BeyondTrust

Privileged Remote Access
B Series Appliance Interface 7.0 (/appliance)

©2003-2023 BeyondTrust Corporation. 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.

TC:12/7/2023

Table of Contents

BeyondTrust Appliance B Series Web Interface **4**
Log in to the BeyondTrust Appliance B Series Administrative Interface **5**
Status Basics: View B Series Appliance Details **6**
Status Health: View PRA Virtual Appliance Health Details **7**
Users: Change Password and Username, Add User, Delete User **8**
SAML: Set Up User Authentication through a SAML Identity Provider **9**
Networking **10**
IP Configuration: Configure IP Address and Network Settings 10
SNMP: Enable Simple Network Management Protocol **14**
Static Routes: Set Up Static Routes for Network Communication **16**
Storage **17**
Status: Disk Space and Hard Drive Status 17
Specific to the BeyondTrust B300P B Series Appliance 17
Specific to the BeyondTrust B400P B Series Appliance 18
Hardware Failure Notification (B300P and B400P Only) 18
Encryption: Encrypt Session Data **19**
Security **20**
Certificates: Create and Manage TLS Certificates 20
Certificate Installation 20
Certificates 22
Certificate Requests 23
TLS Configuration: Choose TLS Ciphers and Versions **25**
Appliance Administration: Restrict Accounts, Networks, and Ports, Enable a STUN Server, Set Up Syslog, Enable Login Agreement, Reset Admin Account **26**
Email Configuration: Configure B Series Appliance to Send Email Alerts **28**
Configure via SMTP 28
Configure via OAuth2 for Microsoft Azure AD 28
Configure via OAuth2 for Google 30
Secret Store: Store and Access Secrets **36**
Add AWS Secret Store 36
Updates: Check for Update Availability and Install Software on Privileged Remote Access **38**

©2003-2023 BeyondTrust Corporation. 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.

Support Utilities: Debug Network Problems 40
Advanced Support: Contact BeyondTrust Technical Support 42

©2003-2023 BeyondTrust Corporation. 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.

BeyondTrust Appliance B Series Web Interface

This guide is designed to help you configure and manage the B Series Appliance through its **/appliance** web interface. The B Series Appliance serves as the central point of administration and management for your BeyondTrust site.

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 at www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/hardware-sra/. Once BeyondTrust is properly installed, you can begin accessing your endpoints immediately. Should you need any assistance, please contact BeyondTrust Technical Support at www.beyondtrust.com/support.

©2003-2023 BeyondTrust Corporation. 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.

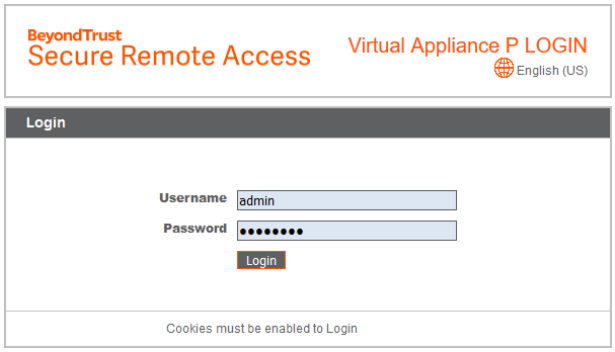
Log in to the BeyondTrust Appliance B Series Administrative Interface

After installation of the B Series Appliance, log in to the B Series Appliance administrative interface by going to your B Series Appliance's public URL followed by **/appliance** (e.g., http://access.example.com/appliance).

Default Username: **admin**

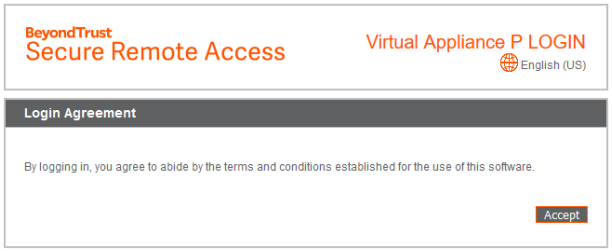
Default Password: **password**

You will be prompted to change the administrative password the first time you log in.[1]



> ***Note:*** *For security purposes, the administrative username and password for the* ***/appliance*** *interface are distinct from those used for the* ***/login*** *interface and should be managed separately.*

You may restrict access to the login screen by enabling a prerequisite login agreement that must be confirmed before the login screen is displayed.



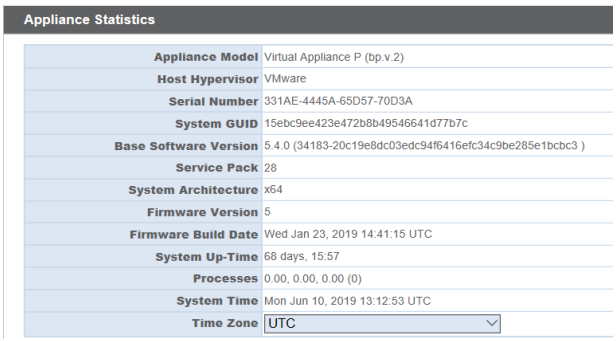
> *If you wish to enable the prerequisite login agreement, please see "Appliance Administration: Restrict Accounts, Networks, and Ports, Enable a STUN Server, Set Up Syslog, Enable Login Agreement, Reset Admin Account" on page 26.*

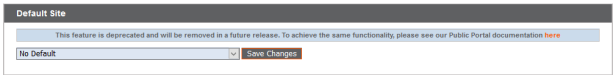
[1]Passwords must be at least 8 characters in length and include each of the following: an uppercase letter, a lowercase letter, a number, and a special symbol.

©2003-2023 BeyondTrust Corporation. 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.

Status Basics: View B Series Appliance Details

The **Basics** page gives you information about your B Series Appliance and allows you to monitor your system. You can also set your local time to any valid global time zone. The system time is displayed in UTC by default.

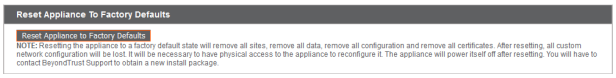




In nearly all scenarios, this setting can be left unchanged. BeyondTrust discourages multiple sites on one B Series Appliance. However, if your setup requires more than one site responding to one IP address, select a default site to respond should someone enter the IP address directly rather than the domain name. If more than one DNS entry directs to this IP address and you select **No Default**, an error message appears if someone tries to access your site by entering the IP address.

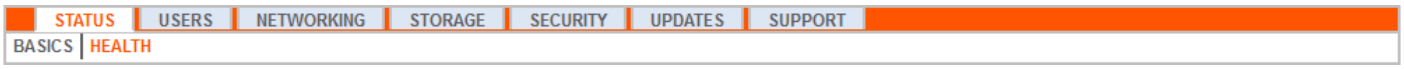
From this page, you can also reboot or shut down your B Series Appliance. Although rebooting your B Series Appliance is not required, you may want to make a monthly reboot part of your regular maintenance. You do not need physical access to the B Series Appliance in order to perform this reboot.

Please do not do the following unless instructed to do so by BeyondTrust Technical Support: Clicking the **Reset Appliance to Factory Defaults** button reverts your B Series Appliance to its factory state. This completely removes all data, configuration settings, sites, and certificates from your B Series Appliance. Once the B Series Appliance is reset, it also powers itself off.



©2003-2023 BeyondTrust Corporation. 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.

Status Health: View PRA Virtual Appliance Health Details



> ***Note:*** *The **Health** tab is visible only for sites supported by a PRA Virtual Appliance or Cloud Appliance.*

The **Health** page allows you to monitor the state of your Virtual or Cloud Appliance. It displays information pertaining to how many CPUs are in use as well as the amount of memory and storage being used. View the **Status** and **Notes** columns for suggestions on how to improve the health of your B Series Appliance.

