



BeyondTrust

Remote Support 23.3 Cloud Admin Guide

Table of Contents

Remote Support Administrative Interface	6
Log in to the Administrative Interface	7
Search /login Administrative Interface	9
App Switcher	9
Status	10
Information: View BeyondTrust Remote Support Software Details	10
Representatives: View Logged In Reps and Send Messages	12
What's New: See Software Release Details	13
User Menu	14
Consoles and Downloads: Launch the Web Rep Console and Download the Desktop Representative Console	15
Consoles and Downloads: Download Virtual Smart Card Installer	17
My Account: Change Email and User Settings, and Enable Extended Availability Mode	18
My Account: Change Password Settings and add Passwordless Authenticators	20
Configuration	22
Options: Manage Session Queuing Options, Record Sessions, Set Up Text Messaging	22
Issues: Manage Support Issues	25
Support Teams: Group Representatives into Teams	27
Skills: Route Issues to Representatives	32
Access Sponsors: Create Groups of Privileged Users	34
Support Buttons: Deploy Support Buttons for Quick Session Start	35
Custom Fields: Create and Modify Fields for Public Portal Issue Submissions	41
MS Teams: Enable and Customize the Microsoft Teams Integration	42
MS Teams: Service Now Virtual Agent Integration	43
Jump	53
Jump Clients: Manage Settings and Install Jump Clients for Unattended Access	53
Jump Groups: Configure Which Representatives Can Access Which Jump Items	62
Jump Policies: Set Schedules for Jump Clients	64
Jump Item Roles: Configure Permission Sets for Jump Items	66
Jumpoint: Set Up Unattended Access to a Network	69
Jump Items: Import Shortcuts to Jump Items	71

Vault for Remote Support	79
Discovery: Discover Accounts, Endpoints, and Services in a Domain	79
Accounts: Manage Vault Accounts	83
Vault Account Groups: Add and Manage Account Groups	93
Account Policies: Add and Manage Account Policies	96
Endpoints: Manage Discovered Endpoints	98
Services: View and Manage Discovered Services	99
Domains: Add and Manage Domains	100
Options: Configure Global Default Account Policy Settings and Password Length for Account Rotation	102
Rep Console	104
Rep Console Settings: Manage Default Rep Console Settings	104
Custom Links: Add URL Shortcuts to the Representative Console	110
Canned Messages: Create Messages for Chat	111
Canned Scripts: Create Scripts for Screen Sharing or Command Shell Sessions	113
Special Actions: Create Custom Special Actions	116
Users and Security	118
Users: Add User Permissions for a Representative or Admin	118
User Accounts for Password Reset: Allow Reps to Administer User Passwords	136
Rep Invite: Create Profiles to Invite External Representatives to Sessions	138
Security Providers: Enable LDAP, Active Directory, RADIUS, Kerberos, SAML for Reps, and SAML for Public Portals	139
Session Policies: Set Session Permission and Prompting Rules	155
Group Policies: Apply User Permissions to Groups of Users	164
Kerberos Keytab: Manage the Kerberos Keytab	184
Licensing: Assign Representatives to License Pools	185
Reports	187
Support: Report on Session Activity	187
Presentation: Report on Presentation Activity	190
Licensing: Report on Peak License Usage	191
Vault: Report on Vault Account and Rep Activity	192
Compliance: Anonymize Data to Meet Compliance Standards	193
Jump Item: Report on Jump Item Activity	195
Syslog: Download Report Containing All Syslog Files on the Appliance	197

Public Portals	198
Public Sites: Customize the Support Portal	198
Schedule: Set Public Portal Open Hours	203
HTML Templates: Customize the Web Interface	205
Customer Notices: Create Messages for the Customer Notification System	206
File Store: Upload Resource Files	208
iOS Configuration Profiles: Add Apple Configuration Profiles	209
Surveys: Enable the Customer Exit Survey and Representative Survey	212
Customer Client: Modify the Invitation Email, Display Options, Connection Options	216
Presentation: Modify the Invitation Emails and Display Options	225
Localization	228
Real-Time Chat: Translate Chat Messages Between Rep and Customer	228
Languages: Manage Installed Languages	231
Search: View Customized Text in Enabled Languages	232
Management	233
Software: Download a Backup, Upgrade Software	233
Security: Manage Security Settings	237
Site Configuration: Enable Prerequisite Login Agreement	246
Email Configuration: Configure the Software to Send Emails	247
Outbound Events: Set Events to Trigger Messages	255
API Configuration: Enable the XML API and Configure Custom Fields	258
Support: Contact BeyondTrust Technical Support	261
Remote Support Cloud Appliance	262
Status > Basics: View Cloud Appliance Details	263
Storage > Encryption: Encrypt Session Data	264
Security > Certificates: Create and Manage TLS Certificates	265
Create a Custom Hostname for Your BeyondTrust Cloud Site	270
Security > TLS Configuration: Choose TLS Ciphers	272
Security > Appliance Administration: Set Syslog over TLS	273
Security > Email Configuration: Configure the Cloud Appliance to Send Email Alerts	274
Configure via SMTP	274
Configure via OAuth2 for Microsoft Azure AD	275
Configure via OAuth2 for Google	278

Security > Secret Store: Store and Access Secrets on the Cloud Appliance	283
Updates: Check for Update Availability and Install Software in BeyondTrust Cloud	285
Ports and Firewalls	286
Disclaimers, Licensing Restrictions, and Tech Support	287

Remote Support Administrative Interface

This guide offers a detailed overview of **/login** and is designed to help you administer BeyondTrust users and your BeyondTrust software. The BeyondTrust Appliance B Series serves as the central point of administration and management for your BeyondTrust software and enables you to log in from anywhere that has internet access in order to download the representative console.

Use this guide only after an administrator has performed the initial setup and configuration of the B Series Appliance as detailed in the [BeyondTrust Appliance B Series Hardware Installation Guide](http://www.beyondtrust.com/docs/remote-support/getting-started/deployment/hardware) at www.beyondtrust.com/docs/remote-support/getting-started/deployment/hardware. Once BeyondTrust is properly installed, you can begin supporting customers immediately. Should you need any assistance, please contact BeyondTrust Technical Support at www.beyondtrust.com/support.

Log in to the Administrative Interface

Login

The user administrative interface enables administrators to create user accounts and configure software settings. Log in to the user administrative interface by going to your B Series Appliance's URL followed by `/login`.

Although your B Series Appliance's URL can be any registered DNS, it will most likely be a subdomain of your company's primary domain, for example, `access.example.com/login`.

Default Username: **admin**

Default Password: **password**

Because BeyondTrust Remote Support is licensed by concurrent users, you can set up as many accounts as you need, each with unique usernames and passwords.



Note: When logging into the administrative interface for the first time, BeyondTrust Cloud administrators are required to click through and accept the BeyondTrust EULA.

If two-factor authentication is enabled for your account, enter the code from the authenticator app.



Note: If more than one language is enabled for your site, select the language you want to use from the dropdown menu. You can also change the language of your choice after logging in to the admin site.



For more information on 2FA, please see [How to Use Two Factor Authentication with BeyondTrust Remote Support at `www.beyondtrust.com/docs/remote-support/how-to/2-factor-authentication/`](https://www.beyondtrust.com/docs/remote-support/how-to/2-factor-authentication/).

Use Passwordless Login

FIDO2-certified authenticators can be used to securely log in to the desktop representative console, web rep console, and the `/login` administrative interface without entering your password. You can register up to 10 authenticators.

If passwordless login has been enabled, **Authenticate Using** may default to **Passwordless FIDO2**, or it can be selected. The exact process for passwordless login depends on the type of device and manufacturer.

You can enable passwordless login and set the default authentication after logging into the `/login` administrative interface, by navigating to **Management > Security**, and then registering passwordless authenticators at **My Account > Security**.



Note: Passwordless login for the desktop representative console on macOS or Linux systems is supported only for roaming authenticators (such as the YubiKey hardware security keys). Platform or integrated authenticators (such as Face ID and fingerprint scanners) are not supported for the desktop representative console login when using macOS or Linux systems.

Use Integrated Browser Authentication

If Kerberos has been properly configured for single sign-on, you can click the link to use integrated browser authentication, allowing you to enter directly into the web interface without requiring you to enter your credentials.



For more information, please see *Kerberos Server for Single Sign-On* at <https://www.beyondtrust.com/docs/remote-support/how-to/integrations/security-providers/kerberos/index.htm>.

Forgot your password?

If password reset has been enabled from the **/login > Management > Security** page and the SMTP server has been set up for your site, this link is visible. To reset your password, click the link, enter and confirm your email address, and then click **Send**. If there is more than one user sharing the same email address, you are required to confirm your username. You will receive an email with a link that takes you back to the login page. On the login screen, enter and confirm your new password, and then click **Change Password**.

Login Agreement

Administrators may restrict access to the login screen by enabling a prerequisite login agreement that must be confirmed before the login screen is displayed. The login agreement can be enabled and customized from the **/login > Management > Site Configuration** page.

Search /login Administrative Interface

From every page within Remote Support /login, you can search for settings and features within the administrative interface using the search bar in the top-right corner. This feature searches for static text, including titles and labels, within the entirety of /login. Search results are listed in a dropdown, grouped by page. You can click any of the items in the listed search results to be taken directly to the page within /login. Titles and labels specific to your search are highlighted on the page.

**Note:**

- *Search results include only areas within /login where you have permissions.*
- *User-entered items are not searched.*
- *Search supports all languages supported by /login — all languages are searched and indexed.*

App Switcher


If you have BeyondTrust Identity Security Insights, you can connect Remote Support and other BeyondTrust cloud applications, and then switch between applications without needing to re-enter credentials. The App Switcher menu appears in the same place in all applications: in the upper right. In Remote Support, the menu appears between the **Search** field and the **User Menu**.

Click the menu for a list of connected applications, and click the desired application. There can be more than one instance of an application, except for Identity Security Insights.

The menu does not appear if there are no connected applications. The menu is automatically removed if all connected applications are removed, or if it has not been used for 60 days. Re-entering credentials may be necessary in some circumstances, depending on the login configuration of the different applications. Configuration of this feature is managed in BeyondTrust Identity Security Insights.

Status

Information: View BeyondTrust Remote Support Software Details

 Status	INFORMATION
------------------------------------------------------------------------------------------	-------------

Site Status

The main page of the BeyondTrust Remote Support /login interface gives an overview of your B Series Appliance statistics. When contacting BeyondTrust Technical Support for software updates or troubleshooting purposes, you may be asked to email a screenshot of this page.

Time Zone

An administrator can select the appropriate time zone from a dropdown, setting the correct date and time of the B Series Appliance for the selected region.

Total Jump Clients Allowed

Review the total number of active and passive Jump Clients which are allowed on your system. If you need more Jump Clients, contact BeyondTrust Technical Support.

Full Support Licenses

View the number of licenses available on your BeyondTrust Appliance B Series. If you need more licenses, contact BeyondTrust Sales.

Chat Support Licenses

View the number of chat licenses available on your BeyondTrust Appliance B Series. If you need more licenses, contact BeyondTrust Sales.

License Packs

Lists installed one-time and recurring license packs, providing their counts, active status, start and end dates, and recurring status. Customers who have subscription based licenses may add on multiple individual license packs that either expire (burst) or reactivate (seasonal).



Note: Active license packs are included in the count of full support licenses; however, they cannot be assigned to license pools.

Restart Remote Support Software

You can restart the BeyondTrust software remotely. Restart your software only if instructed to do so by BeyondTrust Technical Support.

Client Software

This is the hostname to which BeyondTrust client software connects. If the hostname attempted by the client software needs to change, notify BeyondTrust Technical Support of the needed changes so that Support can build a software update.

Connected Clients

View the number and type of BeyondTrust software clients that are connected to your BeyondTrust Appliance B Series.

ECM Clients

View the number of BeyondTrust Endpoint Credential Managers (ECM) that are connected to your BeyondTrust Appliance B Series. Also, view information about the location and connection time for each ECM.

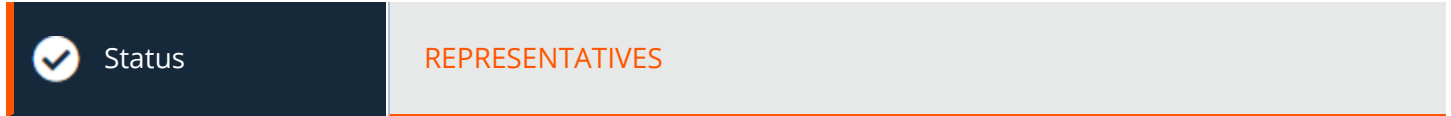


Note: To ensure optimal up-time, administrators can install up to five ECMs on different Windows machines to communicate with the same site on the BeyondTrust Appliance B Series. A list of the ECMs connected to the B Series Appliance site can be found at **/login > Status > Information > ECM Clients**.



Note: When multiple ECMs are connected to a BeyondTrust site, the B Series Appliance routes requests to the ECM that has been connected to the B Series Appliance the longest.

Representatives: View Logged In Reps and Send Messages



Logged In Representatives

View a list of representatives logged into the representative console, along with their login time and whether they are running support or presentation sessions.

Terminate Session

You can terminate a representative's connection to the representative console.

Send Message to Representatives

Send a message to all logged-in representatives via a pop-up window in the representative console.

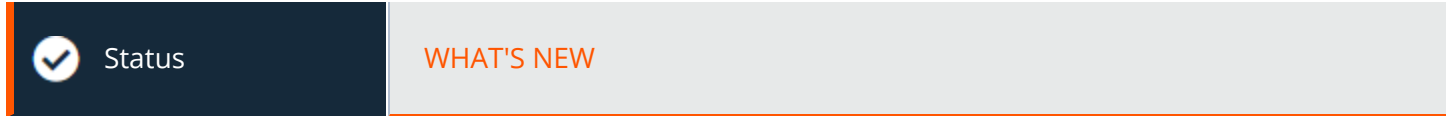
Extended Availability Representatives

View representatives who have extended availability mode enabled. Enabling extended availability mode does consume a license.

Disable Extended Availability

You may disable a representative's extended availability in order to free up a license.

What's New: See Software Release Details



What's New

Easily review BeyondTrust features and capabilities newly available with each release. Learning about new features as they become available can help you make the most of your BeyondTrust deployment.

The first time you log in to the administrative interface after a BeyondTrust software upgrade, the **What's New** page will receive focus, alerting you that new features are available on your site. You must be an administrator to view this tab.

The information shown on the **What's New** page is also available to representatives in the representative console, from the **Help > About** menu.



For more information, please see [Updates and Features Lists](https://www.beyondtrust.com/docs/remote-support/updates/index.htm) at <https://www.beyondtrust.com/docs/remote-support/updates/index.htm>.

User Menu

The user dropdown menu, located in the upper-right corner of the screen, offers access to a few key features from anywhere on the admin site. Click the user icon to view the logged-in user name and email address, and available links and options.

Log Out: Click to log out of the /login administrative interface. This does not log you out of any consoles. Those must be logged out separately.

Change Email Settings, Display Names, or Photo: This is a link to **My Account > Profile**.

Change Password: This is a link to **My Account > Security**.

Launch Web Rep Console: This gives you convenient access to the web rep console from anywhere in /login.

Download Representative Console: This gives you a quick link to download the web rep console.

Enable Extended Availability: Click to enable this feature in the representative console. Once enabled, this option switches to **Disable**, and can be clicked again to disable this feature.

Language: Displays the current language. If more than one language is enabled for your site, select the language you want to use from the dropdown menu. This language is also applied to the web rep console.

Color Scheme: Select your preferred color scheme for the /login administrative interface. You can switch between **Light** and **Dark** modes, or **System**, which uses whatever mode is selected for your system.



For more information on these features, please see the following:

- ["My Account: Change Email and User Settings, and Enable Extended Availability Mode" on page 18](#)
- ["Change Your Password" on page 20](#)
- [Use Extended Availability to Stay Accessible when Not Logged In at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/extended-availability.htm>](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/extended-availability.htm)

Consoles and Downloads: Launch the Web Rep Console and Download the Desktop Representative Console



Consoles & Downloads

REP CONSOLE

Web Rep Console

Launch the web rep console, a web-based representative console. Access remote systems from your browser without having to download and install the full representative console.

Representative Console

Choose Platform

Choose the operating system on which you wish to install this software. This dropdown defaults to the appropriate installer detected for your operating system.



For more information, please see [Web Rep Console Guide](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/web/index.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/web/index.htm>.

Download Representative Console

Download the BeyondTrust representative console installer in order to provide remote support.

To install the representative console without displaying any windows, spinners, errors, or other visible alerts, append **/S** to the end of the EXE command, though for mass deployment, BeyondTrust recommends using the MSI installer.

For system administrators who need to deploy the console installer to a large number of systems, the Microsoft Installer can be used with your systems management tool of choice. In your command prompt, when composing the command to install the console using an MSI, change to the directory where the MSI was downloaded and enter the command included on the **My Account** page.

You can include optional parameters for your MSI installation.

- **INSTALLDIR=** accepts any valid directory path where you want the console to install.
- **RUNATSTARTUP=** accepts **0** (default) or **1**. If you enter 1, the console runs each time the computer starts up.
- **ALLUSERS=** accepts **""** (default) or **1**. **""** is the default value. This attribute is only needed when specifying per-machine installs.

ALLUSERS="" results in a single user install. This forces the representative console to install in the same context that is being used to run the MSI installation. This is not ideal if Local System is used to run the installation, as is often the case with mass deployment tools. There is no way to target the install to a specified user via MSI parameters, so if you are deploying the MSI through an automated deployment system while using the single user install flag, the deployment system must run the MSI installation in the context of the same user who is expected to log in to the console.

- **SHOULD AUTOUPDATE=1** If you install for only the current user, you can choose to have the console automatically update each time the site is upgraded by entering a value of **1**; a value of **0** (default) does not auto-update, and the console will need to be manually reinstalled when the site is upgraded. If you install the console for all users, it does not auto-update.
- **/quiet** or **/q** runs the installer without displaying any windows, spinners, error, or other visible alerts.



Note: If you use **ALLUSERS=1** with **SHOULD AUTOUPDATE=1**, the representative console should not be expected to auto-update. If you use **SHOULD AUTOUPDATE=1** without **ALLUSERS=1**, the representative console should auto-update without requiring any credentials beyond those of the BeyondTrust user and the active Windows user. No admin credentials are necessary.



IMPORTANT!

When a representative console is installed via MSI, there is still some information that needs to be retrieved from the B Series Appliance. During the initial login, a token is provided to the representative console which is used to request software updates. If no user logs into the representative console before the B Series Appliance is upgraded, or if an MSI from a previous version is used to install the representative console, the console fails to update because it does not have the necessary token. If this occurs, the following error displays

"Error communicating with server while updating software. Please upgrade your software by downloading it from the web site. (1.1gws)"

For this reason, if representative consoles are mass deployed via MSI, please take the necessary steps to ensure users authenticate with their consoles at least once prior to any updates being installed on the BeyondTrust Appliance B Series.



For more information, please see the following:

- [BeyondTrust Representative Console](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/index.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/index.htm>
- [Mass Deploying BeyondTrust Software to Macs](https://www.beyondtrust.com/docs/remote-support/how-to/mass-deploy-mac/index.htm) at <https://www.beyondtrust.com/docs/remote-support/how-to/mass-deploy-mac/index.htm>

Consoles and Downloads: Download Virtual Smart Card Installer



Consoles & Downloads

DRIVERS

Download Virtual Smart Card Installer

A virtual smart card allows you to authenticate to a remote system using a smart card on your local system.



Note: This feature is not supported for ARM-based Windows systems.

Choose Windows Architecture

Choose the operating system on which you wish to install this software. This dropdown defaults to the appropriate installer detected for your operating system.

If you need to use a local smart card on a remote system being supported, you must install the BeyondTrust Remote Support Virtual Smart Card driver on both the representative and customer systems. Download and distribute the appropriate Virtual Smart Card Representative (VSC Representative Installer) driver to all representatives within your support center who require remote smart card functionality. The driver can be installed manually or via a software deployment tool. Once the driver is installed, it creates a service: Remote Support VSC Representative Service.

My Account: Change Email and User Settings, and Enable Extended Availability Mode



My Account

PROFILE

Change Your Email Settings

Email Address

Set the email address to where email notifications are sent, such as password resets or extended availability mode alerts.

Preferred Email Language

If more than one language is enabled on this site, set the language in which to send emails.

Password

Enter the password for your /login account, not your email password.

Change Your Display Names

Private Display Name

Your name as displayed in all internal communications between representatives, on chat transcript reports, team activity reports, and so forth.

Public Display Name

Your name as displayed to customers.



Note: By default, these two fields are in sync, so anything you type in the **Private Display Name** field is copied automatically to the **Public Display Name** field. To change your public display name, type in the name you want your customers to see. To put the fields back in sync, simply make them identical again.

Change Your Photo

Change or delete the photo that is associated with your account. This photo is displayed in the customer client chat window and in the /login administrative interface. The image used must be in .png or .jpeg format, no more than 1 MiB in size, and with a minimum 80x80

pixel size. Click **Choose File** to select an image. Once the selected file name is displayed, click **Upload** to use it, or **Cancel**, if you do not wish to keep the image you just selected. If the image selected has the correct dimensions, a message displays indicating the upload was successful.

Extended Availability Mode

Enable or Disable

Enable or disable Extended Availability Mode by clicking the **Enable/Disable** button. Extended Availability Mode allows you to receive email invitations from other users requesting to share a session when you are not logged into the console.



For more information, please see [Use Extended Availability to Stay Accessible When Not Logged In](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/extended-availability.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/extended-availability.htm>.



For more information, please see [Customer Client: Support Session Interface](https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-support-interface.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-support-interface.htm>.

My Account: Change Password Settings and add Passwordless Authenticators



My Account

SECURITY

Change Your Password

BeyondTrust recommends changing your password regularly.

Username, Current Password, New Password

Verify that you are logged into the account for which you want to change the password, and then enter your current password. Create and confirm a new password for your account. The password may be set to whatever you choose, as long as the string complies with the defined policy set on the **/login > Management > Security** page.

Passwordless Authenticators

This feature is available only if enabled under **Management > Security**. The default authentication method is also selected here. Either authentication method can be selected when logging in.

FIDO2-certified authenticators can be used to securely log in to the representative console (Windows only), web rep console, and /login without entering your password. You can register up to 10 authenticators.

Only FIDO2-certified hardware authenticators that perform user verification – biometrics or PIN – are allowed.

There are two types of authenticators:

Roaming

Roaming authenticators, or cross-platform security keys like YubiKeys, are FIDO2-certified external devices that use biometrics or a PIN for user verification. They can be used instead of your password when logging into the representative console (Windows only), web rep console, and /login on any machine and supported operating system that allows the use of external FIDO2 authenticators.

Platform

Platform authenticators such as Windows Hello or macOS Touch ID are integrated, FIDO2-certified biometric authenticators. These authenticators are tied to the machine where you registered the authenticator. They can be used instead of your password when logging into the representative console (Windows only), web rep console, and /login. On macOS and Linux, platform authenticators can only be used in the browser they were registered in. Incognito or private browsing windows cannot be used for authentication.

Register and Manage Authenticators

The screen shows all registered authenticators, with their name, type, registration date and time, and last usage date and time. Registered authenticators can be edited or deleted by selecting them and clicking the appropriate icon.

To register a new authenticator, click **Register**.

Select **Roaming** or **Platform**, depending on your requirements.

Enter an **Authenticator Name**. Choose a name to help you identify this authenticator when viewing all registered authenticators in a list.

Enter your BeyondTrust Remote Support **Account Password**. This is the password used to log in with *Username & Password* authentication, not the authenticator's PIN or passcode. It is used to confirm your identity before allowing a new authenticator to be registered to your account. It is not associated with the authenticator in any way.

Click **Continue**.

The remaining steps for registering your authenticator depend on the type, the manufacturer, the browser, and the OS.



Tip: The browser or OS can timeout the authentication if there are delays responding to prompts.

Set up authenticators (for example, YubiKey or Windows Hello) within the OS before registering the authenticator. It is important to follow the manufacturer's directions. For example, YubiKey Bio requires a PIN at setup, even for fingerprint authentication.

Windows Hello can be set up using a PIN and a fingerprint. If this is done, either method can be used, regardless of how it is registered.

Registering an authenticator might fail if the browser and OS combination does not support passwordless authentication. For example, Firefox 110 does not support passwordless authentication for Linux and macOS. A warning message is usually generated in these cases.



Note: Authenticators usually record failed authentication attempts, and may lock. They must be reset following the manufacturer's instructions. A failed authentication at the authentication device does not count as a failed login to the BeyondTrust site, as the incorrect information is not submitted to the site.

Two Factor Authentication

Activate Two Factor Authentication

Activate two-factor authentication (2FA) to increase the level of security for users accessing /login and the BeyondTrust representative console. Click **Activate Two Factor Authentication** and scan the displayed QR code using an authenticator app, such as Google Authenticator. Alternatively, you can manually enter the alphanumeric code displayed below the QR code into your authenticator app.

The app automatically registers the account and begins providing you with codes. Enter your password and the code generated by the authenticator app you selected, and then click **Activate**. Please note that each code is valid for 60 seconds, after which time a new code is generated. Once you log in, you have the option to switch to a different authenticator app or disable 2FA.



Note: If 2FA was deployed by your administrator, you do not have the option to disable it.



For more information on 2FA, please see [How to Use Two Factor Authentication with BeyondTrust Remote Support at www.beyondtrust.com/docs/remote-support/how-to/2-factor-authentication/](https://www.beyondtrust.com/docs/remote-support/how-to/2-factor-authentication/).

Configuration

Options: Manage Session Queuing Options, Record Sessions, Set Up Text Messaging



Configuration

OPTIONS

Support Session Queuing Options

Require Closed Sessions on Logout or Quit

If you check **Require Closed Sessions on Logout or Quit**, then users will be unable to log out of the console if they currently have any session tabs open.

Session Fallback Rules

There are five rules for when a representative's connection to a session is lost or terminated: (1) If the session is shared, it transfers to the representative who has been sharing the session the longest. If not shared, it transfers to (2) the last queue it was in, (3) the queue in which it entered, or (4) a designated fallback queue. This second set of rules can be turned on or off for normal sessions (attended), Jump sessions (unattended), or both. (5) Finally, if no representative is found, the session ends.



Note: If the session is in a persistent queue, the above logic does not apply. You can enable persistent queues from the **Configuration > Support Teams** page.

Enable Rules 2, 3, and 4 for Normal Sessions and/or Jump Sessions

Turn on the middle three fallback rules for customer-initiated sessions and/or unattended sessions.



For more information, please see [View Support Sessions in Queue](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/queues.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/queues.htm>.

Equilibrium Options

Show Session Information in All Alert Dialog Boxes

When a session is assigned, the representative receives an alert. If **Show Session Information in All Alert Dialog Boxes** is checked, all session assignment alerts display the support request information.



For more information, please see [Accept a Session to Start Support](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/accepting-a-session.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/accepting-a-session.htm>.

Support Session Logging Options

Enable Screen Sharing / Show My Screen Recording / Command Shell Recording

Choose if screen sharing sessions, Show My Screen sessions, and/or command shell sessions should be automatically recorded as videos.

Screen Sharing / Show My Screen Recording Resolution / Command Shell Recording Resolution

Set the resolution at which to view session recording playback.



Note: All recordings are saved in raw format; the resolution size affects playback only.

Enable Automatic Logging of System Information

Choose if system information should be automatically pulled from the remote system at the beginning of the session to be available later in the session report details.

System Information Logging for Mobile Platforms

When supporting mobile platforms, choose **Standard** to pull a small set of data or **Extended** to pull all available information.



Note: These site-wide settings may be overridden by public site settings and customer preference, as configured on the **Public Portals > Customer Client** page.

Presentation Logging Options

Enable Screen Sharing Recording

Choose if presentations should be automatically recorded as videos.



Note: When you start a presentation and are waiting for attendees to join, the recording will not begin until the first attendee has joined the presentation. If no one joins the presentation, a session recording will not be created.

Screen Sharing Recording Resolution

Set the resolution at which to view presentation recording playback.

Peer to Peer Options

Enabling peer-to-peer connections for support sessions enhances the performance of the Screen Sharing, File Transfer, and Command Shell support tools. Additional firewall configuration might be required to successfully establish peer to peer connections.

Disabled

Disables Peer to Peer connections. To enable this feature, you must choose a server to negotiate the session. When screen sharing, file transfer, or remote shell is detected, the peer-to-peer connection is attempted. If successful, this creates a direct connection between the representative and the client systems, while still sending a second data stream to the B Series Appliance for auditing purposes. If for any reason a peer-to-peer connection cannot be established, the session traffic defaults to the B Series Appliance-mediated connection.

Use BeyondTrust Hosted Peer-to-Peer Server

This is the default setting. BeyondTrust clients attempt to reach a peer-to-peer connection through the server hosted by BeyondTrust. This requires that your BeyondTrust clients can make outbound UDP 3478 connection requests to `stun.bt3ng.com`. This setting is expected to work in most situations.

Invitation Email Options

Enable client-side emails for support and presentation invitations

When enabled, representatives can send support and presentation invitation emails from a local email client, such as Outlook. These emails are sent using the representative's email account. The representative can view and modify the email, if desired.

Enable server-side emails for support invitations

If enabled, representatives can send support invitation emails from the B Series Appliance rather than their local email client. A dialog prompts the representative to specify the email recipient. The representative cannot preview or modify the subject or body of the email. The email address from which server-side emails are sent can be customized per portal from the **Public Portals > Customer Client** page, or the address specified on the **Management > Email Configuration** page can be used.

i For more information see [Generate a Session Key to Start a Support Session at https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/session-keys.htm](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/session-keys.htm).

SMS Gateway

SMS Gateway URL

Enter a secure SMS gateway URL from your ISP or third-party gateway provider to give representatives the option to send support access keys via SMS text messages. Send support messages via SMS to a mobile device from within the representative console. SMS messages sent in this manner to other mobile devices will still receive a session link. The SMS communication is not logged in the B Series Appliance.

Issues: Manage Support Issues



Configuration

ISSUES

Support Issues

Create support issues to streamline your customers' experience when requesting support on the public portal. Issues created may be configured to appear on the dropdown menu of the issue submission form and comprise a list of the support problems most likely to be experienced by your customers.

Since support issues need to be routed to support teams, you need to create teams before you create support issues.



For more information, please see [Configure Team Settings](https://www.beyondtrust.com/docs/remote-support/how-to/equilibrium/configure-team-settings.htm) at <https://www.beyondtrust.com/docs/remote-support/how-to/equilibrium/configure-team-settings.htm>.



For more information, please see [Assign Skills to Issues](https://www.beyondtrust.com/docs/remote-support/how-to/equilibrium/assign-skills-issue.htm) at <https://www.beyondtrust.com/docs/remote-support/how-to/equilibrium/assign-skills-issue.htm>.

Add New Support Issue, Edit, Delete

Create a new issue, modify an existing issue, or remove an existing issue.

Add or Edit a Support Issue

Description

Add a brief description of an issue you expect to see as a support ticket. If the issue submission form is enabled, this description is visible to customers and is used to help representatives quickly determine what type of problem the customer is experiencing. The description may also be visible to representatives requesting help from within a support session.

Code Name

Set a code name for integration purposes. If you do not set a code name, one is created automatically.

Route To

Use the **Route To** dropdown menu to have this issue routed to a specific team.

Priority

Set the issue's priority to **High**, **Medium**, or **Low**, depending on how you want the issue to be handled by the system. The default is **Medium**.

Allow representatives to request help for this support issue

Next, check the box if you want to allow representatives to request help for this support issue while in a session. If checked, the issue is listed in the **Request Help** flyout window of the representative console when the **Session Sharing** option is selected.

Needed Skills

Issues can be associated with the skills needed to best resolve them. Skills can be **More Preferred**, **Less Preferred**, or **Ignored**, depending on the level of knowledge required to resolve a given issue. This will determine how support requests are routed and handled by the system.

Support Teams: Group Representatives into Teams



Configuration

SUPPORT TEAMS

Manage Support Teams

Grouping support representatives into teams aids efficiency by assigning leadership within groups of representatives as well as by helping to direct customers to the representative best suited to solve a given problem. In the representative console, each team appears as a separate queue for waiting support sessions.

Add New Team, Edit, Delete

Create a new team, modify an existing team, or remove an existing team. Deleting a team does not delete those user accounts, only the team with which they are associated.

Add or Edit Support Team

Team Name

Create a unique name to help identify this team.

Code Name

Set a code name for integration purposes. If you do not set a code name, one is created automatically.

Comments

Add comments to help identify the purpose of this team.

Persistent Queue

If this option is checked, support sessions remain in this queue even if no representatives are available. A session in this queue remains in the queue indefinitely until a representative or API operation handles the session. This option provides additional flexibility for custom session routing management.

Group Policies

Note any group policies which assign members to this team. Click the link to go to the **Group Policies** page to verify or assign policy members.

Portal Access

Representatives can only access portals where their team has been granted access. Portal access options allow members of a team to access all portals or selected portals.

Allow members of this team to access all portals

Check the box to allow members of the selected team access to all portals.

Allow members of this team to access the following portals

This option only appears if the option above is not checked. Check the box for each portal that members of the selected team can access. Members of a team should always have access to the default portal. Unchecked portals do not appear on the list of portal options when the representative generates a session key.

Team Members

Search for users to add to this team. You can set each member's role as a **Team Member**, **Team Lead**, or **Team Manager**. These roles play a significant part in the **Dashboard** feature of the representative console.

In the table below, view existing team members. You can filter the view by entering a string in the **Filter by name** text box. You can also edit a member's settings or delete a member from the team.

To add a group of users to a team, go to **Users & Security > Group Policies** and assign that group to one or more teams in a given role.



Note: You may see some users whose **Edit** and **Delete** options are disabled. This occurs when a user is added via group policy.

You can click the group policy link to modify the policy as a whole. Any changes made to the group policy apply to all members of that policy.

You also can add the individual to the team, overriding their settings as defined elsewhere.

Equilibrium Settings

Manage automatic session routing for this team using equilibrium.

Routing Algorithm

If this is set to **Least Busy**, a session in this queue is assigned to the least busy representative who is available to take sessions from this queue. If it is set to **Skills Match, Least Busy**, then if a session has needed skills marked and is in this queue, that session is assigned to the representative with the best skills match who is available to take sessions from this queue.

Alert Timeout

A representative has as long as is set here to either accept or reject an assigned session. If the representative rejects the session or fails to respond before the timeout, the session will be reassigned to the next best matched representative who is available to take sessions from this queue.

Waiting Session Rule

You also can create a **Waiting Session Rule**. If enabled, set how long a session is allowed to remain in this queue. Then choose the action to take if the session waits for longer than the set time. You can either transfer the session to an overflow queue, or you can mark the session as overdue. A session that becomes overdue plays an audio alert, flash in the queue, causes the queue itself to flash, and displays a pop-up notification. These notifications can be modified in the representative console settings.



For more information, please see [Equilibrium for Automatic Session Routing guide](https://www.beyondtrust.com/docs/remote-support/how-to/equilibrium/index.htm) at <https://www.beyondtrust.com/docs/remote-support/how-to/equilibrium/index.htm>.

Dashboard Settings

Within a team, a user can administrate only others with roles lower than their own.



Note: Roles apply strictly on a team-by-team basis, so a user may be able to administrate another user in one team, but not be able to administer that same user in another team.

Monitoring Team Members from Dashboard

If enabled, a team lead or manager can monitor team members from the dashboard. Choose a selection to **Disable** the ability to monitor, restrict monitoring to **Only Representative Console**, or allow a team lead or manager to monitor a team member's **Entire Screen**. Monitoring affects team leads and managers for all teams on the site.

Enable Monitor Indicator

If this option is checked, a team member whose screen is being monitored sees a monitoring icon on their screen.

Enable Session Transfer and Take Over in Dashboard

If this option is checked, a team lead can take over or transfer a team member's sessions. Similarly, a team manager can administrate both team members and team leads. The team lead must have start session access to the Jump Item that was used to create the session, unless the option below is also checked.

Allow Team Managers/Leads to use "Transfer", "Take Over" and "Join Session" for sessions that are started from Jump Items to which they do not have "Start Session" access

If this option is checked, a team lead can join or take over a team member's sessions, even if the team lead does not have start session access to the Jump Item that was used to create the session.



For more information, please see [Monitor Team Members in the Dashboard](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/dashboard.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/dashboard.htm>.

Team Chat History

Enable Replay of Team Chat History

If this option is checked, chat messages to everyone in the **Team Chat** area of the representative console persist between representative console logins.

This prevents loss of chat history if the connection is lost. This does not affect chat within a session, or private chats.

Hours of Team Chat History to Replay

By default, 8 hours of history is retained. This can be changed from a minimum of 1 to a maximum of 24, using the **+** and **-** icons or entering the desired value. The time is set in one hour increments. Click **Save** after changing the time.



Note: A maximum of 1000 chat messages is replayed. This limit applies regardless of the number of hours selected.

Rep Status

Configure up to 10 status codes to allow representatives to indicate their status when they opt out of automatic session assignment. When representatives change their status, the new status displays in the representative console dashboard for all team managers. Representative status changes are also logged in the Team Activity Report.

Add New Rep Status Code, Edit, Delete

Create a new rep status code, modify, or remove an existing rep status code. There are 3 predefined status codes: **Available**, **Away**, and **Busy**. The **Available** status code may not be modified or deleted. The **Away** and **Busy** status codes may be modified but not deleted.

Display Name

Create a unique name to help identify this rep status code.

Code Name

Set a code name for integration purposes. If you do not set a code name, one is created automatically.

Display As

Select the **Away** or **Busy** option. This is what team members see for each representative's status in the **Dashboard** feature in the representative console when the representative is using this status code.

Auto Status Options

Select default statuses to display in the representative console dashboard when a representative is idle or busy and they have not manually changed their status.

Rep Idle Status

Specify a status to automatically set when the representative is idle.

Rep Busy Status

Specify a status to automatically set when the representative is busy.

Skills: Route Issues to Representatives



Configuration

SKILLS

Skills

Skills are the areas of expertise covered by your representatives. As an administrator, you need to create a list of these skills, which are ranked in broad categories according to their importance. These root skills can be assigned a number of sub-skills. For instance, the root skill for "Antivirus" can contain a list of common antivirus programs, each a particular sub-skill necessary to properly address a customer support issue dealing with antivirus-related problems.

Representatives associated with a given skill are listed on the right. If no representative is associated with a skill, go to **Users & Security > Users**, select a user to edit, and click on the **Availability Settings** to configure skills.



Note: In order to be able to create and edit skills, this permission has to be set per user. Go to **Users & Security > Users**, scroll down to the **Permissions** section, and make sure **Allowed to Edit Skills** permission is checked. Administrators are automatically granted this permission.

To create or edit skills, go to **Configuration > Skills**.

New Root Skill

To begin, create a list of root skills as general categories.

New Skill

Add skills under the root skills.

Edit, Delete

Modify an existing object or remove an existing object.

Change Ranking

If you need to change a root skill's rank, click on **Change Ranking**. You will now be able to drag and drop skills into their new positions.

Skills

Root skills and their sub-categories display in the **Skills** tree. You can use the orange arrows to expand or collapse each section.

Root skills are ranked sequentially from more critical to less critical. When Equilibrium is enabled, the system will try first to match all the root skills, but if that is not possible, it will begin to peel away lower ranking skills first, one at a time, until a match is found.

Display Name

Create a unique name to help identify this skill.

Code Name

Set a code name for integration purposes. If you do not set a code name, one is created automatically.



For more information, please see [Configure Skills to Route Issues to Representatives](https://www.beyondtrust.com/docs/remote-support/how-to/equilibrium/configure-skills.htm) at <https://www.beyondtrust.com/docs/remote-support/how-to/equilibrium/configure-skills.htm>.

Import User Skills

Once created, skills can be assigned to representatives from the **Users & Security > Users** page.

When dealing with a larger number of representatives and/or skill sets, it may be easier to assign skills to representatives using bulk import. Use **Choose File** to upload a CSV file with the usernames and associated skills. The CSV file should use the following format:

```
"username1", "skill_code_name"  
"username1", "skill_code_name2"  
"username2", "skill_code_name"
```

Please note that the skills listed for a given representative on the import file will override any skills already associated with that user. If you need to remove all associated skills with a particular user, leave the skill code name empty ("username3", "").



For more information, please see [Configure Skills to Route Issues to Representatives](https://www.beyondtrust.com/docs/remote-support/how-to/equilibrium/configure-skills.htm) at <https://www.beyondtrust.com/docs/remote-support/how-to/equilibrium/configure-skills.htm>.



For more information, please see [Assign Skills to Representatives](https://www.beyondtrust.com/docs/remote-support/how-to/equilibrium/assign-skills-rep.htm) at <https://www.beyondtrust.com/docs/remote-support/how-to/equilibrium/assign-skills-rep.htm>.



For more information, please see [Skills Routing Algorithms](https://www.beyondtrust.com/docs/remote-support/how-to/equilibrium/skills-routing-algorithms.htm) at <https://www.beyondtrust.com/docs/remote-support/how-to/equilibrium/skills-routing-algorithms.htm>.

Access Sponsors: Create Groups of Privileged Users



Configuration

ACCESS SPONSORS

Access Sponsor Groups

Create access sponsor groups to enable a representative with restricted permissions to request a more highly privileged representative to perform certain actions on their behalf, such as elevating a customer client to administrative rights or entering credentials for a remote system.

Add New Access Sponsor Group, Edit, Delete

Create a new group, modify an existing group, or remove an existing group.

Add or Edit Access Sponsor Groups

Name

Create a unique name to help identify this group. This name should help representatives determine the correct access sponsor group from which to request assistance.

Description

Add a brief description to summarize the purpose of this group.

Group Members

Add lower-privileged representatives as Requestors to this group, and add higher-privileged representatives as Sponsors.



For more information, please see [Accept an Access Request to Offer Elevation Help](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/access-requests.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/access-requests.htm>.

Support Buttons: Deploy Support Buttons for Quick Session Start



Configuration

SUPPORT BUTTONS

Support Button Mass Deployment Wizard

Deploying a Support Button on your customer's computer installs a customer client on their machine, providing a quick, seamless method of starting support sessions. The Support Button does NOT maintain a connection to the B Series Appliance, but rather provides a customer-initiated method of requesting support. Depending on the configuration of the Support Button and the support site, clicking the Support Button will connect the customer to a previously defined representative or team, allow the customer to enter a session key, or allow the customer to submit an issue submission form. Support Buttons can be installed on Windows, Mac, and Linux computers.



Note: This feature is not supported for ARM-based Windows systems.



For more information, please see [Manage Support Buttons](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-button-management-interface.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-button-management-interface.htm>.



For more information, please see [Support Button: Quickly Request Support](https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/support-button.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/support-button.htm>.

Description

Create a unique name to help identify this Support Button. This name is helpful when managing deployed Support Buttons.

Public Portal

Select the public portal through which this item should connect for a support session. If a session policy is assigned to this public portal, that policy may affect the permissions allowed in sessions started through this item.

Language

If more than one language is enabled on this site, set the language this Support Button should use. Support Buttons do not detect the local language when they are run; they only use the default language assigned during deployment.

Team

Specify whether starting a session from this Support Button should place the customer in your personal queue or a team queue.

Deployed Support Buttons Are Valid For

Set the lifespan of the button. The customer can use this button to start sessions for only as long as specified here. If the customer clicks this button after it has expired, an invalid session key message will display, and the browser will refresh to your support portal. This time does NOT affect how long the installer remains active or how long a session can last.

Install Mode

Choose whether to install the Support Button for a single user or for all users on the remote system. Deploying a Support Button for all users is available only for Windows platforms. Also, if you make any changes to a Support Button profile, a single-user Support Button will automatically incorporate those changes the next time it connects, while an all-user Support Button will have to be redeployed in order to receive those changes. For the best experience, redeploy all-user Support Buttons each time you upgrade your BeyondTrust software. Note that all-user Support Buttons may not be removed from within the representative console; they must be uninstalled directly from the target computer.

Profile

Select a profile to use from the dropdown menu.

Create

Click to create the Support Button.

Download Now

Platform

Choose the operating system on which you wish to install this software. This dropdown defaults to the appropriate installer detected for your operating system.

For system administrators who need to push out the Support Button installer to a large number of systems, the MSI option can be used with your systems management tool of choice. In your command prompt, when composing the command to install the Support Button using an MSI, change to the directory where the MSI was downloaded and enter the command included on the **Support Button** page.



Note: Unlike the representative console, Support Buttons installed from an MSI do auto-update.

When installing a Support Button executable on remote Windows machines, you can specify a custom install directory path where you want the Support Button to install. If the install directory you specify does not exist, it will be created, assuming the installation has sufficient permissions on the local system. You can specify the install directory using either the MSI installation package or the EXE installation package. Installation to custom paths is not supported on Mac or Linux systems.

The syntax for the EXE installation is:

```
bomgar-scc-w07dc30w8ff8h51116g785zgh151hdfe8y6z7jgc408c90 --cb-install-dir "C:\Support Button"
```

where `bomgar-scc-w07dc30w8ff8h51116g785zgh151hdfe8y6z7jgc408c90` is the filename of your executable install client and `"C:\Support Button"` is the path you wish the installation to use.

The syntax for the MSI installation is

```
msiexec /i bomgar-scc-win64.msi KEY_INFO=w0hdc301hd18wxj8xjfd8z6jzyefz7wzd1gwwd6c408c90  
INSTALLDIR="C:\Support Button"
```

where `bomgar-scc-win64.msi` is the name of your MSI installation package, `w0hdc301hd18wxj8xjfd8z6jzyefz7wzd1gwwd6c408c90` is the key of your installation package, and `"C:\Support Button"` is the path you wish the installation to use.

To install a Support Button without displaying any windows, spinners, errors, or other visible alerts, append `--silent` to the end of the EXE command or `/quiet` to the end of the MSI command.

Download

You can download the installer immediately if you plan to distribute it using a systems management tool or if you are at the computer to which you need later access.



Note: Because some browsers require that the installer be saved before it can be run, there may be some confusion about when the Support Button is fully installed. The downloaded `bomgar-scc-{uid}.exe` file is not the button itself but rather the installer for the button. This executable file must be run to complete the installation.

Deploy to Email Recipients

Email

You can also email the installer to one or more remote users. Multiple recipients can install the client from the same link. Click on the **Direct Download Link** to copy the link.

Support Button Profiles - Add

Create a new profile, modify an existing profile, or remove an existing profile. You can edit but not delete the default Support Button profile.

Name

Create a unique name to help identify this profile. This name should help a representative decide which profile to assign to a Support Button.

Icon

Upload the file containing the customized button icon. The file must be a PNG file, no larger than 150KB and with a minimum height and width of 128 pixels. The height and width must be equal.

Title

The title is used as the title of the desktop icon.

Short Title

The short title is used when the customer's operating system limits the title length.

Deployment Locations

Select where the Support Button should be deployed, whether to the desktop or the menu. The menu option is only supported on Windows, Mac, and Linux systems.

Allow direct access to queue

Select if the customer can use the Support Button to connect directly to a specified queue (the queue is specified by the **Team** dropdown in the Support Button Mass Deployment Wizard).

Embedded Support Button Registry File Generator

Use the **Embedded Support Button Registry File Generator** to create registry files which will embed the Support Button into the title bar of an application. An embedded Support Button gives support providers the ability to streamline the support path for specific applications. For example, if your support team frequently handles issues with Microsoft Outlook, you can embed a Support Button within Outlook. You can configure this embedded Support Button to point to a specific issue so that when a customer clicks the button, a session will immediately start with the team best suited to handle Outlook problems. Embedded Support Buttons are a Windows-only feature.

To create an embedded Support Button, a Support Button must first be deployed on the remote system. You may wish to define the Support Button profile so that neither the desktop shortcut nor the menu shortcut is created.

Install Mode

Select whether to install for all users on a system or a single user.

Executable Name

Enter the name of the program in which you want to embed a Support Button. Do not include the file path.

Issue

Optionally, select an issue that will be associated with sessions started from this embedded Support Button. You can alternatively select **No Issue Assigned**.

Show Front-End Survey

Checking **Show Front End Survey** prompts the customer to describe their issue before starting a session. If this option is unchecked, the session will start immediately, without any further customer input.

External Key

You can add an external key to assign to sessions started from this embedded Support Button.

Delete

Remove an existing application from this registry file.

Add New Row

To add multiple applications to one registry file, click **Add New Row** and enter the information for another application.

Import a Registry File

To edit an embedded Support Button's functionality, you can import the registry file and modify its entries. When complete, click **Create Registry File**. Running the registry file will overwrite the existing registry entries.

Create Registry File

When you have finished adding executables in which you want to embed Support Buttons, click **Create Registry File**. This prompts you to save a registry file to your system. Using Active Directory or a deployment tool, deploy the registry file to all remote systems which should use these embedded Support Buttons. After running the registry file, the remote user will have to log off and back on for the Support Button registry entry to be created.



Note: It is a best practice to save a copy of any generated registry files. Registry file information is not saved on the BeyondTrust Appliance B Series.

Now, when one of the designated applications is run, a Support Button will appear in the top right corner, beside the minimize button. Clicking this embedded Support Button will start a session as defined by its profile and its registry file settings.



Note: Running a Support Button registry file on a system that already has Support Button registry entries will overwrite the original registry entries. Therefore, if you have embedded a Support Button in one application and you wish to embed it in another, the new registry file must contain both executable names. If the new registry file contains only the new executable name, then the embedded Support Button will appear only in the new application and not in the previous application.

To remove an embedded Support Button from a specific application without adding it to another application, you must edit the registry. Using Notepad or a similar editor, open the registry file you initially deployed and insert a hyphen in front of each registry key you wish to delete. Save the registry file and redeploy it to remove the registry entry. An example of a registry entry marked for deletion is presented below.

```
[-HKEY_LOCAL_MACHINE\Software\Test]
```



For more information about registry entries, please see <https://support.microsoft.com/kb/310516>.



Note: Uninstalling the Support Button will remove it from all embedded programs but will not delete the registry entries. Thus, if another Support Button is installed for the same site, it will inherit the previous registry entries and will appear embedded in the same programs.

i For more information, please see *Manage Support Buttons* at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-button-management-interface.htm>.

Custom Fields: Create and Modify Fields for Public Portal Issue Submissions



Configuration

CUSTOM FIELDS

Custom Fields

You can configure up to 30 custom fields. Custom field values can be created and configured for individual support sessions using the public portal issue submission configuration, as well as certain API operations. They are visible in the BeyondTrust representative console.

Create New Field, Edit, Delete

Create, modify, or delete a custom field. Deleted custom fields no longer display in the representative console or the session reports.

Add or Edit a Custom Field

Display Name

Create a unique name to help identify this field.

Code Name

Set a code name for integration purposes. If you do not set a code name, one is created automatically.

Show in Representative Console

Check this box if you want this field to display in the representative console.



Note: To select issues to display in the public portal, as well as the order in which they should appear, go to **Public Portals > Use Issue Submission Survey**. Add or edit a public site and select **Use Issue Submission Survey**. Choose available fields to display.

MS Teams: Enable and Customize the Microsoft Teams Integration



Configuration

MS TEAMS

Microsoft Teams Integration

When enabled, this feature allows you to extend your support capabilities within Microsoft Teams. MS Teams can support multiple Remote Support teams and use the integration, differently if desired, for all the different portal sites. Administrators can prepare custom greetings and deploy customizable BeyondTrust Remote Support bots for their organization that enables their users to chat with support representatives and accept session invitation links in the Microsoft Teams chat.

