Privileged Access 18.2 Available Features

Features for Access Console Users

Feature Name	Description	
Multi-Platform Support	Endpoint	Access Console
Windows	Windows XP - Windows 10 Fall Windows Server 2003 - 2016	Windows XP - Windows 10 Fall Windows Server 2003 - 2012 R2
Mac OS X	OS X 10.7 - 10.13	OS X 10.10 - 10.13
Linux	Fedora 24 - 26 RedHat Enterprise 6 - 7 CentOS 6.5 and 7 SLES 12 Ubuntu 16.04 - 17.10 Ubuntu 18.04	Fedora 24 - 26 RedHat Enterprise 6 - 7 CentOS 6.5 and 7 SLED 11 SP2 - 12 SLES 12 Ubuntu 16.04 - 18.04
Mobile Devices	N/A	Apple iOS 9.0+ (iPhone, iPad, iPod touch)
	N/A	Android 4.0+ (Phone) Android 3.0+ (Tablet) Android HTC 4.0+ Android Samsung 2.3+ (Phone/Tablet)
Virtual Machines	N/A	Citrix XenDesktop 7 VMWare View 5 VMWare Horizon 6 Citrix XenApp 6.5+
Virtual Appliances	vSphere 5.1 - 6.5 Hyper-V Server 2012 R2 Windows Server 2012 R2 with Hyper-V role enabled Hyper-V Server 2016 Azure	
Unattended Systems	Laptops, Desktops, Servers, ATMs, Kiosks, POS Systems, etc.	
Cloud Access Controls	Securely connect to and manage your cloud infrastructure, including Windows, RedHat, CentOS, and Ubuntu Linux VMs powered by AWS, Azure, VMware, and other IaaS providers. Headless Linux configurations are also supported.	
Network Devices	Routers, Switches and Devices via SSH/Telnet	
Multi-Language Support	View Bomgar applications and interfaces in English, Dutch, French, German, Italian, and Japanese. Bomgar supports international character sets.	
Access Console Toolset	Use advanced access tools to interact with remote systems.	
3D Touch Support for iOS	The Bomgar mobile access console uses iOS 3D Touch Support capabilities offered by the iPhone 6S and 6S Plus devices to start sessions faster and more efficiently. By tapping and holding the Bomgar Access Console icon on your iOS device, you can quickly access the three most viewed Jump Items, and you can seamlessly transition between active sessions.	

Feature Name	Description
Access Console	Access remote endpoints by connecting to them through the Bomgar Appliance.
Advanced Web Access	Advanced Web Access enables administrators to appropriately manage privileged access controls over assets that utilize modern web technology in a secure, scalable, and controlled manner. The auditing capability gives your organization the visibility it needs to adhere to both internal security policies and any applicable industry compliance requirements.
Annotations	While screen sharing, use annotation tools to draw on the remote screen. Drawing tools, including a free-form pen and scalable shapes, can aid in collaborating with other users.
Bomgar Access Extender	Bomgar Protocol Tunneling extends the remote connectivity and auditing capabilities of proprietary and/or 3rd party applications, such as integration control systems or custom database tools. Bomgar simplifies this complex task into a consumable process that removes the need for an intricate VPN solution.
Bomgar SUDO Manager	Shell Jump credential injection can be used in conjunction with SUDO.
Canned Scripts	Use pre-written scripts from either the Command Shell interface or the Screen Sharing interface, increasing session efficiency by automating common processes.
Command Shell	Directly access the command shell for system diagnostics, network troubleshooting, or low-bandwidth access, without screen sharing.
Credential Injection	When accessing a Windows-based Jump Client, perform credential injection into the login screen as well as the “Run As” special action. Additionally, gain access to SQL Server using credentials from your endpoint credential manager.
Custom Links	From within a session, click a button to open your browser to an associated CRM record.
Custom Special Actions	Create access console special action shortcuts for tasks specific to your environment, streamlining the effort for your team to complete repetitive tasks.
Customizable Notifications	Granularly configure which events trigger alerts in the access console and upload custom audio files.
Elevate Endpoint Client	Elevate the endpoint client to have administrative rights. Special actions can be run in the current user context or in system context.
Endpoint Credential Management	Use credentials stored in a password vault for nearly all session types. Credentials from the endpoint credential manager can be used for RDP login, Run As from special actions, performing Remote Push, and Shell Jump initiation (SSH). Install multiple endpoint credential managers on different systems to avoid downtime.
File Transfer	Transfer files to and from the remote file system.
Multi-Monitor Support	View multiple monitors on the remote desktop.
Multi-Session Support	Run multiple simultaneous sessions.
Peer-to-Peer Sessions	Network and protocol enhancements allow for direct peer-to-peer connections. A direct connection between a user and an endpoint bypasses the appliance, thus enhancing the performance of screen sharing, file transfer, and remote shell.
Privileged Web Access Console	A web-based Bomgar access console that uses HTML5 to provide access to endpoints. The privileged web access console removes the requirement of having to download and install the Bomgar access console client.