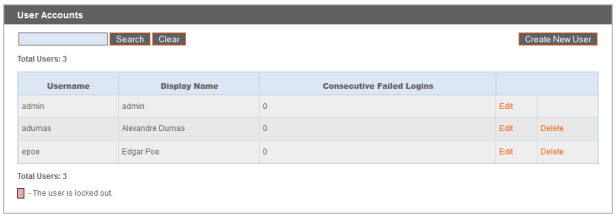
Hardware Health

	Value	Status	Notes
CPU	Count: 8 Model: Intel(R) Xeon(R) CPU E5-2697 v3 @ 2.60GHz Speed: 2593.993 MHz Reservation: 0 MHz Limit: Unlimited		• Consider allocating a CPU Reservation to this VM of at least 500 MHz to help maintain functionality when the host's CPUs are under contention.
Memory	Physical: 16051 MiB Used: 15342 MiB Swap Used: 1187.33203125 MiB Reservation: 0 MiB Limit: 3145727 MiB Host Ballooning: 0 MiB Host Swapping: 0 MiB		• Memory swapping could indicate that this appliance is undersized for the current workload. • Consider allocating a Memory Reservation to this VM for the full amount of physical memory to avoid host swapping, which is detrimental to performance.
Storage	Total Space: 279.998 GiB		

©2003-2023 BeyondTrust Corporation. 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.

Users: Change Password and Username, Add User, Delete User

On the **Users** page, you can add, edit, or delete administrative users for the /appliance interface. You can also change an administrator's username, display name, or password. BeyondTrust recommends changing your password regularly to protect against unauthorized access.



> **Note:** *You must have at least one user account defined. The BeyondTrust Appliance B Series comes with one account predefined, which is the admin account. You can keep just the admin account, create additional accounts, or replace the admin account.*

> *To set account restriction rules, including password expiration and history, please see "Appliance Administration: Restrict Accounts, Networks, and Ports, Enable a STUN Server, Set Up Syslog, Enable Login Agreement, Reset Admin Account" on page 26.*

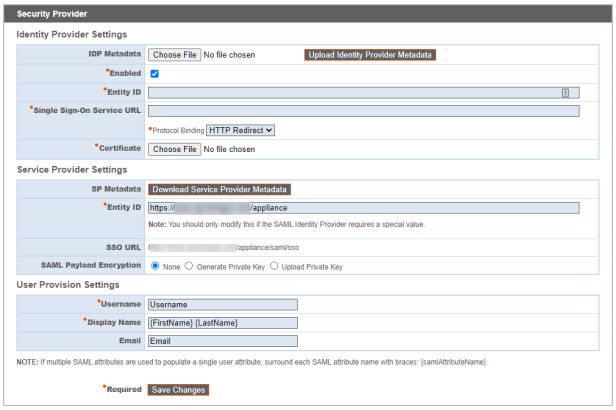
©2003-2023 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

SAML: Set Up User Authentication through a SAML Identity Provider

Configure your B Series Appliance to allow users to authenticate to the /appliance interface using SAML.

> ***Note:*** *To use SAML authentication, you must have an identity provider such as Okta, OneLogin, Azure AD, or ADFS.*

To set up the connection, start with the **Service Provider Settings** section. If your identity provider (IDP) allows you to upload metadata from the service provider (SP), click **Download Service Provider Metadata**. This gives you an XML file that you can upload to your IDP when creating the application. Alternatively, copy and paste the **Entity ID** and **SSO URL** into your IDP.



> ***Tip:*** *The **Entity ID** may be called **Audience URI** in your identity provider.*

By default, **SAML Payload Encryption** is disabled, but you may generate or upload a private key to enable it. To have the B Series Appliance generate a private key and certificate, select **Generate Private Key** and click **Save Changes**. Then, click **Download SP Certificate** and upload the generated certificate to your identity provider. To provide the private key and certificate yourself, select **Upload Private Key**, choose the certificate file, and enter its password, if needed. You must upload the same certificate file to your identity provider.

After saving the application in your identity provider, you may have the option to download its metadata. If so, upload that file to your B Series Appliance with the **Upload Identity Provider Metadata** button. Alternatively, copy and paste the **Entity ID** and **Single Sign-On Service URL** into your B Series Appliance, in the **Identity Provider Settings** section.

> ***Tip:*** *The **Entity ID** may be called **Identity Provider Issuer** or **Issuer URL**, and the **Single Sign-On Service URL** may be called **SAML 2.0 Endpoint**.*

Protocol Binding determines whether an HTTP POST occurs or whether the user is redirected to the sign-on URL. Leave this set to **HTTP Redirect** unless otherwise required by your identity provider. You must also provide the IDP **Certificate**, which you can download from the IDP.

Under **User Provision Settings**, map the **Username**, **Display Name**, and **Email** to the corresponding attributes in your identity provider.

Click **Save Changes** to save the SAML configuration.

Now, on the /appliance login page, users will see a link to **Use SAML Authentication** below the **Login** button. Users who have been assigned to the application created in your IDP can click this link to log in. If they are not already signed into the IDP, they will be redirected to the IDP to log in before being redirected back to /appliance.

©2003-2023 BeyondTrust Corporation. 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.

Networking

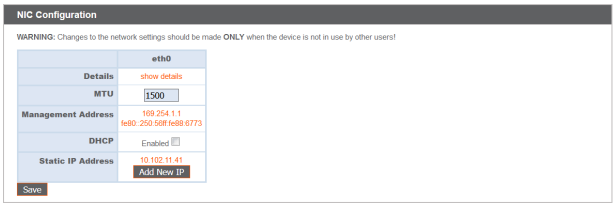
IP Configuration: Configure IP Address and Network Settings

Companies with advanced network configurations can configure multiple IP addresses on the B Series Appliance's ethernet ports. Using multiple ports can enhance security or enable connections over non-standard networks. For example, if employees are restricted from accessing the internet but need to provide off-network support, using one port for your internal private network and another for the public internet allows users worldwide to access systems without breaching your network security policies.

NIC teaming combines your system's physical NICs into a single logical interface. NIC teaming operates in active-backup mode. One of the NICs is used to carry all network traffic. If the link on that NIC is lost for any reason, the other NIC becomes active. Before activating NIC teaming, please ensure that both NICs are connected to the same network segment (subnet) and that you have IP addresses configured on only one of the existing NICs.

> ***Note:*** *If you are using a Virtual or Cloud Appliance environment, the* ***Enable NIC Teaming*** *option is not available.*

Although multiple IP addresses can be assigned to each Network Interface Controllers (NIC), do not configure either NIC such that it has an IP address that is in the same subnet as an IP address on the other NIC. In this scenario, packet loss occurs with packets originating from the IP on the NIC that does not have the default gateway. Consider the following example configuration:



- eth0 is configured with the default gateway of 192.168.1.1
- eth0 is assigned with 192.168.1.5
- eth1 is assigned with 192.168.1.10
- Both eth0 and eth1 are connected to the same subnet switch

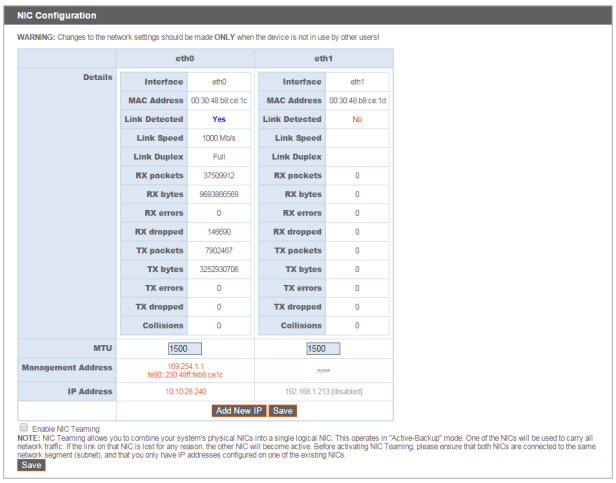
Given this configuration, traffic from both NICs is sent to the default gateway (192.168.1.1) regardless of which NIC received traffic. Switches configured with dynamic Address Resolution Protocol (ARP) send packets randomly to either eth0 (192.168.1.5) or eth1 (192.168.1.10), not both. When eth0 receives these packets from the switch destined for eth1, eth0 drops the packets. Some switches are configured with static ARP. These switches drop all packets received from eth1 since this NIC does not have the default gateway and is not present in the static ARP table of the gateway. If you wish to configure redundant NICs on the same subnet, use NIC teaming.

