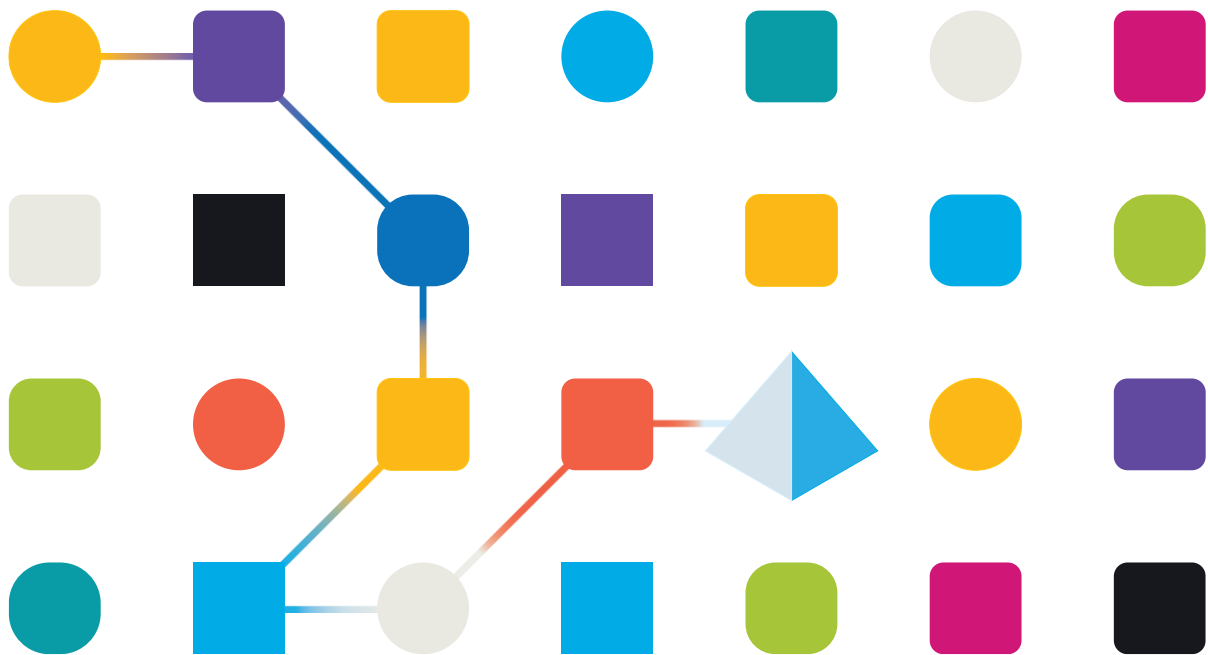


G-Cloud 15 Service Definition Document

SS&C Blue Prism Cloud



Trademarks and copyright

The information contained in this document is the proprietary information of Blue Prism Limited. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, without the written permission of Blue Prism Limited.

© **Blue Prism Limited, 2001 – 2026**

®Blue Prism is a registered trademark of Blue Prism Limited

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

Blue Prism Limited, 2 Cinnamon Park, Crab Lane, Warrington, WA2 0XP, United Kingdom
Registered in England: Reg. No. 4260035. Tel: +44 870 879 3000. Web: www.blueprism.com

Disclaimer

The contents of this document are for information and evaluation purposes only, and all conditions, warranties and/or representations, whether express or implied by statute, law or otherwise, are hereby excluded to the fullest extent permitted by law. Details of the Product and any associated warranty are outlined in the Supplier Terms and the applicable Documentation. Capitalised terms used in this paragraph have the meanings given in the Supplier Terms.



Blue Prism Cloud 2024

19 November 2025

Your Blue Prism Cloud 2024 platform

The Blue Prism Cloud 2024 is the full Platform-as-a-Service (PaaS) solution from SS&C | Blue Prism. This platform is provisioned from the cloud and delivers products from the full portfolio of SS&C | Blue Prism software pre-built and configured for your use, including the digital workers.

Blue Prism Cloud 2024 has been independently audited and is fully certified to SOC 2 (type II). SOC 2 (System and Organization Controls 2) is an internationally recognized compliance standard for service organizations, which specifies how organizations should control, manage, and protect customer data. The standard is based on security, availability, processing integrity, confidentiality, and privacy trust criteria. Further information can be found here: <https://soc2.co.uk>.

- i** BPC is available as a hosted service on both Microsoft Azure and Amazon Web Services (AWS), with availability depending on the version. All versions are supported on Microsoft Azure, while AWS hosting is exclusive to version [2022](#).

Available in Blue Prism Cloud 2024

SS&C Blue Prism® 7.4	The latest release of SS&C Blue Prism's RPA software solution unlocks new application modelling capabilities, introduces improvements to Enhanced Application Modeller and Smart Vision, and improves the usability of our automation design interfaces. Full release notes are available here. i The Blue Prism Enterprise version available to you is dependent on which release of Blue Prism Cloud 2023 you are using: • Blue Prism 7.4 is available with 2024.2 • Blue Prism 7.3 is available with 2024.1
SS&C Blue Prism® Hub 5.1.1	Hub provides secure access to management information and user administration. Hub has been created as a lightweight application populated by a series of plugins and features, including Hub Control Room, SS&C Blue Prism Interact, SS&C Blue Prism Decision, and SS&C Blue Prism Automation Lifecycle Management.

SS&C Blue Prism® Interact 5.1.1	Interact provides a collaboration interface that enables organizations to involve users in parts of a process that are otherwise automated. Interact is a customizable web portal that can be used within your organization and accessed via a browser from any computer on your corporate network. Interact acts as both an interface between human and digital workers for data input by the user, and a presentation layer for any information that needs to be displayed to a user. The Interact plugin within Hub enables automation developers to create web-based forms that will allow a user to interact with automations within the Interact web application.
SS&C Blue Prism® Automation Lifecycle Management 5.1.1	Automation Lifecycle Management enables business analysts to capture and document their organization's business process definitions along with the applicable applications and any business exceptions. ALM is a plugin within Hub. Wireframer is supplied within the ALM plugin. Wireframer enables the user to efficiently define business objects that can be used as part of an automation process.
SS&C Blue Prism Hub Control Room 5.1.1	Hub Control Room plugin provides Blue Prism users with the ability to view and manage Blue Prism activity for all their environments. Hub Control Room requires Blue Prism, the Blue Prism API, and Authentication Server. Hub Control Room is a plugin within Hub.
SS&C Blue Prism Decision 5.1.1	Decision provides Blue Prism users with the ability to train and deploy intelligent machine-learning decision-making models within their Digital Workforce, without requiring any data science expertise. Decision is a plugin within Hub, with a Model Service API.
SS&C Blue Prism® Director 1.0.3	Director enables automation developers to align

	business metrics to their varied workloads, driving priorities and service level agreements (SLAs) to determine the order in which individual queue items are executed.
OCR	OCR manages the extraction and translation of information from document images into machine usable data using optical character and image recognition approaches.

Other versions

To view this page for other versions of Blue Prism Cloud, and to access additional guidance for those versions, use the links below:

- [Blue Prism Cloud 2023](#)
- [Blue Prism Cloud 2022](#)
- [Blue Prism Cloud 2021](#)

Blue Prism Cloud 2023.1 to Blue Prism Cloud 2024.1 comparison overview

Blue Prism Cloud 2024.1 includes new product releases from the SS&C Blue Prism product portfolio, as well as the platform/configuration changes detailed in the Blue Prism Cloud 2022 and 2023 comparison overviews. Since Blue Prism Cloud 2021, the advancement of the SS&C Blue Prism products has introduced new and improved features, along with additional supported authentication configurations. An overview of these changes is provided in the sections below:

- [Blue Prism 7.3](#)
- [SS&C Blue Prism Hub 5.1.1](#)
- [SS&C Blue Prism Interact 5.1.1](#)
- [SS&C Blue Prism Automated Lifecycle Management 5.1.1](#)
- [SS&C Blue Prism Decision 5.1.1](#)
- [SS&C Blue Prism Director 1.0.3](#)



For a full list of features and updates, see the [release notes](#).

Blue Prism 7.3

The following changes are available in SS&C Blue Prism Enterprise 7.3, compared to version 7.1:

- **Native Citrix Virtual Apps and enhanced Citrix Virtual Desktops** automation capabilities offer

increased security and more flexibility when automating Citrix environments.

- **Improved flexibility, failover, and resilience of Active Directory integration** in Blue Prism Enterprise through more granular configuration options and support for multiple Domain Name Controllers (DNCs) in a multi-forest/multi-domain environment.
- **The Beta release of our Enhanced Application Modeller**, which offers modernized and improved building of accurate and robust application models.
- **Smart Vision spy mode**, our latest Surface Automation technology for Application Modeller. Leverage our new no-code editor and AI-powered human-like vision to model application user interfaces to accelerate automation development, reduce maintenance, and improve robustness. To utilize the new Smart Vision spy mode a Smart Vision enabled license is required. Smart Vision enabled licenses are expected to be available to customers from January 2024 onwards.

SS&C Blue Prism Hub 5.1.1

The following changes are available in SS&C Blue Prism Hub 5.1.1 compared to version 5.0:

- Introduction of .NET 8 (8.0.8) for the Hub framework and plugins to align with Microsoft ongoing support for .NET.
- Password security in Authentication Server has been increased for native users.
- Enhanced authentication with SAML and OIDC - Provides increased flexibility for user authentication by providing the ability to configure the Authentication Server for use with a SAML or OIDC provider.
- Support for multiple Domain Name Controllers (DNCs) - Improved flexibility, failover and resilience through support for multiple Domain Name Controllers (DNCs) in a multi-forest/multi-domain environments.
- Support for users without email addresses using AD Authentication – Users authenticated using AD Integration will not be required to have email addresses assigned to them to log in to Hub.
- Support for Interact API for AD authenticated users – Enables AD authenticated users to access all functionality offered by the Interact API endpoints.

SS&C Blue Prism Interact 5.1.1

The following changes are available in SS&C Blue Prism Interact 5.1.1 compared to version 5.0.

- Introduction of .NET 8 (8.0.8) to align with Microsoft ongoing support for .NET.
- Password security in Authentication Server has been increased for native users.
- Support for Interact Teams management allowing the ability to manage users and their role-based access according to teams segregated by function, geography, etc.

SS&C Blue Prism Automation Lifecycle Management 5.1.1

The following changes are available in SS&C Blue Prism Automation Lifecycle Management 5.1.1 compared to version 5.0:

- Introduction of .NET 8 (8.0.8) to align with Microsoft ongoing support for .NET.
- Password security in Authentication Server has been increased for native users.

SS&C Blue Prism Decision 5.1.1

The following changes are available in SS&C Blue Prism Decision 5.1.1 compared to version 5.0:

- Introduction of .NET 8 (8.0.8) to align with Microsoft ongoing support for .NET.

SS&C Blue Prism Director 1.0.3

The following changes are available in SS&C Blue Prism Director 1.0.3 compared to version 1.0:

- Introduction of .NET 8 (8.0.8) to align with Microsoft ongoing support for .NET.

Product roadmap

For more information on further planned features, see the product roadmap on the [Blue Prism portal](#).

Blue Prism Cloud on Azure

Blue Prism Cloud is provided as a Platform-as-a-Service (PaaS).

For more information, see:

- [Microsoft Azure Services overview](#)
- [DNS requirements for the Blue Prism Cloud platform](#)
- [Required access to customer platforms by Blue Prism Cloud Operations](#)
- [Blue Prism Cloud platform expansion](#)
- [Blue Prism Cloud Data Vault and Partitioner](#)
- [Blue Prism Cloud Data Vault access details](#)
- [Accessing your Blue Prism Cloud platform](#)
- [Connectivity and access](#)
- [Data Security](#)

Microsoft Azure Services overview

Blue Prism utilizes Microsoft Azure Services for providing the underlying infrastructure for Blue Prism® Cloud 2024. For the responsibility matrix for the platform, see [Responsibility assignment](#).

Microsoft Azure Services is an ever-expanding set of cloud services that enable Blue Prism Cloud to deliver Robotic Process Automation (RPA) services to our client base on a global scale, being able to provide a localized data center infrastructure.

Blue Prism Cloud is delivered as a Platform-as-a-Service (PaaS) from an Azure Data Center and is designed to automate and digitize the execution of knowledge work performed by human workers.

The service is provided using a number of Virtual Machines (VMs). These are configured to support the

different Blue Prism Cloud components and are configured into different subnets to provide security segregation zones. Network Security Groups (NSGs) are established to ensure only acceptable traffic flows between the subnets and the Virtual Private Network (VPN) connection to the client site. More details of the underlying infrastructure can be found in the [Connectivity and Access datasheet](#).

When Blue Prism deploy a new service to a client, a new subscription from Microsoft is used to provide the high-level segregation. Subscription segregation ensures that no clients can see each others environments.

The subscription is normally established in the data center which is closest to the client office. For geographical location information on data centers where Blue Prism can deploy to, including the locations of US Government approved regions, see [Microsoft Azure – Global infrastructure](#).

The minimum configuration of a client subscription is nine virtual machines, and also utilizes Azure Kubernetes Service (AKS). The configuration consists of:

- 1 x Management Server
- 2 x Blue Prism Application Server
- 5 x Production Digital Workers
- 1 x Development Digital Worker
- AKS cluster, supporting SS&C | Blue Prism Hub, SS&C | Blue Prism Interact, and SS&C | Blue Prism Director
- New client subscriptions also include an additional virtual machine hosting the OCR service. For existing customers, this service is included on the Blue Prism Application Server.

The databases to support Blue Prism Cloud are not configured on a VM but are delivered using Microsoft Azure DB services. This ensures that the databases are in continual operational status irrespective of a component level failure as the underlying technology supports replication. Disaster recovery services ensure that a point in time recovery can be performed to allow a controlled rollback to anywhere within the last seven days. Because of the level of resiliency built into the platform Blue Prism Cloud offer as standard a 99.9% service level agreement for availability.

Blue Prism also utilize Microsoft Cognitive Services to deliver their IADA.ai service.

The VMs are built with the following configuration:

	Digital Worker VMs	All other VMs
Virtual CPU cores	2	4
RAM	8 GB	16 GB
Storage	128 GB	128 GB
Operating system	Microsoft Windows 11 Enterprise, version 24H2, 64-bit	Microsoft Windows Server 2022

Blue Prism monitor the VMs and ensure that they are running efficiently, where issues are identified they are investigated and action undertaken to rectify.

DNS requirements for the Blue Prism Cloud platform

Typically, your customer platform uses your DNS servers to resolve host names and URLs to the IP addresses of the servers and services which host Blue Prism Enterprise, Blue Prism Interact and Blue Prism Hub. The IP addresses for the servers are local and/or private IPs within the platform Virtual Network address space and are provided at platform handover.