Feature Name	Description
Reboot/Auto-Reconnect[1]	Reboot and automatically reconnect to the remote computer.
Remote Registry Editor	Access and edit the remote Windows registry without requiring screen sharing.
Remote Screenshot	Capture a screenshot of the remote system.
Restrict Endpoint Interaction[2]	Disable the endpoint's mouse and keyboard input and conceal the screen to avoid interference and ensure privacy while you are working.
Smart Card Support	In a session, use authentication credentials contained on a smart card that physically resides on the user's system.
Special Actions	Access common actions such as Registry Editor, Event Viewer, System Restore, etc. Perform actions in User or System context. With the Run As special action on a Windows system, you may select credentials from an endpoint credential manager.
System Information	View in-depth system information in an easily navigable interface. Interact with services and processes and uninstall software without requiring screen sharing.
Touch ID Authentication for iOS	Authenticate to the access console via the iOS device's built-in Touch ID capability.
Virtual Pointer	Display a pointer on the remote screen, helpful when collaborating with another user.
Wake-on-LAN	Remotely access computers, even when they are turned off. Send Wake-on-LAN packets to a Jump Client host to turn on that computer, if the capability is enabled on the computer and its network.
Collaboration	Work with other users and experts to resolve support cases.
Access Invite	Invite anyone – internal or external – into a shared session with one-time, limited access.
Extended Availability	Users can be in notification mode. If invited to share a session, you will receive an email notification.
Portal Branding	Upload an image of your company logo to display on the public-facing web pages of your Privileged Access site. This logo is visible when someone accepts an access invite, goes to the public recording page, responds to an extended availability message, or responds to a request for Jump approval.
Session Sharing	Collaborate with other users by sharing a session with a team member.
Teams	Collaborate with other users who share similar skill sets or areas of expertise.
User-to-User Screen Sharing	Collaborate with other users by instantly sharing your screen with a team member.
Jump Technology	Access unattended remote desktops, servers, and other systems.
Jump Client	Access any Windows, Mac, or Linux system. Centrally manage and report on all deployed Jump Clients.
Jumpoint	Access unattended Windows systems on a network, with no pre-installed client. Connect through proxy servers by storing credentials.
Jump Zone Proxy	Use a Jumpoint as a proxy to access systems on a remote network that do not have a native internet connection.
Microsoft Remote Desktop Protocol (RDP) Integration	Conduct remote desktop protocol (RDP) sessions through Bomgar. Users can collaborate in sessions, and sessions can be automatically audited and recorded.

[1] Reboot/Auto-Reconnect is not supported on Mac computers.

[2] Restrict Endpoint Interaction is limited to disabling the mouse and keyboard on Windows 8 and above.

Feature Name	Description
Scripted Jump	Automatically start a session from an external program by initiating a Jump Item via a script.
Shell Jump	Connect to SSH/telnet-enabled network devices through a deployed Jumpoint.
VNC Integration	Connect to VNC servers through Bomgar. Users can collaborate in sessions, and sessions can be automatically audited and recorded.
Chat	Communicate easily with teammates both in and out of shared sessions.
Session Chat	Chat with other users in a shared session.
Spell Check	Catch misspellings and view suggested corrections.
Team Chat	Chat with all users on a team or with an individual.

