intended audience

This reference guide is intended for use by system architects, technicians, and designers who are seeking to gain an understanding of the product architecture, and the implementation options available when deploying the solution in any of a combination of single or multi-server deployment patterns.

About this guide

This guide provides an introduction to each of the available components within a Blue Prism environment and provides detailed information relating to the various options and design decisions that can be considered as part of the implementation. It focuses on core best practice architectural patterns and is not intended to cover non-standard deployments.

It is recommended that, to start, users should become familiar with the various components that feature within a Blue Prism environment and identify the architecture most suited to the deployment being considered.

Document summary and quick links

This document provides high-level architecture examples, followed by an overview of individual components and how they can be scaled. It then outlines environment configuration, including network connectivity, high availability, and security.

Blue Prism architecture overview

There are two main deployment architecture options:

- **Standard Blue Prism Enterprise** – This can be installed and used independently of other components.

  Single sign-on can be configured using Blue Prism's legacy built-in single sign-on method; or Authentication Server, which requires Blue Prism Hub.

- **Standard Blue Prism Enterprise, plus Hub Control Room** – This requires the Hub platform, Authentication Server, and the Blue Prism API, which establishes a connection between the Hub Control Room and Blue Prism.

Each implementation of a Blue Prism environment consists of a database along with any of the composite components, each of which provide functionality based on the requirements of the business.

System architecture changes in Blue Prism Enterprise version 7

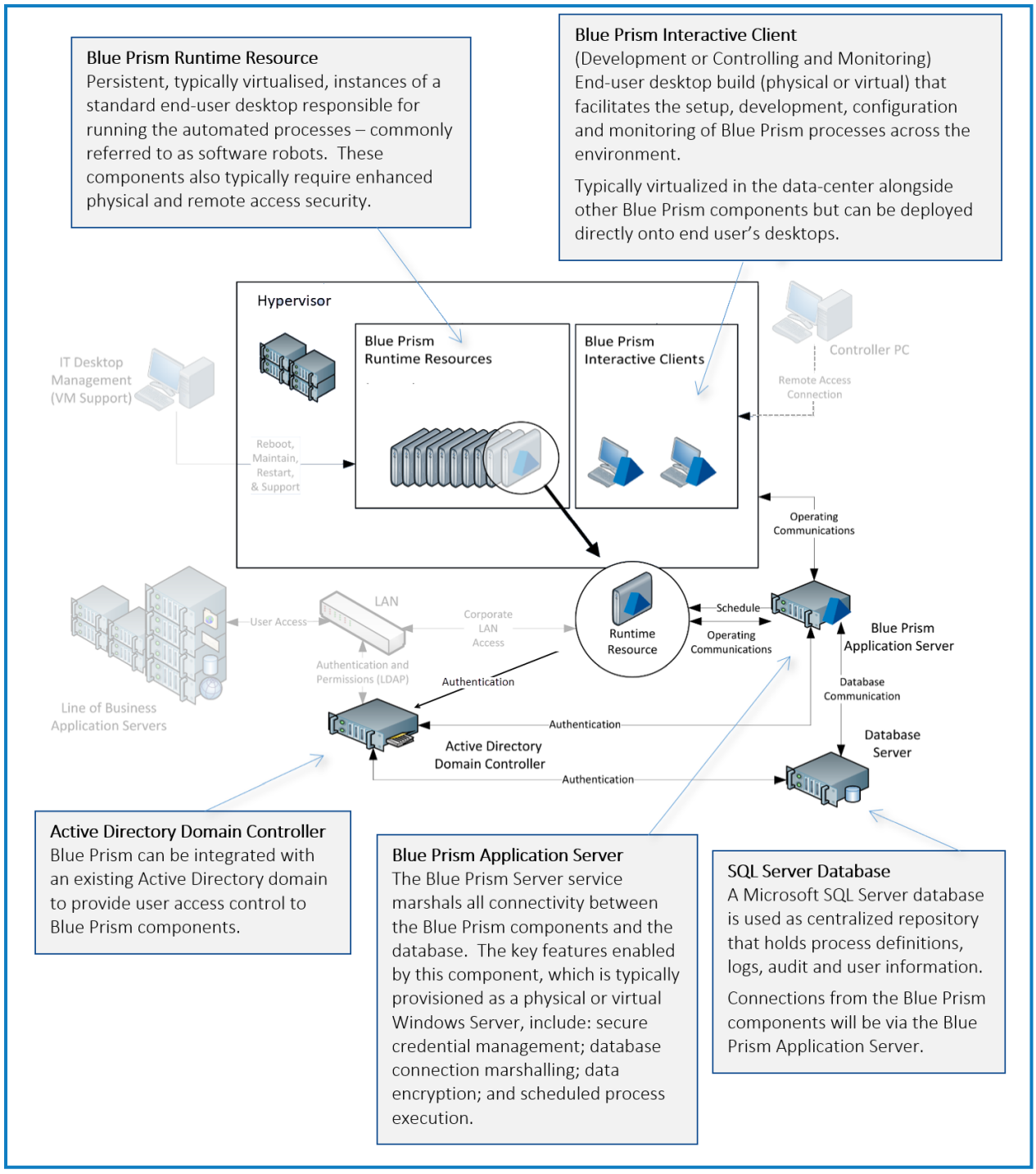
The following system architecture components were introduced for Blue Prism version 7:

- **Controlling digital workers at scale** – With Application Server Controlled Resources (ASCR), interactive clients communicate with available runtime resources via the application server, meaning that individual connections don't need to be made.
- **Native messaging host for browser extensions** – A native messaging host application is used to communicate with each of the browser extensions (Chrome, Edge, and Firefox).
- **Authentication Server (optional)** – A centralized way of providing common authentication for users across Blue Prism Enterprise, the Blue Prism API, and Hub.
- **Browser-based Control Room (optional)** – Provides dashboards and data views that allow users to view and manage Blue Prism activity for all their environments.
- **Blue Prism API (optional)** – Provides a common interface for components such as the Hub Control Room to connect with the Blue Prism database.

It is recommended that you review the Blue Prism version 7 release notes for details of these features and any differences between versions.

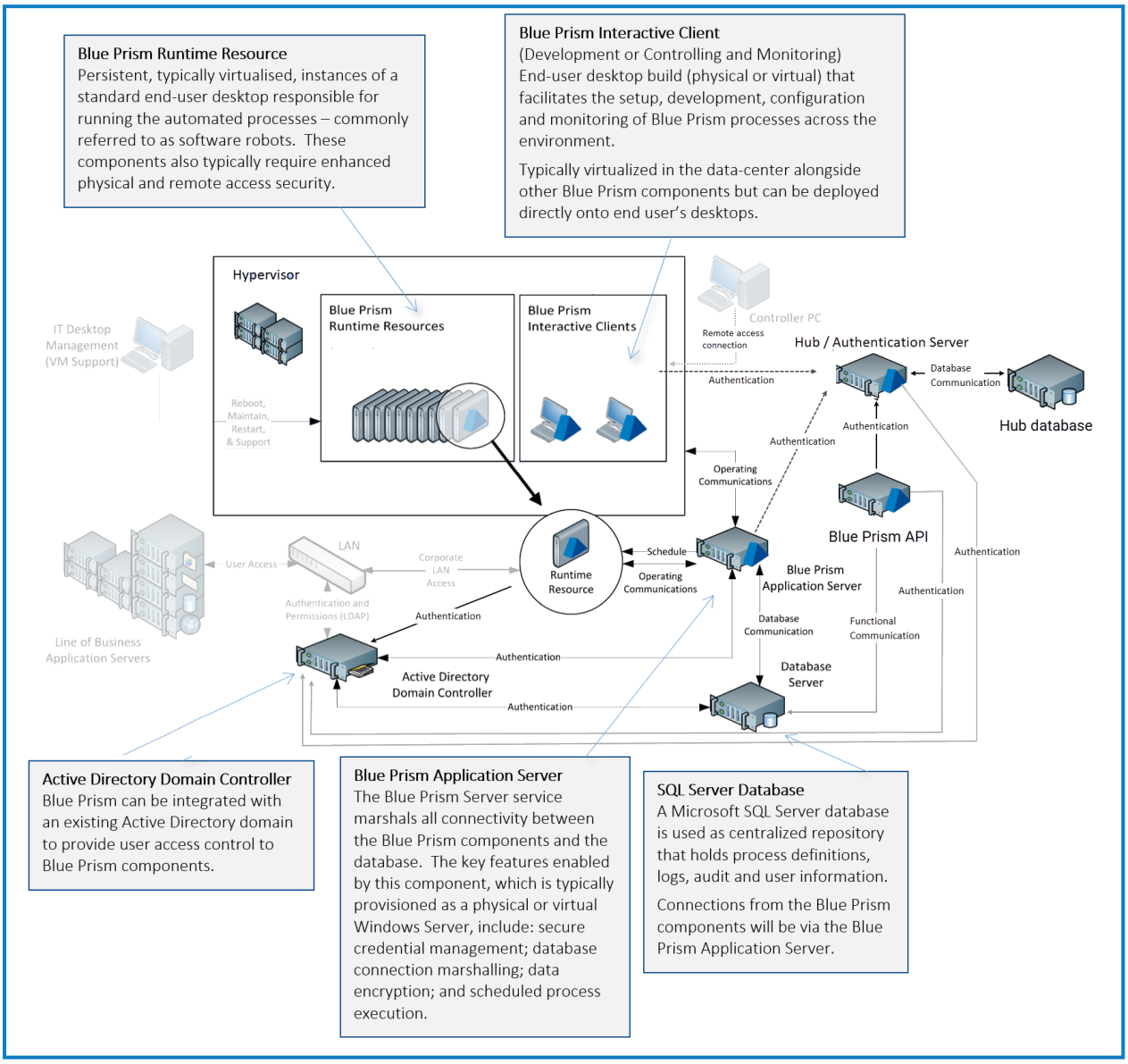
Standard Blue Prism Enterprise architecture

The following diagram depicts the standard Blue Prism Enterprise architecture.



Blue Prism Enterprise with Hub Control Room architecture

The following diagram depicts Blue Prism Enterprise with Hub Control Room architecture, which requires Hub, Authentication Server, and the Blue Prism API.



Component architecture examples

This section focuses on the main architecture design patterns recommended by Blue Prism. Whilst other configurations are possible, these should be discussed with your Blue Prism Technical Consultant to determine their scalability, security, and resilience.

Whilst the majority of Blue Prism environments are built on virtualized hardware, the components are equally suited to physical equipment. As such, the architecture diagrams in this guide do not differentiate between physical or virtualized configurations.

The latest information about the minimum specifications of each Blue Prism component can be found in Blue Prism software and hardware requirements.

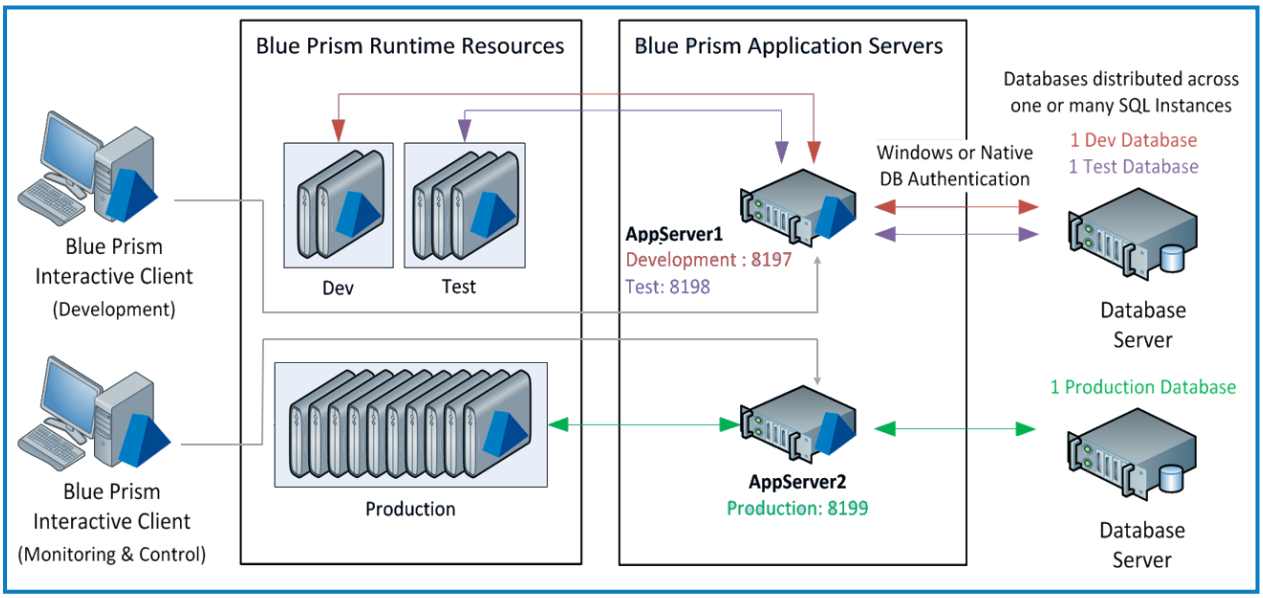
In each of the following examples the specifications for the Blue Prism runtime resources and Blue Prism interactive clients remain the same.

> The specification of interactive clients and the runtime resources used for development must meet the collective recommendations of all applications to be automated on that device, for example, SAP, Office, Temenos, or FiServ. A useful indicator is to base the specification on an equivalent device used by an end-user to perform the tasks that are to be automated.

Data-center secured: 25 runtime resources

Controllers and process developers should use their own physical PC as interactive clients, rather than virtualized runtime resources. Runtime resources and application servers can optionally be configured on virtual machines.

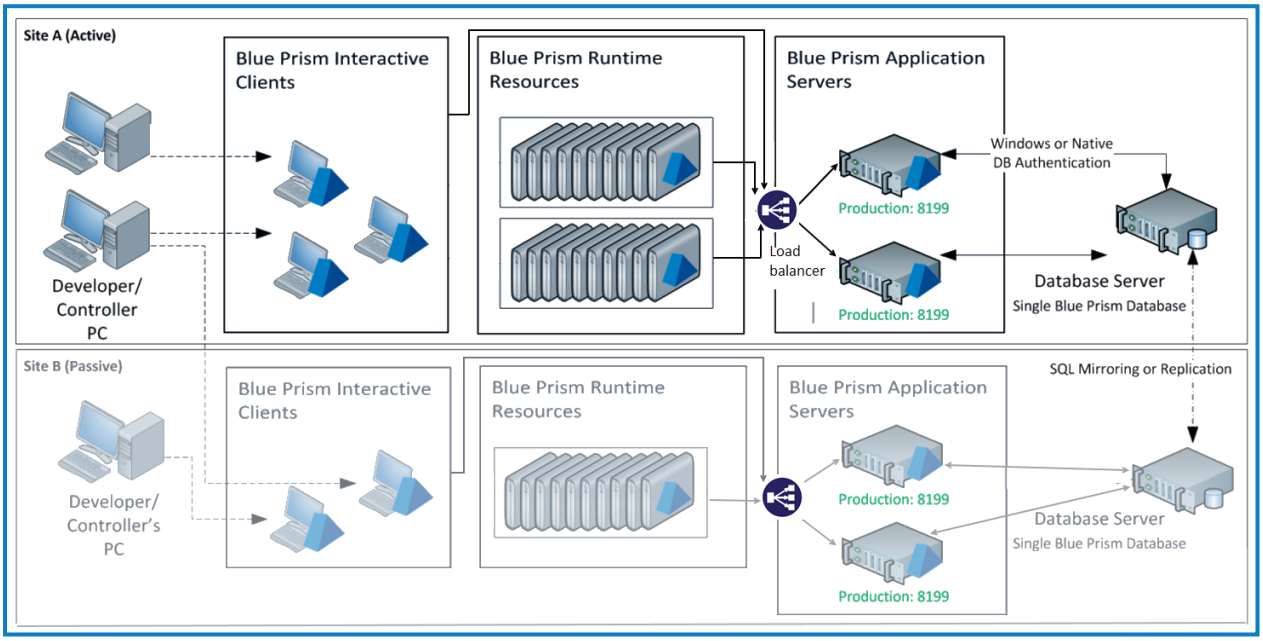
The following diagram shows default and configured port numbers, for details of the default ports for each component, see Default ports on page 49.



