blueprism®

Software Robots - the Virtual Workforce

Infrastructure Reference Guide

REFERENCE GUIDE

Version: 5.0.23.2

Contents

1. Introduction

1.1. Intended audience

This reference guide is intended for use by system architects and designers who are seeking to gain an understanding of the product architecture, and the implementation options available when deploying the solution.

1.2. About this document

The document provides an introduction to each of the 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 is recommended that, to start, readers 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. The relevant guides can then be used to provide supplementary information and design considerations for the chosen deployment model.

1.3. Information

Summary information about the Blue Prism components and examples architectures are provided, followed by a series of guides; each dedicated to the specific features, functionality and consideration of each:

- Blue Prism Interactive Client Guide.
- Blue Prism Runtime Resource Guide.
- Blue Prism Application Server Guide.
- Blue Prism Database Server Guide.

A number of supplementary guides also provide guidance and include:

- User Accounts, Remote Access and Security Guide.
- Active Directory Integration Guide.
- Blue Prism Network Connectivity Guide.
- Blue Prism Virtualization Guide.
- Blue Prism Monitoring Guide.

Within this document there are a number of external references to data sheets and user guides that focus on specific topics – such references will be presented underlined and colored blue for ease of identification.

2. Blue Prism Architecture Overview

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

Blue Prism Runtime Resource
Persistent, typically virtualised, instances of a standard end-user desktop responsible for running the automated processes – commonly referred to as software robots. These components also typically require enhanced physical and remote access security.

Blue Prism Interactive Client
(Development or Controlling and Monitoring)
End-user desktop build (physical or virtual) that facilitates the setup, development, configuration and monitoring of Blue Prism processes across the environment.

Typically virtualized in the data-center alongside other Blue Prism components, but can be deployed directly onto end user's desktops.

Active Directory Domain Controller
Blue Prism can be integrated with an existing Active Directory domain to provide user access control to Blue Prism components.

Blue Prism Application Server
The Blue Prism Server service marshals all connectivity between the Blue Prism components and the database. The key features enabled by this component, which is typically provisioned as a physical or virtual Windows Server, include: secure credential management; database connection marshalling; data encryption; and scheduled process execution.

SQL Server Database
A Microsoft SQL Server database is used as centralized repository that holds process definitions, logs, audit and user information.

Connections from the Blue Prism components will be via the Blue Prism Application Server.

3. Component Architecture Examples

3.1. Overview

There are a large number of configurations that can be applied to a Blue Prism deployment and these should be reviewed to determine the features, scalability and resilience required of the environment(s) being deployed. Having an indication of the required features of the deployment will assist with the understanding of the subsequent informational guides.

This section provides a series of examples which illustrate some of the configurations that could be applicable dependant on a number of factors such as the size and business criticality of the proposed system.

Information about the minimum specifications of each Blue Prism component can be found within the respective guides such as the **Blue Prism Database Server Guide**.

The Blue Prism Network Connectivity Guide provides an overview of the typical communication that occurs between each of the Blue Prism components.

In each of the following examples the specifications for the **Blue Prism Runtime Resources** and **Blue Prism Interactive Clients** remain static:
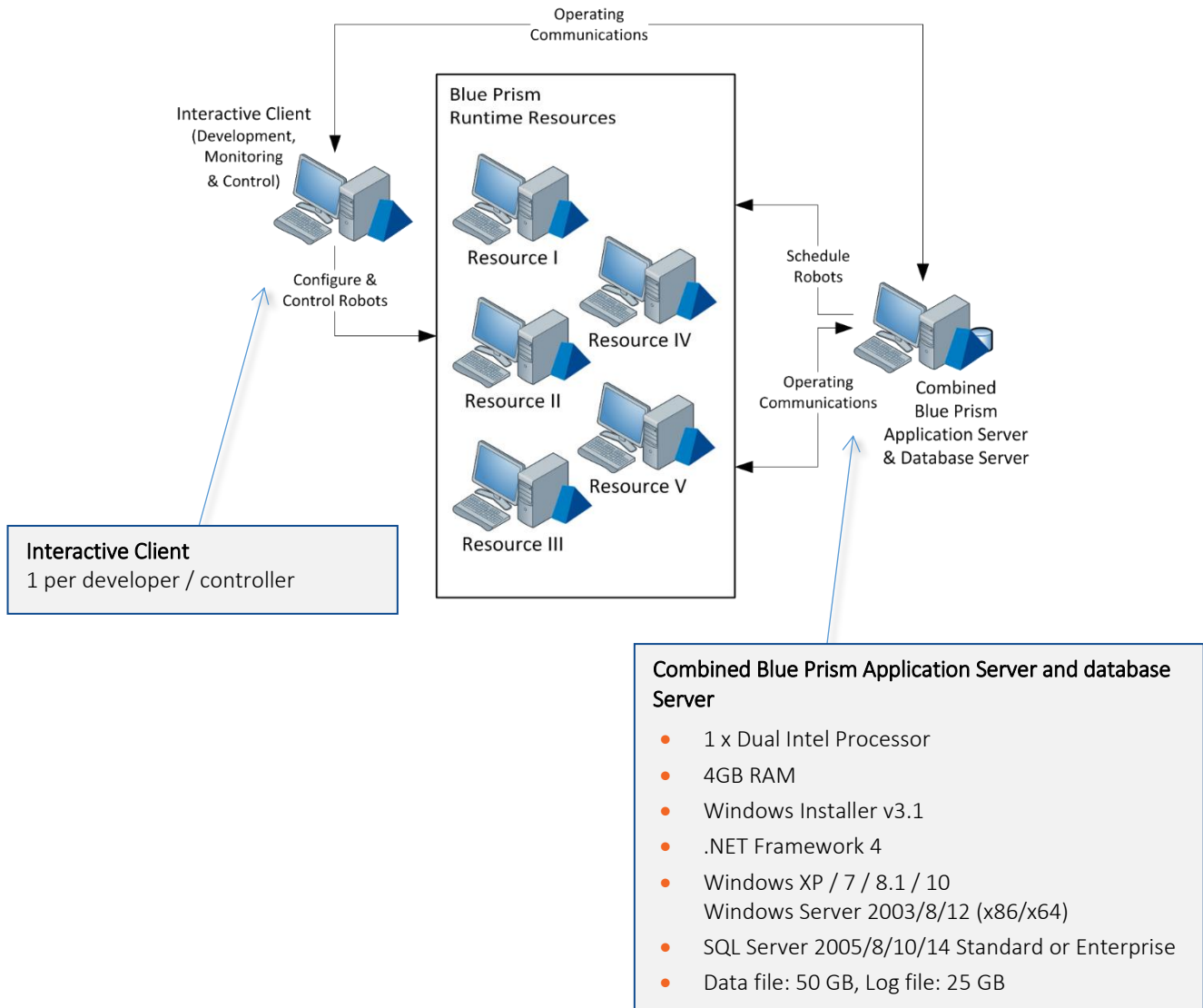
Blue Prism Component	Minimum Recommended Requirements
Interactive Clients (Controlling and Monitoring)	- Intel Xeon Processor 2GB RAM & 10GB free disk space - Windows XP / 7 / 8.1 / 10 (32 or 64-bit) - Windows Server 2003 / 2008 / 2012 (32 or 64-bit) - Windows Installer v3.1 .NET Framework 4
Interactive Clients (Development)	- Interactive Clients (Controlling and Monitoring) plus: - Access to all in-scope applications
Runtime Resources (Robots)	- Intel Xeon Processor 2GB RAM & 10GB free disk space - Windows XP / 7 / 8.1 / 10 (32 or 64-bit) - Windows Server 2003 / 2008 / 2012 (32 or 64-bit) - Windows Installer v3.1 .NET Framework 4 - Access to all in-scope applications

> The specification of Interactive Clients used for development and the Runtime Resources must meet the collective recommendations of the in-scope target applications. (E.g. SAP, Office, Kana etc.)
>
> A useful indicator is to base the specification on an equivalent device used by an end-user to automate those same applications.

3.2. Interim pilot desktop-based, IT secured: 5 Runtime Resources

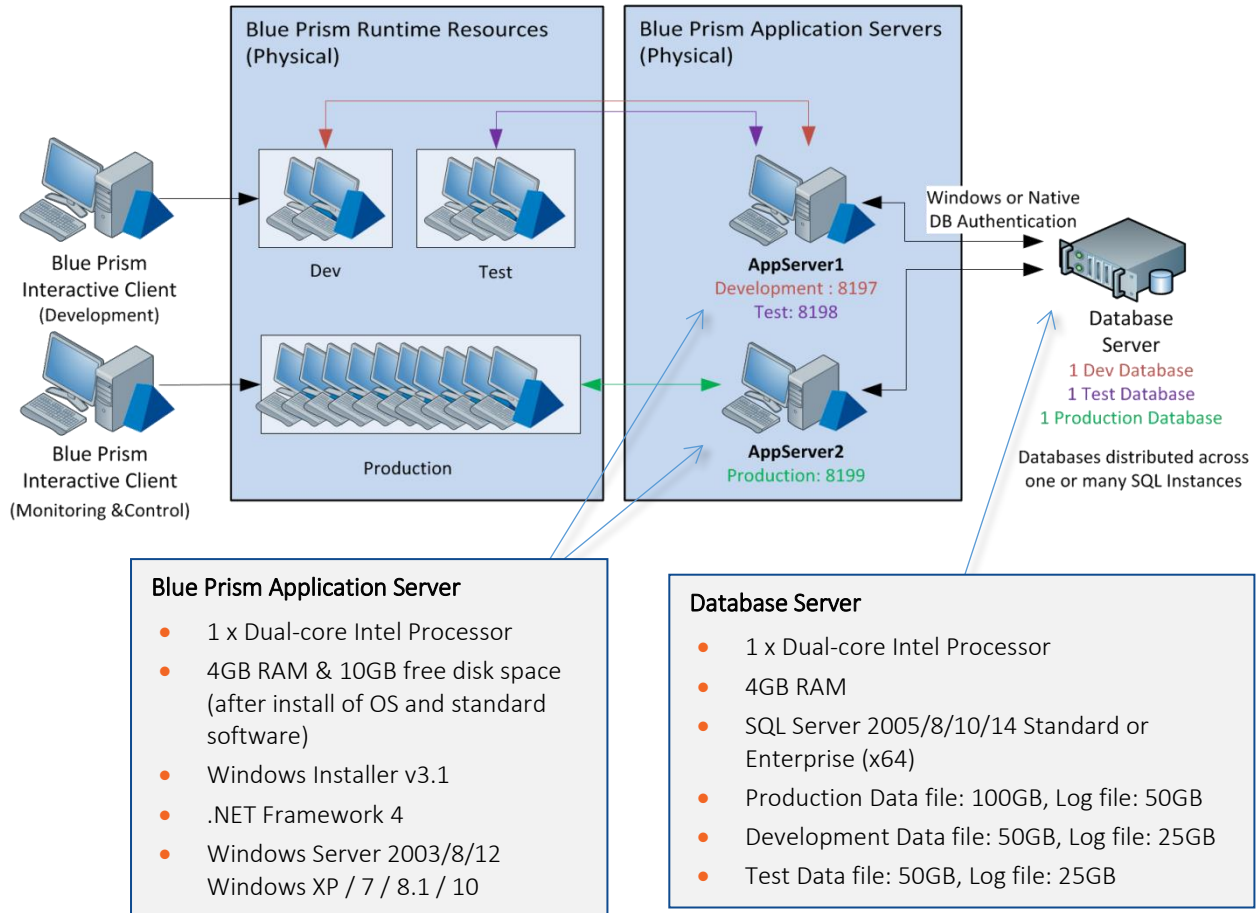A desktop-based scenario that is quick to provision but **not suitable** for production scenarios.

Interactive Client
1 per developer / controller

Combined Blue Prism Application Server and database Server

- 1 x Dual Intel Processor
- 4GB RAM
- Windows Installer v3.1
- .NET Framework 4
- Windows XP / 7 / 8.1 / 10
  Windows Server 2003/8/12 (x86/x64)
- SQL Server 2005/8/10/14 Standard or Enterprise
- Data file: 50 GB, Log file: 25 GB

Advantages	Constraints
• Very quick to implement / provision • Re-uses existing desktops • Requires minimal investment • Low level of dependency on IT	• No separate development or test environment - production resources must be sacrificed for development and test activities • There must be commonality across desktop builds • SQL Server Express database may be used, but performance and capacity may be limiting • Physical security of components must be considered

3.3. Desktop-based, IT secured: 10 Runtime Resources

A desktop-based deployment where all Blue Prism components (excluding the database) are deployed to desktops that are physically secured by IT.