Follow the on-screen instructions to setup the integration.



Note: You must check **Enable the Microsoft Teams Integration** to view the instructions.

Select a Portal

If you have multiple public portals, select the portal for the integration from the **Select a public site to edit** dropdown. To set up Teams integration for multiple portals, repeat the process below for each portal.

Enable the Microsoft Teams Integration

Check this option to enable the MS Teams integration, and display the **Configuration Instructions** and configuration options.

Basic Configuration

Follow the on-screen instructions, Step 1, items 1 through 7, to deploy a custom bot for your Azure tenant, and obtain the information to complete the **Basic Configuration** fields. This requires working in your Azure portal.

Bot Configuration

Follow the on-screen instructions, Step 1, item 8, to set up the Bot profile.

Deploy the Bot to the Microsoft Teams Tenant

As per the on-screen instructions, Step 2, items 1 through 4, once the configuration is complete, click **Download Teams Manifest Package** and upload the file to the Microsoft Teams admin center.

MS Teams: Service Now Virtual Agent Integration

ServiceNow provides a chat API to connect with its Virtual Agent automated assistant, as well as an integration with Microsoft Teams that allows Microsoft Teams users to interact directly with ServiceNow. When a BeyondTrust user communicates with the Remote Support chat interface, there is no direct method of interacting with the ServiceNow resources except by switching to another Microsoft Teams channel.

This integration with ServiceNow allows the user to access the ServiceNow Virtual Agent without switching to another Microsoft Teams channel while using the Remote Support chat interface. This allows the user to get automated assistance first and then transition to a live support representative, if necessary, within the same Microsoft Teams chat.



Note: Translating the text and formatting from Virtual Agent to Microsoft Teams is supported. Images and file uploads are not supported in this release.

Supported Formats

The following Virtual Agent UI Types are supported:

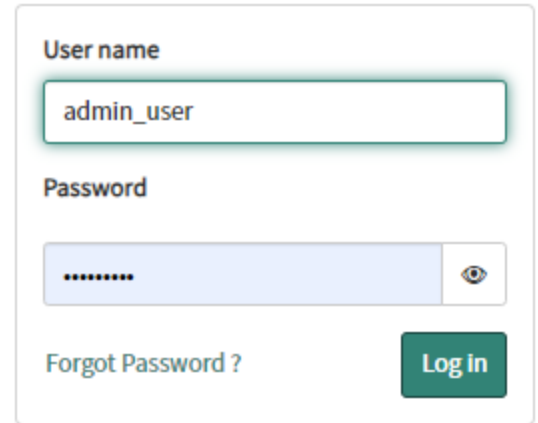
- DefaultPicker
 - TopicPickerControl
 - Picker
 - Boolean
- DefaultText
 - OutputText
 - InputText
- DefaultGroupedPartsOutputControl
 - GroupedPartsOutputControl
- DefaultOutputCard
 - OutputCard

In the above cases, only the text portions are translated and sent to Microsoft Teams.

OAuth Setup

Follow the steps below to configure authentication for Remote Support in ServiceNow:

1. Log in to ServiceNow.

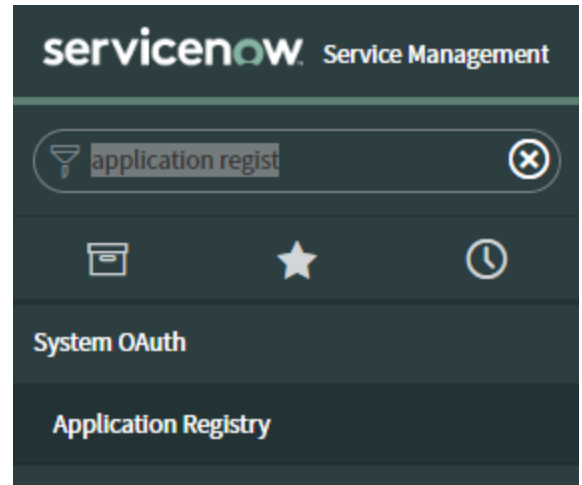


User name

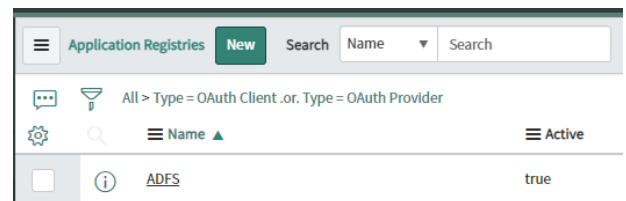
Password

[Forgot Password ?](#)

2. In the upper left-hand corner of the interface, go to **All > OAuth-Application Registry**. You can search for “Application Registry” in the search field at the top.
3. Click on Application Registry.

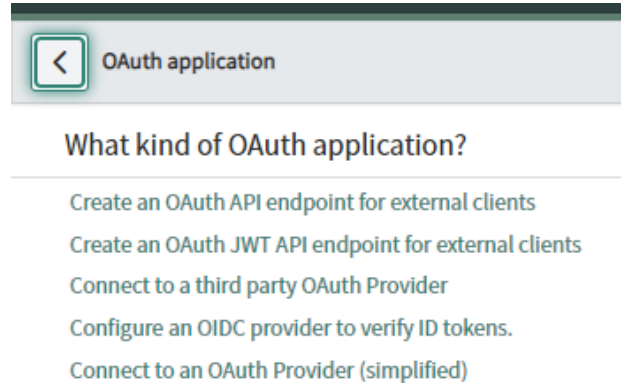
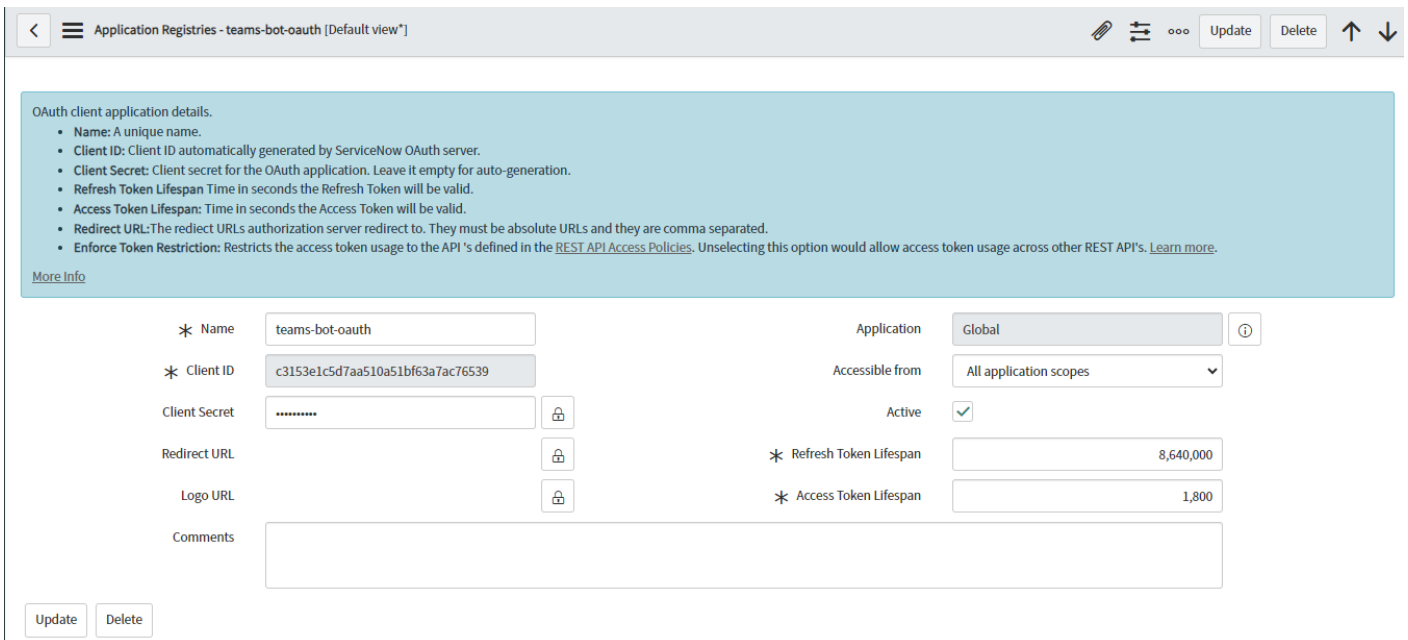


4. Click **NEW** at the top.



Application Registries		New	Search	Name	Search
All > Type = OAuth Client .or. Type = OAuth Provider					
		Name		Active	
<input type="checkbox"/>		ADFS			true

5. The OAuth Application window displays and show the list of OAuth application types.
6. Select **Create an OAuth API endpoint for external Clients**.
7. The OAuth client application details form appears.

Application Registries - teams-bot-oauth [Default view*]

OAuth client application details.

- Name: A unique name.
- Client ID: Client ID automatically generated by ServiceNow OAuth server.
- Client Secret: Client secret for the OAuth application. Leave it empty for auto-generation.
- Refresh Token Lifespan: Time in seconds the Refresh Token will be valid.
- Access Token Lifespan: Time in seconds the Access Token will be valid.
- Redirect URL: The redirect URLs authorization server redirect to. They must be absolute URLs and they are comma separated.
- Enforce Token Restriction: Restricts the access token usage to the API's defined in the [REST API Access Policies](#). Unselecting this option would allow access token usage across other REST API's. [Learn more.](#)

[More Info](#)

* Name: teams-bot-oauth Application: Global ⓘ

* Client ID: c3153e1c5d7aa510a51bf63a7ac76539 Accessible from: All application scopes ▼

Client Secret: 🔒 Active:

Redirect URL: 🔒 * Refresh Token Lifespan: 8,640,000

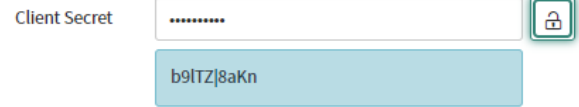
Logo URL: 🔒 * Access Token Lifespan: 1,800

Comments:

Update Delete

8. Enter a **Name** for this authorization, for example, *BeyondTrust Microsoft Teams Bot Authentication*.
9. Copy and save the **Client ID**. In the example above, this is **c65466ba7fd1f910d6fd28f07e38a1e3**. The client ID is required when configuring the Remote Support appliance to use ServiceNow Virtual Agent.
10. Leave the **Client Secret** blank to generate a secret automatically.
11. Ensure **Application** is set to *Global*.
12. Ensure **Accessible from** is set to *All application scopes*.
13. Ensure **Active** is checked.
14. Use the defaults provided for **Refresh Token Lifespan** and **Access Token Lifespan**.
15. Click Submit
16. The list of tokens displays. Click on the name you just created.

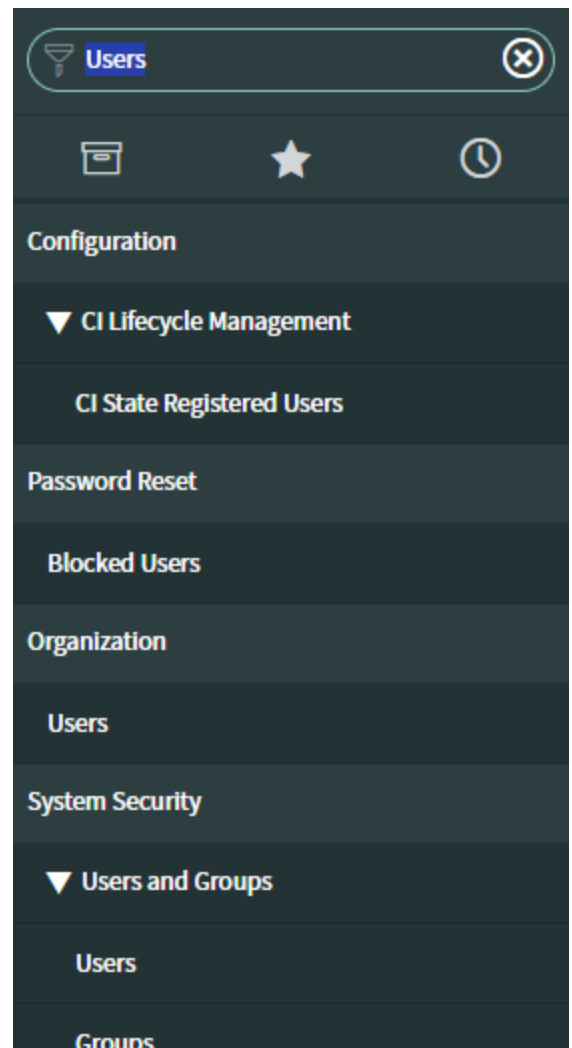
17. When the record displays, click on the lock symbol next to the **Client Secret** field.
18. Copy the **Client Secret**. The client secret is required when configuring the Remote Support appliance to use ServiceNow Virtual Agent.

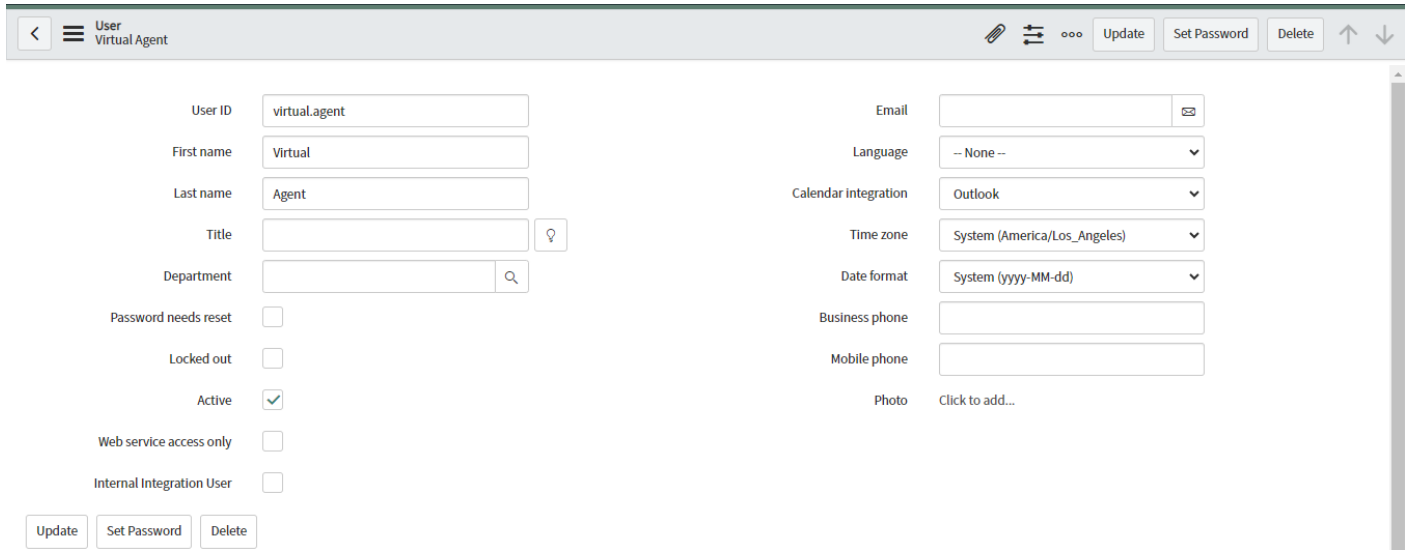


Set up the Virtual Agent Interface User

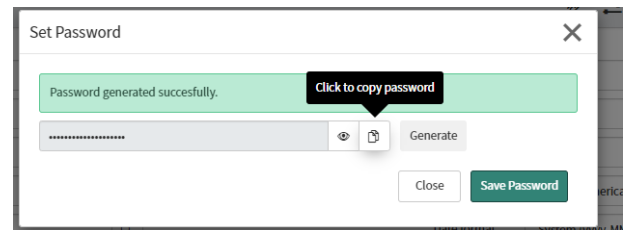
A separate user account must be created to connect the Remote Support chatbot to the ServiceNow Virtual Agent bot, to allow the Remote Support chatbot to log in. ServiceNow provides a default user for the virtual agent. This is configured as follows:

19. In the upper left-hand corner of the interface, go to **All > System Security > Users and Groups**.
20. Click on **Users**.
21. A list of users displays on the right.
22. Search for *Virtual Agent* in the search field at the top.
23. Click the User ID **virtual.agent**.





24. Copy the **User ID** . It is required later.
25. Click **Set Password**.
26. In the **Set Password** dialog, click **Generate**. There is no option to choose a password, however this password is temporary. A confirmation message confirms a password has been generated.
27. Copy the password, using the **Click to copy password** button. The password is required later.
28. Click **Close**.



Verify and Refresh Password

29. Log out of ServiceNow.
30. Log in to ServiceNow, using the Virtual Agent User ID and generated password saved above.
31. The system requires you to change the password from the generated password. Enter the generated password and create and enter a new password that meets the stated requirements.
32. Click **Submit**.

i System administrator requires you to change your password

Change Password

User name:
virtual.agent

Current Password:

Password Requirements:

- Minimum 8 characters
- Maximum 40 characters
- At least 1 lowercase letter(s)
- At least 1 uppercase letter(s)
- At least 1 digit(s)

New password:

Confirm New Password:

Configure the Output Response REST Endpoint

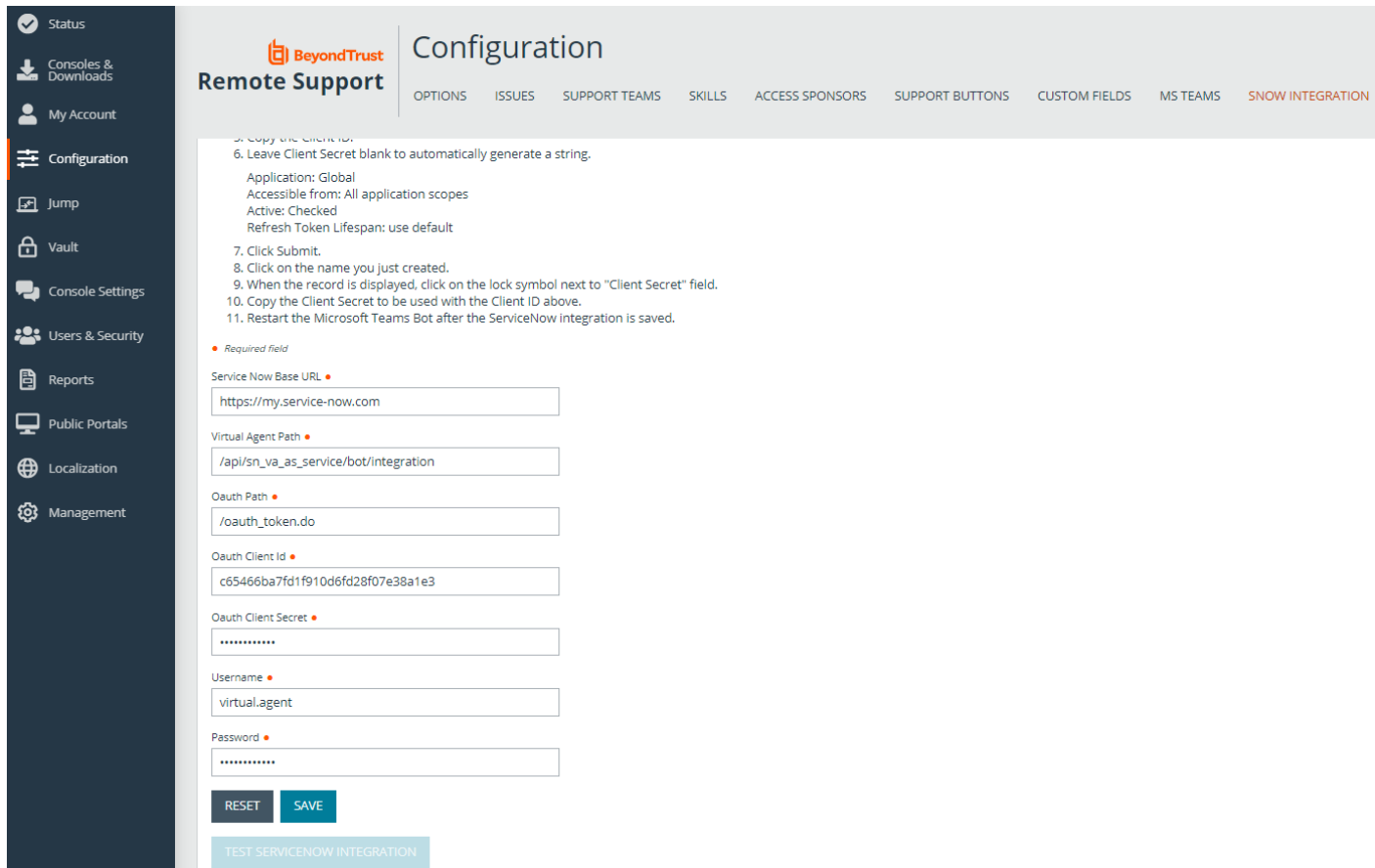
33. Within ServiceNow, Navigate to **All > System Web Services > Outbound > REST Message**.
34. Click **VA Bot to Bot record**.
35. Enter the response endpoint for the Microsoft Teams bot in the Endpoint field, then click **Update**.



Note: This is the endpoint for the primary bot server, where the response will be sent from the ServiceNow bot to Microsoft Teams.

BeyondTrust Remote Support Configuration

36. Log in to the BeyondTrust Remote Support administrative /login interface.
37. Navigate to **Configuration > SNOW INTEGRATION**.
38. Complete this form, using information saved when setting up the integration in ServiceNow.



Configuration

Options: ISSUES SUPPORT TEAMS SKILLS ACCESS SPONSORS SUPPORT BUTTONS CUSTOM FIELDS MS TEAMS **SNOW INTEGRATION**

3. Copy the Client ID.
 6. Leave Client Secret blank to automatically generate a string.
 Application: Global
 Accessible from: All application scopes
 Active: Checked
 Refresh Token Lifespan: use default
 7. Click Submit.
 8. Click on the name you just created.
 9. When the record is displayed, click on the lock symbol next to "Client Secret" field.
 10. Copy the Client Secret to be used with the Client ID above.
 11. Restart the Microsoft Teams Bot after the ServiceNow integration is saved.

• Required field

Service Now Base URL •

Virtual Agent Path •

OAuth Path •

OAuth Client ID •

OAuth Client Secret •

Username •

Password •

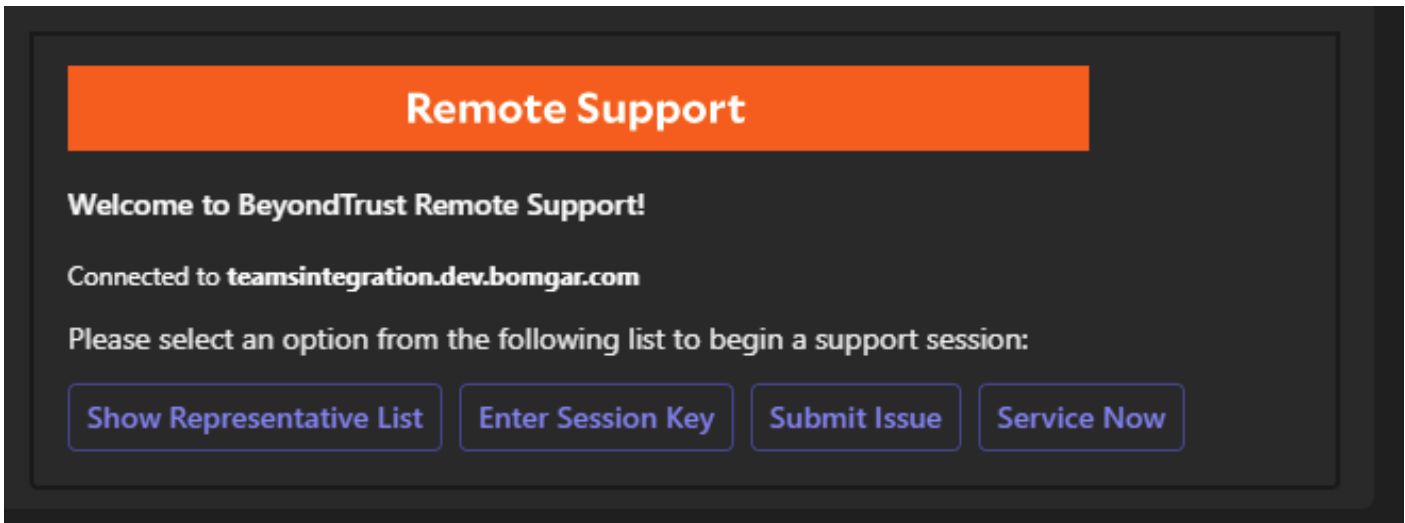
RESET **SAVE**

TEST SERVICENOW INTEGRATION

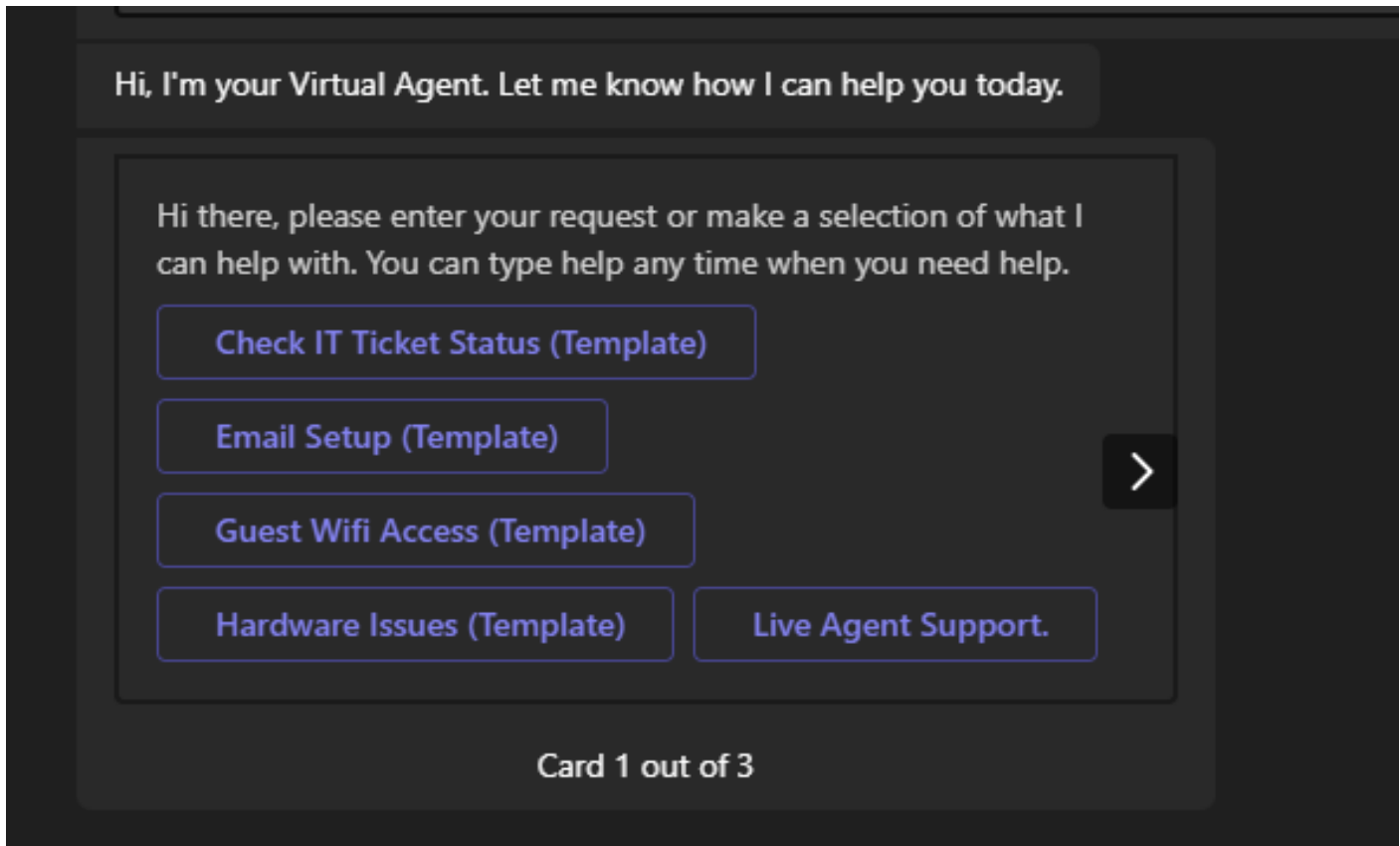
39. Set the **ServiceNow Base URL** to the https address of the ServiceNow instance used to configure the Virtual Agent.
40. Set the **OAuth Client ID** to the Client ID saved above.
41. Set the **OAuth Client Secret** to the Client Secret saved above.
42. Set the **Username** to *virtual.agent*.
43. Set the **Password** to the new password created above.
44. Click **SAVE**. This enables **TEST SERVICENOW INTEGRATION**.
45. Click **TEST SERVICENOW INTEGRATION**. A message confirms the integration is successful. If the integration is not successful, review all entered data and try again.
46. Details such as **Access Token** display after the test. There is no need to save this information.
47. Click Status in the left menu, and click **RESTART REMOTE SUPPORT SOFTWARE**.

View the Remote Support Virtual Agent

1. Go to the BeyondTrust Remote Support MS Teams channel.
2. Enter *Hello*.
3. The Remote Support Welcome banner includes the new ServiceNow button.



4. Click **Service Now**.
5. A dialogue with the ServiceNow Virtual Agent begins. The responses depend on how the ServiceNow Virtual Agent is configured. An example is shown below.



- The path and end of the conversation depend on how the Service Now Virtual Agent is configured. If the Service Now Virtual Agent has answered the question, the agent automatically terminates the conversation.

Multi Support Bot 10:48 AM

You have no active incidents or requested items.

The conversation has ended. If you need help again, type hi.

Remote Support

Welcome to BeyondTrust Remote Support!

Connected to teamsintegration.dev.bomgar.com

Please select an option from the following list to begin a support session:

Show Representative List

Enter Session Key

Submit Issue

Service Now

Should you need any assistance, please log into the [Customer Portal](https://beyondtrustcorp.service-now.com/csm) at <https://beyondtrustcorp.service-now.com/csm> to chat with Support.

Jump

Jump Clients: Manage Settings and Install Jump Clients for Unattended Access



JUMP CLIENTS

Jump Client Installer List

This list shows all previously installed active Jump Client installers. Administrators and privileged users can view, download, delete, or extend Jump Client installers.

A warning message appears at the top of the list: *Installing more than one Jump Client as the same user or more than one Jump Client as a service on the same system is being phased out in a future release. In the Representative Console you may use the **copy** action on a Jump Client to apply different policies to the same endpoint. Click **Dismiss** to remove the warning message.*

Generic Jump Client Installer Download

The generic installer allows you to create Jump Client and Jumpoint installers that are not tied to a specific Jump Client or Jumpoint. Generic installers can be used for automated or ephemeral deployments on VM images, and do not require authenticating and downloading the Jump Client or Jumpoint-specific installer once deployed.

To use the generic Jump Client installer, select your desired platform, and click **Download**. When prompted, copy the Jump Client-specific key to complete the installation.

Jump Client Mass Deployment Wizard

To access the Jump Client Mass Deployment Wizard, click **Add** at the top of the Jump Client Installer List.

The Mass Deployment Wizard enables administrators and privileged users to deploy Jump Clients to one or more remote computers for later unattended access.



For more information, please see [Remote Support Jump Client Guide: Unattended Access to Systems in Any Network](https://www.beyondtrust.com/docs/remote-support/how-to/jump-clients/index.htm) at <https://www.beyondtrust.com/docs/remote-support/how-to/jump-clients/index.htm>.

Jump Group

From the **Jump Group** dropdown, select whether to pin the Jump Client to your personal list of Jump Items or to a Jump Group shared by other users. Pinning to your personal list of Jump Items means that only you (and higher ranking roles on your team, such as Team Lead and Team Manager if you are a Team Member, and Team Manager if you are a Team Lead) can access this remote computer through this Jump Client. Pinning to a shared Jump Group makes this Jump Client available to all members of that Jump Group.

Allow Override During Installation

Some Mass Deployment Wizard settings allow override, enabling you to use the command line to set parameters that are specific to your deployment, prior to installation.

This Installer Is Valid For

The installer remains usable only as long as specified by the **This Installer is Valid For** dropdown. Be sure to leave adequate time for installation. If someone should attempt to run the Jump Client installer after this time, installation fails, and a new Jump Client installer must be created. Additionally, if the installer is run within the allotted time but the Jump Client is unable to connect to the B Series Appliance within that time, the Jump Client uninstalls, and a new installer must be deployed. The validity time can be set for anywhere from 10 minutes to 1 year. This time does NOT affect how long the Jump Client remains active.

Once a Jump Client has been installed, it remains online and active until it is uninstalled from the local system either by a logged-in admin user with appropriate permissions, by a user from the Jump interface, or by an uninstall script. It can also be uninstalled, or extended, from the Jump Client Installer List. A user cannot remove a Jump Client unless the user is given appropriate permissions by their admin from the /login interface.

Public Portal

Select the public portal through which this item should connect for a support session. If a session policy is assigned to this public portal, that policy may affect the permissions allowed in sessions started through this item.

Name

Enter a **Name** for the Jump Item. This name identifies the item in the session tabs. This string has a maximum of 128 characters.

Comments

Add **Comments**, which can be helpful in searching for and identifying remote computers. Note that all Jump Clients deployed via this installer have the same comments set initially, unless you check **Allow Override During Installation** and use the available parameters to modify the installer for individual installations.

Tag

Adding a **Tag** helps to organize your Jump Clients into categories within the representative console.

Jump Policy

You can apply a **Jump Policy** to this Jump Client. Jump Policies are configured on the **Jump > Jump Policies** page and determine the times during which a user can access this Jump Client. If no Jump Policy is applied, this Jump Client can be accessed at any time.

Customer Present Session Policy and Customer Not Present Session Policy

Choose session policies to assign to this Jump Client. Session policies assigned to this Jump Client have the highest priority when setting session permissions. The **Customer Present Session Policy** applies when the end user is determined to be present. Otherwise, the **Customer Not Present Session Policy** applies. The way customer presence is determined is set by the **Use screen state to detect**

Customer Presence Jump Client setting. Customer presence is detected when the Jump Client session starts. The session policy used for the session does not change throughout the session, regardless of any changes in the customer's presence while the session is in progress.

Jumpoint Proxy

If you have one or more Jumpoints set up as proxies, you can select a Jumpoint to proxy these Jump Client connections. As a result, if these Jump Clients are installed on computers without native Internet connections, they can use the Jumpoint to communicate with your B Series Appliance. The Jump Clients must be installed on the same network as the Jumpoint selected to proxy the connections.

Maximum Offline Minutes Before Deletion

You can set the **Maximum Offline Minutes Before Deletion** of a Jump Client from the system. This setting overrides the global setting, if specified.

Attempt an Elevated Install if the Client Supports It

If **Attempt an Elevated Install if the Client Supports It** is selected, the installer attempts to run with administrative rights, installing the Jump Client as a system service. If the elevated installation attempt is unsuccessful, or if this option is deselected, the installer runs with user rights, installing the Jump Client as an application. This option applies only to Windows and Mac operating systems.



Note: A Jump Client pinned in user mode is available only when that user is logged in. In contrast, a Jump Client pinned in service mode, with elevated rights, allows that system to always be available, regardless of which user is logged in.

Prompt for Elevation Credentials if Needed

If **Prompt for Elevation Credentials if Needed** is selected, the installer prompts the user to enter administrative credentials if the system requires that these credentials be independently provided; otherwise, it installs the Jump Client with user rights. This applies only if an elevated install is being attempted.

Customer Client Start Mode

Select **Minimized** to start the customer client minimized. It does not take the focus, and appears only in the taskbar or dock when a session is started through this Jump Client.

Select **Hidden** to start the customer client hidden. It does not take the focus, and appears only as an icon in the system tray when a session is started through this Jump Client.

Mass Deploy Help

For system administrators who need to push out the Jump Client installer to a large number of systems, the Windows, Mac, or Linux executable or the Windows MSI can be used with your systems management tool of choice. You can include a valid custom install directory path where you want the Jump Client to install.


You can also override certain installation parameters specific to your needs. These parameters can be specified for both the MSI and the EXE using a systems administration tool or the command line interface. When you mark specific installation options for override during installation, you can use the following optional parameters to modify the Jump Client installer for individual installations. Note that if a parameter is passed on the command line but not marked for override in the /login administrative interface, the installation fails. If the installation fails, view the operating system event log for installation errors.



Note: It is common to receive an error message during the install, regarding a layout or appearance issue. This can be disregarded.

Command Line Parameter	Value	Description
--install-dir	<directory_path>	Specifies a new writable directory under which to install the Jump Client. This is supported only on Windows and Linux. When defining a custom install directory, ensure that the directory you are creating does not already exist and is in a location that can be written to.
--jc-name	<name...>	If override is allowed, this command line parameter sets the Jump Client's name.
--jc-jump-group	user:<username> jumpgroup:<jumpgroup-code-name>	If override is allowed, this command line parameter overrides the Jump Group specified in the Mass Deployment Wizard.
--jc-public-site-address	<public-site-address-hostname>	If override is allowed, this command line parameter associates the Jump Client with the public portal which has the given hostname as a site address. If no public portal has the given hostname as a site address, then the Jump Client reverts to using the default public site.
--jc-session-policy-present	<session-policy-code-name>	If override is allowed, this command line parameter sets the Jump Client's session policy that controls the permission policy during a support session if the customer is present at the console.
--jc-session-policy-not-present	<session-policy-code-name>	If override is allowed, this command line parameter sets the Jump Client's session policy that controls the permission policy during a support session if the customer is not present at the console.
--jc-jump-policy	<jump-policy-code-name>	If override is allowed, this command line parameter sets the Jump Policy that controls how users are allowed to Jump to the Jump Client.
--jc-max-offline-minutes	<minutes>	The maximum number of minutes a Jump Client can be offline before it is deleted from the system. This setting overrides the global setting if specified.
--jc-ephemeral		Sets the maximum number of minutes a Jump Client can be offline before it is deleted from the system to 5 minutes. This is a convenience option that specifies the Jump Client as being ephemeral and is functionally equivalent to specifying --jc-max-offline-minutes 5
--jc-tag	<tag-name>	If override is allowed, this command line parameter sets the Jump Client's tag.
--jc-comments	<comments ... >	If override is allowed, this command line parameter sets the Jump Client's comments.
--silent		If included, the installer shows no windows, spinners, errors, or

other visible alerts.

-  **Note:** When deploying an MSI installer on Windows using an `msiexec` command, the above parameters can be specified by:
1. Removing leading dashes (`--`)
 2. Converting remaining dashes to underscores (`_`)
 3. Assigning a value using an equal sign (`=`)

MSI Example:

```
msiexec /i bomgar-scc-win32.msi KEY_INFO=w0dc3056g7ff8d1j68ee6wi6dhwzfeeggzyzh7c40jc90
jc_jump_group=jumpgroup:server_support jc_tag=servers
```

When deploying an EXE installer, the above parameters can be specified by:

- Adding dashes
- Add a space between the parameter and the value instead of an equal sign

EXE Example:

```
bomgar-scc-[unique id].exe --jc-jump-group jumpgroup:servers --jc-tag servers
```

Other rules to consider:


- `installdir` has a dash in the EXE version but no dashes in the MSI version.
- `/quiet` is used for the MSI version in place of `--silent` in the EXE version.


 For more information, please see [Mass Deploying BeyondTrust Software to Macs at https://www.beyondtrust.com/docs/remote-support/how-to/mass-deploy-mac/index.htm](https://www.beyondtrust.com/docs/remote-support/how-to/mass-deploy-mac/index.htm).

Download or Install the Client Now

Platform

Choose the operating system on which you wish to install this software. This dropdown defaults to the appropriate installer detected for your operating system.

 **Note:** Unlike the representative console, Jump Clients installed from an MSI do auto-update.

 **Note:** To install a Jump Client in service mode on a Linux system, the Jump Client installer must be run by root, but the Jump Client service should not be run under the root user context. A service mode Jump Client allows the user to start a session even if no remote user is logged on, as well as to log off the current remote user and log on with different credentials. A Linux Jump Client installed in user mode cannot be elevated within a session.

Use the following syntax to add executable permissions to the file, wherein **{uid}** is a unique identifier consisting of letter and numbers:

1. Add executable permissions to the file:

```
sudo chmod +x ./Downloads/bomgar-scc-[uid].desktop
```

2. Run the installer as the root user using the **sudo** command:

```
sudo sh ./Downloads/bomgar-scc-[uid].desktop
```

Download/Install

You can download the installer immediately if you plan to distribute it using a systems management tool or if you are at the computer to which you need later access.



Note: Once the installer has run, the Jump Client attempts to connect to the B Series Appliance. When it succeeds, the Jump Client appears in the Jump interface of the representative console. If the Jump Client cannot immediately reach the B Series Appliance, then it continues to reattempt connection until it succeeds. If it cannot connect within the time designated by **This Installer Is Valid For**, then the Jump Client uninstalls from the remote system and must be redeployed.

Deploy to Email Recipients

Email

You can also email the installer to one or more remote users. Multiple recipients can install the client from the same link. Click on the **Direct Download Link** to copy the link.



For more information on the Mass Deployment Wizard, please see [Deploy Jump Clients During a Support Session or Prior to Support](https://www.beyondtrust.com/docs/remote-support/how-to/jump-clients/deploying.htm) at <https://www.beyondtrust.com/docs/remote-support/how-to/jump-clients/deploying.htm>.

Jump Client Statistics

An administrator can choose which statistics to view for all Jump Clients on a site-wide basis. These statistics are displayed in the representative console and include CPU, console user, disk usage, a thumbnail of the remote screen, and uptime.

Active Jump Client Statistics Update Interval

The **Active Jump Client Statistics Update Interval** determines how often these statistics are updated. Managing which statistics are viewed and how often can help to regulate the amount of bandwidth used. The more active Jump Clients you have deployed, the fewer the statistics and the longer the interval may need to be.

Upgrade

Maximum bandwidth of concurrent Jump Client upgrades

You can regulate the bandwidth used during upgrades by setting **Maximum bandwidth of concurrent Jump Client upgrades**. The maximum upgrade bandwidth is 100MiB/s.



Note: This setting does not affect representative console upgrades or Support Button deployments.

Maximum number of concurrent Jump Client upgrades

Set the maximum number of Jump Clients to upgrade at the same time. Note that if you have a large number of Jump Clients deployed, you may need to limit this number to regulate the amount of bandwidth consumed. The maximum number allowed is 500.



Note: This setting does not affect representative console upgrades or Support Button deployments.

Automatic Jump Client Upgrades

Use the radio buttons below to control automatic Jump Client upgrades. You can:

- Permanently disable Jump Client upgrades.
- Temporarily enable Jump Client upgrades for the current upgrade cycle.
- Permanently enable Jump Client upgrades.



Note: In order to be able to manually update Jump Clients in the Web Rep Console, you must first disable Automatic Jump Client Upgrades.

Maintenance

Number of days before Jump Clients that have not connected are automatically deleted

If a Jump Client goes offline and does not reconnect to the B Series Appliance for the number of days specified by the **Number of days before Jump Clients that have not connected are automatically deleted** setting, it is automatically uninstalled from the target computer and is removed from the Jump interface of the representative console.



Note: This setting is shared with the Jump Client during normal operation so that even if it cannot communicate with the site, it uninstalls itself at the configured time. If this setting is changed after the Jump Client loses connection with the B Series Appliance, it uninstalls itself at the previously configured time.



Note: The setting must be configured for 15 days or more.

Number of days before Jump Clients that have not connected are considered lost

If a Jump Client goes offline and does not reconnect to the B Series Appliance for the number of days specified by the **Number of days before Jump Clients that have not connected are considered lost** setting, it is labeled as lost in the representative console. No specific action is taken on the Jump Client at this time. It is labeled as lost only for identification purposes, so that an administrator can diagnose the reason for the lost connection and take action to correct the situation.



Note: To allow you to identify lost Jump Clients before they are automatically deleted, set this field to a smaller number than the deletion field above.



Note: The setting must be configured for 15 days or more.



Tip: You can set Jump Clients to allow or disallow simultaneous Jumps from the **Jump > Jump Items > Jump Settings** section. If allowed, multiple users can gain access to the same Jump Client without an invitation to join an active session by another user. If disallowed, only one user can Jump to a Jump Client at a time. Only an invitation by the user who originated the session can allow for a second user to access the session.



For more information, please see [Configure Jump Client Settings](https://www.beyondtrust.com/docs/remote-support/how-to/jump-clients/settings.htm) at <https://www.beyondtrust.com/docs/remote-support/how-to/jump-clients/settings.htm>.

Uninstalled Jump Client Behavior

Uninstalled Jump Client Behavior determines how a Jump Client deleted by an end user is handled by the representative console. Depending on the option made in the dropdown, the deleted item can either be marked as uninstalled and kept in the list or actually be removed from the list of Jump Items in the representative console. If the Jump Client cannot contact the B Series Appliance at the time it is uninstalled, the affected item remains in its offline state.

Restrict Local Uninstall/Disable of Jump Clients

Restrict Local Uninstall/Disable of Jump Clients limits the remote user's ability to uninstall or disable Jump Clients from the right-click context menu, reducing the need to reinstall Jump Clients that should not have been uninstalled. If this option is enabled, only users with appropriate privileges on the target machine may uninstall the Jump Client via the host system's *uninstall programs* mechanism.

Miscellaneous

Allow Representatives to attempt to wake up Jump Clients

Allow Representatives to attempt to wake up Jump Clients provides a way to wake up a selected Jump Client by broadcasting Wake-on-LAN (WOL) packets through another Jump Client on the same network. Once a WOL is attempted, the option becomes unavailable for 30 seconds before a subsequent attempt can be made. WOL must be enabled on the target computer and its network for

this function to work. The default gateway information of the Jump Client is used to determine if other Jump Clients reside on the same network. When sending a WOL packet, the user has an advanced option to provide a password for WOL environments that require a secure WOL password.

Use screen state to detect Customer Presence

Use screen state to detect Customer Presence sets how customer presence is determined. Customer presence is used when choosing whether to use the Customer Present Session Policy or the Customer Not Present Session Policy. If checked, the customer is determined to be present only if a user is logged in, the screen is not locked, and a screen saver is not running. If unchecked, the customer is considered present if a user is logged in, regardless of screen state.

Allow ad-hoc sessions to be started from existing Jump Clients

If this option is checked, and there is already a Jump Client installed on the user's system, an elevated session launches from the existing Jump Client. This applies to both the portal and the session generation API.



Note: For the elevated session to start, a similar permission must be granted for each Public Portal. Please see "[Attempt to launch sessions from installed Jump Clients](#)" on page 199.

Jump Groups: Configure Which Representatives Can Access Which Jump Items

 Jump

JUMP GROUPS

Jump Groups

A Jump Group is a way to organize Jump Items, granting members varying levels of access to those items. Users are assigned to Jump Groups from this page or from the **Users & Security > Group Policies** page.

Add New Jump Group, Edit, Delete

Create a new group, modify an existing group, or remove an existing group.

Search Jump Groups

To quickly find an existing group in the list of **Jump Groups**, enter the name, part of the name, or a term from the comments. The list filters all groups with a name or comment containing the entered search term. The list remains filtered until the search term is removed, even if the user goes to other pages or logs out. To remove the search term, click the **X** to the right of the search box.

Add or Edit Group

Name

Create a unique name to help identify this group. This name helps when adding Jump Items to a group as well as when determining which users, and group policies are members of a Jump Group.

Code Name

Set a code name for integration purposes. If you do not set a code name, one is created automatically.

Comments

Add a brief description to summarize the purpose of this Jump Group.

Group Policies

This displays a listing of the group policies which assign users to this Jump Group.

Allowed Users

Search for users to add to this Jump Group. You can set each user's **New Member Role** to set their permissions specific to Jump Items in this Jump Group, or you can use the user's default Jump Item Roles as set on the **Users & Security > Group Policies** page or the **Users & Security > Users** page. A Jump Item Role is a predefined set of permissions regarding Jump Item management and usage.

Existing Jump Group users are shown in a table, along with their assigned role and how the role was granted. You can filter the view by entering a string in the **Filter by name** text box. You can also edit a user's settings or delete a user from the Jump Group.

To add groups of users to a Jump Group, go to **Users & Security > Group Policies** and assign that group to one or more Jump Groups.



Note: Edit and delete functionality may be disabled for some users. This occurs either when a user is added via group policy or when a user's system Jump Item Role is set to anything other than **No Access**.

You can click the group policy link to modify the policy as a whole. Any changes made to the group policy apply to all members of that group policy.

You can click the user link to modify the user's system Jump Item role. Any changes to the user's system Jump Item role apply to all other Jump Groups in which the user is an unassigned member.

You also can add the individual to the group, overriding their settings as defined elsewhere.



For more information, please see [Use Jump Groups to Determine Which Users Can Access Which Jump Items](https://www.beyondtrust.com/docs/remote-support/how-to/jumpoint/jump-groups.htm) at <https://www.beyondtrust.com/docs/remote-support/how-to/jumpoint/jump-groups.htm>.

Jump Policies: Set Schedules for Jump Clients

 Jump

JUMP POLICIES

Jump Policies

Jump Policies are used to control when certain Jump Items can be accessed by implementing schedules.



For more information on creating and using Jump Policies, please see [Create Jump Policies to Apply to Jump Items at https://www.beyondtrust.com/docs/remote-support/how-to/jumpoint/policies.htm](https://www.beyondtrust.com/docs/remote-support/how-to/jumpoint/policies.htm).

Add, Edit, Delete

Create a new policy, modify an existing policy, or remove an existing policy.

Add or Edit a Policy

Display Name

Create a unique name to help identify this policy. This name should help users identify this policy when assigning it to Jump Clients.

Code Name

Set a code name for integration purposes. If you do not set a code name, one is created automatically.

Description

Add a brief description to summarize the purpose of this policy.

Jump Schedule: Enabled

Set a schedule to define when Jump Items under this policy can be accessed. Set the time zone you want to use for this schedule, and then add one or more schedule entries. For each entry, set the start day and time and the end day and time.

If, for instance, the time is set to start at 8 PM and end at 5 PM, a user can start a session using this Jump Item at any time during this window but may continue to work past the set end time. Attempting to re-access this Jump Item after 5 PM, however, results in a notification that the schedule does not permit a session to start. If necessary, the user may choose to override the schedule restriction and start the session anyway.

Force session to end when schedule does not permit access

If stricter access control is required, check **Force session to end when schedule does not permit access**. This forces the session to disconnect at the scheduled end time. In this case, the user receives recurring notifications beginning 15 minutes prior to being

disconnected.

Jump Item Roles: Configure Permission Sets for Jump Items

 Jump

JUMP ITEM ROLES

Jump Item Roles

A Jump Item Role is a predefined set of permissions regarding Jump Item management and usage. Jump Item Roles are applied to users from the **Jump > Jump Item Roles** page or from the **Users & Security > Group Policies** page.

If more than one role is assigned to a user, then the most specific role for a user is always used. The order of specificity for Jump Item Roles, from most specific to least specific, is:

- The role assigned to the relationship between a user and a Jump Group on the **Jump > Jump Item Roles** page
- The role assigned to the relationship between a user and a Jump Group on the **Users & Security > Group Policies** page
- The **Jump Item Roles** configured for a user on the **Users & Security > Users** page or the **Users & Security > Group Policies** page



Note: A new **Jump Item Role** called **Auditor** is automatically created on new site installations. On existing installations it has to be created. This role only has a single **View Reports** permission enabled, giving admins the option to grant a user just the permission to run Jump Item reports, without the need to grant any other permission.

