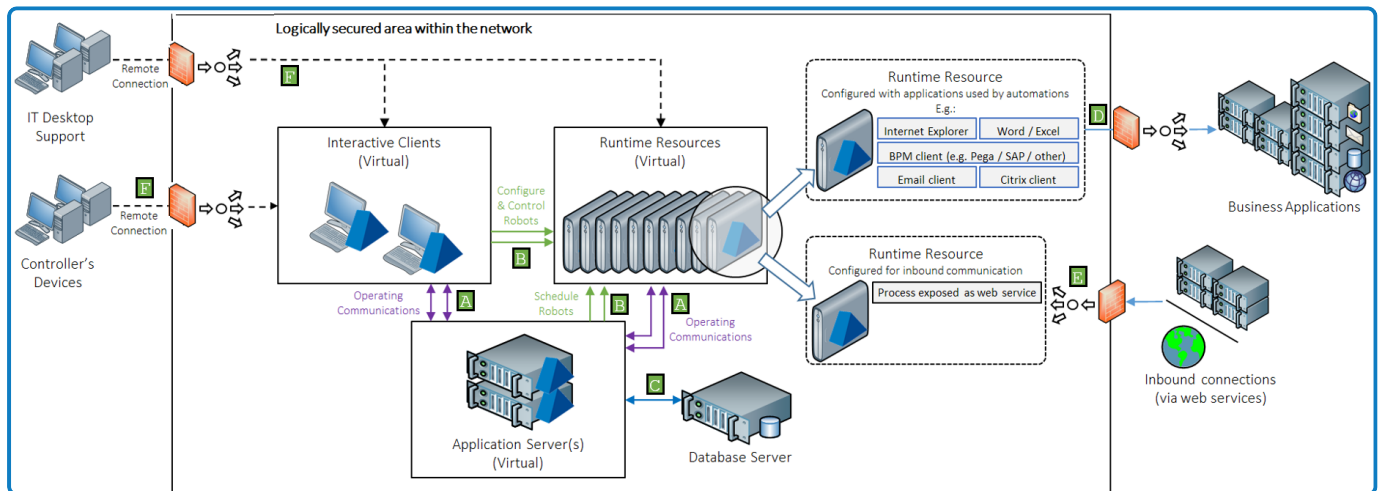


Securing Blue Prism Network Connectivity

This guide enables architects and system implementers to understand how to secure the network connectivity associated with Blue Prism. The diagram provides an overview of the common communication that occurs with the Blue Prism platform.

⚠ This guide provides details of how to configure Blue Prism in a secure enterprise environment. However, it is advised that you also consult the Robotic Operating Model (ROM) Security information on the [Blue Prism Portal](#) for recommendations of best practice.



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.
Instructional connection to runtime resources	B E	Instructions received by runtime resources. For example, 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	Runtime resources interact with business applications as part of process automations.	Dependent on the security provided by each respective third-party target application based on the nature of each connection.
Remote connectivity	F	Users controlling the platform commonly use a remote connectivity tool to access centrally deployed devices.	Leverages the security provided by the respective third-party remote connectivity tool.

Blue Prism network security

To strengthen Blue Prism network security, role-based access control (RBAC) should be utilized and only specific users, such as infrastructure administrators, should be granted access to application servers and network communication configuration. All other users should be denied access by default. Explicit allow/deny access should be configured for all users and the principle of 'Least Privilege' followed.

These controls should also extend to the users of Blue Prism, so that only those who need access to the platform are allowed and are only given the level of authority required to carry out their role, while all others are denied access by default.

