


Required access to customer platforms by Blue Prism Cloud Operations

Introduction

Blue Prism® Cloud deployments are designed to maintain a standard level of access which allows the Blue Prism Cloud Platform Operations team to fulfill the SLA obligations and Support Terms as set forth in our agreements. These access requirements must not be prohibited or blocked.

 Refer to the following documents on the Blue Prism Portal:

- [Blue Prism Cloud Service Level Agreement](#).
- [Blue Prism Cloud Support Terms](#) – see section 12.

Required Access Controls

Blue Prism Cloud deploys the following standard access controls to maintain an optimal platform and to meet the obligations set forth in our SLA agreement and Support Terms. Customers must not remove or block:

- Local administrative accounts on all virtual machines.
 - Customers can, if they wish reset the password in accordance to their own policy. Blue Prism would then change the password when the account is required for use by Blue Prism Cloud, after which the account would fall back into the customers policy.
 - This account is used to log on to the Virtual Machines to execute support requests and management activities including but not limited to; troubleshooting and verification, system and Blue Prism applications log collection, upgrade activities.
- Ability to execute remote scripting and command line interface based instructions via the cloud services provider or invoke commands leveraging the cloud services platform's guest agent, and the local system account utilizing unsigned scripts and an unrestricted execution policy, on all Blue Prism Cloud virtual machines.
 - Remote scripting and command line interface based instructions are used in actions and activities such as but not limited to; upgrades, platform changes, platform deployment and expansions, platform configuration data collection.
- Ability to connect to Blue Prism Cloud virtual machines through Remote Desktop.
 - Blue Prism Cloud engineers must utilize our secure access process including management approvals prior to being able to create a remote desktop connection to the management server.
 - RDP from outside of the platform is used as an initial step to access the Management Server only. To access other virtual machines within the platform, Blue Prism Cloud engineers would utilize RDP from the management server (within the platform).

- In some cases, internal customer policy may require enforcement of customer network controls. In these instances, amendments must be made on the customer network to allow necessary traffic for Blue Prism Cloud security and monitoring toolsets. This includes internet traffic to allow agents and monitoring tools the ability to communicate.

Removal of Access Controls

Blocking the Blue Prism Cloud required access controls, security and/or monitoring toolsets places the SLA agreement and Support Terms at risk. Both SLA and Support Terms may (at Blue Prism's discretion) be downgraded to “best effort” based on these access limitations.

Examples of changes to access controls that impact support SLA and Terms include:

- Customer side Security and/or GPO policies that block remote scripting and commands
- Customer removal of Blue Prism Cloud local admin accounts
- Restriction of internet traffic that prevents agent reporting, or command execution
- Customer access control tooling and policy that impacts Blue Prism Cloud RDP access to platform and access to ALL virtual machines.

Blue Prism Cloud Operations User Access

Any access to customer platforms by Blue Prism team members is controlled and governed. Only Blue Prism Cloud Operations and Support team members are able to request access.

As a precursor to accessing customer platforms, and as part of the mandatory access route for Blue Prism Cloud Operations and Support teams, a secure workstation recording tool is used to monitor and record system access and activity on workstations. The tool records all activities performed by Blue Prism Cloud Operations and Support teams on customer platforms. Recordings are stored for 30 days – after which, they are automatically deleted.

Initially, Blue Prism Cloud Operations and Support team members will use Active Directory accounts and multi-factor authentication to log into the Cloud Management Portal and the users with the appropriate permissions will be able to request access to the secure workstation. That access is approved by management with restrictions to level of access. The remote desktop access to the workstation itself is also time-bound. The Blue Prism Cloud Operations and Support team user then requests access to the customer platform from the secure workstation, again access is approved by management based upon a stated requirement, and only the appropriate access level for that requirement is granted. The access is again time-bound and is only allowed from a single location (the secure workstation).