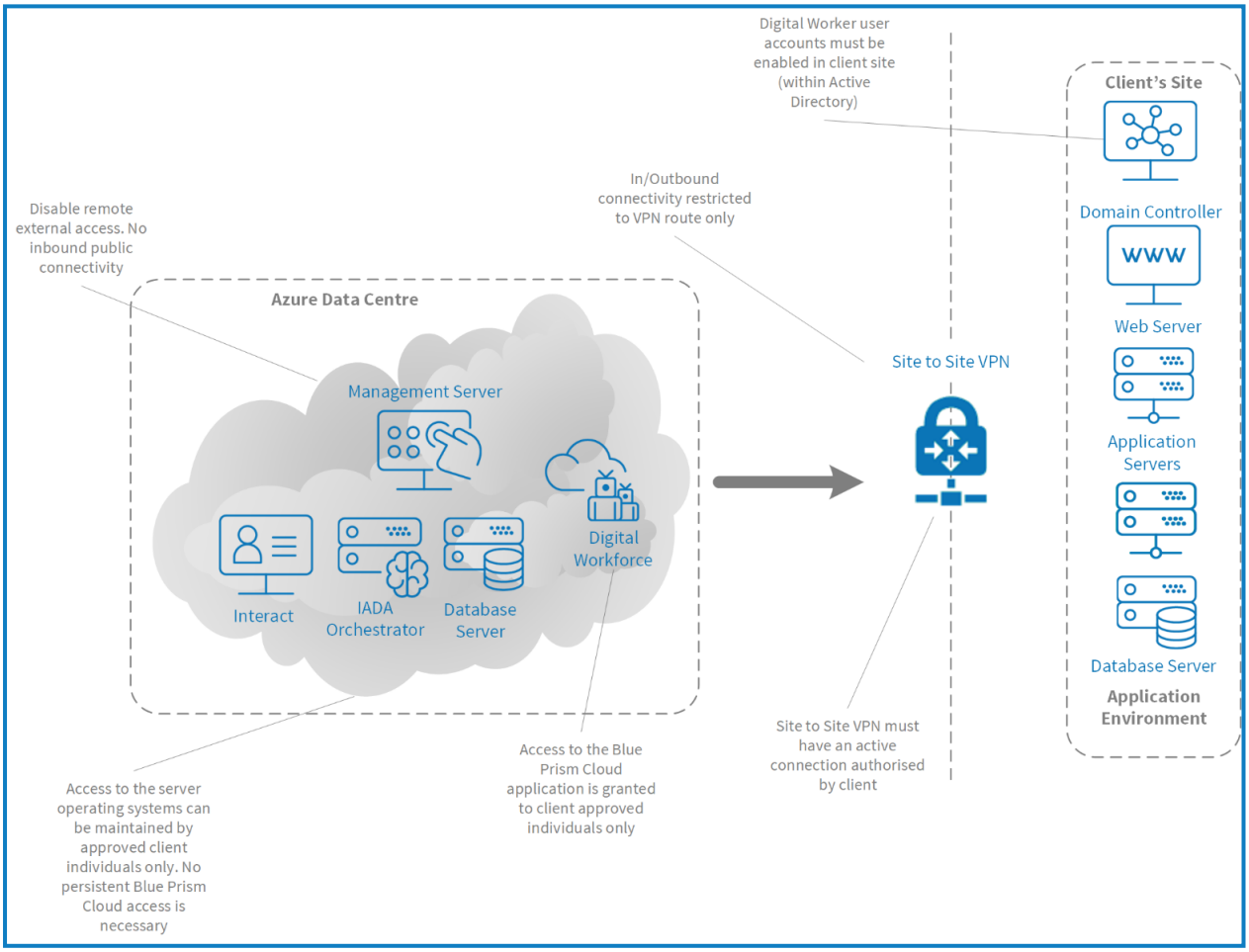
Connectivity and Access

This section outlines the connectivity of the Blue Prism Cloud platform to a client 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.

The Blue Prism Cloud digital workforce is a Software-as-a-Service (SaaS) solution deployed into Microsoft Azure. The digital workers emulate a user executing knowledge-based work and connects to the client 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 Centre connectivity to the client site identifying key safeguards.



Connecting a digital workforce to your organization

This section details information for the client or partner side responsibilities in the deployment of a Blue Prism Cloud platform.