Data-center secured with disaster recovery (DR): 100 runtime resources

An environment which is entirely secured within the data center and which illustrates:

- Two sets of 50 runtime resources connected to load-balanced application servers.
- Interactive clients which are used remotely.
- A DR site with up to 100 runtime resources and a single application server connected to a replicated copy of the database.

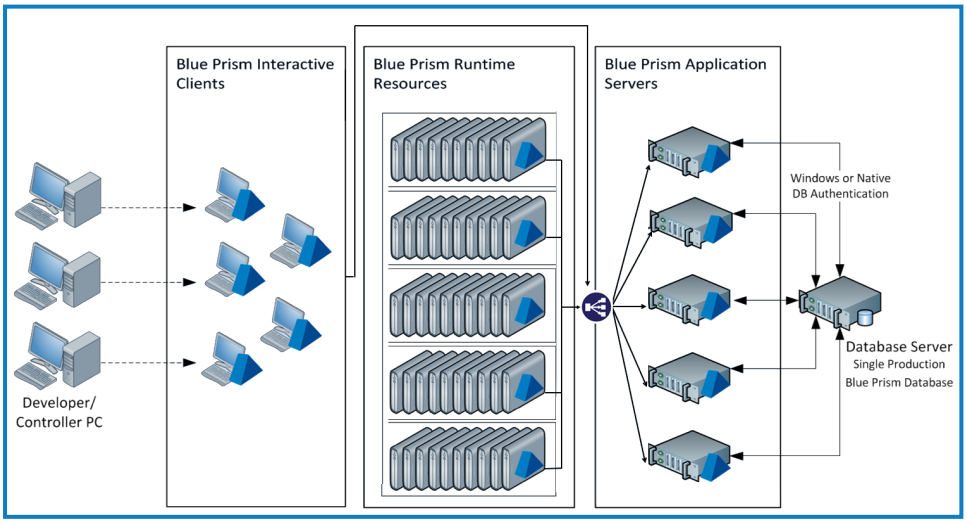


The load balancer indicated in the diagram above can be your organization's preferred choice.

Data-center secured: 500 runtime resources

An environment which is entirely secured within the data center and which illustrates:

- Five sets of 100 runtime resources, each with a dedicated application server.
- Interactive clients which are used remotely.



Advantages and constraints of virtualized hardware

Whilst the majority of Blue Prism environments are built on virtualized hardware, the components are equally suited to physical equipment. The following table lists the advantages and constraints of the use of virtual environments.

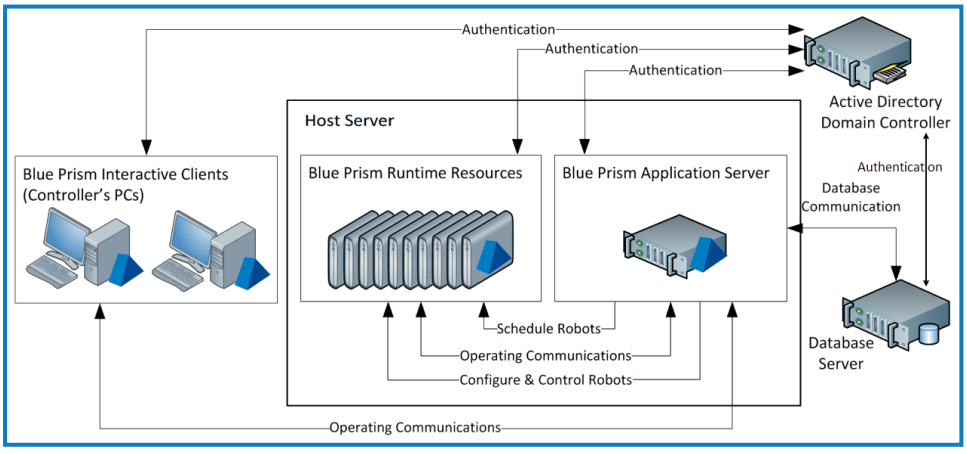
Advantages	Constraints
• Quick to scale – as already virtualized. • Database performance and capacity easily scaled. • Process development and test can be delivered without constraining production (separate development and test environments and dedicated runtime resources). • Virtualization aids commonality across components. • Separate application servers for development/test versus production allows product releases to be applied separately.	• Speed to implement/provision. • Cost of virtualization technology. • Development / test environments to be provisioned separately.

Architecture considerations

This section describes considerations when planning your Blue Prism environment.

Active Directory integrated

Blue Prism should be integrated with Active Directory for the management of user access and control. A non-integrated configuration is possible, but not recommended. The following diagram shows the request and data flow of Active Directory authentication. This functionality is documented in Active Directory Integration.

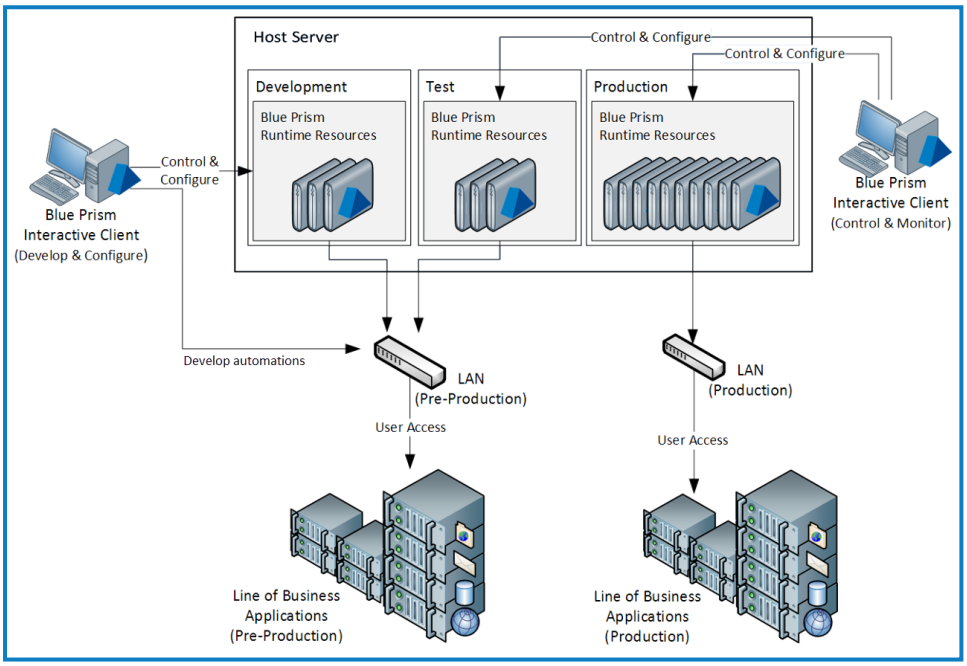


Optionally, both native authentication and Active Directory can be utilized in a Blue Prism Enterprise environment. In this case, native authentication should only be used for a super administrator account, with highly restricted user access for authentication users only, in order to administer Active Directory issues if they occur. Active Directory should be the standard user authentication option.

Access to line of business applications

The Blue Prism components that require access to the line of business applications that are automated as part of a process are the:

- **Blue Prism runtime resources** – Required for automations.
- **Blue Prism interactive clients** – This is only necessary for those that are used for specifically developing and configuring the processes. For example, the interactive clients in the development environment are used to design and configure the process and will need to be able to access the line of business applications, whereas the interactive clients in the production and test environment could only be used for monitoring and controlling the runtime resources so would not need this access. This is shown in the diagram below.



It is also common for the components in each environment to be configured to interact with appropriate instances of the applications. For example, the runtime resources in the development and test environment would ideally be configured to interact with non-production instances of the line of business applications.

Disaster recovery scenarios

It is highly recommended that disaster recovery is considered as part of a Blue Prism deployment plan. Blue Prism can be deployed to cater for a range of disaster recovery scenarios and can operate as part of active/active and active/passive infrastructures. The following considerations are relevant to both types of deployment:

- Any cases being worked at the time of failure will be reported as exceptions and must be either reset or referred for manual attention. Commonly these are reviewed as part of the business as usual management that is carried out by the controllers who oversee the platform.
- Each Blue Prism Server must be configured with identical encryption schemes.
- Runtime resources are resolved by their network name, which is typically the machine ID. The machines on Site B will have different IDs to those in Site A, so alternative DR schedules may be required to start the processes on these alternative machines. Resource pools may be used to aid this process.

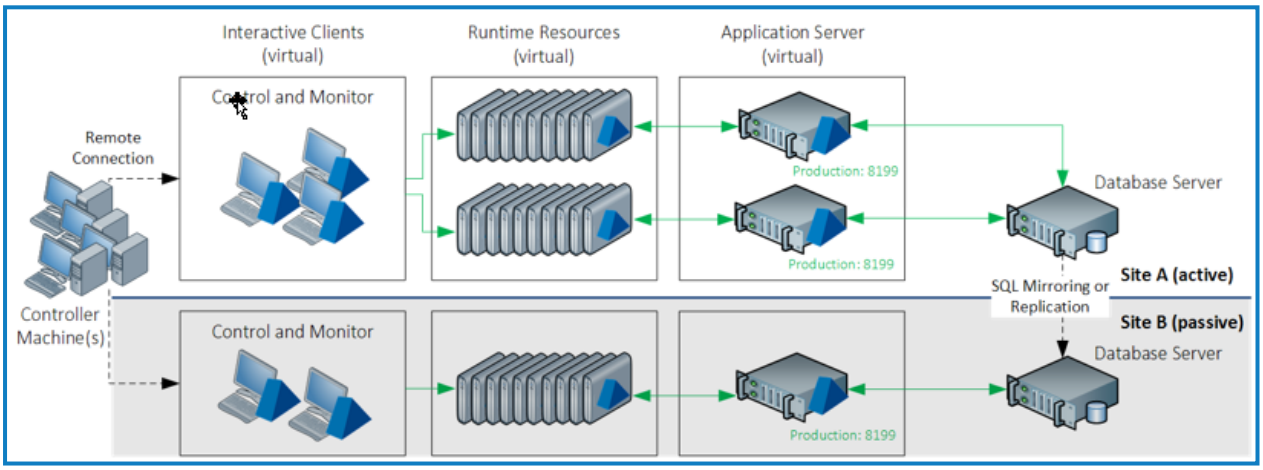
- The database must be replicated accurately and frequently in order to maintain the state of the cases being worked in the Blue Prism queues.
- Latency considerations must be reviewed if routing Application Server or Database traffic across sites.

Active/passive

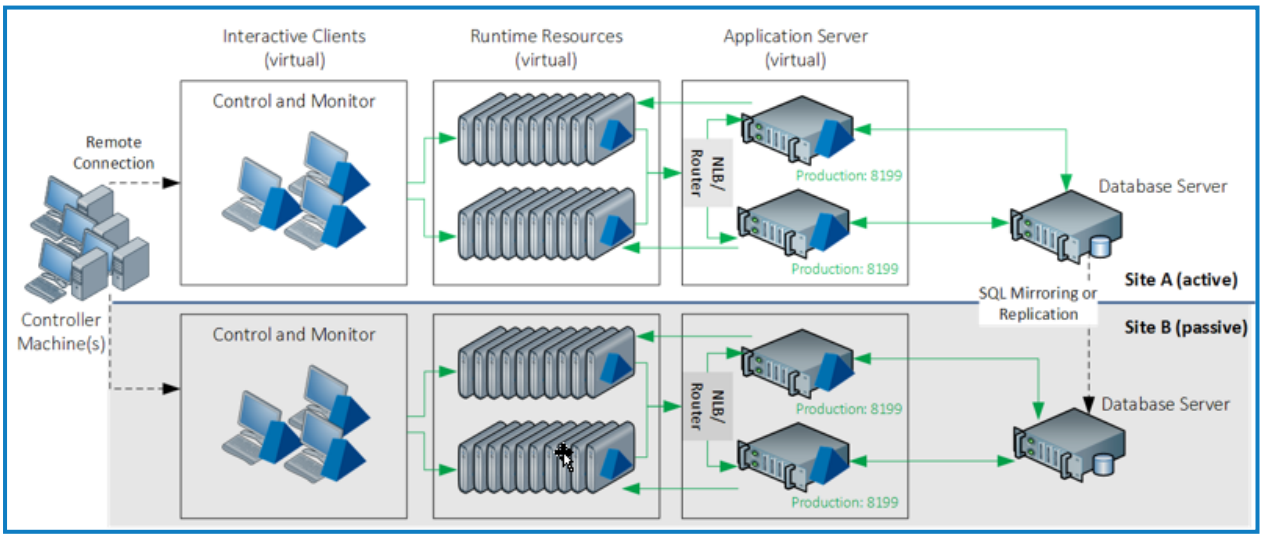
In addition to the general considerations, the following considerations may also be relevant for active/passive infrastructures:

- When Site B is activated, the network names of devices must either match those in Site A or the interactive clients and schedules must resolve the names to the new network address – this is outside the scope of Blue Prism.
- It may be necessary to configure alternative schedules that use the identifiers of the DR runtime resources in the event of failover.

Active/passive with statically allocated application server



Active/passive with balanced application servers

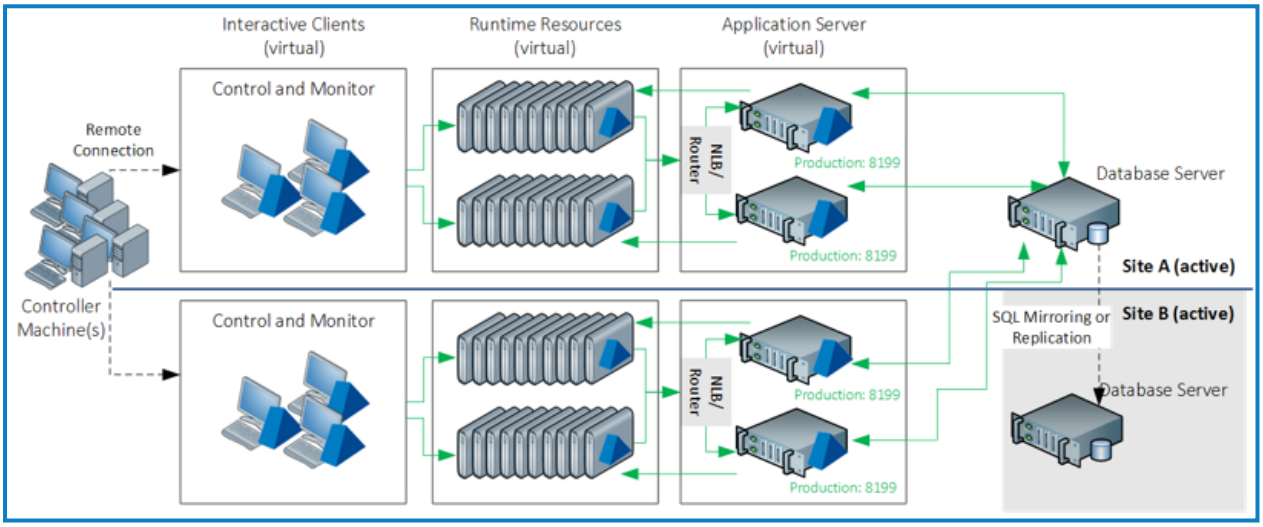


Active/active

In addition to the general considerations, the following considerations may also be relevant for active/active infrastructures:

- The database connectivity for both sites should be considered:
  - Where there is a high latency connection between sites, only application servers with a low latency database connection should be used.
  - Interactive clients must have a low latency connection with application servers.
- If only a subset of runtime resources are available, any schedules must be considered. Resource pools can assist in this process by masking the location of the resources and using an available resource from the specified pool.