Add New Jump Item Role, Edit, Delete

Create a new role, modify an existing role, or remove an existing role.

Add or Edit Jump Item Role

Name

Create a unique name to help identify this role. This name helps when linking a Jump Item Role with a user or group of users in a Jump Group.

Description

Add a brief description to summarize the purpose of this role.

Permissions

Jump Group or Personal Jump Items

Create and deploy new Jump Items

Enables the user to create Jump Items and install them on remote systems.

Move and Copy Jump Items

Enables the user to move or copy Jump Items from one Jump Group into another. This permission must be enabled on both Jump Groups. Copied Jump Items can be edited.

 For more information on how to copy Jump Items, please see [Jump Items: Use Jump Items to Support Remote Systems at https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/jump-interface.htm](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/jump-interface.htm).

Remove existing Jump Items

Enables the user to delete Jump Items.

Jump Item

Start Sessions

Enables the user to Jump to remote systems.

Edit Tag

Enables the user to edit a Jump Item's tag field.

Edit Comments

Enables the user to edit a Jump Item's comments field.

Edit Public Portal

Enables the user to set the public portal with which a Jump Item is associated.

Edit Jump Policy

Enables the user to set which, if any, Jump Policy is applied to a Jump Item.

Edit Session Policy

Enables the user to set which, if any, session policy a Jump Item should use. Changing the session policy may affect the permissions allowed in the session.

Edit Connectivity and Authentication

Enables the user to modify a Jump Item's connection and authentication information. This includes such fields as hostname, Jumpoint, port, and username, among others.

Edit Behavior and Experience

Enables the user to modify the behavior of Jump Items. This includes such fields as connection type, display size, and terminal type, among others.



For more information, please see [Use Jump Item Roles to Create Permission Sets for Jump Items at https://www.beyondtrust.com/docs/remote-support/how-to/jumpoint/jump-item-roles.htm](https://www.beyondtrust.com/docs/remote-support/how-to/jumpoint/jump-item-roles.htm).

Jumpoint: Set Up Unattended Access to a Network



JUMPOINT

Jumpoint Management

BeyondTrust's Jump Technology enables a user to access computers on a remote network without having to pre-install software on every machine. Simply install a single Jumpoint agent at any network location to gain unattended access to every PC within that network.

Add New Jumpoint, Edit, Delete

Create a new Jumpoint, modify an existing Jumpoint, or remove an existing Jumpoint.

Redeploy

Uninstall an existing Jumpoint and download an installer to replace the existing Jumpoint with a new one. Jump shortcuts associated with the existing Jumpoint will use the new Jumpoint once it is installed.



Note: When an existing Jumpoint is replaced, its configuration is not saved. The new Jumpoint must be reconfigured.

Enable network browsing

At the bottom of the **Jumpoint** page is the option to **Enable network browsing**. If checked, a permitted user can view and select systems from the network directory tree. If unchecked, a user can access a system through a Jumpoint only by entering the system's hostname or IP address. Either way, the user must provide valid credentials to the remote system before gaining access.

Add or Edit Jumpoints

Name

Create a unique name to help identify this Jumpoint. This name should help users locate this Jumpoint when they need to start a session with a computer on its same network.

Code Name

Set a code name for integration purposes. If you do not set a code name, one is created automatically.

Comments

Add comments to help identify the purpose of this Jumpoint.

Disabled

If checked, this Jumpoint is unavailable to make Jump connections.

Clustered

If checked, you will be able to add multiple, redundant nodes of the same Jumpoint on different host systems. This ensures that as long as at least one node remains online, the Jumpoint will be available.

Enable Shell Jump Method

If you want users to be able to connect to SSH-enabled and Telnet-enabled network devices through this Jumpoint, check **Enable Shell Jump Method**.

Group Policies

This displays a listing of the group policies which allow users access to this Jumpoint.

Allowed Users

New Member Name

Search for users to add to this Jumpoint. Users who are allowed to use this Jumpoint can start sessions with and/or create Jump Items connecting through this Jumpoint, as their permissions allow.

In the table below, view existing Jumpoint users. You can filter the view by entering a string in the **Filter by Name** text box. You can also delete the user from the Jumpoint.

To add a group of users to a Jumpoint, go to **Users & Security > Group Policies** and assign that group to one or more Jumpoints.



Note: You may see some users whose **Delete** options are disabled. This occurs when a user is added via group policy.


You can click the group policy link to modify the policy as a whole. Any changes made to the group policy apply to all members of that policy.

You also can add the individual to the Jumpoint, overriding their settings as defined elsewhere.



For more information, please also see [Configure and Install a Jumpoint at https://www.beyondtrust.com/docs/remote-support/how-to/jumpoint/installation-windows.htm](https://www.beyondtrust.com/docs/remote-support/how-to/jumpoint/installation-windows.htm).


Jump Items: Import Shortcuts to Jump Items


Jump

JUMP ITEMS

Jump Shortcuts Mass Import Wizard

Create Jump Shortcuts to start standard support sessions, to start Remote Desktop Protocol sessions or VNC sessions, to Shell Jump to SSH-enabled or Telnet-enabled network devices, or to start Intel® vPro sessions.



Note: Linux Jumpoints can only be used for RDP, SSH/Telnet, and VNC sessions, allowing for credential injection from user or Vault, as well as RemoteApp functionality and Shell Jump filtering. Clustered Jumpoints can only add new nodes of the same OS. You cannot mix Windows and Linux nodes.

When creating a large number of Jump shortcuts, it may be easier to import them via a spreadsheet than to add them one by one in the representative console.



For more information, please see [Use Jump Shortcuts to Jump to Remote Systems at https://www.beyondtrust.com/docs/remote-support/how-to/jumpoint/jump-shortcuts.htm](https://www.beyondtrust.com/docs/remote-support/how-to/jumpoint/jump-shortcuts.htm).

Download a Template Suitable for Importing Jump Shortcuts


From the dropdown in the **Jump Shortcuts Mass Import Wizard** section, select the type of Jump Item you wish to add, and then click **Download Template**. Using the text in the CSV template as column headers, add the information for each Jump shortcut you wish to import. Optional fields can be filled in or left blank.

Upload Jump Shortcuts Mass Import Template


Once you have completed filling out the template, click **Import Jump Shortcuts** to upload the CSV file containing the Jump Item information. The CSV file should use the format described in the tables below. The maximum file sized allowed to be uploaded at one time is 5 MB. Only one type of Jump Item can be included in each CSV file.

Local Jump Shortcut Help


Parameter	Description
Hostname	The hostname of the endpoint to be accessed by this Jump Item. This string has a maximum of 128 characters.
Name	Enter a Name for the Jump Item. This name identifies the item in the session tabs. This string has a maximum of 128 characters.
Jump Group	The code name of the Jump Group with which this Jump Item should be associated.

Parameter	Description
	 Note: When using the import method, a Jump Item cannot be associated with a personal list of Jump Items.
Tag (optional)	You can organize your Jump Items into categories by adding a tag. This string has a maximum of 1024 characters.
Comments (optional)	You can add comments to your Jump Items. This string has a maximum of 1024 characters.
Jump Policy (optional)	The code name of a Jump Policy. You can specify a Jump Policy to manage access to this Jump Item.
Public Portal (optional)	The public portal through which this Jump Item should connect.
Customer Present Session Policy (optional)	The code name of a session policy. You can specify a session policy to manage the permissions available on this Jump Item when a customer is present.
Customer Not Present Session Policy (optional)	The code name of a session policy. You can specify a session policy to manage the permissions available on this Jump Item when a customer is not present.


Remote Jump Shortcut Help

Parameter	Description
Hostname	The hostname of the endpoint to be accessed by this Jump Item. This string has a maximum of 128 characters.
Jumpoint	The code name of the Jumpoint through which the endpoint is accessed.
Name	Enter a Name for the Jump Item. This name identifies the item in the session tabs. This string has a maximum of 128 characters.
Jump Group	The code name of the Jump Group with which this Jump Item should be associated.  Note: When using the import method, a Jump Item cannot be associated with a personal list of Jump Items.
Tag (optional)	You can organize your Jump Items into categories by adding a tag. This string has a maximum of 1024 characters.
Comments (optional)	You can add comments to your Jump Items. This string has a maximum of 1024 characters.
Jump Policy (optional)	The code name of a Jump Policy. You can specify a Jump Policy to manage access to this Jump Item.
Public Portal (optional)	The public portal through which this Jump Item should connect.
Customer Present Session Policy (optional)	The code name of a session policy. You can specify a session policy to manage the permissions available on this Jump Item when a customer is present.
Customer Not Present Session Policy (optional)	The code name of a session policy. You can specify a session policy to manage the permissions available on this Jump Item when a customer is not present.

Local VNC Jump Shortcut Help


Parameter	Description
Hostname	The hostname of the endpoint to be accessed by this Jump Item. This string has a maximum of 128 characters.
Port (optional)	A valid port number from 100 to 65535 . Defaults to 5900 .
Name	Enter a Name for the Jump Item. This name identifies the item in the session tabs. This string has a maximum of 128 characters.
Jump Group	The code name of the Jump Group with which this Jump Item should be associated. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  Note: When using the import method, a Jump Item cannot be associated with a personal list of Jump Items. </div>
Tag (optional)	You can organize your Jump Items into categories by adding a tag. This string has a maximum of 1024 characters.
Comments (optional)	You can add comments to your Jump Items. This string has a maximum of 1024 characters.
Jump Policy (optional)	The code name of a Jump Policy. You can specify a Jump Policy to manage access to this Jump Item.
Public Portal (optional)	The public portal through which this Jump Item should connect.
Session Policy (optional)	The code name of a session policy. You can specify a session policy to manage the permissions available on this Jump Item.

Remote VNC Jump Shortcut Help

Parameter	Description
Hostname	The hostname of the endpoint to be accessed by this Jump Item. This string has a maximum of 128 characters.
Jumpoint	The code name of the Jumpoint through which the endpoint is accessed.
Port (optional)	A valid port number from 100 to 65535 . Defaults to 5900 .
Name	Enter a Name for the Jump Item. This name identifies the item in the session tabs. This string has a maximum of 128 characters.
Jump Group	The code name of the Jump Group with which this Jump Item should be associated. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  Note: When using the import method, a Jump Item cannot be associated with a personal list of Jump Items. </div>
Tag (optional)	You can organize your Jump Items into categories by adding a tag. This string has a maximum of 1024 characters.


Parameter	Description
Comments (optional)	You can add comments to your Jump Items. This string has a maximum of 1024 characters.
Jump Policy (optional)	The code name of a Jump Policy. You can specify a Jump Policy to manage access to this Jump Item.
Public Portal (optional)	The public portal through which this Jump Item should connect.
Session Policy (optional)	The code name of a session policy. You can specify a session policy to manage the permissions available on this Jump Item.

Remote RDP Jump Shortcut Help

Parameter	Description
Hostname	The hostname of the endpoint to be accessed by this Jump Item. This string has a maximum of 128 characters.
Jumpoint	The code name of the Jumpoint through which the endpoint is accessed.
Username (optional)	The username to sign in as.
Domain (optional)	The domain the endpoint is on.
Quality (optional)	The quality at which to view the remote system. Can be low (2-bit gray scale for the lowest bandwidth consumption), best_perf (default - 8-bit color for fast performance), perf_and_qual (16-bit for medium quality image and performance), best_qual (32-bit for the highest image resolution), or video_opt (VP9 codec for more fluid video). This cannot be changed during the remote desktop protocol (RDP) session.
Console Session (optional)	1 : Starts a console session. 0 : Starts a new session (default).
Ignore Untrusted Certificate (optional)	1 : Ignores certificate warnings. 0 : Shows a warning if the server's certificate cannot be verified.
Name	Enter a Name for the Jump Item. This name identifies the item in the session tabs. This string has a maximum of 128 characters.
Jump Group	The code name of the Jump Group with which this Jump Item should be associated. <div style="border: 1px solid black; background-color: #e1f5fe; padding: 5px;">  Note: When using the import method, a Jump Item cannot be associated with a personal list of Jump Items. </div>
Tag (optional)	You can organize your Jump Items into categories by adding a tag. This string has a maximum of 1024 characters.
Comments (optional)	You can add comments to your Jump Items. This string has a maximum of 1024 characters.
Jump Policy (optional)	The code name of a Jump Policy. You can specify a Jump Policy to manage access to this Jump Item.
Public Portal (optional)	The public portal through which this Jump Item should connect.
Session Policy (optional)	The code name of a session policy. You can specify a session policy to manage the permissions available


Parameter	Description
	on this Jump Item.

Local RDP Jump Shortcut Help


Parameter	Description
Hostname	The hostname of the endpoint to be accessed by this Jump Item. This string has a maximum of 128 characters.
Username (optional)	The username to sign in as.
Domain (optional)	The domain the endpoint is on.
Quality (optional)	The quality at which to view the remote system. Can be low (2-bit gray scale for the lowest bandwidth consumption), best_perf (default - 8-bit color for fast performance), perf_and_qual (16-bit for medium quality image and performance), best_qual (32-bit for the highest image resolution), or video_opt (VP9 codec for more fluid video). This cannot be changed during the remote desktop protocol (RDP) session.
Console Session (optional)	1 : Starts a console session. 0 : Starts a new session (default).
Ignore Untrusted Certificate (optional)	1 : Ignores certificate warnings. 0 : Shows a warning if the server's certificate cannot be verified.
Name	Enter a Name for the Jump Item. This name identifies the item in the session tabs. This string has a maximum of 128 characters.
Jump Group	The code name of the Jump Group with which this Jump Item should be associated. <div style="border: 1px solid black; background-color: #e6f2ff; padding: 5px; margin-top: 10px;">  Note: When using the import method, a Jump Item cannot be associated with a personal list of Jump Items. </div>
Tag (optional)	You can organize your Jump Items into categories by adding a tag. This string has a maximum of 1024 characters.
Comments (optional)	You can add comments to your Jump Items. This string has a maximum of 1024 characters.
Jump Policy (optional)	The code name of a Jump Policy. You can specify a Jump Policy to manage access to this Jump Item.
Public Portal (optional)	The public portal through which this Jump Item should connect.
Session Policy (optional)	The code name of a session policy. You can specify a session policy to manage the permissions available on this Jump Item.


Shell Jump Shortcut Help

Parameter	Description
Hostname	The hostname of the endpoint to be accessed by this Jump Item. This string has a maximum of 128

Parameter	Description
	characters.
Jumpoint	The code name of the Jumpoint through which the endpoint is accessed.
Username (optional)	The username to sign in as.
Protocol	Can be either ssh or telnet .
Port (optional)	A valid port number from 1 to 65535 . Defaults to 22 if the protocol is ssh or 23 if the protocol is telnet .
Terminal Type (optional)	Can be either xterm (default) or VT100 .
Keep-Alive (optional)	The number of seconds between each packet sent to keep an idle session from ending. Can be any number from 0 to 300 . 0 disables keep-alive (default).
Name	Enter a Name for the Jump Item. This name identifies the item in the session tabs. This string has a maximum of 128 characters.
Jump Group	The code name of the Jump Group with which this Jump Item should be associated. <div style="border: 1px solid black; background-color: #e1f5fe; padding: 5px;">  Note: When using the import method, a Jump Item cannot be associated with a personal list of Jump Items. </div>
Tag (optional)	You can organize your Jump Items into categories by adding a tag. This string has a maximum of 1024 characters.
Comments (optional)	You can add comments to your Jump Items. This string has a maximum of 1024 characters.
Jump Policy (optional)	The code name of a Jump Policy. You can specify a Jump Policy to manage access to this Jump Item.
Session Policy (optional)	The code name of a session policy. You can specify a session policy to manage the permissions available on this Jump Item.
Public Portal (optional)	The public portal through which this Jump Item should connect.

Intel vPro Shortcut Help

Parameter	Description
Hostname	The hostname of the endpoint to be accessed by this Jump Item. This string has a maximum of 128 characters.
Jumpoint	The code name of the Jumpoint through which the endpoint is accessed.
Name	Enter a Name for the Jump Item. This name identifies the item in the session tabs. This string has a maximum of 128 characters.
Jump Group	The code name of the Jump Group with which this Jump Item should be associated. <div style="border: 1px solid black; background-color: #e1f5fe; padding: 5px;">  Note: When using the import method, a Jump Item cannot be associated with a personal list of </div>

Parameter	Description
	 <i>Jump Items.</i>
Tag (optional)	You can organize your Jump Items into categories by adding a tag. This string has a maximum of 1024 characters.
Comments (optional)	You can add comments to your Jump Items. This string has a maximum of 1024 characters.
Jump Policy (optional)	The code name of a Jump Policy. You can specify a Jump Policy to manage access to this Jump Item.
Public Portal (optional)	The public portal through which this Jump Item should connect.

i For more information, please see [Use Jump Shortcuts to Jump to Remote Systems at https://www.beyondtrust.com/docs/remote-support/how-to/jumpoint/jump-shortcuts.htm](https://www.beyondtrust.com/docs/remote-support/how-to/jumpoint/jump-shortcuts.htm).

Jump Item Settings

Simultaneous Jumps

For Jump Client, Local Jump, Remote Jump, Local VNC, Remote VNC, Intel® vPro

Set **Simultaneous Jumps** to **Join Existing Session** to provide a way for multiple users to gain access to the same Jump Item without an invitation to join an active session by another user. The first user to access the Jump Item maintains ownership of the session. Users in a shared Jump session see each other and can chat.

If **Join Existing Session** is selected, there is an option to apply the setting to copies of Jump Clients.

- If checked, a user can join a session that was started from another copy of a Jump Client in a different Group. Session permissions are based on the original Jump Client that started the session.
- If not checked, a user cannot join a session that was started from another copy of a Jump Client, unless it is the same Jump Group.

Set this option to **Disallow Jump** to ensure only one user can Jump to a Jump Item at a time. Only an invitation by the user who originated the session can allow for a second user to access the session.

This setting applies to the following Jump Item types:

- Jump Client
- Local Jump
- Remote Jump
- Local VNC
- Remote VNC
- Shell Jump
- Intel® vPro

For Remote RDP, Local RDP

Set **Simultaneous Jumps** to **Start New Session** to provide a way for multiple users to gain access to the same Jump Item without an invitation to join an active session by another user. For RDP, multiple users may gain access to a Jump Item, but each starts an independent session.

Set this option to **Disallow Jump** to ensure only one user at a time can Jump to a Jump Item. Only an invitation by the user who originated the session can allow for a second user to access the session.

This setting applies to Local and Remote RDP Jump Item types only.

Vault for Remote Support

Discovery: Discover Accounts, Endpoints, and Services in a Domain



Vault

DISCOVERY

BeyondTrust Vault is a credential store that exists on the B Series Appliance, enabling discovery of and access to privileged credentials. You can manually add privileged credentials, or you can use the built-in discovery tool to scan and import Active Directory and local accounts into BeyondTrust Vault.



For more information, please see the [Vault Guide](https://www.beyondtrust.com/docs/remote-support/how-to/vault/index.htm) at <https://www.beyondtrust.com/docs/remote-support/how-to/vault/index.htm>.

Discovery: Windows Domain

With the BeyondTrust Vault add-on, you can discover Active Directory accounts, local accounts, Windows service accounts, and endpoints. Jumpoints are used to scan endpoints and discover the accounts associated with those endpoints.

Click **New Discovery Job** to initiate a discovery. The options are:

- **Windows Domain:** Discover endpoints, domain accounts, and local accounts accessible from a Jumpoint on a Windows domain.
- **Local Windows Accounts on Jump Clients:** Discover local Windows accounts on machines where an active, service mode Jump Client is currently online.



Note: The *Local Windows Accounts on Jump Clients* option only displays if you have the **Jump Clients** permission located in **Users & Security > Users > Representative Permissions > Jump Technology**. If you have any issues, contact your site administrator.

Click **Continue** to start the discovery process.

If you selected **Windows Domain**, follow the steps in the **Add Domain** section. If you selected **Local Windows Accounts on Jump Clients**, follow the steps in the **Discovery: Jump Client Search Criteria**.



For more information on Jumpoints, please see [BeyondTrustRemote Support Jumpoint Guide](https://www.beyondtrust.com/docs/remote-support/how-to/jumpoint/index.htm) at <https://www.beyondtrust.com/docs/remote-support/how-to/jumpoint/index.htm>.

Add Domain

DNS Name of the Domain

Enter the DNS name for your environment.

Jumpoint

Choose an existing Jumpoint located within the environment you wish to discover accounts.

Management Account

Select the management account needed to initiate the discovery job. Choose to use a new account, which requires a **Username**, **Password**, and **Password Confirmation** to be entered. Or choose to use an existing account discovered from a previous job or added manually in the **Accounts** section.

Username

Enter a valid username to use for discovery (username@domain).

Password

Enter a valid a password to user for discovery.

Confirm Password

Re-enter the password to confirm.



Note: You can define which parts of a domain to run a **Discovery/Import** job. Once you select the required fields for a **Discovery Job**, you can refine the search by specifying which OU's to target or entering LDAP queries.

Discovery Scope

Select the objects you wish Vault to discover:

- **Domain Accounts**
- **Endpoints**
- **Local Accounts**
- **Services**

You can enter a **Search Path**, or leave it blank to search all OUs and containers. You can also use an **LDAP Query** to narrow the scope of user accounts and endpoints searched.

Discovery: Jump Client Search Criteria

Enter one or more search criteria to find active Jump Clients you'd like to use to discover local Windows accounts. All text field searches are partial and case-insensitive. Jump Clients that match all the search criteria will be displayed on the next page for you to select before discovery begins.



Note: The following types of Jump Clients cannot be used for local account discovery and will not be included in the search results:



- *Jump Clients that are currently offline or disabled*
- *Jump Clients that are not running as an elevated service*
- *Jump Clients that are installed in a domain controller*
- *Passive Jump Clients*

Jump Groups

Administrators can search for Jump Clients via their Jump Groups and their attributes. If the user is not a member of any Jump Group, the **Jump Groups** selection section is grayed out and either a tool tip or note is shown indicating that user must be a member of at least one Jump Group to proceed with the Jump Client discovery process. This is similar to how domain discovery works when a user is not a member of a Jumpoint during discovery or not a member of a Jump Group when importing an endpoint.

You can search **All of Your shared Jump Groups** or **Specific Jump Groups**.

Jump Client Attributes

You can select one or more shared Jump Groups. Private Jump Groups are not supported.

One or more Jump Client attributes can be entered. If more than one search criteria is entered, only Jump Clients matching all criteria are used for discovery.

The following attributes can be used as search criteria:

- **Name:** The Jump Client's name as it appears in the **Name** column in the Representative Console.
- **Hostname:** The Jump Client's hostname as it appears in the **Hostname/IP** column of the Representative Console.
- **FQDN:** The Jump Client's fully qualified domain name, as it appears under the **FQDN** label of the Jump Client details pane in the Representative Console.
- **Tag:** The Jump Client's tag as it appears in the **Tag** column of the Representative Console.
- **Public/Private IP:** The Jump Client's public and private IP addresses, as they appear under the **Public IP** label of the Jump Client details pane in the Representative Console. Jump Clients whose IP address starts with the given search value will match.

Click **Continue** to initiate the discovery.

Discovery: Select Jump Clients

This screen displays the Jump Clients that will be used in discovery. Select one or more and click **Start Discovery**.

Discovery Results

The results display a list of discovered **Endpoints** and **Local Accounts**. Select one or more and click **Import Select**.

Import Discovered Items

A list of the selections you made displays.

Account Group

Select from which account group you want to import, then click **Start Import**. A warning display indicating this process cannot be stopped once it has started. Click **Yes** to proceed, or **No** to abort.

Importing

A message displays indicating the import was completed successfully. A list of **Endpoints** and **Local Accounts** displays.

Accounts

Search Shared/Personal Accounts

If you get an extensive list of accounts discovered, use the **Search** field to search accounts by **Name**, **Endpoint**, or **Description** (by **Name** and **Description** only for personal accounts).

Toggle between **Shared** and **Personal** accounts. Select one or more accounts. Click ... to **Rotate Password**, **Edit** or **Delete** the account. You can also click **Rotate** at the top of the page to rotate the password for the select accounts.

Discovery Jobs

View discovery jobs that are in progress for a specific domain, or review the results of successful and failed discovery jobs.

View Results

Click **View Results** for a discovery job to view the **Discovery Results**, which includes discovered endpoints, local accounts, domain accounts, and services found in the domain.

You can filter the list of items based on their attributes using the filter box above the grid. For each tab, click the **i** next to the filter box to see which attributes can be searched.

Select which endpoints, accounts, and services to import and store in your BeyondTrust Vault instance. For each list item you wish to import, check the box beside it and click **Import Selected**.



For more information, please see [Discover Domains, Endpoints, and Accounts Using BeyondTrust Vault at https://www.beyondtrust.com/docs/remote-support/how-to/vault/discovery.htm](https://www.beyondtrust.com/docs/remote-support/how-to/vault/discovery.htm).

Accounts: Manage Vault Accounts



Vault

ACCOUNTS

View and manage information about all discovered and manually added accounts.



Note: Vault can import, rotate, and manage up to 60,000 accounts.

Available information for shared accounts includes:

- **Type:** The type of account, specifically, whether it is a domain or a local account, or a generic password account.
- **Name:** The name of the account.
- **Username:** The username associated with the account.
- **Group:** The name of the account group to which the account belongs.
- **Endpoint:** The endpoint with which the account is associated.
- **Description:** Short description about the account.
- **Last Checkout:** The last time the account was checked out.
- **Password Age:** The age of the password.
- **Status:** The status of the account. For example, warnings, errors, and if the account is checked out are indicated in this column. This column is auto-hidden when there aren't any statuses to indicate for any accounts. Multiple statuses are stacked and indicated in different colors. You can mouse-hover over a specific status to view more details about it.



Tip: You can filter the list of shared accounts displayed using the filters for **Group** and **Password Age**.

Based on this information, you can perform various actions, including credential check-out/check-in and credential rotation.

Available information for personal accounts includes:

- **Type:** The type of account, specifically, whether it is a domain or a local account, or a generic password account.
- **Name:** The name of the account.
- **Owner:** The name of the person who created and owns the account.
- **Description:** Short description about the account.
- **Password Age:** The age of the password.



Tip: You can filter the list of shared accounts displayed using the filters for **Owner** and **Password Age**.

Accounts

Add Account

Click **Add** to manually add a shared or personal generic account to BeyondTrust Vault.

Search Shared Accounts

Search for a specific shared account or a group of accounts based on **Name**, **Endpoint Name**, and **Description**.

Select Visible Columns

Click the **Select Visible Columns** button (columns icon) above the **Accounts** grid and select the columns to display in the grid.

Check Out and Check In a Shared Account

Click **Check Out** to view and use the credential. When selected, the **Account Password** prompt appears, displaying the credential for 60 seconds to allow you to copy the password. Once the prompt is closed, the **Check In** option becomes available. When finished using the account, click **Check In** to check the password back into the system.



For more information, please see [Check Out Credentials from the /login Interface at https://www.beyondtrust.com/docs/remote-support/how-to/vault/check-out.htm](https://www.beyondtrust.com/docs/remote-support/how-to/vault/check-out.htm).

Ellipsis Menu for Shared Accounts

Click ... to view more actions, such as **Rotate Password**, **Edit**, and **Delete**. When **Rotate Password** is selected, the system automatically rotates or changes the password. When **Edit** is selected, you can modify the account's information. The **Delete** option removes the account from the **Accounts** list.



For more information, please see [Rotate Privileged Credentials Using BeyondTrust Vault at https://www.beyondtrust.com/docs/remote-support/how-to/vault/rotation.htm](https://www.beyondtrust.com/docs/remote-support/how-to/vault/rotation.htm).

Search Personal Accounts

Search for a specific personal account or a group of accounts based on **Name** and **Description**.

View Password for Personal Account

Click **View Password** to view and use the credential. When selected, the **Account Password** prompt appears, displaying the credential for 60 seconds to allow you to copy the password.

Edit Personal Account

Click **Edit Account** to modify the account's information, specifically **Name**, **Description**, **Username**, and **Password**.

Add Shared Account

The **Add > Shared Generic Account** option allows you to add accounts without having to run a discovery job. Instead, you can manually enter information about the account. This option is helpful in situations where a shared account or username/password combination can be used to access many different systems.

Name

Enter a name for the account.

Description

Enter a brief and memorable description of the account.

Username

Provide the username for the account.

Authentication

Select the authentication method for the account: **Password** or **SSH Private Key**, or **SSH Private Key With Certificate**.



Note: If you use an SSH private key for authentication, you must provide a private key for the account in OpenSSH format. Optionally, you can include the passphrase associated with the private key.

Password and Confirm Password

If **Password** is selected for authentication, you must enter the password for the account and confirm the password.

SSH Private Key

If **SSH Private Key** is selected for authentication, you must enter the SSH private key for the account.

SSH Private Key With Certificate

If **SSH Private Key With Certificate** is selected for authentication, you must enter the SSH private key for the account, and the SSH key passphrase if applicable. You must also provide the SSH public certificate for the account.

SSH Key Passphrase

If applicable, enter the SSH private key's passphrase.

Account Policy

Select a specific policy for the account or leave **Account Policy** set to the default value of **Inherit Policy Settings**, in which case the account inherits the policy settings of the account group. If no account group is selected for the account, the account inherits the policy settings set for the global default account policy on the **Vault > Options** page.

Account Group

Select a group from the list to add the shared account to an account group. If a group is not selected, the account is added to the **Default Group**.

Group Policies

If the account was added to any group policies, they are listed here, along with their Vault account roles.

Account Users

New User Name

Select users who are allowed to access this account, as well as their Vault account role, and then click **Add**.

New Member Role

Select the Vault account role for the new user, and then click **Add**. Users can be assigned one of two roles:

- **Inject** (default value): Users with this role can use this account in Remote Support sessions.
- **Inject and Checkout**: Users with this role can use this account in Remote Support sessions and can check out the account on `/login`. The **Checkout** permission has no affect on generic SSH accounts.



Note: The **Vault Account Role** is visible in the list of users added to the Vault Account.



Note: When upgrading to a BeyondTrustRemote Support installation with the Configurable Vault Checkout feature, all existing **Vault Account Memberships** that were configured in Group Policies before the upgrade will have their **Vault Account Role** set to **Inject and Checkout** by default after the upgrade.



IMPORTANT!

Vault Account Role Precedence: Vault Account Roles can be assigned to both users and group policies. This means the same user could have different roles for a single Vault account. One role could be assigned by the user's group policies, while a different role could be assigned by the user's explicit access to the Vault Account. In such cases, the system uses the most-specific role for that user. Therefore, the system will let the role assigned on the **Edit Vault Account** page override the role assigned on the user's group policy. When the role is overridden in such a way, the word "overridden" appears on the **Edit Vault Account** page for the user's group policy membership. This behavior is consistent with the order of precedence for Jump Item Roles.



Note: User accounts with the **Allowed to Administer Vault** permission are implicitly allowed to access every Vault account.

Jump Item Associations

Select the type of **Jump Item Associations** for the account. The **Jump Item Associations** setting determines which Jump Items the account is associated with, so the account is available only for relevant target machines in the representative console during credential injection attempts. Select one of the following associations methods:

- **Inherited from the Account Group:** Associations for this account are determined by the associations defined in this account's **Account Group**.
- **Any Jump Items:** This account can be injected within any session started from a Jump Item in which the account is applicable.
- **No Jump Items:** This account cannot be injected into any session started from a Jump Item.
- **Jump Items Matching Criteria:** This account can be injected only within sessions started from Jump Items that match the criteria you define, in which the account is applicable.
 - You can define a direct association between Vault accounts and specific Jump Items by selecting the Jump Items from the list, and then clicking **Add Jump Item**.
 - You can further define the association between Vault accounts and Jump Items by specifying matching criteria based on the following Jump Item attributes. If configured, the account is available for injection for any Jump Items that match the specified attribute criteria in addition to any specific Jump Items you added as matching criteria.
 - **Shared Jump Groups:** Select a Jump Group from the list.
 - **Name:** This filter is matched against the value that appears in the **Name** column of the jump item in the representative console.
 - **Hostname / IP:** This filter is matched against the value that appears in the **Hostname / IP** column of the Jump Item in the representative console.
 - **Tag:** This filter is matched against the value that appears in the **Tag** column of the Jump Item in the representative console.
 - **Comments:** This filter is matched against the value that appears in the **Comments** column of the Jump Item in the representative console.



*Tip: Click the **i** icon for each option and attribute to view more specific information about it.*



Note: Local accounts are available for injection within the endpoints on which they were discovered.

Add Personal Account

Name

Enter a name for the account.

Description

Enter a brief and memorable description of the account.

Username

Provide the username for the account.

Authentication

Select the authentication method for the account: **Password** or **SSH Private Key**, or **SSH Private Key With Certificate**.



Note: If an SSH private key is selected for authentication, you must provide a private key for the account in OpenSSH format. Optionally, you can include the passphrase associated with the private key.

Password and Confirm Password

If **Password** is selected for authentication, you must enter the password for the account and confirm the password.

SSH Private Key

If **SSH Private Key** is selected for authentication, you must enter the SSH private key for the account.

SSH Private Key With Certificate

If **SSH Private Key With Certificate** is selected for authentication, you must enter the SSH private key for the account, and the SSH key passphrase if applicable. You must also provide the SSH public certificate for the account.

SSH Key Passphrase

If applicable, enter the SSH private key's passphrase.

Edit Local Account

Name

View or edit the name used for the account.

Description

View or edit the description of the account.

Username

View the username associated with the account.

Password and Confirm Password

Enter a new password for the account, or leave the field blank to keep the existing password. Confirm the password entered.

Password Age

View the age of the existing password.

Account Policy

Select a specific policy for the account or leave **Account Policy** set to the default value of **Inherit Policy Settings**, in which case the account inherits the policy settings of the account group. If no account group is selected for the account, the account inherits the policy settings set for the global default account policy on the **Vault > Options** page.

Allow Simultaneous Checkout

If the account can be checked out and used by multiple users or sessions at the same time, select this option.

Account Group

Select a group from the list to add the shared account to an account group. If a group is not selected, the account is added to the **None** system group.

Endpoint Name

View which endpoint or endpoints are associated with the account.

Endpoint Hostname

View the hostname of the associated endpoints.

Account Users

Select users who are allowed to access this account, as well as their Vault account role, and then click **Add**.



Note: User accounts with the **Allowed to Administer Vault** permission are implicitly allowed to access every Vault account.

Jump Item Associations

Select the type of **Jump Item Associations** for the account. The **Jump Item Associations** setting determines which Jump Items the account is associated with, so the account is available only for relevant target machines in the representative console during credential injection attempts. Select one of the following associations methods:

- **Inherited from the Account Group:** Associations for this account are determined by the associations defined in this account's **Account Group**.
- **Any Jump Items:** This account can be injected within any session started from a Jump Item in which the account is applicable.
- **No Jump Items:** This account cannot be injected into any session started from a Jump Item.
- **Jump Items Matching Criteria:** This account can be injected only within sessions started from Jump Items that match the criteria you define, in which the account is applicable.
 - You can define a direct association between Vault accounts and specific Jump Items by selecting the Jump Items from the list, and then clicking **Add Jump Item**.
 - You can further define the association between Vault accounts and Jump Items by specifying matching criteria based on the following Jump Item attributes. If configured, the account is available for injection for any Jump Items that match the specified attribute criteria in addition to any specific Jump Items you added as matching criteria.

- **Shared Jump Groups:** Select a Jump Group from the list.
- **Name:** This filter is matched against the value that appears in the **Name** column of the jump item in the representative console.
- **Hostname / IP:** This filter is matched against the value that appears in the **Hostname / IP** column of the Jump Item in the representative console.
- **Tag:** This filter is matched against the value that appears in the **Tag** column of the Jump Item in the representative console.
- **Comments:** This filter is matched against the value that appears in the **Comments** column of the Jump Item in the representative console.

Edit Domain Account

Name

View or edit the name used for the account.

Description

View or edit the description of the account.

Username

View the username associated with the account.

Password and Confirm Password

Enter a new password for the account, or leave the field blank to keep the existing password. Confirm the password entered.

View Password History

View the dates and times of password changes. Click **Reveal** to temporarily show the password. Click **Use** to set the password of this account to that password.

Password Age

View the age of the existing password.

Account Policy

Select a specific policy for the account or leave **Account Policy** set to the default value of **Inherit Policy Settings**, in which case the account inherits the policy settings of the account group. If no account group is selected for the account, the account inherits the policy settings set for the global default account policy on the **Vault > Options** page.

Distinguished Name

View the distinguished name for the account.

Account Group

Select a group from the list to add the shared account to an account group. If a group is not selected, the account is added to the **Default Group**.

Account Users

Select users who are allowed to access this account, as well as their Vault account role, and then click **Add**.



Note: User accounts with the **Allowed to Administer Vault** permission are implicitly allowed to access every Vault account.

Jump Item Associations

Select the type of **Jump Item Associations** for the account. The **Jump Item Associations** setting determines which Jump Items the account is associated with, so the account is available only for relevant target machines in the representative console during credential injection attempts. Select one of the following associations methods:

- **Inherited from the Account Group:** Associations for this account are determined by the associations defined in this account's **Account Group**.
- **Any Jump Items:** This account can be injected within any session started from a Jump Item in which the account is applicable.
- **No Jump Items:** This account cannot be injected into any session started from a Jump Item.
- **Jump Items Matching Criteria:** This account can be injected only within sessions started from Jump Items that match the criteria you define, in which the account is applicable.
 - You can define a direct association between Vault accounts and specific Jump Items by selecting the Jump Items from the list, and then clicking **Add Jump Item**.
 - You can further define the association between Vault accounts and Jump Items by specifying matching criteria based on the following Jump Item attributes. If configured, the account is available for injection for any Jump Items that match the specified attribute criteria in addition to any specific Jump Items you added as matching criteria.
 - **Shared Jump Groups:** Select a Jump Group from the list.
 - **Name:** This filter is matched against the value that appears in the **Name** column of the jump item in the representative console.
 - **Hostname / IP:** This filter is matched against the value that appears in the **Hostname / IP** column of the Jump Item in the representative console.
 - **Tag:** This filter is matched against the value that appears in the **Tag** column of the Jump Item in the representative console.
 - **Comments:** This filter is matched against the value that appears in the **Comments** column of the Jump Item in the representative console.

Edit Personal Generic (Password) Account

Name

View or edit the name used for the account.

Description

View or edit the description of the account.

Username

View the username associated with the account.

Password and Confirm Password

Enter a new password for the account, or leave the field blank to keep the existing password. Confirm the password entered.

Vault Account Groups: Add and Manage Account Groups



Vault

ACCOUNT GROUPS

Shared Vault accounts can be added to an account group to allow Vault admins to grant users access to multiple shared Vault accounts more efficiently. Account groups can also be used to associate a group of shared Vault accounts to a group policy.



Note: A shared Vault account can belong to only one group at a time and personal Vault accounts cannot be added to an account group.

Account Groups

Add, view, and manage account groups.

Add Account Group

Click **Add** to add an account group, add Vault accounts to the group, and grant users access to the group of shared Vault accounts.

Search Account Groups

Search for a specific account groups based on **Name** or **Description**.

Add Account Group

The **Add Account Group** option allows you to add account groups for the purpose of granting users access to multiple Vault accounts at once.

Name

Enter a name for the account group.

Description

Enter a brief and memorable description of the account group.

Account Policy

Select a specific policy for the account group or leave **Account Policy** set to the default value of **Inherit Policy Settings**, in which case the accounts in this account group inherit the policy settings set for the global default account policy on the **Vault > Options** page.

Group Policies

If the account group was added to any group policies, they are listed here, along with their Vault account roles.

Accounts

Source Account Group

Filter the list of accounts available to add to the group by selecting a group from the **Source Account Group** list.

Search Selected Account Group

Filter the list of accounts available to add to the group by searching for an account group. You can search by **Name**, **Endpoint**, and **Description**.

Accounts in Group "Default Group"

List of Vault accounts available to add to the account group.

Add

Select accounts from the list of available groups, and then click **Add** to add them to the **Accounts in This Group** list.

Remove

Select accounts from the list of **Accounts in This Group**, and then click **Remove** to remove them from the account group.

Search This Account Group

Filter the list of **Accounts in This Group** by searching for an account group by **Name**, **Endpoint**, and **Description**.

Accounts in This Group

List of Vault accounts that exist in this account group.

Allowed Users

New User Name

Select users who are allowed to access this account.

New Member Role

Select the Vault account role for the new user, and then click **Add**. Users can be assigned one of two roles:

- **Inject** (default value): Users with this role can use this account in Remote Support sessions.
- **Inject and Checkout**: Users with this role can use this account in Remote Support sessions and can check out the account on **/login**. The **Checkout** permission has no effect on generic SSH accounts.



Note: The **Vault Account Role** is visible in the list of users added to the Vault account.

Jump Item Associations

Select the type of **Jump Item Associations** for the account group. The **Jump Item Associations** setting determines which Jump Items the accounts in this account group are associated with, so that only the accounts relevant to the target machine are available in the representative console during credential injection attempts. Select one of the following associations methods:

- **Any Jump Items:** Accounts in this group can be injected into any Jump Item session in which the accounts are applicable.
- **No Jump Items:** Accounts in this group cannot be injected into any Jump Item session.
- **Jump Items Matching Criteria:** Accounts in this group can be injected only into Jump Item sessions that match the criteria you define, in which the accounts are applicable.
 - You can define a direct association between applicable accounts in this account group and specific Jump Items by selecting the Jump Items from the list, and then clicking **Add Jump Item**.
 - You can further define the association between applicable accounts in this account group and Jump Items by specifying matching criteria based on the following Jump Item attributes. If configured, accounts in this account group are available for injection for any Jump Items that match the specified attribute criteria in addition to any specific Jump Items you added as matching criteria.
 - **Shared Jump Groups:** Select a Jump Group from the list.
 - **Name:** This filter is matched against the value that appears in the **Name** column of the Jump Item in the representative console.
 - **Hostname / IP:** This filter is matched against the value that appears in the **Hostname / IP** column of the Jump Item in the representative console.
 - **Tag:** This filter is matched against the value that appears in the **Tag** column of the Jump Item in the representative console.
 - **Comments:** This filter is matched against the value that appears in the **Comments** column of the Jump Item in the representative console.



Tip: Click the *i* icon for each option and attribute to view more specific information about it.



Note: Local accounts are available for injection within the endpoints on which they were discovered.

Account Policies: Add and Manage Account Policies



Vault

ACCOUNT POLICIES

Vault account policies provide a method to define account settings related to password rotation and credential checkout and apply those settings to multiple accounts at once.

Multiple account policies that apply to a single Vault account are applied in the following order, from top to bottom:

- The account policy associated with the Vault account
- The account policy associated with the Vault's account group
- The global default account policy settings

If multiple account policies define a setting, then the value from the first applied policy is used.

Account Policies

Add, view, and manage account policies.

Add Account Policy

Click **Add** to add an account policy.

Copy Account Policy

Click **Copy** to copy an existing account policy.

Edit Account Policy

Click **Edit** to modify an existing account policy.

Add Account Policy

Add a new account policy.

Display Name

Enter a name for the account policy.

Code Name

Set a code name for integration purposes. If you do not set a code name, Remote Support creates one automatically.

Description

Enter a brief and memorable description of the account policy.

Permissions

Automatic Password Management

Scheduled Password Rotation Rules

- Select **Allow** to schedule passwords for Vault accounts to automatically rotate when the password reaches a specified maximum age.
- Select **Deny** to disable scheduled password rotation for Vault accounts.

Maximum Password Age

If scheduled password rotation is enabled, specify the maximum number of days a password can be in place for Vault accounts before it is automatically rotated.

Account Settings

Automatically Rotate Credentials after Check In Rules

- Select **Allow** to automatically rotate passwords after a credential is checked in.
- Select **Deny** to disable the automatic rotation of passwords after a credential is checked in.

Allow Simultaneous Checkout Rules

- Select **Allow** to enable the ability for Vault credentials to be checked out simultaneously.
- Select **Deny** to disable the ability for Vault credentials to be checked out simultaneously.



Note: If a setting in an account policy is not defined, it inherits the settings from the global default account policy, configured from the **Vault > Options** page in /login.

Endpoints: Manage Discovered Endpoints



Vault

ENDPOINTS

Endpoints

View information about all discovered endpoints, such as the name, hostname, operating system, domain, and distinguished name of the system, along with information about the accounts associated with those systems.

Search Endpoints

Search for a specific endpoint or a group of endpoints based on **Name**, **Hostname**, **Description**, or **Domain Name**.

Select Visible Columns

Click the **Select Visible Columns** button (columns icon) above the **Endpoints** grid and select the columns to display in the grid.

Accounts

View the number of accounts associated with each endpoint. Click the **Accounts** link to view the accounts associated with the system.

Jump Items

View the number of jump items associated with each endpoint. Click the **Jump Items** link to view the jump items associated with the system.

Services

View the number of Windows services associated with each endpoint. Click the **Services** link to view the services associated with the system.

Edit

Modify the endpoint's information, specifically **Name**, **Description**, and **Hostname**.



Note: If Windows services were discovered and imported into the Vault, any service used by the endpoint is listed and the user account that runs the service is indicated.

Delete

Delete the endpoint from the **Endpoints** list.

Services: View and Manage Discovered Services



Vault

SERVICES

Services

View the list of services found during discovery along with their associated endpoints and accounts, as well as the last status for each service. You also have the option to restart the service upon rotation of the service account.

Search Account Groups

Search for specific services or a group of services based on **Short Name**, **Description**, **Endpoint (Hostname)** or **Username**.

Restart

Check the **Restart** box for the service to have the service restarted when the account running the service is rotated.

Delete

Delete the service from the **Services** list.

Domains: Add and Manage Domains



Vault

DOMAINS

Add, view, and manage information about your domains.

Domains

Add Domain

Click **Add** to manually add a new domain to the **Domains** list.

Domain Name

View the name of the domain.

Jumpoint

View the Jumpoint used to discover accounts and endpoints on the domain.

Management Account

View the management account associated with the Jumpoint and domain.

Discover

Click **Discover** to initiate the Jumpoint to scan and discover endpoints and accounts on the domain.

Edit

Click **Edit** to modify domain information.

Delete

Click **Delete** to delete this domain from the **Domains** list.

Add or Edit Domain

DNS Name

Enter the **DNS Name** of the domain.

Jumpoint

Choose an existing Jumpoint located within the environment you wish to discover accounts.

Management Account

Select the management account needed to initiate a discovery job for this domain. Choose to use a new account, which requires a **Username**, **Password**, and **Password Confirmation** to be entered. Or choose to use an existing account discovered from a previous job or added manually in the **Accounts** section.

Scheduled Domain Discovery

Enable and configure domain discovery to run on a set schedule.

Enable Scheduled Discovery

Check the box to enable the **Discovery Schedule** options.

Discovery Schedule

Select the days of the week and the time for the discovery job to run.

Discovery Scope

Select the objects you wish Vault to discover:

- **Domain Accounts**
- **Endpoints**
- **Local Accounts**
- **Services**

You can enter a **Search Path**, or leave it blank to search all OUs and containers. You can also use an **LDAP Query** to narrow the scope of user accounts and endpoints searched.

Options: Configure Global Default Account Policy Settings and Password Length for Account Rotation



Vault

OPTIONS

Global Options

Configure the settings for the global default account policy.

The global default account policy must define an option for each setting. If an account does not have a setting defined using a specific policy, it inherits the policy from the account group. If the account group does not have a setting defined using a specific policy, it inherits the policy from the global default account policy.

Automatic Password Management

Scheduled Password Rotation Rules

- Select **Allow** to schedule passwords for Vault accounts to automatically rotate when the password reaches a specified maximum age.
- Select **Deny** to disable scheduled password rotation for Vault accounts.

Maximum Password Age

If scheduled password rotation is enabled, specify the maximum number of days a password can be in place for Vault accounts before it is automatically rotated.

Account Settings

Automatically Rotate Credentials after Check In Rules

- Select **Allow** to automatically rotate passwords after a credential is checked in.
- Select **Deny** to disable the automatic rotation of passwords after a credential is checked in.

Allow Simultaneous Checkout Rules

- Select **Allow** to enable the ability for Vault credentials to be checked out simultaneously.
- Select **Deny** to disable the ability for Vault credentials to be checked out simultaneously.

Generated Passwords for Account Rotation

Define the length of passwords generated during account rotation for domain and local accounts. You may set a minimum length of **20** characters and a maximum length of **256** characters.



Note: Password lengths do not apply to SSH and personal accounts.

Password Length

Set the minimum and maximum number of characters allowed for the password generated during manual, automatic, and scheduled password rotation for accounts that are rotated through Windows API (non-Azure accounts).

Password Length of AADDS Accounts

Set the minimum and maximum number of characters allowed for the password generated during password rotation of Azure Active Directory Domain Services (AADDS) accounts through MS Graph API.

Rep Console

Rep Console Settings: Manage Default Rep Console Settings



Rep Console

REP CONSOLE SETTINGS

Manage Representative Console Settings

You can configure the default representative console settings for your entire user base, applying a consistent representative console user experience and increasing team efficiency. You can force settings, allow settings to be overridden by the user, or leave settings unmanaged. If you select **Unmanaged**, the BeyondTrust default setting will be displayed alongside for your consideration.

Each **Enable** or **Disable** setting provides an administrative checkbox option to become a forced setting. Forced settings take effect on the user's next login and do not allow configuration in the console. Unforced settings may be overridden by a user through the settings window in the representative console.



For more information, please see [Change Settings and Preferences in the Representative Console](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/settings.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/settings.htm>.

A forced setting cannot be overridden unless an administrator deselects the **Forced** checkbox option for that setting in the **/login** administrative interface.

Choose the settings you want to be the default for your users, and click the **Save** button at the bottom of the page.

Note that saved settings take effect only upon login to the console. Even if you save and apply the changes by clicking the **Apply Now** button at the top of the page, detailed later, the user will not use the new settings until login.

If, for instance, you wish to set up default settings for new users but leave existing users' settings unchanged, save your managed settings but do not apply them. This will make it so all new representative console logins will begin with your managed default settings. Existing users will have forced settings applied upon next login, but all other settings will remain unchanged.

Global Settings

Spell checking enabled

From the **Global Settings** section, you can choose to enable or disable spell check for chat and session notes. Currently, spell check is available for US English only.

Disable automatic session assignment on login

If automatic session assignment is disabled on login, then the user will not be assigned sessions automatically until they choose to opt in.

Configurable session side bar

Choose if you want the session menu icon to display, if the sidebar can be detached, and if the widgets on the session sidebar can be rearranged and resized.

Quick Start Buttons



For more information, please see *Representative Console User Interface* at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/representative-console-overview.htm>.



Note: Use the *Forced* option to prevent support reps from overriding the managed defaults.

Start Session

Display a **Start** button at the top of the representative console. Clicking this button walks the user through the ways your customer can start a support session.

Session Key

At the top of the representative console, display a session key generation button.

Support Buttons

At the top of the representative console, display a button to launch the Support Button management interface.

Shell Jump

At the top of the representative console, display a button to launch a Shell Jump session.

Jump To

At the top of the representative console, display a button to launch a local or remote Jump session.

Intel® vPro

At the top of the representative console, display a button to launch access to a provisioned vPro Jumpoint.

