


# Privileged Remote Access 23.1 Available Features



For more information on platform support, please see the [Features Compatibility](https://www.beyondtrust.com/docs/privileged-remote-access/updates/features-compatibility.htm) guide at <https://www.beyondtrust.com/docs/privileged-remote-access/updates/features-compatibility.htm>.

## Features for Access Console Users

### Multi-Platform Support

| Platform                     | Endpoint  | Access Console  |
|------------------------------|---|---|
| <b>Windows</b>               | Windows 7 SP1<br>Windows 10<br>Windows 11<br>Windows Server 2016 - 2022   | Windows 10<br>Windows 11  |
| <b>macOS</b>                 | macOS 10.14 - 10.15<br>macOS 11 (Big Sur) x86 and xApple<br>macOS 12 (Monterey)<br>macOS 13 (Ventura)   | macOS 10.14 - 10.15<br>macOS 11 (Big Sur) x86 and xApple<br>macOS 12 (Monterey)<br>macOS 13 (Ventura) |
|                              |  <b>Note:</b> PRA clients for macOS can run natively on Apple Silicon without relying on Rosetta 2.  |   |
| <b>Linux</b>                 | Fedora 35-36<br>RedHat Enterprise 8.5, 8.6, 9.0<br>Ubuntu 20.04 LTS, 22.04 LTS  | RedHat Enterprise 8.5, 8.6, 9.0<br>Ubuntu 20.04 LTS, 22.04 LTS  |
| <b>Mobile Devices</b>        | N/A   | Apple iOS 12.0+   |
|                              | N/A   | Android 8.0+  |
| <b>Virtual Machines</b>      | N/A   | Citrix XenDesktop 7<br>VMWare Horizon 8<br>Citrix XenApp 6.5  |
| <b>PRA Virtual Appliance</b> | vSphere 6.7 - 7.0<br>Azure<br>AWS - AMI Sharing<br>Hyper-V<br>Nutanix   |   |
| <b>Unattended Systems</b>    | Laptops, Desktops, Servers, ATMs, Kiosks, POS Systems, Raspberry Pi, etc.   |   |
| <b>Cloud Access Controls</b> | Securely connect to and manage your cloud infrastructure, including Windows, Red Hat, CentOS, and Ubuntu Linux VMs powered by AWS, Azure, VMware, and other IaaS providers. Headless Linux configurations are also supported. |   |

| Platform                            | Endpoint  | Access Console |
|-------------------------------------|---|----------------|
| <b>Cloud Access AWS KMS Support</b> | AWS Key Management Service (KMS) makes it easy to create and manage cryptographic keys and control their use in AWS services and applications. AWS KMS is a secure and resilient service that uses hardware security modules. |                |
| <b>Network Devices</b>              | Routers, Switches and Devices via SSH/Telnet  |                |
| <b>Multi-Language Support</b>       | View BeyondTrust applications and interfaces in English, Dutch, French, German, Italian, Japanese, Russian, Simplified Chinese, Polish, and Traditional Chinese. BeyondTrust supports international character sets.           |                |

## Access Console Toolset

Use advanced access tools to interact with remote systems.

| Feature Name                       | Description  |
|------------------------------------|--|
| <b>3D Touch Support for iOS</b>    | 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.  |
| <b>Access Console</b>              | Access remote endpoints by connecting to them through the B Series Appliance.  |
| <b>Advanced Web Access</b>         | 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.   |
| <b>Annotations</b>                 | 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.  |
| <b>BeyondTrust Access Extender</b> | 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.   |
| <b>BeyondTrust SUDO Manager</b>    | Shell Jump credential injection can be used in conjunction with SUDO.  |
| <b>Vault</b>                       | <p>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.</p> <p>The <b>Vault Accounts</b> tab in the Access Console enables users to check in and out Vault accounts that the administrator has defined. This enables users to leverage Vault accounts for session activity or locally on their own device, improving user experience and productivity by enabling access to Jump Items and Vault accounts from one location.</p> |
| <b>Cancel Access Request</b>       | 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.   |
| <b>Canned Scripts</b>              | Use pre-written scripts from either the Command Shell interface or the Screen Sharing interface, increasing session efficiency by automating common processes.   |

