Remote Access for Controlling and Monitoring

Introduction

In order to underpin a secure physical or virtual infrastructure, Blue Prism recommend the use of remote access technology to configure, control and monitor Blue Prism solution components.

This data sheet provides guidance on the types of remote access tools that are suitable as well as the features and considerations that should be applied when selecting the technology.

If you have any questions, or require further information, please contact the Blue Prism Support Team (support@blueprism.com).

Remote Access Tool Selection

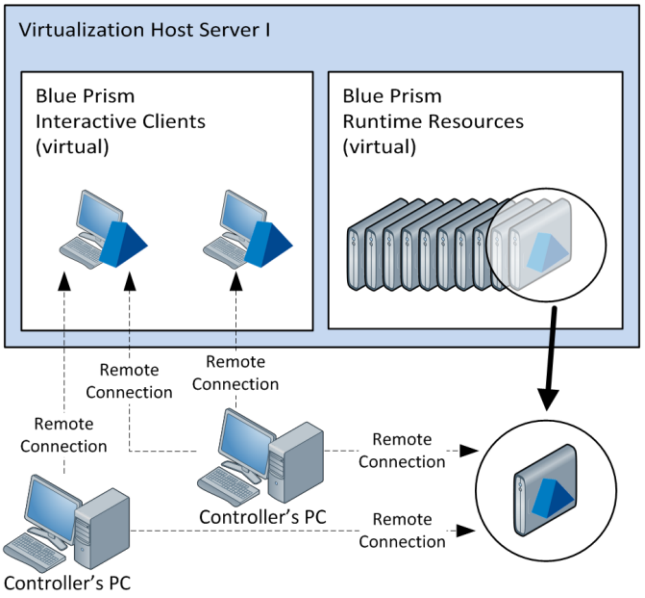

Figure 1: Example of Remote Access Connectivity to a subset of Blue Prism Resources

In different environments, access to the various Blue Prism components is required for the purposes of configuration and development, supporting and maintaining resources and carrying out system start-ups, restarts and shut downs.

Environment	Blue Prism Virtualised Components	
	Interactive Client	**Resource PC**
Development	• Development • Configuration	• Monitoring • Start-up and Restart
Test	• Monitoring • Interactive Debug and Testing	• Monitoring • Start-up and Restart
Production	• Monitoring • Scheduling and Controlling	

Interactive Clients: Where the interactive clients are virtualised is it usual for the Blue Prism controllers and developers to require remote user access to these machines for the purpose of configuring, controlling and monitoring the system depending on the environment type.

Runtime Resources: Whilst there is no predefined requirement for the Blue Prism controllers to access the runtime resources in production, some organisations choose to allow remote access for the purposes of direct monitoring and troubleshooting.

The security implications of allowing this access should be considered as this potentially allows users to directly interact with the actions that are being taken as well as to watch the screens that are being processed which may cause compliance issues if the data being processed is sensitive.

As a result, if remote access is to be granted to production VMs, a remote access tool that provides an audit capability as well as the ability to add a secure login requirement to clusters of remote machines is recommended.

Considerations

When selecting a remote access tool there are a number of considerations:

- **Persistent connectivity**
  The access tool should not cause the original session to be terminated when a different user accesses the same session.
  The second user should be presented with a view of the existing session rather than creating a unique session (and desktop) for each connected user.

- **Disruption or impact on target system**
  The target system's environmental settings should not be changed when a connection is established. (E.g. screen resolution modifications or resizing)

- **Audit facility**
  A level of audit should be provided which tracks the users connected to the various systems along with date time stamps.

- **Security**
  It should be possible to restrict access to particular systems for specific users and ideally this should be integrated into a credential management platform such as Active Directory.

Persistent Connectivity

When operating normally it should be expected that a Blue Prism Interactive Client or Runtime Resource will be logged in and operating as if a physical user were sat carrying out the actions - therefore it is important that when a user **initiates** a remote connection to the resource that:

- The running session is not disconnected or interrupted as a result of the connection.
- The remote user is presented with the desktop of the logged in user / running session and should effectively be able to monitor the actions that the user is taking. (Rather than being presented with their own session / desktop).
- The remote user is able to interact with the system as if they are physically sat at the terminal.
- If an additional remote user attempts to connect that they are either prevented from doing so, or are able to interact with the system as if they are physically sat at the terminal. This should happen without disrupting or disconnecting the previous connections or interrupting the original session.
- It should be possible to connect to the target system even if it is not already logged on (e.g. the remote user should be presented with the windows logon screen)

When a remote user **disconnects** the access it is important that:

- The target system is not automatically locked or logged out but continues running persistently

Disruption / Impact on Target System

When a remote connection is initiated it is important that the target system is not impacted or altered in any way as this may disrupt any work items that are currently being processed.

Some remote access tools are known to change the screen resolution in target environment to suit the display properties of the remote client. An option should exist to leave the virtualised instance's own configuration unchanged, in order to maintain the integrity of the carefully controlled environment.

Audit Facility

Subject to the level of governance and monitoring that is required, it is likely that there will be a need for the remote access tool to provide a level of audit which indicates the date and time that specific users have initiated connections to the various machines.

Security

It is important to understand whether the remote access tool provides a single set of shared credentials per target system; or whether each user has identifiable credentials. This can be important for the purposes of auditing access, as well as ensuring that granular access rules can be applied.

Some remote access tools may also integrate with standard network authentication tools such as Active Directory for the purpose of user access control.

The specific features required of a remote access tool from a security perspective will be subject to the level of governance and control that is required within the organisation.

Tools

The following tools have been implemented successfully to provide remote access to Blue Prism environments however it should be noted that these tools are not specifically endorsed:

- **VMware vSphere**
  Provides the basic requirements for remote access connectivity and is understood to provide good VM based user authentication. Features such as specifying which users can access specific systems and an audit log of connection initiation are also included.

- **VNC**
  Provides the basic requirements for remote access connectivity but uses shared credentials for access control and is not known to have a strong audit capability.

- **DameWare, VMware Console, PCAnywhere**
  These tools are not typically found within enterprise deployments but can be used to fulfil the basic requirements for remote access connectivity.

The following tools have been deemed to be **specifically unsuitable** for providing remote access to Blue Prism environments:

- **Remote Desktop Connection (RDP)**
  The way that this Windows tool (and other tools that use the RDP protocol) handle session management is not compatible with Blue Prism:

  - It requires the remote access credentials to be aligned with the credentials used to authenticate the target system against the network.
  - As a user authenticates any previously connected users are locked out
  - Each connection creates a separate desktop session.
  - The connection is not maintained throughout a system reboot.

Remotely Developing Blue Prism Processes

If remote access is being used to connect to a Blue Prism Interactive Client for the purposes of carrying out process configuration and development, it is necessary to ensure that the connection provided by the chosen tool is sufficiently stable. In particularly it is necessary to validate that the behaviour of application spying is as expected because difficulties have been reported previously with some standard tools including VNC.