RDP

At the top of the representative console, display a button to launch an RDP session.

VNC

At the top of the representative console, display a button to launch a VNC session.

Start Presentation

At the top of the representative console, display a button to schedule or immediately start a new presentation.

Alerts

Audible alerts - Play a sound when a chat message is received

Choose if a sound should be played when the user receives a chat message. If unmanaged or if enabled and not forced, the user may designate a custom sound in WAV format no larger than 1MB.

Visual alerts - Flash the application icon when a chat message is received

Choose if the application icon should flash when the user receives a chat message.

Show status messages in support team chat windows

Choose if the team chat should include status messages, such as users logging in and out, or only chats sent between team members.

Pop-up Notifications

Team Queues

Choose if a user should receive a pop-up notification for chat messages received in a support team chat.

Support Sessions

Choose if a user should receive a pop-up notification for chat messages received in a support session

Audible alerts - Play a sound when a session enters any queue

Choose if a sound should be played when a session enters any of a user's queues.

Audible alerts - Play a sound when a session is overdue in team queues

Choose if a sound should be played when a session is overdue in a team queue.

Visual alerts - Flash the application icon when a session enters any queue

Choose if the application icon should flash when a session enters any of a user's queues.

Visual alerts - Flash the application icon when a session is overdue in team queues

Choose if the application icon should flash when a session is overdue in a team queue.

Prompt when new customer enters personal queue

Set if a user should be prompted when a session enters their personal queue.

Pop-up Notifications

Pop-up notifications appear independent of the representative console and on top of other windows. If the pop-up notification is enabled and not forced or left unmanaged, the user will be able to choose how they receive pop-up notifications.

Personal Queue - New Sessions, Transferred Sessions, Shared Sessions

Choose if a user should receive a pop-up notification for new sessions, transferred sessions, and/or shared sessions in this queue.

Team Queues - New Sessions, Transferred Sessions, Shared Sessions, Overdue Sessions

Choose if a user should receive a pop-up notification for new sessions, transferred sessions, shared sessions, and/or overdue sessions in this queue.

Pop-up Behavior - Location and Duration

Set the default location and duration for pop-up notifications.

Support Session Assignment Alerts

Audible alerts - Play a sound when a session is assigned

Choose if a sound should be played when a session is automatically assigned to a user.

Expiring Assignment Sound

Choose if a sound should be played when an automatically assigned session invitation is about to expire. The alert can be either an audio file or the system beep. If unmanaged or if enabled and not forced, the user may designate a custom sound in WAV format no larger than 1MB.

Support Sessions

Automatically request screen sharing

Choose whether you want your users' sessions to begin with chat only or to immediately request screen sharing.

Automatically detach

Choose if you want to open sessions as tabs in the representative console or to automatically detach sessions into new windows.

Prompt to elevate if customer's secure desktop is enabled

For situations where users may encounter support issues due to a customer's having enabled secure desktop, you can allow your users to be prompted to elevate to run with administrative rights when the session begins.

Default Quality

Set the default quality for screen sharing sessions.

Default Scaling

Set the default size for screen sharing sessions.

Automatically enter full screen mode when screen sharing starts

When screen sharing starts, the user can automatically enter full screen mode.

Automatically collapse the sidebar when full screen mode is used

When the screen sharing session enters full screen mode, the chat bar can automatically collapse.

Show My Screen

Automatically minimize window when showing screen

When a user shows their screen to a customer during a session, you can choose to leave the representative console open or to minimize it to the user's taskbar.

Command Shell

Number of lines of available command history

You can set the number of lines to save in the command shell history. The default value is 500 lines.

Save

Click **Save** to save all of the profile settings you have configured. The confirmation message **Settings profile was successfully edited** will appear at the top of the page. All users who log in to the representative console after you save a new profile will receive the new settings as the default settings.

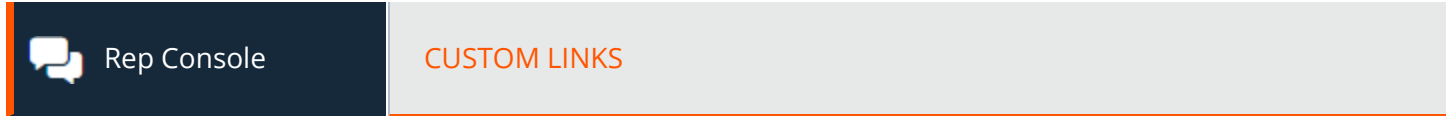
Apply Representative Console Settings

Apply Now

If you wish to push the default settings to your entire user base, click **Apply Now**. The top of the page displays a confirmation message, **Settings profile was successfully applied**.

After applying new settings to your user base, the users will receive an alert dialog for confirmation when they first log in to the representative console after you apply the settings. The dialog warns them that their settings have changed and prompts them with the option simply to acknowledge the dialog or to open their representative console settings window to review the changes.

Custom Links: Add URL Shortcuts to the Representative Console



Custom Links

Create links to sites your users can access during sessions. Examples could be a link to a searchable knowledge base, giving users a chance to look for a solution to the customer's issue, or a customer relationship management (CRM) system with escalation features. In this case, the link could open the CRM system to a page where the user could fill out an escalation form for a team that does not use BeyondTrust.

Links created here become available through the **Links** button on the representative console.

Add, Edit, Delete

Create a new link, modify an existing link, or remove an existing link.

Add or Edit Custom Link

Name

Create a unique name to help identify this link.

URL

Add the URL to which this custom link should direct. Use any of the macros listed below this field in the /login page to customize the text for your purposes.



For more information, please see [Support Session Overview and Tools](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm>.

Canned Messages: Create Messages for Chat



 For more information, please see *Chat with the Customer During a Session* at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/chat.htm>.

Canned Messages

Create canned messages to be used in chat sessions. Using canned messages can decrease response time and help to standardize communication between representatives and customers. You can filter your view by selecting a category or team from the dropdown at the top of the page.

Add, Edit, Delete

Create a new message, modify an existing message, or remove an existing message.

Add or Edit Canned Message

Title

Create a unique name to help identify this message. This name should help representatives locate the message they wish to send.

Message

Create the text that will display in the customer chat. You can use BBCode to do some low level formatting, such as adding bold, colors, or hyperlinks. Click on **Supported BBCode Formatting** to display a list of codes and their resulting applications.



Tip: Messages should be relatively short so they can be viewed without much scrolling in the customer client windows. This applies to both the native client and click-to-chat modes.

Category

Select the category under which this item should be listed.

Team Availability

Select which support teams should be able to use this item.

Canned Messages Categories

Add, Edit, Delete

Create a new category, modify an existing category, or remove an existing category.

Add or Edit Category

Name

Create a unique name to help identify this category. This name should help representatives locate the message they wish to send.

Parent Category

Optionally, select a parent category to nest categories.

Child Categories

View names of and links to any child categories.

Messages

View links to any messages in this category.

Canned Scripts: Create Scripts for Screen Sharing or Command Shell Sessions



Rep Console

CANNED SCRIPTS

Canned Scripts

Create custom scripts to be used in screen sharing and command shell sessions. The script will be displayed in the screen sharing or command shell interface as it is being executed. Executing a script in the screen sharing interface displays the running script on the remote screen. The script will run in the context of the logged-in user when the session is not elevated, and it will run as the local system when the session is elevated. You can filter your view by selecting a category or team from the dropdown at the top of the page.



For more information, please see [Support Session Overview and Tools](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm>.



For more information, please see [Access the Remote Command Shell](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/command-shell.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/command-shell.htm>.

Add, Edit, Delete

Create a new script, modify an existing script, or remove an existing script.

Add or Edit Canned Script

Script Name

Create a unique name to help identify this script. This name should help users locate the script they wish to run.

Description

Add a brief description to summarize the purpose of this script. This description is displayed on the prompt to confirm that the user wants to run the selected script.

Command Sequence

Write the command sequence. Scripts must be written in command line format, similar to writing a batch file or shell script. Note that only the last line of the script may be interactive; you cannot pause the script or prompt for input in the middle of the script.

Within the script, reference an associated resource file using "%RESOURCE_FILE%", making sure to include the quotation marks. Please note that the command sequence is case sensitive.

You can access the resource file's temporary directory using `%RESOURCE_DIR%`. When you run a script with an associated resource file, that file will be temporarily uploaded to the customer's computer.

Team Availability

Select which support teams should be able to use this item.

Categories

Select the categories under which this item should be listed.

Resource File

You may select a resource file to be associated with this script.

Elevation Mode

Select if this script should be available to run in elevated mode only, unelevated mode only, or both.

Available In View-Only Screen Sharing as a Special Action

If this option is checked, this script may be run even when the user is allowed only to view and not control the remote computer. Note that when the user is in view-only screen sharing, the customer receives a prompt to allow the script to run.



Note: If the user is allowed to use canned scripts, all canned scripts are available in full-control screen sharing, regardless of whether this option is checked or unchecked.



For more information, please see [Screen Share with the Remote Customer for View and Control](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/screen-sharing.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/screen-sharing.htm>.

Categories

Add Category, Delete

Create a new category or remove an existing category.

Resources

Choose and Upload Resource

Add any resource files you want to access from within your scripts. The maximum file size allowed is 250MB, with a maximum resource storage space of 1GB.

If you upload a resource file with the same name as an existing resource file, there is a prompt to confirm replacing the file.

- If you click **YES**, the updated resource file is uploaded and used for all applicable canned scripts.
- If you click **NO**, the file is not uploaded.

Delete

Remove an existing resource file.

Special Actions: Create Custom Special Actions



Rep Console

SPECIAL ACTIONS



For more information, please see [Screen Share with the Remote Customer for View and Control](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/screen-sharing.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/screen-sharing.htm>.

Special Actions

Create custom special actions to speed your processes. Custom special actions can be created for Windows, Mac, and Linux systems.

Add, Edit, Delete

Create a new action, modify an existing action, or remove an existing action.

Add or Edit Special Action

Action Name

Create a unique name to help identify this action. During a session, a user can see this name on the special actions dropdown.

Command

In the **Command** field, enter the full path of the application you wish to run. Do not use quotation marks; they will be added as necessary. Windows systems may make use of the macros provided. If the command cannot be located on the remote system, then this custom special action will not appear in the user's list of special actions.

Arguments

If the provided command will accept command line arguments, you may enter those arguments next. Arguments may use quotation marks if necessary, and arguments for Windows systems may use the provided macros.



For help with Windows arguments, search for "command line switches" on docs.microsoft.com/en-us/.

Confirm

If you check the **Confirm** box, then users will be prompted to confirm that they want to run this special action before it will execute. Otherwise, selecting the custom special action from the menu during a session will cause that special action to run immediately.

Run Elevated

Checking this option causes this special action to appear only when the customer client is running in elevated mode. When you run a custom action in elevated mode, you will be prompted either to run it as the system user or to provide credentials for another valid account on the remote system.

Special Actions Settings

Show Built-In Special Actions

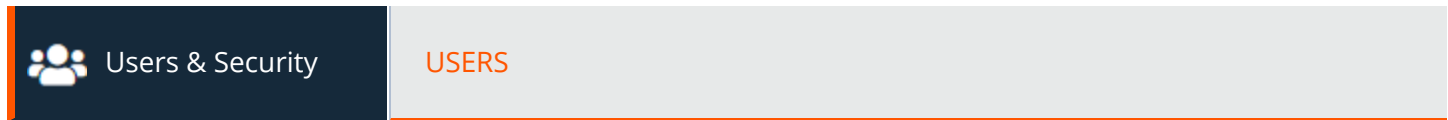
If you want to enable the default special actions provided by BeyondTrust, check **Show Built-In Special Actions**. Otherwise, to enable only your custom special actions, deselect this option.



Note: *The **Windows Security (Ctrl-Alt-Del)** and **Power Control Options** special actions cannot be disabled. Also, disabling the built-in special actions will not disable the default special actions for mobile devices.*

Users and Security

Users: Add User Permissions for a Representative or Admin



User Accounts

View information about all users who have access to your B Series Appliance, including local users and those who have access through security provider integration.

Add, Edit, Delete

Create a new account, modify an existing account, or remove an existing account. You cannot delete your own account.

Search Users

Search for a specific user based on **Last Authenticated As**, **Public Display Name**, **Private Display Name** and **Email Address**.

Security Provider

Select the security provider you want to search.

Synchronize

Synchronize the users and groups associated with an external security provider. Synchronization occurs automatically once a day. Clicking this button forces a manual synchronization.

Select Visible Columns

Use the dropdown menu to select which columns to display.

User Account Report

Export detailed information about your users for auditing purposes. Gather detailed information for all users, users from a specific security provider, or just local users. Information collected includes data displayed under the "show details" button, plus group policy and team memberships and permissions, and passwordless authentication registration and last usage.

Add or Edit User

After making your edits, click **Save** to save your changes to this user.

Username

Unique identifier used to log in.

Display Names

User's name as shown on the public site, in chats, etc. Users can use a public display name, for use with customers, and a private display name, for use in all internal communications.

Display Number

Type a unique ID number or leave this field blank to automatically select the next available number. This number affects the order in which users are listed on the public site.

Photo

Upload a photo to be used as a representative avatar, which is displayed in the customer client chat window and in the **/login** administrative interface. The image used must be in .png or .jpeg format, no more than 1 MiB in size, and with a minimum 80x80 pixel size. Click **Set Photo** to select an image. Set the image dimensions using the slider and the buttons **Fit in Box** and **Fill Entire Box**. When satisfied, click **Crop** to use it, or **Cancel**, if you do not wish to keep the image you just selected. Click **Change Photo** to select a new photo or **Delete Photo** to remove the avatar from this user.

The photo can also be changed or deleted from the **/login > My Account** page.

 For more information, please see *Customer Client: Support Session Interface* at <https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-support-interface.htm>.

Email Address

Set the email address to where email notifications are sent, such as password resets or extended availability mode alerts.

Preferred Email Language

If more than one language is enabled on this site, set the language in which to send emails.

Password

Password used with the username to log in. The password may be set to whatever you choose, as long as the string complies with the defined policy set on the **/login > Management > Security** page.

Must Reset Password at Next Login

If this option is selected, then the user must reset their password at next login.

Password Never Expires

If this option is selected, the password never expires.

Password Expiration Date

Causes the password to expire on a given date.

Memberships

Group Policy Memberships

Listing of the group policies to which the user belongs.

This section allows you to search or select from a dropdown of **Available Group Policies**, and **Add** the policy to the user. Policies selected for the user display in a list which can be filtered.

The user can be removed from one or more group policies by selecting the policy or policies and clicking **Remove**. The default policy cannot be selected.

Unsaved changes to the list are identified as **Addition** or **Removal**. Changes can be undone by selecting the policy or policies and clicking **Undo**.

If the user is a member of multiple group policies, the priority of the policies can be modified by selecting one or more policies and clicking **Priority**, at the upper right of the list.

Group policies selected for a user can be edited by clicking the name of the policy in the list.



Note: Other memberships do not display while a new user is being created. Once the new user has been saved, the other memberships appear, listing any to which the user may have been added, with links for updating these memberships and for reviewing or editing details about the memberships.

Team Memberships

Listing of the teams to which the user belongs.

Jumpoint Memberships

Listing of the Jumpoints which the user can access.

Jump Group Memberships

Listing of the Jump Groups to which the user belongs.

Vault Account Group Memberships

Listing of the Vault Account Groups to which the user belongs.

Account Settings

Decide if a setting should be **Defined** within this policy. If it is, you can select **Final** to prevent other policies of a lower priority from overriding the permission value set by this policy. Select **All** to define all settings in this section.

Two Factor Authentication: Log in with an Authenticator app

Select whether the user is required to log in using an authenticator app, or has the option to do so (default setting). If **Required** is selected, the next time the user tries to login to either the administrative interface or the representative console, a screen displays requiring the activation of two-factor authentication.



For more information on 2FA, please see [How to Use Two Factor Authentication with BeyondTrust Remote Support](https://www.beyondtrust.com/docs/remote-support/how-to/2-factor-authentication/) at www.beyondtrust.com/docs/remote-support/how-to/2-factor-authentication/.

Account Never Expires

If this option is selected, the account never expires.

Account Expiration Date

Causes the account to expire on a given date.

Account Disabled

Disables the account so the user cannot log in. Disabling does NOT delete the account.

Allowed to Change Their Display Names

Enables users to change their display names.

Allowed to Change Their Photo

Enables users to change their avatar photos, which display on the **/login** administrative interface and in the customer client chat window.

Allowed to Show on Public Site

Displays the user's name on all public sites that have the representative list enabled.

Comments

Add comments to help identify the purpose of this account.

Passwordless Authenticators

Listing of the passwordless authenticators registered for this user. Admins can view the name, type, registration timestamp, and last used timestamp. Admins can remove one or more authenticators from this list.

General Permissions

Decide if a setting should be **Defined** within this policy. If it is, you can select **Final** to prevent other policies of a lower priority from overriding the permission value set by this policy. Select **All** to define all settings in this section.

Administration

Administrator

Grants the user full administrative rights.

Allowed to Administer Vault

Enables the user to manage all aspects of the BeyondTrust Vault add-on.

Allowed to Set Passwords

Enables the user to set passwords and unlock accounts for non-administrative local users.

Allowed to Edit Jumpoints

Enables the user to create or edit Jumpoints. This option does not affect the user's ability to access remote computers via Jumpoint, which is configured per Jumpoint or group policy.

Allowed to Edit Public Site

Enables the user to create and modify public site configurations, edit HTML templates, view the translation interface, etc.

Allowed to Edit Customer Notices

Enables the user to create and edit messages used to notify customers, as they are requesting support, of broadly impacting IT outages.

Allowed to Edit File Store

Enables the user to add or remove files from the file store.

Allowed to Edit Canned Messages

Enables the user to create or edit canned chat messages.

Allowed to Edit Support Teams

Enables the user to create or edit support teams.

Allowed to Edit Jump Groups

Enables the user to create or edit Jump Groups.

Allowed to Edit Issues

Enables the user to create and edit issues.

Allowed to Edit Skills

Enables the user to create and edit skills.

Allowed to Edit Support Button Profiles

Enables the user to customize Support Button profiles.

Allowed to Edit Canned Scripts

Enables the user to create or edit canned scripts for use in screen sharing or command shell sessions.

Allowed to Edit Custom Rep Links

Enables the user to create or edit custom links.

Allowed to Edit Access Sponsors

Enables the user to create or edit access sponsor teams.

Allowed to Edit iOS Profiles

Enables the user to create, edit and upload Apple iOS Profile content for distribution to iOS device users.

Reporting

Allowed to View Support Session Reports

Enables the user to run reports on support session activity, viewing only sessions in which they were the primary representative, only sessions in which one of their teams was the primary team or one of their teammates was the primary representative, or all sessions.

Allowed to view support session recordings

Enables the user to view video recordings of screen sharing sessions, Show My Screen sessions, and command shell sessions.

Allowed to View License Usage Reports

Enables the user to run reports on BeyondTrust license usage.

Allowed to View Vault Reports

Enables the user to run reports on Vault activity, viewing all event data or only their event data.

Allowed to View Presentation Session Reports

Enables the user to run reports on presentation activity, viewing only presentations in which they were the presenter, only sessions in which one of their teammates was the presenter, or all presentations.

Allowed to View Support Session Recordings

Enables the user to view recordings of screen sharing sessions and command shell sessions. It does not affect presentation recordings.

Allowed to View License Usage Reports

Enables the user to view Representative License Report.

Allowed to View Syslog Reports

Enables the user to download a ZIP file containing all syslog files available on the appliance. Admins automatically have permissions to access this report. Non-admin users must request access to view this report.

Representative Permissions

Allowed to provide remote support

Enables the user to use the representative console in order to run support sessions. If support is enabled, options pertaining to remote support will also be available. Disable this setting for presentation-only users.

Session Management

Allowed to generate session keys for support sessions within the representative console

Enables the user to generate session keys to allow customers to start sessions with them directly.

i For more information, please see [Generate a Session Key to Start a Support Session at https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/session-keys.htm](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/session-keys.htm).

Allowed to generate access keys for sending iOS profiles

Enables the user to generate access keys to offer iOS content to iOS device users.

i For more information, please see [Generate an Apple iOS Profile Access Key at https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/apple-ios-access-key-management-interface.htm](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/apple-ios-access-key-management-interface.htm).

Allowed to manually accept sessions from a team queue

Enables the user to select and start sessions that are in one of their team queues.

i For more information, please see [Accept a Session to Start Support at https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/accepting-a-session.htm](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/accepting-a-session.htm).

Allowed to transfer sessions to teams which they do not belong to

Enables the user to transfer sessions to teams other than their own. If disabled, user interaction is restricted solely to the user's assigned teams.

i For more information, please see [Support Session Overview and Tools at https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm).

Allowed to share sessions with teams which they do not belong to

Enables the user to invite a less limited set of user to share sessions, not only their team members. Combined with the extended availability permission, this permission expands session sharing capabilities.

i For more information, please see [Support Session Overview and Tools at https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm).

Allowed to invite external support representatives

Enables the user to invite a third-party user to participate in a support session one time only.

i For more information, please see [Invite an External Representative to Join a Session at https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/rep-invite.htm](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/rep-invite.htm).

Allowed to use the Get Next Session feature

Enables the user to start supporting the oldest queued session from all of their teams simply by clicking a button.

i For more information, please see *Accept a Session to Start Support* at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/accepting-a-session.htm>.

Allowed to enable extended availability mode

Enables the user to receive email invitations from other users requesting to share a session even when they are not logged into the representative console.

i For more information, please see *Use Extended Availability to Stay Accessible When Not Logged In* at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/extended-availability.htm>.

Allowed to edit the external key

Enables the user to modify the external key from the session info pane of a session within the representative console.

i For more information, please see *Support Session Overview and Tools* at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm>.

Equilibrium

i For more information, please see *Equilibrium for Automatic Session Routing guide* at <https://www.beyondtrust.com/docs/remote-support/how-to/equilibrium/index.htm>.

Allowed to opt out of session assignments

Enables the representative to mark himself or herself as unavailable for sessions to be assigned using Equilibrium.

Do not assign sessions if the representative is participating in at least

Sets the least number of sessions the representative must be supporting before sessions will no longer be automatically assigned using Equilibrium.

Do not assign sessions if the representative has been idle for at least

Sets the least amount of time the representative must have been idle before sessions will no longer be automatically assigned using Equilibrium.

Rep to Rep Screen Sharing



For more information, please see *Share your Screen with Another Representative* at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/representative-screensharing.htm>.

Allowed to show screen to other representatives

Enables the user to share their screen with another user without the receiving user having to join a session. This option is available even if the user is not in a session.

Allowed to give control when showing screen to other representatives

Enables the user sharing their screen to give keyboard and mouse control to the user viewing their screen.

Support Buttons



For more information, please see *Support Session Overview and Tools* at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm>.

Allowed to deploy and manage Support Buttons in personal queue

Enables the user to deploy and manage personal Support Buttons. This setting affects deploying Support Buttons from both the web interface and the representative console. To deploy a Support Button from within a session, the **Support Button Deployment** session permission must also be allowed.

Allowed to manage Team Support Buttons

Enable the user to modify the Support Buttons deployed to teams they are a member of. If the user is a team lead or manager, they can modify the personal Support Buttons of any team members as well.



For more information, please see *Manage Support Buttons* at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-button-management-interface.htm>.

Allowed to change the Public Portal associated with Support Buttons

Enables the user to set the public portal through which a Support Button should connect. Because session policies may be applied to public portals, changing the portal may affect the permissions allowed in the session.

Allowed to deploy Team Support Buttons

Enables the user to deploy team Support Buttons for teams they are a member of. This setting affects deploying Support Buttons from both the web interface and the representative console. To deploy a Support Button from within a session, the **Support Buttons**

Deployment session permission must also be allowed.

Jump Technology

Allowed Jump Methods

Enables the user to Jump to computers using **Jump Clients**, **Local Jump**, **Local VNC**, **Local RDP**, **Remote Jump**, **Remote VNC**, **Remote RDP**, **Shell Jump**, and/or **Intel vPro**.

Jump Item Roles

A Jump Item Role is a predefined set of permissions regarding Jump Item management and usage. For each option, click the **Edit** button to open the Jump Item Role in a new tab.

The **Default** role is used only when **Use User's Default** is set for that user in a Jump Group.

The **Personal** role applies only to Jump Items pinned to the user's personal list of Jump Items.

The **Teams** role applies to Jump Items pinned to the personal list of Jump Items of a team member of a lower role. For example, a team manager can view team leads' and team members' personal Jump Items, and a team lead can view team members' personal Jump Items.

The **System** role applies to all other Jump Items in the system. For most users, this should be set to **No Access**. If set to any other option, the user is added to Jump Groups to which they would not normally be assigned, and in the representative console, they can see non-team members' personal lists of Jump Items.



For more information, please see [Use Jump Item Roles to Create Permission Sets for Jump Clients](https://www.beyondtrust.com/docs/remote-support/how-to/jump-clients/jump-item-roles.htm) at <https://www.beyondtrust.com/docs/remote-support/how-to/jump-clients/jump-item-roles.htm>.

Presentation

Allowed to give presentations

Enables the representative to give presentations to one or more attendees.



For more information, please see [Give a Presentation to Remote Attendees](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/presentation.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/presentation.htm>.

Allowed to grant control to a presentation attendee

Enables the representative to grant control of their computer to an attendee during a presentation. This setting affects only presentations and does not impact the Show My Screen feature of a support session. Only one attendee at a time can have control. The representative always maintains overriding control.



For more information, please see [Presentation Attendee Client: Join a Presentation](https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-presentation-interface.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-presentation-interface.htm>.

Representative Console

Idle Timeout

Set how long the representative can be idle before being logged out of the representative console. This permission can use the site-wide setting or can override that setting.

Attended and Unattended Session Permissions

Use the same permissions for Unattended sessions

To use the same permissions for both attended and unattended sessions, check **Use the same permissions for Unattended sessions**. Uncheck this box to define attended and unattended permissions separately. You can also copy the permissions from one to the other.

Check **Allow Elevated Access to Tools and Special Actions on the Endpoint** if desired, and if allowed by the Endpoint's platform.

Support Tool Prompting

i For more information, please see *Customer Client: Support Session Interface* at <https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-support-interface.htm>.

Prompting Rules

Choose to ask the customer permission to use any of the support features below. Select **No Prompting** to never prompt, **Always Prompt** to always prompt, or **Prompt for Some Tools** to choose which permissions to prompt for. If **Prompt for Some Tools** is chosen, a **Prompt Customer** option will appear beside each tool with the options to **Never** prompt or to **Always** prompt. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

Allowed to prompt once

If **Screen Sharing** is set to **View and Control** and prompting is enabled, this option appears. Check the box to make the screen sharing prompt request access to all tools during the session, with no further prompts.

Prompting Options

Set how long to wait for a response to a prompt before defaulting to the answer of **Deny** or **Allow**. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

Screen Sharing

Screen Sharing Rules

Enable the user to view or control the remote screen. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.



For more information, please see [Screen Share with the Remote Customer for View and Control](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/screen-sharing.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/screen-sharing.htm>.

Allowed to show their screen to the customer

Enables the user to share their screen with the customer during a support session. This option is available if **View Only** or **View or Control** is selected.



For more information, please see [Show My Screen: Reverse Screen Share](https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/show-my-screen.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/show-my-screen.htm>.

Allowed Customer Restrictions

Set if the user can suspend the remote system's mouse and keyboard input. The user may also prevent the remote desktop from being displayed. This option is available if **View and Control** is selected. If **Display, Mouse and Keyboard** is the selected Customer Restriction, a check box is available to **Automatically request a privacy screen on session start**. Privacy screen is applicable only for sessions started from a Jump Client, a Remote Jump item, or a Local Jump item. We recommend using privacy screen for unattended sessions. The remote system must support privacy screen.



For more information, please see [Restricted Customer Interaction: Privacy Screen, Disable Remote Input](https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/privacy-screen.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/privacy-screen.htm>.

Application Sharing Prompt Behavior

Set if a request for screen sharing should always or never prompt the customer to select applications to share, or if the user can choose whether to prompt for application sharing or not. Selecting **Always** or **Rep Decides** also allows you to predefine application sharing restrictions.



For more information, please see [Application Sharing: Limit What the Representative Can See](https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/application-sharing.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/application-sharing.htm>.

Clipboard Synchronization Direction

This option is available if **View and Control** is selected. Select how clipboard content flows between representatives and end users. The options are:

- **Not allowed:** The representative is not allowed to use the clipboard, no clipboard icons display in the representative console, and cut and paste commands do not work.
- **Allowed from Rep to Customer:** The representative can push clipboard content to the customer but cannot paste from the end user's clipboard. Only the Send clipboard icon displays in the representative console.
- **Allowed in Both Directions:** Clipboard content can flow both ways. Both Push and Get clipboard icons display in the representative console.

i For more information about the Clipboard Synchronization Mode, please see ["Security: Manage Security Settings" on page 237](#).

Annotations

Annotation Rules

Enables the user to use annotation tools to draw on the remote system's screen. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

i More more information, please see [Use Annotations to Draw on the Remote Screen at https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/annotations.htm](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/annotations.htm).

File Transfer

File Transfer Rules

Enables the user to upload files to the remote system, download files from the remote system, or both. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

Accessible paths on customer's filesystem

Allow the user to transfer files to or from any directories on the remote system or only specified directories.

Accessible paths on representative's filesystem

Allow the user to transfer files to or from any directories on their local system or only specified directories.

i For more information, please see [File Transfer to and from the Remote System at https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/file-transfer.htm](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/file-transfer.htm).

Command Shell

Command Shell Rules

Enables the user to issue commands on the remote computer through a virtual command line interface. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.



Note: Command shell access cannot be restricted for Shell Jump sessions.



For more information, please see [Access the Remote Command Shell](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/command-shell.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/command-shell.htm>.

System Information

System Information Rules

Enables the user to see system information about the remote computer. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

Allowed to use system information actions

Enables the user to interact with processes and programs on the remote system without requiring screen sharing. Kill processes; start, stop, pause, resume, and restart services; and uninstall programs.



For more information, please see [View Remote System Information](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/system-info.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/system-info.htm>.

Registry Access

Registry Access Rules

Enables the user to interact with the registry on a remote Windows system without requiring screen sharing. View, add, delete and edit keys, search and import/export keys.



For more information, please see [Access the Remote Registry Editor](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/registry-editor.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/registry-editor.htm>.

Canned Scripts

Canned Script Rules

Enables the user to run canned scripts that have been created for their teams. Note that when the user is in view-only screen sharing, the customer receives a prompt to allow the script to run. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.



For more information, please see [Access the Remote Command Shell](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/command-shell.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/command-shell.htm>.

Elevation

Elevation Rules

Enables the user to attempt to elevate the customer client to run with administrative rights on the remote system. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.



For more information, please see [Elevate the Client](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/elevation.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/elevation.htm>.

Support Button Deployment

Support Button Deployment Rules

Enables the user to deploy or remove a Support Button while in a session. Locations available for deployment depend on the Support Button settings above. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.



For more information, please see [Support Session Overview and Tools](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm>.

Jump Clients Pinning/Unpinning

Jump Clients Pinning/Unpinning Rules

Enables the user to pin or unpin a Jump Client while in a session. Locations available for deployment depend on the Jump Client settings above. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.



For more information, please see [Support Session Overview and Tools](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm>.

Chat

i For more information, please see *Chat with the Customer During a Session* at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/chat.htm>.

Chat Rules

Enables the user to chat with the remote customer. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

Allowed to push URLs to the customer's web browser

Enables the user to enter a URL into the chat area and then click the **Push URL** button to automatically open a web browser to that address on the remote computer.

Allowed to send files using the chat interface

Enables the user to send files via the chat interface.

i For more information, please see *Customer Client: Support Session Interface* at <https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-support-interface.htm>.

Session Termination Behavior

If unable to reconnect within the time you set by **Reconnect Timeout**, choose what action to take. To prevent an end-user from accessing unauthorized privileges after an elevated session, set the client to automatically log the end user out of the remote Windows computer at session end, to lock the remote computer, or to do nothing. These rules do not apply to browser sharing sessions.

Allow users to override this setting per session

You can allow a user to override the session termination setting from the **Summary** tab in the console during a session.

Availability Settings

Decide if a setting should be **Defined** within this policy. If it is, you can select **Final** to prevent other policies of a lower priority from overriding the permission value set by this policy. Select **All** to define all settings in this section.

Full Support License Pool

Choose the license pool to which this representative should belong. When this representative logs into the representative console, a license is consumed from the designated license pool. If **None** is selected, the representative will be able to log in to the representative console only if one or more licenses are left unassigned to license pools and are available.

Skills

Designates the skills assigned to this user. When using skills match for Equilibrium, sessions will be assigned to the user best skilled to handle a particular issue.

i For more information, please see [Assign Skills to Representatives](https://www.beyondtrust.com/docs/remote-support/how-to/equilibrium/assign-skills-rep.htm) at <https://www.beyondtrust.com/docs/remote-support/how-to/equilibrium/assign-skills-rep.htm>.

Login Schedule

Restrict representative log in to the following schedule

Set a schedule to define when users can log in to the representative console. Set the time zone you want to use for this schedule, and then add one or more schedule entries. For each entry, set the start day and time and the end day and time.

If, for instance, the time is set to start at 8 am and end at 5 pm, a user can log in at any time during this window but may continue to work past the set end time. They will not, however, be allowed to log back in after 5 pm.

Force logout when the schedule does not permit login

If stricter access control is required, check this option. This forces the user to log out at the scheduled end time. In this case, the user receives recurring notifications beginning 15 minutes prior to being disconnected. When the user is logged out, any owned sessions will follow the session fallback rules.

User Accounts for Password Reset: Allow Reps to Administer User Passwords



Users & Security

USERS

User Accounts

Administrators can delegate, via user permission, the task of resetting local users' passwords and locked user accounts to another user, without also granting full administrator permissions. Local users may continue to reset their own passwords.

When a privileged non-administrative user enters the **Users & Security > Users** page in the administrative /login interface, they see a limited-view **Users** screen containing **Change Password** links for non-administrative users. The privileged user is not able to edit or delete user accounts. Privileged users are not allowed to reset administrator passwords, or the passwords of security provider users.



Note: Administrators with the **Allowed to set passwords** permission will see no difference in the user interface.

Search Users

Search for a specific user based on **Last Authenticated As**, **Public Display Name**, **Private Display Name** and **Email Address**.

Select Visible Columns

Use the dropdown menu to select which columns to display.

Reset

If a user has one or more failed login attempts, click the **Reset** button beside their name to reset the number back to 0.

Change Password

Change the password for a non-administrative user.

Change Password

Username

Unique identifier used to log in. This field is not editable.

Display Names

User's name as shown on the public site, in chats, etc. Users can use a public display name, for use with customers, and a private display name, for use in all internal communications. This field is not editable.

Email Address

The email address to which email notifications are sent, such as password resets or extended availability mode alerts. This field is not editable.

Comments

Comments about the account. This field is not editable.

Password

The new password to assign to this user account. The password may be set to whatever you choose, as long as the string complies with the defined policy set on the **//login > Management > Security** page.

Email Password Reset Link to User

Send the user an email containing a link to reset the password for their account. This feature requires valid [SMTP](#) configuration for your B Series Appliance, set up on the **//login > Management > Email Configuration** page.

Must Reset Password at Next Login

If this option is selected, then the user must reset their password at next login.

Rep Invite: Create Profiles to Invite External Representatives to Sessions



Users & Security

REP INVITE

Rep Invitation Email

With rep invite, a privileged user can invite an external user to join a session one time only. The invitation email is sent when you invite the external rep to a session.

Select a public site to edit

From the dropdown at the top of the page, select the public site for which you want to edit the rep invitation email.

Subject

Customize the subject of this email. You can localize this text for any languages you have enabled.

Body

Customize the body of this email. Use any of the macros listed below this field in the /login page to customize the text for your purposes. You can localize this text for any languages you have enabled.



For more information, please see [Invite an External Representative to Join a Session at https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/rep-invite.htm](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/rep-invite.htm).

Security Providers: Enable LDAP, Active Directory, RADIUS, Kerberos, SAML for Reps, and SAML for Public Portals



Users & Security

SECURITY PROVIDERS

Security Providers

You can configure your BeyondTrust Appliance B Series to authenticate users against existing LDAP, RADIUS, Kerberos, or SAML servers, as well as to assign privileges based on the preexisting hierarchy and group settings already specified in your servers. Kerberos enables single sign-on, while RSA and other two-factor authentication mechanisms via RADIUS provide an additional level of security.

Add

Create a new security provider configuration. From the dropdown, select LDAP, RADIUS, Kerberos, SAML for Representatives, or SAML for Public Portals.

Change Order

Click this button to drag and drop security providers to set their priority. You can drag and drop servers within a cluster; clusters can be dragged and dropped as a whole. Click **Save Order** for prioritization changes to take effect.

Sync

Synchronize the users and groups associated with an external security provider. Synchronization occurs automatically once a day. Clicking this button forces a manual synchronization.

Disable

Disable this security provider connection. This is useful for scheduled maintenance, when you want a server to be offline but not deleted.

View Log

View the status history for a security provider connection.

Edit, Delete

Modify an existing provider or remove an existing provider.



Note: If you edit the local security provider and select a default policy that does not have administrator permissions, a warning message appears. Ensure other users have administrator permissions before proceeding.

Duplicate Node

Create a copy of an existing clustered security provider configuration. This will be added as a new node in the same cluster.

Upgrade to Cluster

Upgrade a security provider to a security provider cluster. To add more security providers to this cluster, copy an existing node.

Copy

Create a copy of an existing security provider configuration. This will be added as a top-level security provider and not as part of a cluster.

Add or Edit Security Provider: LDAP

Name

Create a unique name to help identify this provider.

Enabled

If checked, your BeyondTrust Appliance B Series can search this security provider when a user attempts to log in to the representative console or `/login`. If unchecked, this provider will not be searched.

User Authentication

This allows this provider to be used to authenticate users. If disabled, this provider may be used only to look up groups for user permissions.

Keep user information synchronized with the LDAP server

The display names are set according to the **User Schema Settings** defined below. If you are planning to sync a user's photo attribute, this option must be checked.

Authorization Settings

Synchronization: Enable LDAP object cache

If checked, LDAP objects visible to the B Series Appliance are cached and synchronized nightly, or manually, if desired. When using this option, fewer connections are made to the LDAP server for administrative purposes, thereby potentially increasing speed and efficiency.

If unchecked, changes to the LDAP server are immediately available without the need to synchronize. However, when you make changes on user policies through the administrative interface, several short-lived LDAP connections may occur as necessary.


For providers that have previously had the synchronization setting enabled, disabling the synchronization option will cause all cached records that are currently not in use to be deleted.


Lookup Groups

Choose to use this security provider only for user authentication, only for group lookups, or for both. **User Authentication** must be selected if you want to turn group lookup off.

Default Group Policy *(Visible Only if User Authentication Allowed)*

Each user who authenticates against an external server must be a member of at least one group policy in order to authenticate to your B Series Appliance, logging into either the /login interface or the representative console. You can select a default group policy to apply to all users allowed to authenticate against the configured server.


 **Note:** If a default policy is defined, then any allowed user who authenticates against this server will potentially have access at the level of this default policy. Therefore, it is recommended that you set the default to a policy with minimum privileges to prevent users from gaining permissions that you do not wish them to have.

 **Note:** If a user is in a default group policy and is then specifically added to another group policy, the settings for the specific policy will always take precedence over the settings for the default, even if the specific policy is a lower priority than the default, and even if the default policy's settings are set to disallow override.

Connection Settings *(Not Visible for Clusters)*

Hostname

Enter the hostname of the server that houses your external directory store.

 **Note:** If you will be using **LDAPS** or **LDAP with TLS**, the hostname must match the hostname used in your LDAP server's public SSL certificate's subject name or the DNS component of its alternate subject name.

Port

Specify the port for your LDAP server. This is typically port **389** for LDAP or port **636** for LDAPS. BeyondTrust also supports global catalog over port **3268** for LDAP or **3269** for LDAPS.

Encryption

Select the type of encryption to use when communicating with the LDAP server. For security purposes, **LDAPS** or **LDAP with TLS** is recommended.



Note: Regular LDAP sends and receives data in clear text from the LDAP server, potentially exposing sensitive user account information to packet sniffing. Both LDAPS and LDAP with TLS encrypt user data as it is transferred, making these methods recommended over regular LDAP. LDAP with TLS uses the StartTLS function to initiate a connection over clear text LDAP but then elevates this to an encrypted connection. LDAPS initiates the connection over an encrypted connection without sending any data in clear text whatsoever.

If you select **LDAPS** or **LDAP with TLS**, you must upload the Root SSL Certificate used by your LDAP server. This is necessary to ensure the validity of the server and the security of the data. The Root Certificate must be in PEM format.



Note: If the LDAP server's public SSL certificate's subject name or the DNS component of its alternate subject name does not match the value in the **Hostname** field, the provider will be treated as unreachable. You can, however, use a wildcard certificate to certify multiple subdomains of the same site. For example, a certificate for ***.example.com** would certify both **support.example.com** and **remote.example.com**.

Bind Credentials

Specify a username and password with which your B Series Appliance can bind to and search the LDAP directory store.

If your server supports anonymous binds, you may choose to bind without specifying a username and password. Anonymous binding is considered insecure and is disabled by default on most LDAP servers.

Connection Method

If you are using an external directory store in the same LAN as your BeyondTrust Appliance B Series, the two systems may be able to communicate directly, in which case you can leave the option **Proxy from appliance through the Connection Agent** unchecked and move on.

If the two systems are unable to communicate directly, such as if your external directory server is behind a firewall, you must use a connection agent. Downloading the Win32 connection agent enables your directory server and your B Series Appliance to communicate via an SSL-encrypted, outbound connection, with no firewall configuration. The connection agent can be downloaded to either the directory server or a separate server on the same network as your directory server (recommended).

In the case above, check **Proxy from appliance through the Connection Agent**. Create a **Connection Agent Password** for use in the connection agent installation process. Then click **Download Connection Agent**, run the installer, and follow the installation wizard. During installation, you will be prompted to enter the security provider name and the connection agent password you created above.

Directory Type *(Not Visible for Clusters)*

To aid in configuring the network connection between your B Series Appliance and your security provider, you can select a directory type as a template. This pre-populates the configuration fields below with standard data but must be modified to match your security provider's specific configuration. Active Directory LDAP is the most common server type, though you can configure BeyondTrust to communicate with most types of security providers.

Cluster Settings *(Visible Only for Clusters)*

Member Selection Algorithm

Select the method to search the nodes in this cluster.

Top-to-bottom first attempts the server with the highest priority in the cluster. If that server is unavailable or the account is not found, the next highest priority server is attempted. The search moves down through the list of clustered servers until either the account is found or it is determined that the account does not exist on any of the specified and available servers.

Round-robin is designed to balance the load between multiple servers. The algorithm chooses at random which server to attempt first. If that server is unavailable or the account is not found, another random server is attempted. The search continues at random through the remaining servers in the cluster until either the account is found or it is determined that the account does not exist on any of the specified and available servers.

Retry Delay

Set how long to wait after a cluster member becomes unavailable before trying that cluster member again.

User Schema Settings

Override Cluster Values *(Visible Only for Cluster Nodes)*

If this option is unchecked, this cluster node will use the same schema settings as the cluster. If checked, you may modify the schema settings below.

Search Base DN

Determine the level in your directory hierarchy, specified by a distinguished name, at which the B Series Appliance should begin searching for users. Depending on the size of your directory store and the users who require BeyondTrust accounts, you may improve performance by designating the specific organizational unit within your directory store that requires access. If you are not sure or if users span multiple organizational units, you may want to specify the root distinguished name of your directory store.

User Query

Specify the query information that the B Series Appliance should use to locate an LDAP user when the user attempts to log in. The **User Query** field accepts a standard LDAP query (RFC 2254 - String Representation of LDAP Search Filters). You can modify the query string to customize how your users log in and what methods of usernames are accepted. To specify the value within the string that should act as the username, replace that value with `*`.

Browse Query

The browse query affects how results are displayed when browsing via group policies. This filters results so that only certain results display in the member selection dropdown when adding members to a group policy.

Object Classes

Specify valid object classes for a user within your directory store. Only users who possess one or more of these object classes will be permitted to authenticate. These object classes are also used with the attribute names below to indicate to your B Series Appliance the schema the LDAP server uses to identify users. You can enter multiple object classes, one per line.

Attribute Names

Specify which fields should be used for a user's unique ID and display names.

Unique ID

This field requests a unique identifier for the object. While the distinguished name can serve as this ID, a user's distinguished name may change frequently over the life of the user, such as with a name or location change or with the renaming of the LDAP store. Therefore, most LDAP servers incorporate some field that is unique per object and does not change for the lifetime of the user. If you do use the distinguished name as the unique ID and a user's distinguished name changes, that user will be seen as a new user, and any changes made specifically to the individual's BeyondTrust user account will not be carried over to the new user. If your LDAP server does not incorporate a unique identifier, use a field that is least likely to have an identical entry for another user.

E-Mail

The email attribute synchronizes the user's email address from LDAP. Please note that the special ? and ! characters cannot be used.

Photo

This field allows you to configure LDAP providers to synchronize representative photos from LDAP. By default, the settings template for Active Directory, Novell eDirectory, and OpenLDAP all use the ***:jpegPhoto** attribute. Administrators can modify the attribute as necessary. If no attribute is specified, then no photos are retrieved from LDAP.

Photos in LDAP must be stored as a JPEG images, either as raw binary data or as Base64-encoded data. BeyondTrust Remote Support automatically detects the encoding and decodes it as needed.

Use the same attribute for public and private display names

If this option is checked, you may specify separate values for the user's private and public display names.

Display Names

These values determine which fields should be used as the user's private and public display names.

Group Schema Settings *(Visible Only if Performing Group Lookups)*

Search Base DN

Determine the level in your directory hierarchy, specified by a distinguished name, at which the B Series Appliance should begin searching for groups. Depending on the size of your directory store and the groups that require access to the B Series Appliance, you may improve performance by designating the specific organizational unit within your directory store that requires access. If you are not sure or if groups span multiple organizational units, you may want to specify the root distinguished name of your directory store.

Browse Query

The browse query affects how results are displayed when browsing via group policies. This filters results so that only certain results display in the member selection dropdown when adding members to a group policy.

Object Classes

Specify valid object classes for a group within your directory store. Only groups that possess one or more of these object classes will be returned. These object classes are also used with the attribute names below to indicate to your B Series Appliance the schema the LDAP server uses to identify groups. You can enter multiple group object classes, one per line.

Attribute Names

Specify which fields should be used for a group's unique ID and display name.

Unique ID

This field requests a unique identifier for the object. While the distinguished name can serve as this ID, a group's distinguished name may change frequently over the life of a group, such as with a location change or with the renaming of the LDAP store. Therefore, most LDAP servers incorporate some field that is unique per object and does not change for the lifetime of the group. If you do use the distinguished name as the unique ID and a group's distinguished name changes, that group will be seen as a new group, and any group policies defined for that group will not be carried over to the new group. If your LDAP server does not incorporate a unique identifier, use a field that is least likely to have an identical entry for another group.

Display Name

This value determines which field should be used as the group's display name.

User to Group Relationships

Relationships

This field requests a query to determine which users belong to which groups or, conversely, which groups contain which users.

Perform recursive search for groups

You can choose to perform a recursive search for groups. This will run a query for a user, then queries for all of the groups to which that user belongs, then queries for all groups to which those groups belong, and so forth, until all possible groups associated with that user have been found.

Running a recursive search can have a significant impact on performance, as the server will continue to issue queries until it has found information about all groups. If it takes too long, the user may be unable to log in.

A non-recursive search will issue only one query per user. If your LDAP server has a special field containing all of the groups to which the user belongs, recursive search is unnecessary. Recursive search is also unnecessary if your directory design does not handle group members of groups.

Test Settings

Username and Password

Enter a username and password for an account that exists on the server you are testing. This account must match the criteria for login specified in the configuration above.

Try to obtain user attributes and group memberships if the credentials are accepted

If this option is checked, your successful credential test will also attempt to check user attributes and group lookup.



Note: For these features to be successfully tested they must be supported and configured in your security provider.

Test

If your server is properly configured and you have entered a valid test username and password, you will receive a success message. Otherwise, you will see an error message and a log that will help in debugging the problem.



For more information, please see [Create and Configure the LDAP Security Provider](https://www.beyondtrust.com/docs/remote-support/how-to/integrations/security-providers/ldap-users/configure-settings.htm) at <https://www.beyondtrust.com/docs/remote-support/how-to/integrations/security-providers/ldap-users/configure-settings.htm>.

Add or Edit Security Provider: RADIUS

Name

Create a unique name to help identify this provider.

Enabled

If checked, your BeyondTrust Appliance B Series can search this security provider when a user attempts to log in to the representative console or `/login`. If unchecked, this provider will not be searched.

Keep display name synchronized with remote system

These values determine which fields should be used as the user's private and public display names.

Authorization Settings

Only allow the following users

You can choose to allow access only to specified users on your RADIUS server. Enter each username separated by a line break. Once entered, these users will be available from the **Add Policy Member** dialog when editing group policies on the `/login > Users & Security`

> **Group Policies** page.

If you leave this field blank, all users who authenticate against your RADIUS server will be allowed; if you allow all, you must also specify a default group policy.

Default Group Policy

Each user who authenticates against an external server must be a member of at least one group policy in order to authenticate to your B Series Appliance, logging into either the /login interface or the representative console. You can select a default group policy to apply to all users allowed to authenticate against the configured server.

LDAP Group Lookup

If you want users on this security provider to be associated with their groups on a separate LDAP server, choose one or more LDAP group servers to use for group lookup.

Connection Settings

Hostname

Enter the hostname of the server that houses your external directory store.

Port

Specify the authentication port for your RADIUS server. This is typically port **1812**.

Timeout (seconds)

Set the length of time to wait for a response from the server. Note that if the response is **Response-Accept** or **Response-Challenge**, then RADIUS will wait the entire time specified here before authenticating the account. Therefore, it is encouraged to keep this value as low as reasonably possible given your network settings. An ideal value is 3-5 seconds, with the maximum value at three minutes.

Connection Method

If you are using an external directory store in the same LAN as your BeyondTrust Appliance B Series, the two systems may be able to communicate directly, in which case you can leave the option **Proxy from appliance through the Connection Agent** unchecked and move on.

If the two systems are unable to communicate directly, such as if your external directory server is behind a firewall, you must use a connection agent. Downloading the Win32 connection agent enables your directory server and your B Series Appliance to communicate via an SSL-encrypted, outbound connection, with no firewall configuration. The connection agent can be downloaded to either the directory server or a separate server on the same network as your directory server (recommended).

In the case above, check **Proxy from appliance through the Connection Agent**. Create a **Connection Agent Password** for use in the connection agent installation process. Then click **Download Connection Agent**, run the installer, and follow the installation wizard. During installation, you will be prompted to enter the security provider name and the connection agent password you created above.

Shared Secret

Provide a new shared secret so your B Series Appliance and your RADIUS server can communicate.

Cluster Settings *(Visible Only for Clusters)*

Member Selection Algorithm

Select the method to search the nodes in this cluster.

Top-to-bottom first attempts the server with the highest priority in the cluster. If that server is unavailable or the account is not found, the next highest priority server is attempted. The search moves down through the list of clustered servers until either the account is found or it is determined that the account does not exist on any of the specified and available servers.

