Privileged Remote Access 20.1 Available Features

Features for Access Console Users

Feature Name	Description	
Multi-Platform Support	Endpoint	Access Console
Windows	Windows XP - Windows 10 Fall Windows Server 2008 SP2- 2016	Windows 7 SP1- Windows 10 Windows Server 2008 SP2- 2012 R2
macOS	macOS 10.10 - 10.15	macOS 10.10 - 10.15
Linux	Fedora 9-30 RedHat Enterprise 5-7 CentOS 6.5 and 7 SLED 11 SP4, 12, & 15 SLES 11 SP4, 12, & 15 Ubuntu 14.04 - 19.04 Ubuntu 18.04.2 LTS	Fedora 9-30 RedHat Enterprise 5-7 CentOS 6.5 and 7 SLED 11 SP4, 12, & 15 SLES 11 SP4, 12, & 15 Ubuntu 14.04 - 19.04 Ubuntu 18.04.2 LTS
Mobile Devices	N/A	Apple iOS 13.0+
	N/A	Android 4.0+ HTC 4.0+ Samsung 4.0+ LG 4.0+
Virtual Machines	N/A	Citrix XenDesktop 7 VMWare View 5 VMWare Horizon 6 Citrix XenApp 6.5+
PRA Virtual Appliances	vSphere 5.0 - 6.7 Hyper-V Server 2012 R2 Windows Server 2012 R2 with Hyper-V role enabled Hyper-V Server 2016 Azure AWS - AMI Sharing	
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 BeyondTrust applications and interfaces in English, Dutch, French, German, Italian, Japanese, Russian, Simplified Chinese, and Traditional Chinese. BeyondTrust supports international character sets.	

Feature Name	Description
Access Console Toolset	Use advanced access tools to interact with remote systems.
3D Touch Support for iOS	The BeyondTrust 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 BeyondTrust 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.
Access Console	Access remote endpoints by connecting to them through the Secure Remote Access 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.
BeyondTrust Access Extender	BeyondTrust 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. BeyondTrust simplifies this complex task into a consumable process that removes the need for an intricate VPN solution.
BeyondTrust SUDO Manager	Shell Jump credential injection can be used in conjunction with SUDO.
BeyondTrust Vault	BeyondTrust Vault is an on-appliance credential store that enables your users to access privileged credentials and inject them directly into an endpoint. Eliminate the need for users to memorize or manually track passwords, increasing productivity and security. Add privileged credentials to Vault manually, or try the built-in Discovery tool to automatically find and protect AD and local credentials.
Cancel Access Request **ENHANCED**	Users can cancel pending Jump Access authorization requests from the Web Console, providing more flexibility and control over the authorization process, extending the existing functionality of the desktop Access Console.
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 Filtering	Protect against common user mistakes during SSH sessions by applying basic filtering to the input at the command line. For devices or appliances where agents are not practical or possible, command filtering provides an extra layer of control for administrators who need to provide access to that endpoint.
Command Shell	Directly access the command shell for system diagnostics, network troubleshooting, or low-bandwidth access, without screen sharing.
Access Console Usability Improvements	Several enhancements were made to the Access Console to improve usability, such as remembering the last security provider used for login, remembering column layouts, and showing the last time an endpoint was rebooted.
Copy and Paste with Web Jump	Users can now utilize the Copy/Paste functionality during a Web Jump session, enabling users to continue to utilize their current processes while using the Web Jump feature.
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.

Feature Name	Description
Credential Injection with Web Jump	Users can now inject a vaulted account with MFA enabled during a Web Jump Access session, enabling users to utilize the same credential injection experience they are used to using in the other access methods.
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 ENHANCED	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. You can define which Vault users can inject credentials while in a session, and which Vault users can view credentials when checked out in /login.
File Transfer	Transfer files to and from the remote file system.
Most Recently Used Jump Items	Most Recently Used Jump Items provides an easy way to find your most frequently accessed Jump Items which saves time by not having to search for frequently accessed endpoints.
Multi-Monitor Support	View multiple monitors on the remote desktop.
Multi-Session Support	Run multiple simultaneous sessions.
Password Injection with Password Safe	Password Injection with BeyondTrust Password Safe is now available for Privileged Remote Access, enabling your users to securely use passwords during access sessions with the click of a button. In addition, it provides an integrated approach to secure third-party vendor access.
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 BeyondTrust 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 BeyondTrust access console client.
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.

[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
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 Remote 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 BeyondTrust. Users can collaborate in sessions, and sessions can be automatically audited and recorded. Settings in the access console allow users to connect with the resolution best suited for their working environment.
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 BeyondTrust. 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 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.
Amazon Web Services (AWS) Deployment Option	Matching customers' needs with different deployment options, the Secure Remote Access appliance is now available in Amazon Web Services. Whether you are a new Privileged Remote Access customer or an existing customer that has an initiative to move your on-premises appliance to AWS, the new AWS deployment provides more options for your preferred deployment.
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.
Configuration APIs NEW	This set of APIs enables Privileged Remote Access administrators to automate and orchestrate administrative tasks within **/login** and the Access Console. There are specific methods exposed via an API that enable a programmatic way to create, list, update, and delete certain configuration items in Privileged Remote Access. For example, administrators can use the API to create local user accounts or delete Jump Clients that have been offline for a specified number of days.
Vault Domain Filtering ENHANCED	Users can traverse Organizational Units (OUs) within the targeted Active Directory Domain when using the Vault Discovery functionality. Vault Discovery allows administrators to discover credentials in the specified network. Administrators can then import credentials into Vault, enabling users to inject and use the discovered credentials within Privileged Remote Access sessions. Being able to traverse the OU's provides greater flexibility, while saving time and resources. Instead of running a general discovery to the domain, admins can specifically target the OU's of the teams and credentials that they wish to manage with Vault, decreasing the amount of managed credentials in Vault, and making it easier to use and control the most important credentials.
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 BeyondTrust 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.