By default, Dynamic Host Configuration Protocol (DHCP) is enabled for your B Series Appliance. DHCP is a network protocol that uses a DHCP server to control the distribution of network parameters, such as IP addresses, allowing systems to automatically request these parameters. This reduces the need to manually configure settings. In this case, when checked, an IP address is obtained from the DHCP server and is removed from the pool of available IP addresses.

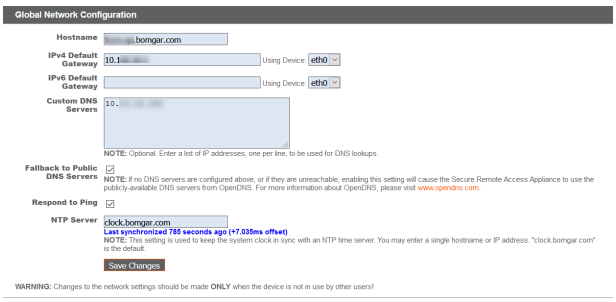
> *To learn more about DHCP, please see What is DHCP? at docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd145320(v=ws.10).*

©2003-2023 BeyondTrust Corporation. 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.

Click **Show Details** to view and verify transmission and reception statistics for each ethernet port on the B Series Appliance.



Under the **Global Network Configuration** section, configure the hostname for your B Series Appliance.



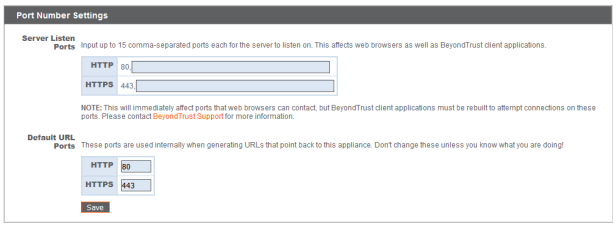
> ***Note:*** *The **Hostname** field does not need to meet any technical requirements. It does not affect what hostname client software or remote users connect to. If the hostname attempted by the client software needs to change, notify BeyondTrust Technical Support of the needed changes so that Support can build a software update. The **Hostname** field exists primarily to help you distinguish between multiple B Series Appliances. It is also used as the local server identifier when making SMTP connections to send email alerts. This is useful if the **SMTP Relay Server** specified at **/appliance > Security > Email Configuration** is locked down. In this case, the configured hostname might have to match the reverse-DNS lookup of the B Series Appliance's IP address.*

Assign a default gateway, selecting which ethernet port to use. Enter an IP address for one or more DNS servers. If DHCP is enabled, the DHCP lease provides you with a default gateway as well as a listing of DNS servers in order of preference. Any statically configured DNS servers listed in the **Custom DNS Servers** field are attempted to be reached first, followed by DNS servers received from DHCP. In the event that these local DNS servers are unavailable, the **Fallback to Public DNS Servers** option enables the B Series Appliance to use publicly available DNS servers from OpenDNS.

> *For more information about OpenDNS, please see www.opendns.com.*

Allow your B Series Appliance to respond to pings if you want the ability to test if the host is functioning. Set the hostname or IP address for a Network Time Protocol (NTP) server with which you wish your B Series Appliance to synchronize.

©2003-2023 BeyondTrust Corporation. 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.

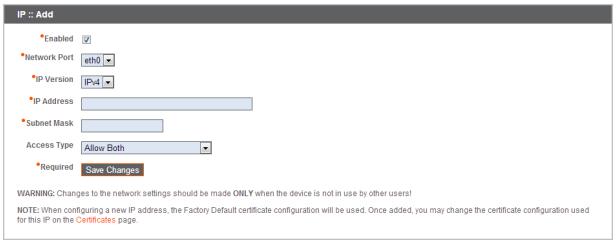


Two settings are available in the **Port Number Settings** area: **Server Listen Ports** and **Default URL Ports**. When configuring these, keep in mind that connections made to valid ports may be rejected by network restrictions set in **/appliance > Security > Appliance Administration** and in **/login > Management > Security**. The opposite is also true: connections made to invalid ports are rejected even if such connections satisfy network restrictions.

The **Server Listen Ports** section allows you to configure ports for the B Series Appliance to listen on. You may specify up to 15 comma-separated ports for HTTP and 15 comma-separated ports for HTTPS. Each port may appear only once in any field, and it may appear in only one field, not both. The B Series Appliance responds to HTTP connections made to any of the ports listed in the HTTP field, and the B Series Appliance responds to HTTPS connections made to any of the ports in the HTTPS field. You cannot change the built-in listen ports (80 and 443).

To access the B Series Appliance on a given port, use a browser that requires you to enter the port in the URL of the browser (e.g., support.example.com:8200). Clients downloaded from the B Series Appliance attempt connections to the ports listed on the **/login > Status > Information** page under **Client Software Is Built to Attempt**. These ports are not configurable from /login or /appliance. To change them, you must contact BeyondTrust Support and have a new update built for your B Series Appliance. Once installed, the update sets the **Attempt** ports as specified by BeyondTrust Support in the parameters of the update.

Default URL Ports are used when generating URLs that point back to the B Series Appliance, such as session keys generated from the access console. When the default ports are blocked on the network (or can be expected to fail for any other reason), you can change the default URL ports to have generated URLs spawn with the ports that you specify. Whatever ports you enter should also be listed in the **Server Listen Ports**; otherwise, the default ports do not connect. For example, if you enter **8080** in the **Default URL Port** field, make sure **8080** is also in the **HTTP** or **HTTPS Listen Port** field. Unlike the listen port fields, you cannot enter more than one port in either of the URL port fields. You cannot enter the same port in both fields.



When adding or editing an IP address, choose whether that IP should be enabled or disabled. Select the network port on which you would like this IP to function. The **IP Address** field sets an address to which your B Series Appliance can respond, while **Subnet Mask** enables BeyondTrust to communicate with other devices.

When editing an IP address that is on the same subnet as another IP address for this B Series Appliance, choose if this IP address should be **Primary**. When this box is checked, the B Series Appliance designates this IP address to be the primary or originating IP address for the subnet. This helps, for example, to ensure that any network traffic originating from the B Series Appliance on that subnet matches and complies with defined firewall rules.

From **Access Type**, you can restrict access over this IP to the public site or all clients (including mobile and web consoles) outside of the normal web traffic. Use **Allow Both** (web and session traffic) to allow access for both the public site and all clients.

It is possible to separate the web and session traffic by changing the configuration of the network. The exact process depends on the existing configuration of the network. For more information, contact Support.

> ***Note:*** *To restrict access to the **/login** interface, set network restrictions under **/login > Management > Security**. To restrict access to the **/appliance** interface, set network restrictions under **/appliance > Security > Appliance Administration**.*

©2003-2023 BeyondTrust Corporation. 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.

When viewing the management IP address[1], the **Telnet Server** dropdown provides three settings: **Full**, **Simplified** and **Disabled**, as detailed below. These settings change the menu options of the telnet server that is available only on this private IP and that can be used in emergency recovery situations. Since the telnet feature is specifically tied to the built-in private IP, it does not appear under any other configured IP addresses.

Setting	Function
Full	Enables the telnet server with full functionality
Simplified	Allows four options: **View FIPS Error**, **Reset to Factory Defaults**, **Shutdown**, and **Reboot**
Disabled	Completely disables the telnet server

[1]Do not delete or modify the management IP address.

©2003-2023 BeyondTrust Corporation. 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.

SNMP: Enable Simple Network Management Protocol

The BeyondTrust Appliance B Series supports Simple Network Management Protocol (SNMP). SNMP is an Internet-standard protocol used for monitoring and managing networked devices.