It is expected that you will provide the IP addresses of your DNS servers that will be used at the point of platform setup. If you do not provide custom DNS servers, Blue Prism Cloud will use the Azure default DNS servers.

If your DNS servers are used, you will need to create custom DNS A records on those DNS servers to resolve DNS for a blueprismcloud.com DNS zone. This allows you to use Blue Prism 7.4 (or later), Hub and Interact 5.1.1 (or later), as these products make use of a Private DNS Zone.

i You must use DNS records and not host files. The use of host files is not supported by the Blue Prism Cloud platform.

Guidance for customers utilizing their DNS servers

If you opt to domain join all of your virtual machines (VMs), all of the VMs should be joined to your domain prior to creating the BluePrismCloud DNS Zone and A-records.

If the platform is using your DNS service and you have not joined any of the VMs to your domain and you have Dynamic DNS registration disabled, you must follow one of the following two options:

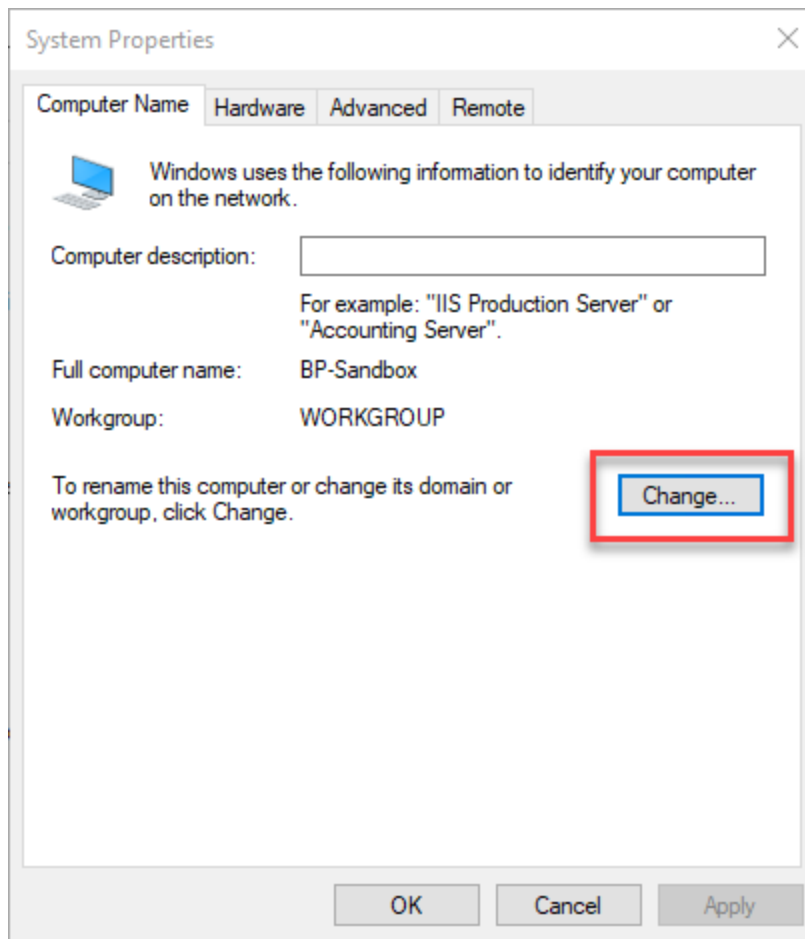
- Enable Dynamic DNS registration – Details for this can be found in [Microsoft's documentation](#).

Or alternatively;

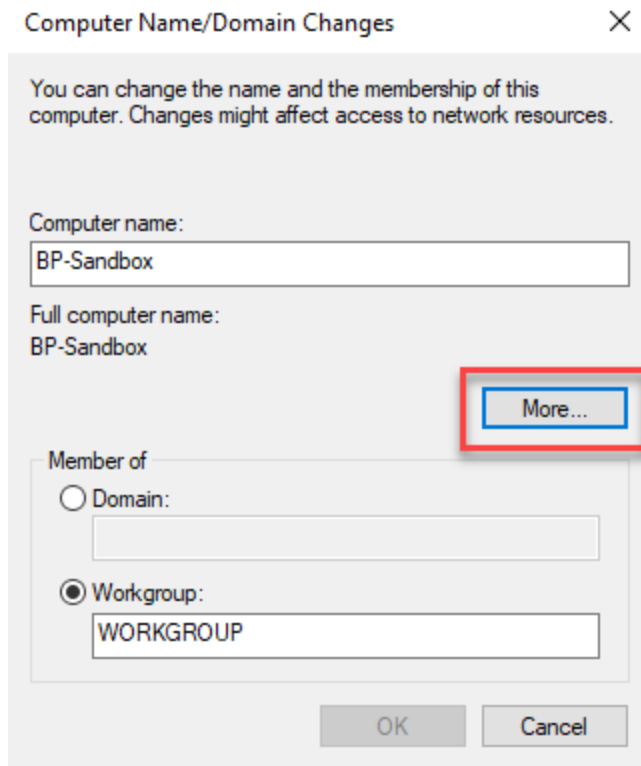
- Input the primary DNS suffix in the VMs that are not domain joined – See [Adjusting the primary DNS suffix on the machine](#) below.

Adjusting the primary DNS suffix on the machine

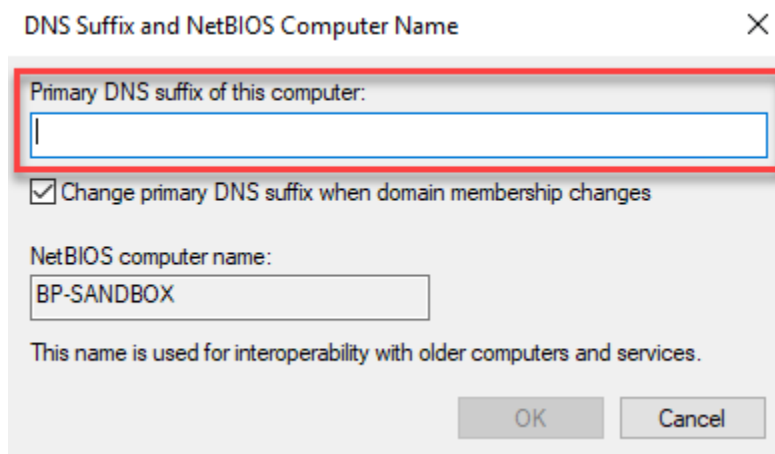
1. On the VM that you want to join to the domain, open the System Properties dialog and click **Change....**



2. On the Computer Name/Domain Changes dialog, click **More....**



3. In **Primary DNS suffix of this computer**, enter your DNS suffix and click **OK**.



The machine will prompt for a reboot.

4. Reboot the VM when possible.

Custom DNS zone and A records

You will need to create the custom DNS zone. How you create a DNS zone will depend on the DNS server being used. For more information, see the following guidance:

- [Microsoft documentation with IPAM](#).
- [BIND official documentation](#).

You will need to create the DNS A records in accordance with the DNS records file provided to you by Blue Prism Cloud Operations team. When you receive the file:

- Ensure all specified DNS records are present in your environment. Where a DNS record does not exist, create the DNS record and associated Private IP.
- Where a DNS record does exist, validate the Private IP. If there are differences between IPs listed in the file and those configured in your environment, do not update the record, please add details to your existing support ticket.

Blue Prism Cloud self-service reboot

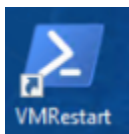
By utilizing Microsoft Azure Functions and Managed Identities, the self-service reboot tool (VMRestart) provides access via the Management Server to the back-end Azure functionality that enables you to directly restart specific virtual machines.

i Azure Functions are serverless solutions provided by Microsoft, which enable a comprehensive set of event-driven [triggers and bindings](#) to be used that connect Blue Prism Cloud functions to other services, without the need to develop additional code.

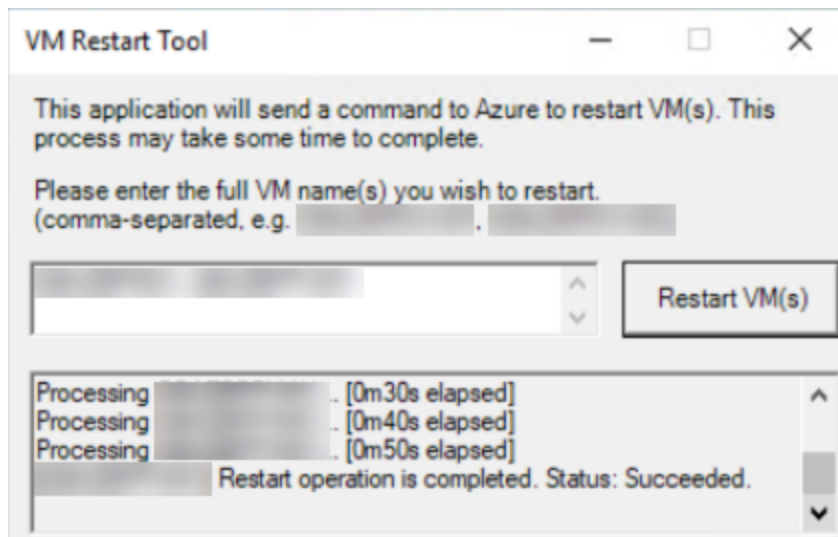
i The self-service reboot tool not only facilitates a restart of the VMs that aren't performing as expected, but also possesses the capability to initiate the startup of a virtual machine that has been accidentally shut down.

VMRestart

1. Log onto your Blue Prism Cloud Management Server.
2. Launch VMRestart using the shortcut on the server desktop.



3. On the VM Restart Tool screen, enter the name of the virtual machine you want to restart. You can enter more than one.



4. Click **Restart VM(s)**.
5. Follow the remaining onscreen instructions and enter any required information.

In the background, the function triggers the restart on the specified virtual machines. If the restart does not execute successfully, an attempt will be made to start the VM from a “non-running” state.

Considerations

- Keep in mind, having to regularly reboot your VMs or a specific VM is usually indicative of some underlying issue. Most Blue Prism Cloud platforms already undergo a standard weekly reboot. If you find yourself rebooting a particular VM often, please raise a support case so that the support team can investigate for any underlying causes.
- Deployment issues can occur if your network/security teams have implemented restrictions allowing our “standard and required” remote scripting, deployment capabilities. You will know if the deployment was blocked, as you will not find VMRestart in the public folder of the Management Server (MS1).

Security and Access

VMRestart utilizes a Managed Identity account for the Management Server to authenticate and has explicit permissions on a specified set of resources in your dedicated Azure Subscription. VMRestart is also explicitly limited to the restart command on the virtual machines.

Accessing your Blue Prism Cloud platform

This guide explains how to access your Blue Prism Cloud Digital Workforce platform. The platform is likely to be accessed by a range of different user profiles, from IT Support through to automation developers and end users.

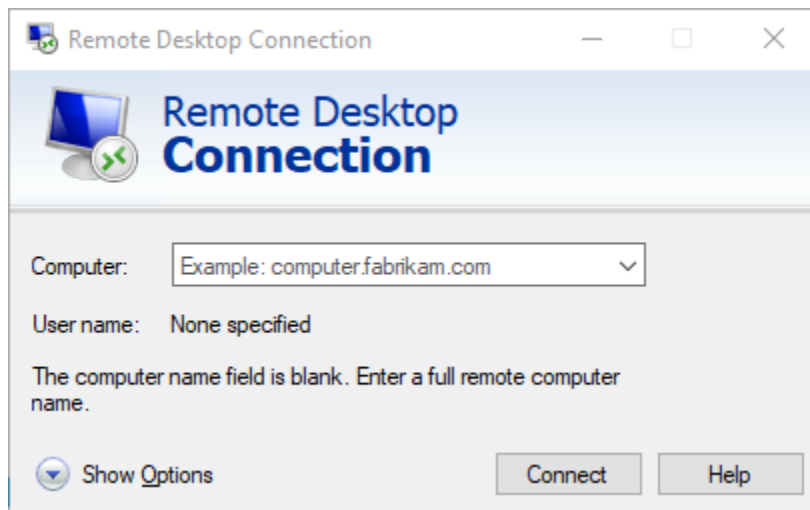
Prerequisites

To be able to access the Blue Prism Cloud platform and the associated components, you will need:

- Established network connection (for example, a VPN connection) between your organization's network and the Blue Prism Cloud platform.
- An Inbound customer Remote Desktop Protocol (RDP) (3389) rule on the Blue Prism Cloud network.
- Your organization must allow outbound RDP traffic from your network to the Blue Prism Cloud platform.

Running Remote Desktop

To access your Blue Prism Cloud Workforce you will need to use an application called Remote Desktop Connection.



To access Remote Desktop Connection:

1. In the Windows Taskbar Search field, type *remote desktop connection* or *mstsc*.
2. Select **Remote Desktop Connection** from the search results.

Remote Desktop Connection opens.

Logging into the Management Server

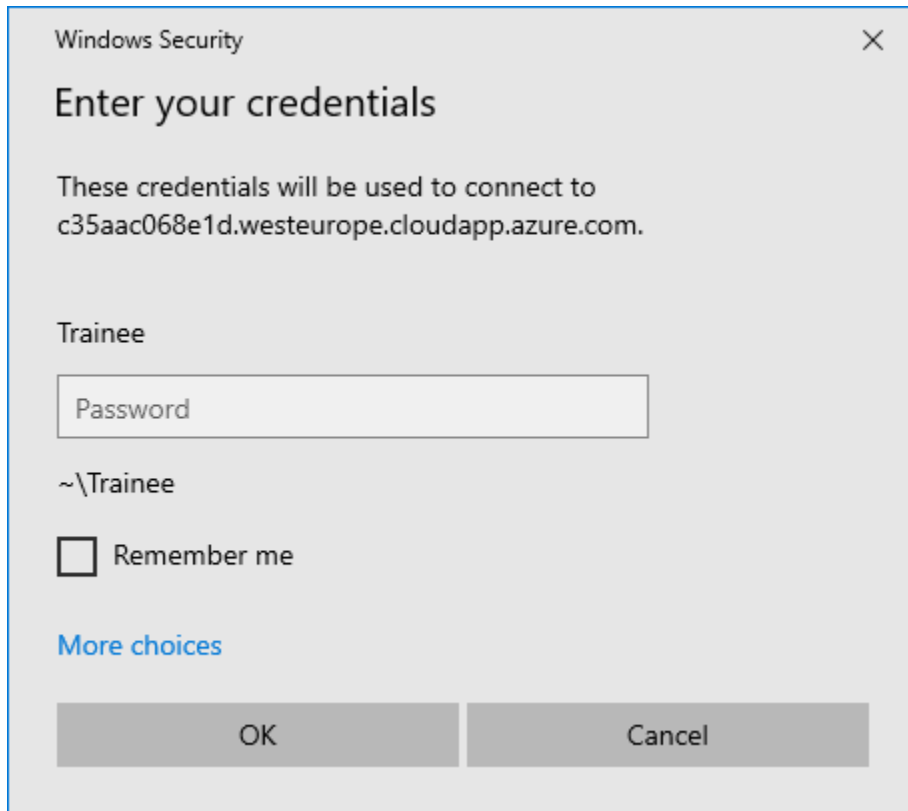
Assuming you have established secure connectivity from your network to your Blue Prism Cloud platform, you will be able to remote desktop to the Management Server on your Blue Prism Cloud platform using the private IP address of the Management Server.