Active/active with balanced application servers

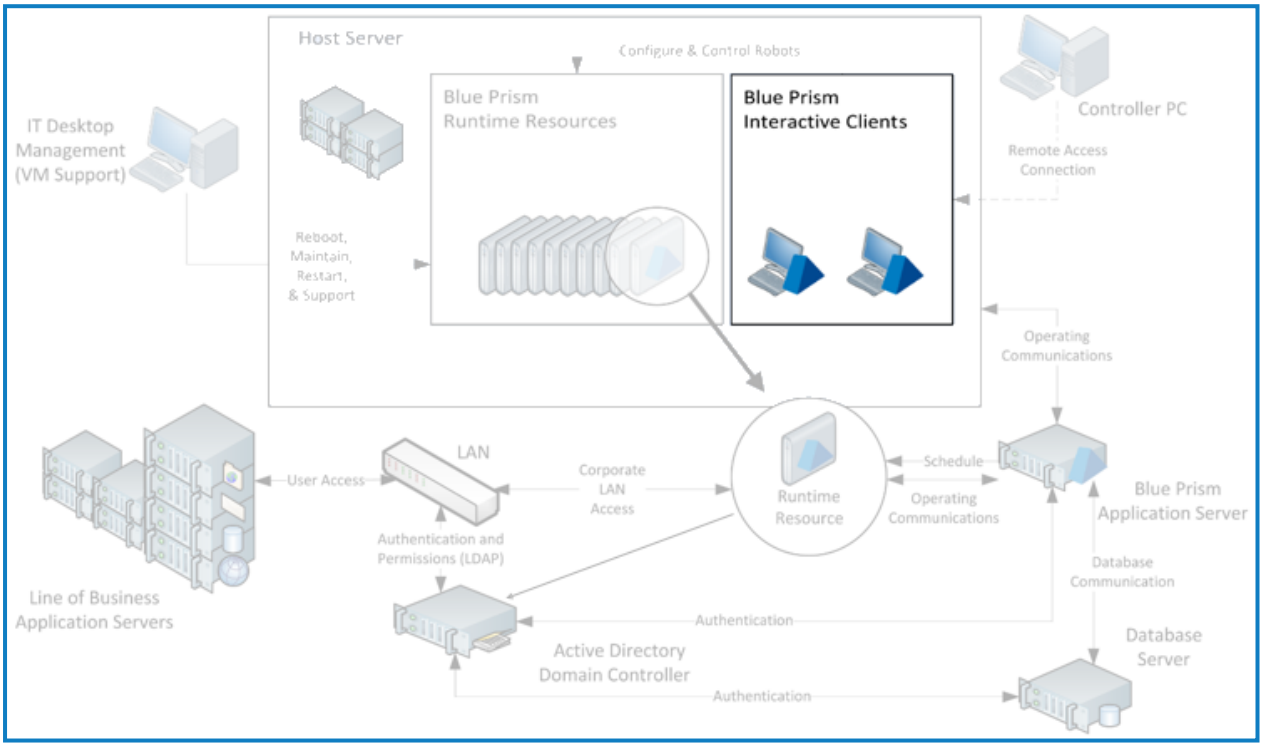


See High availability, redundancy, and disaster recovery on page 55 for information requirements for these scenarios.

Blue Prism interactive client

Interactive clients are used for developing processes and for controlling and monitoring the Blue Prism runtime resources. The core purpose and features offered by an interactive client is dependent on whether it is used in a development or production environment (or both).

Hub Control Room can also be used for controlling and monitoring runtime resources, in addition to other functions. See Blue Prism Hub Control Room on page 35 for details.



Development environment	Production environment
• Design connections to third party applications and systems • Develop, troubleshoot, test processes based on those connections • Package releases for transfer to live environment • Define system settings and configurations	• Initiate processes • Monitor and control runtime resources • Manage work queues • Review business referrals • Review logs and audit and generate reports

Minimum requirements: interactive client

The latest information about the minimum specifications of each Blue Prism component can be found in Blue Prism software and hardware requirements.

All minimum requirements must consider the selected operating system as well as the applications to be automated. Interactive clients can either be deployed to existing user desktops or to a virtualized end-user desktop instance.

Each interactive client requires the Blue Prism application to be installed. Where the interactive client is used for developing and configuring Blue Prism processes, consideration should be given to the installation of and connectivity to target applications; and access must be granted to all in-scope applications.

Frequently asked questions: interactive client

How are interactive clients typically deployed?

It is recommended that interactive clients used by Blue Prism process developers are configured using the same specification as runtime resources, this is commonly a virtualized machine. Controller machines can be deployed on user's physical desktops or virtualized.

What are the security implications of this component?

Interactive clients must be secure, with only authorized users allowed to access the hardware and application. Developers working on interactive clients can modify processes and access credentials used by those processes. It is therefore recommended that role-based access control (RBAC) is implemented such that no users in production environments have permission to open and edit processes or objects. It is also recommended that in pre-production environments where developers are necessarily editing processes, credentials used by those processes correspond to pre-production instances of target applications, rather than production credentials which developers should not have access to.

To strengthen Blue Prism network security, role-based access control (RBAC) should be utilized and only specific users, such as infrastructure administrators, should be granted access to application servers and network communication configuration. All other users should be denied access by default. Explicit allow/deny access should be configured for all users and the principle of 'Least Privilege' followed. These controls should also extend to the users of Blue Prism, so that only those who need access to the platform are allowed and are only given the level of authority required to carry out their role, while all others are denied access by default.

Can a single interactive client be used across multiple environments?

Irrespective of whether the device is provisioned physically or virtually, a single interactive client can be configured to connect to multiple Blue Prism environments of the same version (e.g. Dev/Test/Production). The user selects which environment they wish to connect to as part of the logon procedure.

Does this component need to be backed up?

Typically there is no important information or configuration stored on a Blue Prism interactive client unless a local database is in use (e.g. for development purposes), which we strongly advise against. It is however recommended that where possible a clone of the client should be retained.

It is useful to have a backup of the automate.config file for easier configuration of other/new interactive clients.

Networking: interactive client

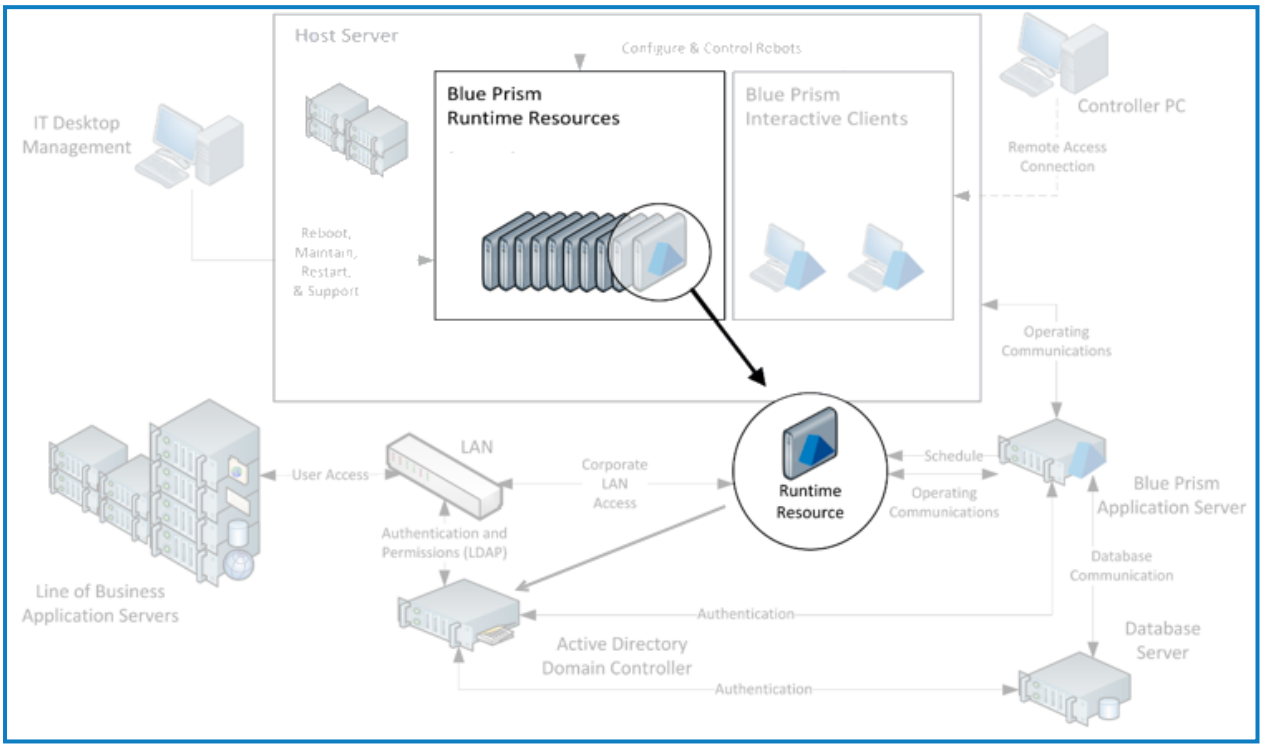
The main components that interactive clients initiate communications with include:

- **Application server** – The application server is used for all database connectivity (WCF) and also to send instructions to runtime resources (TCP).
- **Third-party applications** – See Blue Prism runtime resource on the next page for network considerations where the interactive client is used for developing and configuring processes.

Sample diagrams and default port settings are provided within the Blue Prism network connectivity on page 46.

Blue Prism runtime resource

Blue Prism runtime resources are persistent, typically virtualized, instances of standard end-user desktops running automated processes within a secure environment.



The key features of runtime resources are that they:

- Are centrally controlled.
- Execute assigned processes.
- Connect to the line of business application(s).
- Capture log information (which is then stored in the Blue Prism database).

Blue Prism runtime resources effectively operate a device as if a human operative was working it. Explicitly this means that the runtime resources must be logged in for processes to run, and furthermore, each transaction that is processed would be visible if a screen was connected. This guide contains a number of considerations to mitigate any potential security and governance concerns that this may raise.

Minimum requirements: runtime resources

The latest information about the minimum specifications of each Blue Prism component can be found in Blue Prism software and hardware requirements.

All minimum requirements must consider the selected operating system as well as the applications to be automated.

Runtime resources are typically deployed to virtualized instances of standard end-users desktops.

Each runtime resource requires the Blue Prism application to be installed. Consideration should be given to the installation of and connectivity to target applications; and access must be granted to all in-scope applications.

> Please be aware that starting and running a runtime resource with elevated permissions might affect the interaction with the application that is being automated. Generally, the permissions of the runtime resource must match those of the user context of the target application.

Additionally there are a number of settings and profile configurations that need to be applied. See the following sections for information.

Frequently asked questions: runtime resources

What are the security implications of this component?

As the runtime resources are responsible for executing the automated processes their security is paramount. The Physical Security section contains further information on this topic.

Can a single runtime resource be used across multiple environments?

Whilst it is possible to reconfigure a runtime resource to be connected to a different environment, provided they are running the same version of Blue Prism, it is not recommended to frequently switch which environment a specific runtime resource is assigned to.

Does this component need to be backed up?

Typically there is no important information or configuration stored on a Blue Prism runtime resource. It is however recommended that where possible, a clone of the desktop should be retained, and consideration given to whether any of the runtime resources are used for business critical processing.


It is useful to have a backup of the automate.config file for easier configuration of other/new runtime resources.

Networking: runtime resources

The main components that runtime resources initiate communications with include:

- **Application server**– The application server is used for all database connectivity (WCF). In addition, commands the runtime resources to execute processes come from the application server over a TCP connection. This is referred to as Application Server Controlled Resources (ASCR).
- **Third-party applications** – The type of connectivity required between the runtime resources and third-party applications will depend on the nature of the automation. The majority of Blue Prism automation takes place via the GUI and therefore the runtime resources simply need the same level of access as a typical end-user of the given application. Where deeper connections (e.g. direct database, web service, message queues) are required the appropriate ports and access will need to be configured.
- **Browser extensions** – Native support for automating web pages and applications in Google Chrome, the Chromium-based version of Microsoft Edge, and Mozilla Firefox web browsers is provided using Blue Prism browser extensions. The extensions allow Blue Prism to interact with web pages and applications presented in these browsers, so that business processes that rely on such applications and web pages can easily be modeled.

See Blue Prism Network Connectivity for sample diagrams and default port settings.

Device setup: user accounts

There are a variety of options and settings to be considered and configured for the runtime resources, including:

- User accounts on the next page
- Login methodology on the next page

User accounts

Each runtime resource can be allocated an independent user account to allow it to be appropriately secured. This provides opportunities for comprehensive audit and monitoring. Though it may be beneficial to assign an independent user account to a runtime resource, it is not necessary to tie a runtime resource to one, specific account.

The type of account used to log the respective runtime resource onto the network should be carefully considered as this could restrict the type of applications that can be automated by each of the runtime resources. It should be noted however, that for applications which are not secured using Active Directory integrated authentication, the runtime resources can be configured to use credentials independent of those used to authenticate the device onto the network.

- **Domain Account (Recommended)** – If an Active Directory domain account is used to log on to each Blue Prism runtime resource there are increased options for connecting to applications which are secured using either native or Active Directory integrated authentication (single sign-on). Additionally the Blue Prism runtime resource can used the configured domain account to authenticate against Blue Prism environments that are configured to use single sign-on.
- **Native Authentication**– If using native authentication, single sign-on can still be used to authenticate with the applications that use Active Directory integrated authentication (single sign-on), by using the identity used to log into Windows.

The access and permissions assigned to the accounts used by the runtime resources should be evaluated to see if:

- The accounts are configured to allow access to the necessary applications and network resources that may be required by the processes (including network locations etc.).
- The accounts need to be members of appropriate Active Directory groups.
- The accounts are restricted from performing certain types of action on the local machine that may be required as part of an automated process. (e.g. logging to the event viewer; using the command prompt etc.)

To strengthen Blue Prism network security, role-based access control (RBAC) should be utilized and only specific users, such as infrastructure administrators, should be granted access to application servers and network communication configuration. All other users should be denied access by default. Explicit allow/deny access should be configured for all users and the principle of 'Least Privilege' followed.

These controls should also extend to the users of Blue Prism, so that only those who need access to the platform are allowed and are only given the level of authority required to carry out their role, while all others are denied access by default.

It is advised that you also consult the Robotic Operating Model (ROM) security information on the Blue Prism Portal for recommendations of best practice.

Login methodology

Blue Prism runtime resources must be logged in and listening in order to be able to receive instructions and execute processes. It is therefore necessary to consider the options for how the login will take place each day and following system restarts.

The login options should be considered alongside the subsequent authentication methods that will be used as part of process execution when the runtime resources authenticate with third-party systems.

For example, if the processes automate applications which are secured using Active Directory, it will be necessary for the runtime resources to be logged in using Active Directory domain user accounts.

The authentication options for the runtime resources may include:

- **Automated authentication using the Blue Prism Login Agent (recommended)** – Each runtime resource which has been appropriately configured and where Blue Prism Login Agent has been installed, can be automatically logged in by Blue Prism. The prerequisites for Login Agent must be considered to ensure its suitability in a given environment.
  Blue Prism Login Agent is used to securely store the credentials for each runtime resource and use these to automatically log in, or unlock the device. It additionally provides functionality for managing the passwords and can adhere to password history and complexity rules. This option may be the most suitable where the runtime resources authenticate directly against a secure Active Directory domain and where the processes include automating applications which are secured using Active Directory authentication (single sign-on).

  > This is the recommended option. Any other option should only be used where your organization's IT constraints prevent the use of Login Agent. In such circumstances, it is strongly recommended that a SS&C Blue Prism architect is consulted.

- **Automatic authentication** – Configuring the devices to log in automatically using locally stored credentials allows the respective device to launch the operating system without the need for any manual intervention; however the security of the credentials would need to be considered.
  If the applications to be automated use Active Directory integrated authentication, the automatic login would need to log the resource on to the network using an appropriate domain account. Consideration should also be given to whether the password(s) should be set to expire.
- **Manual authentication** – Named users could be responsible for manually restarting the devices and entering the relevant credentials. Consideration should be given to: the availability of users to carry out the task; the impact this would have on the speed of restarting a machine; the security of the credentials; the impact if it is required out of hours; the suitability of remote connectivity tools for this task.
- **No authentication (Not recommended)** – Removing the need for these components to follow an authentication procedure allows each device to launch the operating system without the need for any manual or automated login interaction. If the applications to be automated use Active Directory integrated authentication this option may not be appropriate.

  > This option is strongly not recommended for any environment.

For further details, see the Login Agent user guide.

Device setup: user profile

A number of user and computer account profile settings that should also be considered are discussed in the following sub-sections. Many of these can be enforced through use of standard IT tools such as Group Policy.

It is recommended that where possible, consistent settings should be applied across all of the Blue Prism runtime resources to ensure commonality and therefore reduce the complexity of process development.

Screensaver and auto-lock

The runtime resources should be configured to allow arbitrary periods of inactivity without entering a locked state, and without the screen being taken over by a screensaver. Application behavior behind a screen-lock is unpredictable and could cause exceptions which are difficult to diagnose. The Blue Prism security recommendations include ensuring that the runtime resources are inaccessible to users therefore removing the security implications of such settings.

Where processes are scheduled to automatically start early in the morning, the runtime resources should be allowed to remain in an idle state overnight. Some processes may involve inherent periods of idleness whilst the applications remain on screen. This too should not result in a lock-out.