This allows tools that collect availability and other statistics via the SNMP protocol to query the B Series Appliance for monitoring purposes.

To enable SNMP for this B Series Appliance, check **Enable SNMPv2** or **Enable SNMPv3**. This enables an SNMPv2 or v3 server to respond to SNMP queries. Enter a value for the **Read-Only Community Name**, the **System Location**, and the **IP Restrictions** for IP addresses that are allowed to query this B Series Appliance using SNMP.

Note: *If no IP addresses are entered in the* ***IP Restrictions*** *field, all hosts are granted access.*

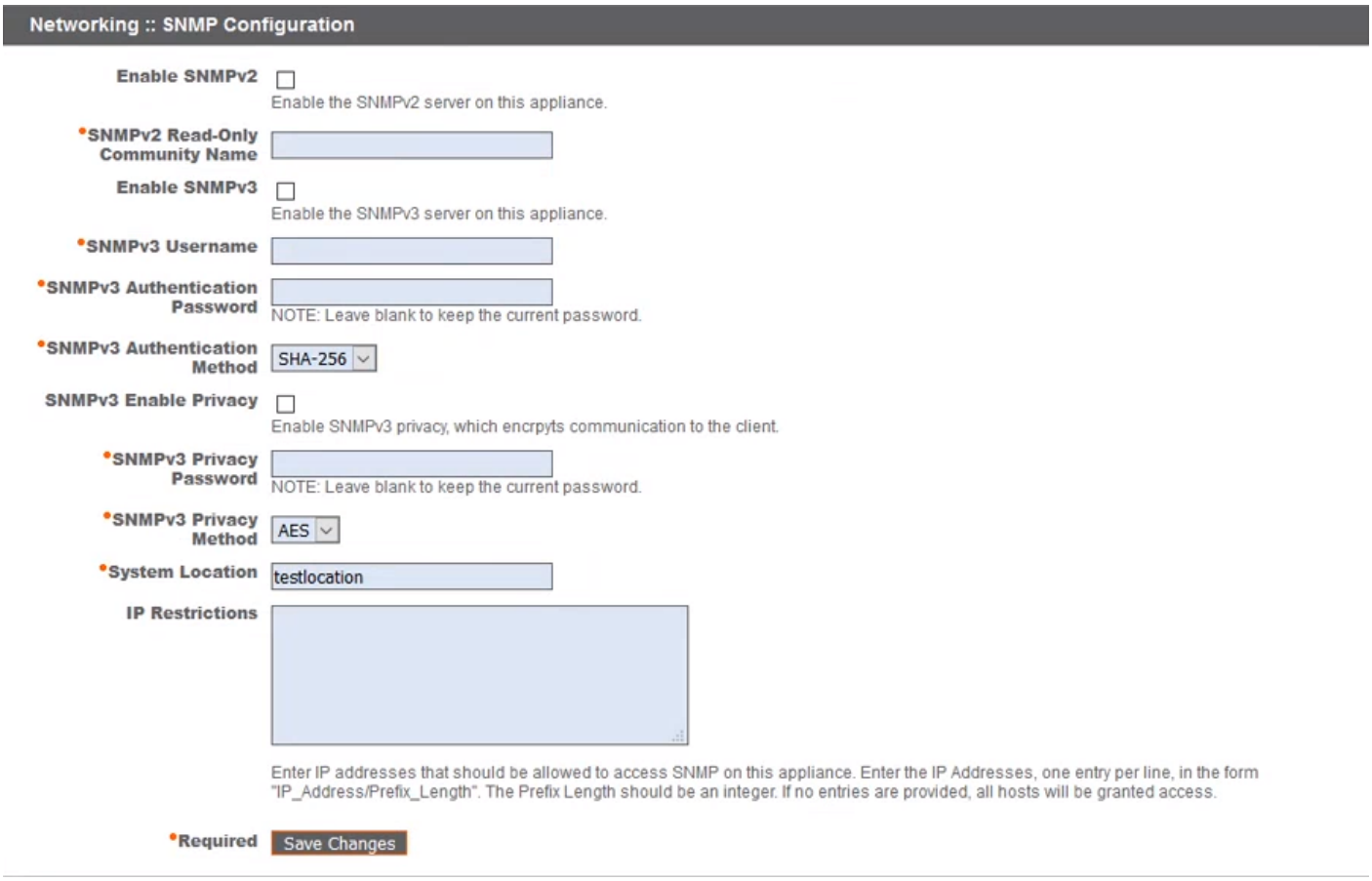
If selecting SNMPv3:

1. Enter a **Username** and **Password**.
2. Select the **Authentication Method** of your choice from the dropdown menu.
3. Check **SNMPv3 Enable Privacy** if you want to encrypt communications to the client.
4. Enter a **Privacy Password** and select a **Privacy Method**.

Click **Save Changes** when done.

For more information on SNMP, please see Simple Network Management Protocol at wikipedia.org/wiki/Simple_Network_Management_Protocol.

©2003-2023 BeyondTrust Corporation. 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.

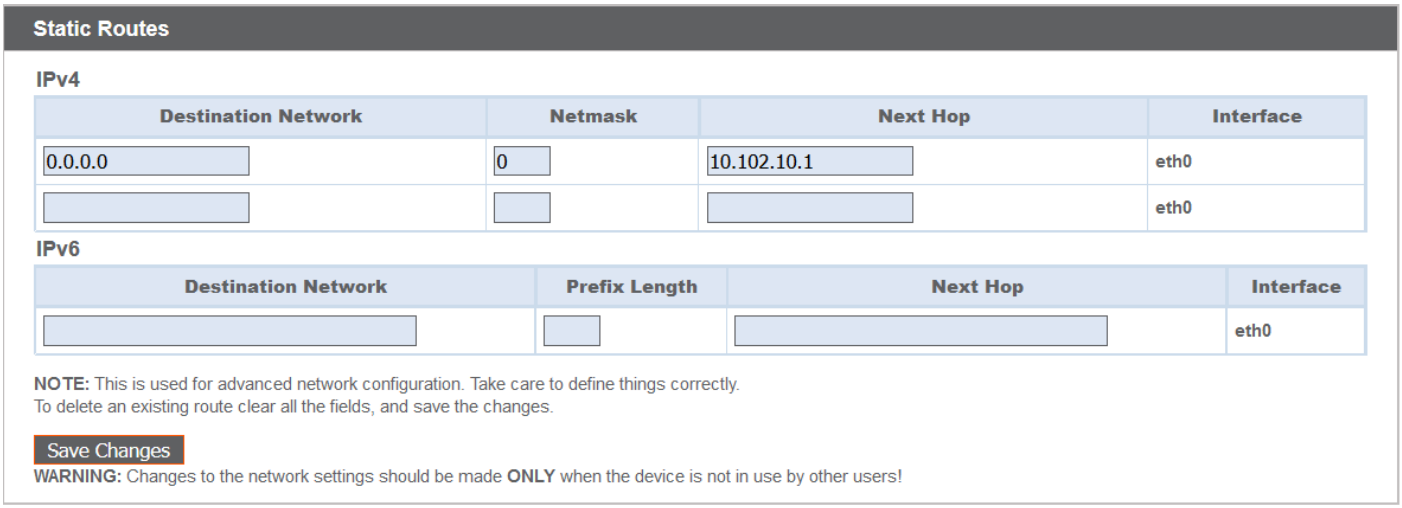


©2003-2023 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

Static Routes: Set Up Static Routes for Network Communication

Should a situation exist in which two networks are unable to talk to each other, you can establish a static route so that an administrator with a computer on one network can connect through the B Series Appliance to a computer on the other network, provided that the B Series Appliance is in a place where both networks can communicate with it individually.

Only advanced administrators should attempt to set up static routes.