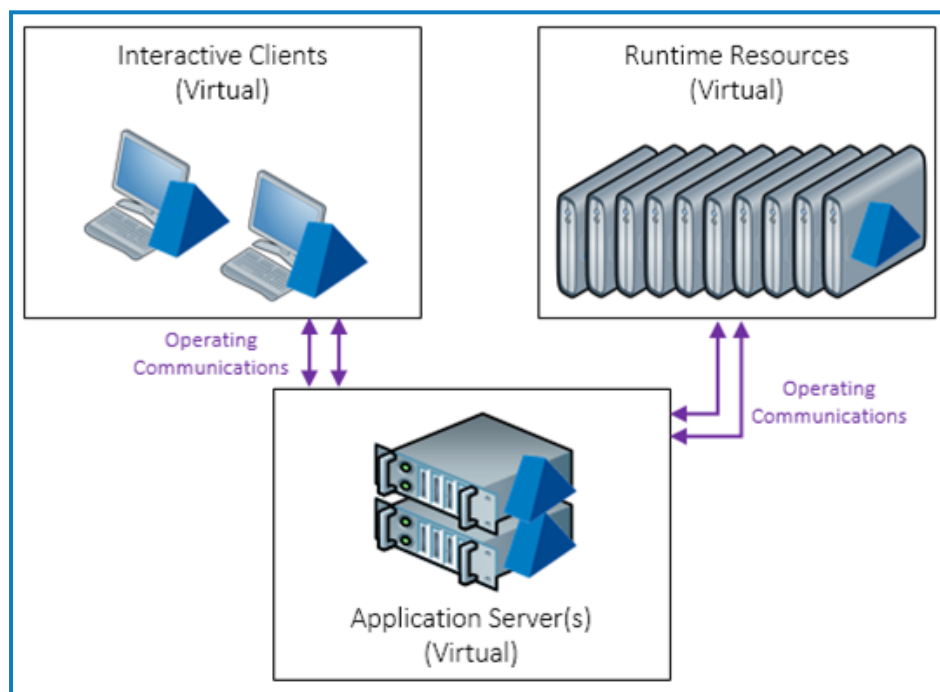
It is advised that you also consult the Robotic Operating Model (ROM) Security information on the [Blue Prism Portal](#) for recommendations of best practice.

Blue Prism connections to application server

The connections between Blue Prism devices and the application server are provided by WCF 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**.

⚠ Blue Prism application servers should not be installed on any domain or network where there is internet facing access. The Blue Prism platform should be implemented into your environment as a separate entity. This can be achieved through network segregation, for example, using jump servers for cross-domain travel, or other similar methods. It is advised that you also consult the Robotic Operating Model (ROM) Security information on the [Blue Prism Portal](#) for recommendations of best practice.

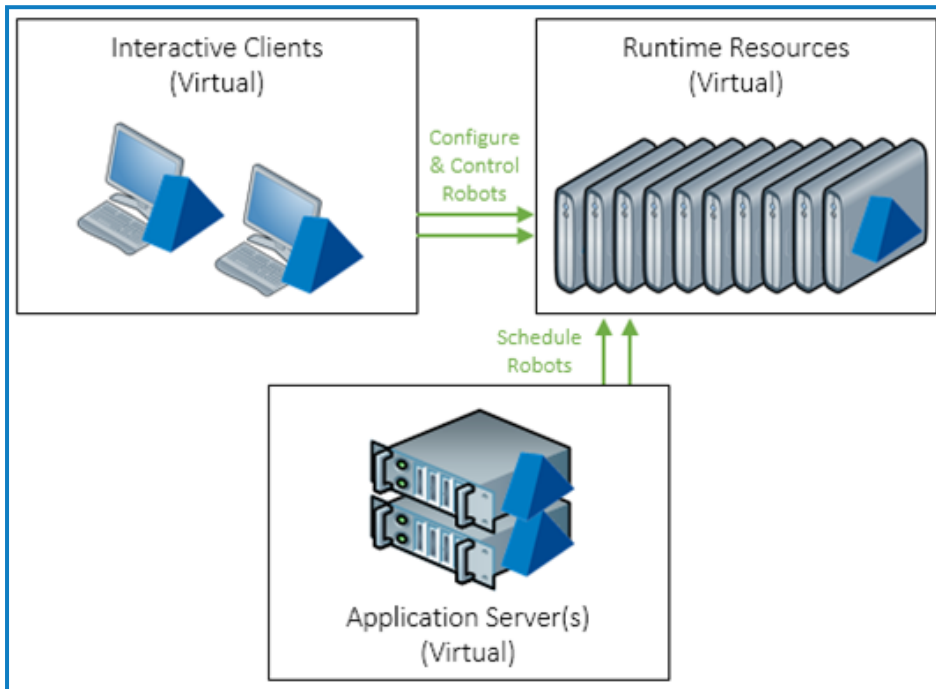


For advanced information about the controls provided by .NET Remoting, see the [Blue Prism Infrastructure Reference Guide](#).