The Management Server is the central access point to the Blue Prism Cloud platform using the Remote Desktop Protocol (RDP). By default, there is a terminal license applied on the server which allows up to 10 concurrent users to access the Blue Prism Cloud platform at any time.

1. In Remote Desktop Connection, type in the internal/private IP address of your Management Server in the Computer field.

- i** The server details such as Private IP, Machine Name, Windows Username and Windows Password should already be with the requested end user upon your Blue Prism Cloud Platform Handover. If you do not have the server details of the Management Server, please visit the [customer support center](#) to request for these to be shared.

The Windows Security dialog displays.



2. Enter your provided credentials: username and password.

Management Server Desktop

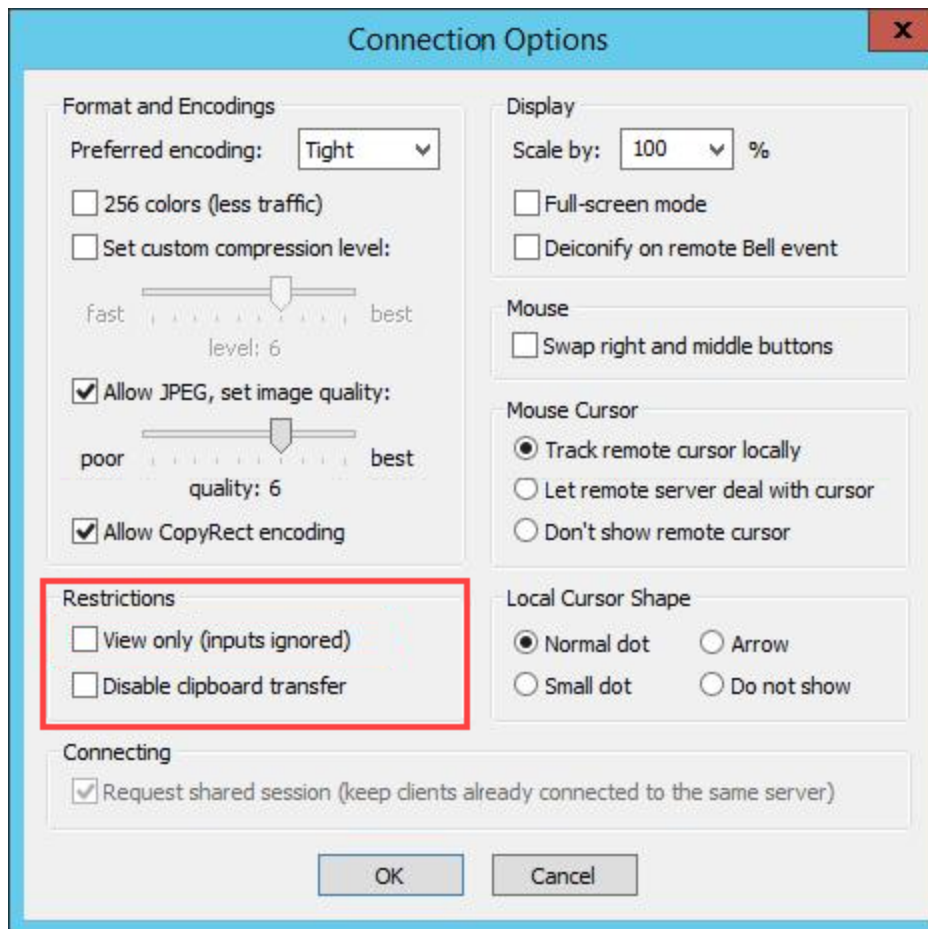
Once logged in you will be able to see the Management Server desktop. It is important to note that no automations are run on the Management Server – the purpose of this system is the management of the digital workforce and is seen as a staging and control area for the automations.

From this desktop, you can do two things:

- View and control the Digital Workers
- Restart an automation.

Accessing the Digital Workers

To access the Digital Workers for operator or developer activities, or IT support access, the method below is recommended.



2. Apply the required restrictions:
 - **View only** – If you make sessions view only, any mouse and keyboard inputs are ignored.
 - **Disable clipboard transfer** – This option should be selected to prevent Digital Workers from attaching to your local clipboard, or other Digital Workers clipboards, causing confusion in the automation and leading to a potential system exception.
3. Click **OK** to save your settings.

Shutting down/closing open application

VNC should be treated like any other application, therefore when a system exception has occurred, Blue Prism recommends that you close all applications that are currently open on the Digital Worker's desktop using the correct methods to log out and close applications. After closing all automation utilized applications, you should close the VNC window.

Accessing your Blue Prism Cloud applications

There are two environments available in your Blue Prism Cloud platform: Development and Production.

Logging into Blue Prism

From the Management Server desktop, you can open the Blue Prism application.

1. Double-click the Blue Prism desktop icon.



Blue Prism launches and the Sign in to Blue Prism dialog displays.

The method you use to log into Blue Prism depends on the authentication method configured by your organization. The Sign in to Blue Prism dialog will only display the information required for the configured authentication method.

2. Select the environment you want to use from the **Connection** drop-down list.
3. To log in, use the appropriate method available to you in the Sign in to Blue Prism dialog:
 - Enter your Blue Prism credentials and click **Sign in using Blue Prism credentials**. These will be provided to you by your Blue Prism system administrator.
 - Click **Sign in using Active Directory**.
 - Click **Sign in using Authentication Server**. You are redirected to the Authentication Server login page. Enter your credentials and click **Log in**.
 - Click **Sign in using Authentication Server**. You are redirected to the Authentication Server login page. Click **Log in using Active Directory**.

For more information, see [Authentication in Blue Prism](#).

Logging into Blue Prism Hub or Blue Prism Interact

From the Management Server desktop, you can open Blue Prism Hub or Blue Prism Interact by either using the Authentication Server desktop shortcut or by entering the URL into an internet browser. For details of supported browsers, see the [Hub FAQs](#).

1. Double-click the Blue Prism Authentication Server desktop icon for the environment that you require. Alternatively, enter the appropriate URL into an internet browser:
 - Development environment: <https://as-dev.blueprismcloud.com/>
 - Production environment: <https://as-prod.blueprismcloud.com/>

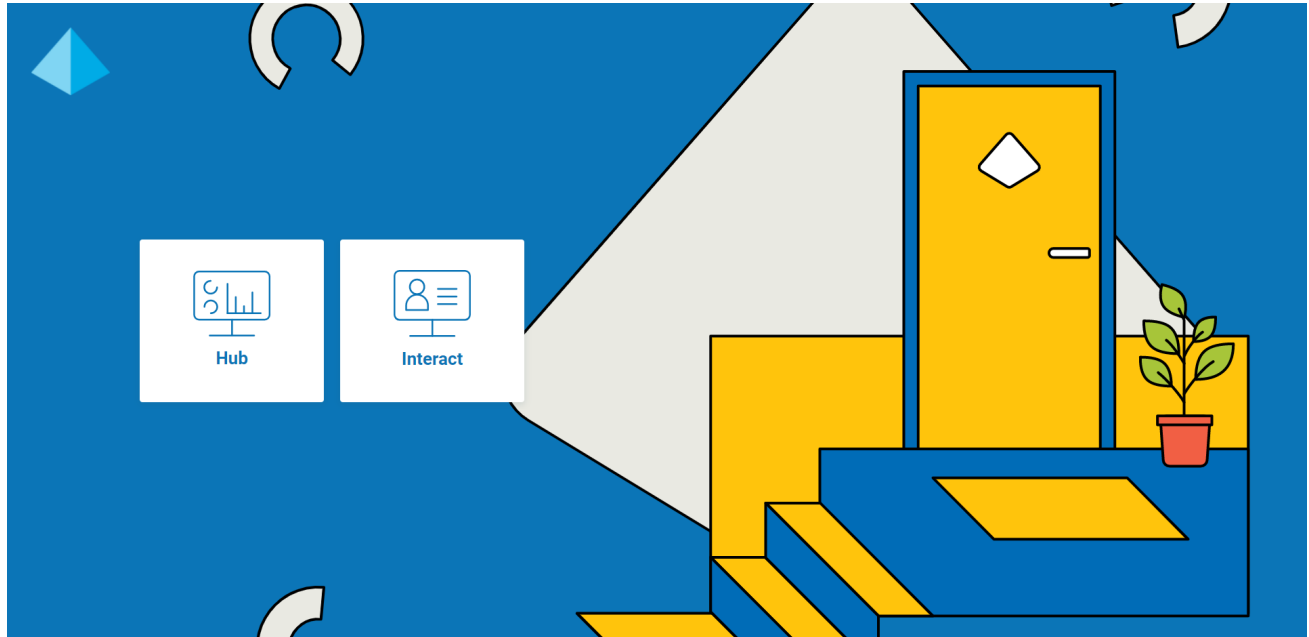
The Authentication Server login page displays.

2. Log in using one of the following methods:
 - Enter your credentials and click **Log in**.

- Click **Log in using Active Directory**. This uses single sign-on so you do not need to enter any credentials.

i The **Log in using Active Directory** option only displays if Active Directory authentication has been enabled in your environment.

The application selection screen displays. You will see a tile for Hub and a tile for Interact, as shown below:



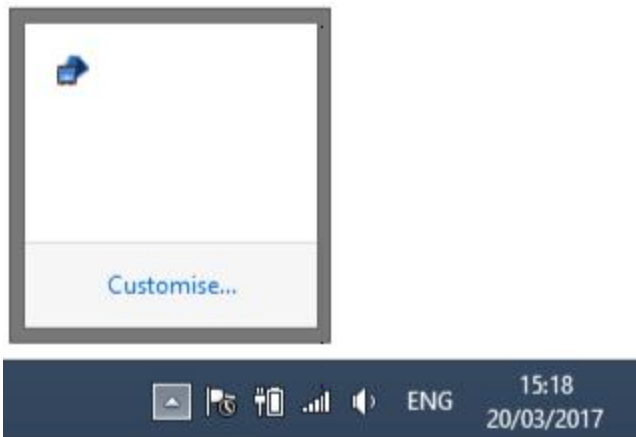
3. Click the appropriate tile to launch the application.

Blue Prism Cloud Listener

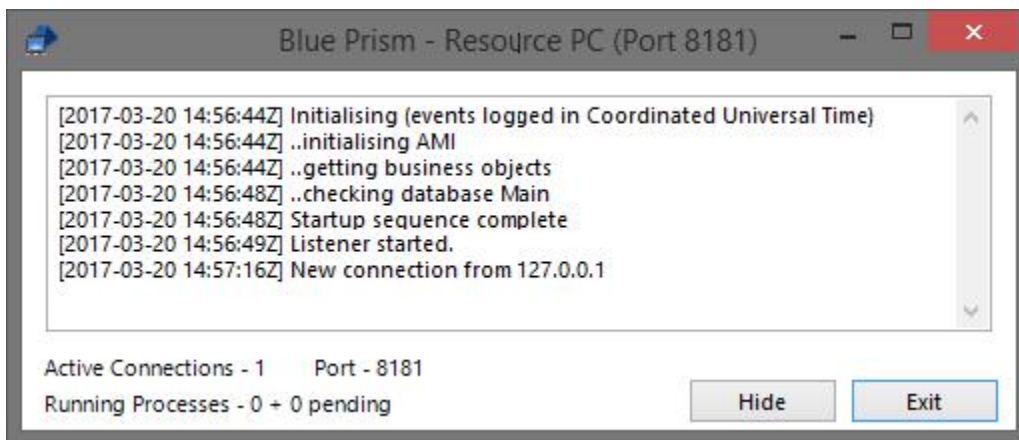
For the automation ecosystem to work, a listener is required to be running on the Digital Worker systems on an exposed port. This creates a symbolic link with the Management Server allowing the Management Server to use the machine as a Digital Worker as part of its digital workforce.

If the listener is not running on a Digital Worker, then the Management Server cannot communicate with the resource (Digital Worker) to initiate or control any automations.

To check if the listener is running on a Digital Worker, you can simply look at the icons in the taskbar on the Digital Worker's desktop to find the below icon – you can expand this list by clicking on the arrow.



If this icon is present, it would suggest that the listener is running on this Digital Worker. However, you should check that there are no obvious errors by right clicking on this icon and selecting **Show** from the context menu.



Here you can see no obvious error codes and the number of Active Connections is greater than zero. You can also check to see if a Digital Worker is ready to accept automations from the Blue Prism Control Room.

Available Resources

Name	State	Members	Last Error
 LAP0001	Connected		

In the above image, we can see that our Digital Worker is connected, with no errors and has a highlighted blue computer symbol next to the name of the Digital Worker.

How to start the listener on a Digital Worker

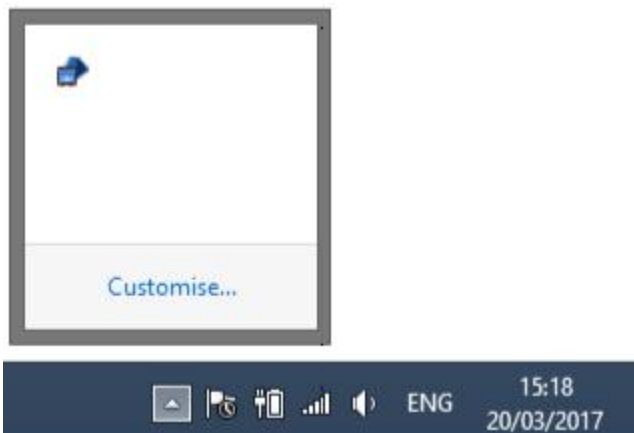
From the Digital Worker's desktop, select either **Start Development Worker Listener** or **Start Production Worker Listener**.

-  Start Development Worker Listener
-  Start Production Worker Listener

The respective worker listener batch file should be in the start-up folder of the local virtual.worker account or dedicated Active Directory (AD) worker account where the automated process will be running on.

How to stop the listener on a Digital Worker

To stop the listener, right click on the icon from the below panel and select **Exit**.



Signing out of the Blue Prism Cloud platform

When you are logged onto the Management Server, you will need to log out of the machine after you have completed your work, rather than just disconnecting. If you simply disconnect, your Windows account will still consume CPU and memory resources.

