blueprism®

Robotic Process Automation Software

Version 5 Feature Summary

USER GUIDE

Version: 5.0.30

For more information please contact:

info@blueprism.com | UK: +44 (0) 870 879 3000 | US: +1 888 757 7476

www.blueprism.com

Contents

Blue Prism Limited, Centrix House, Crow Lane East, Newton-le-Willows, WA12 9UY, United Kingdom
Registered in England: Reg. No. 4260035. Tel: +44 870 879 3000. Web: www.blueprism.com

Introduction

Version 5.0 from Blue Prism, the market leading Enterprise Robotic Process Automation provider, builds on the success of version v4.2 and leverages our experience of delivering enterprise strength RPA capabilities to an ever-growing number of blue chip clients and partners.

Shaped using feedback from sources including customers, partners, industry analysts and the Blue Prism RPA (Robotic Process Automation) thought-leadership team, the platform continues to lead the way in defining the standard for Enterprise RPA.

It extends the enterprise capabilities of the platform and fundamentally shifts the automation paradigm to deliver a Virtual Workforce aligned with the operational objectives and priorities of class-leading organizations and deliverable from the cloud.

This guide provides details of the features that are provided in the version of Blue Prism Version 5.0 specified on the title page.

Feature summary

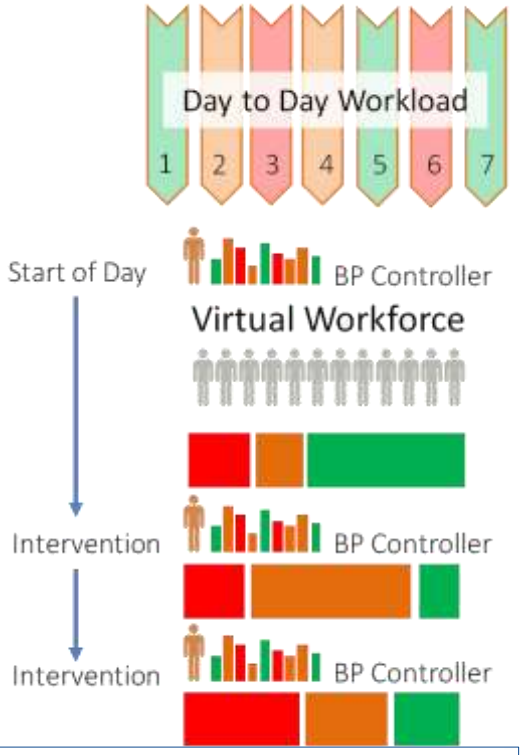
Blue Prism v5 focuses on six core themes, and information is provided below on the features that are delivered against each. These highlights are intended to provide useful insight for experienced users looking to assess and understand the capabilities of Blue Prism version 5.0.

- Virtual Workforce
- Insight and Analysis
- Scalability
- Development and Implementation
- User Experience
- Enterprise Platform

Virtual Workforce

Traditional workforce management provides the ability to allocate the most important work items to team members who have the appropriate training, according to operational priorities such as SLAs, targets or completion times.

The Blue Prism virtual workforce extends this paradigm by providing greater control and flexibility as well as real-time insight and visibility. The virtual workers retrieve work from the queues, apply complex decisions consistently, without bias, and leverage the centralized knowledge repository. This enables the virtual workers to be directed to work on any automated process based on operational demands.



Work Queues

Blue Prism v5 Active Queues elevate the existing work queue functionality by providing a queue-centric approach for dynamically controlling the number of Resources operating against a given queue at a particular time.

This provides the maximum flexibility to adjust the number of Resources assigned to collaboratively work items in the queue based on business demands and is available in addition to the original capability of simply assigning Resources to a process.

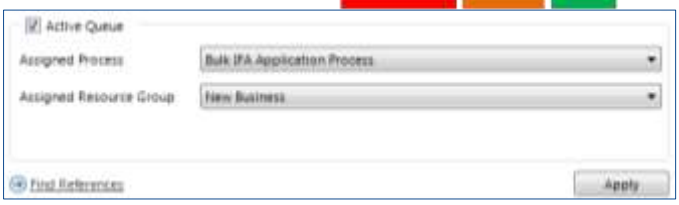


Figure 1: Active Queue configuration

Active Queues are configured within the Work Queue management area of the System tab. A queue is associated with a group of Resources and a Process that has been configured with Safe-Stopping points. These points allow automation developers to manage the wrap-up procedures that will be followed once a stop notification has been received.

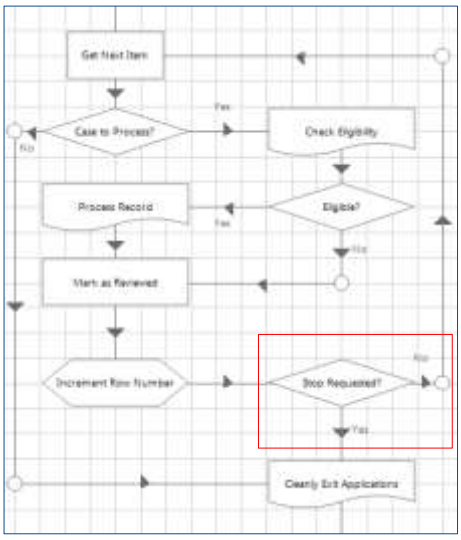


Figure 2: Safe-stop check within a process

Active Queues are designed to work with a specified group of individual Runtime Resources and is not intended for use with Resource Pools.

Figure 3: Centralized panel for dynamically managing Active Queues

Control room filters

Control room filters provide users with rapid access to important and commonly used views.

Session management filters are user specific and apply a predetermined filter to the session activity that is presented within the viewing pane. Commonly these filters are configured to present the sessions related to a specific process within a defined timeframe (i.e. today, last 7 days etc.).

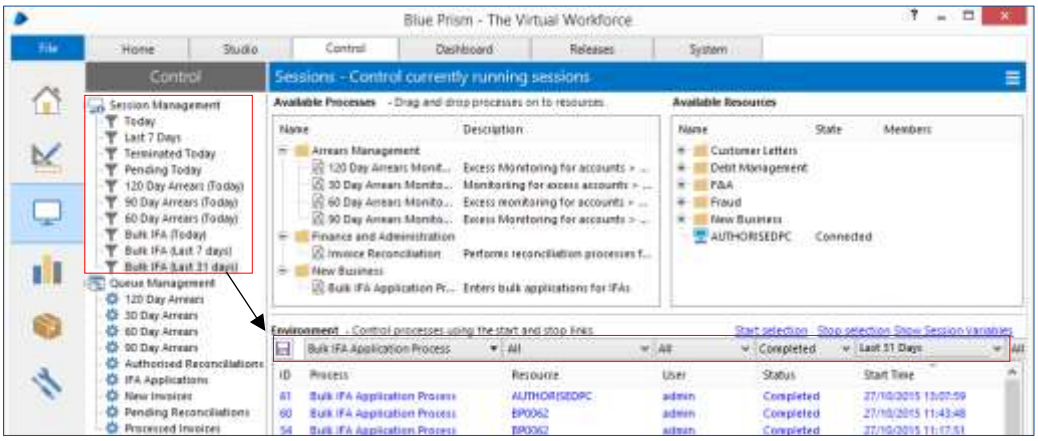


Figure 4: Personal session management filters

Queue management filters are global and provide a common set of criteria that can be applied against any of the Queues. There is also the option to configure a filter as the default to be applied when a particular Queue is selected.

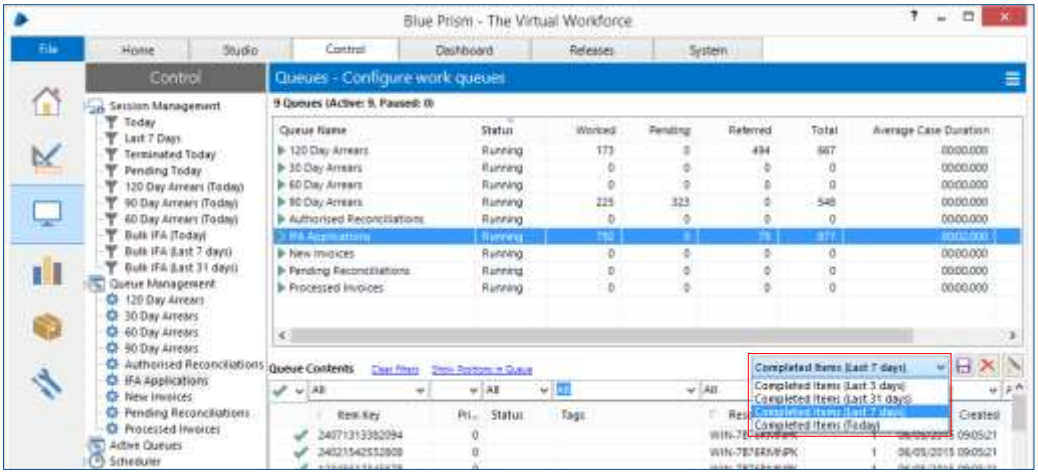


Figure 5: Global queue management filters

Logging levels

Session logging has been extended to provide Errors Only logging which ensures critical information about the workforce can still be captured, even where disk space is a premium.

On each stage when editing a Business Object or Process, the **Disable all logging on this stage option** has been replaced with a selection list with three values:

- Enabled
- Disabled
- Errors Only

Additionally, the logging level for all stages in a Business Object or Process can now be toggled via the Edit menu enabling the setting to be applied for all, or selected, stages across all actions/pages.