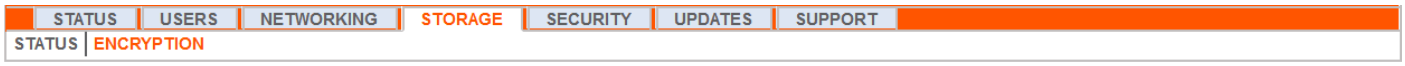


Note: *Static routes can also be created in the console. For more information, please see Secure Remote Access Console Configuration at https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/hardware-sra/console.htm.*

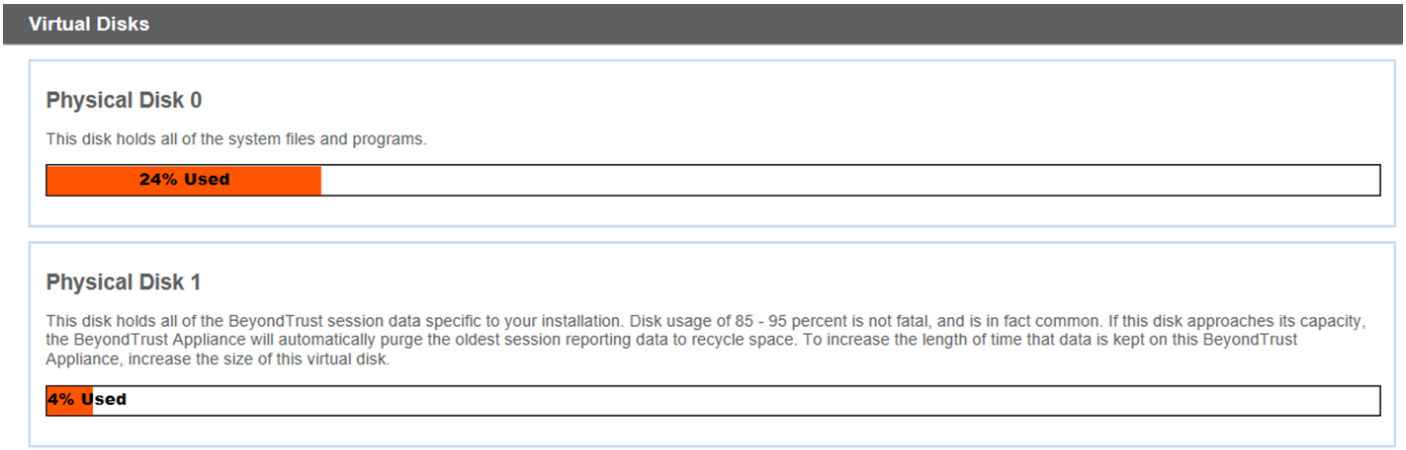
©2003-2023 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

Storage

Status: Disk Space and Hard Drive Status



The **Status** page displays the percentage of your B Series Appliance's hard drive space that is in use.



If you enable all recording features on your site (session, protocol tunneling, and remote shell recordings), or if your overall session count is high, it is common to see a higher amount of disk usage. Note that disk usage of 85-95% is NOT a cause for alarm. If the hard drive should become low on disk space, the B Series Appliance is configured to automatically purge the oldest session data and recycle that disk space for new session data.

Specific to the BeyondTrust B300P B Series Appliance

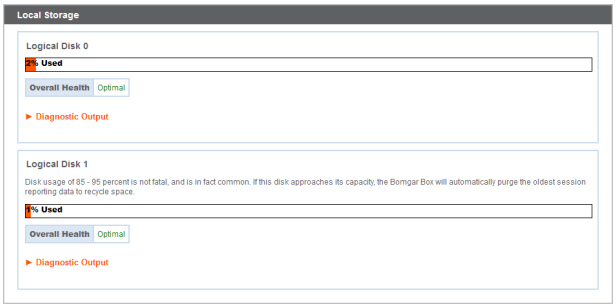
The B300P uses a Redundant Array of Independent Disks to back up your data. RAID 6 is used to allow the B Series Appliance to lose up to 2 of its 4 drives without any data loss. In the event of a failure, remove the corrupted drive and contact BeyondTrust for a return maintenance authorization and repair or replacement drive. When you replace the damaged drive, the B Series Appliance automatically rebuilds the RAID using the new drive. You do not need to power off the B Series Appliance when replacing drives.

©2003-2023 BeyondTrust Corporation. 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.

Specific to the BeyondTrust B400P B Series Appliance

The B400P has two sets of logical Redundant Array of Independent Disks (RAID) disks. This RAID configuration includes eight physical disk drives configured into two logical RAID drives: A RAID 1 configuration that is logical disk 0, and a RAID 6 configuration that is logical disk 1.

If one of the RAID 1 or RAID 6 physical drives fails, no performance impact or data loss occurs. However, second drive failure in the RAID 6 configuration degrades performance, although it does not cause data loss.



Hardware Failure Notification (B300P and B400P Only)

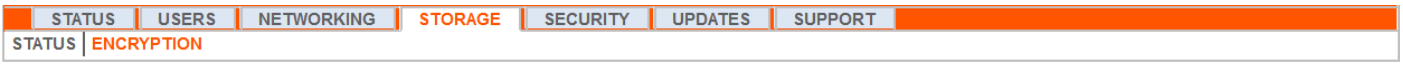
The LEDs on your B Series Appliance also indicate your hard drives' status. Normally, the LEDs blinks to indicate disk activity. Should a hard drive fail, the LED turns red, and an audible alarm warns you of the failure. To turn off the alarm before the system is restored, click the **Silence Alarm** button on this web interface.

Note: *The **Silence Alarm** button is available regardless of whether or not an alarm is sounding at the time. The button cannot be used as an indicator of whether or not an alarm is active at any particular moment.*

Note: *To verify whether an alarm is sounding, check the **Health Status** located immediately above the **Silence Alarm** button. If there is an alarm sounding in the same room as the B Series Appliance and you want to eliminate the B Series Appliance as the source, click the **Silence Alarm** button a few times to cancel any and all possible alarms which might be active.*

©2003-2023 BeyondTrust Corporation. 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.

Encryption: Encrypt Session Data

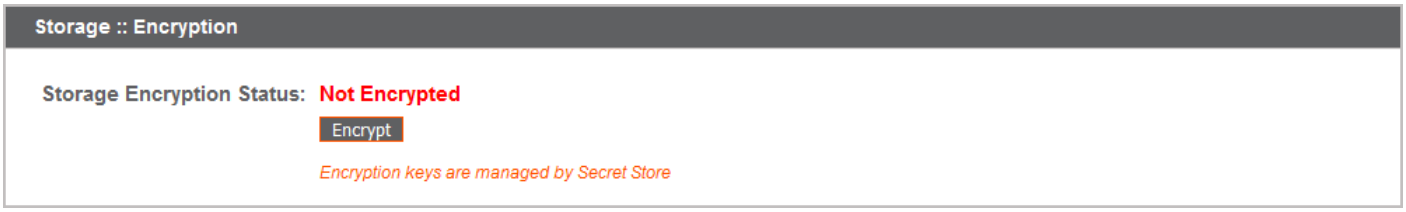


The **Encryption** section allows you to encrypt session data stored on your B Series Appliance. When first encrypting your data, you are limited to 4GB or less of data; however, after the initial encryption, this 4GB limit no longer applies.

If you have not already added a secret store, go to **Security > Secret Store** to add one.

For more information, please see "Secret Store: Store and Access Secrets" on page 36.

Note: *If you have more than 4GB of data to initially encrypt, please contact BeyondTrust Technical Support at www.beyondtrust.com/support.*



©2003-2023 BeyondTrust Corporation. 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.

Security

Certificates: Create and Manage TLS Certificates

Manage TLS certificates, create self-signed certificates and certificate requests, and import certificates signed by a certificate authority.