Instructional connections to runtime resources

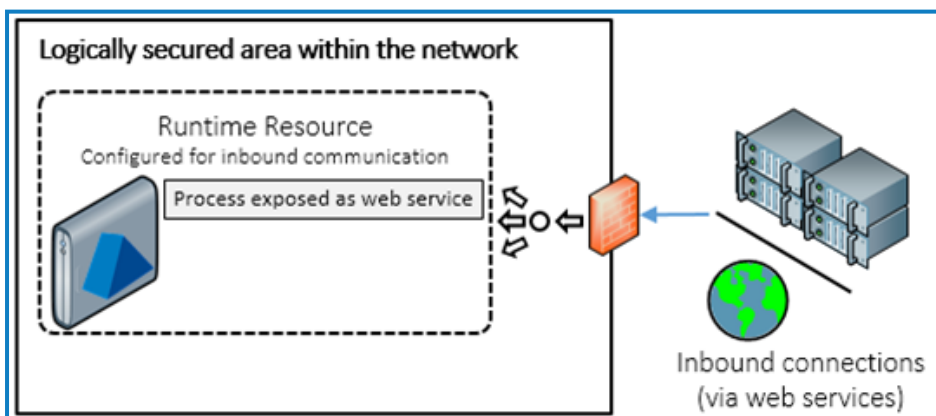
Runtime resources receive communications that can originate from a number of sources including:

- Interactive clients (for example, Control Room)
- Application server(s) (for example, Scheduler)
- External systems consuming (for example, accessing published web services)



The communication is received by a .NET service listening on a designated port (default: 8181) on each device hosting 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 require a HTTPS prefix.



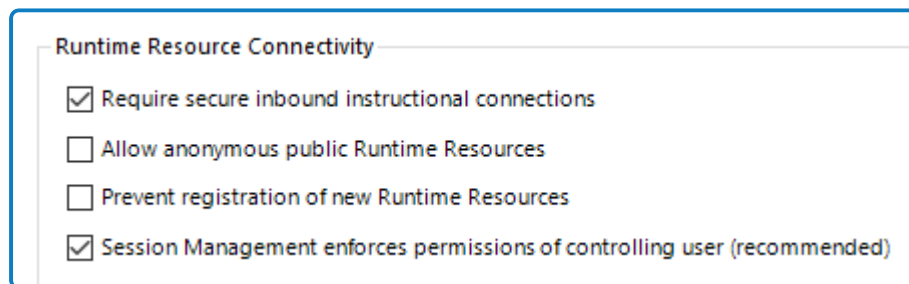
It is important to note that:

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

For more information, see [Configure a runtime resource to leverage a certificate](#).

Runtime resource connectivity

The following options are available from **System > Settings** and their behavior is described below.



Require secure inbound instructional connections

When enabled, only runtime resources that are configured to receive encrypted instructional connections are able to connect to the environment. This requires all runtime resources to be configured with an appropriate certificate. This setting ensures that all instructional connections such as from Control Room or the Scheduler are secured and also results in any objects or processes that are exposed as web services are over HTTPS.

Allow anonymous public runtime resources

When enabled, only runtime resources that are configured to explicitly authenticate using valid Blue Prism credentials are able to connect to the environment. The start-up parameters for the runtime resources must include authentication information when this setting is enabled.

Prevent registration of new runtime resources

Blue Prism can be configured to only allow runtime resources which have been previously registered in the database to establish a connection with the environment. This prevents previously unregistered devices from establishing a successful connection.

This option is only recommended for use in environments where all expected runtime resources have been registered and where the introduction of new resources can be predicted.

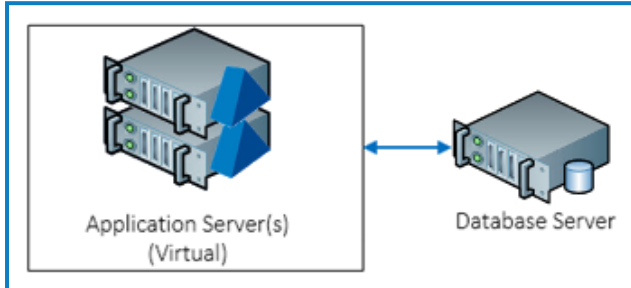
Session Management enforces permissions of controlling user (recommended)

This applies the mechanism for validating that users making requests to runtime resources have authority on the specific object, process, and resources to do so. This setting is enabled by default and disables the legacy programmatic controls: create, delete, and start, replacing them with createas, deleteas, and startas.

If this setting is disabled, the permissions of the user account used to start the runtime resource are validated, rather than the controlling user. This is not recommended and is only provided for backwards compatibility while any scripts that programmatically control the runtime resources are updated to use the recommended mechanism.