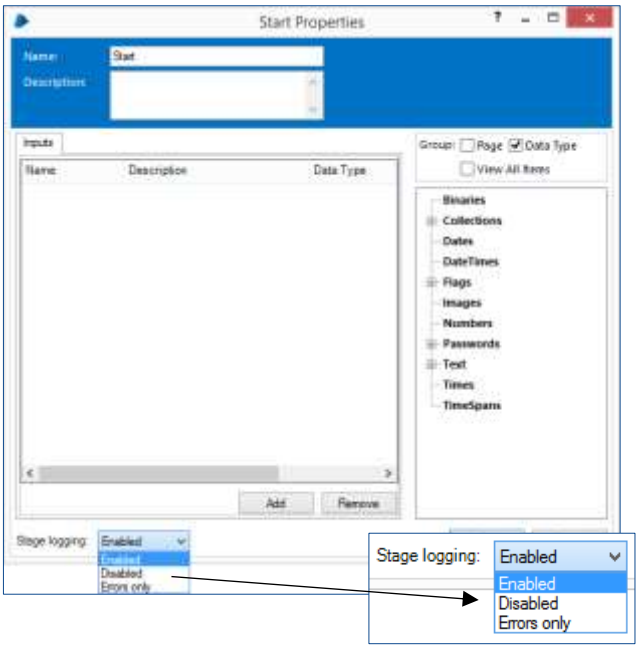


Figure 6: Stage logging level options

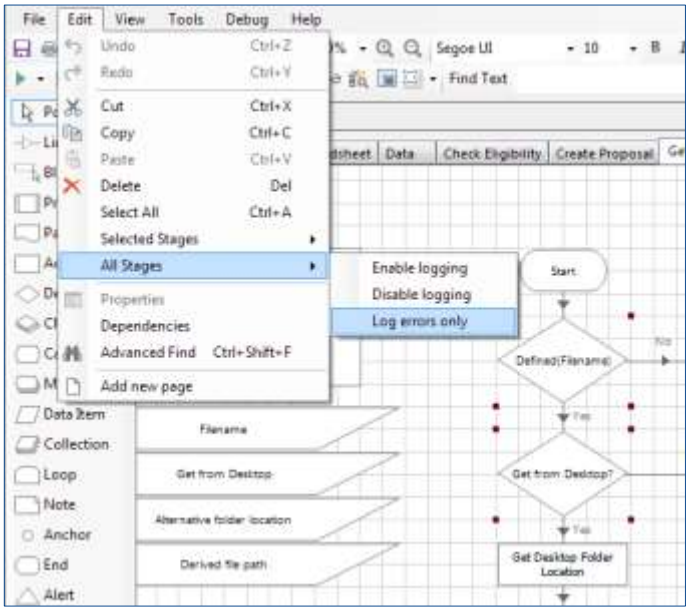


Figure 7: Stage logging level via edit menu

Insight and Analysis

As with any operational team there is an increasing need for greater visibility, insight and analysis of not only the work being carried out, but also utilization, completion rates and processing trends over time.

Blue Prism v5 provides a number of features that deliver insight and analysis within the product and supports the use of external interrogation through a standardized approach.

Management dashboards

When accessing Blue Prism v5 users are presented with the system-wide default dashboard providing immediate visibility of the virtual workforce by providing visualization of key metrics.

A dashboard provides a custom view of a number of Blue Prism metrics composed from a series of tiles.

It can be made private to the user creating it, or global, such that it can be available to all users with the appropriate permissions.

Dashboards are configured once in Edit mode, and tiles are placed by dragging items from the Tile Library into the main viewing pane.

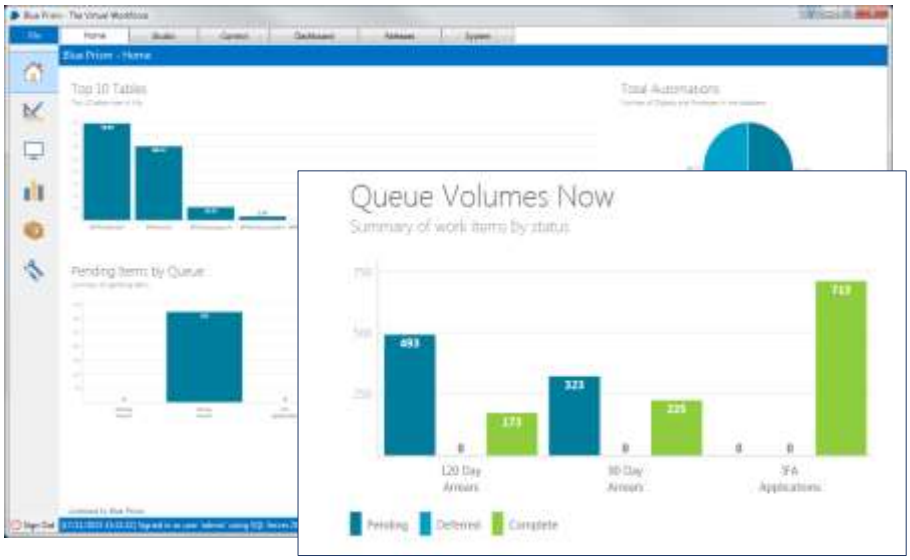


Figure 8: Illustration of dashboard

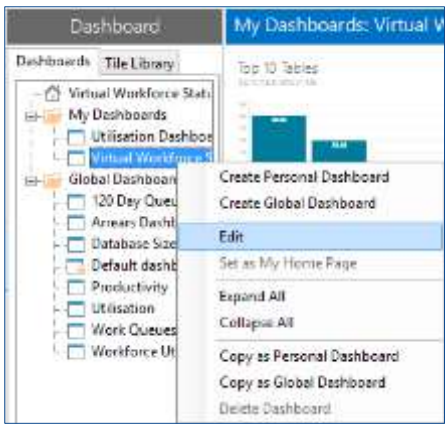


Figure 9: Edit dashboard via context menu

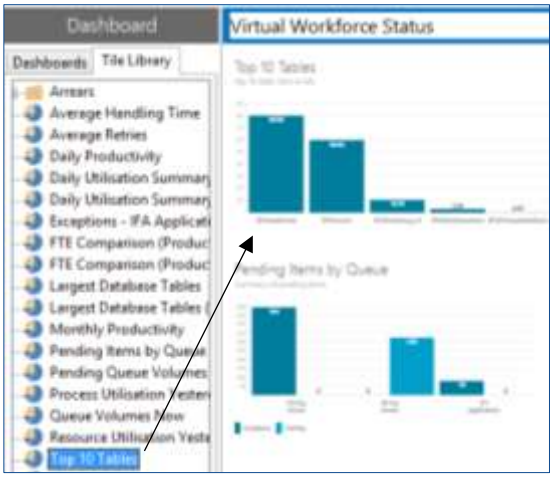


Figure 10: Dragging a Tile onto a dashboard

Tiles

A **tile** is a view of specific metrics, either in the form of a chart or graph, retrieved from a selected **data source** (stored procedure) within the database.

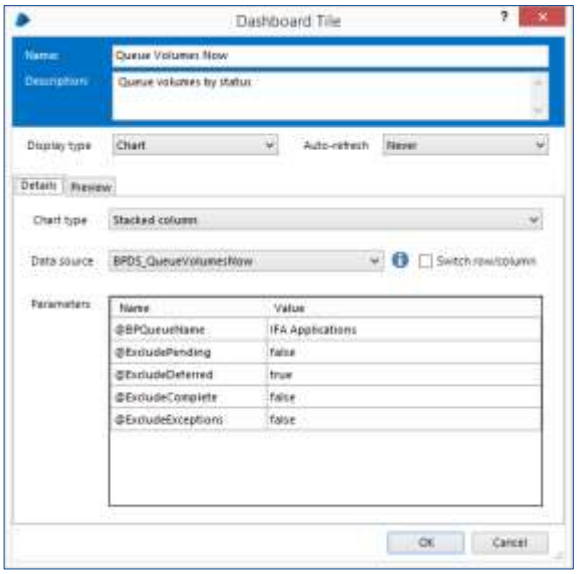


Figure 11: Tile configuration

Various aspects of the tile's behaviour can be modified, such as setting the type of chart that the tile should present within a dashboard (e.g. Bar, Pie, Gauge); the interval between refreshes of the data from the data source and the values to be passed into the parameters that the data source expects.

Data Sources

The **data source** is a stored procedure defined in the Blue Prism database which is called by the tile in order to retrieve the data that it presents. A number of basic data sources are provided with the software; information on these is available in the help and can be presented clicking the information button next to the selection box in the Tile configuration window.

Custom data sources can be created by creating a stored procedure on the database with a name prefixed with "**DS_**" - this will be detected by the Blue Prism tile configuration and will be made available for tiles defined within the environment.

When creating custom stored procedures on the Blue Prism database, consideration should be given to the performance impact that they will have on the system when executed.

External tools

Third-party reporting or analysis tools can consume the configurable data sources, and further custom data sources can be added by expert users. When named appropriately, the custom data sources will automatically be available for selection within a tile.

Data collation utility

To support trend analysis over time, additional real-time insight is captured as processes execute, providing greater variation of metrics. A number of tiles are configured using this information which is collated in addition to the existing runtime statistics.

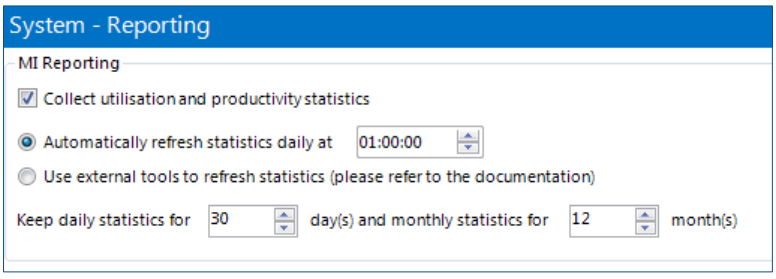


Figure 12: Settings for system reporting

This additional information is only collated where the setting to **Collect utilisation and productivity statistics** is enabled.

This information is summarised periodically and retained based on the subsequent settings.

There is an in-product utility available to automatically refresh the statistics each day, or a manual job can be configured using the provided stored procedures. Further information on the **MI data refresh settings** within the in-product help.

Scalability

Blue Prism v5 continues to build on the enterprise-strength credentials of the platform and sees a number of updates and enhancements to ensure that the underlying technologies remain current as the product is used in an increasingly wide range of situations. This helps to ensure that support is provided for an ever-increasing number of users, distributed across a range of geographic locations.

Trusted Domain Single Sign-On

Version 5.0.24 extends the capabilities when using Single Sign-on to authorize access to the Blue Prism Platform by adding support for users who are members of trusted domains within a common Active Directory Forest. It is now possible for users within any appropriately trusted Domain in the Forest to be configured with access and permissions in Blue Prism. As with previous versions, Blue Prism must be directed to a Domain in which the Active Directory Security Groups that will be directly associated with Blue Prism Security Roles reside.