To sign out:

1. Select the Windows button from the taskbar.
2. Click on your name from the top right of the screen.
3. Select **Sign Out**.

Forced sign out of a user by an administrator

If you have administration privileges for the Digital Worker, you have the capability to sign a user out and terminate processes in a user's session. You should be aware that any unsaved work in a user's session will be lost if you forcibly sign them out. Blue Prism Cloud recommend that you try to resolve the disconnected session by contacting the user directly before forcibly signing them out.

To force the sign out of a user's session:

1. Open Task Manager.
2. Select the **Users** tab.
3. Right-click on a user.
4. Click **Sign off**.

To kill a process under a user's session:

1. Open Task Manager.
2. Select the **Users** tab.
3. Expand the required user's node.
4. Right-click on a process.
5. Select **End task**.

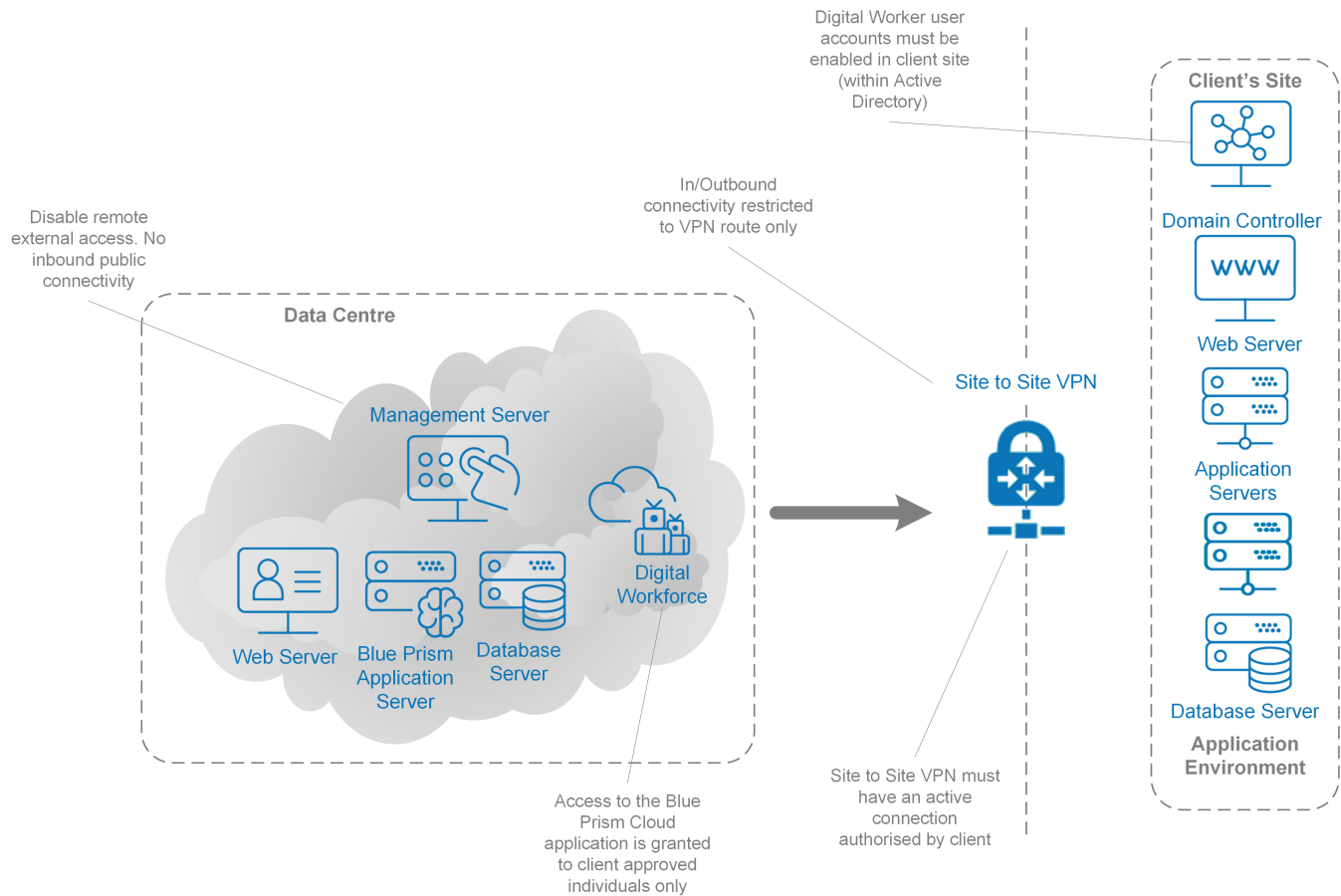
Connectivity and access

This information outlines the connectivity of Blue Prism® Cloud to a customer estate. Detailed are the access requirements of the digital workers to execute the defined processes against the line of business applications as well as for operators and designers to access the platform, it serves as a reference document for any business IT or architectural teams involved in the deployment.

Blue Prism® Cloud is a Platform-as-a-Service (PaaS) solution deployed into [Microsoft Azure Services \(Azure\)](#). The digital workers emulate a user executing knowledge-based work and connect to the customer application(s) through a private network connection, such as Site-to-Site VPN. This enables the digital workforce to exist as a logical extension to the network. Several safeguards are in place to protect the platform from unauthorized access. This document details the controls around this connectivity to prevent

unauthorized access whilst enabling legitimate users' management control to the platform for operational purposes.

The diagram below illustrates the overall Data Center connectivity to the customer site identifying key safeguards.



Connecting a digital workforce to your organization

This page details information for the customer or partner side responsibilities in the deployment of Blue Prism® Cloud.

Site-to-site network connection

A site-to-site network connection forms a secure, persistent connection between the customer subscribed digital workforce resources and the customer environment. The site-to-site network connection ensures that a production platform is accessible from the customer or partner end of the connection only. When configuring a site-to-site network connection, Blue Prism Cloud will configure the connection to a customer specified address range that is compatible with the customer address space. Other connectivity options are available – you can discuss these with Blue Prism Cloud Operations during your initial platform configuration.

Currently supported site-to-site connection providers are:

Azure Blue Prism Cloud platform:

- Site-to-Site VPN
- ExpressRoute – This requires your organization to purchase this from Azure
- VNET Peering – This requires your organization to purchase this from Azure

Domain joining and group policies

Prerequisites

- Network connectivity from the Blue Prism Azure platform to your network must have been established. This will be either a Site-to-Site VPN connection, VNet peering, or ExpressRoute connection.
- Your DNS servers must be added to the custom list of DNS servers in the Azure Virtual Network. The DNS servers on all virtual machines (VMs) must then be updated by restarting the machines or by running a `ipconfig /renew` command on all machines which does not require a restart.
- There should be NSG rules allowing traffic to your DNS and domain controllers. These rules are normally created automatically when deploying the platform using the Azure pipeline. In the case where the customer DNS servers and domain controllers are different, you may need to confirm this with the customer and add any additional servers not listed on the Platform Configuration Form manually to the existing outbound NSG rules and check that routes to these servers exist by looking at the effective routes of a VM network interface.
- There should be a network security group (NSG) rule that allows you to access the management server using RDP. This is normally created manually as part of the manual steps of the platform deployment. If you have not provided a complete list of address ranges that they may access the platform from and may have issue accessing the management server, you should follow the same steps as above and confirm the any additional IP addresses you may need to add to the NSG and check for existing routes.
- You must ensure you allow traffic from the Blue Prism Azure platform to your DNS servers and domain controllers. You should also allow RDP traffic from your network to the management server.
- You must have received and can access the credentials spreadsheet containing the credentials and server IP addresses that you need to use to access the Azure platform.

Dos and don'ts

- Do not manually make configuration changes on any of the Azure Virtual Machine Network Interface Cards (NICs)
- Do not disable or change any of the local Windows admin accounts or exempt msadmin, ioadmin, vwadmin and wsadmin from your policy
- Configure appropriate firewall rules
- Configure OU and security groups for the BPC platform
- Configure mandatory group policies
- Do not disable or block PowerShell

Default local policies for Blue Prism Cloud virtual machines

Blue Prism Cloud VMs are configured with certain local security and computer policy settings by default.

These adjustments ensure optimal performance of the platform and your automations.

Please see our configured local policies below.

Local security policies

These policies are configured in **Security Settings > Local Policies > Security Options**:

Policy	Option
Interactive logon: Do not require CTRL+ALT+DEL	Enabled
Interactive Logon: Message title for users attempting to log on	Empty
Interactive Logon: Message text for users attempting to log on	Empty

Local group policy

These policies are configured in **Computer Configuration > Administrative Templates > Control Panel > Personalization**:

Policy	Option
Local Group Policy Editor: Do not display the lock screen	Enabled

Recommended Active Directory organizational units and security groups

In addition to the local group policies applied to our virtual workforce as standard, there are Active Directory group policy settings required within your Active Directory to assure optimal performance of the Blue Prism Cloud platform.

It is strongly recommended that your Blue Prism Cloud digital workforce is placed in its own Organizational Unit (OU) within your Active Directory and any applicable policies are applied to that OU. For ease of configuration you may also wish to add all BPC users to an appropriate security group.

The recommendations are made to ensure BPC workforce are not impacted by any conflicting Group Policy Objects (GPOs) pre-existing within your domain. GPO conflicts can result in diminished functionality of the platform, in addition to placing the product in an unsupported state.

The following sections specify the GPOs and their relevant directories which need to be configured.

Required customer active directory GPO settings

Setting	Directory	Option
Do not display Server Manager automatically at logon	Computer Configuration > Administrative Templates > System > Server Manager	Enable
Do not display the lock screen	Computer Configuration > Administrative Templates > Control Panel > Personalization	Enable
Interactive logon: Do not require CTRL + ALT + DEL	Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options	Enable
Shut down the system	Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignment  This will allow a user to restart the VM. In the policy properties, select 'Add User or Group' and enter the name of the user or group you wish to have this ability	Add user to
Do not allow clipboard redirection	Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Device and Resource Redirection	Enable
All Removable Storage Classes: Deny All Access	User Configuration > Policies > Administrative Templates > System > Removable Storage Access	Enable
Turn off auto-restart notifications for update installations	Computer Configuration > Administrative Templates > Windows Components > Windows Update	Enable
Machine inactivity limit	Interactive Logon: Machine inactivity limit	Not defined

Setting	Directory	Option
Message text for users attempting to log on	Interactive Logon: Message text for users attempting to log on	Not defined
Message title for users attempting to log on	Message title for users attempting to log on	Not defined

Domain join requirements

In order to ensure your domain services can sufficiently communicate with your Blue Prism Cloud platform, we require your DNS Server IP('s) and your Active Directory Domain Services Server IP('s) before the domain join activity can commence.

The IPs should typically be provided on your completed platform configuration form. With these we can:

- Add the DNS Server address into your platform's Virtual Network configuration
- Create the relevant NSGs to allow appropriate traffic flow between the BPC platform and the client's Domain.
- Customer creates an inbound firewall rule to match traffic highlighted below.

Below is an excerpt of the standard outbound NSG rules we create to allow the flow of traffic; these rules may not apply to all platforms and as such are subject to change.

Priority	1005
Name	Allow-Outbound-Domain-TCP
Source	All ASGs (Application Security Groups) - This covers all the VMs in the BPC platform
Destination	Client Domain Server IPs
Ports	53,88,135,139,389,445,464,636,3268,3269,49152- 65535
Protocol	TCP

Priority	1010
Name	Allow-Outbound-Domain-UDP
Source	All ASGs
Destination	Client Domain Server IPs
Ports	53,123,389
Protocol	UDP

Domain join ports and protocols

 Should your domain services require a set of atypical ports opened for traffic flow, please advise us.

Below are the default ports we configure and their corresponding use:

Port	Use
TCP/UDP 53	DNS
TCP 88	Kerberos Key Distribution Center
UDP 123	Windows Time
TCP 135	Remote Procedure Call
TCP 139	NetBIOS Session Service
TCP/UDP 389	LDAP, DC Locator, Net Logon
TCP 445	SMB, Net Logon
TCP 464	Kerberos Password V5
TCP 636	LDAPS
TCP 3268	Global Catalog over LDAP
TCP 3269	Global Catalog over LDAPS
TCP 49152-65535	Randomly allocated high TCP ports

Customer required connections

BPC require the addition of WireServer to customer required connections. The below information is provided to ensure customers are not blocking traffic to the Azure wire server on specific ports/protocol.

- The VM agent requires outbound communication over ports 80/TCP and 32526/TCP with WireServer (168.63.129.16)
- Azure does not restrict traffic via the NSGs. If this is being blocked its likely to be caused by the local windows firewall on the VM or customers security tooling.

Interact authentication

By default, Interact is configured with named authentication. This means that for every user that accesses the Interact application, the user will need to be manually created and managed going forward. If required, environments can be linked to an existing LDAP Active Directory configuration for user authentication, however, users will need to be manually assigned to roles in Hub to enable access to Interact.

Interact is deployed with a self-signed certificate as standard. If the customer/partner plans to make the environment publicly available, the customer/partner should supply a certificate from a certified authority.

End user and operator access

Customer or Partner Operator access to Blue Prism Cloud is completed through either a Remote Desktop (RDP) connection or browser-based access, depending on the task to be performed.

Application installation

A digital workforce in the execution of an automated process will interact with the customer or third-party application user interfaces. For these activities to be fulfilled the digital workforce requires sufficient privileges to the applications in scope. Any applications accessed through a thick client will need to be installed onto the digital worker operating systems. The installation process is a customer led activity, and should be communicated to Blue Prism Cloud Operations who can support the customer with the process. Any firewall or network configuration required to make the thick client accessible to the internal network will need to be performed in conjunction with Blue Prism Cloud Operations. Details of all ports and protocols required will need to be supplied in advance of any configuration work, to ensure that changes are kept to a minimum.

Customer privileges and managing security

Address space

During the initial configuration of the site-to-site network connectivity (for example, Site-to-Site VPN), the customer or partner specifies the allowed customer IP addresses that the digital workforce should communicate with. Any further changes or expansion to the digital workforce allowed list of IPs is solely in the control of the customer or partner as this change must be completed within the customer estate.

Virtual network access

All digital workforce components are built upon a customer (or customer business unit) specific Virtual Private Network (VPN). This approach along with the use of dedicated customer subscriptions ensures that the network is untenanted, and all traffic secured.

Operating system access

As part of the setup, the digital workforce can be aligned to a customer or partner domain. This action is one of multiple security functions that ensures the components including the operating systems are accessible by authorized customer/partner individuals. Access by Blue Prism Cloud staff must be maintained in accordance with [these standards](#).