Power saver options

The device power saver options should be reviewed to prevent the hardware from being automatically turned off, or scaled down, after periods of inactivity.

Surface automation considerations (font smoothing and display themes)

Where surface automation techniques are to be used as part of process automation, it is necessary for font smoothing to be disabled for the user and computer accounts used by the runtime resources that are responsible for executing those processes.

Display themes should be set to not use transparent or opaque window borders.

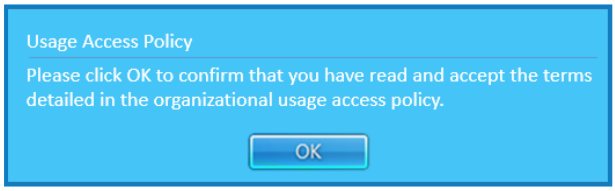
Additionally it may be necessary to remove or reduce compression which can affect the way that the graphical interface is presented to the end-user which in turn can have a negative impact on the interpretation of the screens by the runtime resources.

Pre-login requirements

It is often desirable to implement auto-login functionality for the Blue Prism resources (discussed as part of the Login methodology) however common configurations that can cause problems and that will need to be disabled for the applicable devices include:

- Requiring CTRL, ALT, Delete to be pressed prior to being able to login.

- Acknowledge acceptance of a Usage/Access Policy as part of the login procedure.



Default remote access settings

It is often necessary to disable the default remote access settings for Blue Prism runtime resources. The User Accounts, Remote Access and Security section contains information on the recommended approach for achieving remote connectivity with Blue Prism runtime resources.

SAP GUI Scripting

This setting should be enabled for the appropriate users if automating SAP via the GUI.

Device setup: start-up configuration

Blue Prism runtime resources must be logged in and listening in order to be able to receive instructions and execute processes. It is therefore necessary to consider the following items:

- The login options for the runtime resources.
- The steps required to automatically start Blue Prism.

User account login options

There are a number of options for authenticating the devices onto the network either manually or automatically. These are referenced within the Device setup: user accounts section.

Automatically starting Blue Prism

Once a runtime resource has successfully loaded into windows the Blue Prism client can be started silently using a command line method. This can either be configured to start automatically through use of the Windows Start-Up Group; or Windows Task Scheduler. Alternatively, it may be appropriate to use Group Policy to distribute the start-up task to all runtime resources.

The command line method is:

```
[Blue Prism Install Location]\automate.exe /resourcepc /public
```

For example:

```
C:\Program Files\Blue Prism Limited\Blue Prism Automate\automate.exe" /resourcepc
/public
```

It is strongly recommended to additionally configure the runtime resources to authenticate against the Blue Prism platform by specifying valid Blue Prism credentials.

- Blue Prism native authentication environments: /user [username] [password]
- Blue Prism Single Sign-on environments: /sso

> ⚠ The use of native authentication, rather than single sign-on, is not recommended. However, if native authentication is a requirement, the username and password should only be entered when prompted and not hard-coded into the system.

For more information, see Runtime resource machines running multiple runtime resources below.

Physical security

The security of the Blue Prism runtime resources is paramount as these resources are responsible for executing the automated processes and where relevant will be logged on, and interacting with third-party applications, on screen, via the respective graphical user interfaces (GUI).

It is essential that physical access to these components is restricted to prevent unauthorized users from directly monitoring the actions being taken, and getting access to the data that is being processed. In addition, this helps to prevent users from being able to interrupt the process and take control of the data and applications that the runtime resources have authenticated against.

For security reasons, granting access to the runtime resources once established is not recommended – the ability to restart, shut-down and start up the instances should be sufficient.

Where remote access is granted to the runtime resources, such access should be subject to appropriate control and monitoring. For further information, see User accounts, remote access, and security on page 39.

Runtime resource machines running multiple runtime resources

In certain circumstances, a single runtime resource machine can host multiple Blue Prism runtime resources (i.e. multiple robots can operate simultaneously within a single instance of a windows desktop operating system). This is dependent on the technologies that are automated as part of the processes, which in turn must be developed with this execution approach in mind.

There are a number of potential challenges with this approach:

- Each process that runs simultaneously on a single runtime resource must be able to successfully identify the application(s) that were launched for its use. (For example, if there are five processes each using Microsoft Edge, each process must be able to successfully identify which is the appropriate one to use).

- Conflicts can occur if a thick client application is used as part of processes that run simultaneously, particularly where only one instance of the application can be launched at a given time (for example, Microsoft Outlook).
- Where multiple instances of a single application are used simultaneously, it is necessary that actions taken in one instance, do not affect the others. (i.e. logging out in one instance should not automatically log the user out of all instances).
- It may not be possible to use this approach where the processes use thin client technologies.
- Where the runtime resource connects to an application server, the connection must be configured to use dynamic ports for callback to avoid conflicts. If the callback port is statically defined, it will not be possible to operate multiple runtime resources on a single runtime resource unless a separate connection is configured for each.
- To configure a single runtime resource to have multiple runtime resources it is necessary to modify the start up configuration to initialize multiple instances of Blue Prism, each with its own listening port.

For further information on how to set up this configuration, see the Blue Prism Enterprise Edition Installation Guide.

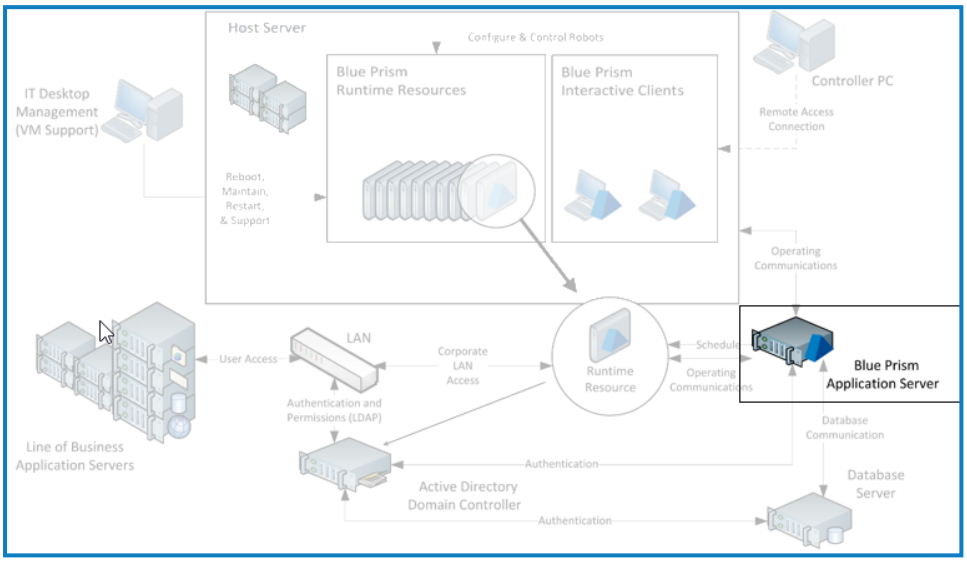
Event log

Typically any errors and warnings generated on the Blue Prism runtime resources are written to the Windows Event Log – it is therefore necessary for the accounts used on these resources to have permissions to create the appropriate entries. Additionally the Windows User Account Control can sometimes restrict this capability.

It is also necessary for the amount of space required by the Event Log to regularly reviewed and for appropriate maintenance to take place.

Blue Prism application server

The Blue Prism application server is an optional, but strongly-recommended, component within a Blue Prism environment.



The key features that are provided by the Blue Prism application server include:

- Marshaling all connectivity between the Blue Prism components, and between those components and the database.
- Provision of the Secure Credential Store.
- Data encryption and decryption capabilities.
- Process execution, which can be scheduled or manually instigated, utilizing Application Server Controlled Resources (ASCR).
- Triggering scheduled automations.

Minimum requirements: application server

The latest information about the minimum specifications of each Blue Prism component can be found in Blue Prism software and hardware requirements.

All minimum requirements must consider the selected operating system as well as the applications to be automated.

Blue Prism Application Servers are typically deployed to virtualized instances of Windows Server although for smaller or initial deployments, physical desktops can be used.

Each application server requires the Blue Prism runtime to be installed, and will require additional setup to enable the data encryption facility. See Install Blue Prism Enterprise Edition for further information.

The specification assumes a single application server that will service between 1 and 50 Blue Prism runtime resources. Whilst an increased specification can enable greater numbers of runtime resources to be serviced, depending on their level of activity (especially logging), it is recommended that a given Blue Prism application server should not be configured to be responsible for more than 100 Blue Prism runtime resources.

Frequently asked questions: application server

How are Blue Prism application servers typically deployed?

Typically they are deployed on to a dedicated, virtualized, Windows Server to provide security and scalability. There is the option to deploy to physical end-user desktops for smaller implementations.

What are the advantages of virtualizing this component?

Virtualizing the Application Server provides greater options for scalability and disaster recovery scenarios.

What are the security implications of this component?

When using Windows Authentication, any service accounts used should have the least privilege required. A firewall should also be installed around your Blue Prism environment, ensuring that only the necessary users and applications have access through the firewall. Overall, ensure the Blue Prism environment is secure, with only authorized users allowed to access the hardware and application.

Each Blue Prism application server instance holds the database connection information and the encryption key for the respective environment and by default this information is available to any user who can connect to the server file system. Common mitigations include:

- Using Windows Authentication for the database connection which negates the requirement to store the username and password within a Blue Prism configuration file.
- Use certificate encryption to protect the information within the configuration file.
- Storing the encryption keys within individual files and manually applying additional controls such as use of transparent encryption and restricting access to the files.

It is strongly recommended that you use certificate encryption for the application server configuration files. If you are using an SQL native connection to the database, using certificate encryption is essential. This can be accessed by clicking **Encryption settings** on the Server Configuration dialog in BPServer.exe and selecting **Use own certificate**.

It is important to note that where access is granted to this component, a given user will have access to this potentially sensitive configuration information for each environment – it is therefore important that this component is suitably secured and subject to restrictions in terms of physical and remote access. For more details, see User accounts, remote access, and security on page 39 and Blue Prism network connectivity on page 46.

Can a single Blue Prism application server be used across multiple environments?

An instance of a Blue Prism Application server services a single environment, however it is possible to co-host multiple application server instances on a single Windows Server.

The Multiple Blue Prism application servers on the next page section contains further information.

Does this component need to be backed up?

Yes, it is important to ensure that as a minimum the data encryption (credentials) key is backed up and stored securely.

Can the application server be containerized?

No, the Blue Prism application server can not run in a containerized setup.

Networking: application server

The main components that application servers initiate communications with include:

- **Runtime resources** – For the purposes of triggering scheduled and manually instigated processes using (ASCR) on a given runtime resource (TCP). See Application Server Controlled Resources (ASCR) for details.
- **Database** – Connectivity with the database server uses SQL server drivers and is therefore configurable. By default connectivity occurs using TCP.
- **Data Gateways** – The Data Gateways process must be enabled and the associated port defined on all application servers that are required to run Data Gateways. See for Data Gateways details.

Due to the high levels of communication between the application server and database it is necessary for application servers and the respective databases to be physically located locally to minimize latency between the components.

⚠ Blue Prism application servers should not be installed on any domain or network where there is internet facing access. The Blue Prism platform should be implemented into your environment as a separate entity. This can be achieved through network segregation, for example, using jump servers for cross-domain travel, or other similar methods. It is advised that you also consult the Robotic Operating Model (ROM) Security information on the Blue Prism Portal for recommendations of best practice.

Application server configuration

The Blue Prism application server section of the *Blue Prism Enterprise Installation Guide* provides instructions on how to configure an installation of Blue Prism to take on the role of a Blue Prism application server.

Multiple Blue Prism application servers

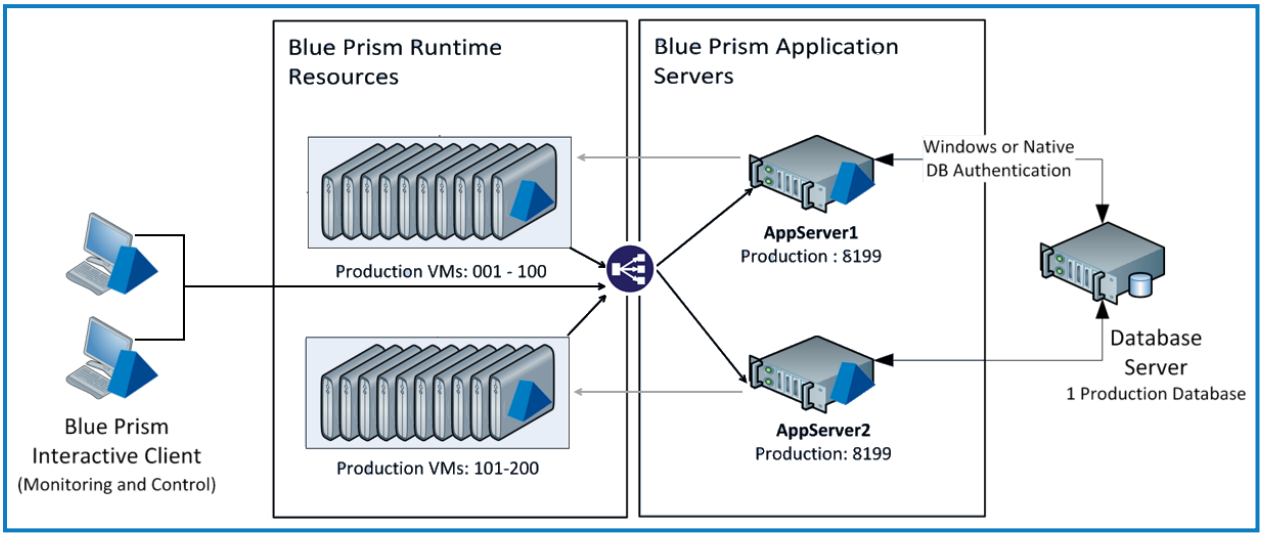
As part of a Blue Prism infrastructure there may be a number of Blue Prism application servers for the purposes of providing resilience and availability, providing scalability for large numbers of runtime resources, or to provide functionality to a number of different environments (development, test, production).

The common configurations for provisioning multiple Blue Prism application servers are described below.

Distributed servers: multiple servers for a single environment

A single environment (e.g. Production) may have a number of application servers to allow the workload to be distributed across them and/or for the purposes of introducing resilience.

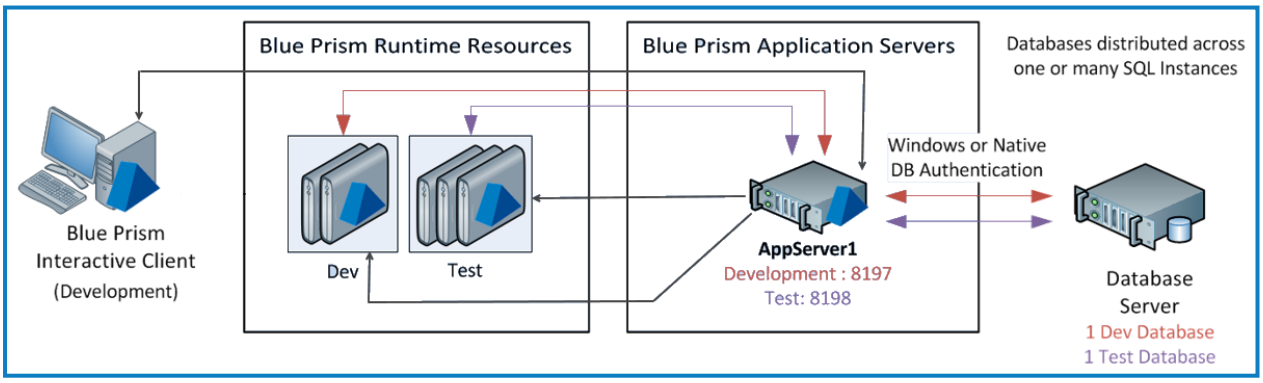
In this scenario each Blue Prism application server would be setup with an identical configuration and would be connected to the same database.



Shared servers: one server for multiple environments

A single Windows Server can be configured to host multiple Blue Prism applications, each of which is responsible for an independent environment (albeit within the same network).

