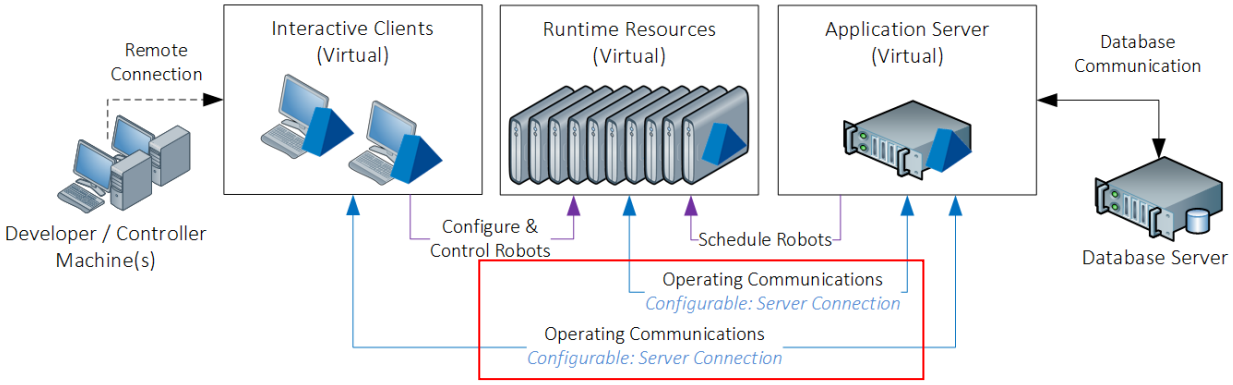
Selecting a BP Server Connection Mode

Introduction

The recommended deployment models for Blue Prism® are that all Interactive Clients and Runtime Resources are connected via a Blue Prism Application Server. The Application Server is responsible for providing a variety of functions, including marshalling connections to the Blue Prism Database.

This guide provides information about selecting the appropriate Blue Prism Server connection mode based on the intended architecture of the deployment as well as the authentication mode required for Blue Prism (i.e. Blue Prism native authentication, or Single Sign-on for Blue Prism).
As highlighted in the diagram below, this guide relates to the two connections marked **Operating Communications**.



Server Connection Mode Summary

The Server Connection Mode dictates the connection mode that must be used by clients for the server to accept the connection. The most appropriate connection mode will be determined by the target architecture of the deployment as well as the authentication mode required for Blue Prism.

- **WCF: SOAP with Message Encryption and Windows Authentication**
  Default connection mode that requires minimal configuration and supports both Blue Prism Native authentication and Single Sign-on for Blue Prism.
- **WCF: SOAP with Transport Encryption and Windows Authentication**
  Requires a manually deployed server-side certificate, and supports both Blue Prism Native authentication and Single Sign-on for Blue Prism. The use of a manually deployed certificate provides control over the encryption that will be applied to the connections.
- **WCF: SOAP with Transport Encryption**
  Requires a manually deployed server-side certificate, and only supports Blue Prism Native authentication. This mode provides support for encrypting the connections between devices across distributed environments and the use of a manually deployed certificate provides control over the encryption that will be applied to the connections.
- **.NET Remoting Secure**
  Provided only for backwards compatibitly. Uses a negotiated encryption mechanism based on the operating system and patching level of the client and server.
  Supports both Blue Prism Native authentication and Single Sign-on for Blue Prism.
- **WCF: Insecure / .NET Remoting Insecure**
  Not recommended. Provided only for troubleshooting purposes or scenarios where appropriate external controls are provided. These modes do not natively provide any communication security or encryption; and they only support Blue Prism Native authentication.