Site to site VPN

The site to site VPN forms a secure, persistent connection between the client subscribed digital workforce resources and the client environment. The site to site VPN as standard ensures that a production platform is accessible from the client or partner end of the connection only. When configuring a site to site VPN, Blue Prism Cloud will configure the Virtual Private Network to a client specified address range that is compatible with the client address space. The 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

The Blue Prism Cloud platform is based upon a Microsoft Windows architecture. Once the Site to Site VPN is in place and the digital workforce deployed, resources are then joined to the client domain. This practice ensures connected resources can inherit client or partner corporate standards for information and cyber security. To support the orchestration of work from the IADA Orchestrator to a digital worker, 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	Not configured

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. However, during the setup of the environment Interact can be linked to an existing Single Sign On (LDAP – Active Directory) environment for user authentication. User management is then performed via the Active Directory servers and any existing joiners/leavers process would continue to operate as previously. Interact is deployed with a self-signed certificate as standard. If the client / partner plans to make the environment publicly available, the client / partner should supply a certificate from a certified authority.

End user and operator access

Client or Partner Operator access to the Blue Prism Cloud is completed through either a Remote Desktop (RDP) or browser-based access, the option chosen is dependent on the task to be performed. Operators who have a requirement to access the platform should have privileges to access Hub and thereafter additional Blue Prism Cloud resources can be accessed utilizing the Hub plugin, Live Access. Hub, the web-based management interface is accessible over HTTPS. End users who are initiating an automated process or outcome will be required access to Interact. Interact is accessible over HTTPS, clients or partners can also apply their own certificates. Interact is not enabled by default to be accessible outside the client domain i.e. it is not available on a public address. This can however be enabled through a change control activity.

Client application installation

A digital workforce in the execution of an automated process will interact with the client or 3rd party application user interface. For these activities to be fulfilled the digital workforce requires sufficient privileges to the applications in scope. Any of the applications which are accessed as a thick client will need to be installed onto the digital worker operating systems. This is a client led activity but will be supported by Blue Prism Cloud. It is important that 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. Details of all ports and protocols required will need to be supplied in advance to any configuration work, to ensure that changes are kept to a minimum.

Client privileges and managing security

Address space

During the initial configuration of the Site to Site VPN, the client or partner specifies the allowed client 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 client or partner as this collocative change must be completed within the client estate.

Virtual network access

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

Operating system access

As part of the setup, the digital workforce will be aligned to a client or partner domain. This action is one of multiple security functions that ensures the components including the operating systems are accessible by authorized client/partner individuals. At the point of handover Blue Prism Cloud's access is revoked.

Patch management and anti-virus

Through domain joining, the windows update and other patch management standards are extended to the digital workforce components. Anti-Virus and Malware protection routines can also be installed upon any of the digital workforce operating systems.

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 Cloud offer an encrypted credentials store, or the ability for a digital worker to access an existing client credentials store as part of an automated process.

Managing your digital workforce

Management of the environment is performed from Hub. To access any of the digital workers the recommended route is Hub Live Access. Users can log on to any digital worker using VNC which is accessed through the Hub Live Access plugin. An alternative is to RDP to the Management Server and from there RDP to the digital workers. The Management Server will support up to 10 concurrent user connections, though each digital worker will only support one connection. This is to ensure that two people are not attempting to run the Process Studio on the same digital worker at the same time. Interact and Hub accessibility is performed via a web browser using secure HTTPS connectivity. Additionally, only one RDP/VNC connection to the IADA Orchestrator's is supported.

> In a future release the Management Server will be removed from the architecture as an active system. A standby system will be deployed which will be configured to support access to the virtual machines for Blue Prism Cloud support purposes.

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 client 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 client's responsibility and the blue is Blue Prism Cloud's responsibility.

During the configuration of the environment, the client 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 client does not have direct access to the deployed SaaS 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.

