

Security standards for network rules

Blue Prism Cloud operates a pinhole security model. As standard, Blue Prism Cloud allows traffic into, and out from, the platform only via specifically designated ports or protocols, running to or from specific sources or destinations, such as specific IP addresses or ranges. Blue Prism Cloud does not allow an 'any' designation for source, destination, port, or protocol. For certain exceptions, any ports or any protocols can be allowed in an outbound rule, this is explained further in [Allowed rules with exception sign-off on the next page](#).

Allowed rules

The following table shows a set of examples for outbound and inbound rule(s) which Blue Prism Cloud can accept as standard.

Application name	Firewall rule name	Source (IP address)	Destination (Destination IP address)	Protocol	Port	Description	Rule acceptance comment
File Share Outboard	Allow-Outbound-FileShare	Digital Workers (Application Security Group - VWs)	172.29.51.0/24	TCP	445	Digital Workers to access the File Share	Rule allowed
FACS Outbound	Allow-Outbound-FACS	Digital Workers (Application Security Group - VWs)	172.29.51.0/24	TCP	26715	Digital Workers to access FACS Workstation	Rule allowed
HTTPS Inbound	Allow-Inbound-HTTP+S	172.29.50.0/25	10.10.51.0/27	TCP	80, 443	Customer Internal Subnet range to access HTTP+S	Rule allowed
File Share Inbound	Allow-Inbound-FileShare	172.23.50.0/26	10.28.40.0/25	TCP	445	Customer Internal Subnet range to access file shares	Rule allowed
RDP Inbound	Allow-Inbound-RDP	172.10.50.0/28	Management Server (Application Security Group - MS)	TCP	3389	Customer Internal Subnet range for RDP Access to Management Server	Rule allowed

Allowed rules with exception sign-off

In certain exceptional scenarios, Blue Prism Cloud can also allow an outbound rule from the digital worker(s) to your organization's network where any port or any protocol is specified.

 Your organization will need to define the IP address or range at your end of network connection.

Your organization accepts the risk and responsibility for the outbound traffic from the platform that it is routed via your internal network, and controlled by your network device. This risk is against Blue Prism Cloud's best practice, as it can allow undefined parameters within the connection, thereby increasing the vulnerability from a security perspective.

To use this exception, the following process needs to be followed:

1. You must raise a request for an exception through Blue Prism Cloud Support.
2. You will be provided with a risk statement to accept and sign off.
3. You must return the accepted risk statement to Blue Prism Cloud Support.

For reference, please see the statement below:

Blue Prism Cloud networking best practices leverage the pinhole methodology. Your request to create *[description of configuration]* goes against our best practices. Allowing unfettered access from the Blue Prism Cloud platform into your on-premises network is not advisable. You, the customer, are responsible for maintaining your on-premise firewall to prevent and mitigate inappropriate access that may result from these changes.

Please reply with confirmation of your request. By confirming, you acknowledge your request to *[description of configuration]* is not consistent with Blue Prism's recommended best practice when configuring and using the Blue Prism Cloud Services. Furthermore, *[Customer]* assumes all risks associated with this configuration and releases Blue Prism from any and all liability which may arise from this configuration.

The following table shows an example rule:

Application name	Firewall rule name	Source (IP address)	Destination (Destination IP address)	Protocol	Port	Description	Rule acceptance comment
HTTP+S Outbound	Allow-Outbound-HTTP+S	Digital Workers (Application Security Group - VWs)	172.29.51.0/24	Any protocol	Any port	Digital Workers to access HTTP+S	This rule will require your organization's acceptance of risk

Not allowed rules

As part of the pinhole security model, Blue Prism Cloud does not allow, as standard, rule(s) that contain an 'any' designation for ports, protocols, source, or destination. The following table shows a set of examples for outbound and inbound rule(s) which Blue Prism Cloud does not accept as standard:

Application name	Firewall rule name	Source (IP address)	Destination (Destination IP address)	Protocol	Port	Description	Rule acceptance comment
FACS	Allow-Outbound-FACS	Digital Workers (Application Security Group - VVs)	Any destination	TCP	26715	Digital Workers to access FACS Workstation	This rule is not allowed as the destination is not defined, such as an IP address or range
HTTP+S	Allow-Outbound-HTTP+S	Digital Workers (Application Security Group - VVs)	172.29.51.0/24	TCP	Any port	Digital Workers to access HTTP+S	This rule is not allowed as the port is not defined, such as a specific port or range of ports
HTTPS	Allow-Inbound-HTTP+S	172.29.50.0/25	Any destination	Any protocol	Any port	Customer Internal Subnet range to access HTTP+S	This rule is not allowed as the destination, protocol and port are not defined
File Share Inbound	Allow-Inbound-FileShare	Any source	10.28.40.0/25	TCP	445	Customer Internal Subnet range to access file shares	This rule is not allowed as the source is not defined with an IP address or range
RDP Inbound	Allow-Inbound-RDP	172.10.50.0/28	Management Server (Application Security Group - MS)	TCP	Any port	Customer Internal Subnet range for RDP Access to Management Server	This rule is not allowed as the port is not defined, such as a specific port or range of ports

 Outbound SMTP connections on TCP port 25 from virtual machines are blocked. This is a Microsoft enforced rule to protect Microsoft's Azure platform, and conform to industry standards to block unsecure SMTP traffic.