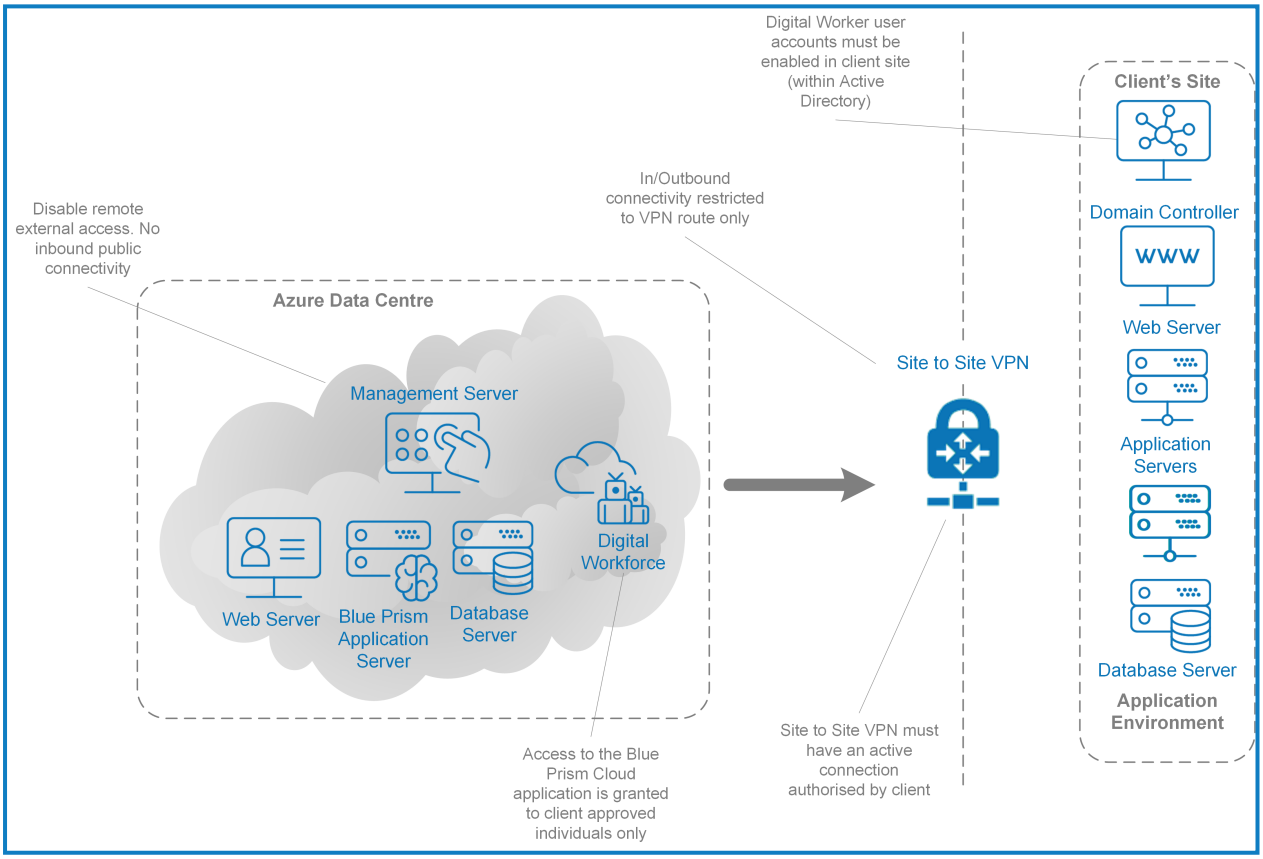
Connectivity and Access

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. The digital workers emulate a user executing knowledge-based work and connects to the customer application(s) through a Virtual Private Network (VPN). Either a Site-to-Site VPN or an Azure ExpressRoute connection can be created where the digital workforce exists 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 Azure Data Center connectivity to the customer site identifying key safeguards.



Connecting a digital workforce to your organization

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

Site-to-Site VPN

The Site-to-Site VPN forms a secure, persistent connection between the customer subscribed digital workforce resources and the customer environment. The Site-to-Site VPN as standard ensures that a production platform is accessible from the customer or partner end of the connection only. When configuring a Site-to-Site VPN, Blue Prism Cloud will configure the Virtual Private Network (VPN) to a customer specified address range that is compatible with the customer address space. Blue Prism Cloud is compatible only with the following Microsoft supported devices:
https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-devices

Domain joining and group policies

Blue Prism Cloud is based upon a Microsoft Windows architecture. Once the Site-to-Site VPN is in place and the digital workforce deployed, resources can then be joined to the customer domain. This practice ensures connected resources can inherit customer or partner corporate standards for information and cyber security. To enable the successful operation of your digital workers, the following Group Policy settings should be enforced:

Policy	Setting
Interactive logon: Do not require CTRL+ALT+DEL	Enabled
Interactive logon: Message title for users attempting to logon	Empty
Interactive logon: Message text for users attempting to log on	Empty
Do not display the lock screen	Enabled

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 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.

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 Security Groups (NSG) to be established. The customer does not have direct access to the deployed PaaS platform within Azure 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 NSG), 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.