| Feature Name                              | Description  |
|---|--|
| <b>Command Filtering</b>                  | Protect against common user mistakes during SSH sessions by applying basic filtering to the input at the command line. For devices or B Series 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.   |
| <b>Command Shell</b>                      | Directly access the command shell for system diagnostics, network troubleshooting, or low-bandwidth access, without screen sharing.  |
| <b>Command Shell Display Settings</b>     | Command shell settings allow for changing the font, color, and size of the displayed text within the access console. Unicode characters are supported within a command shell.  |
| <b>Copy and Paste with Web Jump</b>       | 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.  |
| <b>Credential Injection</b>               | When accessing a Windows-based Jump Client, perform credential injection into the login screen as well as the <b>Run As</b> special action. Additionally, gain access to SQL Server using credentials from your endpoint credential manager.   |
| <b>Credential Injection with Web Jump</b> | 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.   |
| <b>Credential Store Search</b>            | Vault users can now search the credential list when Jumping into a remote system. To leverage this new functionality, a user must only begin typing an account name and the Credential Store presents the matching credentials to the user. This search functionality is limited to credentials that are available in the access console.  |
| <b>Custom Links</b>                       | From within a session, click a button to open your browser to an associated CRM record.  |
| <b>Custom Special Actions</b>             | Create access console special action shortcuts for tasks specific to your environment, streamlining the effort for your team to complete repetitive tasks.   |
| <b>Customizable Notifications</b>         | Configure which events trigger alerts in the access console and upload custom audio files.   |
| <b>Dark Mode – Desktop Access Console</b> | Users can select <b>Use Dark Mode</b> in the desktop console, letting those who prefer to avoid bright screens and reduce eye strain enjoy the updated colors and icons optimized for this theme.  |
| <b>Dark Mode – WEB Access Console</b>     | Users can select <b>Use Dark Mode</b> in the privileged web access console, letting those who prefer to avoid bright screens and reduce eye strain enjoy the updated colors and icons optimized for this theme.  |
| <b>Elevate Endpoint Client</b>            | Elevate the endpoint client to have administrative rights. Special actions can be run in the current user context or in system context.  |
| <b>Endpoint Credential Management</b>     | <p>Use credentials stored in a password vault for nearly all session types. Credentials from the endpoint credential manager can be used for RDP login, <b>Run As</b> from special actions, performing Remote Push, and Shell Jump initiation (SSH). Install multiple endpoint credential managers on different systems to avoid downtime.</p> <p>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.</p> <p>Endpoint Credential Managers can be mapped to Jump Groups. This optional functionality allows administrators using multiple disconnected credential providers, such as Managed Service Providers, to support disconnected environments while leveraging the internal credential providers on those networks for the associated Jump Group. This functionality is not standard; for more information please reach out to BeyondTrust Technical Support.</p> |
| <b>ENHANCED!</b><br><b>File Transfer</b>  | Transfer files to and from the remote file system. Appliances now can be enabled for an integration with an ICAP server for in transit file scanning adding additional layers to allowing and securing how files are transferred.  |

| Feature Name   | Description   |
|--|---|
| <b>Most Recently Used Jump Items</b>                             | 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.   |
| <b>Multi-Monitor Support</b>                                     | View multiple monitors on the remote desktop.   |
| <b>Multi-Session Support</b>                                     | Run multiple simultaneous sessions.   |
| <b>Password Injection with Password Safe</b>                     | Password Injection with BeyondTrust Password Safe is 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.  |
| <b>Peer-to-Peer Sessions</b>                                     | Network and protocol enhancements allow for direct peer-to-peer connections. A direct connection between a user and an endpoint bypasses the B Series Appliance, thus enhancing the performance of screen sharing, file transfer, and remote shell.                                 |
| <b>Privacy Screen</b>  | The Privacy Screen feature of Privileged Remote Access has been updated to support Windows 10 20H1+ and Windows 11, without the need for a secondary driver.  |
| <b>Privileged Web Access Console</b>                             | 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.   |
| <b>Privileged Web Access Console - System Information</b>        | System Information is now available for sessions within the privileged web access console. This functionality was previously limited to the desktop access console.   |
| <b>-Privileged Web Access Console Access Invite</b>              | Users can invite external users or vendors into their existing session for collaboration from the privileged web access console. This functionality was previously limited to the desktop access console.   |
| <b>Privileged Web Access Console Authentication Improvements</b> | The privileged web access console's authentication is now separate from the /login interface. This enhancement also prevents users from being logged out of /login while using the /console interface.  |
| <b>Privileged Web Access Console RDP File Transfer</b>           | Users can send and receive files in RDP sessions from the privileged web access console.  |
| <b>Reboot/Auto-Reconnect<sup>1</sup></b>                         | Reboot and automatically reconnect to the remote computer.  |
| <b>Remote Registry Editor</b>                                    | Access and edit the remote Windows registry without requiring screen sharing.   |
| <b>Remote Screenshot</b>   | Capture a screenshot of the remote system.  |
| <b>Restrict Endpoint Interaction<sup>2</sup></b>                 | Disable the endpoint's mouse and keyboard input and conceal the screen to avoid interference and ensure privacy while you are working.  |
| <b>Smart Card Support</b>  | In a session, use authentication credentials contained on a smart card that physically resides on the user's system. This feature has been enhanced to support Extended APDU.   |
| <b>Special Actions</b>   | Access common actions such as Registry Editor, Event Viewer, System Restore, etc. Perform actions in User or System context. With the <b>Run As</b> special action on a Windows system, you may select credentials from an endpoint credential manager.                             |
| <b>Syslog Access in Reports</b>                                  | Users can download the available syslog files directly from the /login interface. To download the syslog files, you must have the new permission <b>Allowed to View Syslog Reports</b> . This setting is available in both the User and Group Policy pages of the /login interface. |
| <b>System Information</b>  | View in-depth system information in an easily navigable interface. Interact with services and processes and uninstall software without requiring screen sharing.  |

<sup>1</sup>Reboot/Auto-Reconnect is not supported on Mac computers.

