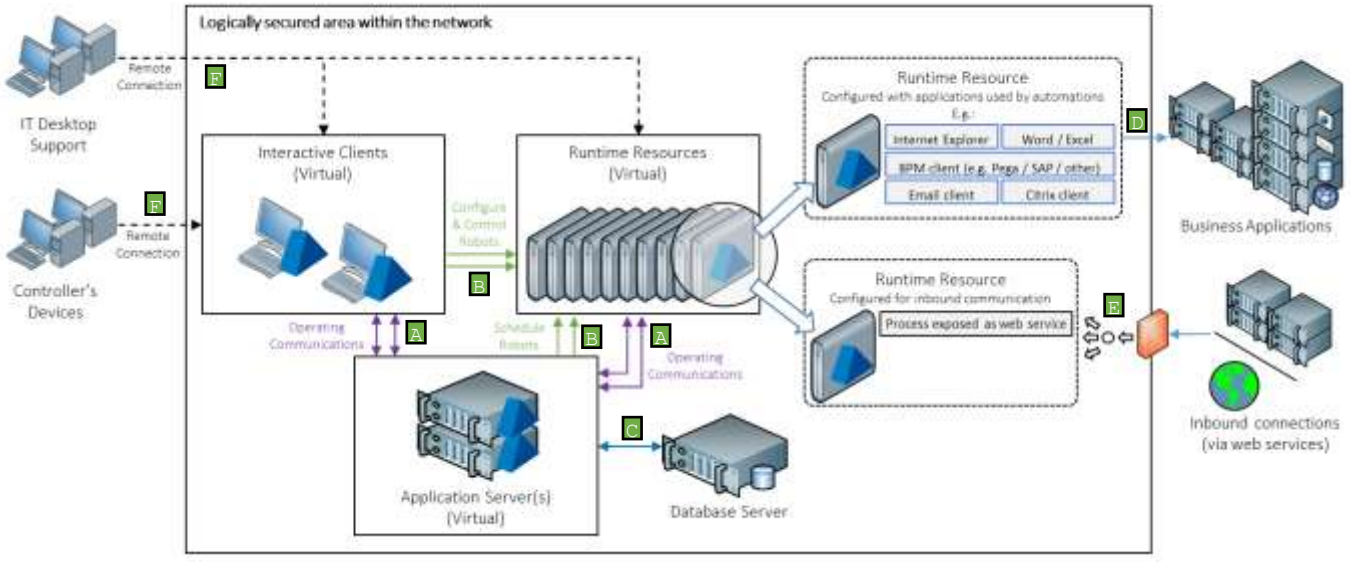
Securing Blue Prism Network Connectivity

This guide is intended to enable architects and system implementers to understand how to secure the network connectivity associated with Blue Prism.

Applies to Blue Prism Enterprise Edition Version 5.0.29+

Overview

The diagram provides an overview of the common communication that occurs with the Blue Prism platform.



Communication		Description	Encryption options
Blue Prism connections to Application Server	A	Primary communication stream for the devices to send data to, and receive data from the database (via the Application Server)	Natively encrypted by default when all Blue Prism components are deployed within an Active Directory Network Infrastructure. Devices can (optionally) explicitly authenticate against the Application Server.
Instructional connection to Runtime Resources	B E	Instructions received by Runtime Resources. E.g. to start/stop processing; or to provide a status update	Certificate-based encryption can be applied by manually deploying an appropriate certificate to each Runtime Resource and updating the device start-up parameters.
Blue Prism database connection	C	The read/write connection between the Application Server and database	Certificate-based encryption can be applied to the connection by leveraging SQL Server functionality which can auto-generate self-signed certificates or leverage an existing verifiable certificate.
Runtime Resources connecting to target applications	D	Runtimes interact with business applications as part of the process automations.	Dependent on the security provided by each respective third-party target application based on the nature of each connection.
Remote connectivity	E	The users who control the platform will commonly use a remote connectivity tool to access centrally deployed devices.	Leverages the security provided by the respective third-party remote connectivity tool.