Blue Prism Application Server

- 1 x Dual-core Intel Processor
- 4GB RAM & 10GB free disk space (after install of OS and standard software)
- Windows Installer v3.1
- .NET Framework 4
- Windows Server 2003/8/12 Windows XP / 7 / 8.1 / 10

Database Server

- 1 x Dual-core Intel Processor
- 4GB RAM
- SQL Server 2005/8/10/14 Standard or Enterprise (x64)
- Production Data file: 100GB, Log file: 50GB
- Development Data file: 50GB, Log file: 25GB
- Test Data file: 50GB, Log file: 25GB

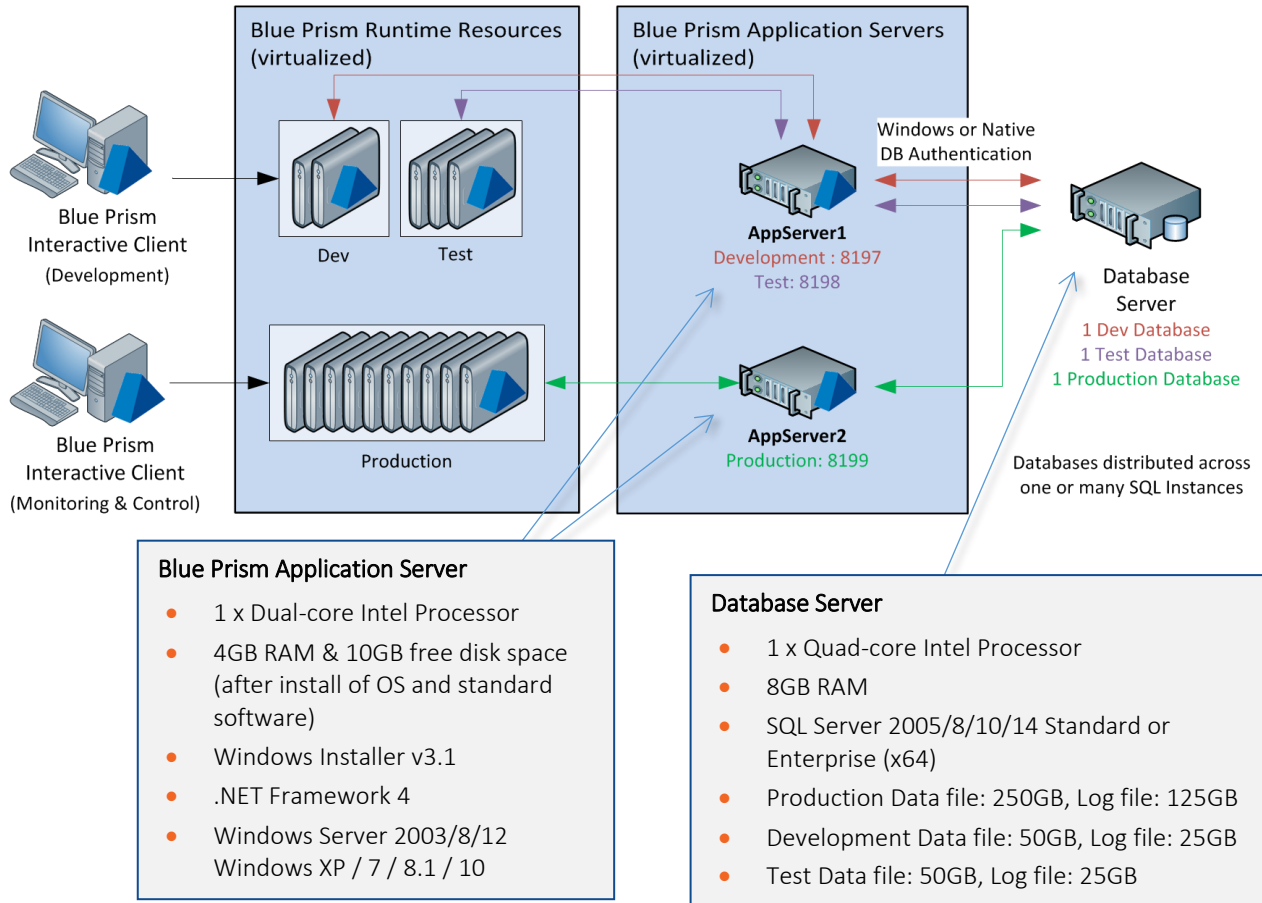| Advantages	Constraints
- Fast to implement / provision - Some re-use of existing desktops - Database is secured and managed by IT - Process development and test can be delivered without constraining production (separate development and test environments and dedicated runtime resources) - Separate Application Servers for Dev/Test versus Production allows product releases to be applied separately.	- Requires commonality across desktop builds - Physical security of components must be considered - Application server may receive a lower level of IT support than required (treated like a workstation vs server)

3.4.   Data-center secured: 25 Runtime Resources

Use of virtualized devices for Runtime Resources and a virtualized Application Server. Controllers and developers use their own physical PC as Interactive Clients.

Blue Prism Application Server

- 1 x Dual-core Intel Processor
- 4GB RAM & 10GB free disk space (after install of OS and standard software)
- Windows Installer v3.1
- .NET Framework 4
- Windows Server 2003/8/12 Windows XP / 7 / 8.1 / 10

Database Server

- 1 x Quad-core Intel Processor
- 8GB RAM
- SQL Server 2005/8/10/14 Standard or Enterprise (x64)
- Production Data file: 250GB, Log file: 125GB
- Development Data file: 50GB, Log file: 25GB
- Test Data file: 50GB, Log file: 25GB

| 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 Dev/Test versus Production allows product releases to be applied separately.	• There may not be an IT support model in place for virtualized desktop devices • Speed to implement / provision • Cost of virtualization technology

3.5.   Data-center secured with DR: 100 Runtime Resources

A fully virtualized environment which is entirely secured within the data-center and which illustrates:

- Two sets of 50 virtualized Runtime Resources, each with a dedicated Application Server.

- Virtualized 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.
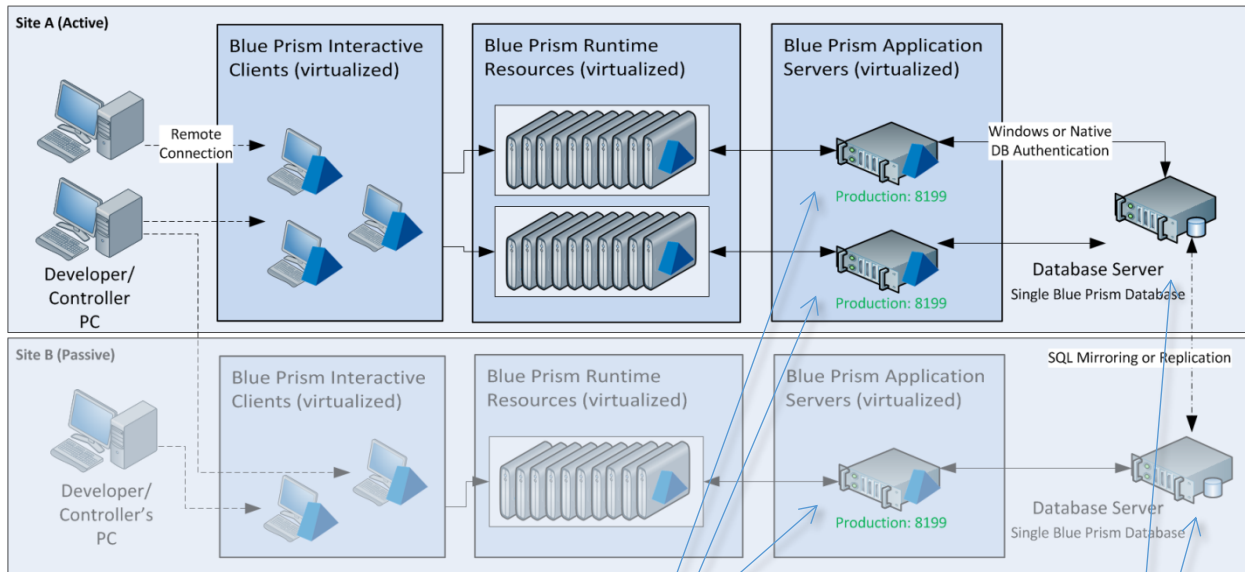
Blue Prism Application Server

- 1 x Dual-core Intel Processor
- 4GB RAM & 10GB free disk space (after install of OS and standard software)
- Windows Installer v3.1
- .NET Framework 4
- Windows Server 2003/8/12 Windows XP / 7 / 8.1 / 10

Database Server

- 2 x Quad-core Intel Processor
- 16GB RAM
- SQL Server 2005/8/10/14 Standard or Enterprise (x64)
- Production Data file: 1TB, Log file: 500GB
- Development Data file: 50GB, Log file: 25GB
- Test Data file: 50GB, Log file: 25GB

| Advantages	Constraints
• Highly resilient and scalable – full capability on standby suitable for business critical processing • No geographic constraints across development, test or production • Consistency across developers and environments that reduces support overhead	• There may not be an IT support model in place for virtualized desktop devices • Speed to implement / provision • Cost of virtualization technology • Development / Test environments to be provisioned separately.

3.6.   Data-center secured: 500 Runtime Resources

A fully virtualized environment which is entirely secured within the data-center and which illustrates:

- Five sets of 100 virtualized Runtime Resources, each with a dedicated Application Server.

- Virtualized Interactive Clients which are used remotely.
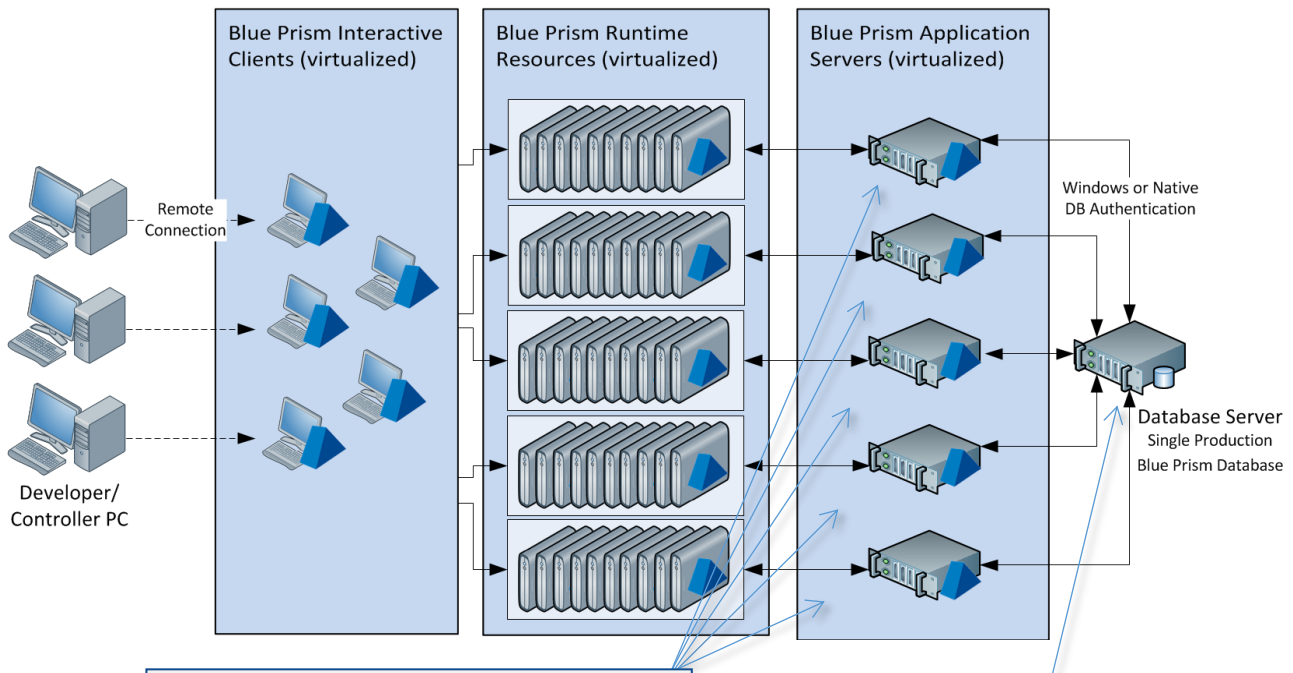
Blue Prism Application Server

- 1 x Dual-core Intel Processor
- 4GB RAM & 10GB free disk space (after install of OS and standard software)
- Windows Installer v3.1
- .NET Framework 4
- Windows Server 2003/8/12 Windows XP / 7 / 8.1 / 10

Database Server

- 4 x Quad-core Intel Processor
- 64GB RAM
- SQL Server 2005/8/10/14 Standard or Enterprise (x64)
- Production Data file: 5TB, Log file: 2.5TB
- Development Data file: 100GB, Log file: 50GB
- Test Data file: 100GB, Log file: 50GB

| Advantages	Constraints
- Quick to scale – as already virtualized - Database performance and capacity easily scaled - Virtualization aids commonality - Basic level of contingency in case of Application Server failure	- There may not be an IT support model in place for virtualized desktop devices - Speed to implement / provision - Cost of virtualization technology - Development / Test environments to be provisioned separately.