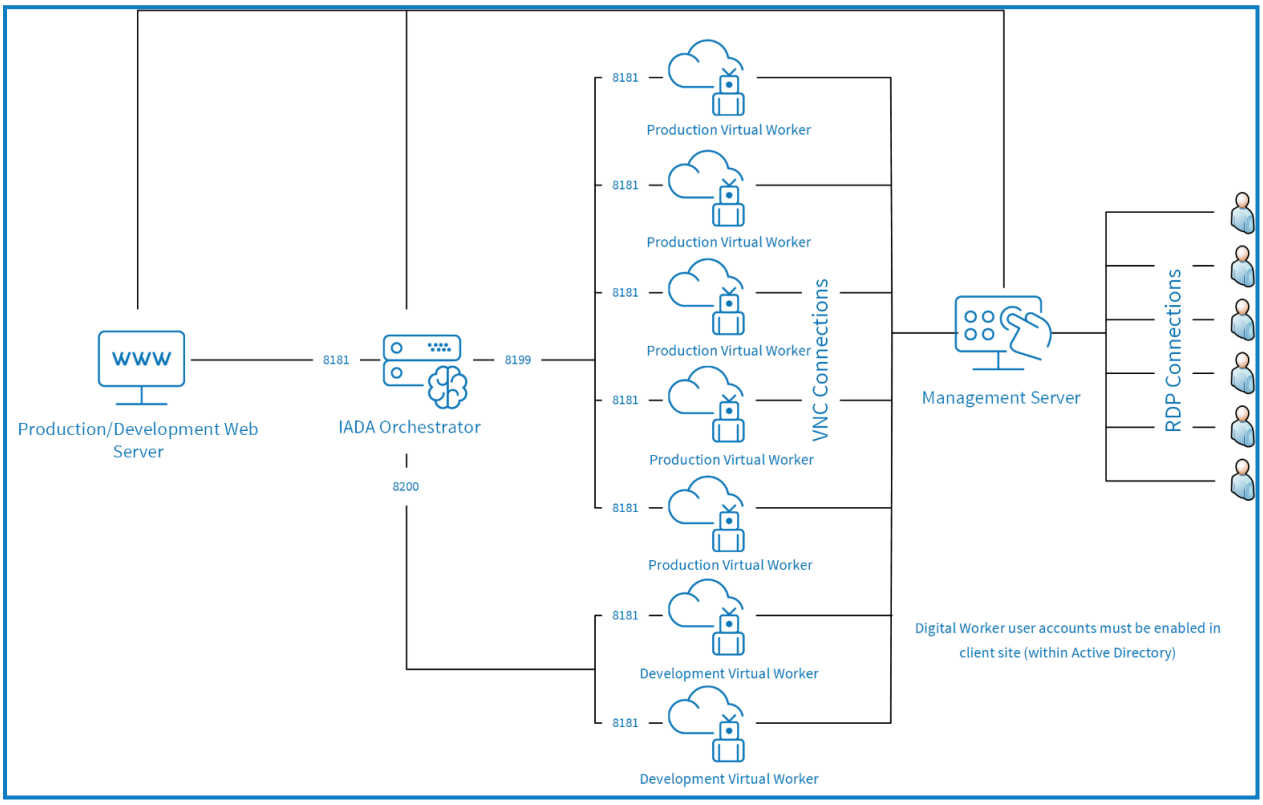
Change management

Blue Prism Cloud maintain an ITIL aligned Change Management process. Any activities requiring a change to be made to the platform, should be requested through cloudsupport@blueprism.com. Any subsequent changes to the configuration of the virtual infrastructure and the networking (including NSG), is performed in conjunction with the Blue Prism Cloud Change Management process and therefore will be planned and approved prior to any commencement of work. During Maintenance windows Blue Prism Cloud will activate a second instance of the Hub and IADA Orchestrator systems. This will enable client / partners to test and verify that the latest release of code is compatible with their own automations and environment.

After testing has been completed the Production instances of Hub and IADA Orchestrator will be upgraded and the secondary instances switched off. This does not apply to Interact where a Production and Development instance of Interact will operate enabling clients / partners to develop and test new process forms before promotion to production.

Knowledge support

Should Blue Prism Cloud be called upon to deliver Knowledge Support (mentoring), access to the environment will be achieved through a client-initiated screen share. Should a longer-term scenario be required, the client can approve access for Blue Prism Cloud via the use of the Azure Just in Time (JiT) function.



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 IADA Orchestrators;
- **FlexiLayout Studio** – a thick client accessible from the IADA Orchestrators;
- **Project Setup Station** – a thick client accessible from the IADA Orchestrators;
- **Verification Station** – a web client accessible from the IADA Orchestrators and digital workers.

Blue Prism Cloud Interact

A standard component of the Blue Prism Cloud digital workforce is the Interact web portal, acting as the initiation and presentation layer of the digital workforce. It allows end users to invoke automations and thus can be presented either publicly or internally to approved users. As standard the Interact portal will be available on a private address, with the client 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 client 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 following table details the responsibility assignment matrix in the form of a RACI chart covering the areas of responsibility for both Blue Prism Cloud and the client through Delivery and Support. The following definitions apply:

- R – Responsible
- A – Accountable
- C – Consulted
- I – Informed

Category	Blue Prism Cloud	Client
Blue Prism Cloud SaaS Delivery		
Blue Prism Cloud deployment	RA	I
Operating Systems Patching	I	RA
Site to Site VPN Setup (Azure)	RA	C
Site to Site VPN Setup (Client)	C	RA
Blue Prism Cloud Application configuration	RA	CI
Backup Management	RA	
Operating System Domain Joining	RA	RC
DNS Record Management	C	RA
Blue Prism Cloud Support		
Platform Availability	RA	I
Platform Upgrades	RA	CI
Platform Maintenance	RA	CI
Microsoft Windows Updates		RA
Anti-Virus and Malware Protection		RA
Process Automation Definition		RA
Process Automation Configuration		RA
Process Automation Support		RA
Blue Prism Cloud Application Management/Operation		RA
Client Application Configuration/Management		RA
Addition of further Digital Workers	RA	CI