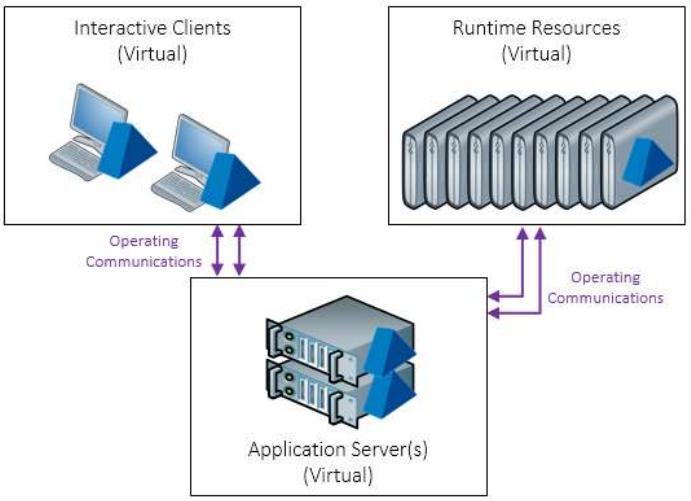
Information on the steps required to apply encryption to each connection is provided in the following sections.

Securing Communications

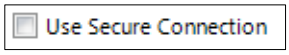
Further information is provided below for each of the connections that may be present within a Blue Prism deployment.

Blue Prism connections to Application Server

The connections between the Blue Prism devices and the Application Server are provided by .NET Remoting which secures and encrypts the connection subject to the following conditions:



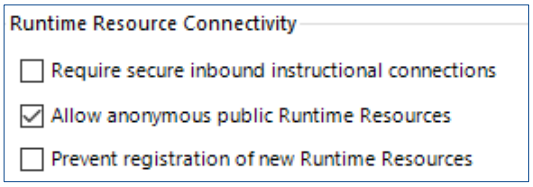
- All Blue Prism devices must be deployed within an Active Directory Network Infrastructure
- The connection settings on each Blue Prism Server and connecting device must be configured to **Use Secure Connection**.



Advanced information on the controls provided by .NET Remoting can be found within the **Blue Prism Infrastructure Reference Guide v5.0 Enterprise Edition**

Controlling connecting Runtime Resources

A number of controls are provided control Runtime Resources that connect into the environment:



- Prevent registration of new Runtime Resources
  When enabled this setting prevent any Runtime Resource that has not been previously registered within the database from establishing a connection. This option is intended for use where there are fixed number of Runtime Resources that have been configured and there is no requirement for additional adhoc Runtime Resources to be registered.
- Allow anonymous public Runtime Resources
  This setting is enabled by default for backwards compatibility to allow public Runtime Resources to connected to the environment without explicitly authenticating.
  Disabling this option requires that all public Runtime Resources provide authentication information when they start-up to ensure that they are authorized to connect to the environment.
    - Blue Prism environments configured with native authentication
      Start-up parameters will need to include /user [username] [password]
    - Blue Prism environments configured for Single Sign-on
      Start-up parameters will need to include /SSO to pass the context of the currently logged in user.

  The user accounts used by Blue Prism Runtime Resources will need to be assigned an appropriate Blue Prism role.