This functionality is accompanied by a refresh of the screens that are used to configure Single Sign-On for Blue Prism.

The **Synchronise Users** action has been replaced by **Refresh User List** which re-evaluates the users who are recognised as being members of Active Directory Security Groups that are associated with a Blue Prism Security Role.

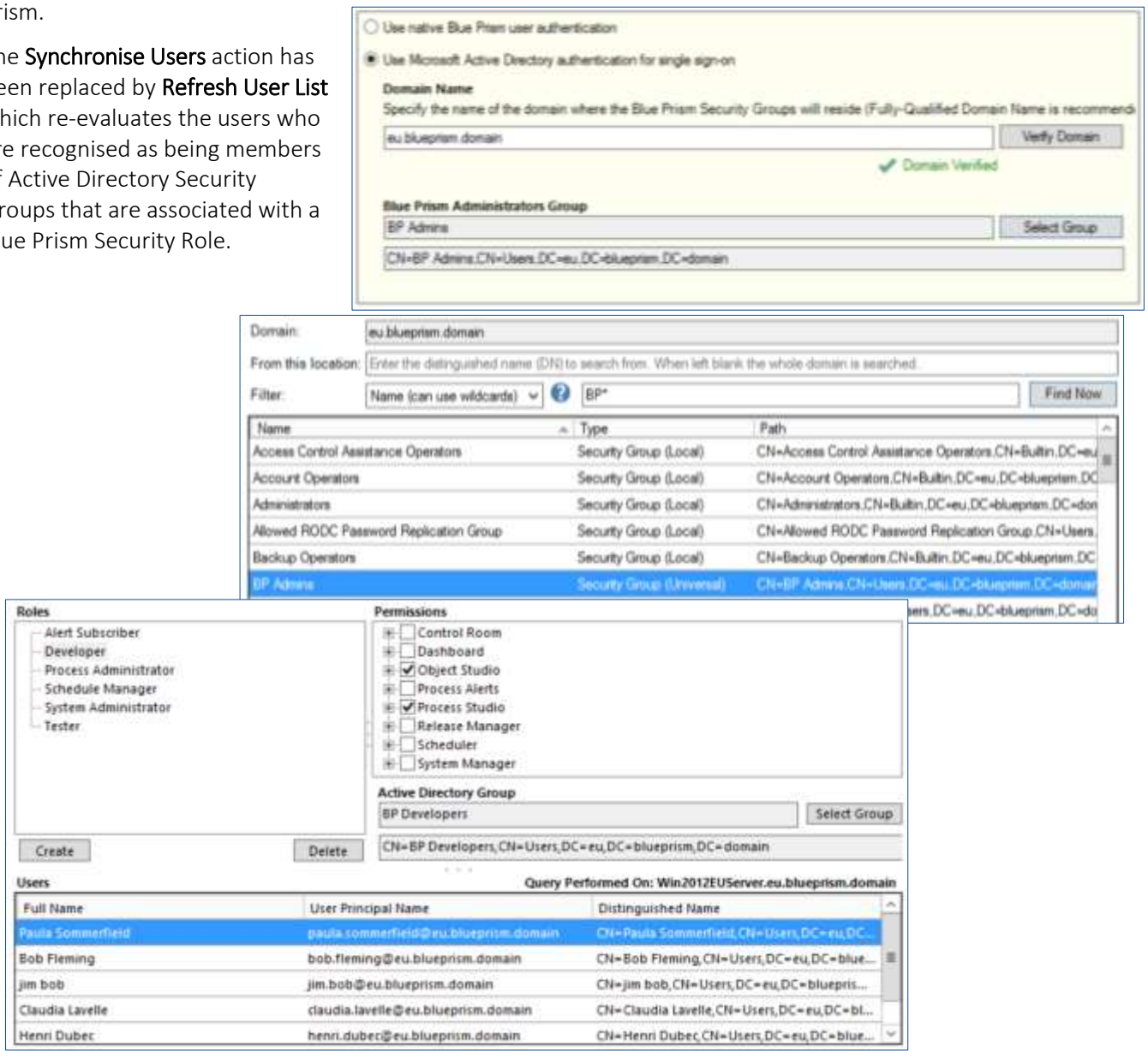


Figure 13: Configure Single Sign-On

Multi-tier grouping structure

A hierarchical grouping mechanism provides flexibility for configuring how items are displayed within Blue Prism. They are particularly useful for organizing Processes, Objects and Resources within a user-friendly structure.

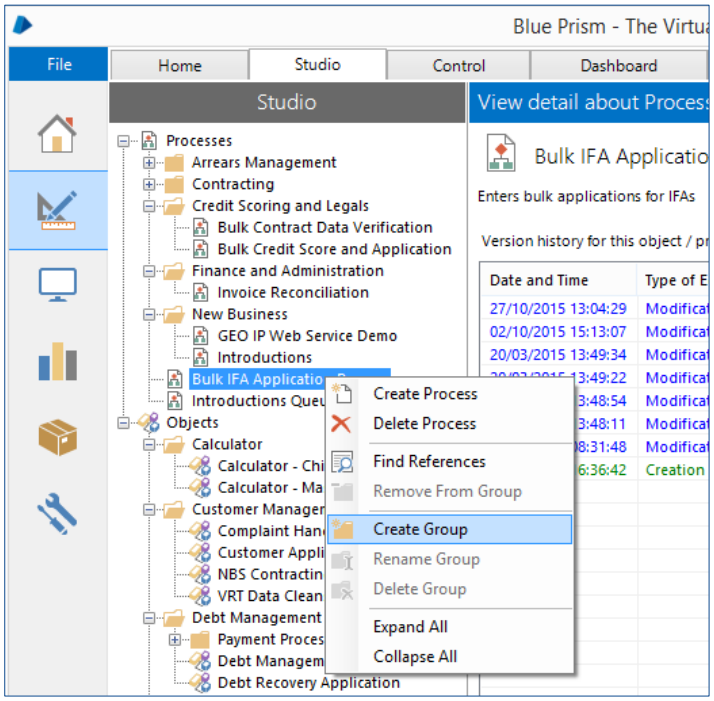


Figure 14: Process and Object groups within Studio

Enhanced data security with Encryption Schemes

Encryption schemes are used to define the settings (algorithm and key location) when writing the data for credentials and encrypted work queues into the database.

Encryption schemes enhance the capabilities for securing sensitive data within the database by:

- Providing a standardized approach for defining the encryption schemes that are available to be used within the environment.
- Allowing use of the AES-256 (Rijndael) algorithm as an optional alternative to 3DES. (v5.0.24 additionally introduced support for an additional AES-256 provider - AesCryptoServiceProvider)
- Allowing multiple encryption schemes to be defined within a single environment.
- Enabling system administrators to select which encryption scheme will be used for processing credentials and for each optionally encrypted work queue.
- Providing the option, when using Application Server based encryption keys (recommended), to have the keys stored within independent files.

The scheme to be used for credentials and optionally for each work queue is configured within the User Interface, and it is the selected scheme that is used when writing the relevant data into the database. Subsequently, data is read using the scheme used to perform the write meaning that the Credential Manager or encrypted work queues can be updated to use a different scheme at any time as this change will only come into affect as information is written to the database.

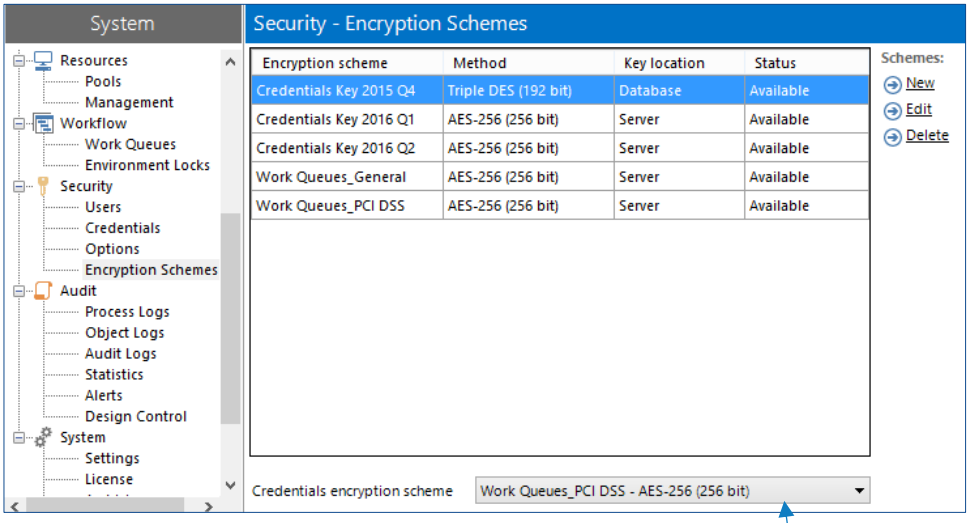


Figure 15: Encryption scheme list and configuration

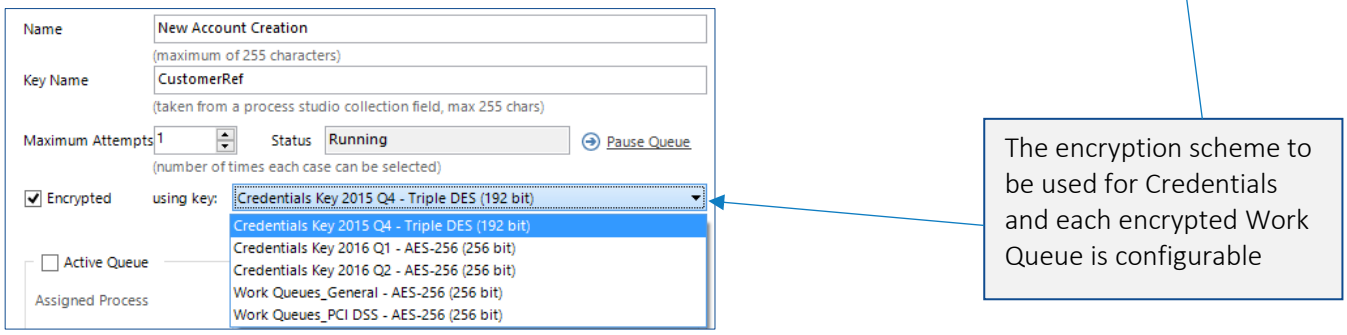


Figure 16: Work Queue configuration

Configuring Encryption Schemes

The encryption schemes that will be available within the environment must first be configured using an Interactive Client. The settings are found within System -> Security -> Encryption Schemes.