3.7. Architecture considerations

### 3.7.1. Active Directory integrated

Blue Prism can be integrated with Active Directory for the management of user access and control. This functionality is documented in the **Active Directory Integration Guide**.
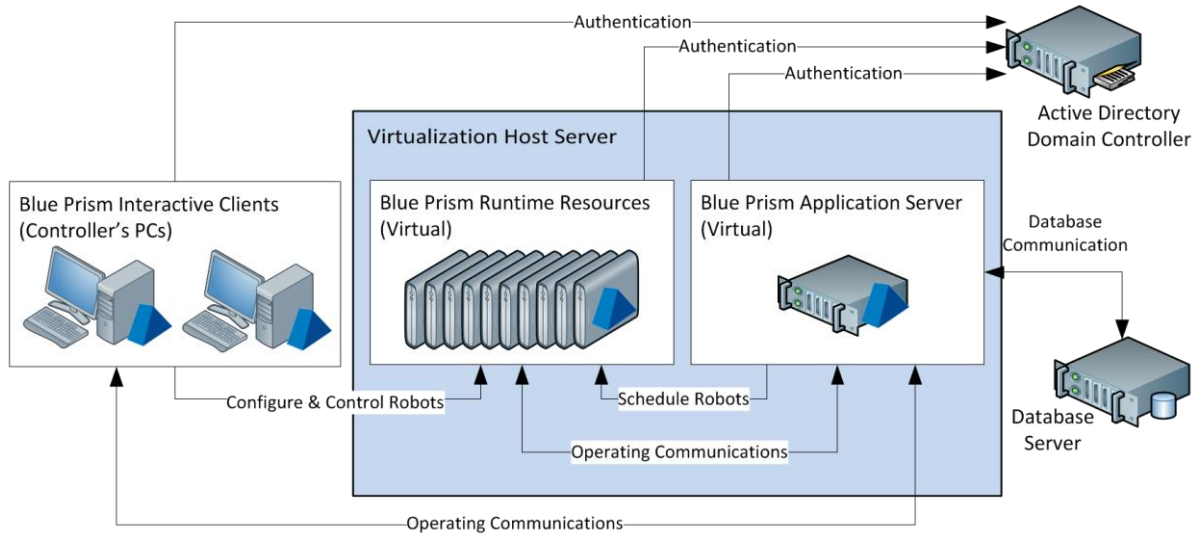
3.7.2. Access to Line of Business applications

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**

- **Blue Prism Interactive Clients** – however 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. (Illustrated below).
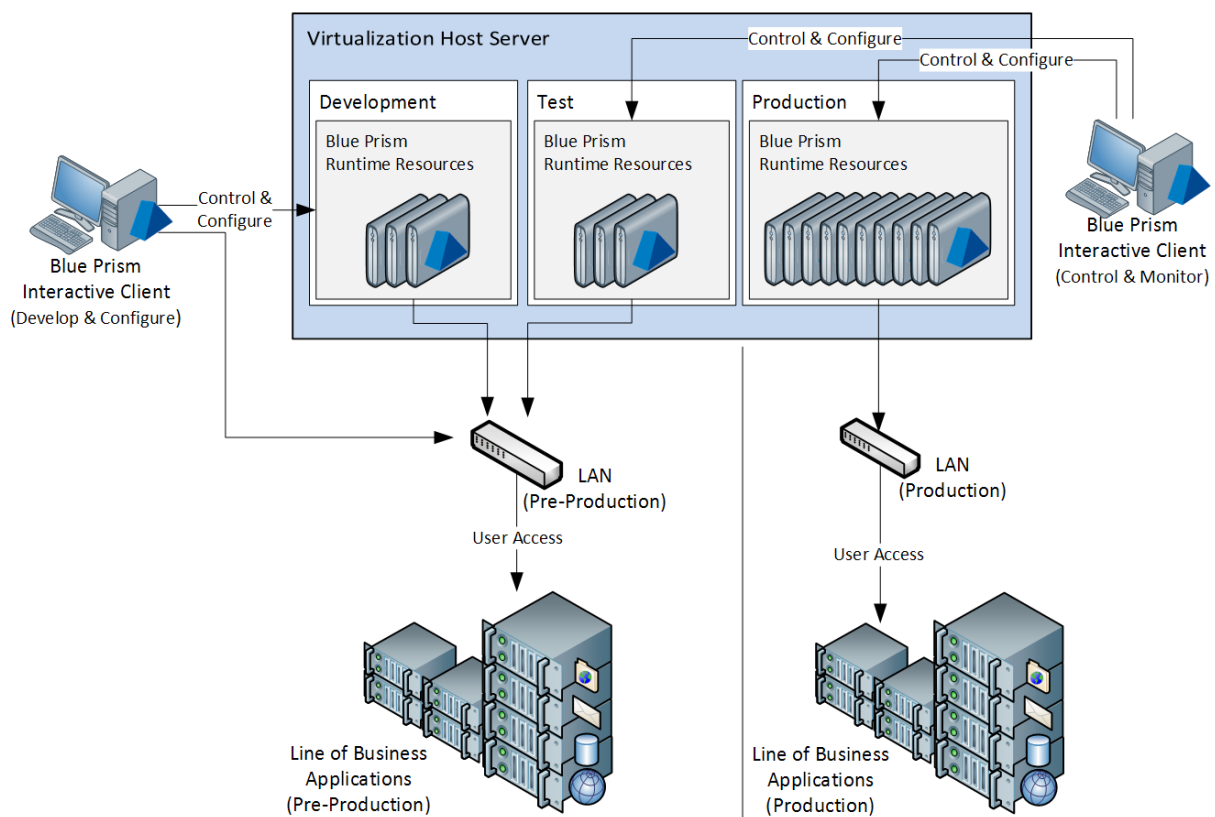
It is also common for the components in each environment to be configured to interact with appropriate instances of the applications. For example, the Runtime Resources in the development and test environment would ideally be configured to interact with non-production instances of the line of business applications.

3.7.3. Disaster recovery scenarios

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 VMs. 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.

3.7.3.1. Active/Passive

In addition to the general considerations, the following considerations may also be relevant

- 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.
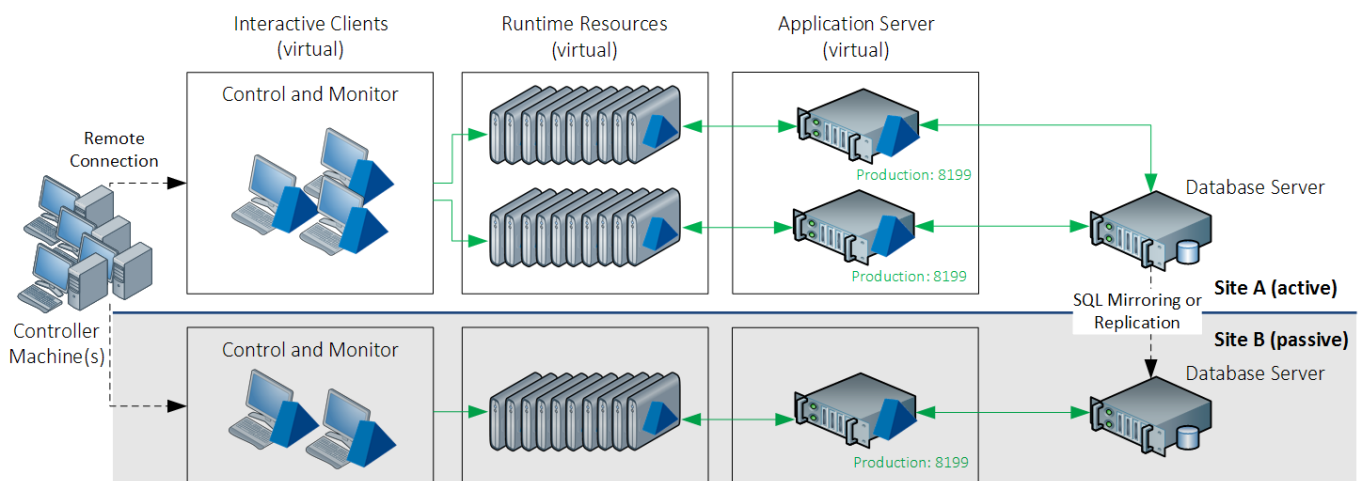

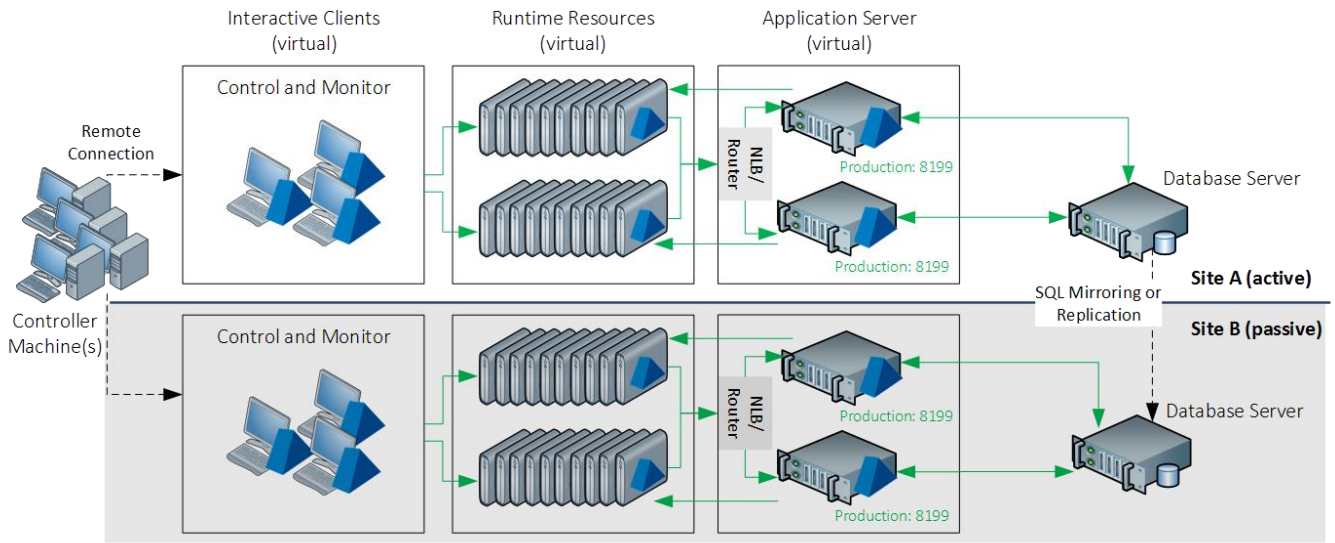Figure 1: Active/Passive with statically allocated Application Server

Figure 2: Active/Passive with balanced Application Servers

3.7.3.2.   Active/Active

In addition to the general considerations, the following considerations may also be relevant

- 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.
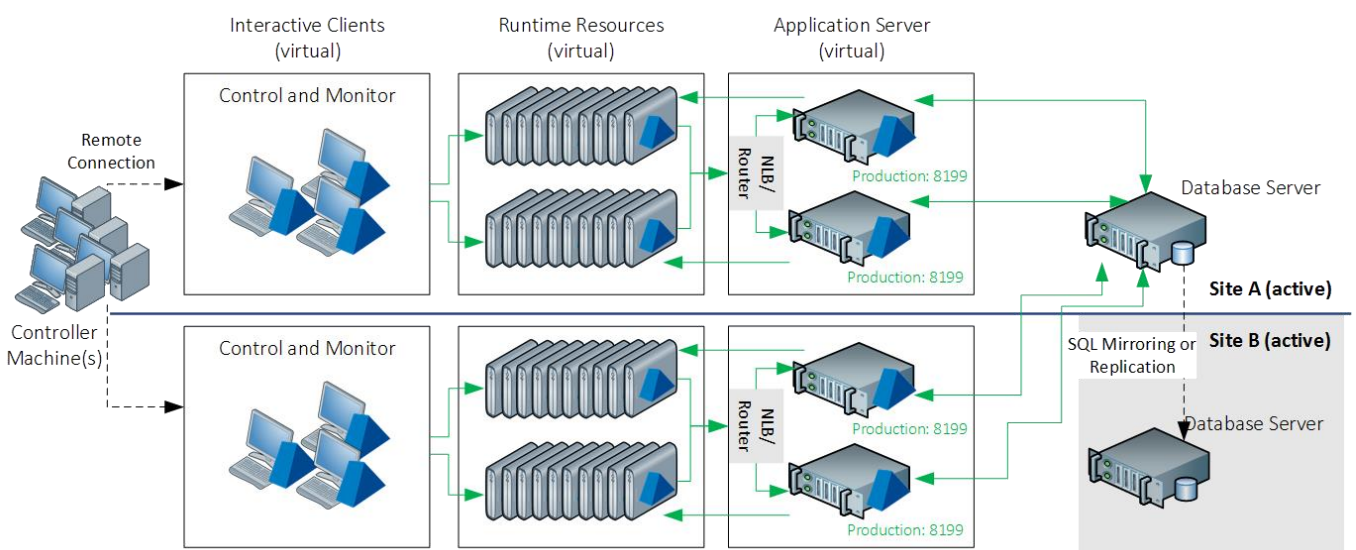

Figure 3: Active/Active with balanced Application Servers

3.7.4. Virtualization host specifications

Specifications of virtualization servers hosting a given number of Blue Prism components are provided to illustrate the appropriate hardware that is required.