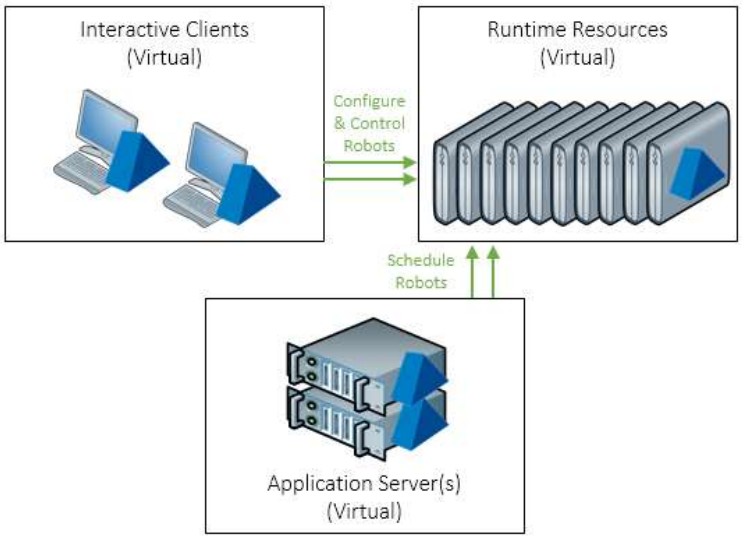
When restricting anonymous public Runtime Resources on a Blue Prism environment configured for Single Sign-on, the Login Agent Server service will need to be configured to Logon as a domain user who has been granted Blue Prism permissions.

Additionally the Login Agent Runtime Resource start-up will need to specify /SSO to pass the context of the service account under which it is running.

Instructional connections to Runtime Resources

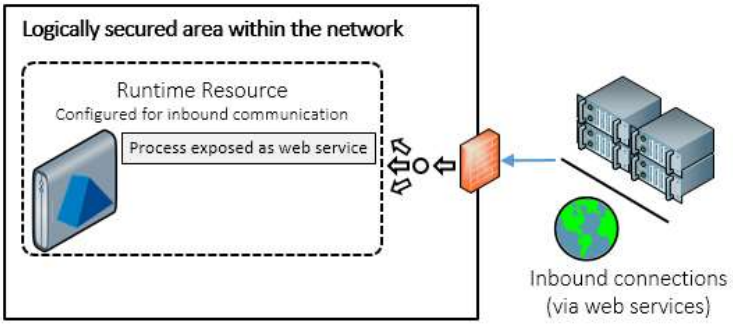
Runtime Resources receive communications which can originate from a number of sources including:

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



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

When appropriately configured, certificate-based encryption is applied to all communication received by the device on a given port irrespective of the origin. Blue Prism web services accessed on configured devices will require a HTTPS prefix.



It is important to note that:

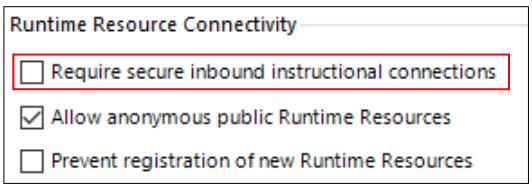
- The certificate common name(s) will need to accurately reflect the paths used for all communications to the Runtime Resource on a given port.
- The devices connecting to the Runtime Resource(s) will need to trust the issuer (Certificate Authority).
- The start-up parameters for the Runtime Resource will need to be configured to leverage the certificate.

Information on **Configuring a Runtime Resource listener to leverage a certificate** is provided in the **Appendix**.

Enforce secure connections

It is possible to enforce all Runtime Resources to only be able to receive encrypted instructional connections by enabling the appropriate setting in Blue Prism. This will require all Runtime Resources to be configured with an appropriate certificate.

This setting only applies to the inbound instructional communications received by Runtime Resources.