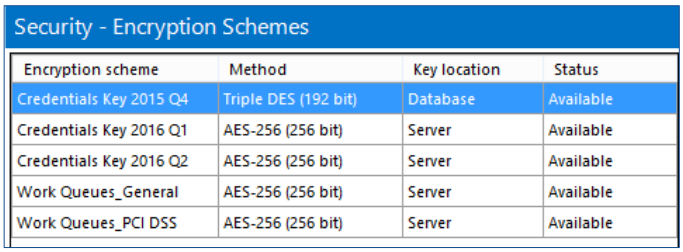


Figure 18: Interactive Client configuration

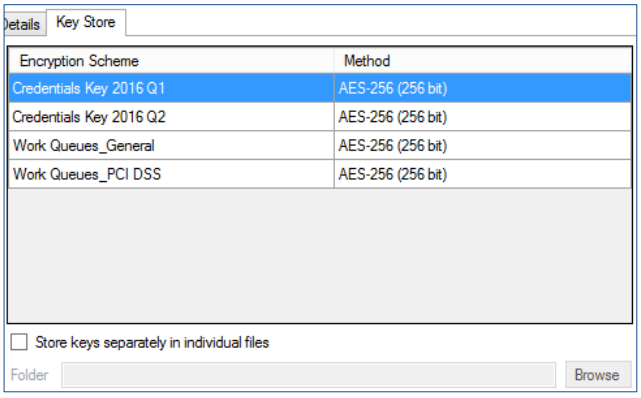


Figure 17: BPServer.exe configuration

It is also necessary to ensure that each Application Server for the environment is configured to have the same schemes and settings before a given scheme is made available and used.

> The encryption schemes configured locally on each Application Server service, must be directly aligned with those configured in the database using the Interactive Client prior to being used.
>
> A copy of each key must be backed up in a secure location - it will be needed to retrieve encrypted data if the server fails.

In order to configure the Encryptions Schemes that will be available within an environment users will require the **Security – Manage Encryption Schemes** permission. Additionally changes will also be required to the configuration of each Application Server.

Applying custom security to the encryption keys

When following the recommended approach of use the Blue Prism server as the location for the encryption keys, a new optional feature is provided that will **Store keys separately in individual files**.

This is provided for system administrators who wish to further secure the file such as by restricting which users can get access, or by applying encryption. When applying additional controls it is important that these are transparent to Blue Prism and that the account(s) used by the Blue Prism Server service retain access.

Re-encrypt Utility

A command line utility (AutomateC /reencryptdata) provides the ability for the platform to be instructed to update all data which has been encrypted using a scheme which is no longer the currently selected scheme for the given purpose (Credential Manager / Work Queue).

The parameter /batchsize controls the maximum number of records that will be updated at a time (default is 1000), /maxbatches controls the maximum number of batches that will be processed (default is 1).

Credential manager expansion

The credential manager provides fields for storing optional data values such as an expiry date and whether it has been marked as invalid. These can be checked when leveraging a credential to ensure that it is suitable for use, or as part of a credential management routine to periodically update passwords that are due to expire.

Additionally, custom attributes can be defined which provide the ability to store supplementary information that may be required when authenticating against a third party system such as the values for mother's maiden name, or town of birth etc.

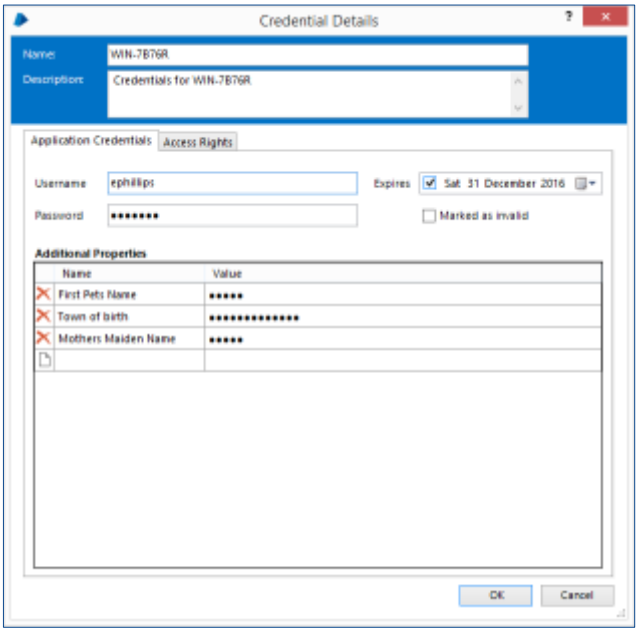


Figure 19: Credential details

Latency

In order to support complex or distributed environments the Runtime Resources (robots) can now be deployed in scenarios where the connection between the component and the Application Server is not low latency. Processes that have been appropriately designed have been successfully validated on Runtime Resources with a round-trip latency connection with the server of up to 400 milliseconds.

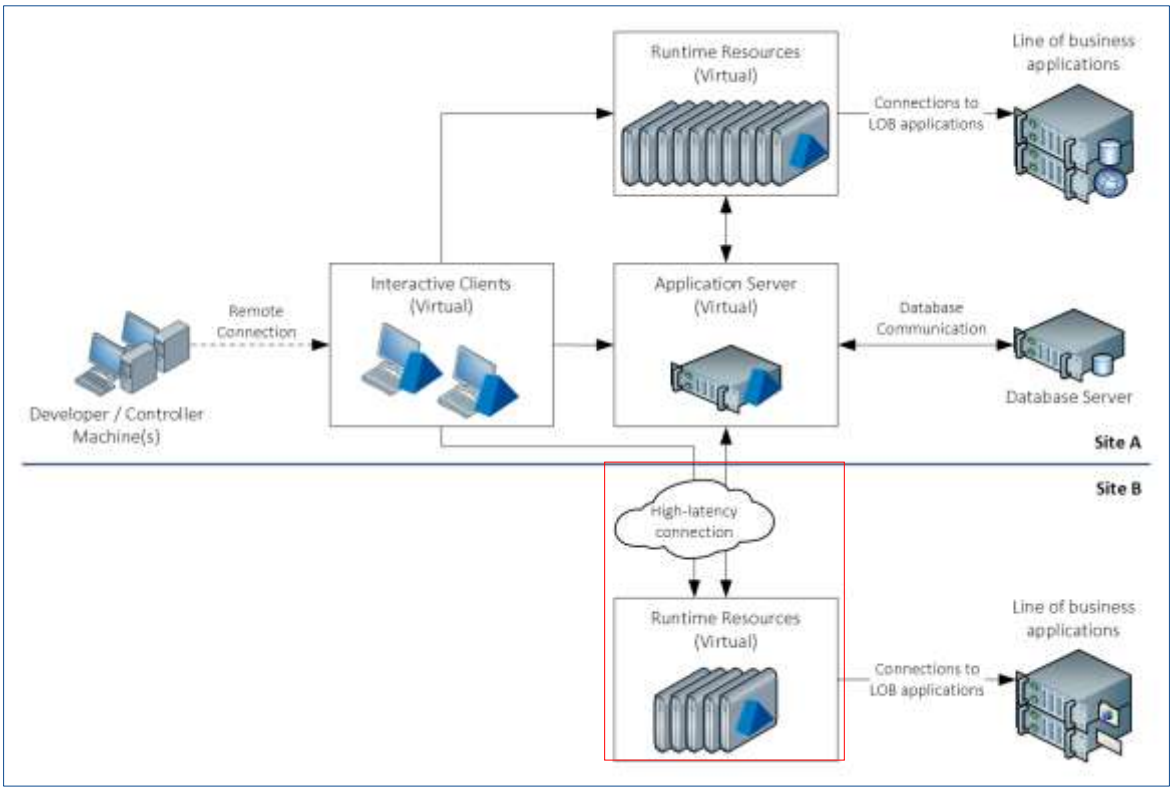


Figure 20: Illustration of high-latency connection support for Runtime Resources

Internationalization

Localization

Supports the deployment of all Blue Prism components onto devices configured for different locales allowing developers and controllers to work with their own locale settings. This accounts for differences in date/time formats as well as the use of different decimal, number grouping and parameter separators.

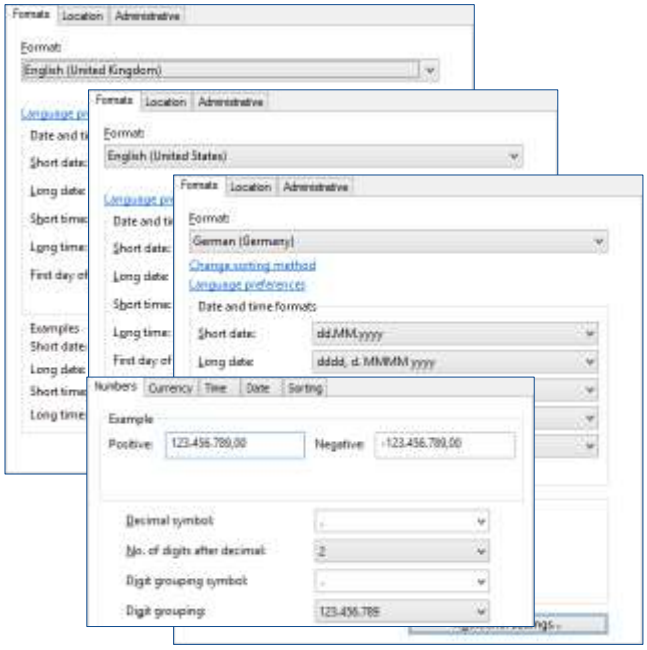


Figure 21: Region/locale settings on the device

Unicode Data Storage

The underlying platform is updated to support the processing and storage of Unicode data within the database to provide the capability to work with any character set (single and double-byte).