Patch management and anti-virus

By default, your Blue Prism Cloud platform will have software patches (such as Windows Updates) deployed every month. The platform will also have Malware protection deployed and configured. The patching schedule can be altered by submitting a [support request](#).

Credential management

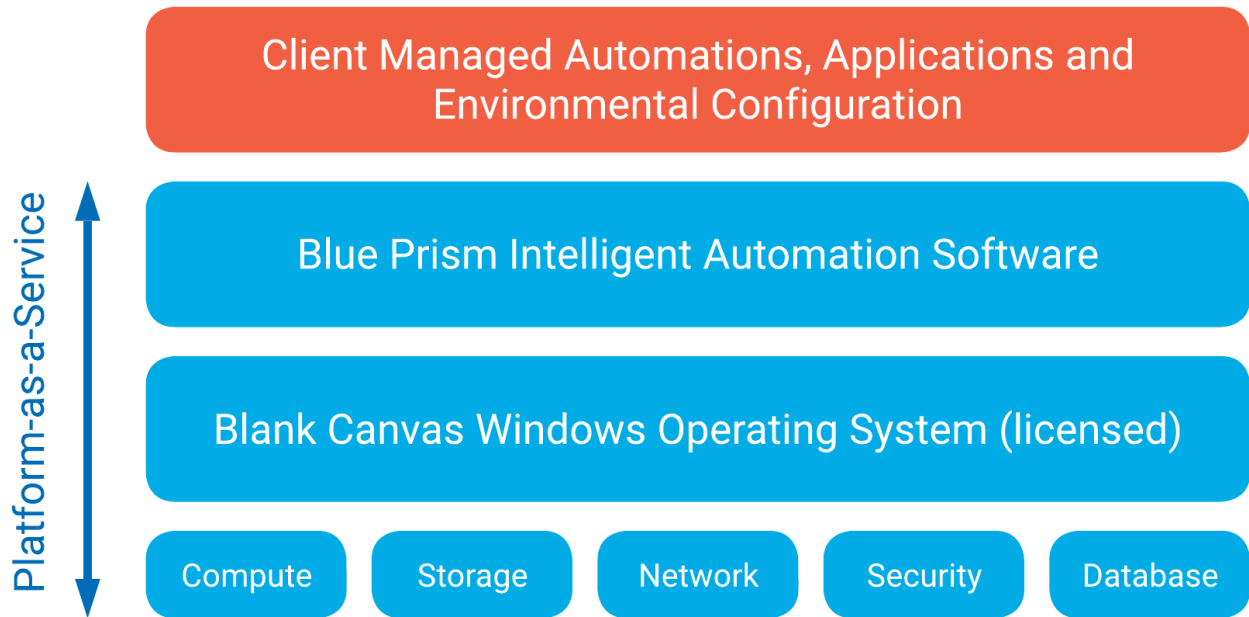
In the delivery of an automated process, the digital workforce will require privileges to complete set tasks. The approach used to authenticate will be dependent on the application. For a web application that uses forms-based authentication, a digital worker will issue a username and password. For applications which use Single Sign On, the digital worker Active Directory user account will be used. The privileges required to deliver the required automated process will be scoped as part of a project deliverable. For any privileges which are controlled through Active Directory, Blue Prism offers an encrypted credentials store, or the ability for a digital worker to access an existing customer credentials store as part of an automated process.

Post deployment access

Platform support

In the delivery of the subscription service, Blue Prism Cloud support the critical components of the digital workforce whilst ensuring only the customer or partner maintains full administrative access to the operating system and application above. This demarcation of responsibility has been denoted in the image below. Where the orange is the customer's responsibility and the blue is Blue Prism Cloud's responsibility.

Blue Prism Cloud Roles and Responsibilities



During the configuration of the environment, the customer must provide details of all white listed IP's, Ports and Protocols are required to enable the network controls to be established. The customer does not have direct access to the deployed PaaS platform within the cloud service provider and so configuration of the virtual environment is performed at initial configuration by Blue Prism Cloud and thereafter subject to change control.

Change management

Blue Prism maintain an ITIL aligned Change Management process. Any activities requiring a change to be made to the platform, should be requested through [Blue Prism Cloud Support](#). Any subsequent changes to the configuration of the virtual infrastructure and the networking (including network controls), is performed in conjunction with the Blue Prism Change Management process and therefore will be planned and approved prior to any commencement of work. It is expected that customers and partners will test and verify that the latest release of code is compatible with their own automations and environment in their development environment before promoting to production.

Blue Prism Cloud OCR

There are several applications within the Blue Prism Cloud Optical Character Recognition (OCR) solution. These are as follows and accessible from the following platforms.

- **Administration and Monitoring console** – a web client accessible from the Application Server;
- **FlexiLayout Studio** – a thick client accessible from the Application Server;
- **Project Setup Station** – a thick client accessible from the Application Server;

- **Verification Station** – a web client accessible from the Application Server and digital workers.

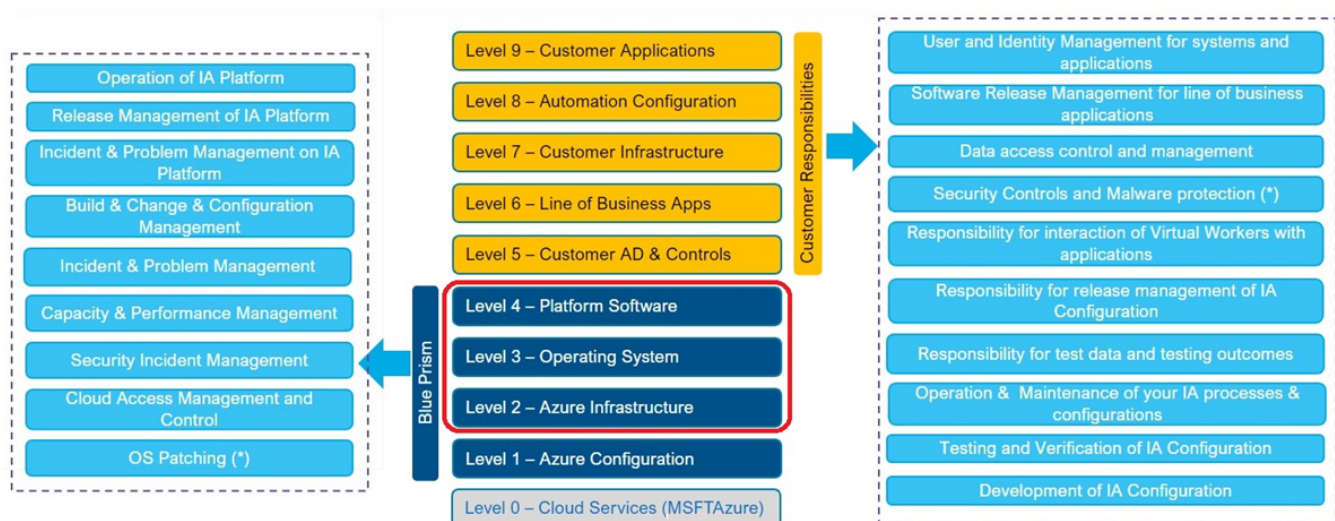
Blue Prism Interact

A standard component of Blue Prism Cloud is the Interact web portal. Interact provides a collaboration interface for end users to provide information to the Digital Workforce as part of an automated process. As standard the Interact portal will be available on a private address, with the customer being able to apply this to an existing domain or sub domain. If the Interact portal is to be joined to a new or existing customer domain, it should be specified during platform setup. Two Interact instances will be active: one for Production the other for Development purposes.

Responsibility assignment

There is a shared responsibility model for the operation of the Intelligent Automation (IA) platform. Blue Prism are responsible for the engineering, operation, and management of the platform.

The image below illustrates the responsibilities for the Blue Prism Cloud platform:



The following table details the responsibility assignment matrix covering the areas of responsibility for both Blue Prism Cloud  and the customer .

Operation	Management Server	Web Server (Supporting Hub and Interact)	Blue Prism Application Server	Database	Production Digital Workers	Development Digital Worker
Level 4 – Cloud Platform Software (Blue Prism products)						

Operation	Management Server	Web Server (Supporting Hub and Interact)	Blue Prism Application Server	Database	Production Digital Workers	Development Digital Worker
Customer UI login credentials				N/A		
Functional application testing				N/A		
Functional readiness testing	Collaboration  	Collaboration  	Collaboration  	N/A	Collaboration  	Collaboration  
Maintain Blue Prism software				N/A		
Log collection				N/A		
Service start-up				N/A		
Service monitoring				N/A		
Service recovery	Collaboration  	Collaboration  	Collaboration  	N/A	Collaboration  	Collaboration  
Level 3 – Operating System						
Operating system login	Collaboration	Collaboration	Collaboration	N/A	Collaboration	Collaboration

Operation	Management Server	Web Server (Supporting Hub and Interact)	Blue Prism Application Server	Database	Production Digital Workers	Development Digital Worker
	 	 	 		 	 
Operating system patching	 or 	 or 	 or 	N/A	 or 	 or 
Operating system version management	Collaboration  	Collaboration  	Collaboration  	N/A	Collaboration  	Collaboration  
Log collection				N/A		
Service start-up				N/A		
Service monitoring				N/A		
Service recovery				N/A		
Level 2 – Azure Infrastructure						
Azure login						
Log collection						

Operation	Management Server	Web Server (Supporting Hub and Interact)	Blue Prism Application Server	Database	Production Digital Workers	Development Digital Worker
Backup and recovery						
Service monitoring						



Notes:

- For digital workers on Levels 3 and 4, if any investigation is needed from the customer application perspective, Blue Prism Cloud will liaise with the customer, as this is a shared responsibility.
- For Level 5 and above, it is the responsibility of the customer to operate, maintain, and manage the infrastructure.

Operational definitions

Azure login	As a Blue Prism Cloud service: Log into Azure service for operation and maintenance.
Backup and recovery	As a Blue Prism Cloud service: Perform backup and recovery of platform state.
Customer UI login credentials	Product user interface (UI) login with customer's credentials for automation operation and maintenance.
Functional application testing	Functional application testing of platform software with customer's operational requirements and data through product UI login or operating system (OS) login.
Functional readiness testing	Functional readiness testing of platform configuration, software, and security configuration.

Log collection	As a Blue Prism Cloud service: Collect any necessary logs for investigation – this refers to database logs, which can only be obtained by BPC. Customer collects Operating System and any associated application logs as per Blue Prism Enterprise/Blue Prism Global Customer Support standards.
Maintain software	As a Blue Prism Cloud service: Maintain deployed software.
Operating system login	Guest operating system login for operation and maintenance. The customer is responsible for customer credentials, and Blue Prism Cloud is responsible for Blue Prism Cloud credentials. BPC requires local administrative accounts for each machine that cannot be deprecated by customer policies.
Operating system patching	As a Blue Prism Cloud service: Perform OS patching. Alternatively, the customer can elect to use their own tooling to maintain entire platform. Customers can elect to have BPC manage patching; If BPC is elected, we will patch all BPC VM's with security and critical patches only; Customers will be responsible for handling ancillary Microsoft patches offered regardless of election; Alternatively customers can manage patching entirely on their own.
Operating system version management	Major OS version changes: Requires approval from BPC; there are times where "if approved" customers can run an in place upgrade. BPC will enforce upgrades if customers allow a version to go end-of-life. Minor OS version changes: Customers doing their own patching can apply minor OS version upgrades at will; Customers who have elected to have BPC manage patching will only receive minor OS version upgrades as previous versions become end-of-life.

Service monitoring	As a Blue Prism Cloud service: Monitor running status and performance of all necessary services (including alert detection).
Service recovery	As a Blue Prism Cloud service: Recover any necessary service from an unavailable state (including standard/ad hoc operation for any incidents or alerts).
Service start-up	As a Blue Prism Cloud service: Confirm all necessary services are up and running (including after maintenance and upgrade).

Whitelisting requirements

Any tools that may alter, inspect, redirect, or block this traffic – such as firewalls, proxies, or other network restrictions – must be configured to allow these communications to pass through unaltered and without interference:

Service	Port/Protocol	Endpoint/URL	Endpoint/ URL Description
Atera Agent	8883/443 (HTTPS)/TCP	pubsub.atera.com pubsub.pubnub.com app.atera.com agenthb.atera.com packagesstore.blob.core.windows.net ps.pndsn.com agent-api.atera.com cacerts.thawte.com agentreportingstore.blob.core.windows.net atera-agent-heartbeat.servicebus.wi	The following list of servers need to be permitted for OUTBOUND traffic over TCP port 8883/443 (HTTPS) in a Proxy and/or Firewall, should you utilize these services.

Service	Port/Protocol	Endpoint/URL	Endpoint/ URL Description
		ndows.net ps.atera.com atera.pubnubapi.com appcdn.atera.com atera-agent-heartbeat- cus.servicebus.windows. net ticketingitemsstoreeu.bl ob.core.windows.net download.visualstudio.m icrosoft.com a32dl55qcodech- ats.iot.eu- west-1.amazonaws.com agentspoliciesprod.blob. core.windows.net	
Azure Monitor	HTTPS	*.ods.opinsights.azure.c om *.oms.opinsights.azure.c om *.azure-automation.net *.handler.control.monito r.azure.com management.azure.com *.monitoring.azure.com *.ingest.monitor.azure.c om	Used by azure monitoring agent.
Azure Storage	HTTPS	*.blob.core.windows.net	URL Suffix used by Azure storage accounts.

Service	Port/Protocol	Endpoint/URL	Endpoint/ URL Description
Microsoft Defender for Endpoint	HTTPS	winatp-gw- uks.microsoft.com winatp-gw- ukw.microsoft.com unitedkingdom.x.cp.wd. microsoft.com	Microsoft Defender for Endpoint Command and Control.
Windows Update	HTTP/HTTPS	emdl.ws.microsoft.com *.dl.delivery.mp.microso ft.com *.windowsupdate.com *.delivery.mp.microsoft. com *.update.microsoft.com *.prod.do.dsp.mp.micros oft.com tsfe.trafficshaping.dsp.m p.microsoft.com	OS Patch Downloads/ Windows and Microsoft Update Connection Points.
Azure Wireserver	HTTP/HTTPS (TCP 80,443,32526)	168.63.129.16	An exception should be added for URLs containing this Azure IP address if using a proxy.
Azure Function Apps	HTTP/HTTPS	*.azurewebsites.net	Backend to Azure Function Apps we may deploy for customer Self-Serve activities: Any tools that may alter, inspect, redirect, or block this traffic - such as firewalls, proxies, or other network restrictions - must be

Service	Port/Protocol	Endpoint/URL	Endpoint/ URL Description
			configured to allow these communications to pass through unaltered and without interference.
Powershell Gallery	HTTPS	powershellgallery.azureedge.net psg-prod-centralus.azureedge.net psg-prod-eastus.azureedge.net onegetcdn.azureedge.net *.vo.msecnd.net *.powershellgallery.com go.microsoft.com nuget.org api.nuget.org	Powershell and Nuget Gallery.