Round-robin is designed to balance the load between multiple servers. The algorithm chooses at random which server to attempt first. If that server is unavailable or the account is not found, another random server is attempted. The search continues at random through the remaining servers in the cluster until either the account is found or it is determined that the account does not exist on any of the specified and available servers.

Retry Delay

Set how long to wait after a cluster member becomes unavailable before trying that cluster member again.

Test Settings

Username and Password

Enter a username and password for an account that exists on the server you are testing. This account must match the criteria for login specified in the configuration above.

Try to obtain user attributes and group memberships if the credentials are accepted

If this option is checked, your successful credential test will also attempt to check user attributes and group lookup.



Note: For these features to be successfully tested they must be supported and configured in your security provider.

Test

If your server is properly configured and you have entered a valid test username and password, you will receive a success message. Otherwise, you will see an error message and a log that will help in debugging the problem.



For more information, please see [Create and Configure the RADIUS Security Provider](https://www.beyondtrust.com/docs/remote-support/how-to/integrations/security-providers/radius/configure-settings.htm) at <https://www.beyondtrust.com/docs/remote-support/how-to/integrations/security-providers/radius/configure-settings.htm>.

Add or Edit Security Provider: Kerberos

Name

Create a unique name to help identify this provider.

Enabled

If checked, your BeyondTrust Appliance B Series can search this security provider when a user attempts to log in to the representative console or `/login`. If unchecked, this provider will not be searched.

Keep display name synchronized with remote system

These values determine which fields should be used as the user's private and public display names.

Strip realm from principal names

Select this option to remove the REALM portion from the User Principal Name when constructing the BeyondTrust username.

Authorization Settings

User Handling Mode

Select which users can authenticate to your BeyondTrust Appliance B Series. **Allow all users** allows anyone who currently authenticates via your Key Distribution Center (KDC). **Allow only user principals specified in the list** allows only user principles explicitly designated. **Allow only user principals that match the regex** allows only users principals who match a Perl-compatible regular expression (PCRE).

Default Group Policy

Each user who authenticates against an external server must be a member of at least one group policy in order to authenticate to your B Series Appliance, logging into either the `/login` interface or the representative console. You can select a default group policy to apply to all users allowed to authenticate against the configured server.

SPN Handling Mode

Allow only SPNs specified in the list

If unchecked, all configured service principal names (SPNs) for this security provider are allowed. If checked, select specific SPNs from a list of currently configured SPNs.

LDAP Group Lookup

If you want users on this security provider to be associated with their groups on a separate LDAP server, choose one or more LDAP group servers to use for group lookup.

i For more information, please see [Configure the BeyondTrust Appliance B Series for Kerberos Authentication](https://www.beyondtrust.com/docs/remote-support/how-to/integrations/security-providers/kerberos-configuration/index.htm) at <https://www.beyondtrust.com/docs/remote-support/how-to/integrations/security-providers/kerberos-configuration/index.htm>.

Add or Edit Security Provider: SAML For Representatives

Name

Enter a unique name to help identify your provider.

Enabled

If checked, your BeyondTrust Appliance B Series can search this security provider when a user attempts to log in to the representative console or `/login`. If unchecked, this provider will not be searched.

Associated Email Domains

This setting only applies if you have more than one active SAML provider and is ignored otherwise.

Add any email domains that should be associated with this SAML provider, one per line. When authenticating, users are asked to enter their email. The domain of their email is matched against this list, and they are redirected to the appropriate identity provider for authentication.

If multiple SAML providers are configured and the user's email does not match any of the associated domain on any provider, then they are not allowed to authenticate.

Identity Provider Settings

Metadata

The metadata file contains all the information needed for the initial setup of your SAML provider and must be downloaded from your identity provider. Save the XML file, and then click **Upload Identity Provider Metadata** to select and upload the selected file.

Entity ID

Unique identifier for the identity provider you are using.

Server Certificate

This certificate will be used to verify the signature of the assertion sent from the identity provider.



Note: The fields for **Entity ID**, **Single Sign-On Service URL**, and **Certificate** are automatically populated from the identity provider's metadata file. If you cannot get a metadata file from your provider, this information can be entered manually. For metadata files with multiple identity providers, enter the **Entity ID** of the desired Identity Provider in the field below before uploading the metadata.

Single Sign-On Service URL

When you want to log in to BeyondTrust using SAML, this is the URL where you are automatically redirected so you can log in.

SSO URL Protocol Binding

Determines whether a user posts or is redirected to the sign on URL. This should be left defaulted to redirect unless otherwise required by the identity provider.

Service Provider Settings

Download Service Provider Metadata

Download the BeyondTrust metadata, which must then be uploaded to your identity provider.

Entity ID

This is your BeyondTrust URL. It uniquely identifies the service provider.

Private Key

If necessary, you can decrypt messages sent by the identity provider, if they support and require encryption. Click **Choose File** to upload the private key necessary to decrypt the messages sent from the identity provider.

User Attribute Settings

SAML attributes are used to provision users within BeyondTrust. The default values match BeyondTrust-certified applications with various identity providers. If you are creating your own SAML connector, you may need to modify the attributes to match what is being sent by your identity provider. If your identity provider requires case-insensitivity for the NameID attribute, select **Use case-insensitive comparison for NameIDs**.

Authorization Settings

Lookup Groups Using This Provider

Enabling this feature allows faster provisioning by automatically looking up groups for this user, using **Group Lookup Attribute Name** and **Delimiter**. We recommend enabling this feature. If not used, SAML users must be manually assigned to group policies after their first successful authentication.

Group Lookup Attribute Name

Enter the name of the SAML attribute that contains the names of groups to which users should belong. If the attribute value contains multiple group names, then specify the **Delimiter** used to separate their names.

If left blank, SAML users must be manually assigned to group policies after their first successful authentication.

Group Lookup Delimiter

If the **Delimiter** is left blank, then the attribute value may contain multiple XML nodes with each one containing a different name.

Available Groups

This is an optional list of SAML groups always available to be manually assigned to group policies. If left blank, a given SAML group is made available only after the first successful authentication of a user member of such group. Please enter one group name per line.

Default Group Policy

Each user who authenticates against an external server must be a member of at least one group policy in order to authenticate to your B Series Appliance, logging into either the /login interface or the representative console. You can select a default group policy to apply to all users allowed to authenticate against the configured server.

If a default policy is defined, any allowed user who authenticates against this server might have access at the level of this default policy. Therefore, we recommend you set the default to a policy with minimum privileges to prevent users from gaining permissions you do not wish them to have.



Note: If a user is in a default group policy and is then specifically added to another group policy, the settings for the specific policy always take precedence over the settings for the default, even if the specific policy is a lower priority than the default, and even if the default policy's settings are set to disallow override.



For more information, please see *SAML for Single Sign-On Authentication* at <https://www.beyondtrust.com/docs/remote-support/how-to/integrations/security-providers/saml/index.htm>.

Add or Edit Security Provider: SAML For Public Portals

Name

The name for your SAML provider is auto-generated and cannot be edited at this time.

Enabled

If checked, your BeyondTrust Appliance B Series can search this security provider when a user attempts to log in to the public portal. If unchecked, this provider is not searched.

Identity Provider Settings

Metadata

The metadata file contains all the information needed for the initial setup of your SAML provider and must be downloaded from your identity provider. Save the XML file, and then click **Upload Identity Provider Metadata** to select and upload the selected file.

Entity ID

Unique identifier for the identity provider you are using.

Server Certificate

This certificate will be used to verify the signature of the assertion sent from the identity provider.



Note: The fields for **Entity ID**, **Single Sign-On Service URL**, and **Certificate** are automatically populated from the identity provider's metadata file. If you cannot get a metadata file from your provider, this information can be entered manually. For metadata files with multiple identity providers, enter the **Entity ID** of the desired Identity Provider in the field below before uploading the metadata.

Single Sign-On Service URL

When you want to log in to BeyondTrust using SAML, this is the URL where you are automatically redirected so you can log in.

SSO URL Protocol Binding

Determines whether a user posts or is redirected to the sign on URL. This should be left defaulted to redirect unless otherwise required by the identity provider.

Service Provider Settings

Download Service Provider Metadata

Download the BeyondTrust metadata, which must then be uploaded to your identity provider.

Entity ID

This is your BeyondTrust URL. It uniquely identifies the service provider.

Private Key

If necessary, you can decrypt messages sent by the identity provider, if they support and require encryption. Click **Choose File** to upload the private key necessary to decrypt the messages sent from the identity provider.

User Attribute Settings

SAML attributes are used to provision users within BeyondTrust. The default values match BeyondTrust-certified applications with various identity providers. If you are creating your own SAML connector, you may need to modify the attributes to match what is being sent by your identity provider. The SAML attributes can also be associated with customer sessions by adding custom fields with matching code names on the **Custom Fields** page in **/login**.



For more information, please see [SAML for Single Sign-On Authentication](https://www.beyondtrust.com/docs/remote-support/how-to/integrations/security-providers/saml/index.htm) at <https://www.beyondtrust.com/docs/remote-support/how-to/integrations/security-providers/saml/index.htm>.

Session Policies: Set Session Permission and Prompting Rules



Users & Security

SESSION POLICIES

Session Policies

With session policies, you can customize session security permissions to fit specific scenarios. Session policies can be applied to users, public sites, and all Jump Items.

i For more information, please see [How to Use Support Session Policies](https://www.beyondtrust.com/docs/remote-support/how-to/session-policies/) at www.beyondtrust.com/docs/remote-support/how-to/session-policies/.

The **Session Policies** section lists available policies. Click the arrow by a policy name to quickly see where that policy is being used; its availability for users, rep invites, and Jump Clients; the support tools configured; and the prompting configured.

Add, Edit, Delete

Create a new policy, modify an existing policy, or remove an existing policy.

Copy

To expedite the creation of similar policies, click **Copy** to create a new policy with identical settings. You can then edit this new policy to meet your specific requirements.

Add or Edit Session Policy

After making your edits, click **Save** to make this policy available.

Display Name

Create a unique name to help identify this policy. This name helps when assigning a session policy to users, public portals, and Jump Clients.

Code Name

Set a code name for integration purposes. If you do not set a code name, one is created automatically.

Description

Add a brief description to summarize the purpose of this policy. The description is seen when applying a policy to user accounts, group policies, and rep invites.

Availability

Users

Choose if this policy should be available to assign to users (user accounts and group policies).

Rep Invite

Choose if this policy should be available for users to select when inviting an external user to join a session.

Jump Items

Choose if this policy should be available to assign to Jump Items.

Dependencies

If this session policy is already in use, you will see the number of users, public portals, and Jump Clients using this policy.

Permissions

For all of the permissions that follow, you can choose to enable or disable the permission, or you can choose to set it to **Not Defined**. Session policies are applied to a session in a hierarchical manner, with Jump Clients taking the highest priority, then support portals, then users, and then the global default. If multiple policies apply to a session, then the policy with the highest priority will take precedence over the others. If, for example, the policy applied to a Jump Client defines a permission, then no other policies may change that permission for the session. To make a permission available for a lower policy to define, leave that permission set to **Not Defined**.



For details and examples, see [How to Use Support Session Policies](https://www.beyondtrust.com/docs/remote-support/how-to/session-policies/) at www.beyondtrust.com/docs/remote-support/how-to/session-policies/.

Set which tools should be enabled or disabled with this policy, as well as which tools should prompt the customer for permission.

Support Tool Prompting



For more information, please see [Customer Client: Support Session Interface](https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-support-interface.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-support-interface.htm>.

Prompting Rules

Choose to ask the customer permission to use any of the support features below. Select **No Prompting** to never prompt, **Always Prompt** to always prompt, or **Prompt for Some Tools** to choose which permissions to prompt for. If **Prompt for Some Tools** is chosen, a **Prompt Customer** option will appear beside each tool with the options to **Never** prompt or to **Always** prompt. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

Allowed to prompt once

If **Screen Sharing** is set to **View and Control** and prompting is enabled, this option appears. Check the box to make the screen sharing prompt request access to all tools during the session, with no further prompts.

Prompting Options

Set how long to wait for a response to a prompt before defaulting to the answer of **Deny** or **Allow**. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

Screen Sharing

Screen Sharing Rules

Enable the user to view or control the remote screen. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.



For more information, please see [Screen Share with the Remote Customer for View and Control](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/screen-sharing.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/screen-sharing.htm>.

Allowed to show their screen to the customer

Enables the user to share their screen with the customer during a support session. This option is available if **View Only** or **View or Control** is selected.



For more information, please see [Show My Screen: Reverse Screen Share](https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/show-my-screen.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/show-my-screen.htm>.

Allowed Customer Restrictions

Set if the user can suspend the remote system's mouse and keyboard input. The user may also prevent the remote desktop from being displayed. This option is available if **View and Control** is selected. If **Display, Mouse and Keyboard** is the selected Customer Restriction, a check box is available to **Automatically request a privacy screen on session start**. Privacy screen is applicable only for sessions started from a Jump Client, a Remote Jump item, or a Local Jump item. We recommend using privacy screen for unattended sessions. The remote system must support privacy screen.



For more information, please see [Restricted Customer Interaction: Privacy Screen, Disable Remote Input](https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/privacy-screen.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/privacy-screen.htm>.

Application Sharing Prompt Behavior

Set if a request for screen sharing should always or never prompt the customer to select applications to share, or if the user can choose whether to prompt for application sharing or not. Selecting **Always** or **Rep Decides** also allows you to predefine application sharing

restrictions.



For more information, please see [Application Sharing: Limit What the Representative Can See at https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/application-sharing.htm](https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/application-sharing.htm).

Clipboard Synchronization Direction

This option is available if **View and Control** is selected. Select how clipboard content flows between representatives and end users. The options are:

- **Not allowed:** The representative is not allowed to use the clipboard, no clipboard icons display in the representative console, and cut and paste commands do not work.
- **Allowed from Rep to Customer:** The representative can push clipboard content to the customer but cannot paste from the end user's clipboard. Only the Send clipboard icon displays in the representative console.
- **Allowed in Both Directions:** Clipboard content can flow both ways. Both Push and Get clipboard icons display in the representative console.



For more information about the Clipboard Synchronization Mode, please see ["Security: Manage Security Settings" on page 237](#).

Annotations

Annotation Rules

Enables the user to use annotation tools to draw on the remote system's screen. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.



For more information, please see [Use Annotations to Draw on the Remote Screen at https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/annotations.htm](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/annotations.htm).

File Transfer

File Transfer Rules

Enables the user to upload files to the remote system, download files from the remote system, or both. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

Accessible paths on customer's filesystem

Allow the user to transfer files to or from any directories on the remote system or only specified directories.

Accessible paths on representative's filesystem

Allow the user to transfer files to or from any directories on their local system or only specified directories.

 For more information, please see [File Transfer to and from the Remote System](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/file-transfer.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/file-transfer.htm>.

Command Shell

Command Shell Rules

Enables the user to issue commands on the remote computer through a virtual command line interface. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.



Note: Command shell access cannot be restricted for Shell Jump sessions.

 For more information, please see [Access the Remote Command Shell](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/command-shell.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/command-shell.htm>.


System Information

System Information Rules

Enables the user to see system information about the remote computer. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

Allowed to use system information actions

Enables the user to interact with processes and programs on the remote system without requiring screen sharing. Kill processes; start, stop, pause, resume, and restart services; and uninstall programs.

 For more information, please see [View Remote System Information](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/system-info.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/system-info.htm>.

Registry Access

Registry Access Rules

Enables the user to interact with the registry on a remote Windows system without requiring screen sharing. View, add, delete and edit keys, search and import/export keys.

i For more information, please see [Access the Remote Registry Editor](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/registry-editor.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/registry-editor.htm>.

Canned Scripts

Canned Script Rules

Enables the user to run canned scripts that have been created for their teams. Note that when the user is in view-only screen sharing, the customer receives a prompt to allow the script to run. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

i For more information, please see [Access the Remote Command Shell](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/command-shell.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/command-shell.htm>.

Elevation

Elevation Rules

Enables the user to attempt to elevate the customer client to run with administrative rights on the remote system. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

i For more information, please see [Elevate the Client](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/elevation.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/elevation.htm>.

Support Button Deployment

Support Button Deployment Rules

Enables the user to deploy or remove a Support Button while in a session. Locations available for deployment depend on the Support Button settings above. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

i For more information, please see [Support Session Overview and Tools](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm>.

Jump Clients Pinning/Unpinning

Jump Clients Pinning/Unpinning Rules

Enables the user to pin or unpin a Jump Client while in a session. Locations available for deployment depend on the Jump Client settings above. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.



For more information, please see [Support Session Overview and Tools](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm>.

Chat



For more information, please see [Chat with the Customer During a Session](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/chat.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/chat.htm>.

Chat Rules

Enables the user to chat with the remote customer. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

Allowed to push URLs to the customer's web browser

Enables the user to enter a URL into the chat area and then click the **Push URL** button to automatically open a web browser to that address on the remote computer.

Allowed to send files using the chat interface

Enables the user to send files via the chat interface.



For more information, please see [Customer Client: Support Session Interface](https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-support-interface.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-support-interface.htm>.

Session Termination Behavior

If unable to reconnect within the time you set by **Reconnect Timeout**, choose what action to take. To prevent an end-user from accessing unauthorized privileges after an elevated session, set the client to automatically log the end user out of the remote Windows computer at session end, to lock the remote computer, or to do nothing. These rules do not apply to browser sharing sessions.

Allow users to override this setting per session

You can allow a user to override the session termination setting from the **Summary** tab in the console during a session.

Export Policy

You can export a session policy from one site and import those permissions into a policy on another site. Edit the policy you wish to export and scroll to the bottom of the page. Click **Export Policy** and save the file.

Import Policy

You may import those policy settings to any other BeyondTrust site that supports session policy import. Create a new session policy and scroll to the bottom of the page. Browse to the policy file and then click **Import Policy**. Once the policy file is uploaded, the page will refresh, allowing you to make modifications. Click **Save Policy** to make the policy available.

Session Policy Simulator

The **Session Policy Simulator** allows you to determine what the outcome of complex policy layering will be. The simulator can also be used to troubleshoot permission errors, such as a permission being unexpectedly unavailable.

Representative

Start by selecting the user performing the session. This dropdown includes user accounts and rep invite policies.

Session Start Method

Select the session start method to use for this simulation.

Public Portal

If you selected **Public Portal**, choose the public portal to use for this simulation of a customer-initiated session.

Support Button

If you selected **Support Button**, search for a deployed Support Button by profile, associated public portal, associated queue, computer name, or description. The associated public portal will be automatically selected above.

Jumpoint or Local Jump

Because local Jumps and Jumpoints are always associated with the default public portal, there are no further settings to define.

Jump Client, Local Jump Shortcut, Remote Jump Shortcut, Local VNC Jump Shortcut, Remote VNC Jump Shortcut, Remote RDP Jump Shortcut, Local RDP Jump Shortcut, Shell Jump Shortcut, Intel® vPro Shortcut

Search for a pinned Jump Client or Jump Shortcut by name, comments, Jump Group, tag, or associated public portal. The associated public portal will be automatically selected above.

Customer Present

If you selected **Jump Client**, you can choose whether the customer should appear as present or not.

Simulate

Click **Simulate**. In the area below, the permissions configurable by session policy are displayed in read-only mode. You can see which permissions are allowed or denied as a result of the stacked policies, as well as which policy set each permission.

Group Policies: Apply User Permissions to Groups of Users



Users & Security

GROUP POLICIES

Group Policies

The **Group Policies** page enables you to set up groups of users who will share common privileges.

Add New Policy, Edit, Delete

Create a new policy, modify an existing policy, or remove an existing policy.



Note: If you edit the group policy that is the default for the local provider, or has local administrator users, and remove administrator permissions, a warning message appears. Ensure other users have administrator permissions before proceeding.

Change Order

Click the **Change Order** button to drag and drop group policies to set their priority. Click **Save Order** for prioritization changes to take effect. When multiple policies apply to a given user, the permissions take effect by starting at the top of the **Group Policies** list, and then moving down the list. If a permission conflicts with a permission applied by a group policy higher in the list, then the lower permission will overwrite the higher, unless the higher was set as **Final**. In short, group policies that appear lower in the list have a higher functional priority than those that are higher.

Search Group Policies

To quickly find an existing policy in the list of **Group Policies**, enter the name, or part of the name. The list filters to all policies with a name containing the entered search term. The list remains filtered until the search term is removed, even if the user goes to other pages or logs out. To remove the search term, click the **X** to the right of the search box.

If you click the **Change Order** button after searching the list, all group policies appear. You can drag and drop group policies to set their priority. When you click **Save Order**, the changes take effect and the list returns to policies with a name containing the entered search term.

Expand All / Collapse All

To assist with searching and navigating the group policies, click the **Expand All** link above the grid to expand the details of all listed group policies. Click **Collapse All** to return to the unexpanded list of group policies.

Copy

To expedite the creation of similar policies, click **Copy** to create a new policy with identical settings. You can then edit this new policy to meet your specific requirements.

Add or Edit Policy

After making your edits, click **Save** to save your changes to this group policy.

Policy Name

Create a unique name to help identify this policy.

Available Members and Policy Members

To assign members, select a member from the **Available Members** list and click **Add** to move it to the **Policy Members** box. Use the **Search** box to find existing members.

You can select users from your local system, or select users or entire groups from configured security providers. To add users or groups from an external directory store such as LDAP, RADIUS, or Kerberos, you must first configure the connection on the **/login > Users & Security > Security Providers** page. If an attempt to add a user from a configured security provider is invalid, the synchronization log error message appears here as well as in the log.

Account Settings

Which account settings should this Group Policy control?

Decide if a setting should be **Defined** within this policy. If it is, you can select **Final** to prevent other policies of a lower priority from overriding the permission value set by this policy. Select **All** to define all settings in this section.

Two Factor Authentication: Log in with an Authenticator app

Select whether the user is required to log in using an authenticator app, or has the option to do so (default setting). If **Required** is selected, the next time the user tries to login to either the administrative interface or the representative console, a screen displays requiring the activation of two-factor authentication.



For more information on 2FA, please see [How to Use Two Factor Authentication with BeyondTrust Remote Support at www.beyondtrust.com/docs/remote-support/how-to/2-factor-authentication/](https://www.beyondtrust.com/docs/remote-support/how-to/2-factor-authentication/).

Account Expiration: Account Never Expires

If this option is selected, the account never expires.

Account Expiration: Account Expiration Date

Causes the account to expire on a given date.

Account Enablement: Account Disabled

Disables the account so the user cannot log in. Disabling does NOT delete the account.

Display Name Editing: Allowed to Change Their Display Names

Enables users to change their display names.

Photo Editing: Allowed to Change Their Photo

Enables users to change their avatar photos, which display on the `/login` administrative interface and in the customer client chat window.

Showing on Public Site: Allowed to Show on Public Site

Displays the user's name on all public sites that have the representative list enabled.

Comments

Add comments to help identify the purpose of this account.

General Permissions

Which general settings should this Group Policy control?

Decide if a setting should be **Defined** within this policy. If it is, you can select **Final** to prevent other policies of a lower priority from overriding the permission value set by this policy. Select **All** to define all settings in this section.

Administration

Administrative Privileges: Administrator

Grants the user full administrative rights.

Vault Administrative Privileges: Allowed to Administer Vault

Enables the user to manage all aspects of the BeyondTrust Vault add-on.

Password Setting: Allowed to Set Passwords

Enables the user to set passwords and unlock accounts for non-administrative local users.

Jumpoint Editing: Allowed to Edit Jumpoints

Enables the user to create or edit Jumpoints. This option does not affect the user's ability to access remote computers via Jumpoint, which is configured per Jumpoint or group policy.

Public Site Editing: Allowed to Edit Public Site

Enables the user to create and modify public site configurations, edit HTML templates, view the translation interface, etc.

Customer Notice Editing: Allowed to Edit Customer Notices

Enables the user to create and edit messages used to notify customers, as they are requesting support, of broadly impacting IT outages.

File Store Editing: Allowed to Edit File Store

Enables the user to add or remove files from the file store.

Canned Message Editing: Allowed to Edit Canned Messages

Enables the user to create or edit canned chat messages.

Support Team Editing: Allowed to Edit Support Teams

Enables the user to create or edit support teams.

Jump Group Editing: Allowed to Edit Jump Groups

Enables the user to create or edit Jump Groups.

Issue Editing: Allowed to Edit Issues

Enables the user to create and edit issues.

Skill Editing: Allowed to Edit Skills

Enables the user to create and edit skills.

Support Button Profile Editing: Allowed to Edit Support Button Profiles

Enables the user to customize Support Button profiles.

Canned Script Editing: Allowed to Edit Canned Scripts

Enables the user to create or edit canned scripts for use in screen sharing or command shell sessions.

Custom Rep Link Editing: Allowed to Edit Custom Rep Links

Enables the user to create or edit custom links.

Access Sponsor Editing: Allowed to Edit Access Sponsors

Enables the user to create or edit access sponsor teams.

iOS Profile Editing: Allowed to Edit iOS Profiles

Enables the user to create, edit and upload Apple iOS Profile content for distribution to iOS device users.

Reporting

Session and Team Report Access: Allowed to View Support Session Reports

Enables the user to run reports on support session activity, viewing only sessions in which they were the primary representative, only sessions in which one of their teams was the primary team or one of their teammates was the primary representative, or all sessions.

Session and Team Report Access: Allowed to view support session recordings

Enables the user to view video recordings of screen sharing sessions, Show My Screen sessions, and command shell sessions.

License Usage Report Access: Allowed to View License Usage Reports

Enables the user to run reports on BeyondTrust license usage.

Vault Report Access: Allowed to View Vault Reports

Enables the user to run reports on Vault activity, viewing all event data or only their event data.

Presentation Report Access: Allowed to View Presentation Session Reports

Enables the user to run reports on presentation activity, viewing only presentations in which they were the presenter, only sessions in which one of their teammates was the presenter, or all presentations.

Allowed to View Support Session Recordings

Enables the user to view recordings of screen sharing sessions and command shell sessions. It does not affect presentation recordings.

Allowed to View License Usage Reports

Enables the user to view Representative License Report.

Syslog Report Access: Allowed to View Syslog Reports

Enables the user to download a ZIP file containing all syslog files available on the appliance. Admins automatically have permissions to access this report. Non-admin users must request access to view this report.

Representative Permissions

Allowed to provide remote support

Enables the user to use the representative console in order to run support sessions. If support is enabled, options pertaining to remote support will also be available. Disable this setting for presentation-only users.

Session Management

Allowed to generate session keys for support sessions within the representative console

Enables the user to generate session keys to allow customers to start sessions with them directly.

i For more information, please see [Generate a Session Key to Start a Support Session at https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/session-keys.htm](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/session-keys.htm).

Allowed to generate access keys for sending iOS profiles

Enables the user to generate access keys to offer iOS content to iOS device users.

i For more information, please see [Generate an Apple iOS Profile Access Key at https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/apple-ios-access-key-management-interface.htm](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/apple-ios-access-key-management-interface.htm).

Allowed to manually accept sessions from a team queue

Enables the user to select and start sessions that are in one of their team queues.

i For more information, please see [Accept a Session to Start Support at https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/accepting-a-session.htm](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/accepting-a-session.htm).

Allowed to transfer sessions to teams which they do not belong to

Enables the user to transfer sessions to teams other than their own. If disabled, user interaction is restricted solely to the user's assigned teams.

i For more information, please see [Support Session Overview and Tools at https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm).

Allowed to share sessions with teams which they do not belong to

Enables the user to invite a less limited set of user to share sessions, not only their team members. Combined with the extended availability permission, this permission expands session sharing capabilities.

i For more information, please see [Support Session Overview and Tools](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm>.

Allowed to invite external support representatives

Enables the user to invite a third-party user to participate in a support session one time only.

i For more information, please see [Invite an External Representative to Join a Session](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/rep-invite.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/rep-invite.htm>.

Allowed to use the Get Next Session feature

Enables the user to start supporting the oldest queued session from all of their teams simply by clicking a button.

i For more information, please see [Accept a Session to Start Support](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/accepting-a-session.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/accepting-a-session.htm>.

Allowed to enable extended availability mode

Enables the user to receive email invitations from other users requesting to share a session even when they are not logged into the representative console.

i For more information, please see [Use Extended Availability to Stay Accessible When Not Logged In](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/extended-availability.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/extended-availability.htm>.

Allowed to edit the external key

Enables the user to modify the external key from the session info pane of a session within the representative console.

i For more information, please see [Support Session Overview and Tools](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm>.

Equilibrium



For more information, please see *Equilibrium for Automatic Session Routing guide* at <https://www.beyondtrust.com/docs/remote-support/how-to/equilibrium/index.htm>.

Allowed to opt out of session assignments

Enables the representative to mark himself or herself as unavailable for sessions to be assigned using Equilibrium.

Do not assign sessions if the representative is participating in at least

Sets the least number of sessions the representative must be supporting before sessions will no longer be automatically assigned using Equilibrium.

Do not assign sessions if the representative has been idle for at least

Sets the least amount of time the representative must have been idle before sessions will no longer be automatically assigned using Equilibrium.

Rep to Rep Screen Sharing



For more information, please see *Share your Screen with Another Representative* at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/representative-screensharing.htm>.

Allowed to show screen to other representatives

Enables the user to share their screen with another user without the receiving user having to join a session. This option is available even if the user is not in a session.

Allowed to give control when showing screen to other representatives

Enables the user sharing their screen to give keyboard and mouse control to the user viewing their screen.

Support Buttons



For more information, please see *Support Session Overview and Tools* at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm>.

Allowed to deploy and manage Support Buttons in personal queue

Enables the user to deploy and manage personal Support Buttons. This setting affects deploying Support Buttons from both the web interface and the representative console. To deploy a Support Button from within a session, the **Support Button Deployment** session permission must also be allowed.

Allowed to manage Team Support Buttons

Enable the user to modify the Support Buttons deployed to teams they are a member of. If the user is a team lead or manager, they can modify the personal Support Buttons of any team members as well.



For more information, please see *Manage Support Buttons* at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-button-management-interface.htm>.

Allowed to change the Public Portal associated with Support Buttons

Enables the user to set the public portal through which a Support Button should connect. Because session policies may be applied to public portals, changing the portal may affect the permissions allowed in the session.

Allowed to deploy Team Support Buttons

Enables the user to deploy team Support Buttons for teams they are a member of. This setting affects deploying Support Buttons from both the web interface and the representative console. To deploy a Support Button from within a session, the **Support Buttons Deployment** session permission must also be allowed.

Jump Technology

Allowed Jump Methods

Enables the user to Jump to computers using **Jump Clients**, **Local Jump**, **Local VNC**, **Local RDP**, **Remote Jump**, **Remote VNC**, **Remote RDP**, **Shell Jump**, and/or **Intel vPro**.

Jump Item Roles

A Jump Item Role is a predefined set of permissions regarding Jump Item management and usage. For each option, click the **Edit** button to open the Jump Item Role in a new tab.

The **Default** role is used only when **Use User's Default** is set for that user in a Jump Group.

The **Personal** role applies only to Jump Items pinned to the user's personal list of Jump Items.

The **Teams** role applies to Jump Items pinned to the personal list of Jump Items of a team member of a lower role. For example, a team manager can view team leads' and team members' personal Jump Items, and a team lead can view team members' personal Jump Items.

The **System** role applies to all other Jump Items in the system. For most users, this should be set to **No Access**. If set to any other option, the user is added to Jump Groups to which they would not normally be assigned, and in the representative console, they can see non-team members' personal lists of Jump Items.

i For more information, please see [Use Jump Item Roles to Create Permission Sets for Jump Clients at https://www.beyondtrust.com/docs/remote-support/how-to/jump-clients/jump-item-roles.htm](https://www.beyondtrust.com/docs/remote-support/how-to/jump-clients/jump-item-roles.htm).

Presentation

Allowed to give presentations

Enables the representative to give presentations to one or more attendees.

i For more information, please see [Give a Presentation to Remote Attendees at https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/presentation.htm](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/presentation.htm).

Allowed to grant control to a presentation attendee

Enables the representative to grant control of their computer to an attendee during a presentation. This setting affects only presentations and does not impact the Show My Screen feature of a support session. Only one attendee at a time can have control. The representative always maintains overriding control.

i For more information, please see [Presentation Attendee Client: Join a Presentation at https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-presentation-interface.htm](https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-presentation-interface.htm).

Representative Console

Idle Timeout

Set how long the representative can be idle before being logged out of the representative console. This permission can use the site-wide setting or can override that setting.

Attended and Unattended Session Permissions

Attended and Unattended Session Policies

Session Policy

Set the prompting and permission rules that should apply to this user's sessions. Choose an existing session policy or define custom permissions for this user. If **Not Defined**, the global default policy will be used. These permissions may be overridden by a higher policy.

Use the same permissions for Unattended sessions

To use the same permissions for both attended and unattended sessions, check **Use the same permissions for Unattended sessions**. Uncheck this box to define attended and unattended permissions separately. You can also copy the permissions from one to the other.

Description

View the description of a pre-defined session permission policy.

Support Tool Prompting

i For more information, please see *Customer Client: Support Session Interface* at <https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-support-interface.htm>.

Prompting Rules

Choose to ask the customer permission to use any of the support features below. Select **No Prompting** to never prompt, **Always Prompt** to always prompt, or **Prompt for Some Tools** to choose which permissions to prompt for. If **Prompt for Some Tools** is chosen, a **Prompt Customer** option will appear beside each tool with the options to **Never** prompt or to **Always** prompt. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

Allowed to prompt once

If **Screen Sharing** is set to **View and Control** and prompting is enabled, this option appears. Check the box to make the screen sharing prompt request access to all tools during the session, with no further prompts.

Prompting Options

Set how long to wait for a response to a prompt before defaulting to the answer of **Deny** or **Allow**. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

Screen Sharing

Screen Sharing Rules

Enable the user to view or control the remote screen. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

i For more information, please see *Screen Share with the Remote Customer for View and Control* at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/screen-sharing.htm>.

Allowed to show their screen to the customer

Enables the user to share their screen with the customer during a support session. This option is available if **View Only** or **View or Control** is selected.

i For more information, please see [Show My Screen: Reverse Screen Share](https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/show-my-screen.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/show-my-screen.htm>.

Allowed Customer Restrictions

Set if the user can suspend the remote system's mouse and keyboard input. The user may also prevent the remote desktop from being displayed. This option is available if **View and Control** is selected. If **Display, Mouse and Keyboard** is the selected Customer Restriction, a check box is available to **Automatically request a privacy screen on session start**. Privacy screen is applicable only for sessions started from a Jump Client, a Remote Jump item, or a Local Jump item. We recommend using privacy screen for unattended sessions. The remote system must support privacy screen.

i For more information, please see [Restricted Customer Interaction: Privacy Screen, Disable Remote Input](https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/privacy-screen.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/privacy-screen.htm>.

Application Sharing Prompt Behavior

Set if a request for screen sharing should always or never prompt the customer to select applications to share, or if the user can choose whether to prompt for application sharing or not. Selecting **Always** or **Rep Decides** also allows you to predefine application sharing restrictions.

i For more information, please see [Application Sharing: Limit What the Representative Can See](https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/application-sharing.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/application-sharing.htm>.

Clipboard Synchronization Direction

This option is available if **View and Control** is selected. Select how clipboard content flows between representatives and end users. The options are:


- **Not allowed:** The representative is not allowed to use the clipboard, no clipboard icons display in the representative console, and cut and paste commands do not work.
- **Allowed from Rep to Customer:** The representative can push clipboard content to the customer but cannot paste from the end user's clipboard. Only the Send clipboard icon displays in the representative console.
- **Allowed in Both Directions:** Clipboard content can flow both ways. Both Push and Get clipboard icons display in the representative console.

i For more information about the Clipboard Synchronization Mode, please see ["Security: Manage Security Settings" on page 237](#).

Annotations

Annotation Rules

Enables the user to use annotation tools to draw on the remote system's screen. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

 More more information, please see [Use Annotations to Draw on the Remote Screen at https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/annotations.htm](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/annotations.htm).

File Transfer

File Transfer Rules

Enables the user to upload files to the remote system, download files from the remote system, or both. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

Accessible paths on customer's filesystem

Allow the user to transfer files to or from any directories on the remote system or only specified directories.

Accessible paths on representative's filesystem

Allow the user to transfer files to or from any directories on their local system or only specified directories.

 For more information, please see [File Transfer to and from the Remote System at https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/file-transfer.htm](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/file-transfer.htm).

Command Shell

Command Shell Rules

Enables the user to issue commands on the remote computer through a virtual command line interface. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.



Note: Command shell access cannot be restricted for Shell Jump sessions.

 For more information, please see [Access the Remote Command Shell at https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/command-shell.htm](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/command-shell.htm).

System Information

System Information Rules

Enables the user to see system information about the remote computer. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

Allowed to use system information actions

Enables the user to interact with processes and programs on the remote system without requiring screen sharing. Kill processes; start, stop, pause, resume, and restart services; and uninstall programs.



For more information, please see [View Remote System Information](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/system-info.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/system-info.htm>.

Registry Access

Registry Access Rules

Enables the user to interact with the registry on a remote Windows system without requiring screen sharing. View, add, delete and edit keys, search and import/export keys.



For more information, please see [Access the Remote Registry Editor](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/registry-editor.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/registry-editor.htm>.

Canned Scripts

Canned Script Rules

Enables the user to run canned scripts that have been created for their teams. Note that when the user is in view-only screen sharing, the customer receives a prompt to allow the script to run. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.



For more information, please see [Access the Remote Command Shell](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/command-shell.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/command-shell.htm>.

Elevation

Elevation Rules

Enables the user to attempt to elevate the customer client to run with administrative rights on the remote system. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

i For more information, please see [Elevate the Client](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/elevation.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/elevation.htm>.

Support Button Deployment

Support Button Deployment Rules

Enables the user to deploy or remove a Support Button while in a session. Locations available for deployment depend on the Support Button settings above. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

i For more information, please see [Support Session Overview and Tools](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm>.

Jump Clients Pinning/Unpinning

Jump Clients Pinning/Unpinning Rules

Enables the user to pin or unpin a Jump Client while in a session. Locations available for deployment depend on the Jump Client settings above. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

i For more information, please see [Support Session Overview and Tools](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm>.

Chat

i For more information, please see [Chat with the Customer During a Session](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/chat.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/chat.htm>.

Chat Rules

Enables the user to chat with the remote customer. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

Allowed to push URLs to the customer's web browser

Enables the user to enter a URL into the chat area and then click the **Push URL** button to automatically open a web browser to that address on the remote computer.

Allowed to send files using the chat interface

Enables the user to send files via the chat interface.

 For more information, please see *Customer Client: Support Session Interface* at <https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-support-interface.htm>.

Session Termination Behavior

If unable to reconnect within the time you set by **Reconnect Timeout**, choose what action to take. To prevent an end-user from accessing unauthorized privileges after an elevated session, set the client to automatically log the end user out of the remote Windows computer at session end, to lock the remote computer, or to do nothing. These rules do not apply to browser sharing sessions.

Allow users to override this setting per session

You can allow a user to override the session termination setting from the **Summary** tab in the console during a session.

Availability Settings

Which availability settings should this Group Policy control?

Decide if a setting should be **Defined** within this policy. If it is, you can select **Final** to prevent other policies of a lower priority from overriding the permission value set by this policy. Select **All** to define all settings in this section.

Full Support License Pool

Choose the license pool to which this representative should belong. When this representative logs into the representative console, a license is consumed from the designated license pool. If **None** is selected, the representative will be able to log in to the representative console only if one or more licenses are left unassigned to license pools and are available.

Login Schedule

Restrict representative log in to the following schedule

Set a schedule to define when users can log in to the representative console. Set the time zone you want to use for this schedule, and then add one or more schedule entries. For each entry, set the start day and time and the end day and time.

If, for instance, the time is set to start at 8 am and end at 5 pm, a user can log in at any time during this window but may continue to work past the set end time. They will not, however, be allowed to log back in after 5 pm.

Force logout when the schedule does not permit login

If stricter access control is required, check this option. This forces the user to log out at the scheduled end time. In this case, the user receives recurring notifications beginning 15 minutes prior to being disconnected. When the user is logged out, any owned sessions will follow the session fallback rules.

Memberships

Which membership settings should this Group Policy control?

Decide if a setting should be **Defined** within this policy. If it is, you can select **Final** to prevent other policies of a lower priority from overriding the permission value set by this policy. Select **All** to define all settings in this section.

Add Support Teams Membership

Search for teams to which members of this group policy should belong. You can set the role as **Team Member**, **Team Lead**, or **Team Manager**. These roles play a significant part in the **Dashboard** feature of the representative console. Click **Add**.

Added teams are shown in a table. You can edit the role of members in a team or delete the team from the list.

Remove Support Teams Membership

Search for teams from which members of this group policy should be removed, and then click **Add**. Removed teams are shown in a table. You can delete a team from the list.

Add Jumpoint Membership


Search for Jumpoints which members of this group policy should be allowed to access, and then click **Add**. Added Jumpoints are shown in a table. You can delete a Jumpoint from the list.

Remove Jumpoint Memberships

Search for Jumpoints from which members of this group policy should not be removed, and then click **Add**. Removed Jumpoints are shown in a table. You can delete a Jumpoint from the list.

Add Jump Group Memberships

Search for Jump Groups to which members of this group policy should belong. You can set each user's [Jump Item Role](#) to set their permissions specific to Jump Items in this Jump Group, or you can use the user's default Jump Item Roles set in this group policy or on the **Users & Security > Users** page. A Jump Item Role is a predefined set of permissions regarding Jump Item management and usage.

 For more information see [Jump Item Roles: Configure Permission Sets for Jump Items at www.beyondtrust.com/docs/remote-support/getting-started/admin/jump-item-roles.htm](https://www.beyondtrust.com/docs/remote-support/getting-started/admin/jump-item-roles.htm).

You can also apply a [Jump Policy](#) to manage user access to the Jump Items in this Jump Group.

Added Jump Groups are shown in a table. You can edit a Jump Group's settings or delete the Jump Group from the list.

Remove Jump Group Memberships

Search for Jump Groups from which members of this group policy should be removed, and then click **Add**. Removed Jump Groups are shown in a table. You can delete a Jump Group from the list.

Add Vault Account Memberships

Search for an account, select the **Vault Account Role**, and then click **Add** to grant members of the policy access to the selected Vault account. Users may have memberships added by other group policies. View **Vault > Accounts** to see all members within each group. Users may be assigned one of two roles for using the Vault account:

- **Inject** (default value): Users with this role can use this account in Remote Support sessions.
- **Inject and Checkout**: Users with this role can use this account in Remote Support sessions and can check out the account on `/login`. The **Checkout** permission has no affect on generic SSH accounts.



Note: Enable the **Add Vault Account Membership** permission to assign a **Vault Account Role** to a Vault account in a group policy. The **Vault Account Role** is visible in the list of accounts added to the group policy.

Add Vault Account Group Memberships

Search for an account group, select the **Vault Account Role**, and then click **Add** to grant members of the policy access to the group of Vault accounts. Users may have memberships added by other group policies. View **Vault > Accounts** to see all members within each group. Users may be assigned one of two roles for using the group of Vault accounts:

- **Inject** (default value): Users with this role can use this account in Remote Support sessions.
- **Inject and Checkout**: Users with this role can use this account in Remote Support sessions and can check out the account on `/login`. The **Checkout** permission has no affect on generic SSH accounts.



Note: Enable the **Add Vault Account Group** permission to assign a **Vault Account Role** to a group of Vault accounts in a group policy. The **Vault Account Role** is visible in the list of account groups added to the group policy.

Export Policy

You can export a group policy from one site and import those permissions into a policy on another site. Edit the policy you wish to export and scroll to the bottom of the page. Click **Export Policy** and save the file.



Note: When exporting a group policy, only the policy name, account settings, and permissions are exported. Policy members, team memberships, and Jumpoint memberships are not included in the export.

Import Policy

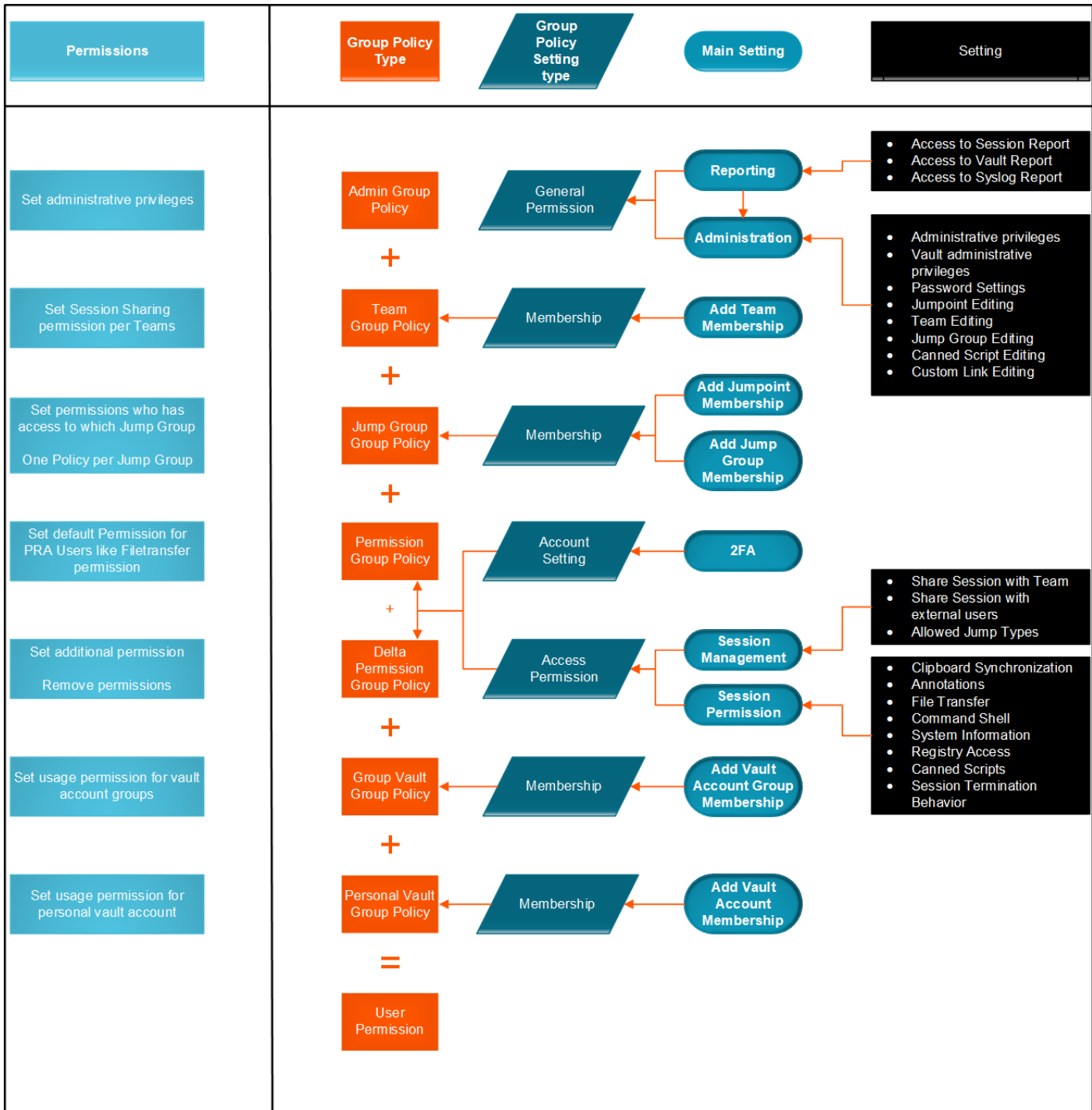
You may import exported group policy settings to any other BeyondTrust site that supports group policy import. Create a new group policy or edit an existing policy whose permissions you wish to overwrite, and scroll to the bottom of the page. Browse to the policy file and then click **Select Policy File**. Once the policy file is uploaded, the page will refresh, allowing you to make modifications. Click **Save** to put the group policy into effect.



Note: *Importing a policy file to an existing group policy will overwrite any previously defined permissions, with the exception of policy members, team memberships, and Jumpoint memberships.*

Sample Policy Matrix

The diagram below is an example of how multiple policies can work together.



Kerberos Keytab: Manage the Kerberos Keytab



Users & Security

KERBEROS KEYTAB

Kerberos Keytab Management

BeyondTrust supports single sign-on functionality using the Kerberos authentication protocol. This enables users to authenticate to the B Series Appliance without having to enter their credentials. Kerberos authentication applies both to the /login web interface and to the representative console.

To integrate Kerberos with your B Series Appliance, you must have a Kerberos implementation either currently deployed or in the process of being deployed. Specific requirements are as follows:

- You must have a working Key Distribution Center (KDC) in place.
- Clocks must be synchronized across all clients, the KDC, and the B Series Appliance. Using a Network Time Protocol server (NTP) is an easy way to ensure this.
- You must have a Service Principal Name (SPN) created on the KDC for your B Series Appliance.

Configured Principles

The **Configured Principals** section lists all of the available SPNs for each uploaded keytab.

Once you have available SPNs, you can configure a Kerberos security provider from the **Security Providers** page and define which user principals may authenticate to the B Series Appliance via Kerberos.

Import Keytab

Choose File

Export the keytab for the SPN from your KDC and upload it to the B Series Appliance.



For more information, please see *Kerberos Server for Single Sign-On* at <https://www.beyondtrust.com/docs/remote-support/how-to/integrations/security-providers/kerberos/index.htm>.

Licensing: Assign Representatives to License Pools



Users & Security

LICENSING

Full Support License Pools

Configure license pools to reflect the structure of your support organization and ensure that each pool has the exact number of licenses to which it is entitled. The table shows the number of reserved licenses and the maximum number of licenses allowed for each pool, along with the number of users who are assigned to this pool. Note that this number does not reflect users assigned via group policy or invited representatives.



Note: Active license packs are included in the count of full support licenses; however, they cannot be assigned to license pools.

Add, Edit, Delete

Create a new pool, modify an existing pool, or remove an existing pool.

Add or Edit Full Support License Pool

Name

Create a unique name to help identify this pool. This name should help administrators assign users or groups to a license pool.

Description

Add a brief description to summarize the purpose of this pool.

Reserved Licenses

The number of licenses which should be reserved for this pool. If all other licenses are in use and a representative who is not part of this pool tries to log in to the representative console, then they will be denied login. The note beneath shows how many unreserved licenses are still available and can be assigned.

Maximum Licenses

The maximum number of licenses which can be consumed by users of this pool. If the maximum number of licenses are already in use by users of this pool, then if another representative who is part of this pool attempts to log in to the representative console, they will be denied login. If you do not wish to set a maximum, check **Unlimited**.

Invited Rep License Pool

Same as inviting rep

When a representative sends a rep invite to an external representative, the invited representative should consume a license from the same pool as the representative who sent the request.

Use the following pool for all invited reps

When a representative sends a rep invite to an external representative, the invited representative should consume a license from the specified pool. If this is set to **None**, then the license used will be drawn from the unreserved licenses.

License Usage Notification

Enable License Threshold Alerts

Receive an email when the number of licenses in use reaches the threshold specified below.

License Threshold Alert Options

Set the license threshold to a total number or a percentage of licenses in use. Set the minimum length of time that must elapse before another email can be sent.

Enable Login Denied Alerts

If checked, an email alert is sent whenever a representative is unable to log in due to insufficient licenses, insufficient reserved slots, or the maximum license limit being reached.