Whilst Unicode storage provides significant advantages, it does require comparatively more disk space which will have a direct impact on the amount of space required to host the Blue Prism database, particularly in relation to the storage of session logs or large work queues. By default, therefore, Session logs are not configured to support Unicode but this feature can easily be enabled from within the System tab.

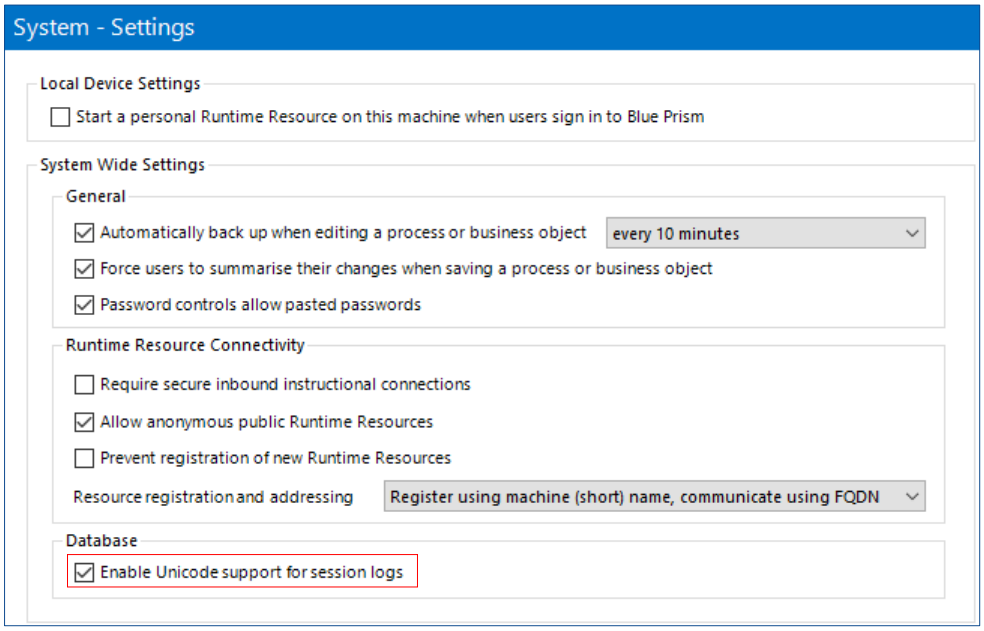


Figure 22: Setting to enable Unicode support session logs

It is recommended that disk space usage and availability is reviewed along with the session log retention and archiving settings for environments upgrading to Blue Prism v5 particularly where Unicode session logging will be enabled. Additionally SQL Server Unicode Compression, whilst not available in all editions of SQL Server, can be used to minimise the amount of disk space required.

Enhanced options for device 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.

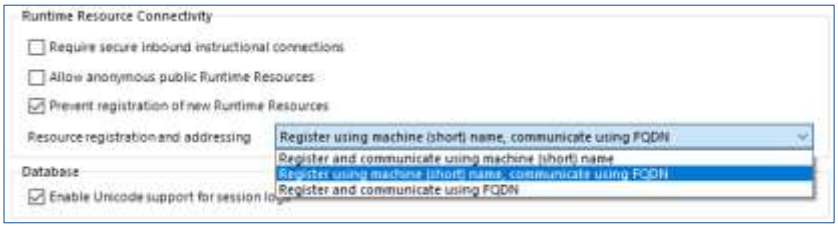


Figure 23: Setting to configure registration options

With Blue Prism v5.0 System Administrators can optionally change this setting if appropriate for the deployment:

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

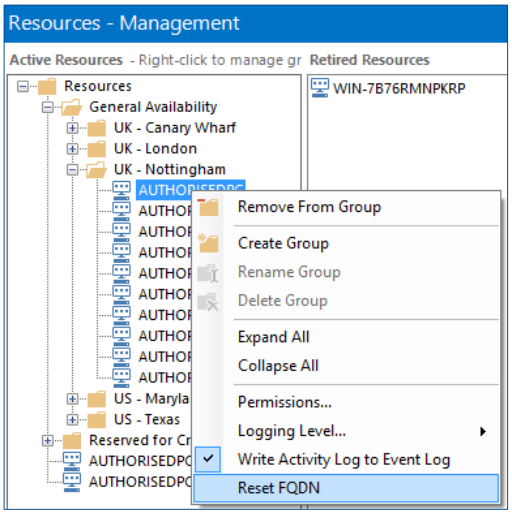


*Figure 24: Reset FQDN setting**

*if a device registers which matches a previously registered short-name but has an FQDN which does not match the one previously registered, the connection will be rejected. In this scenario the FQDN associated with the short-name can be reset within Resource Management. Following the reset, the affected Runtime Resources and all Controllers should be restarted.

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.

Encrypting Instructional Communications received by Runtime Resources

In addition to the mechanisms that are already provided for applying encryption to the inter-component communication, support is now provided for advanced implementations whereby Runtime Resources can be configured to use a local certificate to provide certificate-based encryption for inbound instructional communication.

These communications can originate from a number of sources including:

- Interactive Clients (e.g. Control Room)
- Application Server(s) (e.g. Scheduler)
- External systems consuming (E.g. accessing published web services)

The communication is received by a .NET service listening on a designated port (default: 8181) on each device hosting a Runtime Resource. By default this communication is native TCP however it can be secured 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.

Information on Configuring a Runtime Resource listener to leverage a certificate is provided within the **Blue Prism Data Sheet – Securing Network Connectivity**.

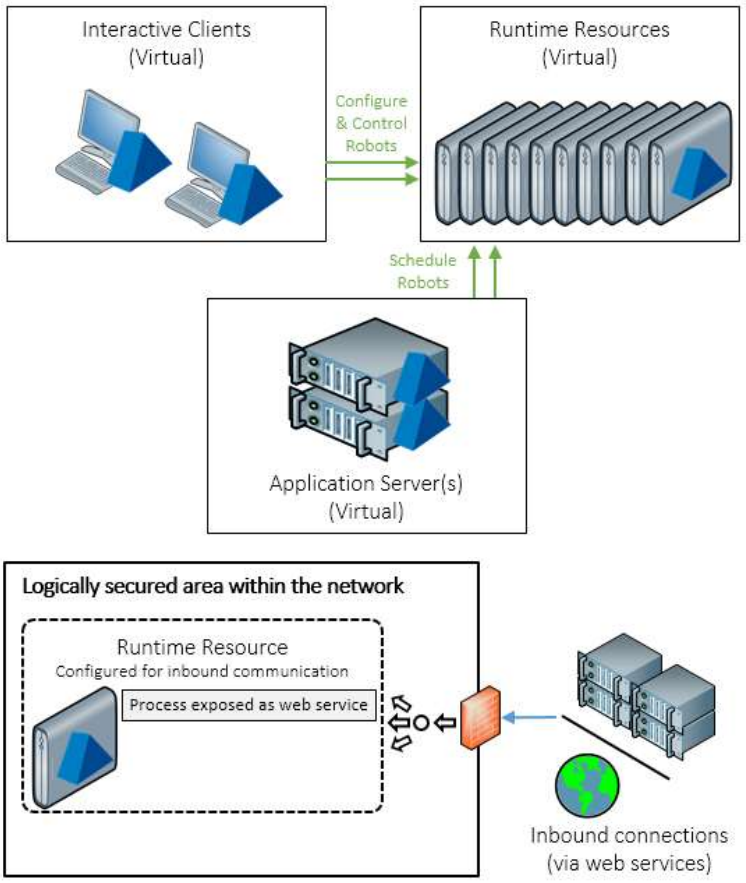


Figure 25: Examples of Instructional Communication

Robot Authentication

Blue Prism Runtime Resources can now be configured to authenticate against the Blue Prism environment when they start-up. This provides greater control over which devices can connect into an environment and therefore which devices are available for work. Additionally it is now possible to explicitly control the permissions that will be granted to a given Runtime Resource by configuring the Blue Prism account that it uses to authenticate.

The configuration that must be added to the start-up parameters of Runtime Resource to instruct it to authenticate is based on the authentication methodology enforced by the Blue Prism platform:

- Blue Prism Native: Use the /user switch. E.g. /user username password
- Single Sign-on: Use the /sso switch. E.g. /sso

The Login Agent Runtime Resource can also be configured to authenticate against the Blue Prism environment by configuring the Login Agent configuration file. When connecting to a Blue Prism environment that is configured for single sign-on, it will also be necessary to configure the Login Agent windows service to run under the context of a domain account that is configured with access to Blue Prism.

Security Controls for Runtime Resources

A number of system-wide configurable options are provided which can be used to only prevent Runtime Resources that do not meet the standard being enforced by the environment from establishing a connection.

- Require secure inbound instructional connections
  Requires Runtime Resources to only accept ionbound instructional connections over a secure channel, and additionally prevents Runtime Resources which are not configured to provide certificate-based encryption for inbound connections from establishing a connection to the environment.

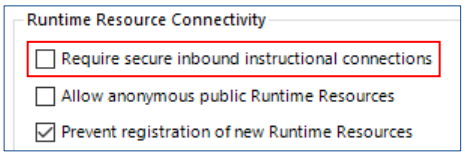


Figure 26: Prevent connections from Resources that are not configured to apply encryption

- Allow anonymous public Runtime Resources
  Provided only for backwards-compatibility, where enabled allows Runtime Resources to connect to the environment without explicitly authenticating. When disabled, only public Runtime Resources that explicitly successfully authenticate against the environment will be able to establish a connection.
- Prevent registration of new Runtime Resources
  When enabled, only Runtime Resources that have previously connected with the environment will be able to establish a connection. This provides administrators wth the ability to prevent new or unexpected Runtime Resources from connecting to the environment.

These settings do not apply personal Runtime Resources which can be configured to automatically start when a user logs into the Blue Prism client.

Development and Implementation

Blue Prism v5 introduces a fresh user interface which reduces the on-boarding time for new users, whilst providing existing users with greater control and access to the features that they need most frequently.

Automation Capability

New features which extend the capabilities of the runtime automation engines include: In-product OCR for interpreting smoothed on-screen fonts; improved Active Accessibility integration options; extended credentials functionality; and support for working with international locales and character-sets (including double-byte).