The choice of virtualization technology and the method in which it is deployed will determine the maximum number of virtual images that can be provisioned on a given host. Guidance should be sought from the technology provider in relation to specific advice or limitations, particularly where high availability (HA) is being implemented as part of the virtualization solution.

The specifications below assume that the following hardware requirements is appropriate for the Blue Prism Runtime Resources:

Example: Blue Prism Runtime Resource	This specification must be reviewed to ensure that it is appropriate to meet the collective recommendations of the in-scope target applications (E.g. SAP, Office, Kana etc.) and the Operating System used.
• Single Processor • 2 GB RAM • 35 GB Hard Disk Drive • Windows desktop Operating System	A useful indicator is to base the specification on an equivalent PC used by an end-user to automate those same applications.

Further information on the minimum requirements for this component can be found within the **Blue Prism Runtime Resource Guide**.

Up to 12 Runtime Resources	**Up to 48 Runtime Resources**
• 1 x Intel Xeon Quad Core • 32 GB RAM • 70 GB Hard Disk Array (OS) • 420 GB Hard Disk Array (Images) • 2 x 1 GB Network Interface Card • ESX or Hyper-V Operating System	• 4 x Intel Xeon Quad Core • 128 GB RAM • 70 GB Hard Disk Array (OS) • 1.7 TB Hard Disk Array (Images) • 2 x 1 GB Network Interface Card • ESX or Hyper-V Operating System

CPU: Assumes that 1:3 physical: virtual ratio is appropriate
RAM: Assumes 4 GB for the Host OS, and 2 GB per Runtime Resource
HDD: The space stated represents the amount of available space required after RAID configuration and assumes that the assumed amount is appropriate for the Operating System and software that will be configured. The hard disks should be provided as a RAID array which offers failover and redundancy.
Host Operating System: The operating systems specified are for illustration only.
The requirements above should be reviewed in light of the operating systems used within the virtualized images, and on the virtualization host.

3.7.5. High availability and redundancy

See the **High Availability and Redundancy Guide** for information.

4.   Blue Prism Interactive Client Guide

4.1.   Overview

Interactive Clients are used for developing processes and for controlling and monitoring the Blue Prism resources. The core purpose and features offered by an Interactive Client is dependent on whether it is used within a Development or Production environment (or both).
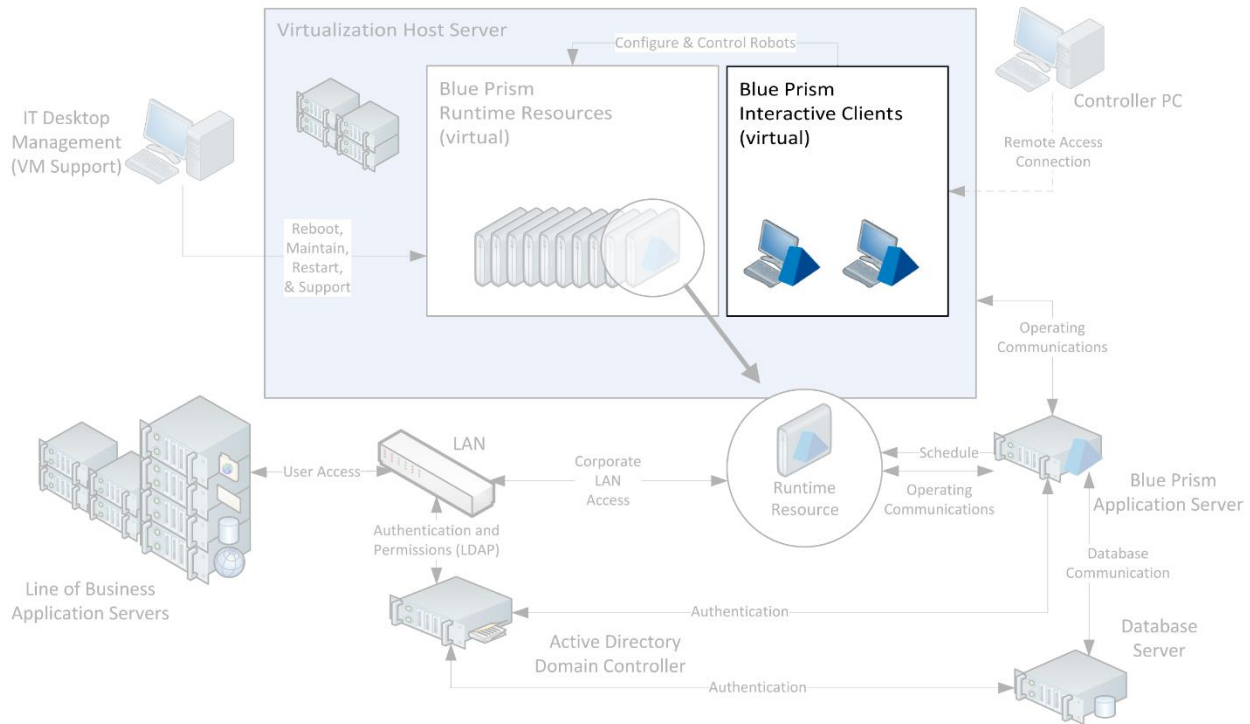
Development Environment	Production Environment
• Design connections to third party applications and systems • Develop, troubleshoot, test processes based on those connections • Package releases for transfer to live • Define system settings and configurations	• Initiate processes • Monitor and control runtime resources • Manage work queues • Review business referrals • Review logs and audit and generate reports

4.2. Minimum requirements[1]

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 runtime to be installed.

Where the Interactive Client is used for developing and configuring Blue Prism processes, access must be granted to all in-scope applications and all pre-requisites specifically required for automating the target application(s) must be installed. Additionally refer to the **Blue Prism Runtime Resource Guide** for settings that may need to be applied on the Interactive Clients used for development.

- Intel Processor
- 2GB RAM
- 10GB free disk space (after install of standard operational software*)
- Windows XP SP3 / 7 / 8.1 / 10 (x86/x64)
- Windows Server 2003 / 8 / 12 (x86/x64)
- Windows Installer v3.1
- .NET Framework 4
- When used for developing/testing:
- Access to all in-scope applications
- Pre-requisites for in-scope applications (.NET, thick-clients, Java Access Bridge, certified terminal emulator, SAP GUI Scripting).

The specification of Interactive Clients used for development must meet the collective recommendations of the in-scope target applications. (E.g. SAP, Office, Kana etc.)

A useful indicator is to base the specification on an equivalent PC used by an end-user to automate those same applications.

4.3. Frequently asked questions

How are Interactive Clients typically deployed?
It is common for Interactive Clients to be deployed to existing users' desktops in the first instance, particularly where all of the users who will be developing and controlling Blue Prism are geographically local to the Blue Prism environment(s). For larger, or enterprise strength, deployments it is recommended that these should be virtual rather than physical.

What are the advantages of virtualizing this component?
The **Blue Prism Virtualization Guide** provides detailed information about the benefits of virtualizing this component.

What are the security implications of this component?
There are no specific security implications for this component as only authorised users can access the installed Blue Prism software installed. Therefore, as a minimum, this component should be subject to standard organization desktop security protocols.

---

[1] All minimum requirements must consider the selected operating system as well as the applications to be automated.
* Examples of standard operational software includes: anti-virus; device monitoring or remote access tools; Microsoft Office; email clients.

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 (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). It is however recommended that where possible a clone of the client should be retained.

4.4.   Networking

The main components that Interactive Clients initiate communications with include:
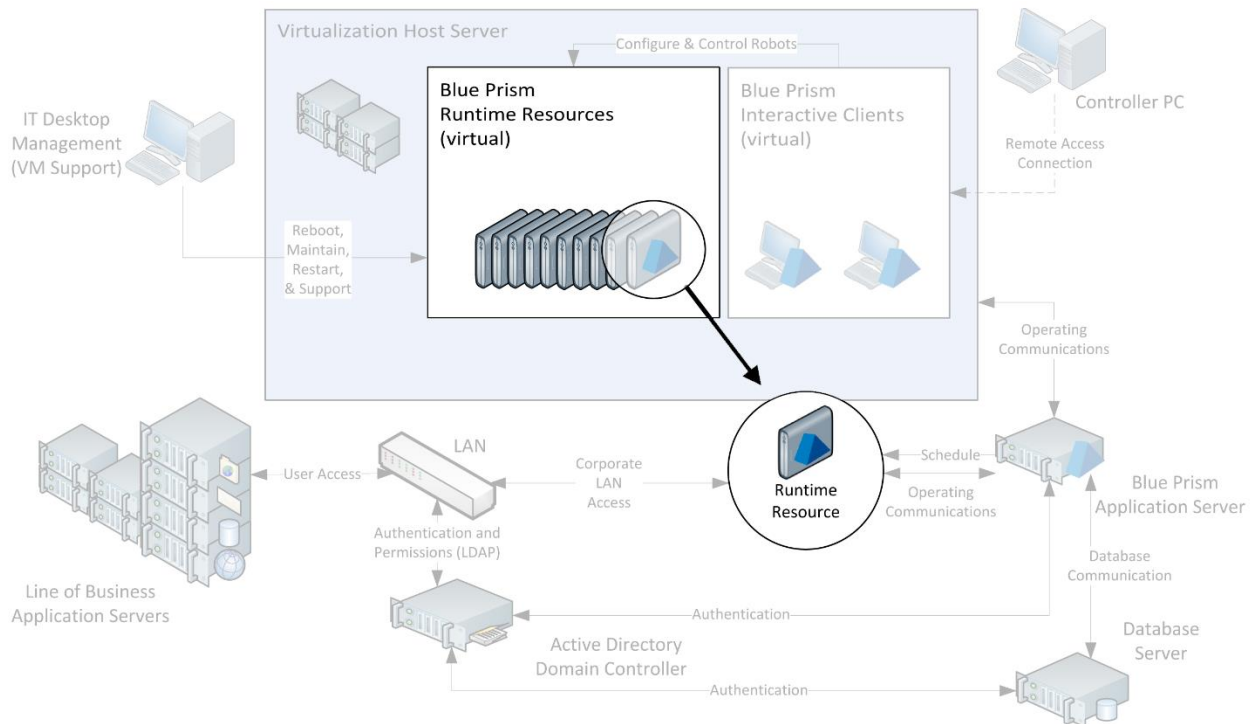
- **Runtime Resources**
  For the purposes of monitoring, controlling and manually triggering processes on a given Runtime Resource (TCP).

- **Application Server**
  The Application Server is used for all database connectivity (.NET Remoting).

- **Third Party Applications**
  See the **Blue Prism Runtime Resource Guide** 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 Guide**.

5. Blue Prism Runtime Resource Guide

5.1. Overview

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 to business application(s).

- Capture log information (which is then stored within the database).

Blue Prism Runtime Resources effectively operate a device as if a human operative was sat 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.

5.2. Minimum requirements[2]

Runtime Resources are typically deployed to virtualized instances of standard end-users desktops although for smaller or initial deployments, physical desktops can be used.

Each Runtime Resource requires the Blue Prism runtime to be installed along with all pre-requisites specifically required for automating the target application(s). Access must also be granted to all in-scope applications.

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

The **Blue Prism Virtualization Guide** provides advice for provisioning a server to host virtual Runtime Resources.