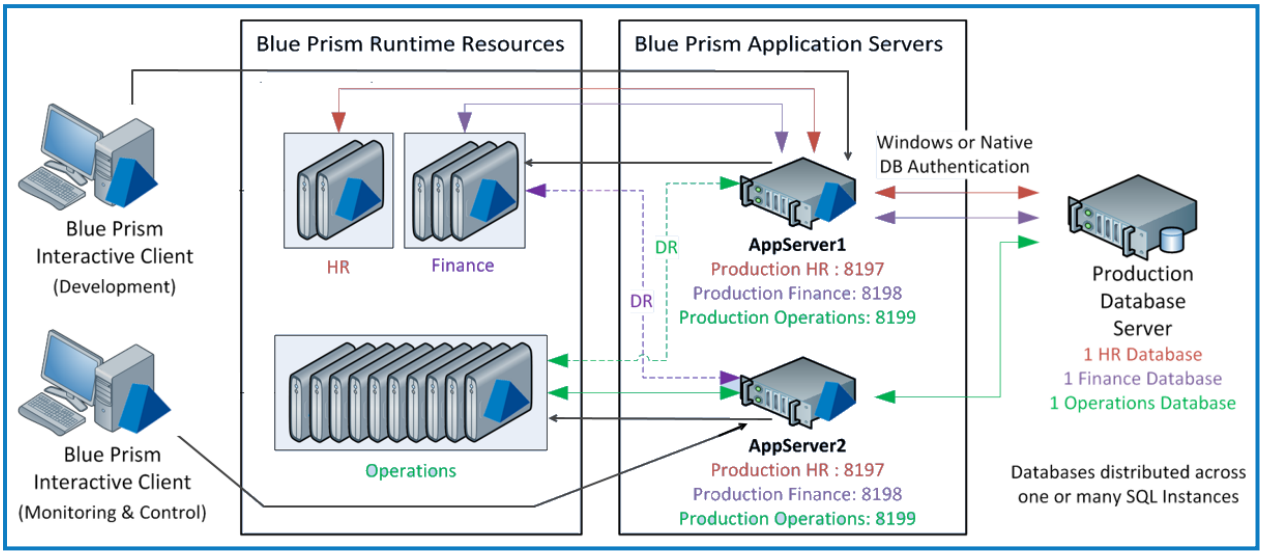
When configuring multiple Blue Prism application servers on a single Windows server it is important to review the combined maximum number of Blue Prism runtime resources that will need to be serviced concurrently.



Hybrid: multiple servers for multiple environments

A hybrid approach can be taken to provide both resilience and the ability to service a high number of Blue Prism runtime resources across multiple environments.

The example below shows a scenario where a separate Blue Prism environment (with a dedicated database) has been used for each core business area and therefore there are a number of production environments to be serviced.



Considerations for deploying multiple application servers

When deploying multiple application servers to for a single environment (e.g. Production), it is necessary to consider the following:

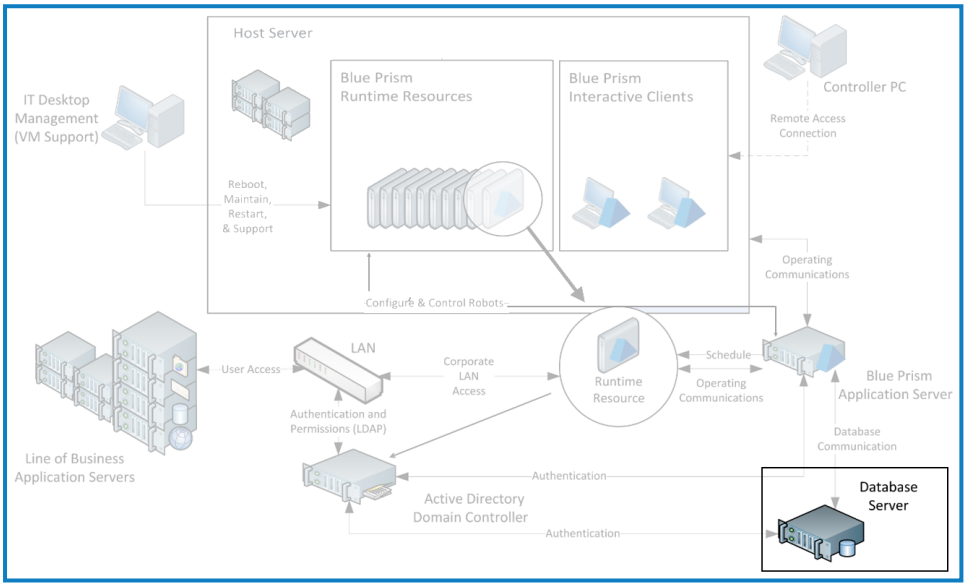
- Where multiple Blue Prism servers are deployed for the same environment each one must be configured to use the same time zone.
- The configuration of the encryption schemes on each server must be identical to allow all servers to perform consistent encryption and decryption of sensitive data.

Blue Prism database server

Each Blue Prism environment uses a Microsoft SQL database as a central repository of configuration data, settings, runtime transactions and logs.

The solution permits any number of instances of the Blue Prism schema to be deployed within a given SQL instance on Microsoft SQL Server, allowing multiple Blue Prism environments to be configured within a single Microsoft SQL instance.

Support is also provided for Microsoft SQL Azure. Refer to the Blue Prism Reference Architecture for Microsoft Azure for further details.



Key features:

- Central repository for all Blue Prism configuration information such as processes, objects, and workflow configuration.
- Third-party system user credentials store.
- Work queue repository.
- Stores audit information and production process log data – a transaction log of each process running in the environment.

Minimum requirements: database server

The latest information about the minimum specifications of each Blue Prism component can be found in Blue Prism software and hardware requirements.

Sizing

The requirements of the database server directly correlate to the number of deployed Blue Prism Runtime Resources. Data file size should be reviewed during implementation according to logging requirements, running hours and data retention policy as this will vary if data is retained for prolonged periods. Backup and log truncation should be reviewed according to business criticality.

Environment	Data file	Log file	Sizing notes
Development	50 GB	25 GB	
Test	50 GB	25 GB	
UAT	5 GB x no of runtime resources	50% of data file	Data file minimum size: 100 GB
Production	5 GB x no of runtime resources	50% of data file	Data file minimum size: 200 GB

For detailed information, and best practice, on sizing your Blue Prism environment, see Scaling your Blue Prism Platform in the Robotic Operating Model (ROM) section of the customer portal.

Frequently asked questions: database server

How are Blue Prism Databases typically deployed?

The database can be deployed to a physical SQL Server instance. Alternatively, it can be deployed to a high-specification, well configured, virtualized database. It is common for non-production databases to be contained within a single SQL instance, and for the production databases to be hosted within a production-strength single SQL instance (often one which offers redundancy through mirroring, clustering or use of AlwaysOn Availability Groups (SQL AAG)).

What are the security implications of this component?

As with all application databases, the Blue Prism database(s) must be secured as this database is the main repository for a range of information including: process configuration; credentials for third-party systems; work queues; logs and audit information.

The sensitive data is encrypted prior to storage however this is not a substitute for database security.

Can a single Blue Prism Database Server be used across multiple environments?

A single Blue Prism Database Server can be used across multiple Blue Prism environments as each environment requires an independent database which can be co-hosted with other Blue Prism databases on a single SQL instance.

Does this component need to be backed up?

Yes, it is important to ensure that the database and logs are subject to frequent, full backups (a complete backup of your SQL Server database) and are also in line with your own data recovery policies.

Are PaaS databases supported?

Yes, your Blue Prism database can be deployed as a service (PaaS) database engine. Currently, Azure SQL, Azure Managed Instance, and AWS RDS are supported databases.

Provisioning a Blue Prism database server

There are a number of settings and considerations to be applied when designing and provisioning a Blue Prism database server. These considerations include topics such as:

- Selecting an appropriate server or instance.
- Disk space configuration and utilization.
- CPU and RAM allocation.
- Database growth.
- Recommended database settings.

Creating/upgrading a Blue Prism database

There are two main options for creating or updating a Blue Prism database:

- **Product driven** – The software will create and maintain the database during installation and upgrades. CREATE and ALTER TABLE privileges are required by the Blue Prism server.
- **Script driven** – SQL scripts for database creation and updates can be generated.

SQL permissions

The minimum SQL permissions required on the Blue Prism database for normal operation are:

- db_datareader
- db_datawriter
- All roles prefixed with bpa_. For example:
  - bpa_ExecuteSP_DataSource_bpSystem
  - bpa_ExecuteSP_DataSource_custom
  - bpa_ExecuteSP_System

The roles prefixed “bpa_” are only available once the database has been configured using the in-product Create Database functions or manually using the CreateScript command.

The minimum SQL permissions do not provide appropriate privileges to carry out Create or Upgrade database actions from within the product, therefore an appropriate administrator account will need to be used when any of these actions are required:

- Create database – dbcreator (server role) or sysadmin (server role)
- Upgrade database:
  - When deleting the existing database – sysadmin (server role)
  - When not deleting the existing database – sysadmin (server role) or dbowner (database role)

To manually execute the Create or Upgrade database scripts (available via Blue Prism Support) against an existing database, the following SQL permissions are required by the user carrying out the actions:

- DBCreate: dbcreator (server role) or sysadmin (server role)
- DBUpgrade: sysadmin (server role) or dbowner (database role)
  - When deleting the existing database – sysadmin (server role)
  - When not deleting the existing database – sysadmin (server role) or dbowner (database role)

Additionally, it is recommended to grant the execute permission to the SQL user running the Blue Prism database to the custom table type `<schemaname>.IntIdTableType`. An example of the SQL command is shown below where [dbo] is the <schemaname> and [User] is the SQL user running the Blue Prism database:

```
GRANT EXEC ON TYPE::[dbo].[IntIdTableType] TO [User]
GO
```

If this permission is not granted, users will be unable to view session logs from Control Room, unless they are an admin user. The Session Logs table will display blank and an error message will show in the Blue Prism Event Logs for the application server, for example:

System.Data.SqlClient.SqlException (0x80131904): The EXECUTE permission was denied on the object 'IntIdTableType', database 'BPv7', schema 'dbo'.

For details of permissions required for Blue Prism users, see User accounts, remote access, and security on page 39.

Maintaining a Blue Prism database server

It is important to ensure that there is regular maintenance of the SQL server to:

- Facilitate a stable platform.
- Highlight potential issues.
- Proactively ensure maximum performance based on the hardware resources available.

The key maintenance topics include:

- Backups.
- General server maintenance.
- Database maintenance and recommended settings.
- Blue Prism in-product maintenance.

Database usage patterns

Communication between the Blue Prism runtime resources, application servers and database is typically moderate to high in volume, and transactional in nature as records are frequently inserted into the session log, along with look-ups and updates being performed within workflow tables.

Consideration should be given to the proximity of the database server to the Blue Prism application server and runtime resources, particularly when implemented across large or multi-site networks. Where network latency is an issue, it will be made more prominent by the frequency of the queries performed.

Commonly the Blue Prism database will receive direct connections only from each Blue Prism application server within a given environment.

In some circumstances, such as where application servers are not deployed, any Blue Prism component can be configured to establish a direct database connection. This will be subject to the application of appropriate routing, authorization, and access settings.

The number of connections that will be established by each directly connecting device is managed by the WCF Framework through use of SQL connection pools.

Blue Prism data

This section introduces a number of the key types of transactional data such as logs and history that are stored within the database as part of ongoing use and operation of Blue Prism.

Sessions and logging

Blue Prism processes contain a number of steps (or stages) that the runtime resources follow as part of executing the process. These stages can represent a variety of actions including: calculations, decisions, reading data from a user interface element, executing a sub-process or action etc.

Sessions are used by Blue Prism to record all of the appropriate stages followed by a runtime resource as part of executing a business process. The amount of logging for each stage is configured as part of the process design but typically each log generated will include:

- The execution time
- The context in which the process is being run
- Any input/output parameters from the stage

Over time, and based on the level of logging that has been configured, the data collected as a result of session logging is often the largest data set within a production Blue Prism environment and the archiving facility can be used to restrict the impact of this.

In order to maintain integrity, the generation of sessions and associated session logs occurs synchronously as part of process initiation and execution. Whilst the amount of data per transaction is low, the frequency and requirement for rapid processing by the database is paramount.

Work queues

Work queues provide the storage and workflow capabilities for processes. Each work item typically represents an individual record - its data, status and history. A work item has a number of statuses including: pending, deferred, locked, completed, and terminated. If a work item is terminated by the process, it may be retried automatically - each queue can be configured with a set number of automatic retries.

Each work item attempt is represented by an individual record in the BPAWorkQueueItem table, therefore if a work item is worked, terminated and a retry action generated, it will be represented by two rows in the table. Work items can be assigned tags which provide supplementary information such as categorisation and these are defined in the BPATag table and each assignment of a tag to a work item attempt is represented by a record in the BPAWorkQueueItemTag table.

The BPAWorkQueueLog is used to record each operation which alters a work item (e.g. additions, status change, deletions).

Audit logs

Audit Logs are used to record all of the following actions:

- Login / Logout
- Changes to environment-wide settings
- Create/Update/Delete of: business objects; processes; queues
- When recording changes to processes and objects all details of the changes being applied are captured to allow for comparison or rollback at a later date.

The audit log table (BPAAuditEvents) can grow to be quite large where there is a high frequency of updates to processes or objects. This typically does not affect production databases as the largest number of changes take place in development or test environments.

Schedule logs

Schedule logs are created for each schedule that is initiated and record the time and outcome for all tasks and sessions that form part of that schedule. Whilst the number of schedule logs may grow to be quite large (the most basic schedule would create a minimum of 6 log records), the amount of information per row is very small so it is unlikely to be cause for concern.

Alerts

Alerts can be configured to indicate to end-users when certain events are detected within sessions or schedules. An alert is targeted to a particular user and has a delivery method (e.g. pop-up box, system sound etc.). Each individual alert is stored in a record on the BPAAlertEvent table.

Security alerts

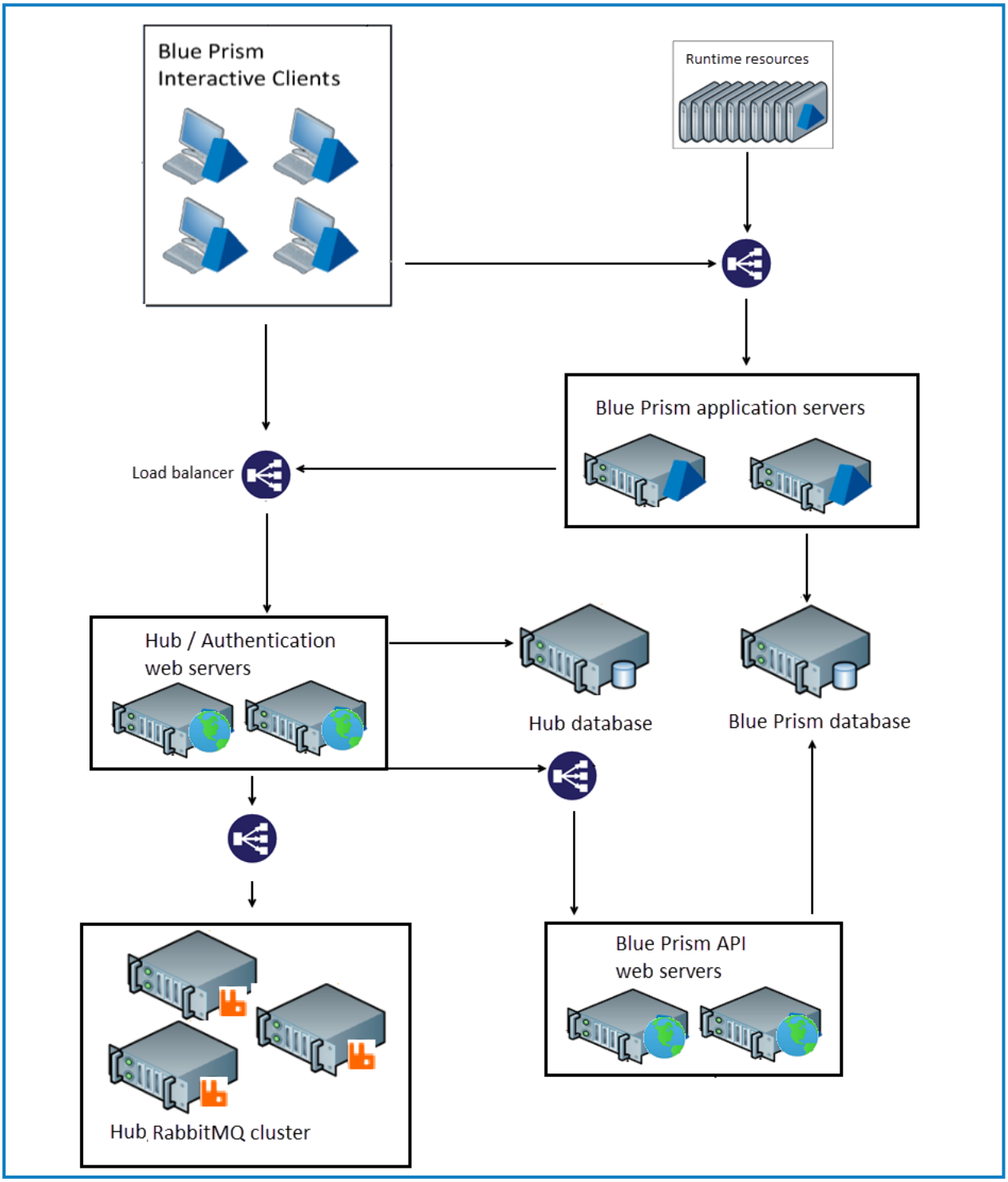
To utilize the session and audit logging mechanisms as a security measure, it is recommended that you implement additional event monitoring and alerts to capture erroneous or unexpected behaviors. For example, monitor for multiple failed log ins from a user in a short space of time.