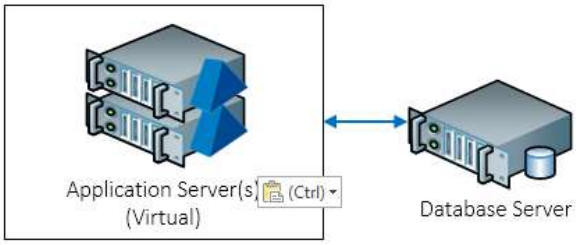


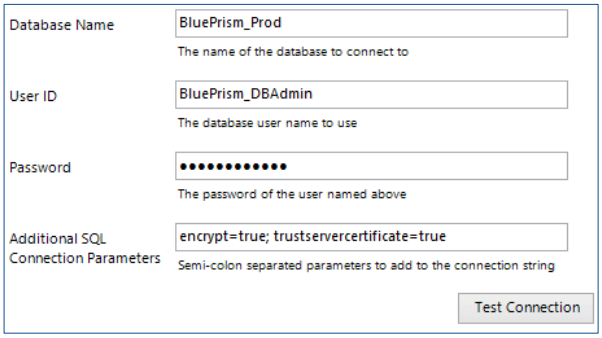
Blue Prism database connection

The communication between Blue Prism and the Microsoft SQL Server database leverages the .NET Framework SqlClient library. By default this is unsecured however the communication can be encrypted by leveraging Microsoft SQL Server functionality.

There are a number of common options approaches:

1. Install a verifiable server certificate on the SQL Server and configure the SQL instance to force encryption for all connections.
2. Install a verifiable server certificate on the SQL Server and configure the Blue Prism database connection to specify that the connection should be encrypted.
   E.g. **encrypt=true**.
3. Configure the Blue Prism database connection to specify that the connection should be encrypted and that server certificates can be trusted without further verification which allows a self-signed certificate on the SQL Server to be leveraged.
   E.g. **encrypt=true; trustservercertificate=true**.



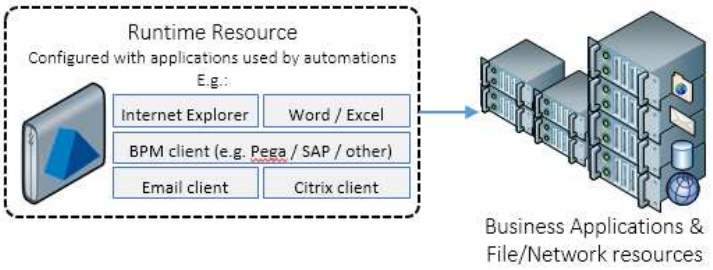


The suitability of the selected approach should be validated using official SQL Server collateral. The actual options available will be determined by the edition of SQL Server.

Runtime Resources connecting to target applications

Runtime Resources are required to be configured with access to all of the applications that are required as part of the automated processes that have been configured. Commonly the paradigm for how Runtime Resources connect to such applications is aligned to how a human user would achieve the same outcome (e.g. both a human and a Runtime Resource access a web site through use of a locally installed web browser).

The security and encryption applied to the connections between the Runtime Resources and the target applications is dependent on the controls provided by each respective third-party target application.

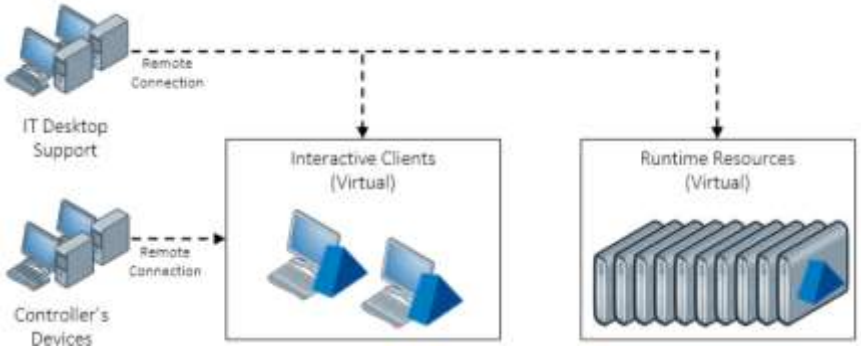


Remote connectivity

Commonly remote connectivity is used by the training Blue Prism users to connect to centrally deploying Interactive Clients. In pre-production environments this will be for the purpose of developing and testing process automations, while in production it will be controlling the platform, reviewing outcomes, adjusting processing priorities etc.

The selected remoting technology will dictate the protection that is applied to each connection.

The **Blue Prism Data Sheet – Remote Access Tools** provides useful information for selecting an appropriate remoting technology. Additionally it explains that Microsoft RDP is not commonly appropriate.