Font recognition for joined characters

Initially available as an early access feature within v4.2, this provides support for interpreting joined characters for scenarios such as where natively two or more characters are presented as one. Additionally learnt characters can now be deleted.

Embedded OCR

Initially available as an early access feature within v4.2, an OCR engine is available within Blue Prism for situations where it is not appropriate to use the native character recognition engine to interact with on-screen text including scenarios such as where smoothed-text is enforced. The functionality leverages pattern matching and complex, language-based text recognition making it also suitable for interacting with scanned, or otherwise-restricted, copies of electronic documents.

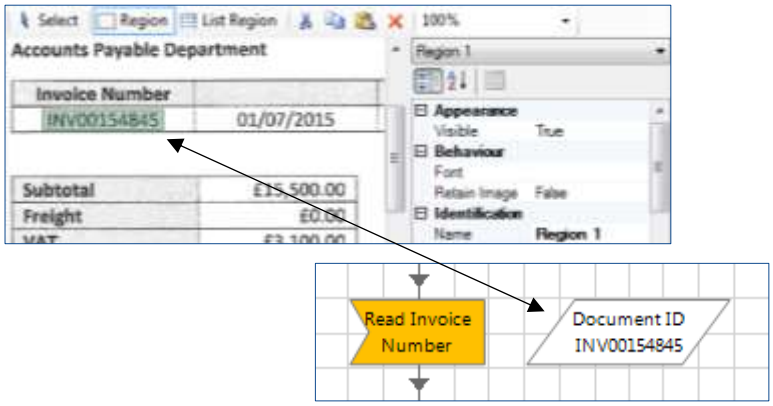


Figure 27: Illustration of reading data using OCR

Windows 10 and Windows Apps

Blue Prism 5.0.23 introduced certification for using Blue Prism on Windows 10 devices and also provided native support for automating Windows 10 store apps. When configuring the Application Manager to connect to an app such as Calculator is it possible to use the installed app name e.g. **<Microsoft.WindowsCalculator>**.

A list of the apps installed on a given device can be retrieved using the PowerShell command:
Get-AppxPackage -AllUsers | Select Name.

Enterprise development

Provides accelerated development of complex automations and includes increased options for object orientation through optional separation of the application model. Additionally there is greater capability for multiple developers to simultaneously work on the same automation whilst dependency tracking functionality provides increased visibility of the various connections and references.

Global application models

Application models can now be referenced from multiple Business Objects allowing large applications be modelled centrally with a series of Business Objects each containing a subset of the required actions. This approach of allowing the model to be separated from the actions not only provides greater flexibility for organizing and managing this portion of the configuration, it also provides greater scope for accelerated development as multiple people can simultaneously work against a shared model.

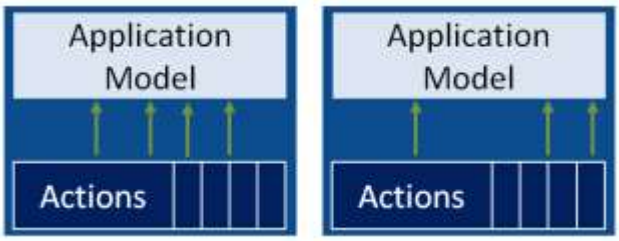


Figure 29: Self-contained business objects

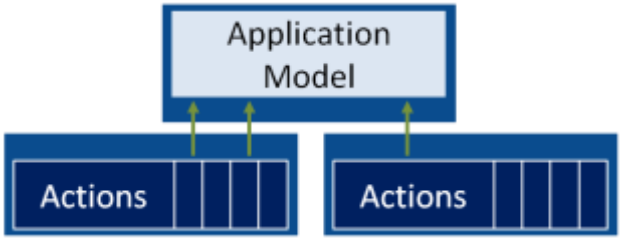
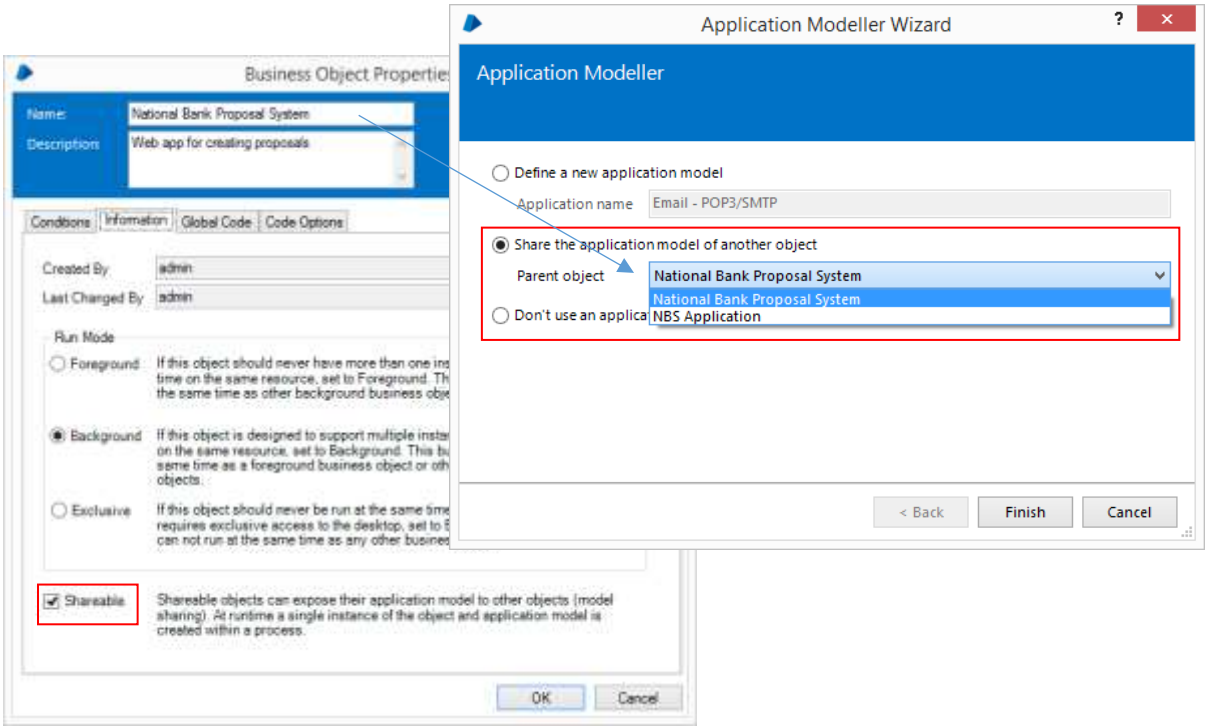


Figure 29: Business objects sharing a global application model

Support for both Self-contained business objects and business objects which share a global application model is provided.



A Business Object must be marked as Shareable in order to be available for selection in the Application Modeller Wizard as shown above.

Copy and paste for actions and pages

Copy and Paste functionality is now provided for Business Object actions and Process pages providing accelerated development and greater control over the structure and arrangement of developed content.

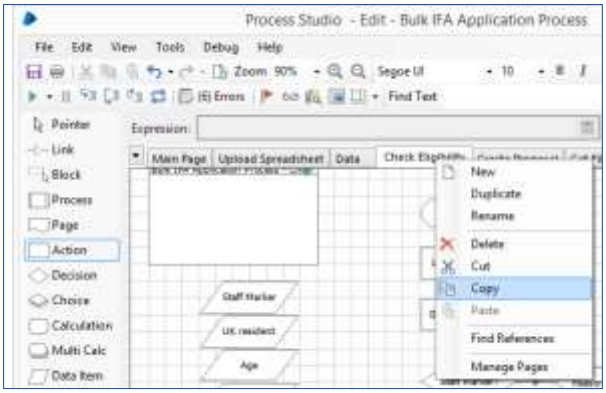


Figure 30: Cut, copy and paste process pages

Copy Queue Items

The ability to copy a queue item to an additional queue is provided, and includes the ability to modify key attributes of the item including tags, item status, priority, and defer until information.

Dependency tracking

Featured throughout the platform, dependency tracking provides an interactive view of how a given component is referenced within a designed process to accelerate development, promote re-use and support maintenance.

Applies to:

- Application models and elements
- Objects and actions
- Processes and pages
- Credentials
- Calendars
- Fonts
- Environment variables
- Web services
- Work queues

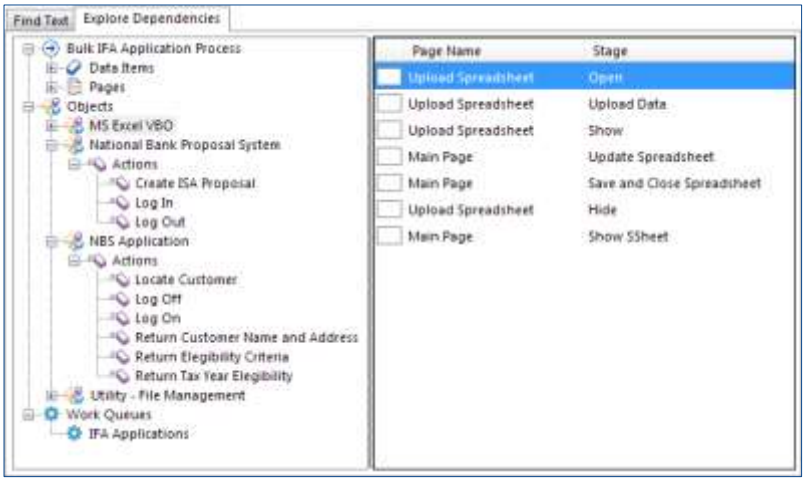


Figure 31: Find References

Version history prominence

The prominence of the version history for Business Objects and Processes has been increased within the user interface. It is now additionally presented within the Studio tab providing immediate visibility of the updates and modifications that have been applied.