Blue Prism Hub Control Room

Hub Control Room is a Hub plugin which provides Blue Prism users with the ability to view and manage Blue Prism activity for all their environments. The Hub Control Room interacts with the Blue Prism database via the Blue Prism API.

The latest information about the minimum specifications of each Blue Prism component can be found in Blue Prism software and hardware requirements.

The following diagram shows the Hub Control Room architecture in a highly available environment.



For details of how to install Hub and the Control Room plugin, see Installing Hub. For details of Hub Control Room plugin, see Control Room.

Frequently asked questions: Hub Control Room

Which version of Blue Prism is required to run the Hub Control Room plugin?

Blue Prism version 7.0 onwards is compatible with the Hub Control Room plugin. See the Blue Prism release notes for details of component compatibility.

Can Blue Prism Hub co-exist on the same application server as Blue Prism Enterprise?

No, Hub should be deployed to its own server.

Does the Hub Control Room plugin have its own database?

Yes, the Hub Control Room database is separate to the Blue Prism database.

Can the Hub Control Room database be hosted on the Blue Prism database server?

Yes, but the scale of your environment must be considered when making this decision.

Can Hub Control Room be installed in a HA configuration?

Yes. See Hub's High availability configuration documentation for details.

Can any other messaging application be used?

No, only RabbitMQ is supported.

Can RabbitMQ be hosted on the Hub server?

Yes, however, this is dependent on the scale of the environment. High availability of RabbitMQ must also be considered.

Can self-signed certificates be used?

Yes, but it is not recommended for UAT /production environments.

Blue Prism API

The Blue Prism API provides a common interface for components such as Blue Prism Hub and subsequently the Control Room plugin to connect with the Blue Prism database. It also provides a series of predefined capabilities that can be used by custom solutions to interact with Blue Prism programmatically using a RESTful API.

> The Blue Prism API depends on the Hub Authentication Server for authentication, as such, it is the only Blue Prism Enterprise component with a dependency on a Blue Prism Hub component.

The latest information about the minimum specifications of each Blue Prism component can be found in Blue Prism software and hardware requirements.

Blue Prism Hub Control Room on page 35 includes a diagram of the Blue Prism API in a highly available environment.

For details of how to install and configure the Blue Prism API, see Blue Prism API.

Frequently asked questions: Blue Prism API

Does the Blue Prism API only work with Authentication Server authentication?

Yes, Authentication Server is required to use the Blue Prism API.

Can the Blue Prism API co-exist on the Hub server?

Yes, but the scale of your environment and high availability must considered when making this decision.

Does the Blue Prism API have its own database?

No, a separate database is not required.

Can the Blue Prism API be installed in a highly available (HA) configuration?

Yes, this is supported.

RabbitMQ and Erlang OTP

RabbitMQ, which is reliant on Erlang OTP, is a queue management system and is a prerequisite for Blue Prism Hub. It handles the communication between the Blue Prism Hub Control Room and Blue Prism Enterprise. It is a distributed message broker system that uses Advanced Messaging Queuing Protocol (AMQP) for transfer of messages. AMQPS can be used for secure message transfer.

A Message Broker Server must be available hosting RabbitMQ Message Broker. For more information, see:

- Installing Hub – Details of RabbitMQ requirements for Blue Prism Hub.
- RabbitMQ.com – RabbitMQ's own user documentation.

User accounts, remote access, and security

There are a number of interactions for which user accounts are required as part of a Blue Prism implementation. Examples of these interactions include:

- The user accounts used by the runtime resources to authenticate against the network or workgroup.
- The user accounts the runtime resources will use to access and automate the line of business applications.
- The user accounts used by Blue Prism controllers, and process developers to configure, develop, release, deploy processes and the associated queues, schedules and settings.

Security should also be considered in reference to:

- Access (including remote access) to the various Blue Prism components (e.g. application server, runtime resources, interactive clients, database server etc.)
- The logical access permissions granted to each user in relation to the actions available to them within a given Blue Prism environment.

User accounts: runtime resource network authentication

Considerations for the user accounts to be used when runtime resources are authenticated to the domain or workgroup include:

- Whether auto-login is required, and how this will be achieved.
- The authentication methods required for the applications that are to be automated (e.g. whether they use Active Directory integrated authentication commonly referred to as Single Sign-On (SSO)).
- Whether the out of the box functionality is to be implemented that allows Blue Prism to automatically manage the credentials used; including periodically resetting these user account passwords (whilst adhering to password complexity and history policies).

Further information is provided in relation to the user accounts and auto-login options in Blue Prism Runtime Resource.

User accounts: line of business applications

It is necessary for the Blue Prism runtime resources to have appropriate access to each of the line of business or third-party applications that are automated within Blue Prism processes. It is recommended that a user account with appropriate permissions is made available for each of the Blue Prism runtime resources that will have a concurrent connection to a given application although there is support for Blue Prism runtime resources to use shared credentials if required.

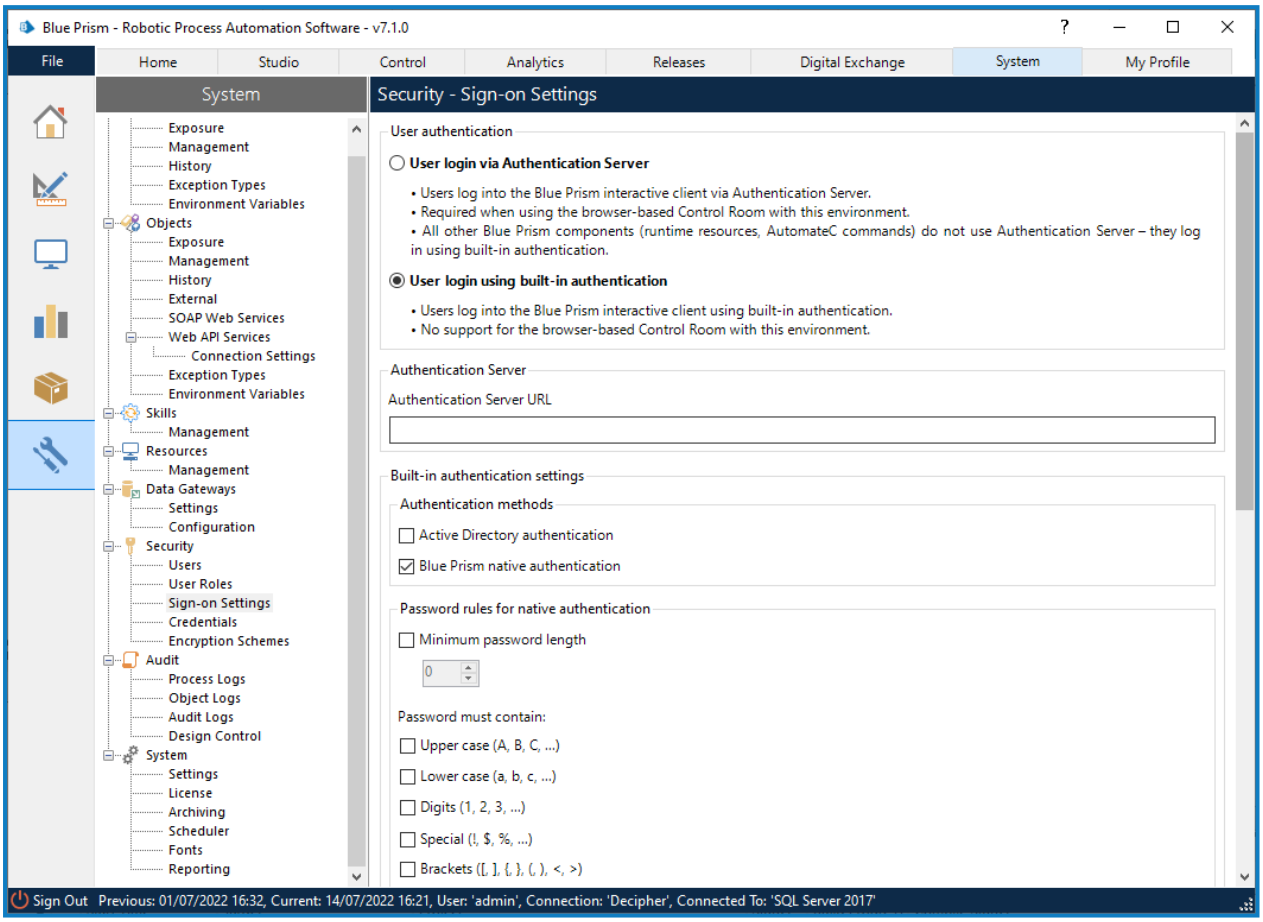
The credentials for the user accounts used as part of a Blue Prism process should be securely stored, independently of the process definition, within a centralized Credential Management repository.

Access to specific credentials should be restricted to specific runtime resources, processes and users in order to prevent authorized use within the environment.

Blue Prism processes can be configured to periodically change the line of business application password (s), taking account of necessary password complexity requirements, which ensures that the credentials are not known by any human operator.

User accounts: Blue Prism users (controllers / process developers)

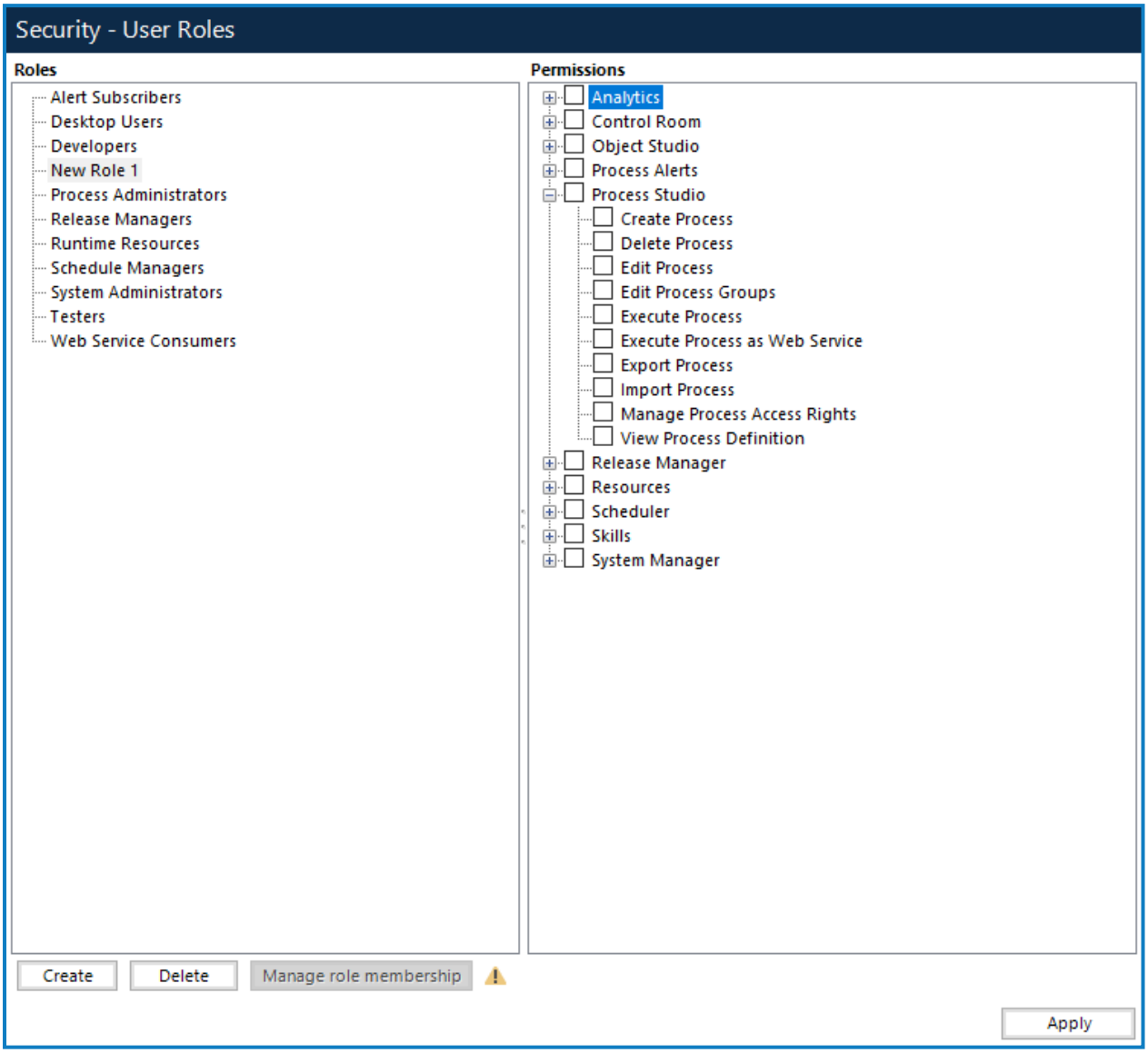
By default, Blue Prism's native authentication is used to manage user access to the Blue Prism application and for assigning appropriate controls and permissions to each user.



Alternatively, Blue Prism can be integrated with Active Directory Domain Services for controlling and configuring user access and control. See Active Directory Integration for more information.

Optionally, both native authentication and Active Directory can be utilized in a Blue Prism Enterprise environment. In this case, native authentication should only be used for a super administrator account, with highly restricted user access for authentication users only, in order to administer Active Directory issues if they occur. Active Directory should be the standard user authentication option.

Irrespective of the type of authentication selected, user access is role-based and configured independently for each environment allowing specific users to have different access dependent on the environment. This further supports the ability to restrict any one user having ubiquitous access across all environments.



Security access

Typically it should be appropriate for all components of the Blue Prism solution (excluding the Blue Prism interactive clients) to be locked down to prevent any access by Blue Prism administrators or users. The only functions required are those typically used by administrators such as: restart; shutdown; start-up; purge event log etc.

Remote access

If there is a requirement to implement remote access for any of the Blue Prism components, the various security implications for each component should be considered – further information is provided within the respective sections:

- Blue Prism runtime resource
- Blue Prism application server
- Blue Prism database server
- Blue Prism API server
- Blue Prism Hub server
- RabbitMQ server

It is also important to select a suitable tool for providing remote access which interacts with the target system in an appropriate manner (e.g. without interrupting the current session), and which provides a suitable level of security and governance – particularly considering that typically a number of the components will already be logged on and available.

Microsoft Remote Desktop Connection (RDP) is explicitly specified as being unsuitable for remote control of a runtime resource, as the remoting connections are intrusive – meaning that the RDP session would interrupt ongoing automated processing.

Security: Logical access permissions

The logical access permissions that need to be configured are typically defined as part of the project initiation and Blue Prism supports using a mixture of bespoke and out-of-the-box security roles to allow each user to be allocated the appropriate access in each environment.

Examples of roles that are often reviewed as part of this definition are included below:

- Create, read, edit, delete processes
- Create, read, edit, delete business objects
- Compare, export, import processes or business objects
- Define release package, create release
- Create, edit, delete schedules
- Full or read-only access to queues / sessions
- Access to define system settings, users, credentials etc.