Required access to customer platforms by Blue Prism Cloud Operations

Introduction

Blue Prism® Cloud deployments are designed to maintain a standard level of access which allows the Blue Prism Cloud Platform Operations team to fulfill the SLA obligations and Support Terms as set forth in our agreements. These access requirements must not be prohibited or blocked.



Refer to the following documents on the Blue Prism Portal:

- [Blue Prism Cloud Service Level Agreement.](#)



- [Blue Prism Cloud Support Terms](#) – see section 12.

Required Access Controls

Blue Prism Cloud deploys the following standard access controls to maintain an optimal platform and to meet the obligations set forth in our SLA agreement and Support Terms. Customers must not remove or block:

- Local administrative accounts on all virtual machines.
 - Customers can, if they wish reset the password in accordance to their own policy. Blue Prism would then change the password when the account is required for use by Blue Prism Cloud, after which the account would fall back into the customers policy.
 - This account is used to log on to the Virtual Machines to execute support requests and management activities including but not limited to; troubleshooting and verification, system and Blue Prism applications log collection, upgrade activities.
- Ability to execute remote scripting and command line interface based instructions via the cloud services provider or invoke commands leveraging the cloud services platform's guest agent, and the local system account utilizing unsigned scripts and an unrestricted execution policy, on all Blue Prism Cloud virtual machines.
 - Remote scripting and command line interface based instructions are used in actions and activities such as but not limited to; upgrades, platform changes, platform deployment and expansions, platform configuration data collection.
- Ability to connect to Blue Prism Cloud virtual machines through Remote Desktop.
 - Blue Prism Cloud engineers must utilize our secure access process including management approvals prior to being able to create a remote desktop connection to the management server.
 - RDP from outside of the platform is used as an initial step to access the Management Server only. To access other virtual machines within the platform, Blue Prism Cloud engineers would utilize RDP from the management server (within the platform).
 - In some cases, internal customer policy may require enforcement of customer network controls. In these instances, amendments must be made on the customer network to allow necessary traffic for Blue Prism Cloud security and monitoring toolsets. This includes internet traffic to allow agents and monitoring tools the ability to communicate.

Removal of Access Controls

Blocking the Blue Prism Cloud required access controls, security and/or monitoring toolsets places the SLA agreement and Support Terms at risk. Both SLA and Support Terms may (at Blue Prism's discretion) be downgraded to “commercially reasonable effort” based on these access limitations.

Examples of changes to access controls that impact support SLA and Terms include:

- Customer side Security and/or GPO policies that block remote scripting and commands
- Customer removal of Blue Prism Cloud local admin accounts
- Restriction of internet traffic that prevents agent reporting, or command execution
- Customer access control tooling and policy that impacts Blue Prism Cloud RDP access to platform and access to ALL virtual machines.

Blue Prism Cloud Operations User Access

Any access to customer platforms by Blue Prism team members is controlled and governed. Only Blue Prism Cloud Operations and Support team members are able to request access.

As a precursor to accessing customer platforms, and as part of the mandatory access route for Blue Prism Cloud Operations and Support teams, a secure workstation recording tool is used to monitor and record system access and activity on workstations. The tool records all activities performed by Blue Prism Cloud Operations and Support teams on customer platforms. Recordings are stored for 30 days – after which, they are automatically deleted.

Initially, Blue Prism Cloud Operations and Support team members will use Active Directory accounts and multi-factor authentication to log into the Cloud Management Portal and the users with the appropriate permissions will be able to request access to the secure workstation. That access is approved by management with restrictions to level of access. The remote desktop access to the workstation itself is also time-bound. The Blue Prism Cloud Operations and Support team user then requests access to the customer platform from the secure workstation, again access is approved by management based upon a stated requirement, and only the appropriate access level for that requirement is granted. The access is again time-bound and is only allowed from a single location (the secure workstation).

Security standards for network rules

Blue Prism Cloud operates a pinhole security model. As standard, Blue Prism Cloud allows traffic into, and out from, the platform only via specifically designated ports or protocols, running to or from specific sources or destinations, such as specific IP addresses or ranges. Blue Prism Cloud does not allow an 'any' designation for source, destination, port, or protocol. For certain exceptions, any ports or any protocols can be allowed in an outbound rule, this is explained further in [Allowed rules with exception sign-off](#).

Allowed rules

The following table shows a set of examples for outbound and inbound rule(s) which Blue Prism Cloud can accept as standard.

Application name	Firewall rule name	Source (IP address)	Destination (Destination IP address)	Protocol	Port	Description	Rule acceptance comment
File Share Outboard	Allow-Outbound-FileShare	Digital Workers (Application Security Group -	172.29.51.0 /24	TCP	445	Digital Workers to access the File Share	Rule allowed

Application name	Firewall rule name	Source (IP address)	Destination (Destination IP address)	Protocol	Port	Description	Rule acceptance comment
		VWs)					
FACS Outbound	Allow-Outbound-FACS	Digital Workers (Application Security Group - VWs)	172.29.51.0/24	TCP	26715	Digital Workers to access FACS Workstation	Rule allowed
HTTPS Inbound	Allow-Inbound-HTTP+S	172.29.50.0/25	10.10.51.0/27	TCP	80, 443	Customer Internal Subnet range to access HTTP+S	Rule allowed
File Share Inbound	Allow-Inbound-FileShare	172.23.50.0/26	10.28.40.0/25	TCP	445	Customer Internal Subnet range to access file shares	Rule allowed
RDP Inbound	Allow-Inbound-RDP	172.10.50.0/28	Management Server (Application Security Group - MS)	TCP	3389	Customer Internal Subnet range for RDP Access to Management Server	Rule allowed

Allowed rules with exception sign-off

In certain exceptional scenarios, Blue Prism Cloud can also allow an outbound rule from the digital worker(s) to your organization's network where any port or any protocol is specified.

 Your organization will need to define the IP address or range at your end of network connection.

Your organization accepts the risk and responsibility for the outbound traffic from the platform that it is routed via your internal network, and controlled by your network device. This risk is against Blue Prism Cloud's best practice, as it can allow undefined parameters within the connection, thereby increasing the vulnerability from a security perspective.

To use this exception, the following process needs to be followed:

1. You must raise a request for an exception through Blue Prism Cloud Support.
2. You will be provided with a risk statement to accept and sign off.
3. You must return the accepted risk statement to Blue Prism Cloud Support.

For reference, please see the statement below:

Blue Prism Cloud networking best practices leverage the pinhole methodology. Your request to create *[description of configuration]* goes against our best practices. Allowing unfettered access from the Blue Prism Cloud platform into your on-premises network is not advisable. You, the customer, are responsible for maintaining your on-premise firewall to prevent and mitigate inappropriate access that may result from these changes.

Please reply with confirmation of your request. By confirming, you acknowledge your request to *[description of configuration]* is not consistent with Blue Prism's recommended best practice when configuring and using the Blue Prism Cloud Services. Furthermore, *[Customer]* assumes all risks associated with this configuration and releases Blue Prism from any and all liability which may arise from this configuration.

The following table shows an example rule:

Application name	Firewall rule name	Source (IP address)	Destination (Destination IP address)	Protocol	Port	Description	Rule acceptance comment
HTTP+S Outbound	Allow-Outbound-HTTP+S	Digital Workers (Application Security Group - VWs)	172.29.51.0 /24	Any protocol	Any port	Digital Workers to access HTTP+S	This rule will require your organization's acceptance of risk

Not allowed rules

As part of the pinhole security model, Blue Prism Cloud does not allow, as standard, rule(s) that contain an 'any' designation for ports, protocols, source, or destination. The following table shows a set of examples

for outbound and inbound rule(s) which Blue Prism Cloud does not accept as standard:

Application name	Firewall rule name	Source (IP address)	Destination (Destination IP address)	Protocol	Port	Description	Rule acceptance comment
FACS	Allow-Outbound-FACS	Digital Workers (Application Security Group - VWs)	Any destination	TCP	26715	Digital Workers to access FACS Workstation	This rule is not allowed as the destination is not defined, such as an IP address or range
HTTP+S	Allow-Outbound-HTTP+S	Digital Workers (Application Security Group - VWs)	172.29.51.0 /24	TCP	Any port	Digital Workers to access HTTP+S	This rule is not allowed as the port is not defined, such as a specific port or range of ports
HTTPS	Allow-Inbound-HTTP+S	172.29.50.0 /25	Any destination	Any protocol	Any port	Customer Internal Subnet range to access HTTP+S	This rule is not allowed as the destination, protocol and port are not defined
File Share Inbound	Allow-Inbound-FileShare	Any source	10.28.40.0/25	TCP	445	Customer Internal Subnet	This rule is not allowed as

Application name	Firewall rule name	Source (IP address)	Destination (Destination IP address)	Protocol	Port	Description	Rule acceptance comment
						range to access file shares	the source is not defined with an IP address or range
RDP Inbound	Allow-Inbound-RDP	172.10.50.0 /28	Management Server (Application Security Group - MS)	TCP	Any port	Customer Internal Subnet range for RDP Access to Management Server	This rule is not allowed as the port is not defined, such as a specific port or range of ports

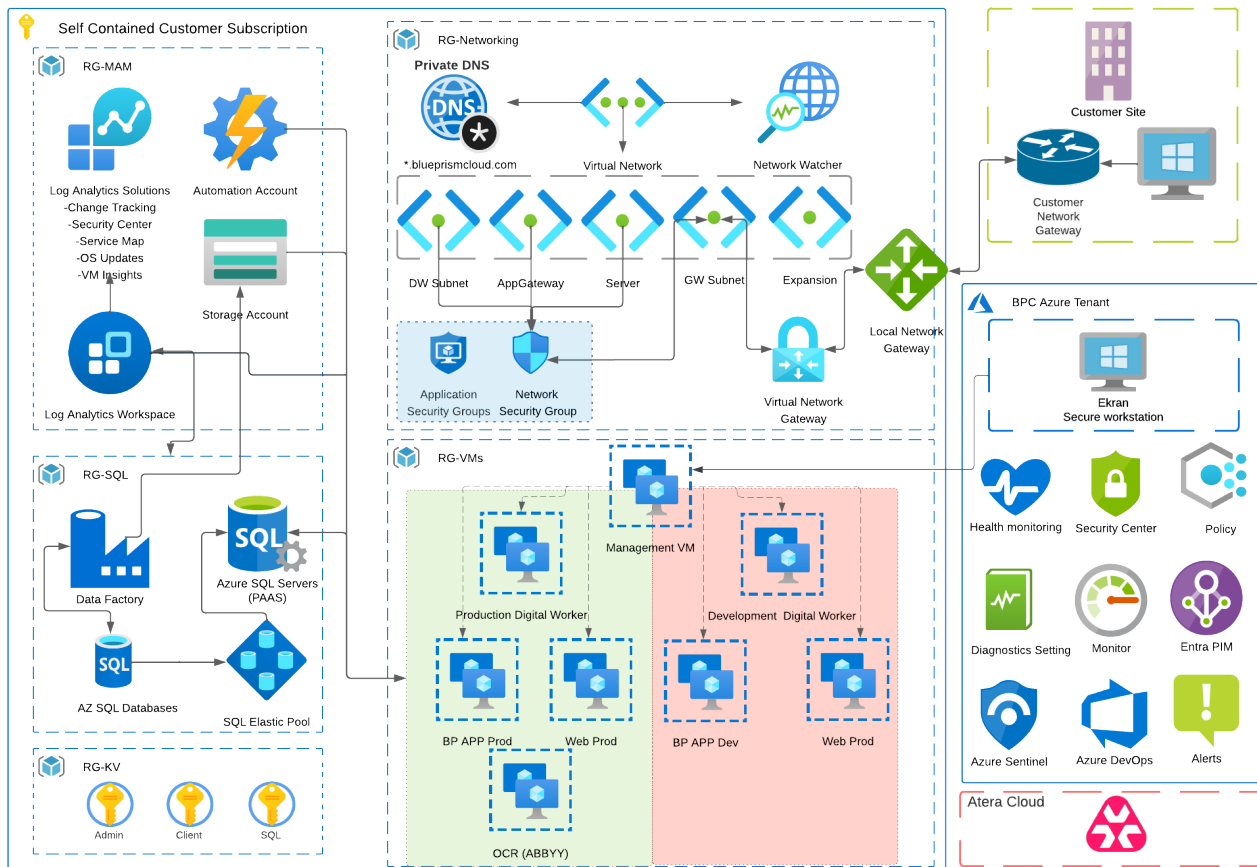


Outbound SMTP connections on TCP port 25 from virtual machines are blocked. This is a Microsoft enforced rule to protect Microsoft's Azure platform, and conform to industry standards to block unsecure SMTP traffic.

Data Security

This guidance details the transition and storage of client data through the Blue Prism® Cloud Digital Workforce platform. The guidance is intended to clarify precisely how client data is used within the platform and where, if applicable, client data is held so that an informed decision can be made regarding the protection of private and sensitive data.

For each of the applicable components in the Blue Prism Cloud Digital Workforce platform, details of data transition and storage are specified. This is performed through responding to a series of questions to explain how data is managed through the platform. These questions are typical of client and partner requests that Blue Prism Cloud have received.



During the deployment of the Blue Prism Cloud platform, Blue Prism do not require access to live client data. It is recommended that only anonymized test data is used which does not show any private or sensitive information. However, should this not be possible Blue Prism have operational controls in place to ensure client data is controlled in accordance with the policies and procedures that are evaluated as part of our ISO27001:2017 accreditation and our role as a data processor according to GDPR.

This document sets out to explain how client data is used within the Blue Prism Cloud Digital Workforce platform and to understand the platform controls that are in place. Client data which is processed within the applications and systems is intended to be never held at rest within the environment, however due to the nature of some clients business processes this is not always possible. The various platform components handle information differently and have distinctive safeguards in place to minimize, if not stop, the storing of client data when / if they are used.

Security recommendations

The following security recommendations should be considered when working with the Blue Prism Cloud Digital Workforce platform:

A Recommendation

r
e
a

B In line with Blue Prism best practices, it is recommended that logging levels should be set to Errors
I Only for production environments, generating limited logs only when an issue presents itself. If
u required, logging levels can then be changed to help diagnose the issue.

e
p Client operators are in control of logging levels and can change them though this is not recommended
r except in the development environment where clients should use non-sensitive information during
i development.

s
m

O Documents should be stored in the client Folder Store/File Share and not within the platform itself.
C Folders are then monitored and once populated, the OCR component will ingest and issue the
R captured fields to a queue in the RPA capability.