<sup>2</sup>Restrict Endpoint Interaction is limited to disabling the mouse and keyboard on Windows 8 and above.

| Feature Name                           | Description  |
|--|--|
| <b>Touch ID Authentication for iOS</b> | Authenticate to the access console via the iOS device's built-in Touch ID capability.  |
| <b>Virtual Pointer</b>                 | Display a pointer on the remote screen, helpful when collaborating with another user.  |
| <b>Wake-on-LAN</b>                     | 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.

| Feature Name                       | Description  |
|------------------------------------|--|
| <b>Access Invite</b>               | Invite anyone – internal or external – into a shared session with one-time, limited access.  |
| <b>Extended Availability</b>       | Users can be in notification mode. If invited to share a session, you will receive an email notification.  |
| <b>Portal Branding</b>             | 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. |
| <b>Session Sharing</b>             | Collaborate with other users by sharing a session with a team member.  |
| <b>Teams</b>                       | Collaborate with other users who share similar skill sets or areas of expertise.   |
| <b>User-to-User Screen Sharing</b> | Collaborate with other users by instantly sharing your screen with a team member.  |

## Jump Technology

Access unattended remote desktops, servers, and other systems.

| Feature Name  | Description  |
|---|--|
| <b>Atlas - Jump Client Traffic Node Connectivity</b>            | Customers using the Atlas configuration can route Jump Clients to route through an Atlas traffic node, enabling greater scalability and geospecific connections.   |
| <b>Copy Jump Items</b>  | You can copy Jump Items and assign them to multiple Jump Groups. This allows setting separate policies and group permissions without requiring additional client installations on the endpoint. Users with appropriate permissions can right click individual or multiple Jump Items to copy them. |
| <b>External Endpoint Search - Password Safe Integration</b>     | Privileged Remote Access users can search for and remotely access Password Safe-Managed RDP and Shell Jump systems that are accessible with a Jumpoint.  |
| <b>Group Policy/Jump Group Search</b>                           | The Group Policy and Jump Group lists in /login provide a search field to make it easier to find the item you're looking for.  |
| <b>Headless Linux Jump Client &amp; Jumpoint Persistence</b>    | The headless Linux Jump Client and Linux Jumpoint include an optional systemd template file to enable easier system service creation on various Linux distributions.   |
| <b>Jump Authorization Requests</b>                              | As soon as it is not needed, an active authorization request can now be revoked by the user who made the request, as can any approver.   |
| <b>Linux Jumpoint – VNC support</b>                             | The Linux Jumpoint supports VNC Jump Shortcuts.  |
| <b>Privileged Remote Access Users Can Approve Jump Requests</b> | Jump requests can be approved by selected Privileged Remote Access users in addition to emails. This allows for better tracking and auditing of who approved a given request.  |