It is necessary to establish any logical access restrictions that will be implemented to provide an appropriate level of control and governance across the various environments. These may include:

- Preventing any development from taking place in the production environment.
- Restricting which users are able to migrate processes (and associated items) between various environments.
- Identifying which users will be responsible for the settings, configuration, user access etc.
- Identifying which users will have access to the various types of audit and logs.

Active Directory integration

This section provides an overview of how Active Directory is integrated with Blue Prism, for more details, see Active Directory Integration. For details of Authentication Server, see the Authentication Server Configuration Guide.

There are a number of common considerations when deploying Blue Prism within an Active Directory Network Infrastructure:

- How runtime resources can authenticate against target business applications using single sign-on.
- A common Active Directory Network Infrastructure allows native encryption of internal Blue Prism communications.
- User access to the Blue Prism platform can be configured to use single sign-on where user accounts reside in trusted forests.

Runtime resources accessing target applications using single sign-on

The 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, for example, 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 account via Active Directory.
- Simplifies access to network resources such as shared drives, mailboxes, printers, and so on.

Active Directory allowing natively secured internal Blue Prism communications

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.

If using the following connection modes with a Blue Prism Server connection, a Service Principal Name (SPN) must be configured against the Active Directory (AD) account under which each Blue Prism Server service instance is running:

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

Further information on securing connections by enabling message security is provided in the Securing Blue Prism Network Connectivity data sheet.

Configuring the Blue Prism platform to authenticate user access via single sign-on

Blue Prism 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 security role after which users will be granted access to the platform based on their Active Directory Security Group membership.

Valid scenarios for deploying Blue Prism with single sign-on include:

- Where all user accounts and all Blue Prism components reside within a single Active Directory forest with appropriate trusts between all relevant domains.
- Where the Blue Prism application server resides within a domain that has appropriate trusts between other domains in the same forest, or other forests; and user accounts and Blue Prism components reside in any of these domains. For more information, see Supported Active Directory infrastructure.
- Where all user accounts and all application servers and interactive clients reside within a single Active Directory forest with appropriate trusts between all relevant domains, and where Blue Prism runtime resources reside outside the domain and network. These Blue Prism runtime resources will not be able to carry out authentication tasks e.g. they cannot be used to host Blue Prism Web Services, and they Blue Prism interactive client on these devices cannot be used.

Where it is not appropriate to use single sign-on for Blue Prism, native Blue Prism authentication can be used.

> Active Directory Integration for user authentication must be configured as part of the database creation therefore it is important to establish whether this is required prior to installing and configuring Blue Prism.

Configuring Active Directory integration

> Further information on Active Directory configuration is provided in the Enterprise Edition Installation Guide and the Active Directory integration guide.

The following steps are required to configure Active Directory integration.

Enable Active Directory authentication in Sign-On settings

As a Blue Prism user with System Administrator privileges, navigate to the System > Security - Sign-on Settings screen in the interactive client and enable the **Active Directory authentication** option.

Configure the required Active Directory security groups.

Within the selected Active Directory domain a Security Group should be created for each Blue Prism role that will be used. Commonly an independent set of Security Groups will be configured for each Blue Prism environment (E.g. Dev, UAT, Production).

The group membership for each of the created Security Groups should then be setup to ensure that the correct AD User Accounts are members of the appropriate groups.

Commonly the Security Groups will be configured with a Domain Local or Universal Scope, and users from any trusted domain within the same forest will either be added directly to the Security Group, or they will be member of a Universal Group which itself is a member of the configured group.

> Built-in Groups or Groups with derived membership such as Domain Users and Authenticated Users should not be used. It is recommended specific Security Groups are created and these should be mapped to Blue Prism Security Roles. Likewise if using nested group membership, the nested groups should not be built-in groups.

Add Active Directory domains

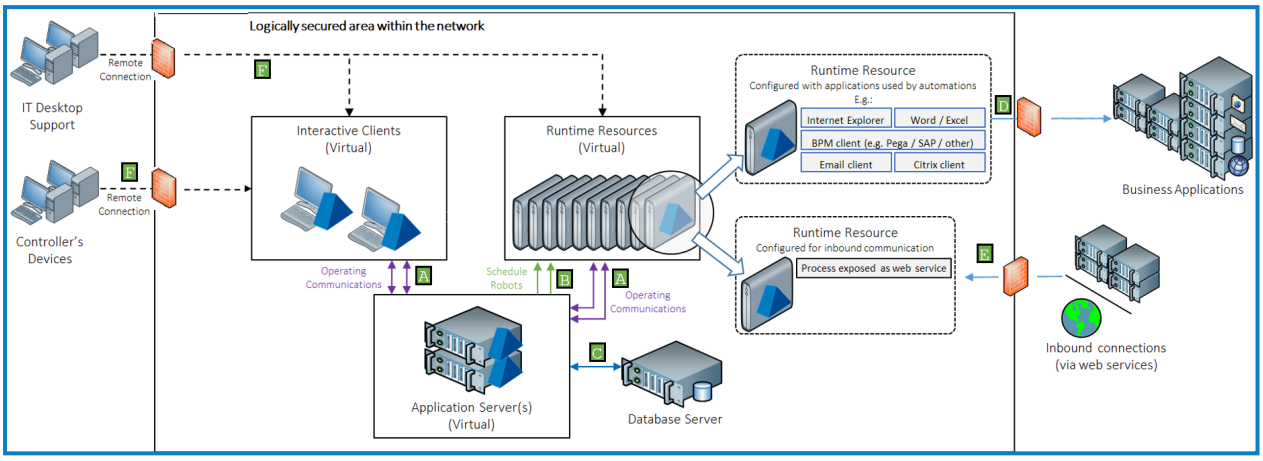
Add an Active Directory domain record for each domain where the user executing Blue Prism server (or the interactive client on a direct database connection) does not have permission to query Active Directory for that domain. For more information, see Active Directory domains.

Associate each Blue Prism Role with the respective Active Directory security group

Within Blue Prism each Blue Prism role should be linked with the appropriate Activity Directory Security Group. It should be noted that it is possible for there to be a different number of security roles based on the environment. For example, a production environment will not normally have a Developer role configured as development should not take place directly within production.

Blue Prism network connectivity

The diagram provides an overview of the common communication that occurs with the Blue Prism platform.



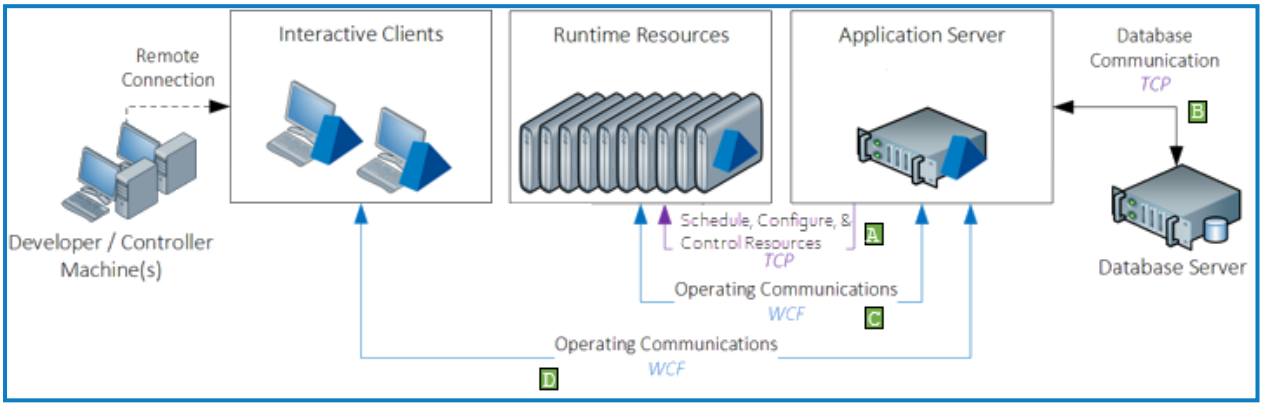
Communication		Description	Encryption options
Blue Prism connections to application server	A	Primary communication stream for the devices to send data to, and receive data from the database (via the application server).	Natively encrypted by default when all Blue Prism components are deployed within an Active Directory Network Infrastructure.
Instructional connection to runtime resources	B E	Instructions received by runtime resources. E.g. to start/stop processing; or to provide a status update.	Certificate-based encryption can be applied by manually deploying an appropriate certificate to each runtime resource and updating the device start-up parameters.
Blue Prism database connection	C	The read/write connection between the application server and database.	Certificate-based encryption can be applied to the connection by leveraging SQL Server functionality which can auto-generate self-signed certificates or leverage an existing verifiable certificate.
Runtime resources connecting to target applications	D	Runtimes interact with business applications as part of the process automation.	Dependent on the security provided by each respective third-party target application based on the nature of each connection.
Remote connectivity	F	The users who control the platform will commonly use a remote connectivity tool to access centrally deployed devices.	Leverages the security provided by the respective third-party remote connectivity tool.

See Default ports on page 49 for more information.

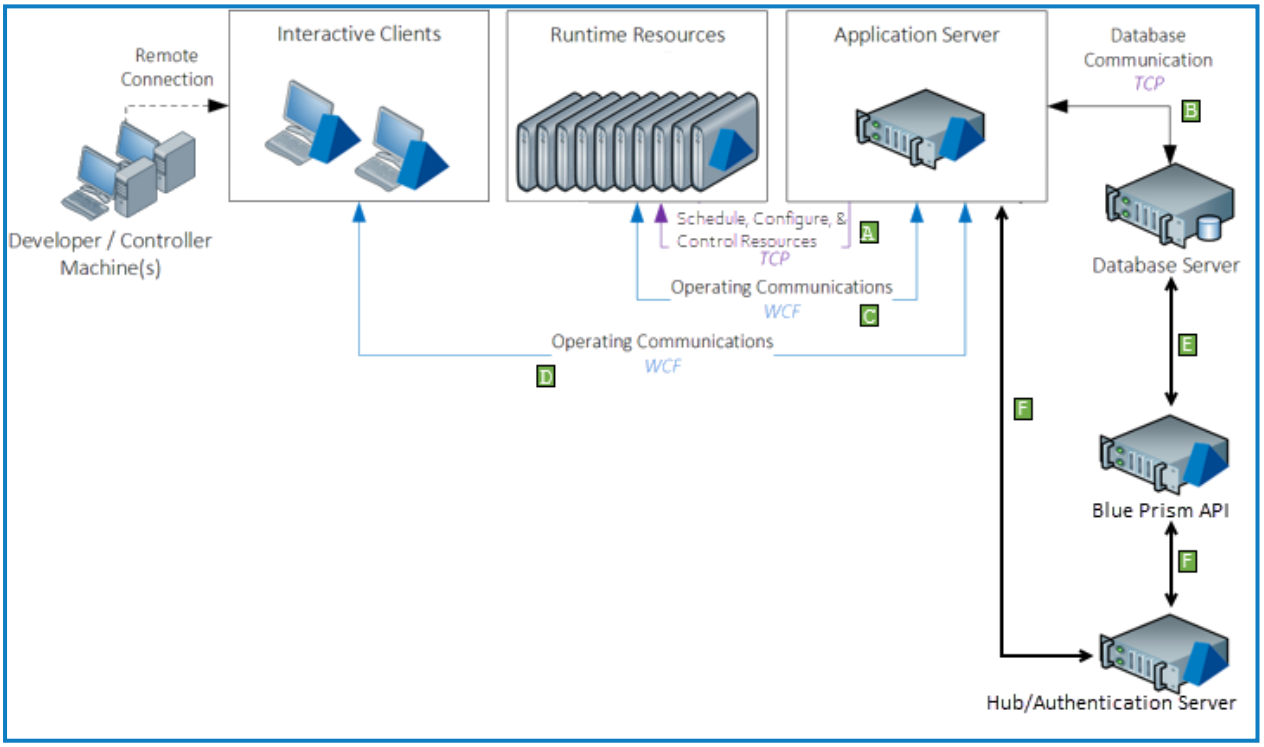
Inter-component communication

This section provides an overview of the key communication channels that are used between the various Blue Prism components.

Standard Blue Prism Enterprise communication



Blue Prism Enterprise with Hub Control Room communication



Communication details

Further information about the typical communication that takes place between the Blue Prism components is detailed in the table below.

Communication		Description
Application server	A	**Instructional: schedule robots (TCP)** Communicates with the appropriate runtime resource to advise that a specific process is scheduled to be run. Once advised, the runtime resource then establishes a WCF/.NET connection with the application server to retrieve the process configuration and for on-going communication. **Instructional: configure and control robots (TCP)** Communicates with the appropriate runtime resource to advise that a specific process is to be run. Once advised, the runtime resource then establishes a WCF/.NET connection with the application server to retrieve the process configuration and for on-going communication.
	B	**Database communication (typically TCP/IP – optionally leveraging certificate-based encryption)** Connects directly to the database for read/write operations as requested by the various Blue Prism components. The connection security is defined by: the connection to SQL Server; the configuration of the SQL Server instance, or through use of external technologies such as IPSec.
Runtime resource	C	**Operating communications (WCF/.NET)** Communication such as, process configuration retrieval; submitting system or process logs; saving changes; and requesting a single-use token prior to communicating with a runtime resource; takes place over a secure WCF connection which is established with the application server. **Instructional: resource pool communications (TCP)** Where implemented, runtime resources communicate with members of the same resource pool for the purpose of distributing process execution tasks.
Interactive client	D	**Operating communications (WCF/.NET)** Communication such as: process configuration retrieval; submitting system or process logs; saving changes; and requesting a single-use token prior to communicating with a runtime resource; takes place over a secure WCF connection which is established with the application server.

Communication		Description
Blue Prism API	E	**Operating Communications (Typically TCP/IP – optionally leveraging certificate-based encryption)** If the API has been configured to use Windows Authentication for the account that the API will use to communicate with the Blue Prism database, the Blue Prism API application pool in IIS will need to be updated to run as a user with appropriate access to the Blue Prism database.
Hub/Authentication server	F	**Operating communications (REST/HTTP)** To interact with the Blue Prism API directly, at least one service account with permission to the Blue Prism API must be created in Blue Prism Hub to store the client ID and secret that users must provide to Authentication Server in order to authenticate their requests. Should users require different levels of permissions for interactions with the API, separate service accounts should be created and assigned the appropriate level of permissions. **Authentication server operating communications (WCF/.NET)** To add users from Authentication Server into Blue Prism and to synchronize the user data, the details of the service account created to make authenticated requests to the Authentication Server API must be configured on the Blue Prism application server.

Default ports

Whilst all ports used by each component are configurable, the default ports are detailed below:

Component	Default port information
Application server	Listens for TCP traffic on **8199** (configurable).
Application Server Controlled Resources (ASCR)	The default value for gRPC is **10000** (configurable). For WCF, this value is applied to the outbound function only. The inbound function defaults to port 80, which is opened on the interactive client and is not currently configurable.
Interactive client	If using .Net Remoting, receives inbound traffic on the callback port number as defined within the connection to the application server.
Runtime resource	Listens for TCP traffic on **8181** (configurable). If using .Net Remoting, receives inbound traffic on the callback port number as defined within the connection to the application server.

Where there are multiple application servers co-hosted on a single operating system it is common for each to use an independent, dedicated port. This may be common where there are multiple Blue Prism environments.

Where there are a multiple runtime resources configured on a single runtime resource machine, each will be configured to listen on an independent, dedicated port.

Latency

Consideration should be given to the connectivity between the Blue Prism components, as any network latency will be made more prominent by the frequency of the queries performed.

Latency must be minimal between the following components:

- Application Server(s) and the respective Database Servers
- Interactive Clients and Application Server(s)

The only communication channels that are designed to support high-latency connections are those to/from the Blue Prism runtime resources, however consideration to this should be applied when designing the process automations to ensure appropriate performance. E.g. in terms of the frequency of communication with the other components such as requesting or writing items from the database, writing logs, updating queue items, auto-save settings etc.

Multi-site single sign-on

If Active Directory forests/domains are hosted on separate physical networks to the Blue Prism application server, it may be necessary to provide domain controller name mapping records to ensure the application server can query the Active Directory domain. For more information, see Troubleshooting – Single sign-on for details.

Name Resolution

The communication that takes place between Blue Prism components requires the ability to resolve the IP address of the target machine using its name. An example of such communication is when the application server instructs a runtime resource to start a process based on the configured schedule, or when a runtime resource communicates with another in the same resource pool.

By default, the communication takes place using the short-name of the target machine (e.g. using robot001, not robot001.mydomain.local) and requires DNS to be configured appropriately.