I When consuming IADA.ai, information is processed externally from a client platform, due to IADA.ai
A leveraging third-party cognitive services. Users of the Digital Workforce platform are in control as to
D what information is sent to IADA.ai within an automation.

A
.
a
i

Components

The sections below provide a question and answer style approach to explain the flow of data within the Blue Prism Cloud Digital Workforce. All aspects of the platform components are included, with the document order being aligned to the event timeline journey of work (business process tasks) execution.

Blue Prism

The following are a set of questions that are asked when inquiring about data flow and storage for Blue Prism.

1. When a digital worker migrates data from one application into another, where is the transient information held?

When a digital worker migrates data from one application to another as part of an automation, information (data) will exist in the memory of the digital worker executing the task. The information will be purged through the following methods:

- If a copy and paste is performed, then any new copy will override the previous value.
- If the data is held in memory the default Windows memory management function will control clean-up. In addition, digital workers should be scheduled for a restart every 24 hours by a client operator.

2. **When an item is written to a Queue, what data is held?**

Data items and timestamps for audit purposes are stored against the work queue item and held within the RPA Database.

3. **When are work Queue items deleted?**

Queue items lifespan are controlled by the operators of the platform, recommended best practice direct practitioners to clear these out at the end of a process or at least as part of a daily cleanup activity.

4. **When an item is pending completion, where is the data associated with the item held?**

These are held within the session logs within the RPA Database.

5. **When an item is marked as completed, what happens to the data collected as part of the automated process?**

These are held within the session logs within the RPA Database.

6. **When an item is marked as completed, what happens to the original data received?**

These are held within the session logs within the RPA Database.

7. **When a digital worker completes a process, what information is logged?**

Blue Prism Cloud strongly recommend that 'Disabled' is the logging level that is set in the Production environment to minimize the risk of sharing private data.

8. **In Development what is the logging level?**

In Development, Blue Prism Cloud recommend 'Errors Only' as the default logging level across the environment. This can be increased by the client during development if needed by setting the logging level for key Stages only. It is not recommended to set all Stages to 'Enabled' as prolonged periods of increased logging will cause a degradation in service.

9. **In Production what is the logging level?**

In Production, Blue Prism Cloud recommend 'Disabled' as the default logging level across the environment. Logging should not be increased as this control ensures data items or information of interest is not inadvertently collected within the RPA database.

10. **What information is permanently stored within the Blue Prism RPA database?**

The following items are permanently stored:

- Process Workflow Logic
- Application Credentials (optional / where relevant to the business process)
- Environmental Variables, for example, a path to the location of a file or a URL
- Process log information, dependent on logging level set by the client operator

11. **How are the encrypted credentials provided to a digital worker?**

The Blue Prism Application Server retrieves the encrypted credential from the database and then decrypts the returned value before issuing the credential and process to a digital worker. The Blue Prism Application Server to digital worker channel is encrypted using WCF: SOAP with Transport Encryption.

12. **What encryption techniques are used for the Blue Prism database?**

Transparent Data Encryption and AES256 bit encryption. Data in transit is encrypted with Transport Layer Security (TLS).

13. **What options are available for the deletion of log information from the Blue Prism database?**

The logging levels recommended for Production and Development are configured to protect against the inadvertent collection of information. Should the client wish to purge the logs it is possible through manipulation of the SQL database performed by Blue Prism Cloud Support via an agreed Change Request.

Authentication Server

The following are a set of questions that are asked when inquiring about data flow and storage for the Authentication Server component.

Users access the Hub and Interact environments through Authentication Server. Authentication Server contains the configuration settings for connecting to your organization's Blue Prism environment. Authentication Server therefore stores the following information in the Authentication Server database :

- Connection strings to the platform
- LDAP connection settings (if configured) including Group Role mappings
- User credentials and roles assigned
- Configuration details of service accounts
- Synched users between Authentication Server and Blue Prism (if using Blue Prism version 7.0)

1. **What form of encryption does Authentication Server use?**

Users log in through Authentication Server which determines the components they have access to. Authentication Server uses SHA-256 to hash the client secret and client ID.

Password storage – The AspNetIdentity library is used for password hashing and uses the following algorithms:

- PBKDF2 with HMAC-SHA256
- 128-bit salt
- 256-bit subkey
- 10000 iterations

Hub

The following are a set of questions that are asked when inquiring about data flow and storage for the Hub component.

1. What information is stored in Hub?

Hub is primarily a presentation layer of information within the platform and as such does not store a copy of information from Blue Prism. Hub does however store the following items of information:

- Dashboard details, including details of widgets and saved configurations
- License details
- Business process metadata, for example, Process Name, Priority, SLA, and so on
- Email settings
- Plugins installed
- Automation Lifecycle Management (ALM) details, Including Wireframes, Process Definitions, Exceptions and Applications (if installed and licensed)
- Interact form details (if installed and licensed)

The Hub installer generates a PFX certificate and saves it to Trusted Root Certificate Authorities. The Identity Server uses it to encrypt the JWT token and to validate the license file. The JWT token is encrypted by the RSA-SHA-256 algorithm and the key size is 2048 bit.

2. What log information is held in Hub?

In Hub, the following information is logged and presented on the Audit tab:

- Added user
- Edited user
- Retired user
- Made live user
- User login
- Failed login
- User logout
- SMTP settings edited
- Added role
- Edited role
- Deleted role
- Made live authentication
- Edited authentication
- Deleted authentication
- Authentication synced
- Retired authentication
- Added authentication
- Forms submitted
- Forms approved
- Forms declined
- Form status changed (via API)
- Create service account
- Edited service account
- Deleted service account
- Regenerated secret for service account
- Change password
- Created process definition
- Removed process definition
- Deleted process definition

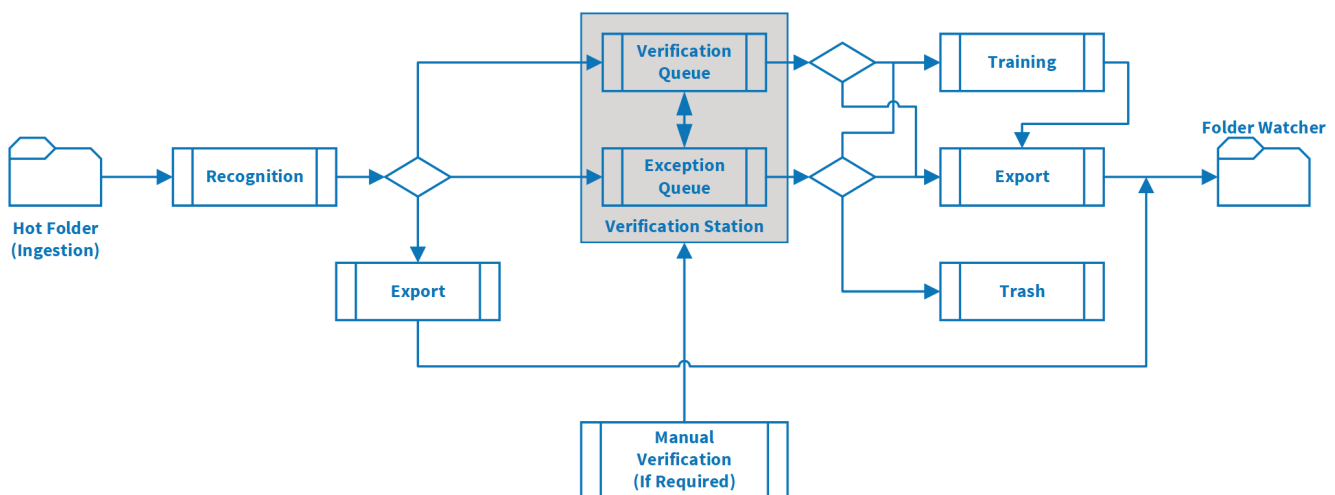
- Increase major – audit logging for increasing the process definition major version
- Sign off started
- Sign off process definition
- Redacted process definition
- Owner redacted process definition
- Sign off finished
- Update to Active Directory users
- Active Directory users created
- Active Directory synchronization started
- Active Directory synchronization completed
- Active Directory synchronization failed
- Active Directory domain added

3. Where is the log information stored in Hub?

Log information is stored in the Audit database.

IADA OCR

The following are a set of questions that are asked when inquiring about data flow and storage for the IADA OCR component. The data flow diagram for IADA OCR is illustrated below:



1. Where does the input file exist?

The file exists in the client local share outside of the Digital Workforce platform. This is referred to as the 'Hot Folder'.

2. How does a document get into the Hot Folder?

It is moved / copied there by either an end user or a digital worker. This is a process dependent decision.

3. What happens to the document within the Hot Folder after processing?

Blue Prism Cloud standard configuration is to delete the document immediately after successful ingestion and it produces a temporary XML copy. The original document is managed via the Image

Import Profile settings. Documents can be configured to be moved into a dedicated subfolder within the same Hot Folder location in the client local share if required.

4. When processing the file (from the Hot Folder), where does the temporary XML copy exist?

This is the process between the Hot Folder and Recognition activity in the diagram above, where a copy is created and stored on a dedicated disk on the Blue Prism Application Server.

5. When is the temporary XML copy removed from the database?

This is deleted upon export.

6. What data is extracted from the file?

A Document Definition template is used to identify the data from the document that is to be extracted. This data is extracted into the temporary XML.

7. How long is the extracted data in the Document Definition held for?

By default, all processed batches are deleted immediately after export. This can be changed by the client to 14 days if required, though it is recommended that delete immediately is used when handling sensitive data.

8. Where does the data extracted as per the Document Definition exist?

The temporary XML that is created and has the extracted data within it, is stored in the OCR database or on the Blue Prism Application Server disk (configurable by support based on usage load) until deleted (see [question 7](#)).

9. What happens to the data once it has been processed?

If the input data is processed without requiring verification, then the OCR function will output the temporary XML of the captured data items into a folder on the Blue Prism Application Server. In the diagram above this is the Recognition to Export route.

10. When a document cannot be automatically processed and requires verification, where does the data exist?

Information is held in the OCR database until verified.

11. During the Verification stage, is any data temporarily / permanently logged?

Any data that is recognized will be stored in a database until verification is complete. After which the document information is exported and the original either deleted or stored as per configuration parameters. It is recommended that the default of 'immediate deletion' is preserved.

12. When training is required on an item that has gone for verification, where does the data exist?

Information is stored in the OCR database and held permanently, see [question 13](#).

13. What is contained within Training Data?

Training data is a full copy of a document or PDF, this includes the page structure but also the field level

information. It is recommended practice that example documents are used when providing training data due to it being persistently stored.

14. During the Verification stage, is any data logged?

Data used during document processing is stored in the OCR database until automatic cleanup of Event log and Report Data occurs, by default it is set to:

- Event Log – deleted automatically after 14 days
- Report Data – deleted automatically after 180 days



No metadata is stored in these logs.

15. In the Verification stage where the item is 'Trashed', what happens to the item?

All document data is permanently removed from the OCR database. Event logs and Report Data will remain; however, no document data is kept.

16. During the Verification stage where an item is sent to 'Training', is any data temporarily / permanently logged?

Any document that is sent to Training will be stored as a whole document, see [question 13](#). It is recommended that the training batch is set to “Lock Training by Operators” in the training batch to stop Operators inadvertently sending sensitive data to the OCR database.

17. What approach is used to read/extract the XML file outputted by the OCR function?

The XML file (housed on the Blue Prism Application Server as above) is polled by FolderWatcher, a Blue Prism Cloud proprietary Windows Service to extracts the data and send to the IADA web service.

18. Does FolderWatcher log any of the extracted data?

No.

19. Does the IADA web service log any of the extracted data?

No.

20. What happens to the XML file created by the OCR function, once FolderWatcher has extracted the data?

FolderWatcher will delete the temporary XML file once it has successfully passed the data to the IADA Web Service.

21. How does the data received by the IADA web service present itself into a Queue?

IADA creates a Queue item record which included the collected data in an Blue Prism collection.

22. What Management Information or Report Data is stored within the platform?

Report Data information stores the following:

- Processing time of a document

- Number of documents processes
- Stages navigated (such as, Verifications, Exceptions, Training, Exports and Trashes)

IADA.ai

The following are a set of questions that are asked when inquiring about data flow and storage for the IADA.ai component covering language translation, sentiment analysis, text analysis, language detection, and extraction of key phrases.

1. When IADA.ai is called, what information is sent by the digital worker?

IADA.ai is a service that takes one or many inputs and produces one or many outputs. For example, the input may be an email body with the second input being a target language the message should be translated into. In this scenario, both the email body and the specified language choice would be sent by the digital worker. This information is not obfuscated and therefore the sending of personal data and information has to be controlled by the organization.

2. What information is logged by the digital worker when calling IADA.ai?

The logging levels set by the RPA would be used when the digital worker calls IADA.ai, please refer to the [Blue Prism section](#) of this document.

3. Where does IADA.ai reside?

IADA.ai resides within a centralized Blue Prism Cloud Microsoft Azure subscription which is external to any client or partner platform subscription or account.

4. Where is the information processed?

Information is processed within the IADA.ai web application which resides within the Blue Prism Cloud Microsoft Azure subscription – thereafter, a Microsoft Cognitive service is called which also processes the sent data by IADA.ai. The Microsoft Cognitive service does not log nor store any information other than a record of the event.

Interact

The following are a set of questions that are asked when inquiring about data flow and storage for the Interact component.

1. How is data added to an Interact form?

Forms are populated by a user or digital worker with the appropriate levels of access with text data and / or an attached file.

2. When a form has been completed but not submitted (so is in a draft state) where does the data exist?

The data is held within Interact, be it a text value, numerical value or file attachment, this is stored within the Interact database. If the **Purge data on submission** option is set for a form, data can only be purged once the form has been submitted. This option is not enabled by default. To prevent data being stored, it is recommended that you enable this option when designing your forms.

3. What log information is held in Interact?

See [question 2](#) in the [Hub section](#) for more details on the audited information.

4. Where is the log information stored in Interact?

Log information is stored within the Audit database.

5. When a form has been completed and submitted where does the data exist?

The data is stored in the Interact database for auditability purposes. The data may also be stored in the RPA database and any end-point databases defined within the automation.

Fields/attachments marked as sensitive (using the **Purge data on submission** functionality) are deleted from Interact.

6. How is a submitted form presented to a Queue for execution by a digital worker?

Interact uses the Interact Remote API to send all the collect data to the queue.

7. Does the Interact Remote API log any of the extracted data?

No.

8. When a digital worker sends information to Interact, where is the data stored?

All data sent by the digital worker will be stored against the Interact submission (within the Interact database).