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:

- Install a verifiable server certificate on the SQL Server and configure the SQL instance to force encryption for all connections.
- 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**

Database Name	<input type="text" value="BluePrism_Prod"/>
	The name of the database to connect to
User ID	<input type="text" value="BluePrism_DBAdmin"/>
	The database user name to use
Password	<input type="password" value="••••••••"/>
	The password of the user named above
Additional SQL Connection Parameters	<input type="text" value="encrypt=true; trustservercertificate=true"/>
	Semi-colon separated parameters to add to the connection string
<input type="button" value="Test Connection"/>	

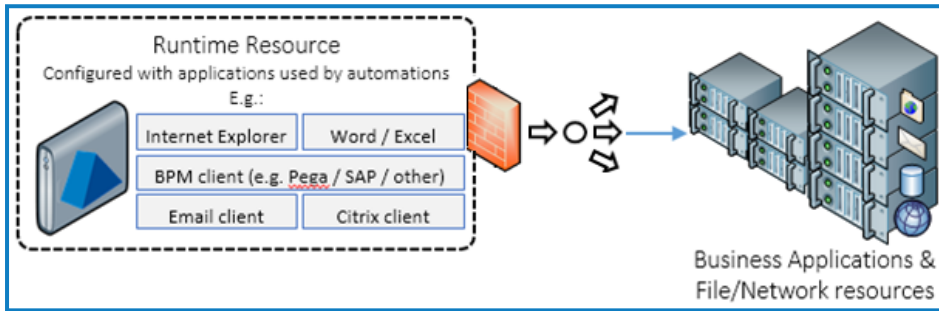
- Configure the Blue Prism database connection to specify that the connection should be encrypted and that server certificates can be trusted without further verification which allows a self-signed certificate on the SQL Server to be leveraged.
For example: **encrypt=true; trustservercertificate=true.**

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

Runtime resources connecting to target applications

Runtime resources must be configured with access to all 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 (for example, both a human and a runtime resource access a web site through use of a locally installed web browser).

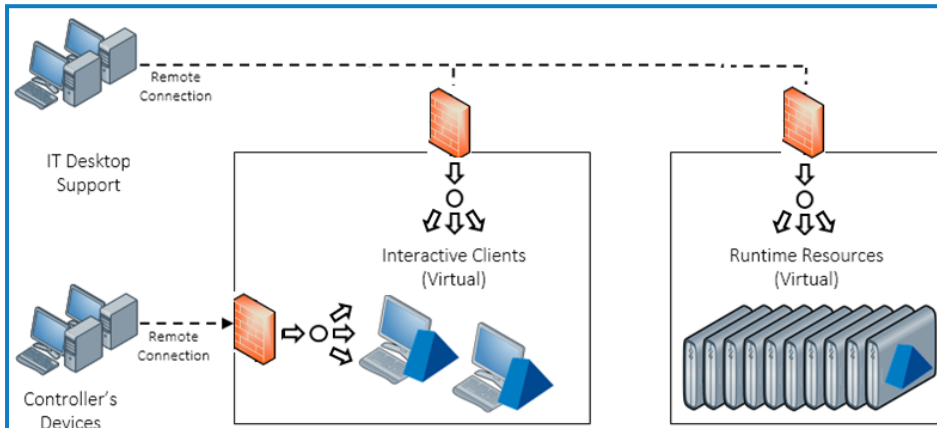
The security and encryption applied to the connections between the runtime resources and the target applications is dependent on the controls provided by each respective third-party target application.



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, or adjusting processing priorities.

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



The [Blue Prism 6 - Remote Access Tool Data Sheet](#) provides useful information for selecting an appropriate remoting technology. Additionally, it explains that Microsoft RDP is not commonly appropriate.

Configure 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 (for example, 8181).


- Identify the network names 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 influences the name.
- Generate a certificate where the common name represents all network names that may be used to address the device. This certificate must be generated by a Certificate Authority that is trusted by all connecting devices (for example, application servers, interactive clients, and where present, external systems that generate inbound connections to the platform).
- Deploy the certificate to the certificate store on the device (for example, 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.
- Identify the thumbprint of the certificate (for example, by using Microsoft Management Console and the Certificates 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.
- 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
- If using Login Agent, update the LoginAgentService.config within the ProgramData location to ensure the sslcert argument is specified.


The XML to be inserted is of the format:

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

For example:

```
<?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 (for example, 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 that require secure connections and those which do not. A central setting within Blue Prism can be used to prevent all associated Runtime Resources from accepting any instructional communications which are not encrypted.