License Alert Contact

Enter one or more email addresses to which emails should be sent. Separate addresses with a space. This feature requires valid [SMTP](#) configuration for your B Series Appliance, set up on the **/login > Management > Email Configuration** page.

Reports

Support: Report on Session Activity



Reports

SUPPORT

Support Reports

Administrators and privileged users can generate broad, comprehensive reports and also apply specific filtering to customize reported information based on clear-cut needs.

Report Type

Generate activity reports according to four separate report types: **Session**, **Summary**, **Customer Exit Survey**, and **Representative Survey**.

Filters

Apply filtering options as needed to derive more customized reports from the basic report types. Enable one or more filters as you wish, but only sessions that match all filters selected will be shown.

Session ID or Sequence Number

This unique identifier requires that you specify the ID (LSID) or sequence number for the single session you seek. This is often helpful if you have an external ticketing system or CRM integration. You cannot combine this filter with others.

Date Range

Select a start date for which to pull reporting data. Then select either the number of days for which to pull your report or an end date.

Customer

Filter sessions by customer name, company name, computer name, public IP, or private IP.

Public Site

Filter to focus your reporting on a specific public site.

Representative

Use the dropdown to choose the type of representative participation you want to include. Choose sessions where any representative joined, no representative joined, or a specific representative participated, or where any representative within a team participated, including

sessions that were never associated with the specified team.

Team

Use the dropdown to choose the type of team participation you want to include. Choose sessions that were assigned to at least one team, sessions that were never assigned to a team, or sessions that were assigned to a specific team.

External Key

Filter to report sessions that used the same specific external key.

Include only completed sessions

Filter to include only sessions that have been completed. This excludes sessions that are still running.

Group By *(Visible Only for Summary Reports)*

Choose to group summary report data by representative, by team, or by public site.

Support Session Report Results

View all sessions that match the criteria specified on the previous page. Session reports include basic session information along with links to session details, chat transcripts, and video recordings of screen sharing, Show My Screen, and command shells. Click **Select Visible Columns** to choose which information to view.

Support Session Detail

Session reports detail a record of the full chat transcript, the number of files transferred (and details on failed file transfers), and the permissions requested and granted. Specific command information relevant to *Run As* commands, including credentials, is also provided, but this reporting can be disabled in "[Security: Manage Security Settings](#)" on page 237. Other information includes the public site through which the session was run, session duration, local and remote computer names and IP addresses, and remote system information (if enabled). Reports can be viewed online or downloaded to your local system.

If session recording is enabled, view a video playback of individual sessions, including captions of who was in control of the mouse and keyboard at any given point during the session. Similarly, if Show My Screen recording is enabled, view and download videos of the representative's system during a Show My Screen session. If command prompt recording is enabled, you can also view recordings of all command shells run during the session. All recordings are stored on the B Series Appliance in a raw format and are converted to compressed format when viewed or downloaded.

Summary Report

Summary reports provide an overview of activity over time, categorized by representative, team, or public site. Statistics include the total number of sessions run, the average number of sessions per weekday, and the average duration of sessions.

Customer Exit Survey or Representative Survey Report

View reports of answers to your custom surveys, delimited by public site. A column will be added for each question you include on your surveys and will be titled according to the name designated in the **Report Header** field. For multiple-choice questions, the **Logged Value** will be displayed as the answer. If representatives are also given access to the representative survey during the session, and the administrator has used it to create a detailed workflow, those questions and/or fields, along with the representative's responses, are also displayed on the report.

Team Activity Report

View all team activity that matches the criteria specified on the previous page. Team activity reports include information about users as they log in or out of the representative console, chat messages sent between team members, representative status changes, rep-to-rep screen sharing actions as logged in chat, and files shared and downloaded.

Date Range

Select a start date for which to pull reporting data. Then select either the number of days for which to pull your report or an end date.

Filters

Select either **Team** or **User** to view all activity that matches the provided criteria. Team and User activity reports include information about users as they log in or out of the representative console, chat messages sent between team members, user-to-user screen sharing actions as logged in chat, and files shared and downloaded.



Note: All items listed within Remote Support reports are ordered from newest to oldest.

Presentation: Report on Presentation Activity



Reports

PRESENTATION

Presentations

Range Start, Range End

Select a start date for which to pull reporting data. Then select either the number of days for which to pull your report or an end date.

Presentation Report Results

View all presentations that match the criteria specified on the previous page. Presentation reports include basic presentation information along with links to presentation details, chat transcripts, and video recordings. Click **Select Visible Columns** to choose which information to view.

Licensing: Report on Peak License Usage



Reports

LICENSING

Representative License Report

Date Range

Select a start date for which to pull reporting data. Then select either the number of days for which to pull your report or an end date.


Group By

Choose to group peak license utilization report data by hour, day, or month.

License Usage Report

View reports of peak license usage times. View the number of logged in representatives, the number of representatives in extended availability mode, and the total number of licenses in use.

Vault: Report on Vault Account and Rep Activity


Reports

VAULT

Vault Account Activity Report

Date Range


Select a start date for which to pull reporting data. Then select either the number of days for which to pull your report or an end date.

Account

To see all events which involved a specific BeyondTrust Vault stored account, type in the account name, or select the account from the dynamic pop-up list.

Performed By

To see all events involving a specific user, type the username or part of it, and then select the user from list. To see all events performed by the system, click in the box, and then select **System** from the list. To see all events involving an API account, type **api** in the box, and then select the api account from the list.

 **Note:** If a user has been anonymized in an effort to follow compliance standards, the **Vault Account Activity** report may display pseudonyms for user data or may indicate information has been deleted. To learn more about data anonymization and deletion for compliance efforts, please see [Compliance: Anonymize Data to Meet Compliance Standards at https://www.beyondtrust.com/docs/remote-support/getting-started/admin/compliance.htm](https://www.beyondtrust.com/docs/remote-support/getting-started/admin/compliance.htm).

 For more information, please see the [Vault Guide at https://www.beyondtrust.com/docs/remote-support/how-to/vault/index.htm](https://www.beyondtrust.com/docs/remote-support/how-to/vault/index.htm).

Vault Account Activity Report Results

Because users can be granted separate access to use and check out accounts, the **Vault Account Activity Report** distinguishes between the two. This allows administrators to tell the difference between a user who is able to view the account's password and a user who is only able to inject credentials in a session.

In the **Vault Account Activity Report**, the **Data** column shows information associated with the event. The **Credentials Checked Out** event contains a **Details** link in the new **Data** column when credentials are checked out while in a session. This link redirects to the **Support Session Detail Report** in which the credentials were used.

 **Note:** If the credentials are checked out from **/login**, then no **Details** link is present in the **Data** column.

Compliance: Anonymize Data to Meet Compliance Standards



Reports

COMPLIANCE



IMPORTANT!

By default, the **Compliance** tab is disabled. If your organization requires this functionality, please contact BeyondTrust Support at <https://www.beyondtrust.com/docs/index.htm#support>.

Representative Anonymization

Information about representatives as well as the actions performed during support sessions can be made anonymous to meet privacy regulations and compliance standards.

To anonymize data, select a representative and then click **Search Representative Activity**. The system returns a list of the information found for the representative along with a randomly generated, proposed replacement term for the information. You can also choose to **Add Custom**. This allows you to enter and to search for customized information, such as account numbers.

To modify the replacement text, click the **Edit** button. Within the **Edit Replacement** prompt, set the desired **Replacement**. Choose to **Edit in All History** or **Edit in Only This Session**.

The list updates with the new replacement term and displays, "All support sessions, presentation sessions, team activity, and Vault account activity events for this representative will be marked as anonymized at: (date and time)." After reviewing the replacement terms and timestamp, click **Delete User and Anonymize** to begin the anonymizing process for the entire software. Before starting the anonymization process, you must enter your display name to confirm that you want to perform this action.



IMPORTANT!

All session recordings are deleted as a part of the anonymization request.

Customer Anonymization

Information about customers receiving support as well as the actions performed during support sessions can be made anonymous to meet privacy regulations and compliance standards.

To anonymize data, enter the customer's name, computer name, or IP address into the field. Select the **Partial match** checkbox if partial matches should be listed. Then click **Search Customer Activity**. If data is found, the system returns a list of the information found for the customer along with a randomly-generated, proposed replacement term for the information. You can also choose to **Add Custom**. This allows you to enter and to search for customized information, such as account numbers.

To modify the replacement text, click the **Edit** button. Within the **Edit Replacement** prompt, set the desired **Replacement**. Choose to **Edit in All History** or **Edit in Only This Session**.

The list updates with the new replacement term and displays, "The selected support sessions and presentation sessions will be marked as anonymized at: (date and time)." After reviewing the replacement terms and timestamp, click **Anonymize Selected Sessions** to begin the anonymizing process for the entire software. Before starting the anonymization process, you must enter your display name to confirm that you want to perform this action.

**IMPORTANT!**

All session recordings are deleted as a part of the anonymization request.

Status

Review information about anonymization jobs, including, found terms, replacement terms, the type of data being anonymized, and the status of the job.

The job status is automatically refreshed every 15 seconds, and the status for completed requests remains available for 24 hours.



Note: This status information is also available in the **Support Session Detail** and **Presentation Detail** reports.



Note: For environments where failover or Atlas is configured, the anonymization of data is not complete until synchronization across all nodes or backup B Series Appliances has occurred.

Jump Item: Report on Jump Item Activity



Reports

JUMP ITEM

Administrators and privileged users can generate broad, comprehensive reports and also apply specific filtering to customize reported information based on clear-cut needs. All Jump Item events are logged. By default, logs are saved for 90 days, although this limit can be modified in **Days to Keep Jump Item Logging Information** in **Management > Security > Miscellaneous**.



Note: Make sure the **View Reports** permission is enabled in **Jump > Jump Item Roles > Permissions**. This option is enabled by default for all built-in administrators (the first admin account created on new site installs).



Note: A new **Jump Item Role** called **Auditor** is automatically created on new site installations. On existing installations it has to be created. This role only has a single **View Reports** permission enabled, giving admins the option to grant a user just the permission to run Jump Item reports, without the need to grant any other permission.

Users can view the following events related to Jump Items on Jump Groups (Personal or Shared):

- Jump Item Created
- Jump Item Deleted
- Jump Item Copied From
- Jump Item Copied To
- Jump Item Moved From
- Jump Item Moved To
- Jump Item Session Started

The following information is included as part of the event:

- The time at which the event occurred.
- If the event was initiated by a user, the user's identifying information is associated to that event. This could be a user, API account, or system information. The data in this column is shown as a hyperlink for **User** and **API Account** generated events. When clicked, it links to that **User** or **API Account** edit page, assuming that the user or API account has appropriate permission to view the report.
- The event type.
- Jump Item Type, which is one of the supported Jump Item types, for example, Jump Client, Remote Jump, Remote RDP, etc.
- Name of the Jump Item. The data in this column is shown as a hyperlink. When clicked, the reporting view changes to show the events belonging to only that specific Jump Item. The title of the page also changes to **All Jump Item Events for: <Jump Item Name>**.
- Name of the Jump Group. This is the source Jump Group for **Jump Item Copied From** and **Jump Item Moved From** events, and destination Jump Group for **Jump Item Copied To** and **Jump Item Moved To** events.
- Any additional data that is specific to the logged event. This field can be used to store the destination Jump Group for the events related to Jump Items **Copy** and **Move**.

Reporting data is included in backups.

i For more information, please see "[Days to Keep Jump Item Logging Information](#)" on page 242.

Filters

You can find Jump Item events that match the following filters. You may use multiple filters, but only Jump Item events matching all the filters you enable are retrieved.

Date Range

Select a start date for which to pull reporting data. Then select either the number of days for which to pull your report or an end date.

Jump Group

Filter sessions by Jump Items belonging to a certain Jump Group. If selected, the following options are available:

- Find all sessions started from Jump Items belonging to a specific Jump Group.
- Find all sessions started from personal Jump Items for a specific user.
- Find all sessions in your personal Jump Group.

Jump Item

Click on the search field to find all events involving a specific Jump Item.

Performed by

Click on the search field to find all events involving a specific user, API account, or the system.

Click **Show Report** when done.

Syslog: Download Report Containing All Syslog Files on the Appliance



Reports

SYSLOG


Syslog Report

Download Syslog Files

Click the **Download Syslog Files** button to download a ZIP file containing all syslog files available on the Appliance.

Public Portals

Public Sites: Customize the Support Portal

 Public Portals

PUBLIC SITES

Public Sites

Configure one or more public sites for your BeyondTrust Appliance B Series. A public site is a website where your customers can start a session and through which all session traffic will be directed.

Add New Site, Edit, Delete

Create a new site, modify an existing site, or remove an existing site.

Add or Edit Public Site

Name

Create a unique name to help identify this site. This name helps you determine the public portal through which a customer entered. The default site name cannot be changed.

Site Addresses

Each site must have at least one DNS that resolves to your BeyondTrust Appliance B Series. Multiple hostnames can direct to one site, but one hostname cannot be used for multiple sites.

Default Support Button Profile

Choose which Support Button profile to use for this public site, either the default profile or a customized profile. The button profiles are configured from the **Configuration > Support Buttons** page.

Public Template

Configure the page design and layout by selecting a public web template, configured from the **Public Portals > HTML Templates** page.

 For more information, please see *Customize the Public Site Web Template* at <https://www.beyondtrust.com/docs/remote-support/how-to/customize-portals/html-templates.htm>.

Require SAML Authentication

If **SAML For Public Portals** is configured on the **Users & Security > Security Providers** page, this option is available. If checked, customers must authenticate with an identity provider before a session is initiated using the public support portal.

Display Customer Notices

You can opt to display customer notices on the public site. If this option is checked, the notices are displayed on the public portal, warning customers of potential problems they may be experiencing and for which no support may be needed at this time. This way customers may never enter the support queue, thus allowing representatives to dedicate their attention to customers who need assistance. Customer notices are configured on the **Public Portals > Customer Notices** page.



Note: The same customer notice can be used across several sites, or on a custom portal. The XML for the public portal contains a section where all current notifications are shown. This ensures that messages are always in sync across several sites.



For more information, please see [Choose Connection Options](https://www.beyondtrust.com/docs/remote-support/how-to/customize-portals/connection-options.htm) at <https://www.beyondtrust.com/docs/remote-support/how-to/customize-portals/connection-options.htm>.

Attempt to launch sessions from installed Jump Clients

If this option is checked, and there is already a Jump Client installed on the user's system, an elevated session launches from the existing Jump Client. This applies to both the portal and the session generation API.



Note: For the elevated session to start, a similar permission must be granted for the Jump Client. Please see "[Allow ad-hoc sessions to be started from existing Jump Clients](#)" on page 61.

Representative List

Use Representative List

The representative list displays the names of all logged-in representatives, sorted according to display number. When a customer clicks a name and runs the customer client, a session immediately appears in that representative's personal queue.

Choose if this session initiation option should be available for this support portal. Select if this option should be enabled for the public site and the API, enabled for the API but hidden on the public site, or disabled.



Note: A representative giving a presentation will by default be removed from the representative list, although this exclusion from the representative list can be overridden by selecting **Showing on Representative List** from the representative console.

Display Help Text

Choose if you would like to display help text for this option on the public site. You may customize the text displayed. To revert to the default text, delete the text from the field and then save the blank field.

Start Session Using Click-To-Chat

Uncheck to start sessions with the full customer client rather than web-based chats. Starting sessions with web-based chats is the recommended way to start sessions.

Presentation List

Use Presentation List

The presentation list displays active presentations. For a presentation to be listed here, the representative must have started the presentation and selected to show the presentation on the public site. When a customer clicks a presentation name and runs the client, they will immediately join that presentation.

Display Help Text

Choose if you would like to display help text for this option on the public site. You may customize the text displayed. To revert to the default text, delete the text from the field and then save the blank field.

Session Keys

Use Session Keys

You can generate a session key for a support session or presentation and give it to your customer beforehand, requesting them to submit it on your public site. Running the customer client from a session key places the customer in the queue with the representative who generated the key.

Choose if this session initiation option should be available for this support portal. Select if this option should be enabled for the public site and the API, enabled for the API but hidden on the public site, or disabled.

Display Help Text

Choose if you would like to display help text for this option on the public site. You may customize the text displayed. To revert to the default text, delete the text from the field and then save the blank field.

Start Session Using Click-To-Chat

Uncheck to start sessions with the full customer client rather than web-based chats. Starting sessions with web-based chats is the recommended way to start sessions.

Prompt before downloading the Remote Support Customer Client

Checking the option to prompt the customer requires the remote user to confirm that they would like to start a support session or join a presentation before beginning the BeyondTrust client download. If this option is unchecked, the client download begins as soon as the customer submits the session key or follows the session key link.

Issue Submission Survey

Use Issue Submission Survey

Your customer can fill out an issue submission survey to request support.

Choose if this session initiation option should be available for this support portal. Select if this option should be enabled for the public site and the API, enabled for the API but hidden on the public site, or disabled.

Session Queue Selection

If you set the survey to display common issues, your customer can select the type of problem they are experiencing. Then they will be placed in queue for the team that owns the selected issue.

If you set the survey to list available representatives, your customer will be placed in the selected representative's personal queue. Note that all representatives are displayed, regardless of team membership.

Display Issues for All Teams

Select **Display Issues for All Teams** to list all configured issues, or select the teams whose issues you want to display on this site.

Available/Displayed Fields

From the available fields, select which information fields should display on this site. Go to **Configuration > Custom Fields** to create and manage these fields.

Display Help Text

Choose if you would like to display help text for this option on the public site. You may customize the text displayed. To revert to the default text, delete the text from the field and then save the blank field.

Start Session Using Click-To-Chat

Uncheck to start sessions with the full customer client rather than web-based chats. Starting sessions with web-based chats is the recommended way to start sessions.



For more information, please see the [API Programmer's Guide](http://www.beyondtrust.com/docs/remote-support/how-to/integrations/api) at www.beyondtrust.com/docs/remote-support/how-to/integrations/api.

Post-Session Landing Page

Enable Post-Session Landing Page

Choose per site whether to display a customer exit survey on the BeyondTrust landing page, to redirect your customer to an external URL, or not to send your customer to any landing page

i For more information, please see [Customize the Uninstall Message and Exit Surveys](https://www.beyondtrust.com/docs/remote-support/how-to/customize-portals/post-session-behavior.htm) at <https://www.beyondtrust.com/docs/remote-support/how-to/customize-portals/post-session-behavior.htm>.

Available/Displayed Questions

If you enable the BeyondTrust landing page, select which questions should appear in this site's survey. Questions are configured on the **Public Portals > Exit Surveys** page.

Enable Customers to Download Chat Transcript and/or Session Recording

If you enable the BeyondTrust landing page, you also may choose to provide the customer with a link to download the chat transcript and/or the video recording of the session.

External Landing URL

If you enable a custom landing page, set the external landing URL to which customers should be directed after a support session.

Representative Survey

Enable Representative Survey

You can choose to display a representative survey. The survey will display when a session is completed. It is also possible to allow the representative access to the survey during a session. This option allows administrators to use the survey to create detailed workflows containing external web links with resources, as well as to ensure that representatives record specific information or follow a preset number of support steps. The option to display the survey during a session is configured on the **Public Portals > Exit Surveys** page.

i For more information, please see [Representative Survey](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/representative-exit-survey.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/representative-exit-survey.htm>.

Available/Displayed Questions

If you enable a representative survey, select which questions to display. Questions are configured on the **Public Portals > Exit Surveys** page.

Schedule: Set Public Portal Open Hours



Public Portals

SCHEDULE

Regular Portal Schedules

Configure one or more schedules of regular business hours for your public portals. Outside of these scheduled hours, session start methods other than session keys are removed from your public site, and a portal closed message displays on your public site.

Add New Schedule, Edit, Delete

Create a new schedule, modify an existing schedule, or remove an existing schedule.

Add/Edit a Schedule

Schedule Name

Create a unique name to help identify this schedule.

Portal Closed Message

Create the text to display outside of regularly scheduled hours. Messages can contain macros indicating the next open business day and time. You can use macros, as well as BBCode to do some low level formatting, such as adding bold, colors, or hyperlinks. Click on **Macros** or **BBCode** to display a list of codes and their resulting applications.

Schedule

Set a schedule to define when customers can initiate support sessions. Set the time zone you want to use for this schedule, and then add one or more schedule entries. For each entry, set the start day and time and the end day and time.

If, for instance, the time is set to start at 8 am and end at 5 pm, a customer can start a session at any time during this window. Sessions already in progress are allowed to continue past the schedule end. If session keys are enabled, a representative can send a customer a session key to start a session even outside of the public site schedule.

Apply to the following Public Sites

If you have more than one public site, select which should follow this schedule.

Uses these Holidays

Select any created holidays which should apply to this schedule. Associations made here also apply to the holiday schedule settings.

Holiday Portal Schedules

When a holiday schedule is applied to a regular schedule, the hours set in the holiday schedule override the normal business hours. Holiday schedules can be used to set days off, days with abbreviated hours, or even days with extended hours.

Add New Holiday, Edit, Delete

Create a new holiday schedule, modify an existing holiday, or remove an existing holiday.

Add/Edit a Holiday

Holiday Name

Create a unique name to help identify this holiday schedule.

Date

Set the date when this holiday schedule should apply.

Portal Closed Message

Create the text to display outside of scheduled hours for this date. You can use macros, as well as BBCode to do some low level formatting, such as adding bold, colors, or hyperlinks. Click on **Macros** or **BBCode** to display a list of codes and their resulting applications.

Schedule

Either select **Closed all day** or set a start time and end time.

Apply to the Following Portal Schedules

Select any created regular schedules to which this holiday schedule should apply. Associations made here also apply to the regular portal schedule settings.



For more information, please see [Show Notices and Business Hours on the Public Portal](https://www.beyondtrust.com/docs/remote-support/how-to/customize-portals/portal-messages.htm) at <https://www.beyondtrust.com/docs/remote-support/how-to/customize-portals/portal-messages.htm>.

HTML Templates: Customize the Web Interface



Public Portals

HTML TEMPLATES

Public Site Web Template

Customize your public site's HTML to be consistent with the rest of your web site.

Add or Edit Template

Select an existing template that you want to edit or select **Add** to create a new template.

Name

When creating additional templates, give each a unique name to identify it for further editing or to apply it to a public site.

Template HTML

Macros replace real-time data such as the session initiation options and the language selection dropdown. This enables you to position these elements anywhere on the page.

BeyondTrust recommends leaving the public site unaltered unless you have a working knowledge of HTML format.

Revert to Factory Default HTML

After customizing the site, you can return the public site to its original state by clicking **Revert to Factory Default HTML** at the bottom of the coding window.

Help Icon

Change Help Icon

You can upload a new image to serve as the help icon on the public portal.

Revert to Factory Default Help Icon

To restore BeyondTrust's original help icon for a template, click the **Restore to Factory Default Help Icon** button.



For more information, please see [Customize the Public Site Web Template](https://www.beyondtrust.com/docs/remote-support/how-to/customize-portals/html-templates.htm) at <https://www.beyondtrust.com/docs/remote-support/how-to/customize-portals/html-templates.htm>.

Customer Notices: Create Messages for the Customer Notification System



Public Portals

CUSTOMER NOTICES

Customer Notices

Notify customers, as they are requesting support, of broadly impacting IT outages to avoid flooding your BeyondTrust representatives. These messages can be set to expire at a pre-determined time and applied to one or more public portals.

Once created, customer notices are displayed on the public portal and in Support Button start windows, so that customers get the information they need before even attempting to initiate a session. Notices also appear in the customer client chat window at the beginning of a session and/or when sent from the /login interface.

Administrators and authorized representatives can create up to 10 messages per portal, with each message allowed up to 1,020 characters.

Although messages are not configurable per language, you can create different messages for the languages supported on the same portal.

Administrators can create and edit customer notices and also can grant this right to representatives without administrative privileges.

Add New Customer Notice, Edit, Delete

Create a new notice, modify an existing notice, or remove an existing notice.

Send

Push a customer notice to all holding sessions.

Add or Edit Customer Notice

Name

Create a unique name to help identify this notice. This name is not displayed to the customer.

Notice Text

Create the text to display in the customer client, on the public portal, and in Support Buttons. You can use macros, as well as BBCode to do some low level formatting, such as adding bold, colors, or hyperlinks. Click on **Macros** or **BBCode** to display a list of codes and their resulting applications.



Note: Messages should be relatively short so they can be viewed without much scrolling in the customer client windows. This applies to both the native client and click-to-chat modes.

Expires On

Enter a date for the notice expiration. If you select **Never Expires** the notice will remain on your site until it is manually deleted. Expired notices are automatically deleted 24 hours after their expiration date.

Public Sites

If you have more than one public site, select which ones will display the notice. You can select multiple portals.



For more information, please see [Show Notices and Business Hours on the Public Portal](https://www.beyondtrust.com/docs/remote-support/how-to/customize-portals/portal-messages.htm) at <https://www.beyondtrust.com/docs/remote-support/how-to/customize-portals/portal-messages.htm>.

File Store: Upload Resource Files



Public Portals

FILE STORE

About

Use the online file store to save files you need to reference from your HTML template, such as image files and style sheets. You can also use the file store as a central point of access for files frequently needed during support sessions.

Accessibility

Show File Listing for File Store at /files

If this option is checked, any files uploaded here are accessible by browsing to your support site hostname followed by /files (e.g., support.example.com/files).

View the File Store

If the option above is checked, click this button to view your online file store.

File Store Statistics

View the number of files uploaded, the maximum capacity available, and the maximum file size. The file store limit is 25 MB.

Contents

Upload

Browse for files and upload them to your file store.

Files in File Store

View a list of files uploaded to your file store.

Delete Selected Files

Select one or more files from the list above and click this button to remove those files from your file store.



For more information, please see *Customizing the BeyondTrust Support Portal* at <https://www.beyondtrust.com/docs/remote-support/how-to/customize-portals/file-store.htm>.

iOS Configuration Profiles: Add Apple Configuration Profiles



Public Portals

IOS CONFIGURATION

iOS Configuration Profiles

BeyondTrust supports distribution of Apple iOS configuration profiles, allowing support representatives to offer public and private, administrator-configured profiles to iOS device users for downloading to their iPhone®, iPad™ and iPod touch® devices.



For more information, please see *iOS Configuration Profiles* at <https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/apple-ios/iosconfigurationprofiles.htm>.



IMPORTANT!

To ensure that configuration profiles are downloaded to iOS devices over an encrypted HTTPS connection, you must check the **Force Public Site to Use HTTPS** checkbox on the **Management > Security** page of the /login administrative interface. Otherwise, profile downloads will occur over unencrypted HTTP connections.

To administer Apple iOS settings, you must use an admin account. To create or modify Apple iOS configuration profiles, you must have the user account permission **Allowed to Edit iOS Profiles**. For a representative to give customers access to private configuration profiles, they must have the account permission **Allowed to generate access keys for sending iOS profiles**. In the /login administrative interface, select **Users & Security > Users** and/or **Group Policies** to modify account permissions.

After setting up and exporting a configuration profile from Apple's free iPhone Configuration Utility, use the /login administrative interface in BeyondTrust to make the profile available. You may find the iPhone Configuration Utility on Apple's iPhone Support web site.

Add New Profile, Edit, Delete

Create a new profile, modify an existing profile, or remove an existing profile.

Add or Edit iOS Configuration Profile

Name

Create a unique name to help identify this profile. This iOS configuration profile name should help the user select the right profile when browsing your support portal.

File

Upload the Apple iOS Profile you created with the iPhone Configuration Utility software. Note that the underlying Apple iOS Profile must be altered to change the contents of the iOS device profiles you wish to distribute to iOS device users.

Description

Add a brief description to summarize the purpose of this profile.

Public

Check the **Public** checkbox to make the profile appear in a list visible to any iOS user that browses your public portal. Note that the iOS users will not see a traditional representative list or issue submission dialog when browsing the public portal.

Leaving the **Public** checkbox unchecked allows you to restrict access to the iOS Profile you created. To download private profile content, users must enter an access key you generate in the representative console.

Settings

Select a Public Site to Edit

From the dropdown, select the public site for which you want to configure settings.

iOS Configuration Profiles Link Enabled

If this option is checked, customers on iOS devices will see a link to the iOS configuration profiles portal when they access the public site. This page displays any public profiles you have available, and it provides a text entry box where customers can submit an access key their representative has provided, directing the customers to a private configuration profile.

Portal

Title

Customize the title of the iOS portal page. You can localize this text for any languages you have enabled.

Message

Customize the text that will display on the iOS portal page. You can localize this text for any languages you have enabled.

Invitation Email

When a representative generates an Apple iOS profile access key from the representative console, the access key can be sent in an email to the iOS user.

Subject

Customize the subject of this email. You can localize this text for any languages you have enabled.

Message

Customize the body of this email. Use any of the macros listed below this field in the /login page to customize the text for your purposes. You can localize this text for any languages you have enabled.



For more information, please see [Manage the Apple iOS Configuration Profiles Page](https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/apple-ios/manageprofilespage.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/apple-ios/manageprofilespage.htm>.

Surveys: Enable the Customer Exit Survey and Representative Survey



Public Portals

EXIT SURVEYS

Customer Exit Survey or Representative Survey

Configure questions to implement in customer and representative surveys, useful in monitoring satisfaction levels and incident resolution rates. Questions are assigned to a support site's surveys from the **Public Portals > Public Sites** page.

Allow representatives to modify the survey during a support session

Allow the representative to have access to the survey during a session. Administrators can use the survey to create detailed workflows containing external web links with resources, as well as to ensure that representatives record specific information or follow a preset number of support steps.

Add New Question, Edit, Delete

Create a new question, modify an existing question, or remove an existing question.

Preview Survey

Preview how all survey questions will appear to your customers. Previewing the representative survey shows the basic format, though styles appear differently in the representative console.

Customer Exit Survey or Representative Survey: Add New Question

Question Type

Choose from several types of questions, including radio buttons, check boxes, dropdown menus, text boxes, and text areas.

Question Text

Enter the question text as you would like it to appear on the survey.

Question Name

Assign the question a name for internal formatting.

Report Header

Assign the question a header to identify it on your survey reports.

Answer Required

For representative surveys, set if the representative should be required to answer the question before closing the session.

CSS Style

You may define a CSS style for a customer exit survey question. This options is provided for web development. Users unfamiliar with HTML and CSS are recommended to leave these fields blank.

CSS Classes

You may define CSS classes for a customer exit survey question. This options is provided for web development. Users unfamiliar with HTML and CSS are recommended to leave these fields blank.

HTML ID

You may define an HTML ID for a customer exit survey question. This options is provided for web development. Users unfamiliar with HTML and CSS are recommended to leave these fields blank.

Allow Multiple Selections

For a dropdown menu, you can choose to allow multiple selections.

Size of Text Box

For a text box, set the size of the text entry field.

Max # of Chars in Answer

For a text box, set the maximum number of characters that can be entered.

Text Area Size

For a text input area, set the size of the text entry field.

Display Order

Choose the order in which you would like the question to appear on the survey. Lower numbers appear first.

Default Value

For a text box or text input area, you may insert default text into the field.

Appear on the Default Public Site

If you select this option, this question will automatically be added to the survey for your default support site. Because only ten questions can appear on any given survey, you will receive an error if you attempt to save a question that would exceed this limit on your default site

survey. To create a question for use on another survey, deselect the check box and then save.

Display Value

For each option available to a radio button group, a check box group, or a dropdown menu, assign a display value that will appear to the customer.

Logged Value

For each option available to a radio button group, a check box group, or a dropdown menu, assign a logged value that will be saved in the exit survey reports.

Selected by Default

For a radio button group, a check box group, or a dropdown menu, you can choose to have an option selected by default.

Display Order

For a radio button group, a check box group, or a dropdown menu, set the order in which these options will appear below the question.

Sort Ascending

For a radio button group, a check box group, or a dropdown menu, sort the options in ascending order.

Sort Descending

For a radio button group, a check box group, or a dropdown menu, sort the options in descending order.

Add Option

Add multiple options to a radio button group, a check box group, or a dropdown menu.

Preview Question

Preview how this survey question will appear to your customers. Previewing a representative survey question shows the basic format, though styles appear differently in the representative console.



for more information, please see [Customize the Uninstall Message and Exit Surveys](https://www.beyondtrust.com/docs/remote-support/how-to/customize-portals/post-session-behavior.htm) at <https://www.beyondtrust.com/docs/remote-support/how-to/customize-portals/post-session-behavior.htm>.



For more information, please see [Customer Exit Survey: Submit Feedback](https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-exit-survey.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-exit-survey.htm>.



For more information, please see *Representative Survey* at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/representative-exit-survey.htm>.

Customer Client: Modify the Invitation Email, Display Options, Connection Options



Public Portals

CUSTOMER CLIENT

Select a public site to edit

From the dropdown, select the public site for which you want to configure settings.



Note: Default invitation email, customer agreement, and messaging is provided in all supported languages. Users can update this text. However, once new text is saved to the database, the default text is overwritten and cannot be retrieved.

Invitation Email

Create a custom email message with unique support session instructions for each public site.

From Address

As an option, you can use the **From Address** field to set up system-generated email invitations instead of an invitation that uses the representative's local email client. If configured in this manner, session invitations are sent from a centralized, system-wide address (e.g., admin@support.example.com). This may be particularly useful if your representatives have enterprise email restrictions due to safety or privacy concerns. If the **From Address** field is left blank, the emails will use the *from address* as configured on the **Email Configuration** page.



Note: To enable system-wide emails, make sure that **Enable server-side emails for support invitations** is checked on the **/login > Configuration > Options** page.



For more information, please see "[Email Configuration: Configure the Software to Send Emails](#)" on page 247.

Subject

Customize the subject of this email. You can localize this text for any languages you have enabled.

Body

Customize the body of this email. Use any of the macros listed below this field in the **/login** page to customize the text for your purposes. You can localize this text for any languages you have enabled.

Customer Agreements

i For more information, please see *Customer Client: Support Session Interface* at <https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-support-interface.htm>.

Full Client Sessions

Display Customer Agreement Before Full Client Sessions

Customize the text of this agreement. You can localize this text for any languages you have enabled.

Title

Customize the title of the agreement. The end-user sees this in the title bar of the prompt. You can localize this text for any languages you have enabled.

Acceptance Timeout

If the customer does not accept the agreement within the set **Acceptance Timeout**, the session will end. This applies to unattended sessions only.

Text

Provide the text for the full-client customer agreement. You can localize this text for any languages you have enabled.

Click-to-Chat Sessions

Display Customer Agreement Before Click-to-Chat Sessions

Enable an agreement that the customer must accept before entering a click-to-chat session.

Unattended Sessions

Display Customer Agreement Before Unattended Sessions

Enable an agreement which must be acknowledged before entering an unattended session.

Title

Customize the title of the agreement. The end-user sees this in the title bar of the prompt. You can localize this text for any languages you have enabled.

Acceptance Timeout

If the customer does not accept the agreement within the set **Acceptance Timeout**, the session ends. This applies to both full-client and click-to-chat sessions.

Automatic Behavior

Choose whether unattended endpoints automatically accept or reject sessions started through a Jump Client, Remote Jump, and Jump Items.

Text

Provide the text for the full-client customer agreement. You can localize this text for any languages you have enabled.

Display Options

Show Prompts

To set how prompts appear to your customers during a support session, choose to show prompts as text links in the chat window or as pop-ups above the chat window. The pop-up option does not apply to mobile clients or click-to-chat sessions.

Start Customer Client Minimized for Attended Sessions

Choose to unobtrusively start the customer client minimized and without taking focus in customer-initiated sessions.

Show public site hostname in window title

Choose to display the hostname of your public site in the title bar of the window.

When pinning a Jump Client, set the default behavior such that Customer Clients launched from that Jump Client will start minimized

Choose to unobtrusively start the customer client minimized and without taking focus in Jump Client sessions.

Start Customer Client Minimized for Sessions started via local Jump or Jumpoint

Choose to unobtrusively start the customer client minimized and without taking focus in local Jump or Jumpoint sessions.

Display Session Recording Prompt Before Full Client Sessions

If this option is checked, then at the beginning of a session, the customer will be prompted to allow session recordings. If the customer allows recordings, then the session will be recorded as configured for this public portal. If the customer refuses recordings, then the session will continue, but no recordings will be made. This applies to screen sharing recordings, command shell recordings, and system information logging.

Display Customer Notices in Customer Client

If this option is checked, then until the session is accepted, the customer client will display both customer notices already active when the session was requested as well as customer notices created and sent. Following each notice will be a link to end the session if the notice addresses a known problem for which the customer was requesting support.

Messaging

Customer Greeting

Display Customer Greeting Before Session

The customer greeting appears within the chat window once the session is in queue. You can localize this text for any languages you have enabled.

Let customers know their session status by providing them with feedback regarding their position in queue and estimated wait time. Providing customers with this information creates a better chance they will stay in the queue and get the service they need.

Wait time and position are calculated per queue. A customer's position in queue is determined by the age of the session on a first come, first served basis. The wait time is estimated using the most recent sample of sessions that came through the queue and were answered by a representative. A minimum of five sessions is needed to provide enough data for a reliable wait time calculation.

Messages are configured using macros. Copy the **%POSITION_IN_QUEUE%** and **%ESTIMATED_WAIT_TIME%** macros into the text box.



Note: The macros expand into full sentences describing the customer's position in the queue, as well as the estimated amount of time the customer has to wait.

On-Hold Message

Display On-Hold Message

The on-hold message displays at intervals until a representative accepts the session. You can localize this text for any languages you have enabled.

Let customers know their session status by providing them with feedback regarding their position in queue and estimated wait time. Providing customers with this information creates a better chance they will stay in the queue and get the service they need.

Wait time and position are calculated per queue. A customer's position in queue is determined by the age of the session on a first come, first served basis. The wait time is estimated using the most recent sample of sessions that came through the queue and were answered by a representative. A minimum of five sessions is needed to provide enough data for a reliable wait time calculation.

Messages are configured using macros. Copy the **%POSITION_IN_QUEUE%** and **%ESTIMATED_WAIT_TIME%** macros into the text box.



Note: The macros expand into full sentences describing the customer's position in the queue, as well as the estimated amount of time the customer has to wait.

On Hold Message Interval

Set the number of minutes to wait between sending each on-hold message.

Text

Provide the text for the on-hold message.

Maximum Estimated Wait Time

Provide the longest time to show customers they may have to wait.

Orphaned Message

Display Orphaned Session Message

If a customer requests a session when no representatives are available, an orphaned session message can be displayed. You can localize this text for any languages you have enabled.

And Open This URL

If a session is orphaned, the customer's web browser can be automatically opened to a specified URL, such as a knowledge base or contact page.

Text

Provide the text for the orphaned message.

Chat Window Banner

Change Chat Banner

Upload an image banner for the client window. This image must be a 256-color (8-bit) Windows Bitmap file (BMP) and must be 480 pixels wide. The recommended image height is 40 pixels. As soon as you upload a new banner, all new sessions use that image. Currently running sessions are not affected.

Revert to Default

Revert to the default banner. As soon as you revert to the default, all new sessions use that image. Currently running sessions are not affected.

Watermark

Show on-screen indicator when a representative is in session with the customer (Windows and macOS only).

Check the box to add a watermark to the screen during a session.

Change Watermark

Upload a custom watermark image to display on the client desktop. This custom image replaces the default BeyondTrust watermark. The image must be a .png or .bmp file between 32x32 and 256x256 pixels wide. For best results, the recommended image size is 128x128 pixels. You can resize the selected image by using the slider or by clicking on the **Fit in Box** or the **Fill Entire Box** buttons. Click **Save Watermark** to save the changes, or **Discard Changes** if you do not wish to keep the image you just selected.

When the watermark is rendered on the customer's screen, a 40% transparency is applied, allowing you to upload a fully opaque image without concern that it will obstruct the customer's desktop view.



Note: If you upload an image that is already partially transparent, a further 40% transparency is applied, which may cause the image to be more transparent than desired.



Note: After customers upgrade to BeyondTrust Remote Support 17.1, the watermark for all public portals defaults to the new watermark.



For more information, please see [Modify the Customer Client Appearance](https://www.beyondtrust.com/docs/remote-support/how-to/customize-portals/customer-client-appearance.htm) at <https://www.beyondtrust.com/docs/remote-support/how-to/customize-portals/customer-client-appearance.htm>.

Revert to Default

Revert to the default image. As soon as you revert to the default, all new sessions use that image. Currently running sessions are not affected.

Session Policy

Session Policy

Assign a session policy to sessions associated with the public site selected at the top of this page. This session policy may affect the permissions allowed in sessions started through this site.



For more information, please see [Set Jump Client Pinning and Unpinning Permissions](https://www.beyondtrust.com/docs/remote-support/how-to/jump-clients/permissions.htm), at <https://www.beyondtrust.com/docs/remote-support/how-to/jump-clients/permissions.htm>.

Logging Options

Enable Screen Sharing Recording

For the public site selected at the top of this page, choose if you want to record screen sharing sessions. You can enable or disable recordings, or you can use the site-wide setting configured on the **Configuration > Options** page. This setting may be overridden by customer preference as configured above by the setting **Display Session Recording Prompt Before Full Client Sessions**.

Enable Command Shell Recording

For the public site selected at the top of this page, choose if you want to record command shell sessions. You can enable or disable recordings, or you can use the site-wide setting configured on the **Configuration > Options** page. This setting may be overridden by customer preference as configured above by the setting **Display Session Recording Prompt Before Full Client Sessions**.

Enable Automatic Logging of System Information

For the public site selected at the top of this page, choose if you want to automatically log system information at the beginning of a session. You can enable or disable recordings, or you can use the site-wide setting configured on the **Configuration > Options** page. This setting may be overridden by customer preference as configured above by the setting **Display Session Recording Prompt Before Full Client Sessions**.

Post-Session Behavior

Show the uninstall message when the support session ends

After a session is complete and if a Jump Client is not installed, customers can be notified that the BeyondTrust software has been uninstalled.

Custom Uninstall Message

Set the text of the uninstall message. You can localize this text for any languages you have enabled.



For more information, please see [Customize the Uninstall Message and Exit Surveys at https://www.beyondtrust.com/docs/remote-support/how-to/customize-portals/post-session-behavior.htm](https://www.beyondtrust.com/docs/remote-support/how-to/customize-portals/post-session-behavior.htm).

Connection Options

Reconnect Timeout

Determine how long a disconnected customer client should attempt to reconnect.

Restrict customer access to the computer if the customer client loses its connection or if all of the representatives in a session are disconnected

If the session connection is lost, the remote system's mouse and keyboard input can be temporarily disabled, resuming either when the connection is restored or when the session is terminated.

Allow reps to override this setting per session

You can allow a user to override the session termination setting from the **Summary** tab in the console during a session.

Click-to-Chat

Name Prompt

Customize the name prompt to display a specific question or statement when a user starts a click-to-chat session. The default text is "Please enter your name".

Elevation Prompt

Customize the text you wish to appear to the user when requesting to elevate a click-to-chat session. The default text is "%REP_NAME% is requesting to elevate to full remote support which will allow more features like screen sharing and file transfer. You will be required to run an application that will be sent to you. Do you wish to continue?"



Note: The %REP_NAME% macro is replaced with the public display name of the representative sending the elevation request.

HTML <head> Injection

Users with the **Allowed to edit public sites** permission can insert custom HTML code into the <head> element of the page that renders the HTML5 click-to-chat client.

Other Options

Automatic Elevation

Select how to handle elevation of the customer client on a remote Windows system. If **Never attempt to elevate** is selected, the customer client will never attempt to run with administrative rights unless the representative expressly requests elevation. If you have selected **Attempt to elevate only if doing so will not prompt the customer**, then the customer client will attempt to run as an administrator, but only if doing so will not prompt the remote user for permission. If **Always attempt to elevate** is selected, then the customer client will always attempt to run as an administrator; at the beginning of a session, the remote customer may receive a prompt to allow elevation.

Allow the customer to limit applications shared during screen sharing when not expressly required to do so

If you choose to allow the customer to limit applications shared, your customer will have the option to define which applications you can or cannot view during a screen sharing session. If this option is deselected, customers will receive this option only if the representative specifically requests or is only allowed to request limited control.

Allow the rep to override a customer's disabled Ctrl-Alt-Del (CAD) injection policy (only Windows Vista® and above)

When supporting Windows Vista or above, the representative may attempt to override a customer's disabled Secure Attention Sequence injection policy in order to send a Ctrl-Alt-Del command

Allow the customer to offer files using the chat interface

If you need to prevent file transfers from customer to representative, you can disable the customer's ability to offer files during chat sessions.

Play chat sound notifications in the customer client on supported platforms

You may set the customer client to play a notification sound when a new message is displayed.

Allow customer client to temporarily disable hardware acceleration during screen sharing

You may permit the customer client to detect when a video card driver is causing very high CPU usage on the remote computer; if so detected, the customer client may temporarily disable hardware acceleration during screen sharing to speed the remote support connection.

Presentation: Modify the Invitation Emails and Display Options



Public Portals

PRESENTATION



Note: The presentation feature must be enabled when your support site is built. If it is not available and you need to run presentations, please contact Support or your site administrator.



IMPORTANT!

The presentation feature is being deprecated as of Remote Support 22.1 and is not included in new site deployments. For upgrades, it is turned ON, but you can opt to turn it OFF. If you have a new site deployment and you need to run presentations, please contact Support or your site administrator.



For more information, please see [Give a Presentation to Remote Attendees](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/presentation.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/presentation.htm>.



For more information, please see [Presentation Attendee Client: Join a Presentation](https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-presentation-interface.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-presentation-interface.htm>.

Presentation Attendee

Scheduled Presentation Invitation Email



Note: Currently, only one presentation attendee client configuration is available. Presentation attendee clients cannot be configured per public site.

Send an email inviting attendees to a presentation scheduled for the future.



If the **Invite** button is missing in the presentation schedule dialogue, confirm that client side emails have been configured and enabled on your instance. For more information, please see ["Email Configuration: Configure the Software to Send Emails"](#) on [page 247](#).

Subject

Customize the subject of this email. You can localize this text for any languages you have enabled.

Body

Customize the body of this email. Use any of the macros listed below this field in the /login page to customize the text for your purposes. You can localize this text for any languages you have enabled.

In Progress Presentation Invitation Email

Send an email inviting attendees to a presentation already in progress.

Subject

Customize the subject of this email. You can localize this text for any languages you have enabled.

Body

Customize the body of this email. Use any of the macros listed below this field in the /login page to customize the text for your purposes. You can localize this text for any languages you have enabled.

Presentation Attendee Client

Display Options

Display Attendee Agreement Before Sessions

The **Attendee Agreement** is displayed before the BeyondTrust client download to ensure that your attendee is aware of the program's screen sharing functionality.

Display Customer Greeting Before Session

The **Greeting** welcomes your attendee, requests them to wait until the presentation begins, and provides audio conference details if you have configured them in the representative presentation sidebar. You can localize this text for any languages you have enabled.

Text

Customize the text of this agreement. You can localize this text for any languages you have enabled.

Expiration Timeout

Should the presenter fail to be online when the presentation is supposed to begin, the **Expiration Timeout** determines the length of time the attendee will be allowed to wait before being disconnected.

Display Orphaned Attendee Message

Should the presenter fail to be online when the presentation is supposed to begin and does not join before the expiration timeout is reached, attendees may be shown this message. You can localize this text for any languages you have enabled.

Chat Window Banner

Change Attendee Banner

Upload an image banner for the client window. This image must be a 256-color (8-bit) Windows Bitmap file (BMP) and must be 480 pixels wide. The recommended image height is 40 pixels. As soon as you upload a new banner, all new sessions use that image. Currently running sessions are not affected.

Revert to Default

Revert to the default banner. As soon as you revert to the default, all new sessions use that image. Currently running sessions are not affected.

Post-Session Behavior

Custom Uninstall Message

At the end of the presentation, your attendee will be notified that BeyondTrust has been uninstalled. You can localize this text for any languages you have enabled.

Localization

Real-Time Chat: Translate Chat Messages Between Rep and Customer



Localization

REAL-TIME CHAT

BeyondTrust's optional integration with GeoFluent or AWS Amazon Translate gives your support desk a global advantage by translating chats between reps and customers in real time. Without a language barrier, your support team can reach customers across the globe.

Messages between a customer and a representative can be translated in real time if this feature is enabled. Customers who start sessions using the public portal can select their language from the dropdown menu at the top of the page. Representatives can select their preferred chat language from the **Settings > Global Settings** page in the representative console.

To set up a translation integration, you need to have an account with the translation service.

For GeoFluent, you need a [Lionbridge GeoFluent account](https://www.lionbridge.com/get-in-touch/), available at <https://www.lionbridge.com/get-in-touch/>. Once your account is created, subscribe to the language pairs desired. Language pairs are directional. For example, an English-to-French language pair translates English words to French, but does not translate French words to English. In this example, a second language pair, French-to-English, is required to support the French-to-English translation.

For Amazon Translate, you need to be using Amazon Web Services, and obtain an AWS access key.

Once the account is ready, you configure the service provider in the /login administrative interface, enable real-time chat in the representative console, and, if desired, add a session language option to public portals.

Configure a Service Provider

Follow these steps to configure the translation service provider in BeyondTrust Remote Support:

1. Log in to the administrative interface.
2. Click **Localization** in the left menu, and then click the **REAL-TIME CHAT** tab.
3. Select **AWS** or **GeoFluent** as the **Service Provider**.
4. For GeoFluent:
 - a. A default **GeoFluent API URL** displays. The default is suitable for North American users. Other areas may see improved performance using the URL <https://api-eu.geofluent.com>. Your GeoFluent representative can help you decide if you need to change this value.
 - b. Enter your **API Key**.
 - c. Enter your **API Secret**.
 - d. Click **Save**.
 - e. The system tests the connection and displays the status. If the **Current Status** is not **OK**, confirm the entered values. If necessary, contact GeoFluent for assistance.
 - f. Once the status is **OK**, the **Language Pairs** selected in GeoFluent display on the lower part of the screen.
 - g. Check **Enable Real-Time Chat Translations** to make the feature available to representatives.

5. For AWS:
 - a. For **Region**, enter the AWS region code of the AWS data center to use for translation (e.g. "us-east-1").
 - b. Enter the **Key** to the AWS access token.
 - c. Enter the **Secret** access key generated by AWS.
 - d. Click **Save**.
 - e. The system tests the connection and displays the status. If the **Current Status** is not **OK**, confirm the entered values. If necessary, contact AWS for assistance.
 - f. Once the status is **OK**, the list of supported languages displays on the lower part of the screen.
 - g. Check **Enable Real-Time Chat Translations** to make the feature available to representatives.

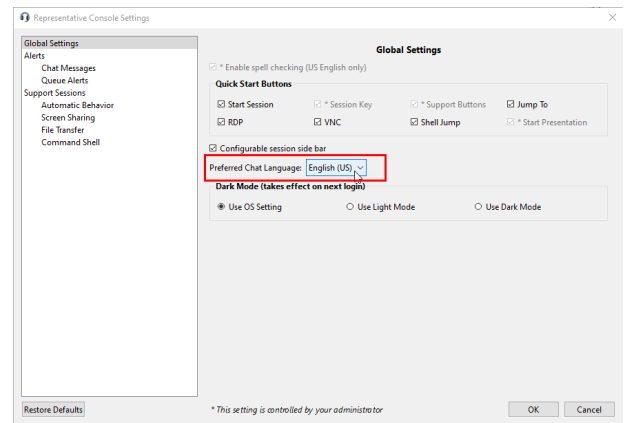


For a list of Amazon Regions, please see [Regions and Zones - Amazon Elastic Compute Cloud](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html) at <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html>.