- Intel Processor
- 2GB RAM
- 10GB free disk space (after install of standard operational software*)
- Windows XP SP3 / 7 / 8.1 / 10 (x86/x64)
- Windows Server 2003 / 8 / 12 (x86/x64)
- Windows Installer v3.1
- .NET Framework 4
- Access to all in-scope applications
- Pre-requisites for in-scope applications (.NET, thick-clients, Java Access Bridge, certified terminal emulator, SAP GUI Scripting).

The specification of Interactive Clients used for development must meet the collective recommendations of the in-scope target applications. (E.g. SAP, Office, Kana etc.)

A useful indicator is to base the specification on an equivalent PC used by an end-user to automate those same applications.

5.3. Frequently asked questions

How are Blue Prism Runtime Resources typically deployed?
Typically they are deployed into a secure, virtual environment to provide security and scalability. There is the option to deploy to physical end-user desktops but this increases complexity from a commonality and security perspective.

What are the advantages of virtualizing this component?
The **Blue Prism Virtualization Guide** provides detailed information about the benefits of virtualizing this component.

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, it is not recommended to frequently switch which environment a specific Runtime Resource is assigned to.

---

[2] All minimum requirements must consider the selected operating system as well as the applications to be automated.
* Examples of standard operational software includes: anti-virus; device monitoring or remote access tools; Microsoft Office; email clients.

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.

5.4.   Networking

The main components that Runtime Resources initiate communications with include:

- **Application Server**
  The Application Server is used for all database connectivity (.NET Remoting).

- **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.

Sample diagrams and default port settings are provided within the **Blue Prism Network Connectivity Guide**.

5.5.   Device setup: user accounts

There are a variety of options and settings to be considered and configured for the Runtime Resources.

5.5.1.   User accounts

Each Runtime Resource can be allocated an independent user account to allow it to be appropriately secured, and provides opportunities for comprehensive audit and monitoring.

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.

- **Native Authentication**
  If using native authentication the Blue Prism Runtime Resource will not be able to authenticate with the applications that use Active Directory integrated authentication (single sign-on).

- **Domain Account**
  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).

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.)

5.5.2.   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:

- **No authentication**
  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.

- **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.

- **Automated authentication using the Blue Prism Login Agent** (recommended)
  Each Runtime Resource which has been appropriately configured[3] and where Blue Prism Login Agent has been installed, can be automatically logged in by Blue Prism.
  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).

  Further information on Blue Prism Login Agent is available within the following collateral:

  o   Blue Prism Data Sheet - Secure Windows Authentication

  o   Blue Prism User Guide - Login Agent

---

[3] The pre-requisites for Login Agent must be considered to ensure its suitability in a given environment.

5.6. 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.

5.6.1. 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 behaviour 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.

5.6.2. 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.

5.6.3. 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.

5.6.4. 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.

5.6.5. 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 Guide** contains information on the recommended approach for achieving remote connectivity with Blue Prism Runtime Resources.

5.6.6. SAP GUI Scripting

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

5.7. 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.

5.7.1. 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.