| Feature Name   | Description   |
|--|---|
| <b>Jump Client</b>   | Access any Windows, Mac, or Linux system. Centrally manage and report on all deployed Jump Clients. Where permitted by the endpoint's platform, elevated functionality including File Transfer, Command Shell, and Registry Access can be allowed by the administrator.   |
| <b>Jump Client Headless Support for Raspberry Pi OS</b>    | Enables Raspberry Pi secure access to allow privileged users to connect to more types of unattended systems, perform administrative actions, and secure who has access to manage these devices. May work on any Raspberry Pi device that runs Raspberry Pi OS, but only certified against Pi 3B+ and Pi 4B. Supported Operating Systems: <ul style="list-style-type: none"> <li>• Raspberry Pi OS Desktop (2020-08-20-raspios-buster-armhf)</li> <li>• Raspberry Pi OS Lite (2020-08-20-raspios-buster-armhf-lite)</li> </ul>   |
| <b>Jump Client Upgrade Flexibility</b>                     | Administrators can control when their Jump Clients upgrade after upgrading their site to a newer version. Administrators can also test the upgrades of a few endpoints before rolling out the new version to the rest of their environment.   |
| <b>Jumpoint</b>  | Access unattended Windows systems on a network, with no pre-installed client. Connect through proxy servers by storing credentials. Unattended Linux systems, with a Jump Point agent, can also be accessed through RDP and SSH sessions.   |
| <b>Jump Policies Approval – Time Overlap</b>               | Jump Policy approvals can overlap, granting access to different users to the same Jump Item simultaneously.   |
| <b>Linux Jumpoint – Protocol Tunneling</b>                 | The Linux Jumpoint supports the creation of Protocol Tunnel Jump Shortcuts.   |
| <b>Bring Your Own Tools – Jump Clients (Command Shell)</b> | This functionality enables users to leverage their existing native terminal for Jump Client sessions without needing to use the solution's built-in functionality. A setting is available in the access console to configure this extension of the BYOT functionality. It is available for the access console only.   |
| <b>ENHANCED!</b><br><b>Bring Your Own Tools – RDP</b>      | <p>The Bring Your Own Tools functionality enables you to leverage your existing native RDP tool for Remote RDP Jump Shortcuts, while maintaining the benefits of the audit trail and session recordings. This setting enables Remote RDP Jump Shortcuts to include existing native RDP functionality, expanding Jump Item capabilities and improving user experience.</p> <p>We have improved security and user experience when accessing non-domain linked endpoints via RDP. This new functionality allows administrators to directly associate non-domain linked accounts discovered via Jump Clients to RDP Jump Items for that endpoint. The associated API functionality for this feature is also available, allowing administrators to more easily scale and automate the associated administrative tasks.</p> |
| <b>Bring Your Own Tools – SSH</b>                          | The Bring Your Own Tools functionality enables you to leverage your existing native SSH tool for SSH Jump Items, while maintaining the benefits of the audit trail and session recordings. This new setting enables SSH Jump Items to include existing native SSH functionality, expanding Jump Item capabilities and improving user experience. This functionality is available in the access console as a setting that can be enabled or disabled. Administrators can control access to this feature using a global setting in the /login interface located under <b>Jump &gt; Jump Items &gt; Jump Item Settings</b> .   |
| <b>RDP Multi-Monitor Support</b>                           | View multiple monitors on the remote desktop. Traditional Remote RDP Jump Shortcuts support more native RDP screen sizing and scaling of a session across multiple monitors.  |
| <b>Jump Zone Proxy</b>                                     | Use a Jumpoint as a proxy on a remote network to access systems that do not have a native Internet connection. This feature has been enhanced to allow Linux systems to be used as proxy servers. This functionality is no longer limited to Windows Jumpoints.   |

| Feature Name   | Description  |
|--|--|
| <b>Microsoft Remote Desktop Protocol (RDP) Integration</b> | 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.                  |
| <b>Protocol Tunnel Jump Item API</b>                       | The Configuration API allows the creation, deletion, and modification of Protocol Tunnel Jump Items within the system.   |
| <b>Scripted Jump</b>                                       | Automatically start a session from an external program by initiating a Jump Item via a script.   |
| <b>ENHANCED!</b><br><b>Shell Jump</b>                      | Connect to SSH/telnet-enabled network devices through a deployed Jumpoint. SSH sessions can now support in-line multi-factor prompts following the user authentication for added security to remotely access those systems requiring additional multi-factor controls for more native functionality. |
| <b>Web Jump</b>  | Web Jump has been enhanced to support Linux Jumpoints.   |
| <b>Web Jump – Multi-tab Improvements</b>                   | The multiple-tab support for Web Jump sessions has been enhanced to allow users to open additional tabs using a + click on the link. This is Ctrl+Click on Windows and Linux and ⌘ +Click on macOS. Additionally, users can specify whether the new tab opens in the foreground or background.       |
| <b>VNC Integration</b>                                     | 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.

| Feature Name        | Description   |
|---------------------|---|
| <b>Session Chat</b> | Chat with other users in a shared session.  |
| <b>Spell Check</b>  | Catch misspellings and view suggested corrections.  |
| <b>Team Chat</b>    | Chat with all users on a team or with an individual.<br><br>The Team Chat feature within the access console has been enhanced to now preserve the chat history. This allows users to pick up the conversations between other team members so that the history is available when they log back into the console. The administrator can configure a minimum time that this information is replayed in the access console. |

# Features for Managers

## User Management

Centrally manage users and groups.