Certificate Installation

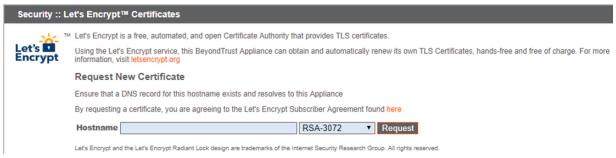
The BeyondTrust Appliance B Series comes with a self-signed certificate pre-installed. However, to effectively use your B Series Appliance, you also need to, at minimum, create a self-signed certificate; preferably requesting and uploading a certificate signed by a certificate authority. BeyondTrust also includes functionality for requesting, obtaining, and automatically renewing its own TLS certificates from the open certificate authority Let's Encrypt.

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**.

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.*

IMPORTANT!

Because DNS can apply only to one B Series Appliance at a time, and because a B Series Appliance must be assigned the DNS hostname for which it makes a certificate request or renewal request, we recommend that you avoid use of Let's Encrypt

©2003-2023 BeyondTrust Corporation. 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.

certificates for failover B Series Appliance pairs.

For more information, please see letsencrypt.org.

***Note:** If the certificate being requested is a replacement, you should select the existing key of the certificate being replaced.*

*If the certificate being requested is a re-key, you should select **New Key** for the certificate.*

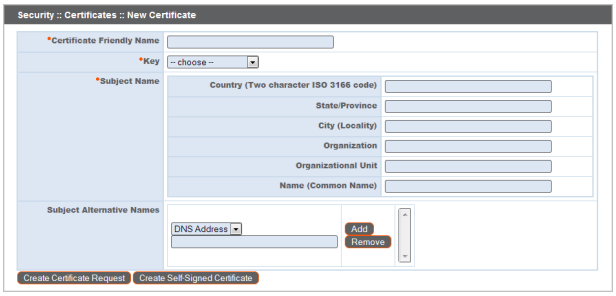
*For a re-key, all information on the **Security :: Certificates :: New Certificate** section should be the same as the certificate for which re-key is being requested. A new certificate friendly name should be used so that it is easy to identify the certificate in the **Security :: Certificates** section.*

*Required information for the re-key can be obtained by clicking on the earlier certificate from the list displayed in the **Security :: Certificates** section.*

For a new key or re-key certificate, the steps to import are the same.

Other CA-Issued Certificates

To create a certificate request:

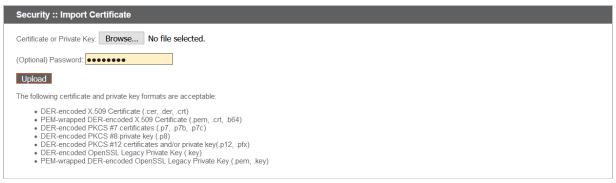


- Locate the **Security :: Other Certificates** section and click **Create**.
- In **Certificate Friendly Name**, enter a name you will use to identify this certificate.
- From the **Key** dropdown, choose the **Existing Key** of your *.beyondtrustcloud.com certificate or select a new key type.
- Enter 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, remote.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 sends you one or more new certificate files, each of which you must install on the B Series Appliance.



©2003-2023 BeyondTrust Corporation. 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.

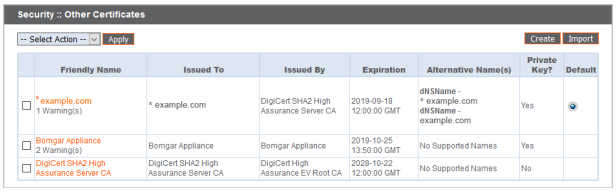
To upload your new certificate files, click **Import**. Browse to the first file and upload it. Repeat this for each certificate sent by your CA. Often, a CA does not send their root certificate, which must be installed on your B Series Appliance. If the root is missing, a warning appears beneath your 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 web site 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. Once done, download it from the CA's root store and import it to your B Series Appliance as described above.

Certificates

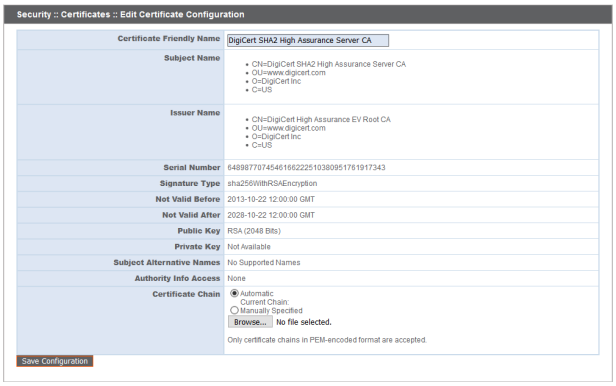
View a table of SSL certificates available on your B Series Appliance.



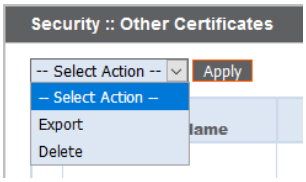
For connections that do not supply a Server Name Indication (SNI) or supply an incorrect SNI, select a default SSL certificate from the list to provide for these connections by clicking the button under the **Default** column. The default SSL certificate cannot be a self-signed certificate nor the default B Series Appliance certificate provided for initial installation.

To learn more about SNI, please see Server Name Indication at https://cio.gov/sni/.

Click a certificate name to view details and manage its certificate chain.

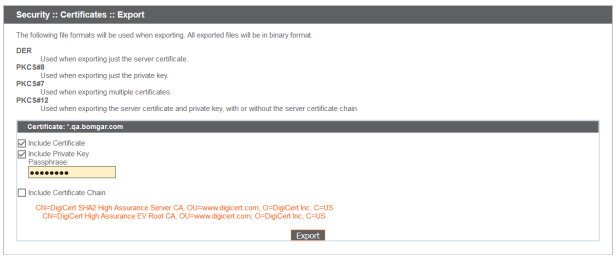


To export one or more certificates, check the box for each desired certificate, select **Export** from the dropdown at the top of the table, and then click **Apply**.



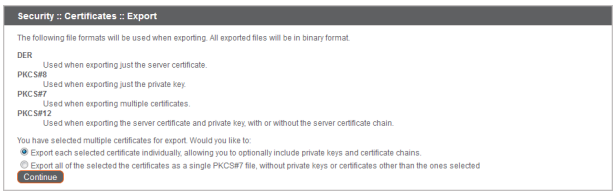
©2003-2023 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

If you are exporting only one certificate, you immediately can choose to include the certificate or the certificate chain if available. Click **Export** to start the download.

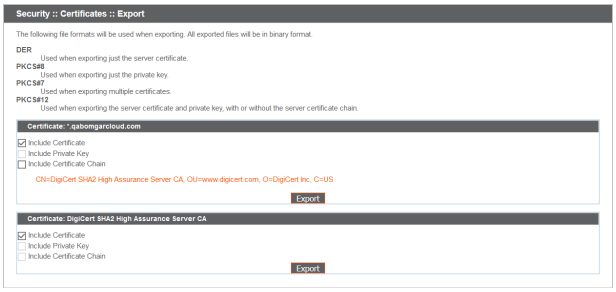


If you are exporting multiple certificates, you have the option to export each certificate individually or in a single PKCS#7 file.

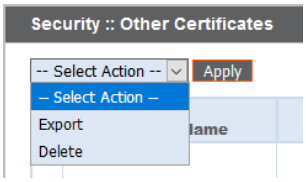
When selecting to export multiple certificates as one file, click **Continue** to start the download. With this option, only the actual certificate files will be exported, without any certificate chains.



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**.