Selecting between WCF connection modes

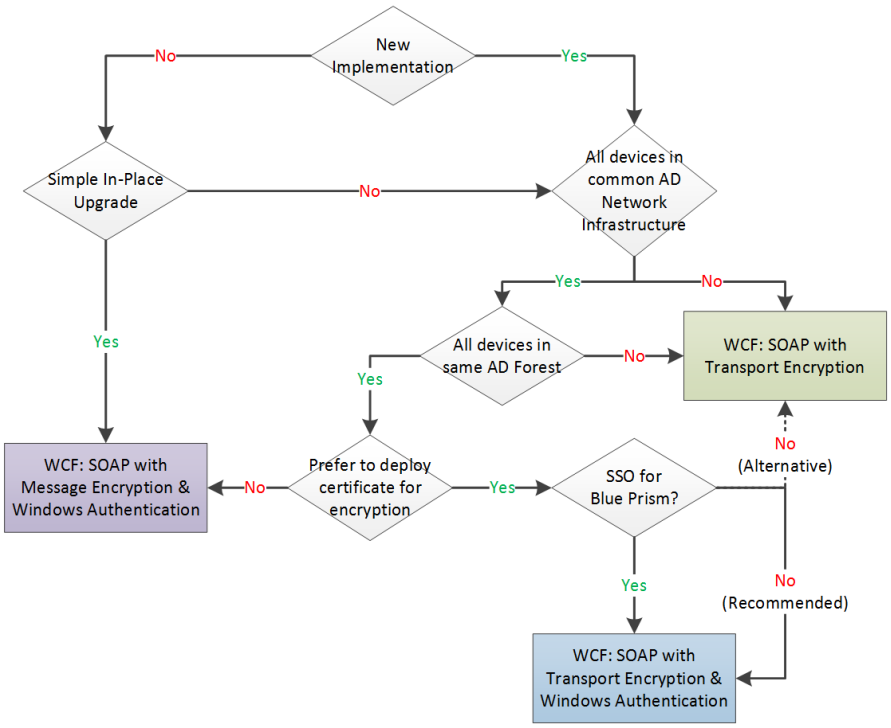
The various WCF modes provide subtly different functionality and support. It is important to consider which mode is most appropriate for a given deployment model.
The table below provides a visual comparison of the key features:

- Transport Mechanism: the type of transport mechanism used to connect the client and server end-points.
- Encrypts Data: whether the mode natively encrypts the data transmitted.
- Requires Trusts: whether the client and server must reside within a command AD network infrastructure.
- Supports SSO: whether Single Sign-on for Blue Prism is supported.
- Requires certificates: whether a server-side certificate needs to be deployed.

Mode	Transport Mechanism	Encrypts Data	Requires Trusts	Supports SSO	Requires Certificates
SOAP with Message Encryption and Windows Authentication	SOAP over HTTP	Yes	Yes	Yes	No
SOAP with Transport Encryption and Windows Authentication	SOAP over HTTPS	Yes	Yes	Yes	Yes
SOAP with Transport Encryption	SOAP over HTTPS	Yes	No	No	Yes
Insecure	SOAP over HTTP	No	No	No	No

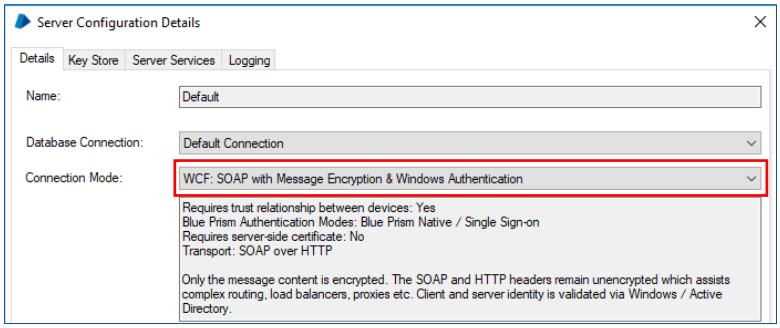
Decision tree for WCF connection modes

The decision tree can be used to identify the mode(s) that may be appropriate for a given deployment based on the target architecture.

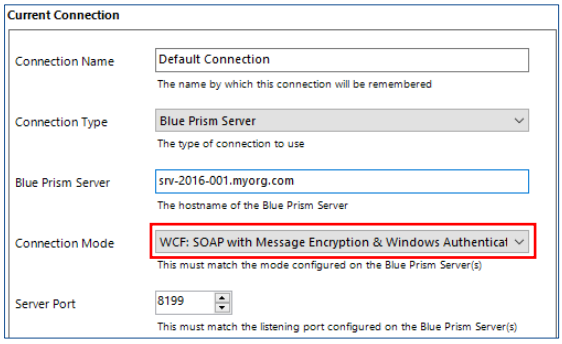


Aligning the Client and Server Connection Mode

Following the configuration of a Blue Prism Server service to receive connections on a given connection mode, it is essential that all connections to that server are made using the selected method. Connections attempted using other modes will be rejected. It is therefore important to ensure that all Blue Prism clients are configured to use the same Blue Prism Server connection mode as the Blue Prism Server that they are expected to connect to.



Server Configuration



Client Connection(s)