| Feature Name                                       | Description  |
|--|--|
| <b>Access Console Device Verification</b>          | Enforce the networks on which your access consoles may be used, or require two factor authentication to log into the access console.   |
| <b>Access Invite</b>                               | Create profiles so that users can invite anyone – internal or external – into a shared session with one-time, limited access.  |
| <b>Administrative Dashboard</b>                    | Oversee team activity, monitor users' access consoles, and join or take over sessions owned by someone else.   |
| <b>Amazon Web Services (AWS) Deployment Option</b> | Matching customers' needs with different deployment options, the B Series 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 B Series Appliance to AWS, AWS deployment provides more options for your preferred deployment.  |
| <b>Application Sharing Restrictions</b>            | 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.   |
| <b>NEW!</b><br><b>BYOT Database Proxy</b>          | Privileged Remote Access can now proxy the Microsoft SQL Server protocol, enabling credential injection and improved auditing capabilities for Privileged Remote Access customers. There is a new setting under Protocol Tunnel Jump items for Database Tunneling.   |
| <b>NEW!</b><br><b>CLI Tool for APIs</b>            | Privileged Remote Access customers now have a simpler method to leverage and interact with the Configuration APIs using a new CLI tool provided by BeyondTrust. When bundled with our expanded documentation, this new tool makes it easier to integrate your Privileged Remote Access instance with cloud environments or other infrastructure. It is available in the API Management section of /login.  |
| <b>ENHANCED!</b><br><b>Configuration APIs</b>      | <p>This set of APIs enables Privileged Remote Access administrators to automate and orchestrate administrative tasks within <b>/login</b> 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. Other enabled use cases include tasks for managing Jump Groups, Jump Items, Vendor Groups and Users, Group Policies, Vault Accounts, Vault Account Groups, and Personal Vault Accounts.</p> <p>The Group Policy Configuration APIs (GET, POST, and PATCH) have been enhanced to allow administrators to read and set the access permission settings.</p> <p>The Configuration API documentation can be found under <b>/login &gt; Management &gt; API Configuration</b>.</p> <p>Privileged Remote Access administrators can now benefit more easily from the automation and onboarding improvements that come with the usage of existing Configuration APIs. In this release, these administrators now have prebuilt scripts that enable automation use cases more simply for specific situations, particularly Jump Item management and automation with AWS, AD, and Azure.</p> |



| Feature Name  | Description  |
|---|--|
| <b>Configurable Login Banner</b>                    | <p>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.</p> <p>The Login Agreement can be presented as part of the access console as a granular setting. Administrators can choose where this agreement is displayed, and the same message is presented when launching the access console or accessing the web administration interface.</p>  |
| <b>Delegate Password Administration</b>             | Delegate the task of resetting local users' passwords to privileged users, without also granting full administrator permissions.   |
| <b>Delegate User Management</b>                     | <p>Administrators can create a group policy type to onboard and manage vendors and other users. An assigned vendor admin for a policy can manage onboarding and offboarding of managed users for that policy.</p> <p>Administrators can define up to 50 vendor groups.</p>   |
| <b>HTTP Outbound Event Enhancements</b>             | Administrators can view the latest status of existing HTTP outbound recipients and have visibility into the number of events queued for each configured recipient.   |
| <b>Vendor Onboarding</b>                            | Improved the user interface for vendor groups, providing more visibility and a streamlined workflow for vendor management. Administrators can see users requiring immediate action, and Vendor User expiration information can be displayed for each user.   |
| <b>Vendor Onboarding - User Registration Portal</b> | Administrators can enable Vendor Users to request or sign up for access through a customizable portal page. This functionality is an addition to the <b>Vendor Groups</b> section on the <b>Users &amp; Security &gt; Vendors</b> page. Administrators can create and customize portal pages for specific vendors, allowing users to register for the access they need, when they need it. The Vendor Portal can be restricted to specific email domains as well as existing network restrictions for the vendor group. Vendor User self-registration through the Vendor Portal always requires approval for user creation by the defined administrator of the vendor group. |
| <b>Vendor Group Increase</b>                        | The vendor group limit is 100.   |
| <b>Vendors - PRA Admin Granularity</b>              | PRA administrators have the option to delegate all notifications and workflow approvals to any PRA user in an associated vendor group. PRA administrator privileges are still required to change security and configuration settings for the vendor group. Previously, all vendor groups required a full PRA administrator to be the recipient of notifications and approvals.   |
| <b>Vendor User Expiration Notification</b>          | Vendor Users can be notified of an upcoming expiration date as well as a notification of expiration. The PRA administrator or the PRA user overseeing the vendor group can extend a Vendor User's expiration date before it is expired. Additionally, vendor administrators can reactivate expired Vendor Users. User activation was limited to the PRA administrator overseeing the vendor group in previous versions.  |
| <b>Vendor User Password Reset</b>                   | Vendor Users can now receive a password reset link. Anyone who can edit the Vendor User page can click the <b>Email Password Reset Link</b> button.  |
| <b>Notification and Approval Workflows</b>          | Notification and approval workflows are available for user onboarding. This decreases manual administration of vendor management and allows faster access for new users.   |
| <b>Message Broadcast</b>                            | Send a pop-up message to all users logged into the access console.   |
| <b>Multi-Factor Authentication</b>                  | 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.   |
| <b>Multiple /appliance User Accounts</b>            | Create multiple user accounts for the /appliance interface. Set rules regarding account lockouts and password requirements. SAML can also be used to log directly into /appliance.   |