5.7.2. 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
```

E.g.

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

For information about configuring multiple Runtime Resources on a single Runtime Resource see the **Runtime Resources with multiple Runtime Resources** section.

5.8. 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 unauthorised users from directly monitoring the actions being taken, and getting access to the data that is being processed. Additionally 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. Further information is available within the **User Accounts, Remote Access and Security Guide**.

5.9. Runtime Resources with multiple Runtime Resources

In certain circumstances, a single Runtime Resource 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. (E.g. if there are 5 processes each using Internet Explorer, 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 (e.g. 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 connect 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 initialise multiple instances of Blue Prism, each with its own listening port.

The Blue Prism User Guide - Installing v5.0 provides instructions on how setup this configuration.

5.10. 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.

Further details on monitoring are contained within the Blue Prism Data Sheet - Monitoring.

6. Blue Prism Application Server Guide

6.1. Overview

The Blue Prism Application Server is an optional, but strongly-recommended, component within a Blue Prism environment.
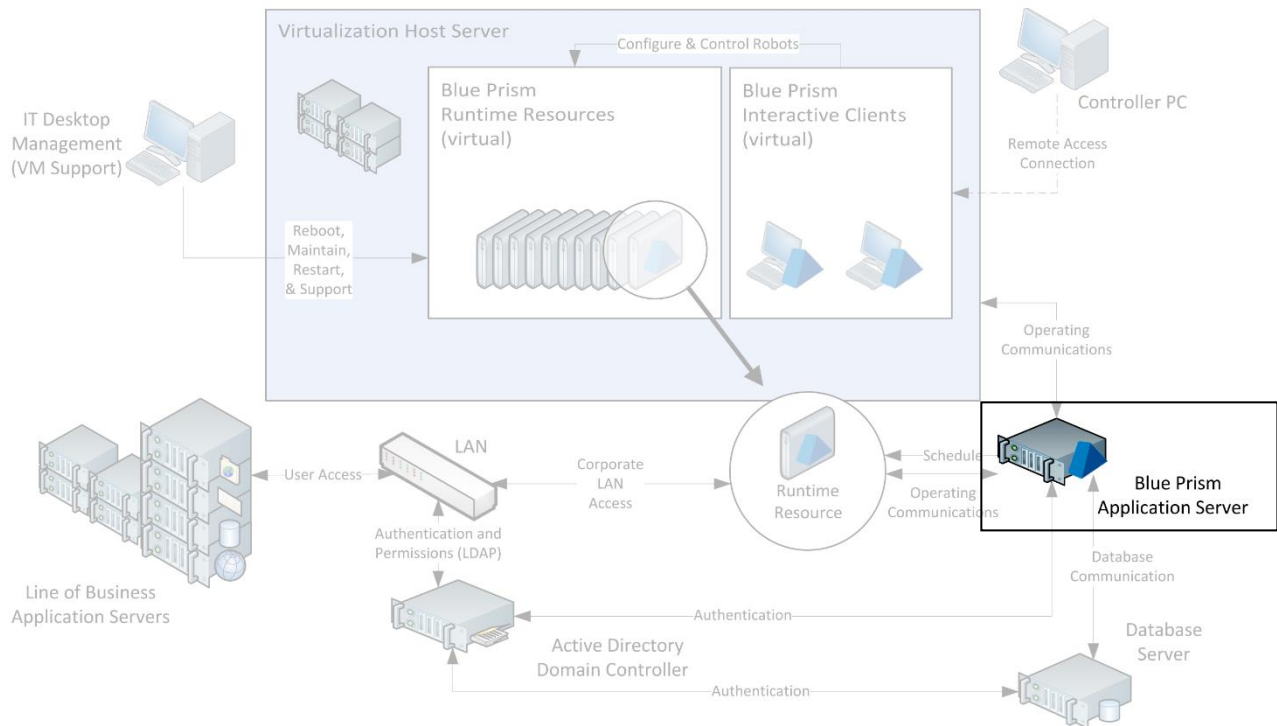
The key features that are provided by the Blue Prism Application Server include:

- Marshalling all connectivity between the Blue Prism components and the database.
- Provision of the Secure Credential Store.
- Data encryption and decryption capabilities.
- Scheduled process execution.

6.2. Minimum requirements[4]

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. The Blue Prism User Guide - Installing v5.0 Enterprise Edition provides 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, 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.

- Intel Dual Core Processor
- 2GB RAM
- 20GB free disk space (after install of standard operational software*)
- Windows Server 2003/8/12 (x86/x64).
- Windows Installer v3.1
- .NET Framework 4.
- x64 installs run in 32-bitmode

6.3. Frequently asked questions

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?
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.

- 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 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.

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** 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.

---

[4] All minimum requirements must consider the selected operating system as well as the applications to be automated.
* Examples of standard operational software includes: anti-virus; server performance monitoring tools; remote access technology

6.4. Networking

The main components that Application Servers initiate communications with include:

- **Runtime Resources**
  For the purposes of triggering scheduled processes on a given Runtime Resource (TCP).

- **Database**
  Connectivity with the database server uses SQL Server drivers and is therefore configurable. By default connectivity occurs using TCP.
  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 minimise latency between the components.

6.5. Application Server configuration

The Blue Prism User Guide - Installing v5.0 provides instructions on how to configure an installation of Blue Prism to take on the role of a Blue Prism Application Server.

In principle the steps include:

1. Configure the service using the **BPServer.exe tool.**

2. Register a **Windows Service** that references the above service configuration.

3. Configure the start-up and logon settings for the Windows Service.
   When SQL is secured using Windows Authentication, the configured Windows Service account will need to have appropriate (minimum) access to the SQL database.
   When Blue Prism is configured to use Single Sign on, the configured Windows Service account will need to have appropriate permissions to access the directory services provider and query users and group membership.

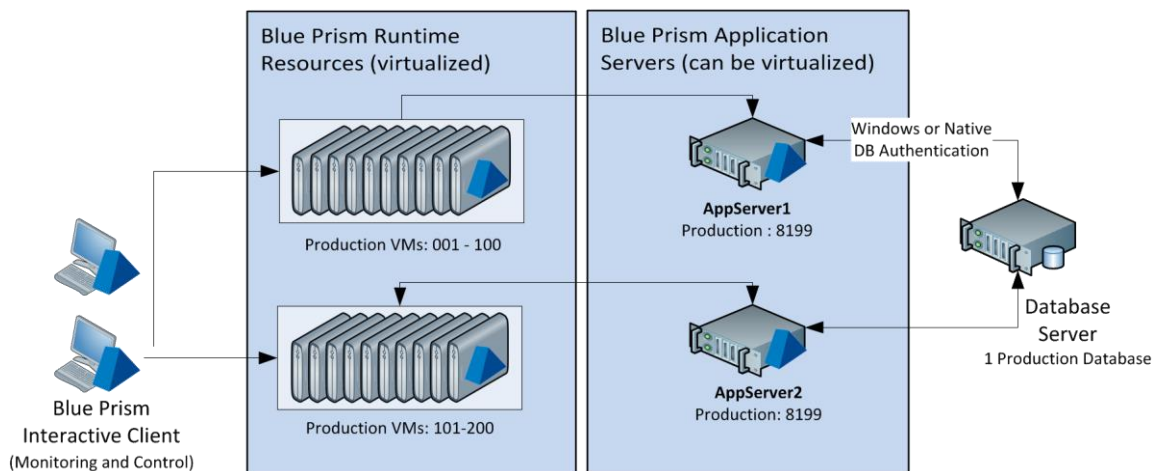## 6.6. Multiple Blue Prism Application Servers

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; or to provide functionality to a number of different environments (Development, Test, Production).

The common configurations for provisioning multiple Blue Prism Application Servers include:

- **Distributed Servers: many 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).
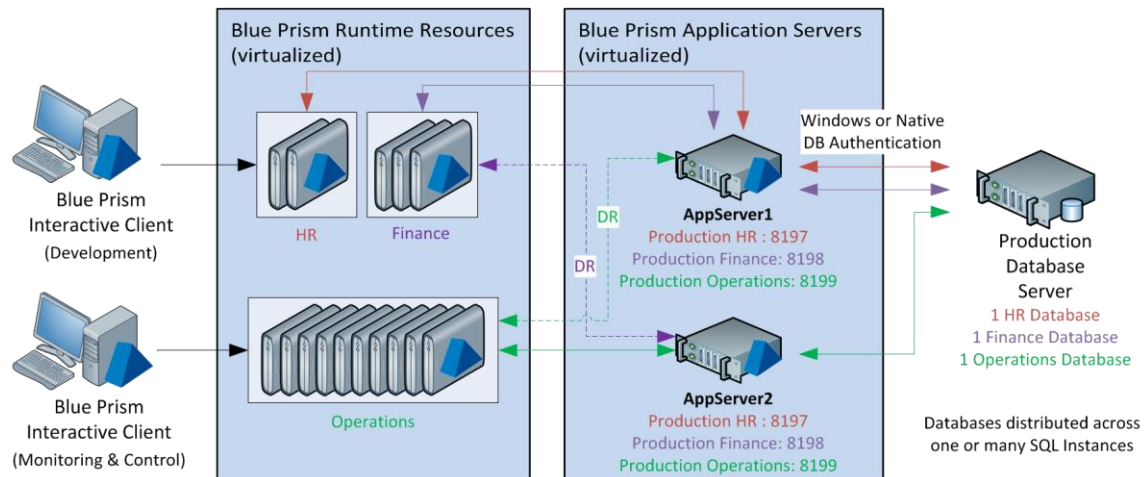 When configuring multiple Blue Prism Application Servers on a single Windows server it is important to review the combined maximum number of Blue Prism Runtime Resources that will need to be serviced concurrently.
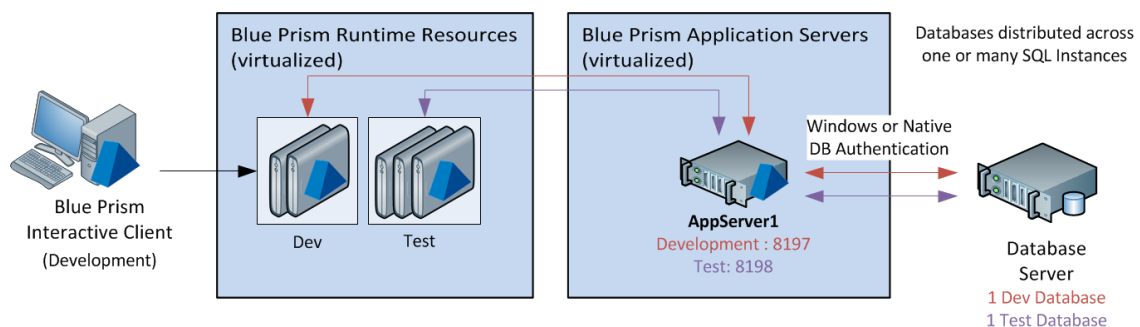
- **Hybrid: many servers for multiple environments**
  A hybrid approach can be taken to provide both resilience and the ability to service a high number of Blue Prism Runtime Resources across multiple environments.
  The example below shows a scenario where it has been decided to have a separate Blue Prism environment (with a dedicated database) for each core business area and therefore there are a number of production environments to be serviced.

6.6.1. 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, all of those which have the scheduler enabled 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.

6.7. High availability and redundancy

See the **High Availability and Redundancy Guide** for information.

7. Blue Prism Database Server Guide

7.1. Overview

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.
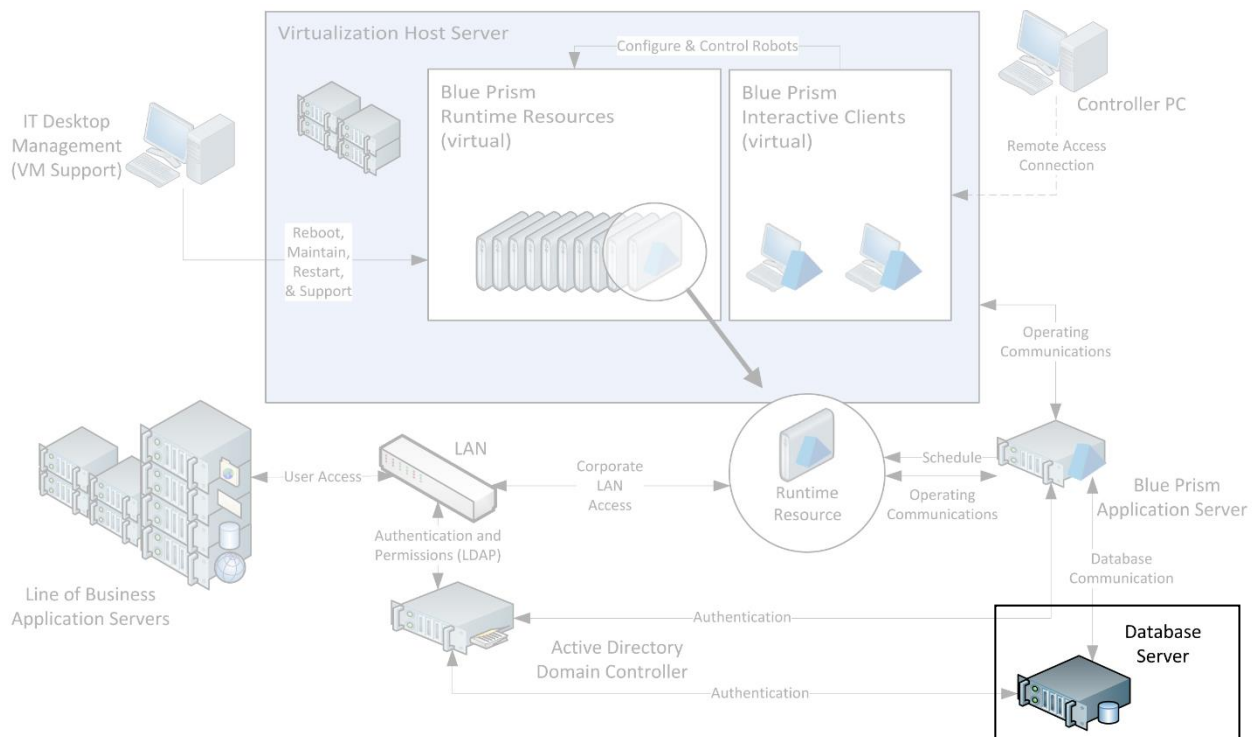
Key Features:

- 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.

7.2. Minimum requirements

Server	• Microsoft Windows Server 2003, 2008, 2008 R2, 2012, 2012 R2 (x86/x64 (recommended))
	• Intel Quad Core Processor
	• 4GB RAM
	• 10,000 RPM SAS Hard Drives (with appropriate RAID configuration)
	• Network card matched to environment
Database	• Microsoft SQL Server 2005, 2008, 2012, 2014 or Microsoft SQL Azure
	• Standard or Enterprise Editions (x86/x64 (recommended))
	• Non-clustered or clustered architecture
	• SQL AlwaysOn Availability Groups
	• Supports shared service infrastructure (e.g. rented space in a shared datacenter)
	• Multiple Blue Prism databases instances supported per server (for multiple environments)
	• SQL collation must be case insensitive and support the 1252 code page (Common examples include: Latin1_CI_AS, SQL_Latin1_CI_AS)

7.2.1. Sizing

The requirements of the database server directly correlate to the number of deployed Blue Prism Runtime Resources.

Environment	Data File	Log File	Sizing Notes
Development	50 GB	25 GB	
Test	50 GB	25 GB	
UAT	10 GB[5] x No of Runtime Resources	50% of Data File[6]	Data file minimum size: 100 GB
Production	10 GB[1] x No of Runtime Resources	50% of Data File[2]	Data file minimum size: 200 GB

---

[5] 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.

[6] Backup and log truncation should be reviewed according to business criticality.

7.3. Frequently asked questions

How are Blue Prism Databases typically deployed?

Typically they are deployed to a physical SQL Server instance. 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 SQL instance (often one which offers redundancy through mirroring, clustering or use of AlwaysOn Availability Groups (SQL AAG)).

What are the advantages of virtualizing this component?

Refer to the **Blue Prism Virtualization Guide** before considering virtualizing this component.

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 backups in line with any data recovery policies.

7.4. 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 utilisation.

- CPU and RAM allocation.

- Database growth.

- Recommended database settings.

Further information is provided with in the Blue Prism Data Sheet - Provisioning a Blue Prism Database Server.

7.4.1. 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 are provided as part of the release request or alternatively the command line utility can generate the SQL scripts.

7.5. SQL Permissions

The minimum SQL permissions required on the Blue Prism database for business as usual or normal operation are:

- Datareader
- Datawriter
- [All roles prefixed with bpa_] E.g.
    - bpa_ExecuteSP_DataSource_bpSystem
    - bpa_ExecuteSP_DataSource_custom
    - bpa_ExecuteSP_System

> The minimum SQL permissions do not provide appropriate privileges to carry out Create, Configure or Upgrade database actions, therefore an appropriate administrator account (e.g. dbowner) will need to be used when any of these actions are required.

7.6. 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; and 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.

Further information is provided with in the Blue Prism Data Sheet – Maintaining a Blue Prism Database Server.

7.7. 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 .NET Framework through use of SQL connection pools.

7.8. 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.

Further information on the key tables within the Blue Prism database is provided within the **SQL Tables** section within the Appendix.

7.8.1. 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 it the process is being run.

- any input/output parameters from the stage.

Overtime, 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.

7.8.2. 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).

7.8.3. 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.

7.8.4. 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.

7.8.5. 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.

8. User Accounts, Remote Access and Security Guide

8.1. Overview

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 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.

8.2. 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 within the **Blue Prism Runtime Resource Guide**.

8.3. 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 are securely stored, independently of the process definition, within a centralised Credential Management repository.

Access to specific credentials is restricted to specific Runtime Resources, processes and users in order to prevent authorised 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.

8.4. User Accounts: Blue Prism users (controllers / 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.
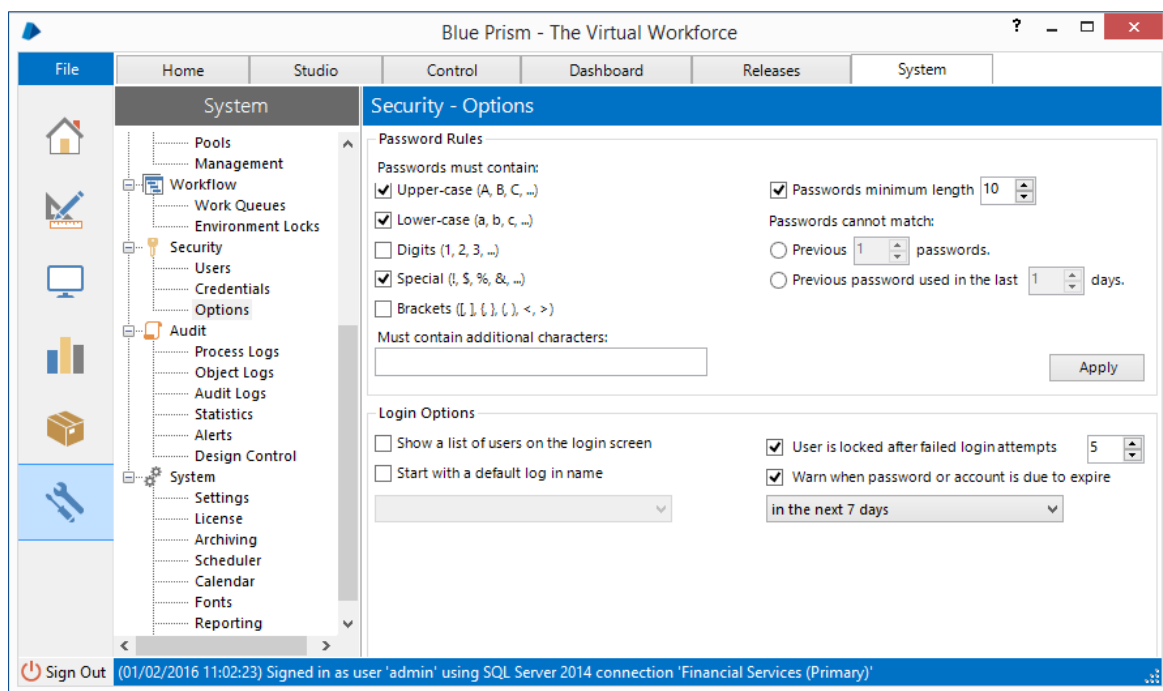
Alternatively Blue Prism can be integrated with Active Directory Domain Services for controlling and configuring user access and control. See the **Active Directory Integration Guide** for more information.

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.
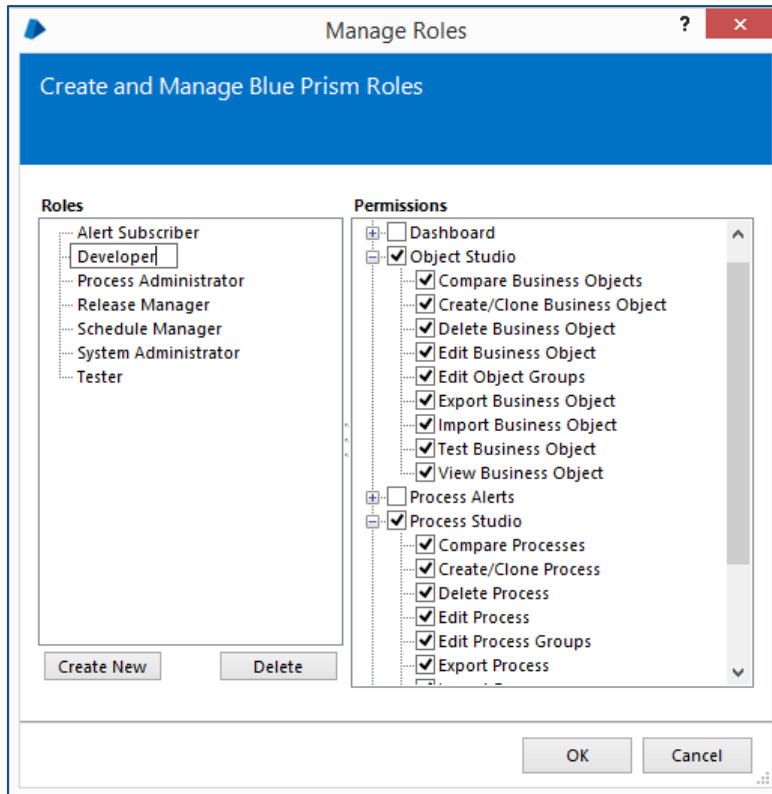
8.5.   Security: Access (including remote access)

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.

8.5.1.   Remote Access