Enable Real-Time Chat Translations in the Representative Console

Once real-time chat translation is enabled, representatives can select their preferred chat language by following these steps:

1. Download and install the updated representative console.
2. Log in and click **File > Settings**.
3. Under **Global Settings**, select the **Preferred Chat Language** from the dropdown list.



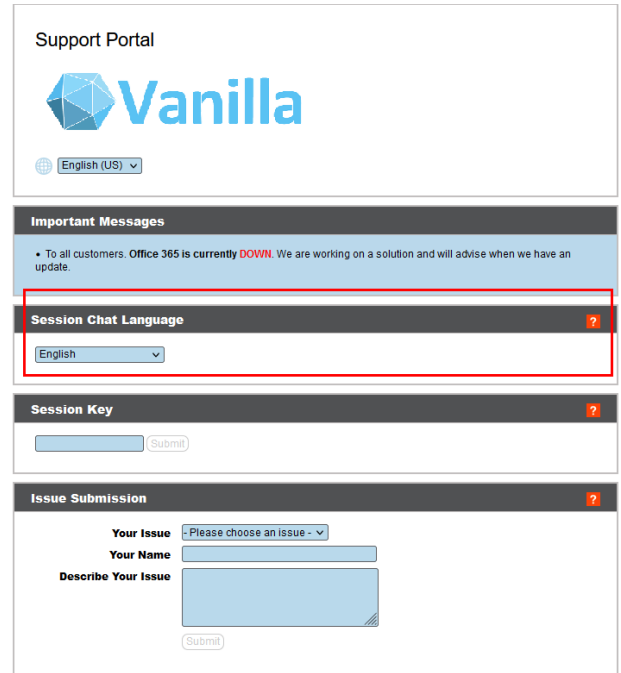
Enable Chat Translation Dropdown Menu on Public Sites

Once real-time chat translations is enabled, a session language option can be added to public portals. This is in addition to the portal language selection option.

Under **Public Portal** on the lower area of the screen, click the **Public Site** link, or click **Public Portals** in the left menu. Repeat the steps below for each site where a session language option is desired.

1. Click the pencil icon to edit the site.
2. Under **Edit Public Site**, check **Display Session Chat Language Dropdown**.

The portal now shows two language dropdowns: one for the portal near the top of the screen, and one for the chat session. The location varies depending on the portal layout and options. The language options for the chat sessions are the language pairs selected in GeoFluent, or available from AWS. This means a user's desired language for the portal may not be available for chat sessions, or vice versa.



The screenshot shows a 'Support Portal' for 'Vanilla'. At the top, there is a language dropdown set to 'English (US)'. Below this is an 'Important Messages' section with a red alert: 'To all customers. Office 365 is currently DOWN. We are working on a solution and will advise when we have an update.' The 'Session Chat Language' section is highlighted with a red box and shows a dropdown menu currently set to 'English'. Below that is a 'Session Key' section with a text input field and a 'Submit' button. At the bottom is an 'Issue Submission' section with a dropdown for 'Your Issue' (set to 'Please choose an issue'), a text input for 'Your Name', a text area for 'Describe Your Issue', and a 'Submit' button.

i For more information, please see the following:

- [Public Site: Request Support at https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/public-site.htm](https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/public-site.htm).
- [Chat with the Customer During a Session at https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/chat.htm](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/chat.htm)

Languages: Manage Installed Languages



Localization

LANGUAGES

Languages

BeyondTrust currently supports English, German, Latin American Spanish, EU Spanish, Finnish, EU French, Italian, Dutch, Polish, Brazilian Portuguese, EU Portuguese, Swedish, Turkish, Japanese, Simplified Chinese, Traditional Chinese, and Russian. BeyondTrust supports international character sets.



Note: Because of translation scheduling, language packs trail slightly behind the English release of any new software version. Also note that for some features localization is limited to 1-byte characters. The use of 2-byte characters (certain language packs) may change expected behavior of some features. The BeyondTrust Jumpoint Configuration interface is not available in translation at this time.

Enabled

If more than one language package is installed, check the box for each language you want to enable. Checking the option makes that language available from the dropdown in the administrative interface, the representative console, and the public site.

Default Language

If more than one language package is installed, select a language to be displayed by default. Click **Update Languages** to save changes.

Installing Language Packs

Language packs must be installed and enabled by the BeyondTrust admin. BeyondTrust Support can build language packs into software updates when requested to do so by customers. Before requesting language packs, check to make sure that they are not already installed and that the active release version supports them. To check for languages and get the necessary update(s), follow these steps:

1. Log in to the BeyondTrust **/login** web interface as an admin user.
2. Navigate to the **Localization** tab and check for the necessary languages.
3. If the languages are listed, check the box for the ones you want to install.
4. If the languages are not listed, contact Support to have a new update built for them.
5. Install any necessary updates and test to see if the desired language(s) appear in BeyondTrust.

Customers can select the language they require from the **language** dropdown menu on the online public portal as well as the exit survey page. Representatives can select the necessary language at the login screen. Admins and reps can select their languages from the dropdown menu in **/login** and **/appliance**.



Tip: It is possible to use a language in a session chat that is not supported by BeyondTrust but is supported by GeoFluent or AWS Amazon Translate. For more information, please see [Real-Time Chat: Translate Chat Messages Between Rep and Customer](https://www.beyondtrust.com/docs/remote-support/getting-started/admin/real-time-chat.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/admin/real-time-chat.htm>.

Search: View Customized Text in Enabled Languages



Localization

LANGUAGES

Search

View all customizable messages on one page. Enter a word or phrase in the search box to narrow the field. Click on the message you wish to modify to see it displayed in all enabled languages. Each message can be modified individually from this page.

The **Default String** cannot be changed and is meant only as a reference for your custom messages. Should you need to revert a message to its original text, delete all of the text from that message box, and save the empty message. The default text in that language will reappear.

Management

Software: Download a Backup, Upgrade Software



Management

SOFTWARE

Backup Settings

It is an important disaster recovery best practice to save a backup copy of your software settings regularly. BeyondTrust recommends backing up your B Series Appliance configuration each time you change its settings. In the event of a hardware failure, a backup file speeds time-to-recovery and, if necessary, allow BeyondTrust to provide you access to temporary hosted services while retaining the settings from your most recent backup.

Backup Password

To password protect your software backup file, create a password. If you do choose to set a password, you are unable to revert to the backup without providing the password.

Include Logged Session Reporting Data

If this option is checked, your backup file includes session logs. If unchecked, session reporting data is excluded from the backup.

Download Backup

Save a secure copy of your software configuration. Save this file in a secure location.

Backup Vault Encryption Key

The Vault encryption key is used to encrypt and decrypt all Vault credentials stored on your BeyondTrust Appliance B Series. If you ever need to restore configuration data from a backup onto a new B Series Appliance, you must also restore the Vault encryption key from a backup to be able to use the encrypted Vault credentials contained in the configuration backup.

Backup Password

To password protect your software backup file, create a password. If you do choose to set a password, you will be unable to revert to the backup without providing the password.

Download Vault Encryption Key

Click the **Download Vault Encryption Key** button to download the Vault encryption key for you to use later.



Note: The Vault encryption key must be password protected.

Restore Settings

Configuration Backup File

Should you need to revert to a backup, browse to the latest backup file that you saved.

Configuration Backup Password

If you created a password for your backup file, enter it here.

Vault Encryption Key Backup File

To provide the Vault encryption key corresponding to the configuration backup, choose the Vault encryption key backup file.

Vault Encryption Key Backup Password

Enter the password you used to download the BeyondTrust Vault encryption key.

Upload Backup

Upload the backup file to your B Series Appliance and restore your site's settings to those saved on the backup.



Note: Restoring the site backup does not revert the help icon to the image present at time of backup, nor does it remove any files added since backup. Not all files are backed up, only the first 50 files under 200KB in size.



For more information, please see [Back Up Procedures](https://www.beyondtrust.com/docs/remote-support/how-to/disaster-recovery/index.htm) at <https://www.beyondtrust.com/docs/remote-support/how-to/disaster-recovery/index.htm>.

Upload Update

Click **Choose File** to manually upload new software packages from BeyondTrust. Confirm that you wish to upload the software package. The **Uploaded Update** section displays additional information to verify your uploaded package. Click **Install** if you wish to complete the installation process, or **Delete Update** if you wish to clear the update staging area. If your update package only contains additional licenses, you can install the update without restarting the B Series Appliance. After confirmation that you wish to install, the page displays a progress bar to notify you of the overall installation progress. Updates made here automatically update all sites and licenses on your BeyondTrust Appliance B Series.



Note: Your B Series Appliance administrative can also use the **Check for Updates** feature of the B Series Appliance interface to automatically search for and install new software packages.

Site Migration

Site migration allows you to migrate configuration settings and data from another BeyondTrust Remote Support site. For example, migration can be used to move from an on-premises installation to a cloud installation. Migration uses an API account to automatically download and restore a backup.

Preparation for Migration

Before migrating the data, please observe these prerequisites and conditions:

- The API account needs read-only or higher access to the command API, and access to the backup and Vault encryption key APIs.
- The administrator needs access to the local admin account to log in, in case security providers do not reconnect properly after the migration.
- If the source site version is earlier than 21.2, the Vault encryption key must be migrated manually.
- If the destination site is a cloud installation, or otherwise does not support passive Jump Clients, any existing passive Jump Clients must be converted to active Jump Clients before migration. If not, they are uninstalled. If the destination site supports passive Jump Clients, such as when migrating to an on-premises installation, passive Jump Clients can be migrated.
- Recordings are not included as part of migration. To retain access to existing recordings, keep the source online with a different host name or use the integration client to back up the recordings before migration.
- After the data has been migrated, additional steps are required to make the new instance fully functional. These steps are listed on the **Site Migration** panel, and are summarized below:
 - Create a new DNS entry for the host name to access the old site.
 - Add the new host name to the old site public portal.
 - Confirm access to the old site.
 - Allow time for DNS entries to propagate across networks.
 - Click the **Restart Software** button on the old site to upgrade clients to use the new site.

Data Migration

1. Enter the following information about the source site to start a migration:
 - **Hostname**
 - **OAuth Client ID**
 - **OAuth Client Secret**
2. Once the information is entered, click **Verify Connection**.
 - A pop-up notification verifies the connection and that the site version is supported.
 - **Reset** can be clicked at any time before starting the migration, if changes are required.
3. If applicable, click **+Choose Certificate** to select the **SSL Certificate** for a self-signed SSL certificate.



Note: Certificates must be in PEM, DER, or CRT format.



***Tip:** An option to **Automatically begin site migration** is available once the connection is verified. Check this option to bypass some of the steps and notifications that follow. If checked, click **Retrieve Backup** and respond to the notifications to complete the migration.*

4. Review displayed information, and if correct, click **Retrieve Backup**. If not correct, click **Reset**.
5. Pop-up confirmation messages appear for the backup file and, if applicable for your version, the Vault encryption key. The file names display on the panel, as well as a **Migrate Site** button.
6. Click **Migrate Site**.
7. A pop-up notification warns that a local account is required, and a second pop-up warns that the migration overwrites data on the current site. Then a **Migration in Process** message displays.
8. When the migration completes, click **Yes** in the pop-up notification to reset the site. Log in again to view the migrated data.
9. Complete the post-migration steps listed on the **Site Migration** panel.

Security: Manage Security Settings



Management

SECURITY

Authentication

Default Authentication Method

The default authentication method is **Username & Password**. If passwordless authentication is enabled, Passwordless FIDO2 can be selected as the default authentication method. If passwordless authentication is enabled, either authentication method can be selected when logging in.

Enable Passwordless FIDO2 Authentication

This feature allows users from the local security provider or vendor users to register and log in with FIDO2-certified authenticators rather than a password. FIDO2 authenticator devices must support CTAP2 and be able to perform user verification using biometrics or a PIN.

This feature is enabled by default. Uncheck to disable the feature. If unchecked:

- The **Passwordless Authenticators** section of **My Account > Security** is hidden.
- The **Passwordless FIDO2** option is not available at the login dropdowns.
- Users are unable to log in using previously registered authenticators.

Unchecking this feature does not remove previously registered authentications. If it is necessary to remove those, they must be deleted before the feature is disabled.

Users with registered passwordless authentication can continue to log in using their username and password. This can be useful if they need to log in using a device that does not support passwordless authentication.

This feature cannot be limited to specific users or user groups.



For more information, and to register authenticators, please see ["Passwordless Authenticators" on page 20](#).

Account Lockout After

Set the number of times an incorrect password can be entered before the account is locked out.

Account Lockout Duration

Set how long a locked-out user must wait before being allowed to reattempt login. Alternatively, require an admin to unlock the account.

Passwords

Minimum Password Length

Set rules for local user accounts regarding the length of passwords.

Default Password Expiration

Set rules for local user accounts regarding how often passwords expire.

Require Complex Passwords

Set rules for local user accounts regarding the complexity of passwords.

Enable Password Reset

Allow users with configured email addresses to reset passwords. The link provided in password reset emails are valid until one of the following events occurs:

- 24 hours has elapsed.
- The link is clicked, and the password is successfully reset.
- The system sends another link to the email address.

Representative Console

Terminate Session If Account Is In Use

If a user tries to log in to the representative console with an account already in use, a checked **Terminate Session** box disconnects the previous connection in order to allow the new login.

Enable Saved Logins

Allow or disallow the representative console to remember a user's credentials.

Log Out Idle Representative After

Set the length of time after which an inactive user is logged out of the representative console to free the license for another user.

Enable Warning and Logout Notification on Idle Timeout

Set if a user should receive a prompt before being logged out due to inactivity. The first notification occurs 30 seconds before logout and the second when logout has occurred.

Remove Representative from Session After Inactivity

This option effectively pushes a user out of a session after the period of inactivity you select. This helps BeyondTrust customers meet compliance initiatives with inactivity requirements. The user is notified 1 minute prior to removal and may reset the timeout.

A user is considered active in a session if any files are being transferred, whether through the file transfer tab or the chat interface, or if they click the mouse or press a key in the session tab. Mouse movement by itself does not count as activity. As soon as activity stops, the inactivity timer begins.

Allow Mobile Representative Console and Web Rep Console to Connect

Give users the option of accessing remote systems through the representative console app for iOS and Android, as well as through the web rep console, a browser-based representative console.

Display Thumbnail View in the Representative Console

When supporting a customer with multiple monitors, this option allows user to see thumbnail images of all available displays. These thumbnail images are not recorded in session recordings. Uncheck this box to show rectangles rather than thumbnails.

Allow Representatives to Take Remote Screenshot

You can allow users to capture screenshots of the remote desktop from the representative console.

Allow Representatives to Control the Customer Client Window

Enabling this setting allows the representative to act as the user in the customer client window, including typing in the chat area, sending files, and interacting with links and buttons. When this setting is disabled, the representative's control of the customer client window is limited to moving and minimizing it.

When requesting to elevate, allow credentials to be entered

When elevating a session to have administrative rights, allow users to enter credentials manually, inject them from a password vault, or provide them through a virtual smart card. This allows users to use authorized privileged credentials to elevate the context of the customer client. Once elevated, the customer client will run in the context of the local system.

Allow Reboot with Cached Login Credentials

In a support session running with administrative rights on a remote Windows™ computer, this allows a representative to reboot the remote machine without the customer's assistance by having the customer enter login credentials prior to the reboot. These credentials can be saved for the duration of the support session, allowing the machine to automatically log in when rebooted multiple times.

Clipboard Synchronization Mode

Clipboard Synchronization Mode determines how users are allowed to synchronize clipboards within a screen sharing session. The available settings are as follows:

- **Automatic:** The customer and representative's clipboards are automatically synchronized when one or the other changes.
- **Manual:** The representative has to click one of the clipboard icons on the representative console to either send content to or pull content from the endpoint's clipboard

You **MUST** restart the software on the status page for this setting to take effect.

Admins can prevent representatives from accessing the clipboard, can allow reps to send data to the endpoint, or can allow reps to have access in both directions (send and receive data). These settings control which clipboard icons the representative sees in the representative console when **Manual** mode is selected, as well as how the synchronization flows in **Automatic** mode.

Granular control of access to the clipboard can be set for session policies and group policies, as well as granted to specific representatives. Please see the links below for each particular case:

- **"Users: Add User Permissions for a Representative or Admin" on page 118:** Users and Security > Users > Add > Attended and Unattended Session Permissions > Screen Sharing
- **"Session Policies: Set Session Permission and Prompting Rules" on page 155:** Users and Security > Session Policies > Add > Permission > Screen Sharing
- **"Group Policies: Apply User Permissions to Groups of Users" on page 164:** Users and Security > Group Policies > Add > Attended and Unattended Session Permissions

Allow Search for External Jump Items

This enables Jump item searching in Remote Support through a fully configured Endpoint Credential Manager (ECM).



Note: You must restart the software for this setting to take effect. When enabling or disabling this setting, you are prompted to restart now or restart later from the **Status** page in /login.

Jumpoint for External Jump Item Sessions

This field is available only when the **Allow Search for External Jump Items** option is checked. All sessions started from external Jump items are performed through the Jumpoint selected here, or in the case where multiple Jumpoints are deployed on endpoints across segmented networks, the Jumpoint used can be selected automatically by matching against an External Jump Item's Network ID. A Jumpoint must be positioned on the network to have connectivity to potentially any of the External Jump Items returned by the ECM.

Select the Jumpoint to use for external Jump Item sessions from the dropdown list of available Jumpoints, or leave the default selection of **Automatically Selected by External Jump Item Network ID** to allow Remote Support to determine which Jumpoint handles the session.

The **External Jump Item Network ID** is an attribute you must set on the Jumpoint from **Jump > Jumpoint** in /login. It is equivalent to the **Workgroup** attribute on managed systems in Password Safe. Its value is matched against the **Network ID** property for external Jump Items returned by the ECM to determine the Jumpoint to handle a session.

External Jump Item Group Name

This field is available only when the **Allow Search for External Jump Items** option is checked. Optionally, enter a name for the external Jump Group, or leave the default option of **External Jump Items**. This name displays as the Jump Group name when viewing Jump Items in the representative console or the web rep console. Click **Save** if you have modified the default group name.

Log "Run As" Special Action Commands in Session Reports

Uncheck this option to stop logging and reporting all *Run As* commands. Since the entire command is logged, any credentials passed as command parameters are logged.

Session Key

Session Key Length

The **Session Key Length** can be set to any number of characters between 7 and 20.

One Time Use Session Key

If **One Time Use Session Key** is checked, a session key cannot be used more than once to create a support session.

Maximum Session Key Timeout

Maximum Session Key Timeout sets the longest time for which a session key may remain valid. From the representative console, a user can set the lifetime of each generated session key up to but no longer than the time defined on this page. If the customer does not use the session key within the allotted time, the key expires, and the user must issue a new session key in order to run a session.

Public Portal

Force Public Site to Use HTTPS

Additional security can be obtained with **Force Public Site to Use SSL (https)**. Using HTTPS forces the internet connection to your public support portal to be SSL-encrypted, adding an additional layer of security to prevent unauthorized users from accessing accounts.

Block External Resources, Inline Scripts, and Inline Styles on the Public Site

Prevent your public site from loading external resources, running inline scripts, or displaying inline styles. This option is effected by sending the Content-Security-Policy (CSP) HTTP header with a value of **default-src 'self'**.

The CSP header tells the browser to ignore resources such as images, fonts, style sheets, scripts, frames, and other subresources from outside its own origin domain. It also ignores inline scripts and styles, whether included in the head or body of the page. This also affects inline scripts and styles added dynamically at runtime from JavaScript.

Any resources you wish to use must be uploaded to the B Series Appliance at **Public Portals > File Store**. You should not enable this option if you have customized your public site template to use inline scripts, inline styles, or resources external to your BeyondTrust site.

Enable Streamlined Session Start

Attempt to start sessions using ClickOnce or Java. If this option is unchecked, the customer client must be manually downloaded and run.

Disable Public Site Indexing

Check **Disable Public Site Indexing** to prevent search engines from indexing public sites hosted by your B Series Appliance.

Miscellaneous

Days to Keep Logging Information

In **Days to Keep Logging Information**, you can set how long logging information should be stored on the B Series Appliance. This information includes the session reporting data and recordings. The maximum duration for which session reporting data and recordings can be retained on a B Series Appliance is 90 days. This is the default value in a new installation. It is possible that session recordings for some sessions within the retention time frame are not available. This could be caused by disk space constraints or the **Days to Keep Logging Information** setting.

The BeyondTrust Appliance B Series runs a maintenance script every day that ensures disk usage does not exceed 90%. Should this be exceeded, the script begins deleting session recordings based on a formula until the disk usage is less than 90%. If the **Days to Keep Logging Information** setting was recently changed, the new setting may take up to 24 hours to go into effect.



If data or recordings must be retained beyond the configured limit, BeyondTrust recommends using the [Integration Client](http://www.beyondtrust.com/docs/remote-support/how-to/integrations/ic) (www.beyondtrust.com/docs/remote-support/how-to/integrations/ic) or the [Reporting API](http://www.beyondtrust.com/docs/remote-support/how-to/integrations/api/reporting) (www.beyondtrust.com/docs/remote-support/how-to/integrations/api/reporting).

Days to Keep Jump Item Logging Information

Choose how long Jump Item reporting data will be accessible from the appliance. Because data is purged only once a day, it may actually be accessible for up to 24 hours beyond what is selected here.

Enable Chat History Recovery

Check this box so that if a session is interrupted and then resumed, the chat window will recover the chat messages.

Require Remote Support Client Verification During Elevation Attempts

You must provide remote support client verification during elevation.

SSL Certificate Validation

You can require **SSL Certificate Validation** to force BeyondTrust software - including representative consoles, customer clients, presentation clients, and Jump Clients - to verify that the certificate chain is trusted, that the certificate has not expired, and that the certificate name matches the B Series Appliance hostname. If the certificate chain cannot be properly validated, the connection is not allowed.

If certificate verification has been disabled and is then enabled, all consoles and clients automatically upgrade the next time they connect. Note that LDAP connection agents are not automatically upgraded but must be reinstalled for this setting to take effect.

When **SSL Certificate Validation** is enabled, security checks in addition to BeyondTrust's built-in security are performed to validate the SSL certificate chain being used to secure communications. It is highly recommended that you do enable SSL validation. If certificate validation is disabled, a warning message appears on your administrative interface. You can hide this message for thirty days.



Note: To enable SSL certificate validation, you must provide your SSL certificate to BeyondTrust so that the certificate can be embedded within your BeyondTrust software.

i For more information, please see [SSL Certificates and BeyondTrust Remote Support at https://www.beyondtrust.com/docs/remote-support/how-to/sslcertificates/index.htm](https://www.beyondtrust.com/docs/remote-support/how-to/sslcertificates/index.htm).

Network Restrictions

Determine which IP networks should be able to access /login, /api, and the representative console on your BeyondTrust Appliance B Series. If you enable network restrictions, you can also enforce the networks on which representative consoles may be used.

Define network rules for the following interfaces:

Admin Interface (/login) and API Interface (/api)

- **Always apply network restrictions:** when selected, you have the option of creating either an allow list containing only allowed networks, or a deny list containing networks that are denied access. When this option is selected, you can determine which restrictions, if any, should apply to the desktop, mobile, and web access consoles.
- **Never apply network restrictions:** when selected, no restrictions are applied and no other options are available to apply restrictions to the desktop, mobile, and web console.

Desktop and Mobile Representative Console

- **Always apply network restrictions:** when selected, it inherits the network restrictions entered for the Admin interface.
- **Never apply network restrictions:** when selected, no restrictions are applied to the desktop and mobile consoles, but you have the option to apply restrictions to the web representative console.
- **Only apply network restrictions for user's first authentication:** this applies restrictions selected above, but only when the user first logs in.

Web Console (/console)

- **Always apply network restrictions:** when selected, the web representative console inherits the restrictions entered for the admin interface.
- **Never apply network restrictions:** when selected, no restrictions are applied to the web representative console, even if restrictions are in effect for the other access console methods.

i For more information, please see [Web Rep Console Guide at https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/web/index.htm](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/web/index.htm).

Define your network restrictions:

Enter network address prefixes, one per line. Netmasks are optional, and they can be given in either dotted-decimal or integer bitmask format. Entries that omit a netmask are assumed to be single IP addresses.

- **Allow list:** Allow only the specified networks
- **Deny list:** Deny the specified networks.

Proxy Configuration

Configure a proxy server to control the dataflow for information sent from the B Series Appliance. This applies to outbound events and API calls.

Proxy Protocol

Configure HTTP or HTTPS proxy types for outbound connectivity from the B Series Appliance.

Enable Proxy Configuration

Check the box to enable the outbound proxy settings.

Proxy Host

Enter the IP address or hostname of your proxy server.

Proxy Port

Enter the port your proxy server uses. The default port is **1080**.

Proxy Username and Password

If your proxy server requires authentication, enter a username and password.

Test

Click **Test** to ensure configuration settings are entered correctly. The current test result is displayed in the **Last Test Result** area. Error messages indicate where configuration settings must be corrected.

ICAP Configuration

You can configure file transfers to pass through the Secure Remote Access Appliance and be scanned by an Internet Content Adaptation Protocol (ICAP) server. If the ICAP server indicates that a file is malicious, it is not sent to the destination.



IMPORTANT!

File transfers cannot be sent to an ICAP server in the following scenarios: Protocol Tunnel Jump-based file transfers, clipboard file transfers within RDP sessions, and external tool file transfers within RDP or Shell Jump sessions. Even with ICAP enabled, these transfers are not scanned.



Note: *Enabling ICAP or changing the ICAP URL requires restarting the appliance to ensure clients are reconnected and properly configured. In an Atlas environment, a sync is required.*



Using ICAP reduces the performance of file transfers due to the added steps and scanning. If the ICAP server is down, file transfers fail.

Improper ICAP configuration prevents Jumpoints from working correctly.

ICAP Settings

Enter the **ICAP Server URL**. This is supplied by your ICAP server vendor. The default port is 1344. If you are using another port, it must be entered with the URL, in this format: **icap://example.com:0000** or **icaps://example.com:0000**.

If the protocol is **icaps://**, check **Use a CA Certificate**. Then click **Choose a Certificate** and upload the certificate.



Note: *If you use a self-signed ICAPS certificate and you do not provide a CA certificate that can validate it, all session file transfers will fail.*

Expired or invalid certificates cause session file transfers to fail, regardless of whether a CA certificate is provided.

Save the ICAP settings before testing.

Test ICAP Connection

After entering and saving the ICAP settings, click **TEST WITH A FILE** and select a file to upload. There are three possible results:

- A connection error. An error header and ICAP logs display (if available).
- A malicious file is detected. A warning header and response details display. The exact nature of the malicious content does not display.
- No problems are detected. The response details display.

Site Configuration: Enable Prerequisite Login Agreement



Management

SITE CONFIGURATION

/login Prerequisite Login Agreement

Enable Login Agreement

You can enable a login agreement that users must accept before accessing the /login administrative interface or the representative console. The configurable agreement allows you to specify restrictions and internal policy rules before users are allowed to log in.

Agreement Title

Customize the title of the agreement. You can localize this text for any languages you have enabled.

Agreement Text

Provide the text for the login agreement. You can localize this text for any languages you have enabled.

Email Configuration: Configure the Software to Send Emails



Management

EMAIL CONFIGURATION

Email Address



Note: If a B Series Appliance is designated as a backup B Series Appliance or a traffic node, the email configuration for that B Series Appliance will be overwritten with the email configuration defined on the primary B Series Appliance.

From Address

Set the email address from which automatic messages from your B Series Appliance will be sent.

SMTP Relay Server

Configure your B Series Appliance to work with your SMTP relay server in order to send automatic email notifications of certain events.

SMTP Relay Server

Enter the hostname or IP address of your SMTP relay server.

SMTP Port

Set the SMTP port to contact this server on.

SMTP Encryption

Based on your SMTP server settings, choose **TLS**, **STARTTLS**, or **None**.

SMTP Authentication Type

To use a form of authentication with this server, select either **Username and Password** or **OAuth2**. Otherwise, select **None**.

Username and Password

Enter a username and password to configure this form of authentication.

OAuth2



For more information, please see the following:



- ["Configure OAuth2 for Azure Active Directory" on page 249](#)
- ["Configure OAuth2 for Google" on page 250](#)

Admin Contact

Default Admin Contact Email Addresses

Enter one or more email addresses to which emails should be sent. Separate addresses with a space.

Send Daily Communication Notice

You can have the B Series Appliance send a daily notification to ensure that alert communication is working correctly.

Send a test email when the settings are saved

If you wish to receive an immediate test email to verify that your SMTP settings are accurately configured, check this option before clicking the **Save** button.

In addition to the test email and daily communication notices that can be configured above, emails are sent for the following events:

- During any failover operation, the product version on the primary node does not match the product version on the backup node.
- During a failover status check, any of the following problems are detected.
 - The current B Series Appliance is the primary node and a shared IP address is configured in /login, but its network interface is not enabled.
 - A shared IP address is configured in /login but is not listed as an IP address in /appliance.
 - The backup node could not contact the primary node, and it also could not contact any of the test IP addresses configured on the **Management > Failover** page.
 - The backup node could not contact any of the test IP addresses configured on the **Management > Failover** page.
 - The backup node's backup operations are disabled on the **Management > Failover** page.
 - The backup node unexpectedly failed to perform a probe of itself, indicating that it is malfunctioning.
 - The backup node failed to contact the primary node using the primary node's hostname.
 - Automatic failover is disabled, and the backup node failed to probe the primary node.
 - Automatic failover is enabled, and the backup node failed to probe the primary node. The backup node will automatically become the primary node if the primary node remains unresponsive.
 - Automatic failover is enabled, and the backup node is automatically becoming the primary node because the primary node was down for too long.
 - The primary node failed to perform a data sync with the backup node sometime in the past 24 hours.

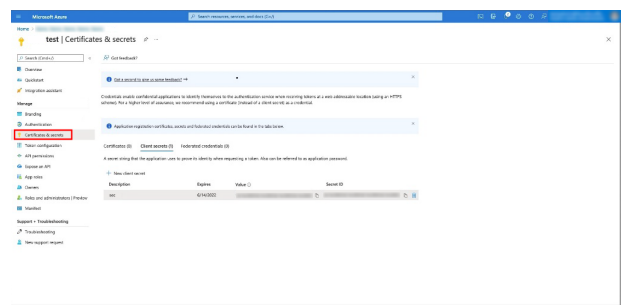
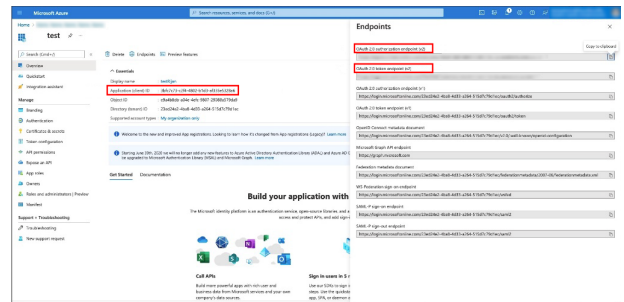
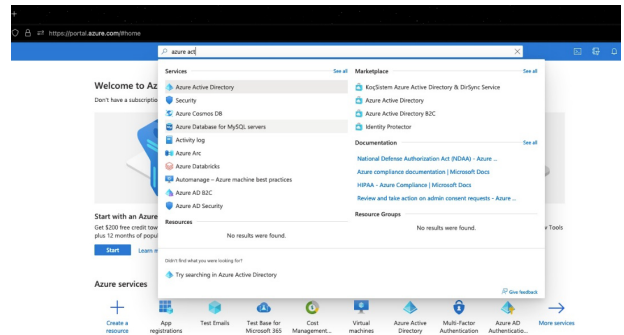
Configure OAuth2 for Azure Active Directory



Note: Before starting configuration on the Azure Active Directory, an Azure/Office 365 Administrator must enable Authenticated SMTP for each account on Exchange online. To do this, go to **Office 365 Admin Portal** (admin.microsoft.com) > **Active Users** > **Mail** > **Manage Email apps** and check **Authenticated SMTP**.

Configure Azure Active Directory

- Log into your Azure console (portal.azure.com), and navigate to **Azure Active Directory**.
- Go to **App registrations**, and select **New registration**.
 - Enter a name, such as **Appliance-OAuth2**.
 - Select the types of account you want to be able to log in to the application through OAuth2. Select **Single Tenant** for internal only.
 - Enter the **Redirect URI** in the form of `https://{URL OF YOUR APPLIANCE}/login/smtplib-verification/`.
 - Click **Register**.
- On the **Overview Page** (selected from the left menu), note the **Application (client) ID**. It is required later.
- Click **Endpoints** (above the **Application (client) ID**).
- Note the **OAuth2.0 authorization endpoint (v2)** URI and the **OAuth token endpoint (v2)** URI. These are required later.
- On the **Certificates & secrets** page (selected from the left menu), note the **Client secret**. It is required later. If you do not have a **Client secret**, click **New client secret** to create one.



Provide Credentials to the SMTP Relay Server

1. Within the Remote Support admin interface, navigate to **Management > Email Configuration**.
2. Under **SMTP Authentication Type**, select **OAuth2**, and enter the following information:
 - **Email:** The email address for the SMTP relay.
 - **SMTP OAuth Provider ID:** The application ID noted earlier.
 - **SMTP OAuth Client Secret:** The client secret noted earlier.
 - **SMTP OAuth Scopes:** Enter **https://outlook.office.com/SMTP.Send offline_access**.
 - **SMTP OAuth Authentication Endpoint:** The authorization endpoint noted earlier.
 - **SMTP OAuth Token Endpoint:** The token endpoint noted earlier.
3. Click **Save**.
4. Now you can verify and connect the provider account. Click **Verify OAuth2 Provider**.

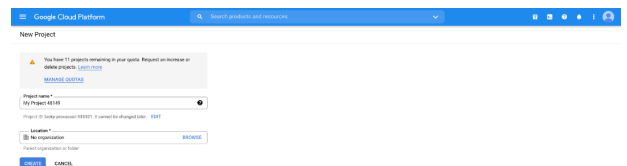
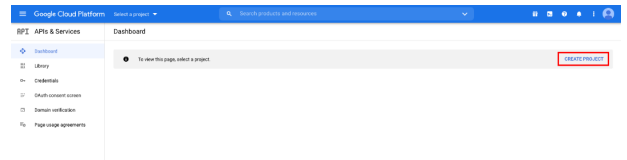


Note: Ensure you are logged into the provider portal as the email address for the SMTP relay, entered above, in the same browser session. You may need to log out of your personal or admin account.

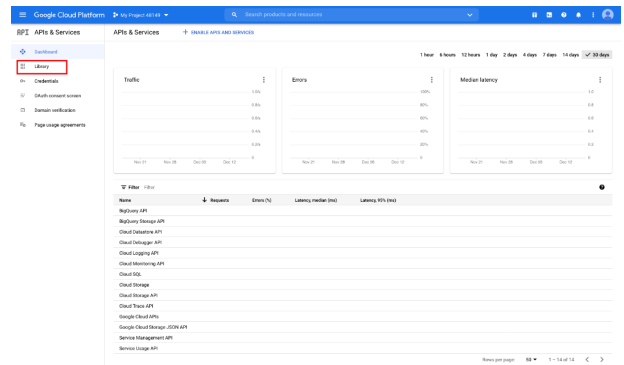
Configure OAuth2 for Google

Configure Google Cloud

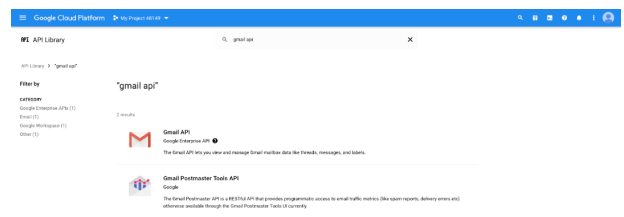
1. Log in to your Google Cloud Platform console (Google Dev Console) (console.cloud.google.com). Use the correct gmail account, as only the owner of the project is able to work with the project. If you do not already have a paid account, you may choose to purchase an account by clicking **Activate** in the top banner. BeyondTrust cannot provide assistance with purchasing an account. Click **Learn More** in the top banner for information regarding the limitations of free accounts.
2. Click **CREATE PROJECT**. You can also use an existing project.
3. Accept the default **Project Name**, or enter a new name.
4. Accept the default **Location**, or select a folder from those available for your organization.
5. Click **CREATE**.



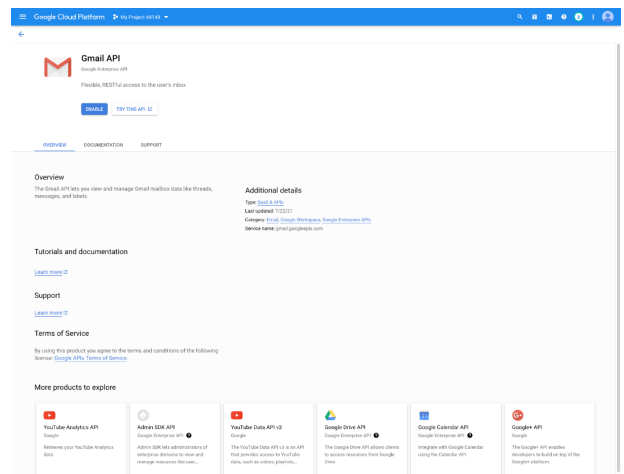
6. The **APIs and services** page appears. Click **Library** in the left menu.



7. Search or browse for the **Gmail API** in the library, and click it.

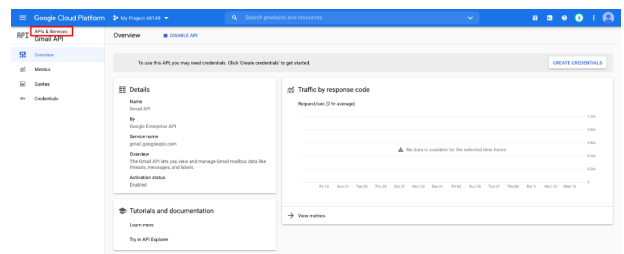


8. The **Gmail API** appears on its own page. Click **ENABLE**.

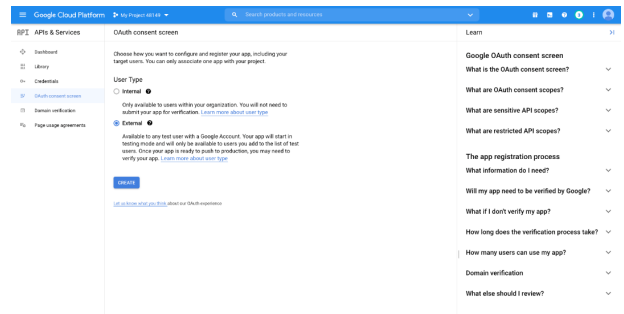


9. The **Gmail API Overview** page appears. Click **APIs & services** in the upper left.

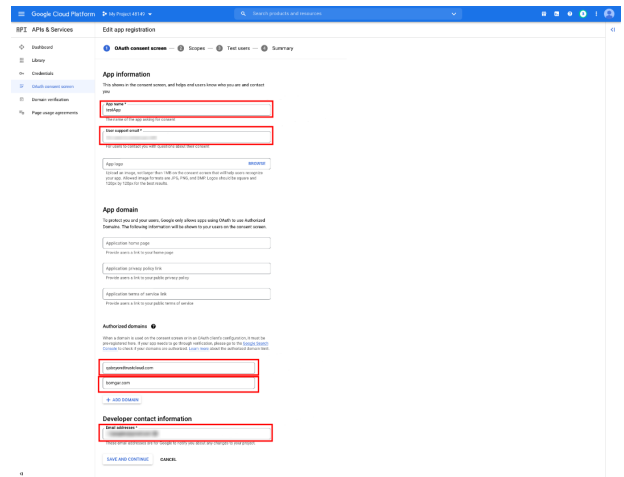
10. The **APIs and services** page appears again. Click **OAuth consent screen** in the left menu.



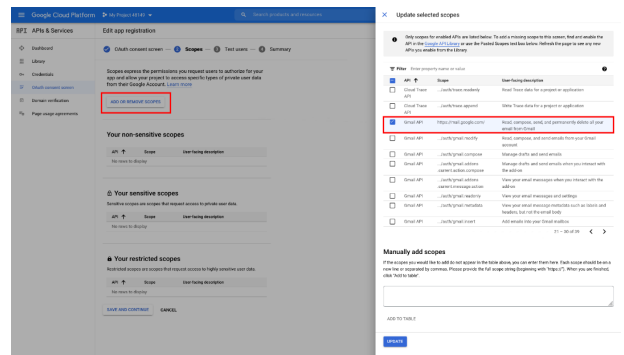
11. Select the **User Type**. Internal allows only users from within the organization, but requires a Google Workspace account.
12. Click **CREATE**.




13. Enter the **App name**.
14. Enter a **User support email** address. This may default to the address you are using to create the project.
15. Enter a logo for the app, if desired. The **App domain** section is also optional.
16. Add the **Authorized domains**. For BeyondTrust test appliances, these are:
 - qabeyondtrustcloud.com
 - bomgar.com
17. Enter the **Developer contact information**. This is the email address you are using to create the project.
18. Click **SAVE AND CONTINUE**.



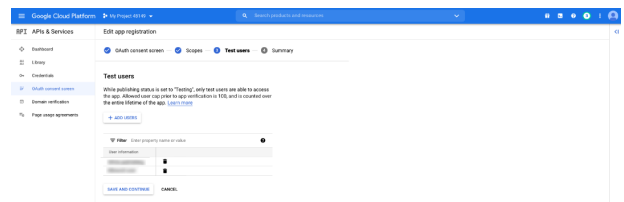
19. Under the **Scopes** tab, click **ADD OR REMOVE SCOPES**. This opens the **Update selected scopes** window.
20. Locate and check the scope **https://mail.google.com/** for the Gmail API.



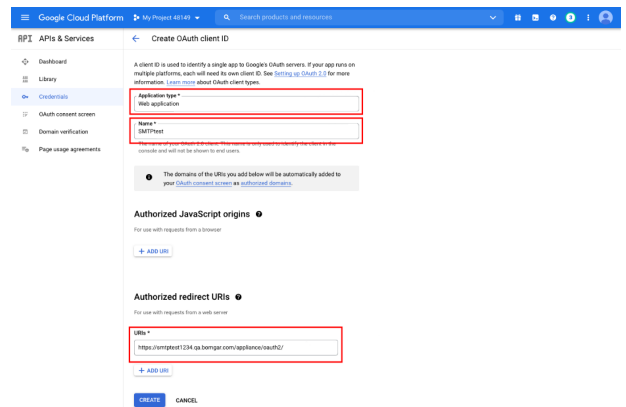
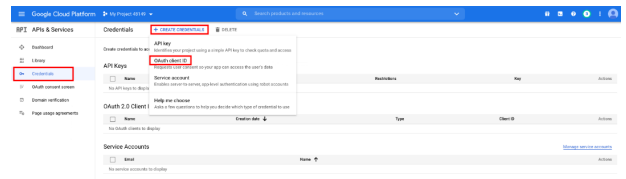
 **Note:** The API does not appear if it has not been enabled.

21. Click **UPDATE**. The **Update selected scopes** window closes.
22. Click **SAVE AND CONTINUE**.

23. Under the **Test users** tab, click **ADD USERS**. This opens the **Add Users** window. Add the users that have access to the application and click **ADD**. Note the limits on test user access and related restrictions.
24. Click **SAVE AND CONTINUE**.
25. Review the Summary, and make any necessary changes or corrections.
26. Click **BACK TO DASHBOARD**.



27. Click **Credentials** in the left menu.
28. Click **CREATE CREDENTIALS** in the top banner and select **OAuth client ID**.
29. On the create credentials page, select **Web application** for the **Application type**. Additional fields appear when this is selected.
30. Enter a name for the application.
31. Scroll down to **Authorized redirect URIs** and click **ADD URI**.
32. Enter the **Authorization Redirect URI** in the form of *https://{URL OF YOUR APPLIANCE}/login/smtp-verification*.
33. Click **CREATE**.
34. A window confirms creation of the OAuth client, and shows the **Client ID** and **Client Secret**. Click to download a JSON file. The file contains information that is needed in the next steps.
35. Click **OK** to return to the APIs and services page.



OAuth client created

The client ID and secret can always be accessed from Credentials in APIs & Services

OAuth access is restricted to the [test users](#) listed on your [OAuth consent screen](#)

Your Client ID
1052081453748-4tuptq4o0vovnakrm672qkaa3kc6s4dn.apps.gcp

Your Client Secret
[REDACTED]

[DOWNLOAD JSON](#)

OK

Provide Credentials to the SMTP Relay Server

1. Within the Remote Support admin interface, navigate to **Management > Email Configuration**.
2. Under **SMTP Authentication Type**, select **OAuth2**, and enter the following information:
 - **Email:** The email address for the SMTP relay.
 - **SMTP OAuth Provider ID:** The **client_id** from the JSON file generated during the Google configuration.
 - **SMTP OAuth Client Secret:** The **client_secret** from the JSON file generated during the Google configuration.

- **SMTP OAuth Scopes:** Enter <https://mail.google.com/>.
 - **SMTP OAuth Authentication Endpoint:** The `auth_uri` from the JSON file generated during the Google configuration.
 - **SMTP OAuth Token Endpoint:** The `token_uri` from the JSON file generated during the Google configuration.
3. Click **Save**.
 4. Now you can verify and connect the provider account. Click **Verify OAuth2 Provider**.



Note: *Ensure you are logged into the provider portal as the email address for the SMTP relay, entered above, in the same browser session. You may need to log out of your personal or admin account.*

Outbound Events: Set Events to Trigger Messages



Management

OUTBOUND EVENTS

HTTP Recipients

You can configure your B Series Appliance to send messages to an HTTP server or to an email address when different events are triggered.

The variables sent by the B Series Appliance arrive as an HTTP POST method and can be accessed by calling the method used to retrieve POST data in your coding language. If the server does not respond with an HTTP 200 to indicate success, the B Series Appliance will re-queue the current event and retry it later.

Add, Edit, Delete

Create a new recipient, modify an existing recipient, or remove an existing recipient.

Add or Edit HTTP Recipient

Enabled

You can uncheck the **Enabled** checkbox to quickly stop the messages for the event handler you set up, as in the event of planned integration testing, for instance.

Name

Create a unique name to help identify this recipient.

URL

Enter the destination URL for this outbound event handler.



Note: BeyondTrust Cloud customers requires the use of URLs beginning with `https`.

Use a CA Certificate

When operating over an HTTPS connection, you must upload the certificate authority's root certificate advertised by the outbound event server.

Send Custom Fields

Choose if custom fields and their values should be sent with the outbound event.

Events to Send

Choose which events should trigger messages to be sent.

Retry Interval

Set how often to retry a failed attempt.

Retry Duration

If an event continues to retry and fail, set how long it should continue to retry before being dropped.

Email Contact

Enter one or more email addresses to which notification should be sent if an error should occur.

Send Email Alert After

Set how long after an error the email should be sent; if the problem is resolved before this time is reached and the event succeeds, no error notification will be sent.

Resend Email Alerts

Set how often error emails should be sent if a failed status should continue.

Email Recipients

Add, Edit, Delete

Create a new recipient, modify an existing recipient, or remove an existing recipient.

Retry Duration

If an event continues to retry and fail, set how long it should continue to retry before being dropped.

Add or Edit Email Recipient

Before you set up your B Series Appliance to send event messages to an email address, verify that your B Series Appliance is configured to work with your SMTP relay server. Go to the **Management > Email Configuration** page to verify settings.

Enabled

Use the **Enabled** checkbox to quickly stop the messages for the event handler you set up, as in the event of planned integration testing, for instance.

Name

Create a unique name to help identify this recipient.

Email

Enter the email address to receive notice of the selected events. You can configure up to ten email addresses, separated by commas.

Require External Key

If this option is checked, emails will be sent only for sessions which have an external key at the time the event occurs.

Events to Send

Choose which events should trigger messages to be sent.

Subject

Customize the subject of this email. You can localize this text for any languages you have enabled.

Body

Customize the body of this email. Use any of the macros listed below this field in the /login page to customize the text for your purposes. You can localize this text for any languages you have enabled.



For more information, please see [Outbound Events Reference Guide -- Variables and Macros](https://www.beyondtrust.com/docs/remote-support/how-to/integrations/outbound-events/index.htm) at <https://www.beyondtrust.com/docs/remote-support/how-to/integrations/outbound-events/index.htm>.

API Configuration: Enable the XML API and Configure Custom Fields



Management

API CONFIGURATION

API Configuration

Enable XML API

Choose to enable the BeyondTrust XML API, allowing you to run reports and issue commands such as starting or transferring sessions from external applications, as well as to automatically back up your software configuration.



Note: Only the **Command, Reporting, and Client Scripting API** calls are enabled/disabled by this setting. Other API calls are configured under **Public Portals**.



For more information, please see the [API Programmer's Guide](http://www.beyondtrust.com/docs/remote-support/how-to/integrations/api) at www.beyondtrust.com/docs/remote-support/how-to/integrations/api.

CLI Client Download

The CLI (Command Line Interface) tool can be downloaded to make it easier to use and configure APIs and automation scripts, and integrate them with your BeyondTrust Remote Support installation. The CLI tool is available for Windows (x64), macOS, and Linux (x64) platforms. Select the appropriate platform and click **Download BTAPE CLI Client**.

The download is a compressed executable file. Extract the file, and save or link it from an executable area (in your PATH).

- For Windows systems: Open the file in a terminal such as Windows Command Prompt or Windows PowerShell.
- For macOS systems: Run the file in the terminal.

The Help information, including options, commands, and variable instructions, displays when the program opens.



For more information on creating APIs with CLI, please see [Use Cases](https://www.beyondtrust.com/docs/remote-support/documents/integrations/rs-api.pdf) examples in the *BeyondTrust Remote Support API Guide*, at <https://www.beyondtrust.com/docs/remote-support/documents/integrations/rs-api.pdf>.

Enable Archive API

Choose to enable the state archive API to download logs of the B Series Appliance's state and of events that occurred on a given date.

API Accounts

An API account stores all of the authentication and authorization settings for the API client. At least one API account is required to use the API, either in conjunction with the Integration Client, with a third-party app, or with your own in-house developed software.

Add, Edit, Delete

Create a new account, modify an existing account, or remove an existing account.

Add or Edit an API Account

Enabled

If checked, this account is allowed to authenticate to the API. When an account is disabled, all OAuth tokens associated with the account are immediately disabled.

Name

Create a unique name to help identify this account.

OAuth Client ID

The OAuth client ID and client secret are used to create OAuth tokens, necessary for authenticating to the API.

The OAuth client ID is a unique ID generated by the B Series Appliance. It cannot be modified. The client ID is considered public information and, therefore, can be shared without compromising the security of the integration.

Comments

Add comments to help identify the purpose of this account.

OAuth Client Secret

The OAuth client secret is generated by the B Series Appliance using a cryptographically secure pseudo-random number generator.



Note: The client secret cannot be modified, but it can be regenerated on the **Edit** page. Regenerating a client secret and then saving the account immediately invalidates any OAuth tokens associated with the account. Any API calls using those tokens will be unable to access the API.

Permissions

Select the areas of the API this account is allowed to use.

Command API

For the command API, choose to deny access, to allow read-only access, or to allow full access.