| Feature Name                                    | Description  |
|---|--|
| <b>Search Functionality in /login</b>           | Users can search for specific sections and settings throughout the administrative interface. This functionality allows easier discovery and access to various information and configuration that would have previously been more difficult to find. This functionality is available everywhere in the /login interface.  |
| <b>Scheduled Discovery</b>                      | The Vault administrator can define a preset day and time to automatically run Vault domain discovery jobs. This feature can provide continuous visibility for administrators regarding domain accounts, endpoints, and local accounts associated with discovery jobs. Accounts and endpoints found in the new discovery job can then be imported into Vault for management.  |
| <b>Service Account Management</b>               | Vault can discover and import Windows service accounts for management. Administrators can leverage this new discovery functionality to gain visibility into the service accounts in the domains managed by Vault, as well as the descriptions and associated services for the accounts.  |
| <b>Session Permission Policies</b>              | 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.   |
| <b>Session Policies for All Jump Items</b>      | Administrators can assign session policies to all Jump Items, enabling additional granularity for Jump Item policies.  |
| <b>Teams</b>                                    | Create teams based on skill set or experience level.   |
| <b>Team Collaboration</b>                       | Define how multiple teams may interact.  |
| <b>Templates</b>                                | 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.   |
| <b>User Accounts</b>                            | Create an unlimited number of named user accounts.   |
| <b>User Account Details Reporting</b>           | Export account information about your user accounts for auditing purposes.   |
| <b>User Collaboration</b>                       | Define session sharing options.  |
| <b>User Login Schedule</b>                      | Exert control over access console availability to specific users by restricting when users are able to log in.   |
| <b>Vault Account Groups</b>                     | Vault administrators can organize Vault accounts into account groups, providing a better management experience for Vault admins. Admins can assign account groups to group policies, rather than only individual Vault accounts, and Vault accounts can be assigned to an account group during the import process.   |
| <b>Vault Accounts associated with Endpoints</b> | Vault accounts are automatically associated with endpoints, providing a better user experience when injecting credentials into Privileged Remote Access sessions. Admins use the Vault Discovery and Import functions to bring accounts and endpoints under Vault management. Once under Vault management, the credential-to-endpoint association automatically occurs for the relevant Jump Items. Users are presented with the associated Vault accounts when injecting during session initiation. |
| <b>Vault – Auto Update Stale Data</b>           | Discovery jobs can automatically detect and update stale read-only attributes on accounts, endpoints, or services that have been onboarded into Vault.   |
| <b>Vault Bulk Rotation</b>                      | 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.           |

| Feature Name   | Description   |
|--|---|
| <b>Vault – Account Policies</b>                          | Vault account policies can be assigned to Vault accounts or Vault account groups, providing administrators with additional granularity regarding Vault account settings. Vault account policies can define whether the account is included in scheduled password rotation, the account's maximum password age, automatic rotation after check-in, and whether the account is available for simultaneous checkout.   |
| <b>Vault - Account Rotation Azure AD Domain Services</b> | Privileged Remote Access enables organizations to properly manage and inject credentials managed by Azure AD Domain Services. Administrators can now leverage the Vault to rotate account credentials managed by Azure Active Directory Domain Services. This new functionality is an addition to the existing ability to discover credentials managed by Azure AD Domain Services.   |
| <b>Vault Configuration APIs</b>                          | 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).  |
| <b>Vault - Configurable Columns</b>                      | Vault administrators can customize and configure the columns which are shown on the Vault Accounts page.  |
| <b>Vault-Configurable Password Length</b>                | Vault administrators can define the password length requirements for Windows local, domain, and Azure AD accounts currently managed by Vault. Administrators can define these requirements by navigating to the <b>/login &gt; Vault &gt; Options</b> page.   |
| <b>Vault Domain Filtering</b>                            | 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 OUs 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. |
| <b>Vault – Jump Item Association</b>                     | Administrators can limit the credentials available for injection in a Jump session by associating Vault accounts and Vault account groups with Jump Items. Associations can be direct or dynamic with the help of match criteria based on Jump Item properties.   |
| <b>Vault Personal Accounts</b>                           | All Privileged Remote Access users can create private generic accounts in their own private Vault. This functionality allows users to manage their own Vault accounts privately for use during Privileged Remote Access sessions. The maximum number of personal accounts per user is 50.   |
| <b>Vault - Search Discovery Results</b>                  | The <b>Vault Discovery Results</b> page in <b>/login</b> provides a search field to make it easier to find the endpoint, account, or service you're looking for. The discovery results also include two additional endpoint columns: <b>Distinguished Name</b> and <b>Operating System</b> name.  |
| <b>Vault Scalability</b>                                 | Vault can now import, rotate, and manage up to 60,000 accounts.   |
| <b>Vault - Windows Service Account Rotation</b>          | Vault can rotate Windows service accounts (local and domain). In addition to account rotation, Vault can restart any services associated with the service account. This feature provides Vault administrators with visibility and control over Windows services and service accounts, improving their security posture and quality of service. Service cluster password rotation is not supported in this release.  |
| <b>Jump Client Discovery and Rotation</b>                | Jump Clients can perform discovery and rotation of local credentials (Windows only). This functionality allows administrators to manage machines individually and set who has access to those machines without the need to set up a local or shared account on the remote system. This feature is to complement the use of Jumpoints in the network for domain-based rotation but also allow for more singular control over smaller groups of machines.   |