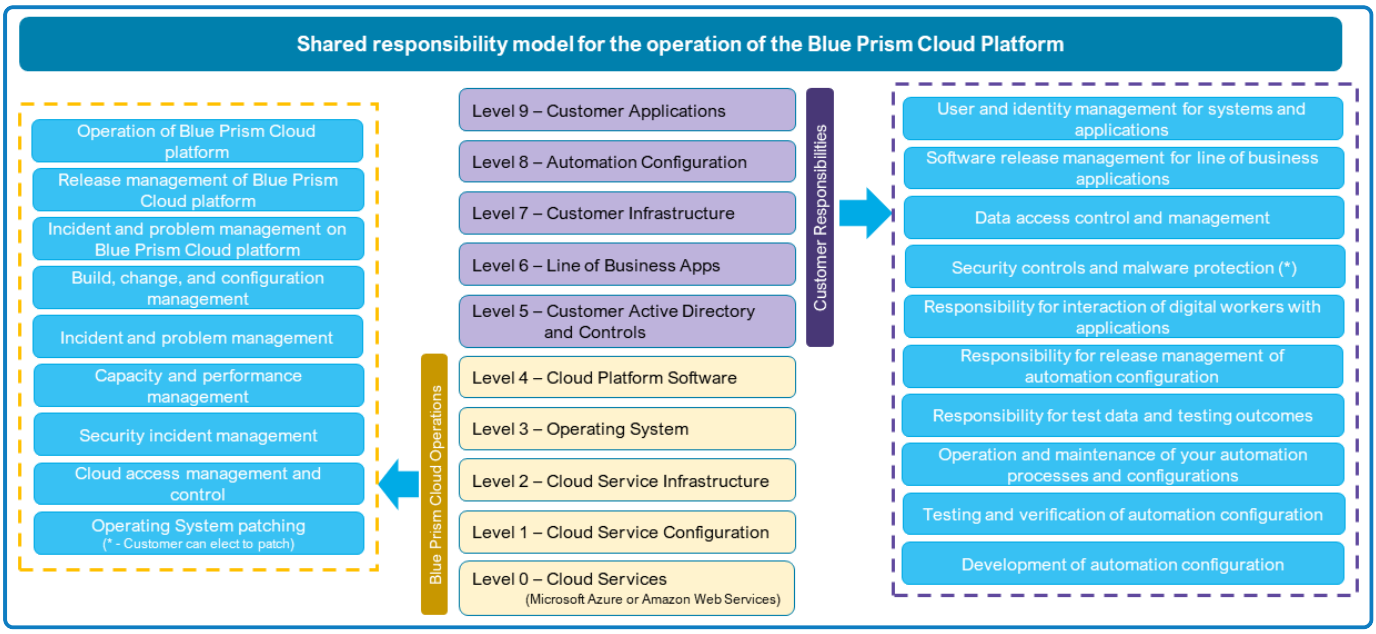
- **Administration and Monitoring console** – a web client accessible from the Application Server;
- **FlexiLayout Studio** – a thick client accessible from the Application Server;
- **Project Setup Station** – a thick client accessible from the Application Server;
- **Verification Station** – a web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

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 (BPC) and the customer (C):

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)						
Customer UI login credentials	C	C	C	N/A	C	C
Functional application testing	C	C	C	N/A	C	C
Functional readiness testing	Collaboration C BPC	Collaboration C BPC	Collaboration C BPC	N/A	Collaboration C BPC	Collaboration C BPC
Maintain Blue Prism software	BPC	BPC	BPC	N/A	BPC	BPC
Log collection	BPC	BPC	BPC	N/A	BPC	BPC
Service start-up	C	BPC	BPC	N/A	BPC	BPC
Service monitoring	BPC	BPC	BPC	N/A	BPC	BPC

Operation	Management Server	Web Server (Supporting Hub and Interact)	Blue Prism Application Server	Database	Production Digital Workers	Development Digital Worker
Service recovery	Collaboration C BPC	Collaboration C BPC	Collaboration C BPC	N/A	Collaboration C BPC	Collaboration C BPC
Level 3 – Operating System						
Operating system login	Collaboration C BPC	Collaboration C BPC	Collaboration C BPC	N/A	Collaboration C BPC	Collaboration C BPC
Operating system patching	C or BPC	C or BPC	C or BPC	N/A	C or BPC	C or BPC
Log collection	BPC	BPC	BPC	N/A	BPC	BPC
Maintain Cloud software	BPC	BPC	BPC	N/A	BPC	BPC
PowerShell CICD	BPC	BPC	BPC	N/A	BPC	BPC
Service start-up	BPC	BPC	BPC	N/A	BPC	BPC
Service monitoring	BPC	BPC	BPC	N/A	BPC	BPC
Service recovery	BPC	BPC	BPC	N/A	BPC	BPC
Level 2 – Azure Infrastructure						
Azure login	BPC	BPC	BPC	BPC	BPC	BPC
Log collection	BPC	BPC	BPC	BPC	BPC	BPC
Backup and recovery	BPC	BPC	BPC	BPC	BPC	BPC
Service monitoring	BPC	BPC	BPC	BPC	BPC	BPC

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.
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.
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.
PowerShell CICD	As a Blue Prism Cloud service: Delivery of platform CICD pipeline code.
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).