Reporting API

For the reporting API, check each permission for this account:

- **Allow Access to Support Session Reports and Recordings**
- **Allow Access to Presentation Session Reports and Recordings**
- **Allow Access to License Usage Reports**
- **Allow Access to Archive Reports**
- **Allow Access to Vault Account Activity Reports**
- **Allow Access to Syslog Reports**

Backup API

Check if this account can use the backup API and has vault encryption key access.

Configuration API

Check if this account can use the configuration API and, if so, if it can manage Vault accounts.

Real-Time State API

Check if this account can use the real-time state API.

Endpoint Credential Manager API

Check if this account can use the endpoint credential manager API.

Network Restrictions

List network address prefixes from which this account can authenticate.



Note: API accounts are not restricted by the network prefixes configured on **/login > Management > Security**. They are restricted only by the network prefixes configured for the API account.

Network Address Allow List

Enter the network addresses you wish to add to the allow list.

Support: Contact BeyondTrust Technical Support



Management

SUPPORT

BeyondTrust Support Contact Information

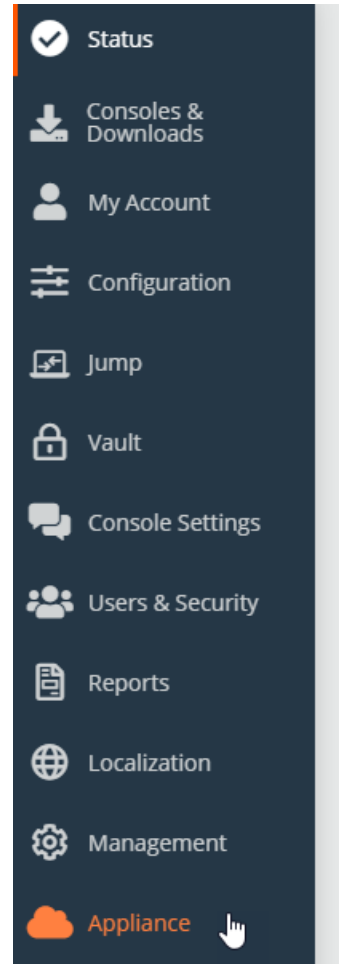
The support page provides contact information should you need to contact a BeyondTrust Technical Support representative.

Advanced Technical Support from BeyondTrust

In the event that a BeyondTrust Technical Support representative should need access to your B Series Appliance, they will provide you with support, access, and override codes to enter on this page to create an appliance-initiated, fully encrypted support tunnel back to BeyondTrust for quick resolution of complex issues.

Remote Support Cloud Appliance

BeyondTrust Cloud customers access B Series Appliance settings from the **Appliance** tab of the /login interface. Clicking the **/login > Appliance** tab opens a new browser tab, where you have access to a select set of B Series Appliance features.



Status > Basics: View Cloud Appliance Details



The **Basics** page gives you information about your BeyondTrust Appliance B Series and allows you to monitor your system.

In the Appliance Statistics section, you can learn important information about your B Series Appliance, including the model number and serial number. You can also set your local time to any valid global time zone. The system time will always be displayed in UTC.

Appliance Statistics	
Appliance Model	Virtual Appliance (br v2)
Host Hypervisor	VMware
Serial Number	427F12022084D08E-ES0C8
System GUID	af62c4859-4a40578a3dca073a12332
Base Software Version	6.1.1 (44144a72d5cca2a0b3302c608f923603c2b0787e121)
Service Pack	31
System Architecture	x64
Firmware Version	0
Firmware Build Date	Fri, Jan 29, 2021 02:32:49 UTC
System Up-Time	21 days, 0:26
Processes	0/20, 0/18, 0/18 (0)
System Time	Thu, Oct 14, 2021, 9:27:04 PM UTC
Time Zone	UTC

Storage > Encryption: Encrypt Session Data


[STATUS](#) | [STORAGE](#) | [SECURITY](#) | [UPDATES](#) | [SUPPORT](#)

ENCRYPTION

The **Encryption** section allows you to encrypt session data stored on your BeyondTrust Appliance B Series. When first encrypting your data, you are limited to 4GB or less of data; however, after the initial encryption, this 4GB limit no longer applies.

If you have not already created a secret store, go to **Security > Secret Store** to add one.

 For more information, please see "[Security > Secret Store: Store and Access Secrets on the Cloud Appliance](#)" on page 283.

 **Note:** If you have more than 4GB of data to initially encrypt, please contact BeyondTrust Technical Support at www.beyondtrust.com/support.

Storage :: Encryption

Storage Encryption Status: **Not Encrypted**

[Encrypt](#)

The storage encryption key will be stored locally. [Click here](#) to add a secret store.

Security > Certificates: Create and Manage TLS Certificates

STATUS	STORAGE	SECURITY	UPDATES	SUPPORT
CERTIFICATES	TLS CONFIGURATION	APPLIANCE ADMINISTRATION	EMAIL CONFIGURATION	SECRET STORE

Manage TLS certificates, create certificate requests, and import certificates signed by a certificate authority.

Certificate Installation

The BeyondTrust Cloud Appliance comes with a pre-installed certificate signed by a certificate authority (CA). This certificate validates the *.beyondtrustcloud.com domain. If you wish to change the fully qualified domain name (FQDN) of your B Series Appliance, you must install a CA-signed certificate which validates your new FQDN. To do this, you must create a certificate signing request (CSR) from the BeyondTrust Cloud Appliance as described below, or use Let's Encrypt to obtain a certificate. If you choose a custom hostname for your B Series Appliance, you may use the built-in Let's Encrypt functionality for your SSL certificate.



For more information on certificates, see [SSL Certificates and BeyondTrust Remote Support](https://www.beyondtrust.com/docs/remote-support/how-to/sslcertificates) at www.beyondtrust.com/docs/remote-support/how-to/sslcertificates.

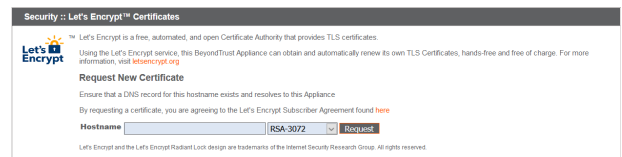
Let's Encrypt

Let's Encrypt issues signed certificates that are valid for 90 days at a time, and can automatically renew themselves indefinitely. In order to request or renew a Let's Encrypt certificate, you must meet the following requirements:

- The DNS for the hostname you are requesting must resolve to the B Series Appliance.
- The B Series Appliance must be able to reach Let's Encrypt on TCP 443.
- Let's Encrypt must be able to reach the B Series Appliance on TCP 80.

To implement a Let's Encrypt certificate, in the **Security :: Let's Encrypt™ Certificates** section complete the following:

- **Hostname:** Enter the fully qualified domain name (FQDN) of the B Series Appliance.
- Use the dropdown to choose the certificate key type.
- Click **Request**.



The screenshot shows the 'Security :: Let's Encrypt™ Certificates' page. It includes a 'Request New Certificate' section with a text input for 'Hostname' and a dropdown menu for 'Certificate Key Type' (currently set to 'RSA3072'). A 'Request' button is visible next to the dropdown. Below the form, there is a small disclaimer: 'Let's Encrypt and the Let's Encrypt/Padlock design are trademarks of the Internet Security Research Group. All rights reserved.'

As long as the above requirements are met, you will be provided a certificate that will automatically renew every 90 days once the validity check with Let's Encrypt has completed.



Note: The B Series Appliance starts the certificate renewal process 30 days before the certificate is due to expire and requires the same process as the original request process does. If it has been unsuccessful 25 days prior to expiry, the B Series Appliance sends daily admin email alerts (if email notifications are enabled). The status will show the certificate in an error state.

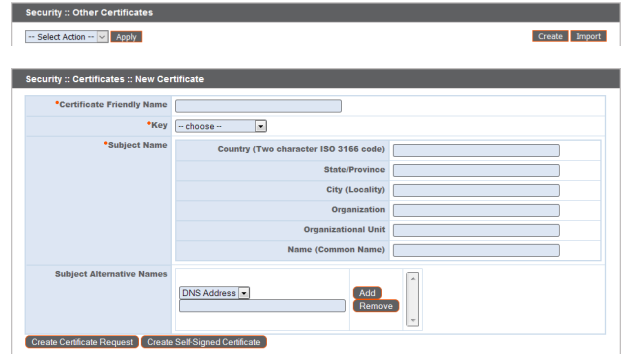


For more information, please see letsencrypt.org.

Other CA-Issued Certificates

To create a certificate request:

- Locate the **Security :: Other Certificates** section and click **Create**.
- In **Certificate Friendly Name**, enter a name you will use to identify this certificate.
- From the **Key** dropdown, choose the **Existing Key** of your *.beyondtrustcloud.com certificate or select a new key type.
- Enter the remaining information pertaining to your organization.
- In the **Name (Common Name)** field, enter a descriptive title for your BeyondTrust site.
- In the **Subject Alternative Names** section, enter your BeyondTrust site hostname and click **Add**. Add a SAN for each DNS name or IP address to be protected by this SSL certificate.




Note: DNS addresses can be entered as fully qualified domain names, such as *access.example.com*, or as wildcard domain names, such as **.example.com*. A wildcard domain name covers multiple subdomains, such as *access.example.com*, and so forth.

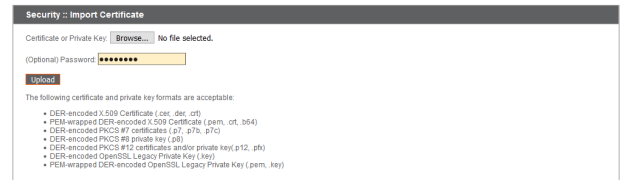
Click **Create Certificate Request**.

To use a CA-signed certificate, contact a certificate authority of your choice and purchase a new certificate from them using the CSR you created in BeyondTrust. Once the purchase is complete, the CA will send you one or more new certificate files, each of which you must install on the B Series Appliance.

To upload your new certificate files, click **Import**. Browse to the first file and upload it. Repeat this for each certificate sent by your CA. Often, a CA will not send their root certificate, which must be installed on your B Series Appliance. If the root is missing, a warning appears beneath your new certificate: "The certificate chain appears to be missing one or more certificate authorities and does not appear to terminate in a self-signed certificate".

To download the root certificate for your B Series Appliance certificate, check the information sent from your CA for a link to the appropriate root. If there is none, contact the CA to obtain it. If this is impractical, search their website for their root certificate store. This contains all the root certificates of the CA, and all major CAs publish their root store online.

Usually, the easiest way to find the correct root for your certificate is to open the certificate file on your local machine and inspect its "Certification Path" or "Certificate Hierarchy". The root of this hierarchy or path is typically shown at the top of the tree. Locate this root certificate on the root store of your CA's online root store. Once done, download it from the CA's root store and import it to your B Series Appliance as described above.




Certificates

View a table of SSL certificates available on your B Series Appliance.

Security :: Other Certificates						
-- Select Action --		Apply		Create		Import
	Friendly Name	Issued To	Issued By	Expiration	Alternative Name(s)	Private Key? Default
<input type="checkbox"/>	example.com 1 Warning(s)	example.com	DigiCert SHA2 High Assurance Server CA	2019-09-18 12:00:00 GMT	dNSName - example.com dNSName - example.com	Yes <input type="radio"/>
<input type="checkbox"/>	Bomgar Appliance 2 Warning(s)	Bomgar Appliance	Bomgar Appliance	2018-10-25 13:50:00 GMT	No Supported Names	Yes <input type="radio"/>
<input type="checkbox"/>	DigiCert SHA2 High Assurance Server CA	DigiCert SHA2 High Assurance Server CA	DigiCert High Assurance EV Root CA	2028-10-22 12:00:00 GMT	No Supported Names	No <input type="radio"/>

For connections that do not supply a Server Name Indication (SNI) or supply an incorrect SNI, select a default SSL certificate from the list to provide for these connections by clicking the button under the **Default** column. The default SSL certificate cannot be a self-signed certificate nor the default B Series Appliance certificate provided for initial installation.

 **Note:** To learn more about SNI, please see [Server Name Indication](https://cio.gov/sni/) at <https://cio.gov/sni/>.

Click a certificate name to view details and manage its certificate chain.

Security :: Certificates :: Edit Certificate Configuration

Certificate Friendly Name: support.example.com

Subject Name:

- CN=qa.bomgar.com
- OU=Remote Support
- O=Bomgar Corporation
- L=Ridgeland
- ST=Mississippi
- C=US

Issuer Name:

- CN=DigiCert SHA2 High Assurance Server CA
- OU=www.digicert.com
- O=DigiCert Inc
- C=US

Serial Number: 15479704919208578551449670942311195506

Signature Type: sha256WithRSAEncryption

Not Valid Before: 2019-01-06 00:00:00 GMT

Not Valid After: 2019-03-27 12:00:00 GMT

Public Key: RSA (2048 Bits)

Private Key: Available

Subject Alternative Names:

- dNSName - support.example.com
- dNSName - businesscompany.example.org

Authority Info Access:

- http://cacerts.digicert.com/DigiCertSHA2HighAssuranceServerCA.crt

Certificate Chain:

- Automatic Current Chain:
 - CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US
 - CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US
- Manually Specified
 - Browse... No file selected.

Only certificate chains in PEM-encoded format are accepted.

Save Configuration

To export one or more certificates, check the box for each desired certificate, select **Export** from the dropdown at the top of the table, and then click **Apply**.

Security :: Other Certificates

-- Select Action -- Apply

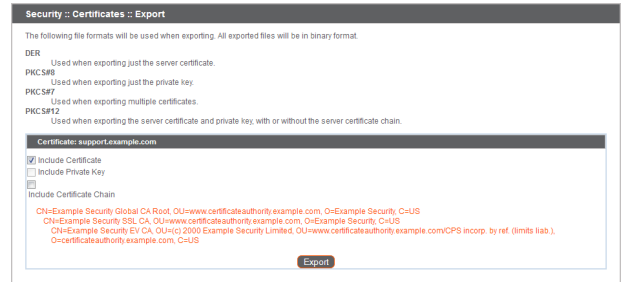
-- Select Action --

Export

Delete

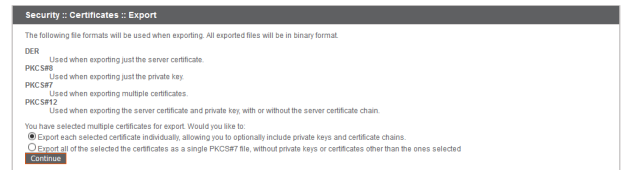
Bomgar Appliance

If you are exporting only one certificate, you immediately can choose to include the certificate and/or the certificate chain if available. Click **Export** to start the download.

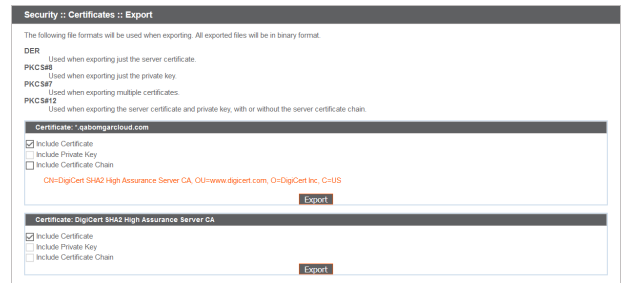


If you are exporting multiple certificates, you will have the option to export each certificate individually or in a single PKCS#7 file.


When selecting to export multiple certificates as one file, click **Continue** to start the download. With this option, only the actual certificate files will be exported, without any certificate chains.

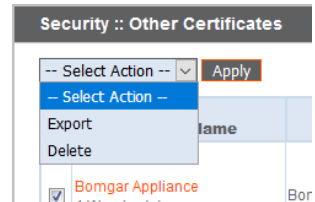


To include certificate chains in the export, select individual export and click **Continue** to view all selected certificates. For each listing, choose to include the certificate and/or the certificate chain if available. Click **Export** to start the download.



To delete one or more certificates, check the box for each desired certificate, select **Delete** from the dropdown at the top of the table, and then click **Apply**.

 **Note:** Under normal circumstances, a certificate should never be deleted unless it has already been successfully replaced by a working substitute.



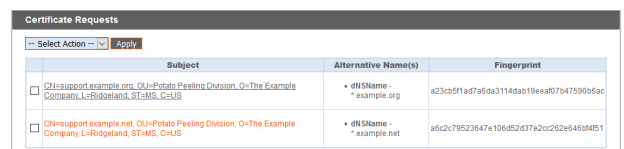
To confirm accuracy, review the certificates you wish to delete, and then click **Delete**.



Friendly Name	Issued To	Issued By	Expiration	Alternative Name(s)	Private Key?
*qa.bomgar.com	*qa.bomgar.com	DigiCert SHA2 High Assurance Server CA	2021-04-30 12:00:00 GMT	DN:Name = *qa.bomgar.com DN:Name = qa.bomgar.com	Yes

Certificate Requests

View a table of pending requests for third-party-signed certificates. Click a certificate request name to view details.



Subject	Alternative Name(s)	Fingerprint
DN:Support example.org, OU=Potato Peeling Division, O=The Example Company, L=Ridgeland, ST=MS, C=US	• DN:Name = *example.org	a23cb5f1a77a5d3114da819ea07b475006f5c
DN:Support example.net, OU=Potato Peeling Division, O=The Example Company, L=Ridgeland, ST=MS, C=US	• DN:Name = *example.net	a6c2c79523647e106d52d3762cc262e46d6f51

Create a Custom Hostname for Your BeyondTrust Cloud Site

STATUS	STORAGE	SECURITY	UPDATES	SUPPORT
CERTIFICATES	TLS CONFIGURATION	APPLIANCE ADMINISTRATION	EMAIL CONFIGURATION	SECRET STORE

To configure your BeyondTrust Cloud Appliance with a custom URL that matches your domain name, please follow the steps below.

1. Register your custom CNAME in DNS (internal and external web host, if necessary), and point it to the BeyondTrust-supplied URL of your Cloud Appliance.
2. Once the site is online, create a certificate signing request (CSR) for submission to your certificate authority.



Note: If you are using an existing wildcard SSL certificate, you can skip to step 5.

- To create the CSR, log in to the /login web interface of your BeyondTrust Cloud Appliance and go to **Appliance > Security > Certificates**.
 - In the **Security :: Certificate Installation** section, click **Create**, and then fill out the CSR form.
 - **Certificate Friendly Name:** Enter your requested CNAME URL.
 - **Key:** Select a key from the dropdown list. Verify with your certificate authority which key strengths they support. Larger key sizes normally require more processing overhead and may not be supported by older systems. However, smaller key sizes are likely to become obsolete or insecure sooner than larger ones.
 - **Country:** Enter your organization's two-character Country code. If you are unsure of your country code, please visit [ISO 3166 country codes](https://www.iso.org/iso-3166-country-codes.html) at www.iso.org/iso-3166-country-codes.html
 - **State/Province:** Enter your jurisdiction name, if applicable. Enter the full name, as some certificate authorities do not accept an abbreviation.
 - **City (Locality):** Enter your city or town.
 - **Organization:** Enter the name of your company.
 - **Organizational Unit:** Enter the name of the group or department within the company than manages the certificate and/or the BeyondTrust deployment for the organization.
 - **Name (Common Name):** Enter your requested CNAME URL.
 - **Subject Alternative Name:** Enter your requested CNAME URL and then click **Add**.
 - Click **Create Certificate Request** and wait for the page to refresh.
3. Export your new CSR.
 - Once back at the **Certificates** page, scroll down to the **Security :: Certificate Requests** section.
 - Click the subject of your new certificate request.
 - Select and copy the **Request Data**, including ----- **BEGIN CERTIFICATE REQUEST** ----- and ----- **END CERTIFICATE REQUEST** -----.
 - Copy the text to a text editor, and do not adjust formatting.
 - Save the document to your workstation as a plain text document such as **BeyondTrustCertRequest.txt**.
 4. Obtain your SSL certificate from a certificate authority.
 - Log in to your certificate authority's web site to obtain your SSL certificate.
 - When asked to submit your CSR, paste the entire text of your BeyondTrust CSR into their site.
 - If required to select a web server type, submit that the server is **Apache-compatible**. If given more than one Apache type as options, select **Apache/ModSSL**.

5. Import your entire SSL certificate chain to your BeyondTrust Cloud Appliance.
 - Log in to your /login web interface and navigate to **Appliance > Security > Certificates**.
 - Click **Import**.
 - Browse to each of your SSL certificate files, one at a time (unzipped).
 - Click **Install Certificate**, if prompted.



Note: If you are importing an SSL certificate from another server, you must import its associated private key file, as well.

6. Send your SSL certificate chain to BeyondTrust Support. BeyondTrust needs this data to rebuild your site software.
 - Log in to your /login web interface and navigate to **Appliance > Security > Certificates**.
 - Find the certificate that is **Issued To** the new CNAME of your Cloud Appliance.
 - Check the box on the left of this particular certificate.
 - Click the dropdown above, select **Export**, and then click **Apply**.
 - On the next page, uncheck the **Private Key** box. Make sure to check the boxes entitled **Include certificate** and **Include certificate chain**.
 - Click **Export** once more.
 - Send an email to BeyondTrust Support with the downloaded SSL certificate file attached.



Note: If you are unable to check the box **Include certificate chain**, then you may be missing one or more certificate segments. Please contact BeyondTrust Support for assistance.



IMPORTANT!

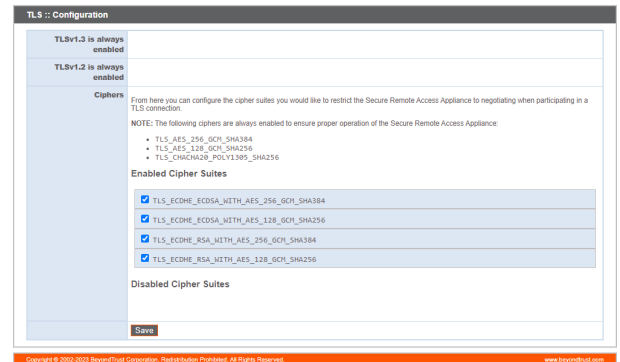
DO NOT send your private key to BeyondTrust! Private key files usually have a **.p12** extension.

7. BeyondTrust Support uses your new SSL certificate data to build a custom software update. When this is ready, BeyondTrust sends you an email with installation instructions.
8. Assign an IP address to the SSL certificate.
 - a. After you apply the custom software update, log in to your /login interface and navigate to **Appliance > Security > Certificates**.
 - b. Select the **Default** radio button next to your new certificate.
9. The custom CNAME accesses your BeyondTrust Cloud site.

Security > TLS Configuration: Choose TLS Ciphers



Select which Cipher suites should be enabled or disabled on your B Series Appliance. Drag and drop Cipher suites to change the order of preference. Note that changes to Cipher suites do not take effect until the **Save** button is clicked.



Security > Appliance Administration: Set Syslog over TLS

STATUS | STORAGE | SECURITY | UPDATES | SUPPORT | CERTIFICATES | TLS CONFIGURATION | **APPLIANCE ADMINISTRATION** | EMAIL CONFIGURATION | SECRET STORE

You can send syslog messages over an encrypted TLS connection to up to three syslog servers.

Enter the hostname or IP address of a syslog host server receiving system messages from this Cloud Appliance using the **local0** syslog facility. If needed, enter a custom port number. You may enter up to three comma-separated servers per field.



Note: If a custom port number is not entered, Syslog over TLS defaults to TCP port 6514.



Note: While the Message Format appears as a dropdown, the only available selection is "Syslog over TLS (RFC 5425)".

Next, click **Choose File** to locate and upload a new trusted certificate. When finished, click **Submit**.



IMPORTANT!

You must upload a new certificate whenever your current certificate expires. Otherwise you may experience a disruption in the syslog events being captured.

Security > Email Configuration: Configure the Cloud Appliance to Send Email Alerts

STATUS	STORAGE	SECURITY	UPDATES	SUPPORT
CERTIFICATES	TLS CONFIGURATION	APPLIANCE ADMINISTRATION	EMAIL CONFIGURATION	SECRET STORE

Your B Series Appliance can send you automatic email notifications. Emails are sent for the following events:

- **Syslog Server has been Changed:** A user on /appliance has changed the syslog server parameter.
- **RAID Event:** One or more RAID logical drives is not in Optimum state (Degraded or Partially Degraded).
- **SSL Certificate Expiration Notice:** An in-use SSL certificate (include either end-entity certificates or any CA certificate in the chain) expires in 90 days or less.

Configure via SMTP



Note: This method does not work for some email services. Please see "[Configure via OAuth2 for Microsoft Azure AD](#)" on page 275 or "[Configure via OAuth2 for Google](#)" on page 278 for alternate configurations.

Security :: SMTP Relay Server

Send From Email Address

Enter a single email address. Email alerts from this Secure Remote Access Appliance will be sent with this as the "From" address.

SMTP Relay Server

Host

Enter an open relay SMTP server, or an SMTP server that will accept email to the Admin Contact addresses below

Port

The SMTP port is typically 25 or 587 for Encryption types: "None", "STARTTLS"; and 465 for Encryption type: "TLS".

Encryption If your SMTP Server supports TLS Encryption, select the desired type

None
 TLS
 STARTTLS

Trusted Certificate

Upload a new Trusted Certificate

No file selected.

If necessary, upload the trusted root certificate (in PEM format) presented by your SMTP server.

Ignore TLS certificate errors.

Only select this if you cannot provide the Trusted Certificate above. This could potentially make you vulnerable to TLS man-in-the-middle attacks.

SMTP Authentication If your SMTP Server requires authentication, enter a username and password

Username

Password

NOTE: Leave blank to keep the current password.

After entering the email addresses for the administrator contacts, save your settings and send a test email to ensure everything works correctly.

Security :: Admin Contact

Admin Contact Email

Enter email addresses, one per line, to be notified of important System events

Send a test email when the settings are saved.

Configure via OAuth2 for Microsoft Azure AD

Configuration requires changing settings on the BeyondTrust appliance and the Microsoft 365 subscription with Azure AD.

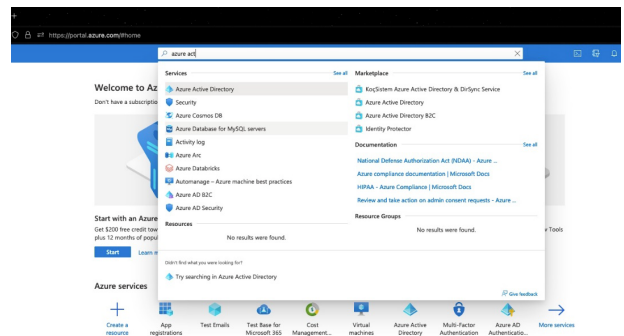
Start by changing settings on the BeyondTrust appliance:

1. Go to **Appliance**, click the **Security** tab and click **Email Configuration**.
2. Change the **Authentication Method** to OAuth2
3. Note the **Authorization Redirect URI**. It is required later.

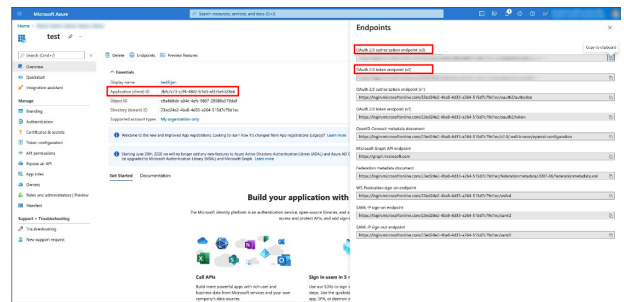
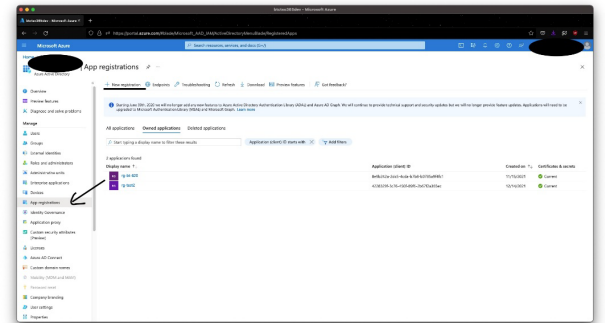
Before starting configuration on the Azure Active Directory, an Azure/Office 365 Administrator must enable Authenticated SMTP for each account on Exchange online. To do this, go to **Office 365 Admin Portal (admin.microsoft.com) > Active Users > Mail > Manage Email apps** and check **Authenticated SMTP**.

Once **Authenticated SMTP** is enabled, perform the following steps in the Azure console:

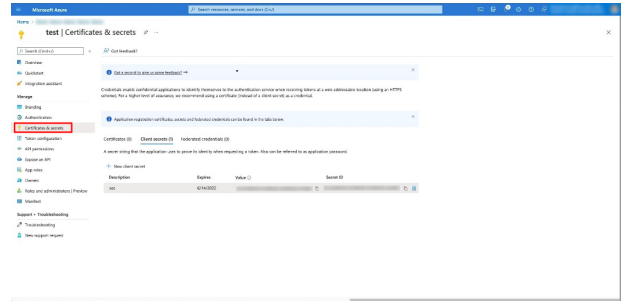
4. Log in to your Azure console (portal.azure.com).
5. Go to **Azure Active Directory**.



6. Go to **App registrations** and select **New registration**.
7. Enter a name, such as Appliance-OAuth2.
8. Select the types of account you want to be able to log in to the application through OAuth2. Select **Single Tenant** for internal only.
9. Enter the **Redirect URI**. This is the **Authorization Redirect URI** obtained from the BeyondTrust appliance at the start of this process.
10. Click **Register**.
11. On the **Overview Page** (selected from the left menu), note the **Application (client) ID**. It is required later.
12. Click **Endpoints** (above the **Application (client) ID**).
13. Note the **OAuth2.0 authorization endpoint (v2)** URI and the **OAuth token endpoint (v2)** URI. These are required later.




14. On the **Certificates & secrets** page (selected from the left menu), note the **Client secret**. It is required later. If you do not have a **Client secret**, click **New client secret** to create one.




The remaining steps are done on the BeyondTrust appliance.

15. Go to **Appliance**, click the **Security** tab, and click **Email Configuration**.
16. Enter the following information noted earlier:
 - **Authorization Endpoint**
 - **Token Endpoint**
 - **Client ID**
 - **Client Secret**
17. Enter the email address for this service as the **Send from Email Address** and the **User email**.

 **Note:** These addresses must match and be a valid account for Azure. If you have Anonymous Email (Send Email as Anyone) enabled for the Azure Tenant, you can add anything in the send email field. If not, use the username of the application owner and the Allowed Users.

18. Enter data for the **Host**, **Encryption**, and **Port** fields.
 - **Host:** smtp.office365.com
 - **Encryption:** STARTTLS
 - **Port:** 587

 **Note:** Default data for Azure is shown, but your installation may use a different host or encryption method. The port is applicable for STARTTLS, but other encryption methods may use a different port.

19. Upload the SMTP server's Root CA Certificate, if required. This step is not required for most large email vendors.
20. Enter the following for **Scopes**: https://outlook.office.com/SMTP.Send offline_access
21. Click **Save Changes**.
22. Click **Authorize**. At the sign in page that appears, accept the permissions request. The mail setting page reloads, and the authorization button is replaced by an authorized message.
23. To test the configuration:
 - Add an **Admin Contact Email**.
 - Check **Send a test email**.
 - Click **Save Changes**.

Configure via OAuth2 for Google

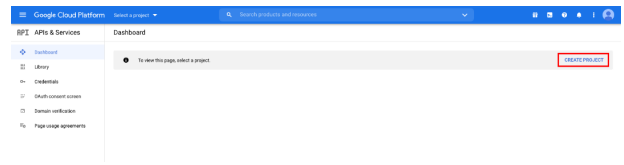
Configuration requires changing settings on the BeyondTrust appliance and the Google Cloud Platform.

Start by changing settings on the BeyondTrust appliance:

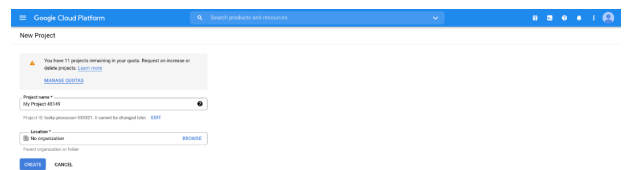
1. Go to **Appliance**, click the **Security** tab and click **Email Configuration**.
2. Change the **Authentication Method** to OAuth2
3. Note the **Authorization Redirect URI**. It is required later.

Now log in to your Google Cloud Platform console (Google Dev Console) (console.cloud.google.com). Use the correct gmail account, as only the owner of the project is able to work with the project. If you do not already have a paid account, you may choose to purchase an account by clicking **Activate** in the top banner. BeyondTrust cannot provide assistance with purchasing an account. Click **Learn More** in the top banner for information regarding the limitations of free accounts.

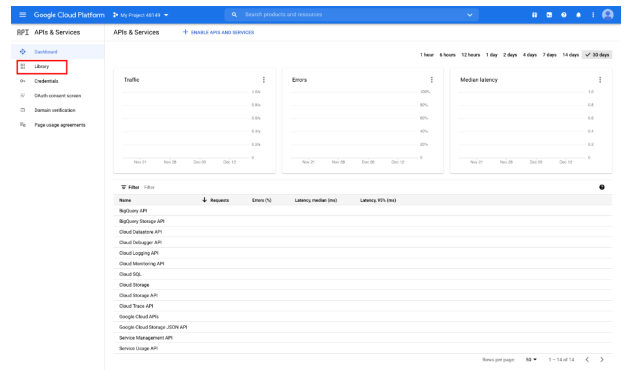
4. Click **CREATE PROJECT**. You can also use an existing project.



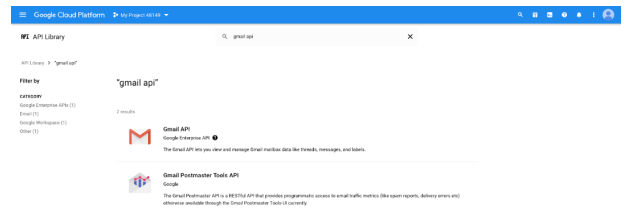
5. Accept the default **Project Name** or enter a name.
6. Accept the default **Location** or select a folder from those available for your organization.
7. Click **CREATE**.



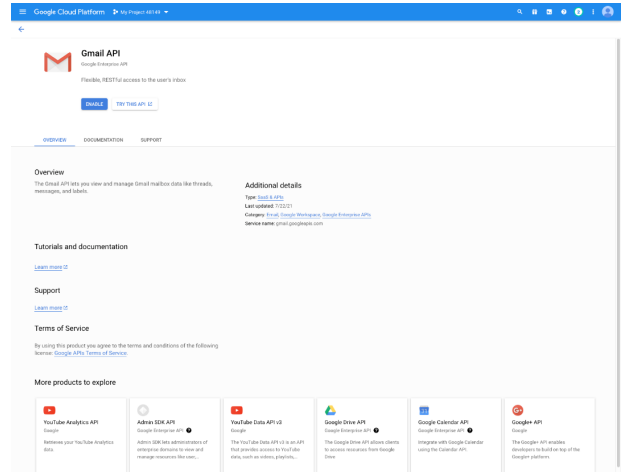
8. The **APIs and services** page appears. Click **Library** in the left menu.



9. Search or browse for the **Gmail API** in the library, and click it.

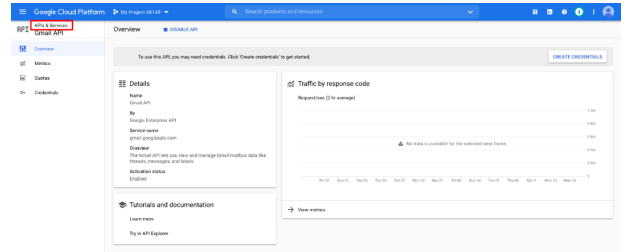


10. The **Gmail API** appears on its own page. Click **ENABLE**.



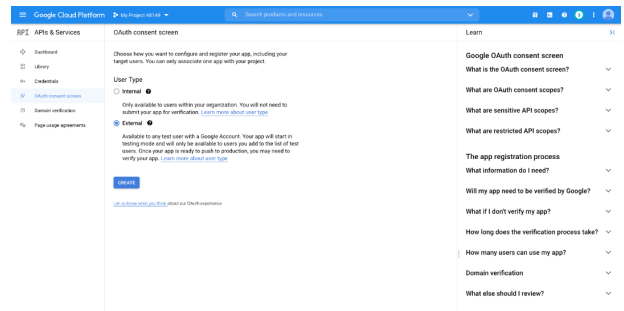
11. The **Gmail API Overview** page appears. Click **APIs & services** in the upper left.

12. The **APIs and services** page appears again. Click **OAuth consent screen** in the left menu.



13. Select the **User Type**. Internal allows only users from within the organization, but requires a Google Workspace account.

14. Click **CREATE**.



15. Enter the **App name**.

16. Enter a **User support email** address. This may default to the address you are using to create the project.

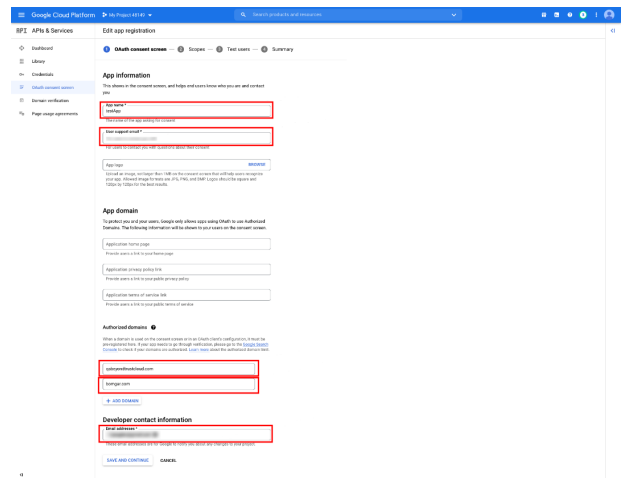
17. Enter a logo for the app, if desired. The **App domain** section is also optional.

18. Add the **Authorized domains**. For BeyondTrust test appliances, these are:


- qabeyondtrustcloud.com
- bomgar.com

19. Enter the **Developer contact information**. This is the email address you are using to create the project.

20. Click **SAVE AND CONTINUE**.

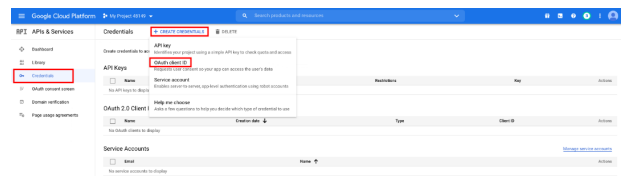
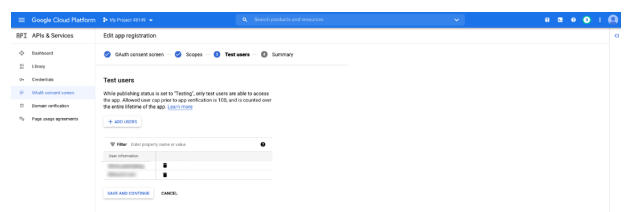
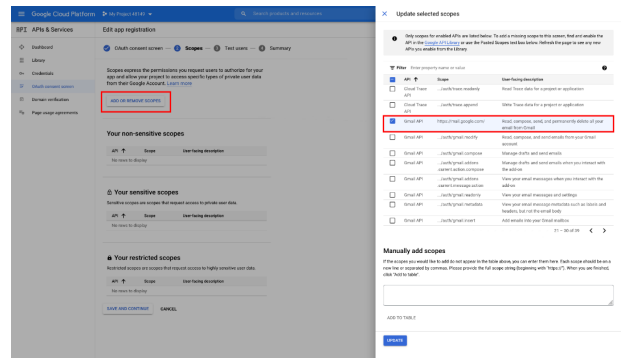


21. Under the **Scopes** tab, click **ADD OR REMOVE SCOPES**. This opens the **Update selected scopes** window.
22. Locate and check the scope **https://mail.google.com/** for the Gmail API.

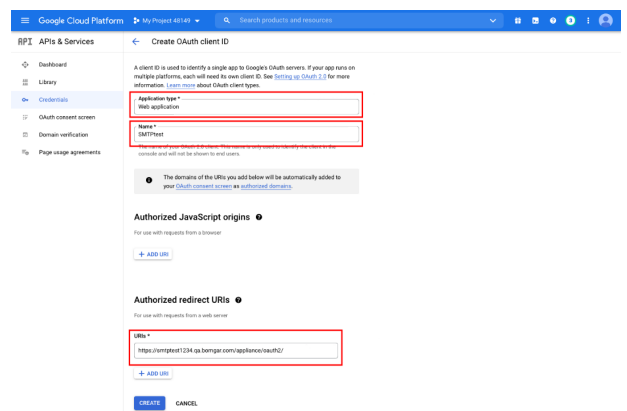
 **Note:** The API does not appear if it has not been enabled.

23. Click **UPDATE**. The **Update selected scopes** window closes.
24. Click **SAVE AND CONTINUE**.

25. Under the **Test users** tab, click **ADD USERS**. This opens the **Add Users** window. Add the users that have access to the application and click **ADD**. Note the limits on test user access and related restrictions.
26. Click **SAVE AND CONTINUE**.
27. Review the Summary, and make any necessary changes or corrections.
28. Click **BACK TO DASHBOARD**.
29. Click **Credentials** in the left menu.
30. Click **CREATE CREDENTIALS** in the top banner and select **OAuth client ID**.



31. On the create credentials page, select **Web application** for the **Application type**. Additional fields appear when this is selected.
32. Enter a name for the application.
33. Scroll down to **Authorized redirect URIs** and click **ADD URI**.
34. Enter the **Authorization Redirect URI** obtained from the BeyondTrust appliance at the start of this process.
35. Click **CREATE**.



36. A window confirms creation of the OAuth client, and shows the **Client ID** and **Client Secret**. Click to download a JSON file. The file contains information that is needed in the next steps.
37. Click **OK** to return to the APIs and services page.


OAuth client created

The client ID and secret can always be accessed from Credentials in APIs & Services

i OAuth access is restricted to the [test users](#) listed on your [OAuth consent screen](#)

Your Client ID
 1052081453748-4tuptq4o0ovnakrm67f2qkaa3kc6s4dn.apps.g...


Your Client Secret
 [REDACTED]

 **DOWNLOAD JSON**

[OK](#)

The remaining steps are done on the BeyondTrust appliance.

38. Go to **Appliance**, click the **Security** tab and click **Email Configuration**.
39. Enter the following information, found in the downloaded JSON file:
 - **Authorization Endpoint**
 - **Token Endpoint**
 - **Client ID**
 - **Client Secret**
40. Enter any email address for this service as the **Send from Email Address**.
41. Enter the **User email**. This must be an email address entered as a **Test user** with access to the application, when you completed the OAuth consent screens.
42. Enter data for the **Host**, **Encryption**, and **Port** fields.
 - **Host:** smtp.gmail.com
 - **Encryption:** TLS
 - **Port:** 465

 **Note:** Default data for Google is shown, but your installation may use a different host or encryption method. The port is applicable for TLS, but other encryption methods may use a different port.

43. Enter your TLS certificate if one is provided by Google. If not, check **Ignore TLS certificate errors**.
44. Enter the following for **Scopes**: https://mail.google.com
45. Click **Save Changes**.
46. Click **Authorize**. After the sign in page that appears, you may receive the warning **Google has not verified this message**, if you have not published the application. The consent page reloads, and the authorization button is replaced by an authorized message.

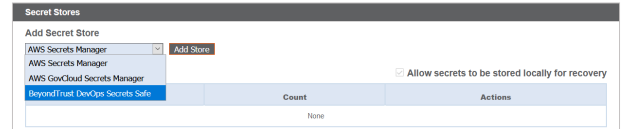
47. To test the configuration:

- Add an **Admin Contact Email**.
- Check **Send a test email**.
- Click **Save Changes**.

Security > Secret Store: Store and Access Secrets on the Cloud Appliance

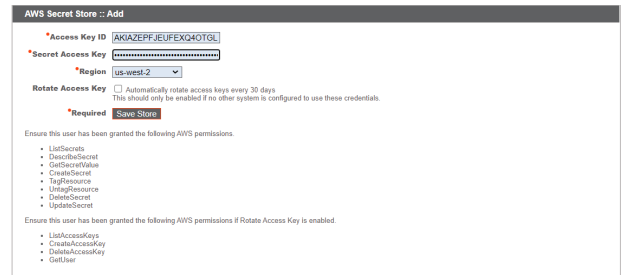
STATUS	STORAGE	SECURITY	UPDATES	SUPPORT
CERTIFICATES	TLS CONFIGURATION	APPLIANCE ADMINISTRATION	EMAIL CONFIGURATION	SECRET STORE

Create and manage secret keys stored in AWS to securely store encryption keys and site data. To add a secret store, select the store from the dropdown, and then click **Add Store**. Provide and save the information for the store as shown in the steps below.



Add AWS Secret Store

1. Provide the **Access Key ID**, **Secret Access Key**, and **Region**.
2. Check the **Rotate Access Key** box only if you are not using any of the same IAM user's credentials in any other system.
3. Click **Save Store**.
4. It is also necessary for any firewall to allow outbound traffic to the IP addresses associated with the region endpoint used for the secret store.



Note: IP addresses may change. Please see the current list of IP addresses at [AWS IP address ranges at https://docs.aws.amazon.com/general/latest/gr/aws-ip-ranges.html](https://docs.aws.amazon.com/general/latest/gr/aws-ip-ranges.html).



For the list of endpoints, please see [AWS Secrets Manager endpoints and quotas at https://docs.aws.amazon.com/general/latest/gr/asm.html](https://docs.aws.amazon.com/general/latest/gr/asm.html).



Note: For added security, configure your AWS Identity and Access Management (IAM) Policy to limit access to resources matching **BeyondTrust-*** on the following permissions:

- DescribeSecret
- GetSecretValue
- TagResource
- UntagResource
- CreateSecret
- DeleteSecret
- UpdateSecret

For more information on managing AWS IAM Policies, see [Managing IAM Policies at https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_manage.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_manage.html).



Note: *If you delete the last remote store, a message displays indicating secrets will be moved locally.*

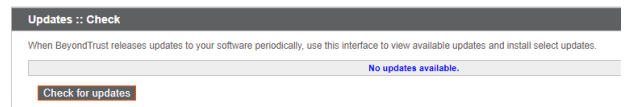
Updates: Check for Update Availability and Install Software in BeyondTrust Cloud



It is good practice to subscribe to the changelog for notifications of new releases. You can check for new releases at any time by clicking **Check for Updates**.

If multiple software packages have been built for your B Series Appliance, each one is listed separately in the list of available updates. Your new software is automatically downloaded and installed when you click the appropriate **Install This Update** button.

If no update packages or patches are available for your B Series Appliance, a message stating *No updates available* is displayed. If an update is available but an error occurred when distributing the update to your B Series Appliance, an additional message is displayed, such as, *An error occurred building your update. Please visit www.beyondtrust.com/support for more information.*



IMPORTANT!

Please be prepared to install software updates directly after download. Once an update has been downloaded, it no longer appears in your list of available updates. Should you need to re-download a software update, contact BeyondTrust Technical Support.

When the BeyondTrust End User License Agreement (EULA) screen appears, fill out the required contact information and click the **Agree-Begin Download** button to accept the EULA and continue the installation.

Note that if you chose to decline the EULA, an error message displays and you are not able to update your BeyondTrust software.

If you have any issues updating after accepting the EULA, please contact BeyondTrust Technical Support at www.beyondtrust.com/support.

During the installation process, the **Updates** page displays a progress bar to notify you of the overall update progress. Updates made here automatically update all sites and licenses on your B Series Appliance.

If you are installing a software update, logged-in representatives will temporarily lose connections to any support sessions and the representative console; therefore, schedule software updates for non-peak hours. However, if your update package contains only additional licenses, you can install the update without interrupting representative connections.



Find current information about the latest BeyondTrust updates and subscribe at <https://www.beyondtrust.com/docs/release-notes/index.htm>.

Please wait while the software is updating.

Note that installation progress may stop for long periods of time while data is being backed up.

You will be automatically redirected when the update is finished.

Do not refresh this page.

Do not reboot the appliance.

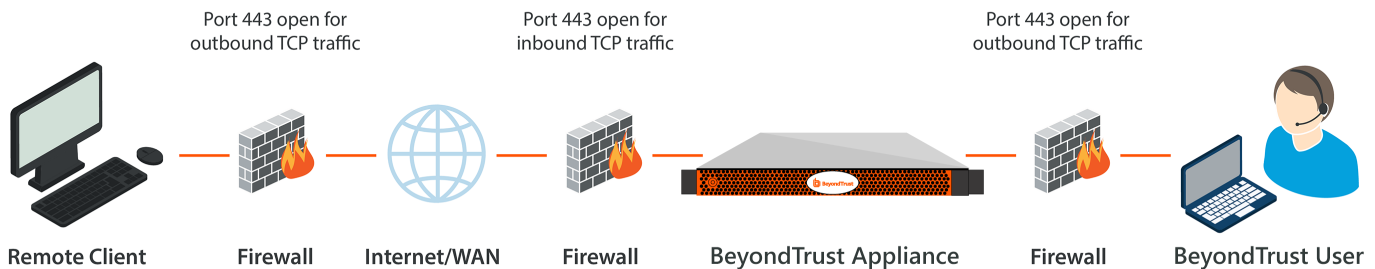
If an error occurs, please contact [BeyondTrust Support](#)



Ports and Firewalls

BeyondTrust solutions are designed to work transparently through firewalls, enabling a connection with any computer with internet connectivity, anywhere in the world. However, with certain highly secured networks, some configuration may be necessary.

TYPICAL NETWORK SETUP: CLOUD 15.1



- Port 443 must be open for outbound TCP traffic on the remote system's and local user's firewalls. More ports may be available depending on your build. The diagram shows a typical network setup; more details can be found in the [BeyondTrust Appliance B Series Hardware Installation Guide](#).
- Internet security software such as software firewalls must not block BeyondTrust executable files from downloading. Some examples of software firewalls include McAfee Security, Norton Security, and Zone Alarm. If you do have a software firewall, you may experience some connection issues. To avoid such issues, configure your firewall settings to allow the following executables, wherein {uid} is a unique identifier consisting of letter and numbers:
 - bomgar-scc-{uid}.exe
 - bomgar-scc.exe
 - bomgar-pac-{uid}.exe
 - bomgar-pac.exe

For assistance with your firewall configuration, please contact the manufacturer of your firewall software.

- Example firewall rules based on B Series Appliance location can be found at www.beyondtrust.com/docs/remote-support/getting-started/deployment/dmz/firewall-rules.htm.

If you should still have difficulty making a connection, contact BeyondTrust Technical Support at www.beyondtrust.com/support

Disclaimers, Licensing Restrictions, and Tech Support

Disclaimers

This document is provided for information purposes only. BeyondTrust Corporation may change the contents hereof without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. BeyondTrust Corporation specifically disclaims any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The technologies, functionality, services, and processes described herein are subject to change without notice.

All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

Licensing Restrictions

One BeyondTrust Remote Support license enables one support representative at a time to troubleshoot an unlimited number of remote computers, whether attended or unattended. Although multiple accounts may exist on the same license, two or more licenses (one per concurrent support representative) are required to enable multiple support representatives to troubleshoot simultaneously.

Tech Support

At BeyondTrust, we are committed to offering the highest quality service by ensuring that our customers have everything they need to operate with maximum productivity. Should you need any assistance, please log into the [Customer Portal](#) at <https://beyondtrustcorp.service-now.com/csm> to chat with Support.

Technical support is provided with annual purchase of our maintenance plan.