## Access Console Toolset

Equip your users with the specific access tools they need.

| Feature Name                                     | Description  |
|--|--|
| <b>Canned Scripts and Custom Special Actions</b> | Create command shell scripts and custom special actions for users to run during sessions, increasing efficiency by automating common processes.  |
| <b>Centralized Access Console Settings</b>       | Define the access console settings for your entire organization. Enforce settings to ensure a consistent experience.   |
| <b>Jump Technology</b>                           | 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 B Series 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. |
| <b>Post Session Lock</b>                         | Set the endpoint client to automatically lock or log out the remote Windows computer when an elevated session ends.  |
| <b>User Permissions</b>                          | 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.

| Feature Name                          | Description   |
|---------------------------------------|---|
| <b>Report Sort Order Changed</b>      | Items listed on the Reporting pages are ordered from newest to oldest.  |
| <b>Endpoint Surface Analyzer</b>      | 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.  |
| <b>Policy-Based Recordings</b>        | 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 <b>Configuration &gt; Options</b> page. This affects screen sharing, user recordings for Protocol Tunnel Jump, and command shell recordings.   |
| <b>License Reporting and Auditing</b> | 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 B Series Appliance and its endpoint license usage and churn. |

| Feature Name                             | Description  |
|--|--|
| <b>RDP Session Forensics</b>             | A setting for RDP Jump Items provides administrators with additional logging details for RDP Jump sessions. Users can leverage this functionality by enabling the <b>Session Forensics</b> setting in the RDP Jump Item properties. This feature captures additional session events, such as <b>Focused Window Changed Even</b> and <b>Mouse Click Event</b> . RDP Session Forensics enhances security by providing administrators with RDP Jump session details that previously were only supported in Jump Client sessions.                                  |
| <b>Reporting Permissions</b>             | Manage each user's reporting privileges.   |
| <b>Jump Item Reporting</b>               | Administrators can now leverage a new report type specific to the administration and configuration of Jump Items. For example, reports can be run for historical Jump Item events, such as creation, deletion, copy, move, etc.  |
| <b>Session Forensics</b>                 | 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. |
| <b>Session Reports</b>                   | 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.  |
| <b>Session Recording Videos</b>          | Record and view annotated videos of sessions and command shell sessions, including command shell sessions.   |
| <b>Summary Reports</b>                   | See an overview of user activity over time.  |
| <b>Team Activity Reports</b>             | View details of activity within a team, including login and logout times, team chats, and files shared.  |
| <b>GDPR Pseudonymization Support</b>     | 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.  |
| <b>Session Anonymization Improvement</b> | Administrators using the anonymization functionality can now run additional anonymization jobs on the same session reports in case a detail was missed in the initial effort. This helps administrators honor a user's right to erasure requests more quickly.   |

## Updates

| Feature Name  | Description   |
|---|---|
| <b>ENHANCED!</b><br><b>Auto-Update Process for Hardened Linux</b> | During the update process, clients now download the update to their own install location and begin the update from there. By executing from the same location, the proper permissions are already in place and allow the update process for hardened Linux systems to be more seamless for Privileged Remote Access administrators. |

## Features for System Administrators

### Mass Deployment

Install BeyondTrust applications on multiple systems simultaneously.

| Feature Name                      | Description   |
|-----------------------------------|---|
| <b>Extractable Access Console</b> | Download a mass-deployable access console to distribute to users prior to or in parallel with upgrading the B Series Appliance.   |
| <b>Mass Deployment Installers</b> | Create mass deployable installer packages for access consoles and Jump Clients.   |
| <b>Mass Import of Endpoints</b>   | 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.

| Feature Name                      | Description  |
|-----------------------------------|--|
| <b>LDAP/Active Directory</b>      | Use LDAP/Active Directory to manage BeyondTrust users.   |
| <b>RADIUS [Multifactor]</b>       | Use RADIUS for authentication.   |
| <b>Kerberos [Single Sign-on]</b>  | Use Kerberos for single sign-on.   |
| <b>Let's Encrypt Support</b>      | 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 B Series 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. |
| <b>SAML [Single Sign-on]</b>      | Use SAML with an Identity Provider to authenticate BeyondTrust users. Admins can set launching the /login or the /console interfaces after using an IdP. SAML can also be used to log directly into /appliance.  |
| <b>SAML Security Provider API</b> | The Configuration API can enable updates to the available group names within a SAML provider. This facilitates automating the onboarding of new user groups.   |
| <b>Password Managers</b>          | Use a password manager such as 1Password or LastPass to log into a mobile access console.  |
| <b>SCIM [Provisioning]</b>        | Use SCIM for user provisioning.  |
| <b>TLS 1.3 Protocol</b>           | Transportation Layer Security protocol 1.3 is used to ensure secure communication between browsers and webservers. Symmetric cryptography is used to encrypt the data transmitted. The keys are uniquely generated for each connection and are based on a shared secret negotiated at the beginning of the session.  |
| <b>Outbound Proxy Support</b>     | A proxy server can be used to send outbound events to a single destination rather than multiple applications. This feature allows administrators to control dataflow from B Series Appliances for outbound events and APIs. This feature allows you to test the connection to verify your settings are correct.  |