Feature	Description
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 BeyondTrust, users must provide a one-time password generated by a separate device or authentication app.
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.
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.
Vault Bulk Rotation NEW	Users and administrators can select groups of Vault credentials and perform a password rotation on all credentials in the selected group, with just one click. This functionality provides administrators with a simple and efficient method to rotate user-selected groups of credentials or all Vault credentials at once, making it simpler to manage large numbers of credentials with Vault, while eliminating the need for time-consuming manual rotation of individual credentials.
Vault Configuration APIs NEW	List Vault accounts with the Vault Configuration API. Vault administrators can also create generic username/password and username/SSH key accounts using the API. This provides a programmatic way to onboard Vault accounts that can't be automatically discovered through Domain Discovery (Active Directory).
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.

Feature	Description
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 BeyondTrust 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 Secure Remote Access Appliance and its endpoint license usage and churn.
RDP Session Forensics NEW	A setting for RDP Jump Items provides administrators with additional logging details for RDP Jump sessions. Users can leverage this new functionality by enabling the **Session Forensics** setting in the RDP Jump Item properties. This feature captures additional session events, such as **Focused Window Changed Even** and **Mouse Click Event**. RDP Session Forensics enhances security by providing administrators with RDP Jump session details that previously were only supported in Jump Client sessions.
Reporting Permissions	Manage each user's reporting privileges.
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.

Feature	Description
Session Reports ENHANCED	View details of each session. Session reports include basic session information along with links to session details, chat transcripts, and video recordings. Also included are details regarding the Access Approver Name, Email Address, and Comments for sessions that require approval. Additionally, the session report contains the Request Reason for sessions that require users to specify a reason for their access request.
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 and consent support in BeyondTrust. BeyondTrust 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 System Administrators

Feature	Description
Mass Deployment	Install BeyondTrust 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 Secure Remote Access 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 BeyondTrust accounts using existing data on directory servers.
LDAP/Active Directory	Use LDAP/Active Directory to manage BeyondTrust users.
RADIUS [Multifactor]	Use RADIUS for authentication.
Kerberos [Single Sign-on]	Use Kerberos for single sign-on.
Let's Encrypt Support	Let's Encrypt is a service provided by the Internet Security Research Group (ISRG). It is a free, automated, and open certificate authority (CA). In /appliance, you can request and automatically renew SSL/TLS certificates used by your Secure Remote Access appliance. Let's Encrypt is configured in the SSL/TLS Configuration section in /appliance for on-premises deployments and the Appliance tab for Cloud deployments.
SAML [Single Sign-on]	Use SAML with an Identity Provider to authenticate BeyondTrust 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 Secure Remote Access Appliance.
Backup Integration Client	Schedule automatic retrieval and storage of software backups.
Appliance Failover	Define and automate redundancy and failover options.
BeyondTrust Atlas Cluster Technology	Atlas technology is now available for Secure Remote Access. With Atlas technology, organizations can manage multiple appliances across the globe from a single administration interface.
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 Secure Remote Access Appliance.
Integration	Integrate BeyondTrust with external systems.
BeyondInsight Integration: Reporting and Session Details NEW	Administrators can leverage the BeyondInsight platform for session details and reports of Privileged Remote Access sessions. This integration includes a new Dashboard view for Privileged Remote Access sessions, which users can access in the BeyondInsight interface. Administrators who utilize the existing reporting functionality of **/login** can continue to view session details, reports, and session recordings in the **/login** interface.
Change Management Workflow Integrations	BeyondTrust 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 BeyondTrust 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.

Feature	Description
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 BeyondTrust into your organization. You can also make fields and their values visible in the access console.
SNMP Monitoring	Monitor the Secure Remote Access 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 Secure Remote Access 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	Utilize SCIM 2.0 REST Endpoints to provision users and groups to the available security providers.

Additional Integration Options

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

Integration Option	Requirements
Service Desk/Systems Management Integrations Automate your integration of BeyondTrust with various service desk and systems management tools by requesting pre-packaged integration adapters, drastically reducing integration time.	Contact BeyondTrust Sales.
CRM/Ticketing Integration Use the BeyondTrust API to create a simple integration between your CRM and BeyondTrust, allowing users to access a CRM record directly from the BeyondTrust access console.	BeyondTrust API 1.19.0+ For a list of which API versions correspond with which BeyondTrust software versions, see www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/api/api-version-reference.htm
3rd Party Professional Integration Services Because BeyondTrust'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 BeyondTrust Sales for references.
BeyondTrust Professional Services Contract with BeyondTrust for custom integration needs.	Contact BeyondTrust Sales.
Security Products Programmatically import BeyondTrust access control logs into your SIEM tool and leverage your password management solution for privileged endpoints.	Contact BeyondTrust Sales.