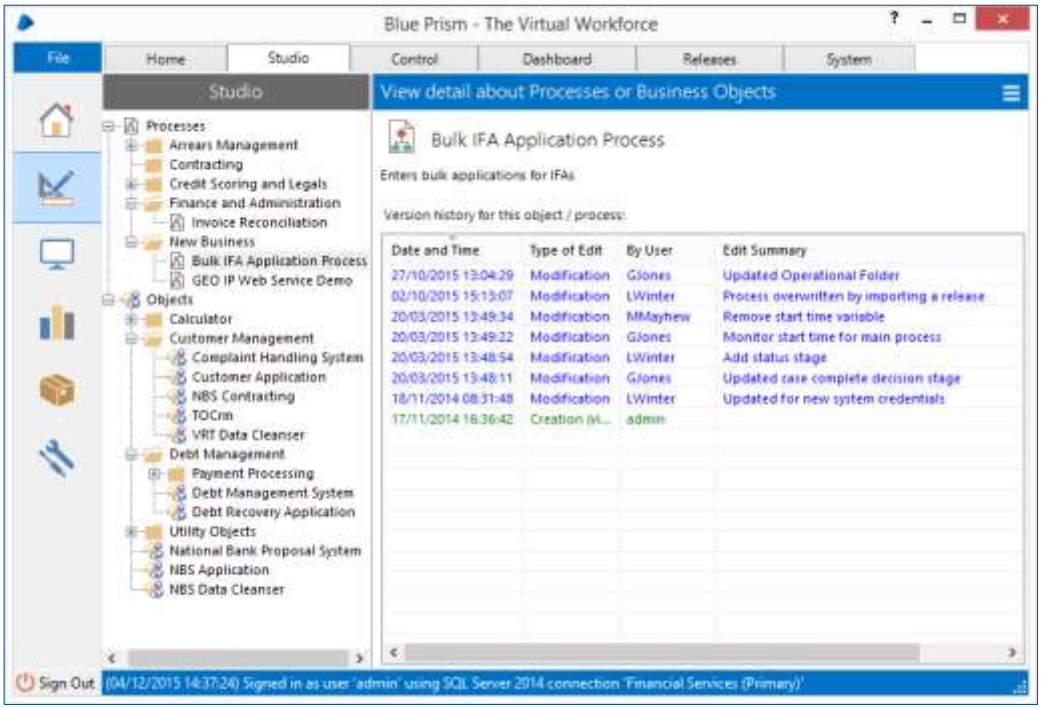


Figure 32: Version history of a process within Studio

Environment License Store

Blue Prism 5.0.24 provides an update the License Key store to allow multiple concurrent license keys to be stored within a given Blue Prism environment and to enable the platform to take advantage of the maximum entitlement across all valid licenses at any one time.

This feature simplifies license management by enabling additional licenses to be purchased and deployed as required and provides the capability to deploy licenses in advance.

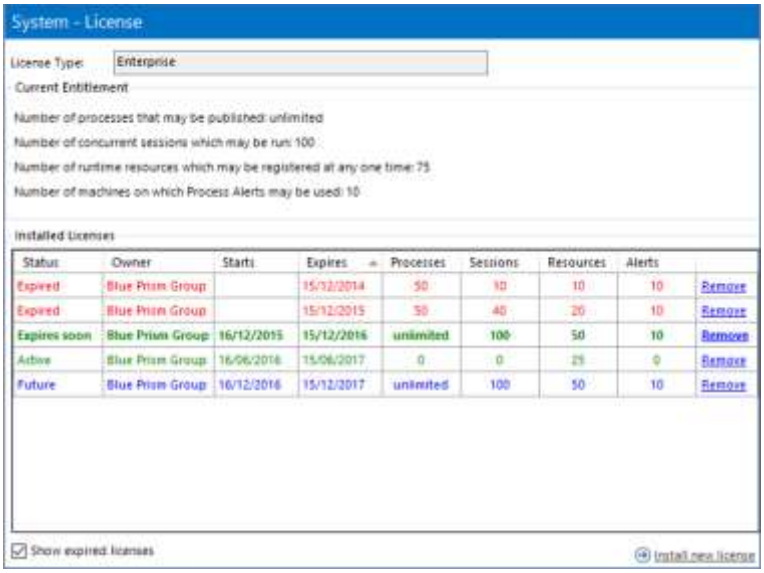


Figure 33: License key store

Login Agent

When installing Blue Prism v5.0.24 and above, the installers for the associated version of Login Agent are now placed within the Blue Prism install location to make it easier to locate a supported version of Login Agent.

When using Login Agent 5.0.23 and above, with Blue Prism 5.0.23 and above, Control Room provides a different icon when it is connected to a Login Agent Runtime Resource to allow users to quickly differentiate them from conventional Runtime Resources.

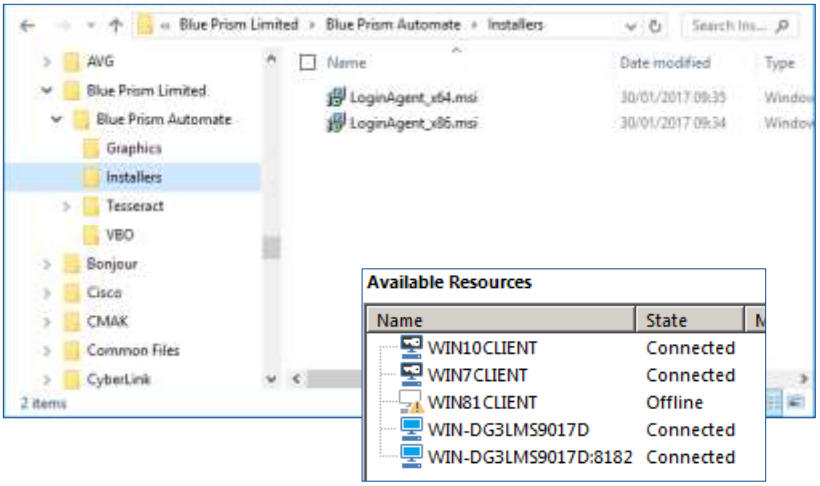


Figure 34: Login Agent Installers and new Control Room Icon

Release manager

Updates to Release Manager extend the items which can be ported between environments to include Groups, Dashboards and Tiles.

When including an item in the package, the facility to show dependencies and easily select the related items that should also be included. Additionally the tree will display any items that will be dynamically included when the release is created (shown in italics).

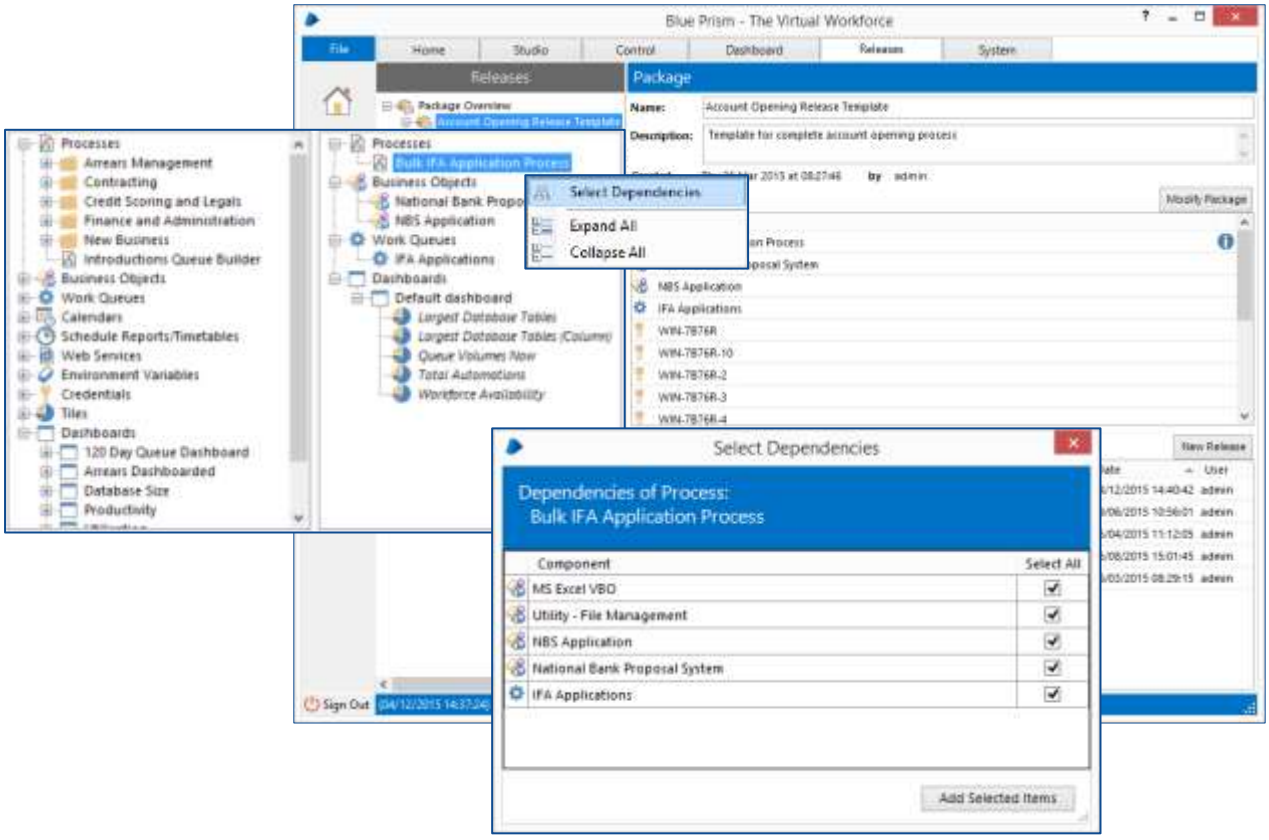


Figure 35: Release Manager

User Experience

Blue Prism v5 introduces a fresh user interface which reduces the on-boarding time for new users, whilst providing existing users with greater control and access to the features that they need most frequently.

Updated user interface

The user interface has been refreshed across the product, providing new features and easier access to common functionality. It incorporates a redesign of the menu structure to provide an intuitive user experience, new context menu options and a new Action button in the top right of each of the main panes.

Figure 36: Updated UI showing dashboard action menu

Introducing Studio

The Studio tab provides a single point of access for developers to manage Business Objects and Processes and features a multi-tier hierarchical grouping structure to aid the organization of developed components.

The development studio has also been refreshed with a sharpened canvas, re-positioned stage toolbox, updated shapes and increased options for zoom. Additionally drag-and-drop is provided from the toolbox to accelerate development.