## Backup and Redundancy

Monitor and back up the B Series Appliance

| Feature Name                                | Description   |
|---|---|
| <b>Backup Integration Client</b>            | Schedule automatic retrieval and storage of software backups.   |
| <b>B Series Appliance Failover</b>          | Define and automate redundancy and failover options.  |
| <b>BeyondTrust Atlas Cluster Technology</b> | Atlas technology is available for Privileged Remote Access. With Atlas technology, organizations can manage multiple B Series Appliances across the globe from a single administration interface. |
| <b>NIC Teaming</b>                          | Combine your system's physical network interface controllers (NICs) into a single logical interface, adding an additional layer of fault tolerance for your B Series Appliance.                   |

## Appliance Migration

Migrate from one appliance type to another.

| Feature Name                    | Description  |
|---------------------------------|--|
| <b>Appliance Migration Tool</b> | Administrators can use the application migration tool to move from an on-premises appliance to a cloud-based appliance, as well as migrate from a physical appliance deployment to a different deployment type. This functionality can be set up under the new section at <b>/login &gt; Management &gt; Software &gt; Site Migration</b> . It allows API-based communication between the appliances and supports migrations from version 19.2.4 to current. |

## Integration

Integrate BeyondTrust with external systems.

| Feature Name  | Description  |
|---|--|
| <b>BeyondInsight Integration: Reporting and Session Details</b> | Administrators can leverage the BeyondInsight platform for session details and reports of Privileged Remote Access sessions. This integration includes a Dashboard view for Privileged Remote Access sessions, which users can access in the BeyondInsight interface. Administrators who utilize the existing reporting functionality of <b>/login</b> can continue to view session details, reports, and session recordings in the <b>/login</b> interface. |
| <b>DevOps Secrets Safe Integration</b>                          | This functionality allows for an integration to DevOps Secrets Safe in the <b>/appliance</b> interface, expanding the options for storing secrets off the appliance for expanded security.   |
| <b>Change Management Workflow Integrations</b>                  | 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.   |
| <b>Custom Links</b>   | 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.  |
| <b>API</b>  | Integrate with external systems and set API permissions.   |
| <b>Custom Fields</b>  | 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.  |

| Feature Name  | Description  |
|---|--|
| <b>Password Safe Integration – External Jump Group – Multiple Jumpoints</b> | The External Jump Groups integration with BeyondTrust Password Safe provides users with a simple workflow to extend access capabilities to systems managed by BeyondTrust Password Safe via RDP and SSH. Administrators can define multiple Jumpoints for flexible access to managed systems within Password Safe. It also includes reporting enhancements related to credential injection events. |
| <b>SNMP Monitoring</b>  | Monitor the B Series Appliance using Simple Network Management Protocol (SNMP). You can set up SNMP v3 and v2 on the /appliance interface.   |
| <b>Syslog Integration</b>   | Send log messages to an external syslog server.  |
| <b>Integration Client</b>   | Transfer session logs, session recordings, and software backups from the B Series Appliance to an external system. Supported systems are Windows-based file systems and Microsoft SQL server. Schedule data transfers to take place automatically.   |
| <b>Governance Integration</b>   | Utilize SCIM 2.0 REST Endpoints to provision users and groups to the available security providers.   |

**i** For more information on DevOps Secrets Safe Integration, please see [Secure Secrets Management for Enterprise DevOps](https://www.beyondtrust.com/resources/datasheets/devops-secrets-safe) at <https://www.beyondtrust.com/resources/datasheets/devops-secrets-safe>.



## 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  |
|--|---|
| <b>Service Desk/Systems Management Integrations</b><br>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.  |
| <b>CRM/Ticketing Integration</b><br>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+<br>For a list of which API versions correspond with which BeyondTrust software versions, see <a href="http://www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/api/api-version-reference.htm">www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/api/api-version-reference.htm</a> |
| <b>3rd Party Professional Integration Services</b><br>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.   |
| <b>BeyondTrust Professional Services</b><br>Contract with BeyondTrust for custom integration needs.  | Contact BeyondTrust Sales.  |
| <b>Security Products</b><br>Programmatically import BeyondTrust access control logs into your SIEM tool and leverage your password management solution for privileged endpoints.   | Contact BeyondTrust Sales.  |