Features for Access Console Users

Features for Managers

Feature	Description
User Management	Centrally manage users and groups.
Access Console Device Verification	Enforce the networks on which your access consoles may be used, or require two factor authentication to log into the access console.
Access Invite	Create profiles so that users can invite anyone – internal or external – into a shared session with one-time, limited access.
Administrative Dashboard	Oversee team activity, monitor users' access consoles, and join or take over sessions owned by someone else.
Application Sharing Restrictions	Limit access to specified applications on the remote Windows or Linux system by either allowing or denying a list of executables. You may also choose to allow or deny desktop access.
Configurable Login Banner	Configure a banner to display before users can log into either the /login interface or the /appliance interface. If the banner is enabled, then users attempting to access either /login or /appliance must agree to the rules and restrictions you specify before being allowed to log in.
Delegated Password Administration	Delegate the task of resetting local users' passwords to privileged users, without also granting full administrator permissions.
Group Policies	Define Bomgar user account permissions for entire groups of users. Group policies integrate easily with external directory stores to assign permissions based on your existing structures.
Inactive Session Timeout	Remove an idle user from a session after a specified time of inactivity.
Message Broadcast	Send a pop-up message to all users logged into the access console.
Multi-Factor Authentication	Gain the security of multi-factor authentication for your local and LDAP user accounts by enabling time-based, one-time passwords. When logging into Bomgar, users must provide a one-time password generated by a separate device or app, such as Bomgar Verify. Alternatively, implement native two-factor authentication using a secure second factor access code that is emailed to a user.
Multiple /appliance User Accounts	Create multiple user accounts for the /appliance interface. Set rules regarding account lockouts and password requirements.
Session Permission Policies	Customize session permissions to fit specific scenarios, not just specific users. You can change the permissions allowed in a session based on the specific endpoint being supported. Session permission policies provide flexibility in building the security model for each specific scenario.
Teams	Create teams based on skill set or experience level.
Team Collaboration	Define how multiple teams may interact.
Templates	Copy an existing security provider, session policy, or group policy to create a new object with similar settings. You also can export a session policy or group policy and import those permissions into a policy on another site.
User Accounts	Create an unlimited number of named user accounts.

Feature	Description
User Account Details Reporting	Export account information about your user accounts for auditing purposes.
User Collaboration	Define session sharing options.
User Login Schedule	Exert control over access console availability to specific users by restricting when users are able to log in.
Access Console Toolset	Equip your users with the specific access tools they need.
Canned Scripts and Custom Special Actions	Create command shell scripts and custom special actions for users to run during sessions, increasing efficiency by automating common processes.
Centralized Access Console Settings	Define the access console settings for your entire organization. Enforce settings to ensure a consistent experience.
Jump Technology	Create Jump Item Roles to easily assign sets of Jump Item permissions to users.
	Collect Jump Items into Jump Groups, granting members varying levels of access to those items.
	Set expiration dates for Jumpoints.
	Create Jump Policies to enforce when Jump Items can be accessed, if a notification of access is sent, or if approval must be granted prior to access.
	Jump Clients unable to connect to the appliance are automatically marked as lost, allowing an administrator to diagnose the reason for the lost connection. Both the lost date and the date at which a Jump Item is deleted can be configured.
	After a software update, Jump Clients update automatically. Users can see which Jump Clients have completed upgrade and can access them right away. While a Jump Client is awaiting upgrade, users can still modify properties without having to wait for the upgrade to complete.
Post Session Lock	Set the endpoint client to automatically lock or log out the remote Windows computer when an elevated session ends.
User Permissions	Restrict or enable toolset components (ex., View or Control, File Transfer, System Information, etc.)
Reports	Report on all session activity; customize, filter and export reports.
Endpoint Surface Analyzer	Know and control how critical endpoints are accessed throughout your organization. Be aware of the listening network port exposure for systems that you manage. Report and keep a running log of critical endpoint network exposure.
Policy-Based Recordings	Disable recordings at the Jump Policy level. If this option is checked, sessions started with this Jump Policy are not recorded, even if recordings are enabled on the **Configuration > Options** page. This affects screen sharing, user recordings for Protocol Tunnel Jump, and command shell recordings.
License Reporting and Auditing	Keep track of the number of endpoint licenses used. You can download a zip file containing detailed information on your Bomgar license use. This file contains a list of all Jump Items (not counting uninstalled Jump Clients), daily counts for Jump Item operations and license usage, and a summary for the Bomgar Appliance and its endpoint license usage and churn.
Reporting Permissions	Manage each user's reporting privileges.