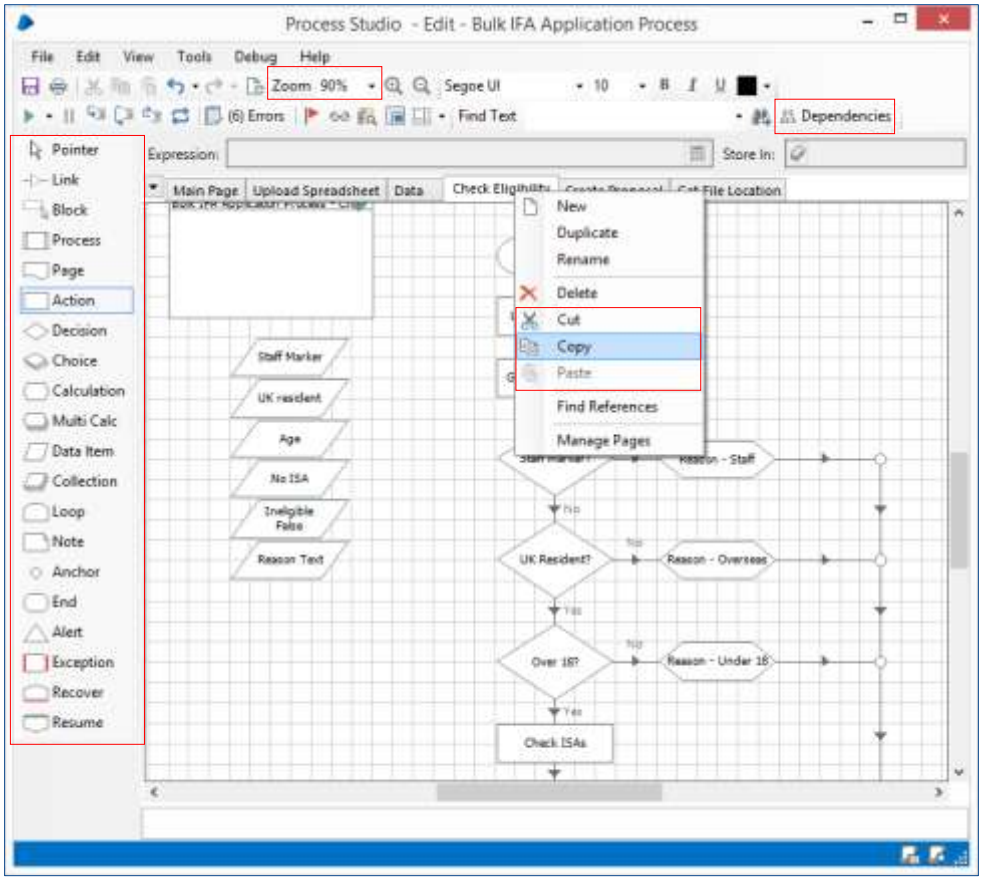


Figure 37: Editing a process with selection of features highlighted

Organization grouping

A hierarchical grouping mechanism provides flexibility for configuring how items are displayed within Blue Prism. Organizing Processes, Objects and Resources within a custom hierarchy helps developers, controllers and release managers alike. Ctrl + drag allows a single item to be present within multiple groups.

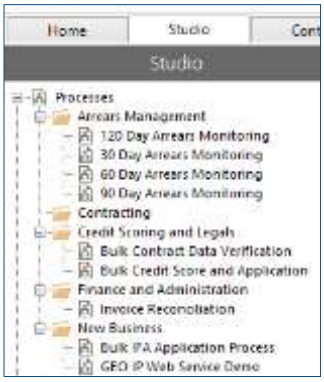


Figure 38: Process grouping

Environment themes

Designed for a multi-environment deployment model (Development, Test, Staging, and Production), users commonly move between different environments. Environment themes provide the ability for each to be configured differently to allow rapid identification when accessed.

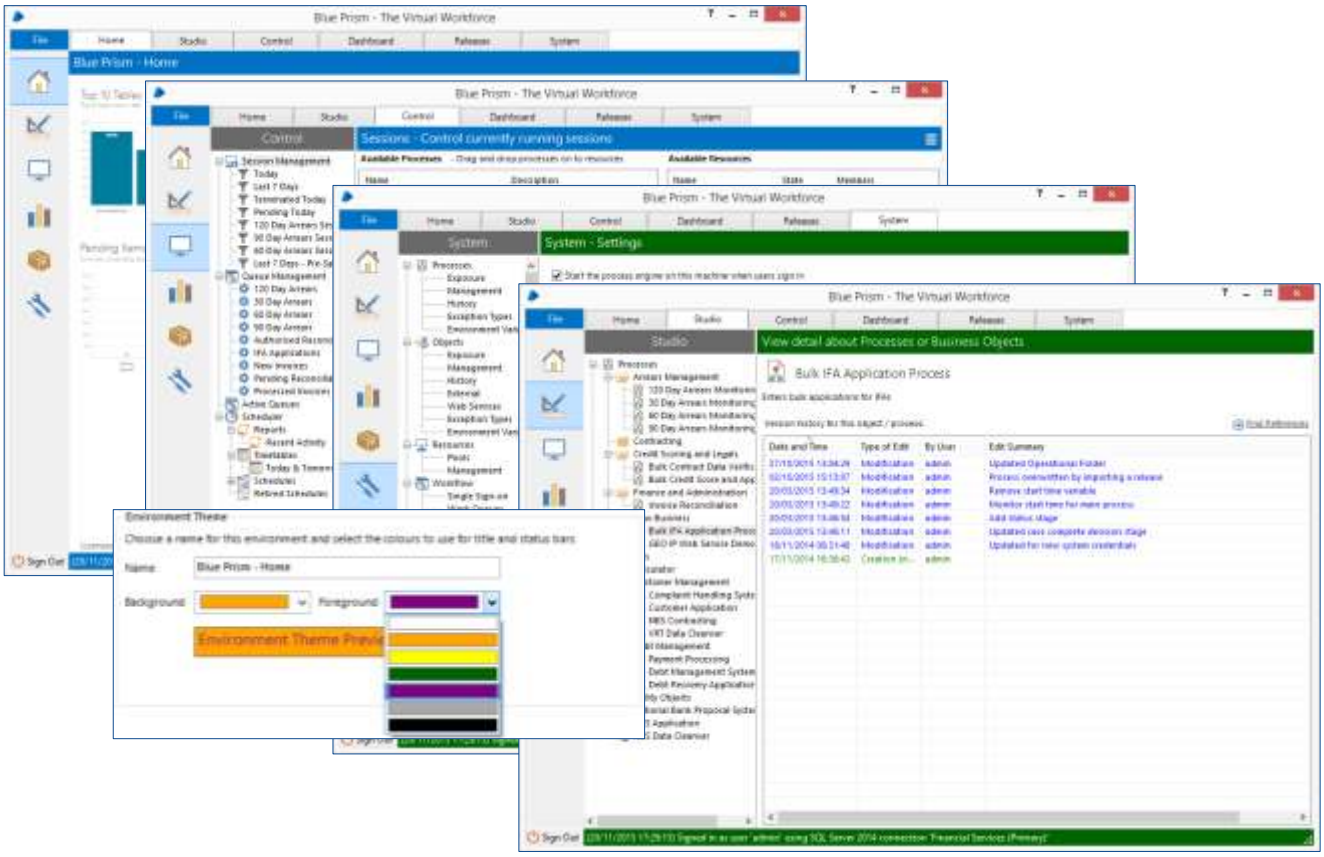


Figure 39: Illustration of two different environment themes

Latest Logon Information

From Blue Prism Version 5.0.23, the status bar at the bottom of the screen has been updated to provide clearer information about the type of connection of connection that is being used as well as the date and time that the user last logged onto the system.

From Blue Prism Version 5.0.29, for connections via the Blue Prism server, the status bar will also include the host name of the server that the client is connected to.

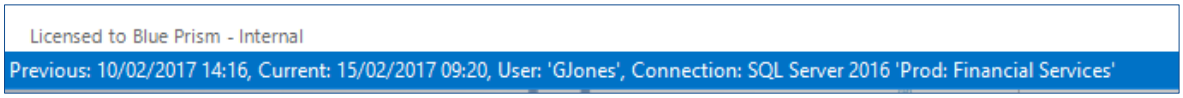


Figure 40: Updated Connection Status Bar

Enterprise platform

Blue Prism is deployed using a grid-based virtualized runtime and control methodology, where lightweight Blue Prism resources are interconnected within the data-center through a series of Blue Prism server components to a back end database.

Blue Prism v5.0 has been extended to provide an updated foundation that meets the needs of enterprise deployments.

Built on .NET 4

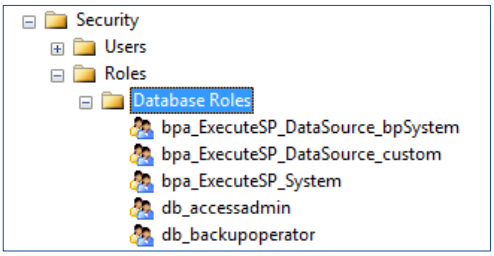
Provided as a native .NET Framework 4 application, support is now provided for advanced users wishing to reference the latest .NET dlls whilst maintaining the compatibility for installing the application on a wide range of modern and historical operating systems including Windows Server 2003 and Windows XP through to Windows Server 2012 and Windows 8.1.

SQL Azure

Initially available as an early access feature within v4.2, support is provided for deploying the Blue Prism database for pre-production environments on Microsoft SQL Azure.

SQL Roles

The SQL access rights for users of the Blue Prism platform are commonly restricted to provide just datareader and datawriter access. Blue Prism v5 leverages a small number of SQL features which are not natively available to these roles and therefore specific SQL roles are introduced to allow SQL DBAs to easily grant the additionally required permissions to the appropriate users.



SQL AlwaysOn Availability Groups

Initially available as an early access feature within v4.2, support for SQL AlwaysOn Availability Groups allows an Availability Group Listener to be selected as the provider hosting the Blue Prism database.

Extendable SQL Database Connection String

Connection Manager has been extended to allow advanced configurators to specify optional parameters that will be included in the connection string when a connection is established with the database.

These will semicolon-separated parameters e.g. Encrypt=true;TrustServerCertificate=true.