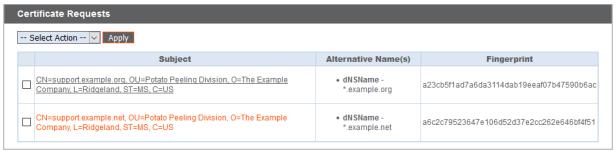


> ***Note:*** *Under normal circumstances, a certificate should never be deleted unless it has already been successfully replaced by a working substitute.*

To confirm accuracy, review the certificates you wish to delete, and then click **Delete.**

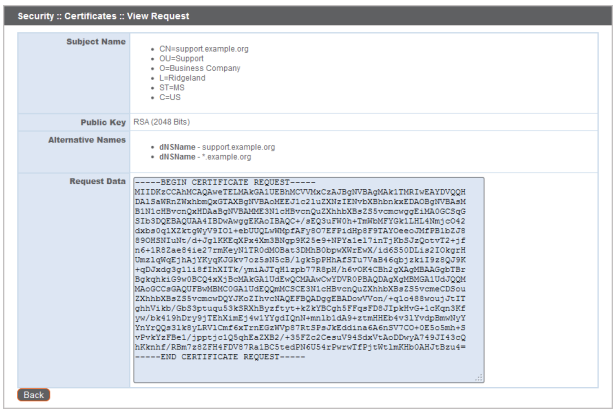
Certificate Requests

View a table of pending requests for third-party-signed certificates. Click a certificate request name to view details.

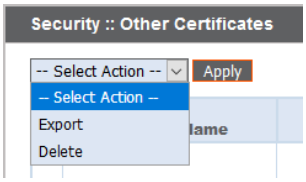


©2003-2023 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

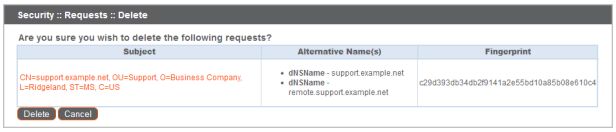
The detail view also provides the request data you give your preferred certificate authority when requesting a signed certificate.



To delete one or more certificate requests, check the box for each desired request, select **Delete** from the dropdown at the top of the table, and then click **Apply**.

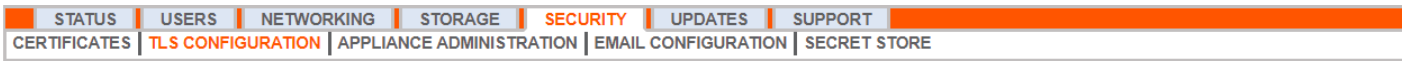


To confirm accuracy, review the certificate requests you wish to delete, and then click **Delete**.

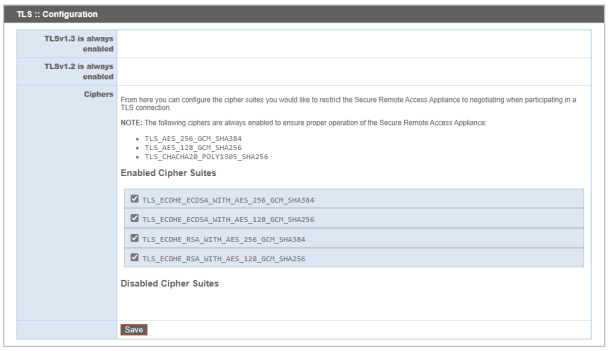


©2003-2023 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

TLS Configuration: Choose TLS Ciphers and Versions



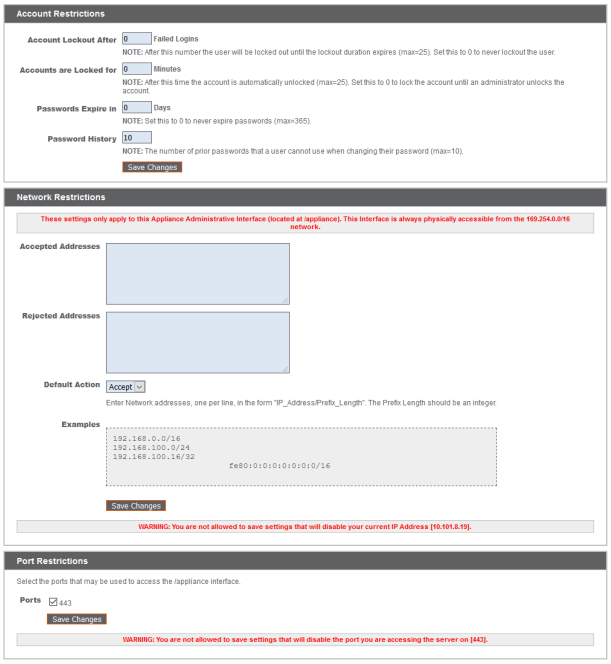
Select which cipher suites should be enabled or disabled on your B Series Appliance. Drag and drop cipher suites to change the order of preference. Changes to cipher suites do not take effect until the **Save** button is clicked.



©2003-2023 BeyondTrust Corporation. 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.

Appliance Administration: Restrict Accounts, Networks, and Ports, Enable a STUN Server, Set Up Syslog, Enable Login Agreement, Reset Admin Account

Manage access to /appliance administrative interface accounts by setting how many failed logins are allowed. Set how long an account is locked out after passing the failed login limit. Also, set the number of days a password may be used before expiration, and restrict the reuse of previous passwords.

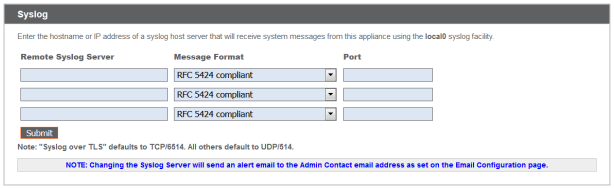


You can restrict access to your B Series Appliance's administrative interface by setting network addresses that are or are not allowed, and you can select the ports through which this interface is be accessible.

In the **Accepted Addresses** field, define IP addresses or networks that are always granted access to /appliance. In **Rejected Addresses**, define IP addresses or networks that are always denied access to /appliance. Use the **Default Action** dropdown to determine whether to accept or to reject IP addresses and networks not listed in either of the above fields. In the case of overlap, the most specific match takes precedence.

If, for example, you want to allow access to 10.10.0.0/16 but reject access to 10.10.16.0/24 and reject access from anywhere else, you would enter **10.10.0.0/16** in the **Accepted Addresses** field, enter **10.10.16.0/24** in the **Rejected Addresses** field, and set the **Default Action** to **Reject**.

The BeyondTrust Appliance B Series can be configured to run a STUN service on UDP port 3478 to help facilitate peer-to-peer connections between BeyondTrust clients. Check the **Enable local STUN service** box to use this functionality.



You can configure your B Series Appliance to send log messages to up to three syslog servers. Enter the hostname or IP address of the syslog host server receiving system messages from this B Series Appliance in the **Remote Syslog Server** field. Select the data format for the event notification messages. Choose from the standards specification **RFC 5424**, one of the legacy **BSD formats**, or **Syslog over TLS**. Syslog over TLS defaults to using TCP port 6514. All other formats default to using UDP 514. However, the defaults can be changed. The B Series Appliance logs are sent using the **local0** facility.

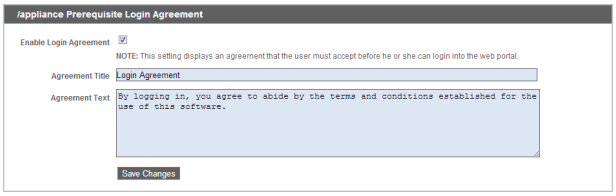
> *For Cloud-specific settings, please see B Series Appliance Administration: Set Syslog over TLS at https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/cloud/syslog-over-tls.htm.*

©2003-2023 BeyondTrust Corporation. 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.

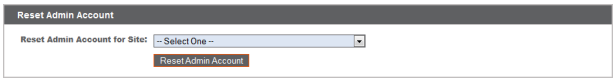
Note: *When changing or adding a syslog server, an alert is emailed to the administrator's email address. The administrator's information is configured at* ***Security > Email Configuration > Security :: Admin Contact****.*

For a detailed syslog message reference, please see the Syslog Message Reference at www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/syslog/.

You can enable a login agreement that users must accept before accessing the /appliance administrative interface. The configurable agreement allows you to specify restrictions and internal policy rules before users are allowed to log in.



You can select a site and click **Reset Admin Account**, which restores a site's administrative username and password to the default should the login be forgotten or need to be replaced.



Note: *If you reset the admin account, any existing session permissions for that account are removed.*

©2003-2023 BeyondTrust Corporation. 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.