System Administrators can optionally change this setting if appropriate for the deployment:

- Register and communicate using machine (short) name – default
- Register using machine (short) name, communicate using FQDN
- Register and communicate using FQDN

Register: The name format used when registering runtime resources is the one which is featured when managing and configuring the platform (e.g. within session logs, schedules and control room etc.).

Changing the name format used for registering components will require each to register as new devices within the environment meaning that any previous runtime resource configuration may need to be repeated (e.g. configuring resource groups and resource pools, assigning access to credentials, schedule configuration etc.).

Connect: The name format used when connecting to the devices and is therefore the name that must be resolvable to an IP address from each of the devices were connections can be initialized.

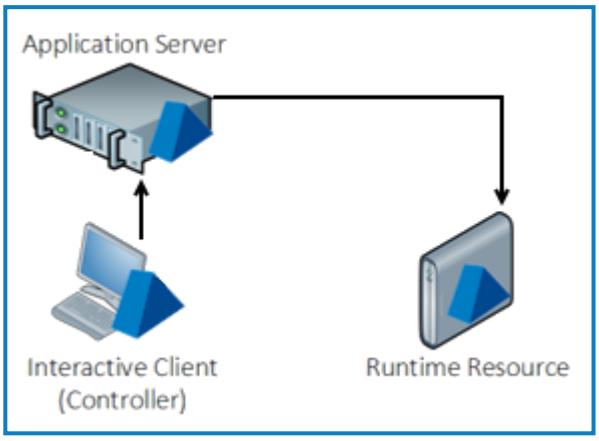
IP Layer Security

In addition to the controls natively provided by the platform, additional network protection can be achieved through use of industry-standard technologies such as IPSec which is able to protect all application traffic over an IP network.

Advanced information

Instructional communication

The instructional communication represents the frequent, lightweight, communications received by the runtime resources. Examples include scenarios such as where the runtime resource receives a request from:



- The Application Server informing the runtime resource to initiate the start process procedure.
- An interactive client manually instructing the runtime resource to initiate the start process procedure via the application server (ASCR).
- Another runtime resource in a ResourcePool to initiate the start process procedure.
- The Interactive Client requesting a status update.
- A third-party system accessing a Blue Prism web service.

Within the Blue Prism platform, these connections are established from each application server to each available runtime resource using its configured listening port (default 8181).

If Transport Layer Security (TLS) is your required communication method, the use of a Transport Encryption connection mode is recommended.

Data security and controls

Protocol: *Native TCP (default); TCP with Certificate-based Encryption (requires advanced configuration)*

By default these communications are unsecured and contain a very high level instruction and do not include sensitive or exploitable information.

The controls implemented for this communication include:

- **Origin authentication** – A single-use token is passed which the receiver validates with the Blue Prism Application Server. This allows the receiver to validate the originator had the authority to issue the message.
- **Session authentication** – A single-use token is passed which the receiver validates with the Blue Prism Application Server. This allows the receiver to validate the originator had authenticated with the Blue Prism Application Server prior to generating the message.

The single-use token referenced above is generated by the Blue Prism Application Server and verified by the recipient via the operational communications channel.

Whilst these instructional communications are unsecured by default, for advanced implementations applicable runtime resources can be configured to apply encryption by leveraging a local certificate. When appropriately configured, certificate-based encryption is applied to all communication received by the device on a given port irrespective of the origin. Blue Prism web services accessed on configured devices will require a HTTPS prefix.

When deploying certificates for this purpose it is important to note that:

- The certificate common name(s) will need to accurately reflect the paths used for all communications to the runtime resource on a given port.
- The devices connecting to the runtime resource(s) will need to trust the issuer (Certificate Authority).
- The start-up parameters for the runtime resource will need to be configured to leverage the certificate.

Operational communication

The operational communication represents the main channel for data transmission between the Application Server and all clients (interactive clients and runtime resources). These connections are established from the respective clients to the Application Server(s) and use WCF (in the default/recommended configuration) which provides encrypted communication, and controls which include: content confidentiality, data integrity protection, origin authentication, message replay protection, non-repudiation, and session authentication.

Examples include scenarios such as where the Application Server receives a request from:

- A runtime resource requesting a process definition after being instructed to start processing.
- A runtime resource writing a log to the database (via the Application Server).
- A runtime resource requesting a credential for use when executing a process.
- An interactive client updating a process definition.
- An interactive client updating an execution schedule.

Each runtime resource (and interactive client) will communicate over a WCF connection with a nominated application server via the server's listening port (default: 8199).

Data security and controls

Protocol: *TCP (WCF)*

The communication is encrypted by default when the default, or any of the recommended configurations, are in use. The security is provided by the WCF Framework and the Operating System.

Legacy .NET Remoting Support

To support legacy installations, it is possible to configure Application Servers and Clients to use .NET remoting instead of WCF for operational communication. Unless the Insecure variant of this option is selected, the connection is established via a secure TCPChannel. Behind the scenes, this is using the NegotiateStream Class, which is the .NET instrumentation of Microsoft's Security Support Provider Interface SSPI architecture.

Because the security negotiation is handled by SSPI, it is transparent to Blue Prism and difficult to determine in all scenarios what encryption and authentication would be used, as this is based on operating system levels, domain configuration and other environmental factors. In most scenarios, the end result would be the use of Kerberos for authentication and sChannel for encryption. Assuming sChannel is selected for encryption, this would mean the Cipher used would be likely to be determined per this article:

https://msdn.microsoft.com/en-us/library/windows/desktop/aa374757(v=vs.85).aspx.

The Key Distribution Center (KDC) for the communications is located on an Active Directory domain controller and uses Active Directory as its account database and, where required, the Global Catalog for directing referrals to KDCs in other domains.

.NET Remoting includes a number of controls when the Blue Prism platform is deployed into an Active Directory network infrastructure.

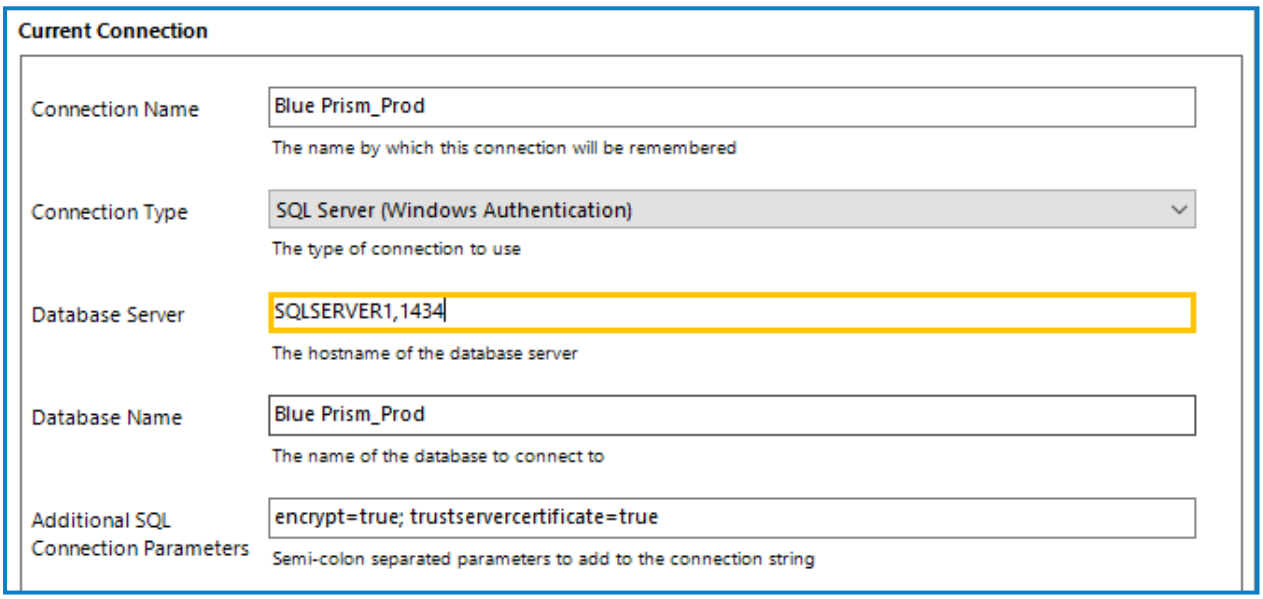
Data encryption is only available for .NET Remoting when Blue Prism is deployed within an Active Directory network infrastructure.

- **Content confidentiality** – .NET NegotiateStream is used to natively provide both key derivation and data encryption/decryption. SPNEGO is used to select the underlying security protocol, and the security context via negotiation between the client and server through use a set of security tokens generated by the SPNEGO GSS-API mechanism.
- **Data integrity** – .NET NegotiateStream is used to natively provide data encryption and signing using the negotiated security mechanism. The signature used as part of the VerifyMessage functionality to validate the integrity of the content.
- **Origin authentication** – Active Directory, as the KDC, performs the role of a trusted third-party and is responsible for providing confidence that the message has genuinely originated from the identified principal in addition to the verification that is applied by interrogating the message signature.
- **Message replay protection** – Reply protection is natively achieved through use of a ticket containing a session key and an encrypted session key identifier which is cached along with the timestamp of the original request.
- **Non-repudiation** – .NET NegotiateStream Protocols use of Active Directory as the KDC and trusted third-party provides confidence that the message is genuine and cannot be repudiated as it contains information (a session key) encrypted with the senders master key which the recipient must contact the trusted third-party to be able to verify.
- **Session authentication** – .NET NegotiateStream Protocol relies on the SPNEGO security protocol which selects between Kerberos (preferred) and NTLM. Authentication is performed as part of the negotiation to select the security protocol through the exchange of opaque security tokens generated by the SPNEGO GSS-API mechanism.

Database communication

The communication between Blue Prism and the Microsoft SQL Server database leverages the .NET Framework SqlClient library. By default this is unsecured however there are a number of common approaches to secure the connection:

- Install a verifiable server certificate on the SQL Server and configure the SQL instance to force encryption for all connections.
- Install a verifiable server certificate on the SQL Server and configure the Blue Prism database connection to specify that the connection should be encrypted. For example, encrypt=true.
- Configure the Blue Prism database connection to specify that the connection should be encrypted and that server certificates can be trusted without further verification which allows a self-signed certificate on the SQL Server to be leveraged. For example, encrypt=true; trustservercertificate=true.



High availability, redundancy, and disaster recovery

Where Blue Prism is running business critical automated processes, the consequence of a production environment failure preventing the successful running of these processes can be serious.

There are three main aspects to consider when configuring Blue Prism for redundancy or resilience:

- **Operational control** – How the platform is configured operationally to execute work can impact the behavior when it responds to a failover or recovers from an outage. This can relate to a number of areas such as process design, demand management, frequency of schedules, management of process exceptions etc.
- **Availability of target systems** – The availability of the business systems which are accessed by the automated processes will impact the ability of the platform to operate successfully.
- **Underlying architecture** – The hardware and core services on which Blue Prism relies must be configured to be appropriately resilient.

This section provides information relating to providing resilience at the architecture level.

For detailed information on load balancing, the deployment options, and the implications for the Blue Prism application operation, see the Load Balancing Reference Guide.

Technical considerations for high availability, redundancy, and disaster recovery

From a technical perspective High Availability (HA) and Disaster Recovery (DR) can be achieved using concepts such as:

- Component redundancy – having n+1 components in your Blue Prism environment.
- Using load balancers across multiple application servers.

  When using multiple application servers each should have the same encryption key.
- Spreading Blue Prism infrastructure across multiple, geographically separate sites.
- SQL database HA concepts such as:
  - Clustering
  - Always On Availability Groups
  - Mirroring
  - Log shipping
  - Multi-site replication
- Keeping offsite backups
- Taking advantage of Blue Prism resource pools
- Resilient process design
- Monitoring components vigilantly.

Resilience of components

The core components which are required to assure availability of the platform are:

- **Database servers** – A core component of the Blue Prism platform and the optional Hub component and, as it is the real-time repository for audit and operational logs, the platform is configured to cease processing whenever the database cannot be contacted. High availability and/or redundancy is achieved through use of native SQL Server technologies (e.g. clustering, mirroring, AlwaysOn Availability Groups) or by third-party redundancy and replication technologies.
- **Application server** – Used to marshall all connections with the database and to provide critical functionality as processes execute. All operating Interactive Clients and runtime resources require a connection to an available application server. As the execution within the platform is stateful, a persistent connection is required. Likewise if the connection between a runtime resource and application server is interrupted, the runtime resource will periodically attempt to reconnect. Redundancy is achieved by provisioning additional application servers; and high availability is achieved through use of routing or load balancing such that traffic is directed to an available component. Due to the stateful nature of execution within the platform, items being actively worked at the time of fail over or re-direction will fail and be routed for human intervention.
- **Hub server** – Hosting Hub and Authentication Server. For details of Hub high availability, see High availability configuration.

  > Depending on the version of Hub you are using, Authentication Server needs to be combined with Hub on the web server.

- **API server** – Hosting the Blue Prism API, required to use the Hub Control Room.
- **RabbitMQ server** – A RabbitMQ cluster, must be installed and configured with three or more hosts. A Message Broker Server hosts RabbitMQ and Erlang OTP. RabbitMQ servers can be configured for load balancing and high availability. This configuration is specific to the RabbitMQ service. To provide load balancing and high availability for RabbitMQ, one virtual service is required. The virtual service must be set to listen on the same port as the RabbitMQ service, which is port 5672 by default. For details of RabbitMQ clustering, see the RabbitMQ Clustering Guide.

Additional platform components include:

- **Runtime resource** – Responsible for executing the processes, each runtime resource is commonly located on a separate virtual device. Redundancy is achieved by provisioning additional runtime resources; and high availability can be achieved through use of Active Queues or Blue Prism resource pools.
- **Interactive client** – The client software accessed by users either to develop and test processes; or to control and monitor the platform. Redundancy is achieved by provisioning additional devices and directing users to an available component as they establish a connection.

Load balancing servers

Load balancers can be used to distribute tasks to the Blue Prism servers (including web servers) in a high availability environment. Load balancers ensure reliability and availability by monitoring the health of applications and only sending requests to servers and applications that can respond in a timely manner. You should use a load balancer best suited for your organization, the recommended load balancers include:

- F5
- Citrix Netscalar
- HAProxy

The simplest approach for load balancing is to use DNS round-robin with a low Time to Live (TTL) setting. Where organizations have existing technologies it can be possible to complement this approach by introducing an application aware utility that is able to validate the health of the Application Server(s) and to manage the DNS records accordingly. Commonly such functionality can be provided with the DNS platform, by software load balancers, or within monitoring platforms such as Tivoli or Microsoft Operations Management.

Alternative solutions such as Microsoft Server Clustering, third-party replication and routing solutions or other software/hardware load balancers may be used to provide this functionality.

Further information on this topic is available the Load Balancing Reference Guide.

Blue Prism component monitoring

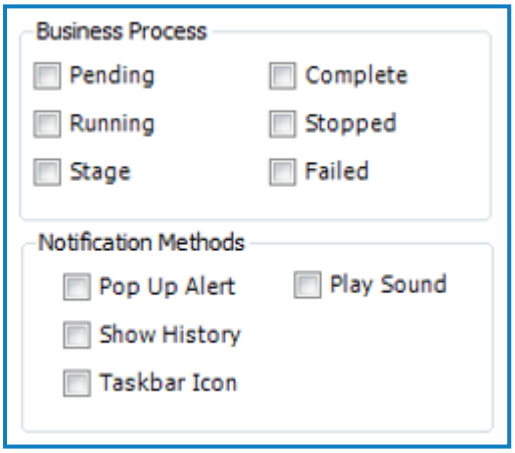
Blue Prism infrastructures will comprise a number of different components each of which can be monitored and polled to verify that it is available and responsive. When monitoring the Blue Prism components, standard third-party tools and techniques can be used to evaluate the following:

- Health of allocated hardware (e.g. disk space, CPU utilisation, network connectivity).
- Availability of specific windows services (e.g. service started, responding on the appropriate port).
- Windows Event Viewer – should be actively reviewed for any errors raised on all devices which are part of a Blue Prism environment.

Additionally, Blue Prism provides a number of features and techniques that can be used to assist with monitoring process execution and any associated errors.

Process and Schedule Alerts can notify administrators or controllers, directly on their own desktop, using a range of indicators including:

- Pop-ups
- Sounds
- Taskbar icons



Additionally custom notification types can be implemented such as sending an email or raising an SNMP trap.