9. Does Interact utilize any encryption to protect its data?

Interact supports encryption as detailed below:

- **Traffic encryption** – Enable HTTPS only communication for production. Requires customers to provide TLS certificates for all web applications and all communication channels must be secured.
- **Data protection** – The Hub installer generates a PFX certificate and saves it to Trusted Root Certificate Authorities. All applications use it to encrypt sensitive data, such as connection strings in the appsettings.json file. Data protection uses the following default algorithms:
 - Encryption Algorithm is AES-256-CBC
 - Validation Algorithm is HMACSHA256
 - The key size is 2048 bit.

Fair usage policy

Please see the [customer portal](#) for the latest SS&C | Blue Prism® Cloud fair usage policy.

Blue Prism Cloud platform expansion

As a Blue Prism Cloud customer, you have two options available for expanding the platform to include more digital workers on a permanent basis:

- **Option 1:** Available for all customer expansions – Deployment of one or more new digital workers, ready for customer configuration including application install, account creation, potential domain join and so on.
- **Option 2:** Only available to platform expansions of more than five additional digital workers – Deployment of five or more new digital workers against which Blue Prism Cloud Operations will run customer-provided scripts (such as PowerShell scripts) to apply customer configurations.

 Alternatively, temporary 'burst' digital workers can be purchased. For more information, see the [Consumption-based pricing FAQ](#).

Prerequisites

As part of the standard agreement, the Blue Prism Cloud Operations team require access to your customer platform to provide the Blue Prism Cloud service, as detailed below. This access is required for a number of services, including platform expansions.

Blue Prism Cloud deploys the following standard access controls to maintain optimal platform resilience and to meet the obligations set forth in our SLA agreement and Support Terms:

- Local administrative accounts on all virtual machines.
- Ability to execute remote scripting and command line interface based instruction to virtual machines.
- Ability to connect to all Blue Prism Cloud virtual machines through Remote Desktop or equivalent tooling.
- Virtual machines must be allowed to communicate back to our various centralized tooling hubs.

In some cases, your internal policies may require enforcement of network controls. In these instances, amendments must be made on your customer network to allow necessary traffic for Blue Prism Cloud security and monitoring toolsets.

Option 1: Deployment of digital workers (standard configuration)

For the provision of the newly contracted number of digital workers, provided as new deployments ready for customer configurations:

- Our Blue Prism Cloud Operations team will contact you, the customer, upon order qualification to provide guidance.
- Once completed, a platform engineer will notify you and will send you the credentials for the new digital workers via an encrypted email.
- You will then need to complete the onboarding tasks for your new digital workers, for example, install any required applications, digital worker accounts, potentially join to your domain.

If you require assistance with network connectivity for your new digital workers, please email support@blueprism.com with the subject set to: "BPC [*Customer/platform name*] New Digital Worker(s) connectivity issue". Otherwise, Blue Prism will consider the digital workers to be successfully in service.

For any future assistance, please contact [Blue Prism Support](#).

Option 2: Deployment of digital workers (using customer provided scripts)

 This option has a minimum expansion requirement of five digital workers.

Deployment of new digital workers against which Blue Prism Cloud Operations will run customer provided scripts (such as PowerShell scripts) to apply customer configurations. For example, these scripts can be used to install applications, configure desktop, or join domains.

For the provision of these digital workers:

- If applicable to the expansion, you will be asked to confirm your chosen expansion method as part of the initial communications.
- Our Blue Prism Cloud Operations team will contact you, the customer, upon order qualification to provide guidance.
- To deploy the digital workers:
 - After initial communication with our team and as indicated by them, you should raise a support ticket by emailing support@blueprism.com with the subject set to: "BPC [*Customer/platform name*] Digital Worker Expansion".

The email must contain:

- Your customer/platform name
- Your customer provided scripts that must conform to the [requirements detailed below](#). The scripts should be in a zip folder with a 'readme' file which includes a brief summary of the scripts. The scripts must be self contained. If you are using PowerShell, the scripts must use PowerShell 5.1.
- Blue Prism Cloud Operations will run the customer provided PowerShell scripts against the group of new workers.
- Once completed, a platform engineer will notify you and will send you the credentials for the new digital workers via an encrypted email.

Script requirements and conditions

- Blue Prism Cloud Operations will run up to five scripts against any group of VMs requested by you, the customer.
- Scripts should not require any inputs or dynamic variables. All resources/artifacts being consumed by the script should be accessible from the Blue Prism Cloud platform. Blue Prism Cloud Operations will not pre-load resources/artifacts.
- Blue Prism Cloud Operations will not troubleshoot errors, failures, or incomplete runs. The scripts will only be run once.
- Use of these scripts is for platform expansion activity only. Any future requests to run scripts will be denied. This is not intended to update or upgrade customer applications, it is only to facilitate expedited onboarding of new VMs.
- Each expansion request using scripts will require a new support ticket to be submitted.

Glossary

This is a glossary of terms for Blue Prism Cloud.

Generic terms

Term	Definition
Automation Lifecycle Management	An intuitive web-based interface that empowers businesses to capture and document the business process definitions along with the applicable applications and any business exceptions. SS&C Blue Prism® Automation Lifecycle Management is provided as a licensed plugin in SS&C Blue Prism® Hub .
Application Server	A component that manages database connections and removes the need to configure direct connections between the various Blue Prism components and the database. When implemented, all Blue Prism components (interactive clients and runtime resources) connect to the Blue Prism Server service.
Component Library	The name given to the repository containing common and reusable automation utilities and procedures which can be used as part of an automation workflow.
Credential Store	A secure repository for retention or encrypted access credentials which may be required by a digital worker when executing a process.
Decision	An intuitive web-based interface that enables users to train and deploy intelligent machine learning decision-making models within their digital workforce, without requiring any data science expertise. SS&C Blue Prism® Decision is provided as a licensed plugin in SS&C Blue Prism® Hub .
Digital Worker	The name given to the resource within the platform which executes the defined automated processes it receives, interacting with the various local and remote applications, systems, tools, and devices required to complete the process. The digital worker is a Windows runtime component, it is the execution layer and emulates the activities of a human. It takes a process, an item, and the necessary credentials and follows the procedural steps to complete the defined task(s).
Director	An REST API which is used by Blue Prism Cloud components to receive and orchestrate work items.
Hub	SS&C Blue Prism® Hub is a web-based technology platform that provides

Term	Definition
	access to plugins, including SS&C Blue Prism® Interact , SS&C Blue Prism® Decision , and SS&C Blue Prism® Automation Lifecycle Management .
IADA.ai	A component that allows access to an evolving range of proprietary and Microsoft cognitive services which can be called as actions from within a workflow and configured by any automation designer or business user.
Intelligent Automation	Intelligent Automation, also referred to as Intelligent Process Automation (IPA) is a term used to reference a combination of robotic process automation and artificial intelligence to provide a more capable digital workforce.
OCR	A sub-component of the platform which manages the extraction and translation of information from document images into machine-usable data using optical character and image recognition approaches.
Interact	An intuitive web-based interface that allows users to interact with digital workforces, triggering execution of automated processes by creating submissions, providing input by completing information or approvals, and/or observing outputs.
Platform	The name given to the digital workforce technology, provided as a subscription-based Platform-as-a-Service (PaaS) onto which customers or partners build business process workflows to automate and digitize work.
Process	The name given to an object-oriented workflow configuration which links decision logic, application objects and other processes to create an automated and digitized work process.
RPA	Robotic Processing Automation (RPA) is the process of a digital worker mimicking a human's actions to complete a rules-based task.
RPO	Recovery Point Objective (RPO) refers to the amount of data at risk. It is the time between data protection events and reflects the amount of data that potentially could be lost during a disaster recovery.
RTO	Recovery Time Objective (RTO) refers to the amount of time taken to recover the environment in the event of a disaster occurring.

Term	Definition
Surface Automation	The technique used by an application object which connects to an application presented through Citrix, RDP, or another thin-client technology by employing image recognition.

Component-specific terms

Automation Lifecycle Management

Term	Definition
Application	The applications that are used as part of the process that is being automated.
Business process	The business process in ALM should reflect your organization's real-world business process that the automation intends to cover. A process definition will be attached to the business process, and the steps for the business process will be contained in the process definition.
Exception	Exceptions are defined for processes and determine what the automation should do if something unexpected happens in the process. For example, an exception can be defined to handle the entry of incorrect credentials. By default, ALM includes an Unplanned Exception which acts to catch any errors that do not have a specific exception defined.
Process definition	A process definition is a document, whether a physical document or an electronic version, that describes in detail a business process. A process definition document should consist of the following: • A summary of what the overall process and solution is. • Definitions of unique language used within the business process. Scope and expectations as to what the automation should achieve. • Volumes, how many instances of this task are going to be ran each day. • Interact design to dictate what the solution would visually look like. • A list of applications that your automation will interact with as well as their versions. • A high-level process map of what the goal is. • Low level steps, keystroke level details of the process. • Inputs, triggers and outputs relevant to the automation. • Exceptions, what varying scenarios should you expect and handle.
Template	A section of a business process or an exception that can be re-used and applied to one or more than process definition. For example, the action of logging into an application may be present in multiple processes, using a "log in" template means that it does not have to be recreated in each process.

Term	Definition
Wireframer	A web-based user interface that enables automation developers to create the structure (wireframe) of the business process that is being automated by defining business objects and actions, along with best practice techniques, and then deploy the wireframe of the automation to Blue Prism where it can be further enhanced.

Blue Prism

Term	Definition
Action	An Action stage allows a business object to be used in a process. It is similar to a Page Reference in that it takes the flow of the process down to another page, but instead of being in the same diagram it is a page within a business object.
Block	Blocks are used for a variety of purposes, such as: • Grouping variables, for example, inputs and output parameters for easier readability • Exception handling, to facilitate handling exceptions thrown by different stages • To avoid infinite loops raised due to exception handling
Business Exception	A business exception is a “planned” exception. This is an expected break in a business process because of potentially missing or incorrectly formatted data. These exceptions can be planned for in the automation and may be recoverable.
Business Object	A business object is an object that models the applications that the digital worker interacts with. It normally has multiple pages to simulate the functions of an application such as: • Opening and closing an application • Writing into fields • Reading messages on screen • Clicking on buttons and menu items.
Component	A component is a mid-layer object that allows you to group common actions from one or more objects together to create a reusable and flexible module that can be embedded in your process workflow, but can also be used in other workflows. Creating these bite-size chunks will improve delivery and follows a holistic deployment approach.
Data Item	Data Items are containers for variables. They are where values are stored that can be used with automations. They can support different types, including:

Term	Definition
	• Binary • Date • DateTime • Flag • Image • Number • Password • Text • Time • TimeSpan For more information, see Data Types in the Blue Prism documentation.
Environment Variable	An environment variable is a dynamic-named value that can affect the behavior of running processes on a computer. They are part of the Environment in which an automation runs. Once an environment variable has been created it is available for use in Object or Process Studio. Environment variables are used to keep the value of that variable dynamic and can be referenced whenever required.
Page	A page is a mechanism for splitting up a complex processes. Pages allow the process to be defined in smaller, less complex sections which can be tested in isolation. A Page Reference is used to join the pages and its contents together.
Process	A process is intended to obey instructions performing a repetitive task. Those instructions could be, for example, extracting data from a spreadsheet. Alternatively, a process might be designed to launch an application and check a diary for available slots for patient appointments.
Queue Item	A queue item is a job that is in a work queue waiting to be processed.
Queue Item Key	The queue item key is a unique identifier of the queue item within the work queue.
Stage	Stages are items that can be used within an automation to simulate the interactions of a human performing a task. For a complete list of the stages, see Stage types in the Blue Prism documentation.

Term	Definition
System Exception	This is an “unplanned” exception typically caused by a failure of a server, service, network, or infrastructure resource. These may be recoverable if the event recovers in a predictable time and the automation has waited for the resource to become available. Otherwise these are unrecoverable exceptions.
Work Queue	A work queue is an internal configurable list that enables a process to manage its workload. A process can use different work queues and a work queue can be shared by multiple processes if required.

Decision

For terms related to Decision, see the [Decision glossary of terms](#).

Director

Term	Definition
Cross-Queue Search	In traditional RPA deployments, work is aligned to a queue and work is selected on a First In First Out (FIFO) basis. Cross-queue search allows all queues to be searched in parallel.
FIFO (First In First Out)	First In First Out means that the items are processed in the same order that they are added to the queue. This is the default order in which items are processed by Blue Prism. If a priority is defined on an item, this will be processed before applying the FIFO principle.
GNPI (Get Next Prioritised Item)	A function available within Director to allow a digital worker to select an item based on its importance. This function allows for cross-queue searching.
Priority	The priority of the item as defined by the business. The priority value must be above zero. The lower the value, the higher the priority.
SLA	The service level agreement for the item as defined by the business. The SLA value is a time span. This is the amount of time within which the work queue item should be completed and processed. The SLA time span value is used by the Director algorithm to produce an SLA deadline. The SLA is taken into account after the priority.

Term	Definition
SLA and Priority Management	The term given to selecting work based on its importance. Each item (a task within one of the various queues of work) is tagged with a priority value and a SLA.

Hub

Term	Definition
Plugins	Self-contained features that can be individually installed to provide information about your digital workforce.
Role	Roles control access to Hub and the plugins. They also define the level of access, for example, a Hub administrator or a Hub user. In addition, there are some automatically generated roles based on the plugins that have been installed. These roles cannot be deleted, but users can be added to and removed from them.
Widgets	A small-scale version of plugins that is used on the Hub Dashboard.

Interact

Term	Definition
Drafts	A holding area for a request that has been partially completed.
Fields	Elements that can be used within a form to capture information from the user.
Form	An entity within Interact that holds a range of properties such as a fields, rules, roles, privilege checks, and association to a queue.
Process	A collection of procedural steps which allow the digital workers to follow a business process, for example, a New Starter Process, allowing a digital worker to understand how a user is onboarded into the organization.

Term	Definition
Queue	A container for items. Queues do not need to be associated to a process (new starter queue) but usually are.
Rules	Dictate how the fields behave depending on user interaction.
Status	A value used to track the lifecycle of a submission.
Submission	The term given to a partially (Draft) or fully (Submitted) completed Interact form.

OCR

Term	Definition
Confidence	The level of confidence the technology has that the characters have been identified correctly.
Document Definition Template	Used to define a structure identifying specific fields or areas of text to extract information from.
Export	The process to produce the output once extracted and verified.
Extraction	The reading of information from the images identified using the Document Definition Template.
FlexiLayout Studio	Used to identify/create the specific areas or regions within a scanned document requiring capture during the recognition process.
Hot Folder	Location where the scanned images are sent prior to recognition.
Ingestion	The process of loading images from the Hot Folder.
Project Setup Station	Used to establish the profile and configuration for the specific project.

Term	Definition
Projects	Used to control the overall process.
Verification	The process used to verify items that did not meet the 100% confidence level.
Verification Station	Used to verify documents or correct verification errors after they have been processed.