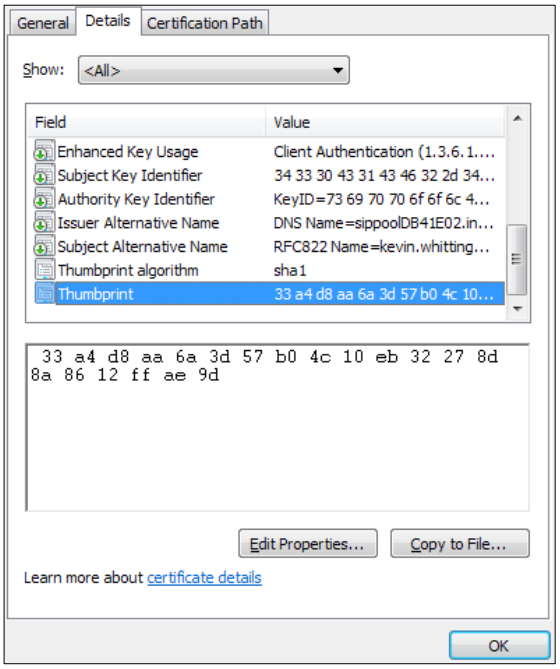


Appendix

Configuring a Runtime Resource to leverage a certificate

The steps below outline the steps required to configure each applicable Runtime Resource listener to use certificate-based encryption for all inbound communication on a given port (e.g. 8181).

1. Idenitfy the network name(s) that are used to address the device
    - When referenced by the Application Server or Interactive Clients, the name used is likely to be affected by the system setting that determines how Runtime Resources are registered and addressed.
    - When referenced by external systems, the routing of the communication will influence the name.
2. Generate a certificate where the common name represents all network names that may be used to address the device. This certificate will need to be generated by a Certificate Authority that is trusted by all connecting devices (e.g. Application Servers, Interactive Clients and, where present, external systems that generate inbound connections to the platform).
3. Deploy the certificate to the certificate store on the device (e.g. through use of group policy; command line; or **Microsoft Management Console** and the **Certificates** snap-in)
   For maximum compatibility select the **Computer Account** and the **Personal** store. Other accounts and stores are supported where appropriate.
4. Identify the thumbprint of the certificate (e.g. by using **Microsoft Management Console** and the **Certficates** snap-in to review the properties; or reviewing the *.cer file).
   When using the value, the white space can be removed to provide a 40 character string e.g. "33a4d8aa6a3d57b04c10eb32278d8a8612ffae9d".
5. Set the start-up command for the Blue Prism Runtime Resource to additionally include the following switch:
   /sslcert [certificate thumbprint]
   E.g.
   automate.exe /resourcepc /port 8181 /sslcert 33a4d8aa6a3d57b04c10eb32278d8a8612ffae9d



6. If using Login Agent, update the LoginAgentService.config within the **ProgramData** location to ensure the **sslcert** argument is specfied.
   The xml to be inserted is of the format:

```
<argument name="sslcert">
    <value>[Cert Thumbprint]</value>
</argument>
```

   E.g.

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <workingdirectory path="C:\Program Files\Blue Prism Limited\Blue Prism
Automate\" />
  <startuparguments>
    <argument name="resourcepc" />
    <argument name="public" />
    <argument name="port">
        <value>8181</value>
    </argument>
    <argument name="sslcert">
        <value>33a4d8aa6a3d57b04c10eb32278d8a8612ffae9d</value>
    </argument>
  </startuparguments>
</configuration>
```

A single certificate can be used multiple times on a given device such as where there are Runtime Resource listeners using different ports (e.g. 8181 and 8182).

Where a multiple-SPN or wildcard certificate is used, it may be possible to deploy the same certificate across multiple devices.

Within a single Blue Prism environment it is possible to have a mixture of Runtime Resources which require secure connections and those which don't.

A central setting within Blue Prism can be used to prevent all associated Runtime Resources from accepting any instructional communications which are not encrypted.