If there is a desire 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 components guides:

- Blue Prism Runtime Resource Guide

- Blue Prism Application Server Guide

- Blue Prism Database Server Guide

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**.

Considerations for selecting a suitable remote access tool are detailed within the Blue Prism Data Sheet – Remote Access Tools.

8.6. 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.

Information about auditing the Blue Prism platform and change management is contained within the Blue Prism Data Sheet – Operational Audit Overview.

Further guidance on establishing appropriate logical access permissions is provided as part of the Blue Prism implementation methodology.

9.   Active Directory Integration Guide

9.1.   Overview

Blue Prism can be integrated with Active Directory Domain Services to provide user access control to Blue Prism components.

Blue Prism recommends using Active Directory Domain Services to assign permissions and to authenticate users as it provides a consistent approach to application security and enables audit trails to be reviewed and related to the appropriate user accounts.

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 for a given environment.

If configured in this way, Blue Prism will authenticate users with the domain controller as specified in the initial configuration. Native Blue Prism authentication is provided if Active Directory integrated authentication is not required.

9.2.   Configuring Active Directory integration

There following steps are required to configure Active Directory integration:

1. **Select to use Microsoft Active Directory authentication as part of the database creation action.**
    This option is provided as part of the database creation wizard, and is irrespective of the method of authentication selected for authenticating with the SQL Server.

2. **Configure the required Active Directory security groups.**
    Within Active Directory a security group should be configured for each of the Blue Prism Roles that are to be used. It should be noted that the number of Blue Prism roles and the permissions associated with each is configurable and therefore the number of security groups required can differ for each Blue Prism implementation.
    The security group member lists should then be configured with the appropriate user accounts.

    It is recommended that an independent set of security groups are defined for each Blue Prism environment that will use Active Directory integrated authentication.

3. **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.
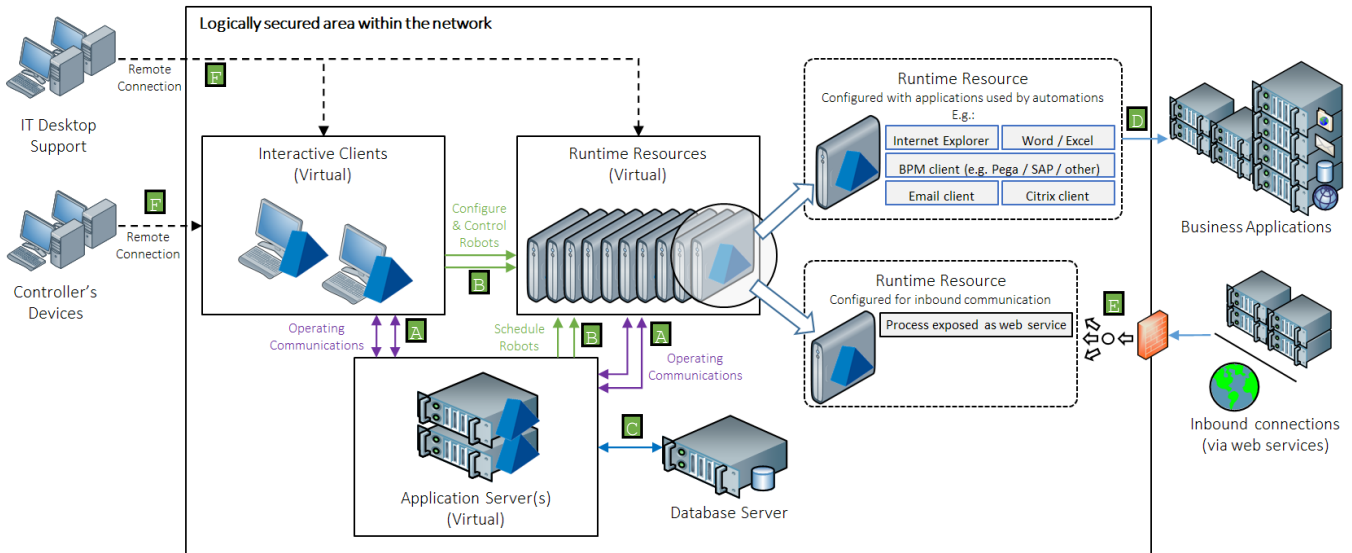
> The Active Directory user accounts for the Blue Prism users and the associated security groups must reside within the domain that Blue Prism is associated with.
> Additionally the users must be direct members of the groups – nested group membership is not supported.

Further information on Active Directory configuration is provided in the Blue Prism User Guide – Installing v5.0

# 10. Blue Prism Network Connectivity Guide

10.1. Overview

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 automations.	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.

10.2. Inter-component Communication

This guide provides an overview of the key communication channels that are used between the various Blue Prism components.
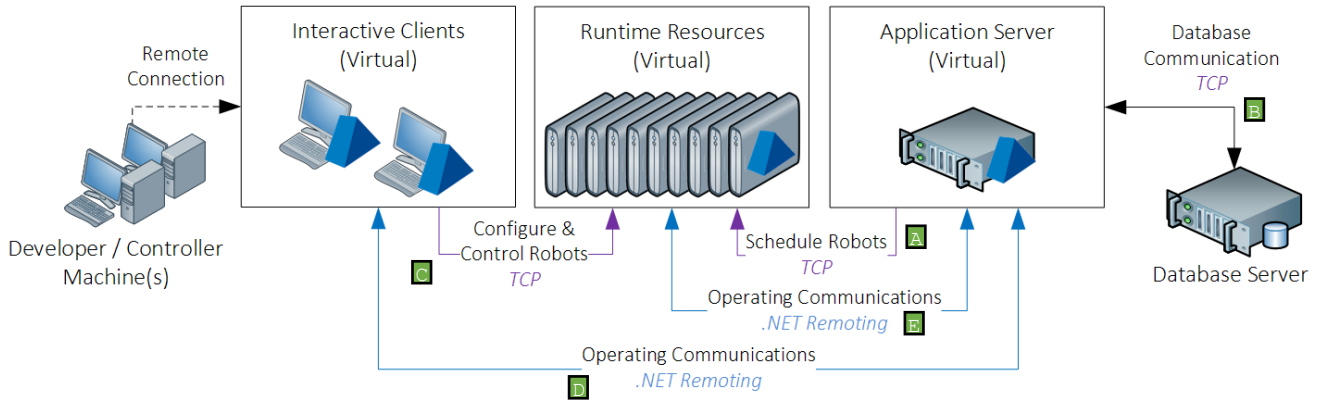
Further informaton about the typical communication that takes place between the Blue Prism components is detailed in the table below.

Application Server	• **Instructional: Schedule Robots** *(TCP)*
	A 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 .NET Remoting connection with the Application Server to retrieve the process configuration and for on-going communication.
	• **Database Communication** *(TCP - optionally leveraging certificate-based encryption)*
	B 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.
Interactive Client	• **Instructional: Configure and Control Robots** *(TCP)*
	C Communicates with the appropriate Runtime Resource to advise that a specific process is to be run. Once advised, the Runtime Resource then establishes a .NET Remoting connection with the Application Server to retrieve the process configuration and for on-going communication.
	• **Operating Communications** (.NET Remoting)
	D 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 .NET remoting connection which is established with the Application Server.
Runtime Resource	• **Operating Communications** (.NET Remoting)
	E 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 .NET remoting 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.

10.2.1. 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)
Interactive Client	• Receives inbound .NET Remoting traffic on the callback port number as defined within the connection to the Application Server.
Runtime Resource	• Listens for TCP traffic on **8181** (configurable) • Receives inbound .NET Remoting 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, each will be configured to listen on an independent, dedicated port.

10.2.2. 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.

10.2.3. Network Address Translation (NAT)

Microsoft's .NET Remoting does not support Network Address Translation (NAT) and therefore NAT is not supported for the inter-component communication that uses this protocol.

10.2.4.   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[7]

- 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.

10.2.5.   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.

---

[7] Resource Management. Following the reset, the affected Runtime Resources and all Controllers should be restarted.

10.3. Advanced Information

10.3.1. 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 it to initiate the start process procedure.

- an Interactive Client manually instructing it to initiate the start process procedure.

- 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.
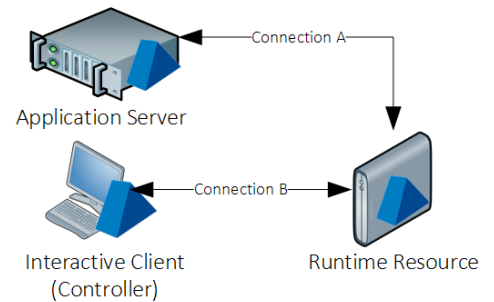
Within the Blue Prism platform, these connections are established from each operational Interactive Client and Application Server, to each available Runtime Resource using its configured listening port (default 8181).

10.3.1.1. 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.

10.3.2. 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 a single Application Server and use .NET Remoting which provides encrypted communication when used within an Active Directory network infrastructure and provides 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 establish a .NET Remoting connection with a nominated Application Server via two steps. Firstly the Runtime Resource connects to the Application Server on its listening port (default: 8199), and subsequently the Application Server will establish a callback connection to the Runtime Resource on the callback port specified (default: 0 = dynamic).

Application Server   Runtime Resource
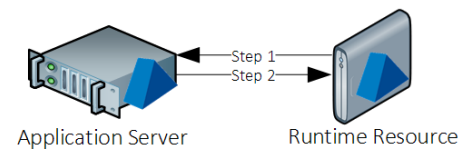
10.3.2.1.   Data Security and Controls

Protocol: TCP (.NET Remoting)

The communication is encrypted by default when all Blue Prism components are deployed within an Active Directory network infrastructure and "use secure connection" is checked at both the application server and client (this is the default setting when installing Blue Prism). The security is provided by the .NET Framework and the Operating System.

When the connection is set to secure, 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[8]:
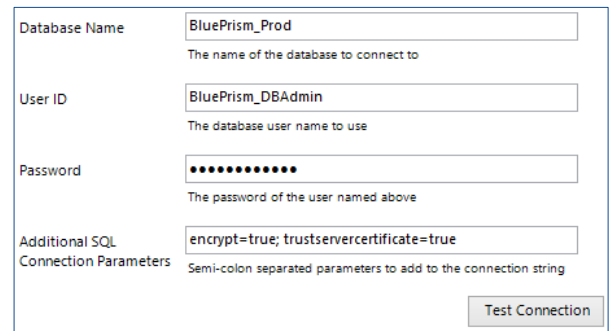
- **Content confidentiality**: .NET NegotiateStream is used to natively provide both key derivation and data encryption/decryption. SPNEGO is used to select the underlying security protocol, and the security context via negotiation between the client and server through use a set of security tokens generated 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.

---

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

10.3.3. 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:

1. Install a verifiable server certificate on the SQL Server and configure the SQL instance to force encryption for all connections.

2. Install a verifiable server certificate on the SQL Server and configure the Blue Prism database connection to specify that the connection should be encrypted.
   E.g. **encrypt=true**.

3. 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.
   E.g. **encrypt=true; trustservercertificate=true**.

Database Name	BluePrism_Prod
	The name of the database to connect to
User ID	BluePrism_DBAdmin
	The database user name to use
Password	••••••••••••
	The password of the user named above
Additional SQL Connection Parameters	encrypt=true; trustservercertificate=true
	Semi-colon separated parameters to add to the connection string
	Test Connection

11.   High Availability and Redundancy Guide

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

- Operational controls: How the platform is configured operationally to execute work can impact the behaviour 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.

11.1. Resilience of Components

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

- **Database server:** a core component of the platform and, as it is the realtime 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 Availlabity 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 interupted, 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 failover or re-direction will fail and be routed for human intervention.

Additional platform components include:

- **Runtime Resource**: responsible for executing the processes, each runtime resource is commonly located on a separate virtual device.

  Rundancy is achieved by provisioning additional Runtime Resources; and High availability can be achieved through use of Active Queues or Blue Prism Resource Pools. Both of these features represent groups of Runtime Resources and provide funtionality to scheduled or manually allocated to be allocated to an available Runtime Resource.

- **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 additonal devices and directing users to an available component as they establish a connection.

11.2. Routing Application Server Connections

The common way of deploying Application Servers is to allocate the Runtime Resources (and Interactive Clients) to a named Blue Prism Server, however there are a number of options for deploying these servers in a load balanced scenario such that the connections from the Runtime Resources and Interactive Clients are distributed.

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.

The following should be considered:

- The selected solution must be entirely transparent to the Blue Prism platform.

- The inter-component communication between the Client(s) and the Server takes place using Microsoft .NET Remoting which does not support NAT. This may be particularly relevant when when using hardware load balancers or complex routing.