Feature	Description
Session Forensics	Session Forensics is a powerful feature that allows you to search across all sessions based on session events. The feature empowers administrators to quickly and effectively identify critical security events, and aids in the prevention of potential security breaches, as well as evidence discovery. Searchable events include chat messages, file transfer, registry editor, session foreground window changed, and shell recordings. Successful matches in stored shell recordings automatically take the user to that point in time in the recording.
Session Reports	View details of each session. Session reports include basic session information along with links to session details, chat transcripts, and video recordings.
Session Recording Videos	Record and view annotated videos of sessions and command shell sessions, including command shell sessions.
Summary Reports	See an overview of user activity over time.
Team Activity Reports	View details of activity within a team, including login and logout times, team chats, and files shared.
GDPR Pseudonymization Support	Allow your organization to meet its GDPR initiatives with pseudonymization support in Bomgar. Bomgar administrators can respond to Right to Erasure requests by searching for specific criteria supplied by the requester. Once reviewed, the results can be anonymized with an automatically generated term or a custom replacement.

Features for Support Managers

Features for System Administrators

Feature	Description
Mass Deployment	Install Bomgar applications on multiple systems simultaneously.
Extractable Access Console	Download a mass-deployable access console to distribute to users prior to or in parallel with upgrading the Bomgar Appliance.
Mass Deployment Installers	Create mass deployable installer packages for access consoles and Jump Clients.
Mass Import of Endpoints	When creating a large number of Jump shortcuts, you can import them via a spreadsheet in the /login interface or via the API. Importing Jump Items saves time and effort over manually adding each one in the access console.
Identity Management	Define Bomgar accounts using existing data on directory servers.
LDAP/Active Directory	Use LDAP/Active Directory to manage Bomgar users.
RADIUS [Multifactor]	Use RADIUS for authentication.
Kerberos [Single Sign-on]	Use Kerberos for single sign-on.
SAML [Single Sign-on]	Use SAML with an Identity Provider to authenticate Bomgar users.
Password Managers	Use a password manager such as 1Password or LastPass to log into a mobile access console.
SCIM [Provisioning]	Use SCIM for user provisioning.
Backup and Redundancy	Monitor and back up the Bomgar Appliance.
Backup Integration Client	Schedule automatic retrieval and storage of software backups.
Appliance Failover	Define and automate redundancy and failover options.
NIC Teaming	Combine your system's physical network interface controllers (NICs) into a single logical interface, adding an additional layer of fault tolerance for your Bomgar Appliance.
Integration	Integrate Bomgar with external systems.
Change Management Workflow Integrations	Bomgar access requests can now require a Ticket ID to be entered as part of the request process. Once entered, the request is sent to your change management system where it can programmatically be denied or allowed using the Bomgar API.
Custom Links	Configure custom links to include a variable for a session's external key, pointing the URL to an associated CRM record. A user can access this link from within a session.
API	Integrate with external systems and set API permissions.
Custom Fields	Create custom API fields to gather information about the endpoint, enabling you to more deeply integrate Bomgar into your organization. You can also make fields and their values visible in the access console.
SNMP Monitoring	Monitor the Bomgar Appliance using Simple Network Management Protocol (SNMP).
Syslog Integration	Send log messages to an external syslog server.
Integration Client	Transfer session logs, session recordings, and software backups from the Bomgar Appliance to an external system. Supported systems are Windows-based file systems and Microsoft SQL server. Schedule data transfers to take place automatically.
Governance Integration New	Utilize SCIM 2.0 REST Endpoints to provision users and groups to the available security providers.

Features for System Administrators

Additional Integration Options

Additional integration options are available to Bomgar customers. Some integrations must be purchased separately from the Bomgar software. Contact Bomgar Sales for details.

Integration Option	Requirements
Service Desk/Systems Management Integrations Automate your integration of Bomgar with various service desk and systems management tools by requesting pre-packaged integration adapters, drastically reducing integration time.	ServiceNow Enterprise
CRM/Ticketing Integration Use the Bomgar API to create a simple integration between your CRM and Bomgar, allowing users to access a CRM record directly from the Bomgar access console.	Bomgar API 1.13.0+ For a list of which API versions correspond with which Bomgar software versions, see www.bomgar.com/docs/privileged-access/how-to/integrations/api/api-version-reference.htm
3rd Party Professional Integration Services Because Bomgar's API and Integration Client conform to industry protocols, it is possible for customers to contract with a third-party professional services provider to outsource integration needs.	Contact Bomgar Sales for references.
Bomgar Professional Services Contract with Bomgar for custom integration needs.	Contact Bomgar Sales.
Security Products Programmatically import Bomgar access control logs into your SIEM tool and leverage your password management solution for privileged endpoints.	HP ArcSight Thycotic Secret Server

Additional Integration Options for Bomgar