- The connection between the Client(s) and the Server is established when the client comes online – the connection is only re-established once it has been forcibly dropped (e.g. when the client or server are no longer able to communicate).

- The return (callback) .NET Remoting connection from the Server to the originating device must bypass the routing device. The diagrams below illustrate the conceptual routing required when connecting a Runtime Resource or Interactive Client with a set of Application Servers.
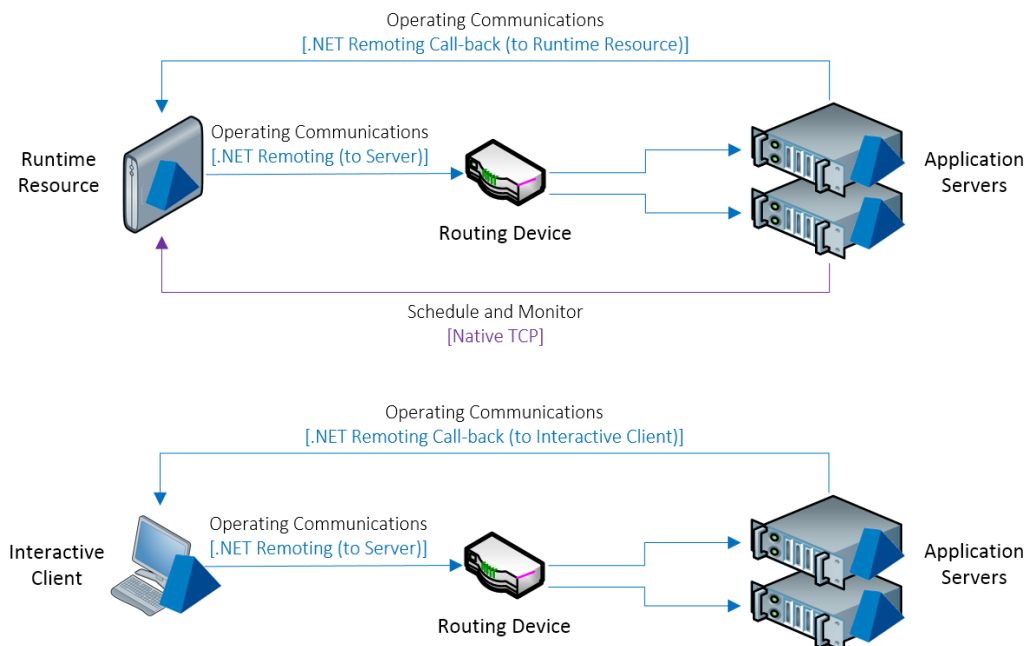
11.3. Multi-site Deployment

Information on configuring Active/Active and Active/Passive deployments is provided within the **Component Architecture Examples**.

12. Blue Prism Virtualization Guide

The **Blue Prism Virtualization Guide** provides a wealth of information in relation to deploying Blue Prism within a virtualized environment. It is available as a separate document via product support.

13. Blue Prism Monitoring Guide

13.1. Overview

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.

Further information on monitoring each of the Blue Prism components is provided in the Blue Prism Data Sheet – Monitoring.

14. Appendix

14.1. References

The following Blue Prism Data Sheets and Guides are available on request:

General Documentation	
Product Overview	High level overview of Robotic Process Automation and the Blue Prism Platform.
Release Notes	Version specific release notes detailing key features and functionality included in the release.

Blue Prism Data Sheets	
Active Directory Integration	Functionality and benefits of AD Integration.
Credential Manager	Features of the credential manager.
Operational Audit Overview	Overview of audit capabilities considerations.
Provisioning a Blue Prism Database Server	Considerations for selecting a suitable database server and provisioning a Blue Prism database.
Maintaining a Blue Prism Database Server	Considerations for maintaining the Blue Prism database.
Monitoring	Monitoring requirements of each Blue Prism component.
Remote Access Tools	Advice about suitability of remote access tools.
Secure Windows Authentication	Overview of auto-login facility for Runtime Resources.
Active Directory Integration	Functionality and benefits of AD Integration.
Credential Manager	Features of the credential manager.
Operational Audit Overview	Overview of audit capabilities considerations.
Virtualization Guide	Overview of the considerations for deploying Blue Prism into a virtualized environment.

Blue Prism User Guides	
Installing v5.0 Enterprise Edition	Installing and configuring Blue Prism Enterprise Edition.
Login Agent	Installing and configuring Login Agent.

14.2. SQL Tables

Information about each of the main Blue Prism database tables is provided below for reference. (Produced against database version 191 which was first available with Blue Prism v5.0.5).

Table Name(s)	Information
BPASession BPASessionLog_Unicode BPASessionLog_NonUnicode	Holds the logs of all the sessions which have been run. Each session created within Control Room or debugged in Process/Object Studio generates a record in BPASession - each logged stage executed in the process generates either a BPASessionLog_Unicode or BPASessionLog_NonUnicode entry (depending on whether Unicode logging has been enabled) linked to the session record. Important fields :- • **startdatetime** indicates when the session or stage was started, • **enddatetime** on BPASession indicates when the session finished - it's NULL if the session is still open / running. • **enddatetime** on BPASessionLog_Unicode/BPASessionLog_NonUnicode indicates when the stage finished if the stage is non-trivial - e.g. an action, subprocess or page stage will have an enddatetime; a calc, end, decision stage will not.
BPAScheduleLog BPAScheduleLogEntry	A log of all high level scheduler events - schedules starting / stopping, tasks starting / stopping, sessions starting / stopping.
BPAAuditEvents	Records all events occurring within the configuration / system management of the Blue Prism software - logins, queue creation/modification, password changes, etc. It also records the full history of the processes and visual business objects in the environment. It is this aspect of the table which will occupy the most physical space. Important fields :- • **eventdatetime** - when the auditable event occurred. • **sCode** - an alphanumeric audit type code - e.g. "modify business object" is `"B004"`; "modify process" is `"P004".` • **oldXML** - the XML representing the previous version of the process/VBO. • **newXML** - the XML representing the new version of the process/VBO.
BPAWorkQueueLog	Retains a log of every operation which alters a work item. For each item being added, locked, modified, retried, finished and deleted a small log record is created. It is also used in the **Get Transaction Data** action which can provide specific queue audit data. The data is retained beyond the lifetime of the work items.
BPAAlertEvent BPAScheduleAlert BPAProcessAlert BPAAlertsMachines	Alerts raised by the scheduler and process engines. BPAScheduleAlert, BPAProcessAlert and BPAAlertsMachines contain the configuration of the alerts. BPAAlertEvent holds the actual alerts raised by the process engine.

Table Name(s)	Information
BPAWorkQueue BPAWorkQueueItem	Represent the queues and work items used in the process. Each queue has a BPAWorkQueue record, each work item attempt has a BPAWorkQueueItem record (e.g. if a work item is terminated and retried, that will result in 2 linked records - one represents the terminated attempt, the other the retry). The item is not automatically deleted after it has been worked, although options are available for manual clean-up. Important fields: **BPAWorkQueueItem.id** - ID uniquely identifying the item (including all its attempts which are in separate records - i.e. the ID is not unique within the table). **BPAWorkQueueItem.ident** - ID uniquely identifying the item attempt - i.e. this *is* unique within the table. **keyvalue** - the key representing the item **loaded** - when the item was added to the queue **locked** - null unless it is currently set as being worked by a process **finished** - when the item was marked as complete / marked with an exception
BPATag BPAWorkQueueItemTag	The text categorising tags applied to an item is in BPATag. The assignment of each tag to a work queue item is in BPAWorkQueueItemTag.
BPAWorkQueueFilter BPAToolPosition	User interface preferences. e.g. filters on the work item view in control room; the position of the toolbars in process/object studio.
BPASysConfig	System configuration information. e.g. license, archiving status, etc.
BPAPref, BPAStringPref BPAIntegerPref	General preferences. e.g. user-specific overrides and system preferences.
BPAProcess BPAExceptionType	The processes and the known exception types used within the processes and the processes' attributes.
BPASchedule BPATask BPATaskSession BPAScheduleTrigger BPAScheduleList BPAScheduleListSchedule	Represent schedules and their configuration. BPAScheduleList represents the configuration of the reports and timetables available within the UI.
BPACalendar BPAPublicHolidayGroup BPANonWorkingDay BPAPublicHoliday BPAPublicHolidayGroupMember BPAPublicHolidayWorkingDay	The calendars defined in this environment. Used within schedules and by the calendars business object
BPACredentials BPACredentialsProcesses BPACredentialsResources BPACredentialsProperties BPACredentialRole	The credentials (encrypted username/password combinations) configured in System Manager.

Table Name(s)	Information
BPAPackage BPAPackageProcess BPAPackageCalendar BPAPackageCredential BPAPackageWorkQueue BPAPackageSchedule BPAPackageScheduleList BPAPackageWebService BPAPackageEnvironmentVar BPAPackageFont BPAPackageDashboard BPAPackageTile BPARelease BPAReleaseEntry	Release Manager tables. • **BPAPackage** and **BPAPackageXXX** tables record the packages defined in the environment • **BPARelease** and **BPAReleaseEntry** record the releases which have been created from those packages and imported into the environment.
BPAProcessBackUp BPAProcessLock	Ancillary process data. e.g. auto-saves from a process / object whilst it is being edited and locks set to ensure that more than one person is not editing a given process/VBO at the same time.
BPAResource BPAResourceRole BPAAliveResources	Represents the resource machines registered in the environment and logs which are currently available.
BPAValCheck BPAValCategory BPAValType BPAValAction BPAValActionMap	Process Validation configuration parameters.
BPAEnvLock	Environment locks which control access to critical sections of executing processes.
BPAUser BPAUserRole BPAUSerRoleAssignment BPAUserRolePerm BPAPerm BPAPermGroup BPAPermGroupMember	The users and their security constraints / permissions.
BPAEnvironmentVar	The environment variables configured in the environment.
BPADBVersion	A record of the database upgrades in this database. This is also used internally to verify the database version that the software is using.
BPAInternalAuth	Used for internal authentication between resources and resource managers (e.g. Control Room and the scheduler).
BPADataTracker	Version number table for arbitrary data - currently used to detect a change to the schedule configuration.
BPAPasswordRules BPAOldPassword	These tables contain the rules used when enforcing password complexity. E.g. contains a history of password hashes to ensure that passwords are not repeated. The rules are defined in system manager.
BPAResourceConfig	Configuration data for external business objects.
BPAFont	Data used for character matching in visual business objects.

Table Name(s)	Information
BPAWebService BPAWebServiceAsset	Definitions of web services registered within the environment.
BPAProcessMITemplate BPAStatistics	Definitions of the management information stats held on sessions.
BPAStatus BPAProcessAttribute BPAResourceAttribute	Code Lookup tables.
BPAScenario BPAScenarioLink BPAScenarioDetail	Testing scenarios for processes – pending deprecation.
BPADashboard BPADashboardTile BPATile BPATileDataSources BPAMIControl BPMIProductivityDaily BPMIProductivityMonthly BPMIProductivityShadow BPMIUtilisationDaily BPMIUtilisationMonthly BPMIUtilisationShadow	Dashboard and associated tile tables, along with the MI reporting repository which can be used to provide information for displaying on them.
BPAProcessActionDependency BPAProcessCalendarDependency BPAProcessCredentialsDependency BPAProcessElementDependency BPAProcessEnvironmentVarDependency BPAProcessFontDependency BPAProcessIDDependency BPAProcessNameDependency BPAProcessParentDependency BPAProcessQueueDependency BPAProcessWebServiceDependency	Object and process dependency information maintained automatically by the application.
BPATree BPAGroup BPAGroupGroup BPAGroupProcess BPAGroupQueue BPAGroupResource BPAGroupTile	Generic group and group membership details for processes, resources and other components defined within the application.
BPARecent BPAReport BPASession_OLD BPASessionLog_OLD BPAProcessEnvVar BPAUserViewPreferencePerProcess BPARealTimeStatsView	Deprecated tables.