Email Configuration: Configure B Series Appliance to Send Email Alerts

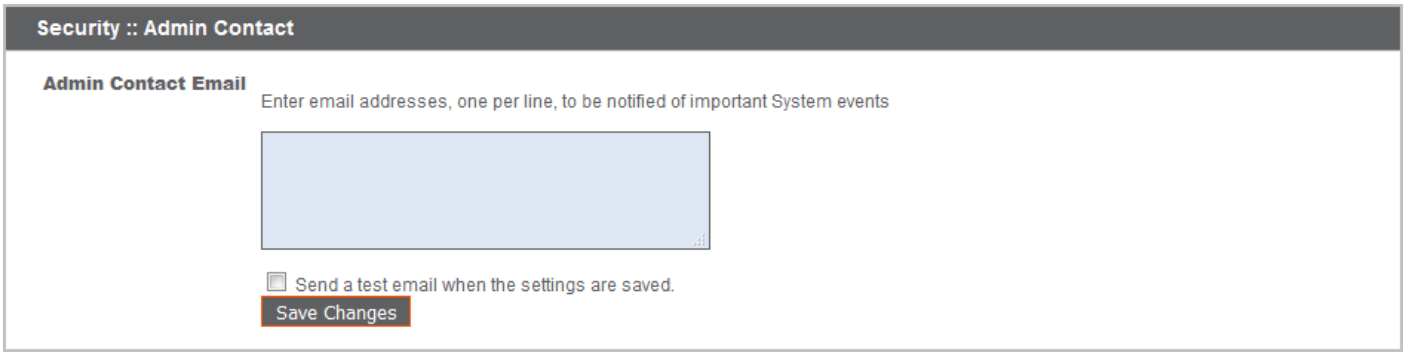
Your B Series Appliance can send you automatic email notifications. Emails are sent for the following events:

- **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 28 or "Configure via OAuth2 for Google" on page 30 for alternate configurations.*

After entering the email addresses for the administrator contacts, save your settings and send a test email to ensure everything works correctly.



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:

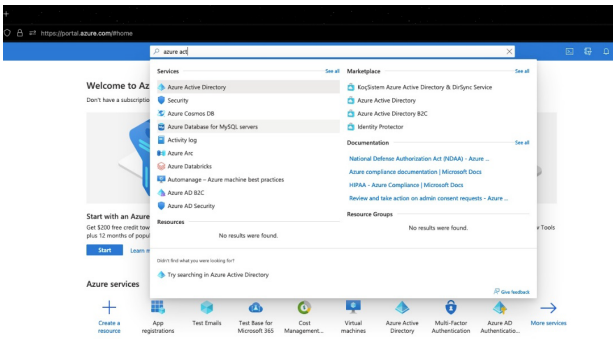
1. Go to **Appliance**, click the **Security** tab and click **Email Configuration**.
2. Change the **Authentication Method** to OAuth2
3. Note the **Authorization Redirect URI**. It is required later.

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**.

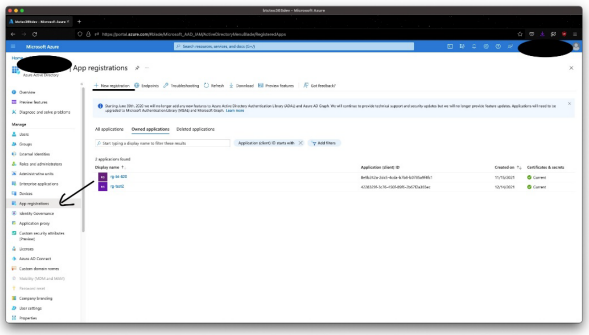
Once **Authenticated SMTP** is enabled, perform the following steps in the Azure console:

©2003-2023 BeyondTrust Corporation. 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.

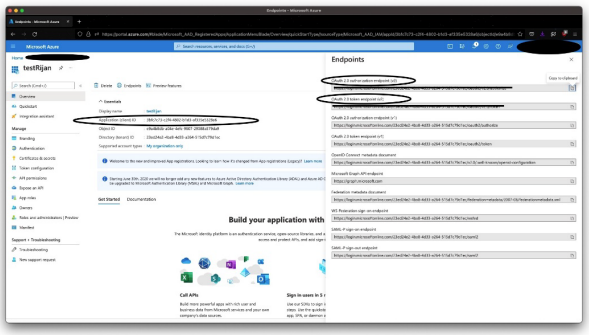
4. Log in to your Azure console (portal.Azure.com).
5. Go to **Azure Active Directory**.



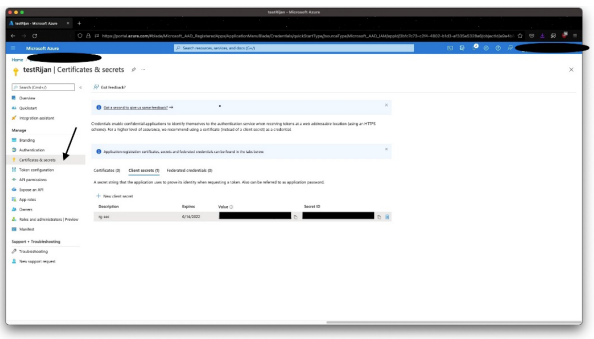
6. Go to **App registrations** and select **New registration**.
7. Enter a name, such as Appliance-OAuth2.
8. Select the types of account you want to be able to log in to the application through OAuth2. Select **Single Tenant** for internal only.
9. Enter the **Redirect URI**. This is the **Authorization 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.

©2003-2023 BeyondTrust Corporation. 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.

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 BeyondTrustappliance and the Google Cloud Platform.

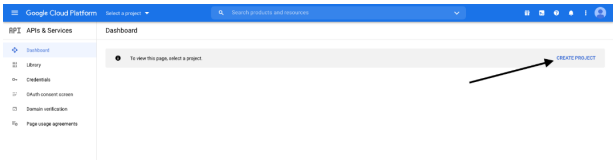
Start by changing settings on the BeyondTrust appliance:

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.

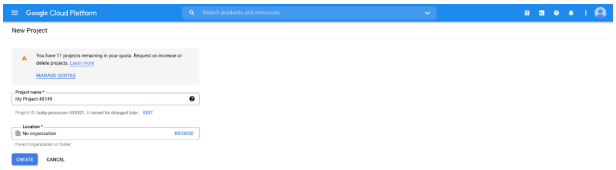
©2003-2023 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

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.

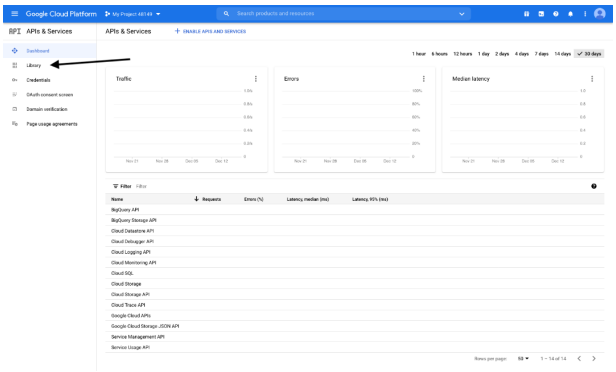
4. Click **CREATE PROJECT**. You can also use an existing project.



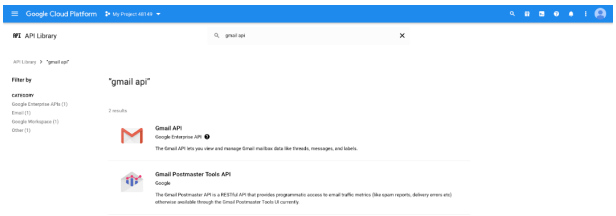
5. Accept the default **Project Name** or enter a name.
6. Accept the default **Location** or select a folder from those available for your organization.
7. Click **CREATE**.



8. The **APIs and services** page appears. Click **Library** in the left menu.

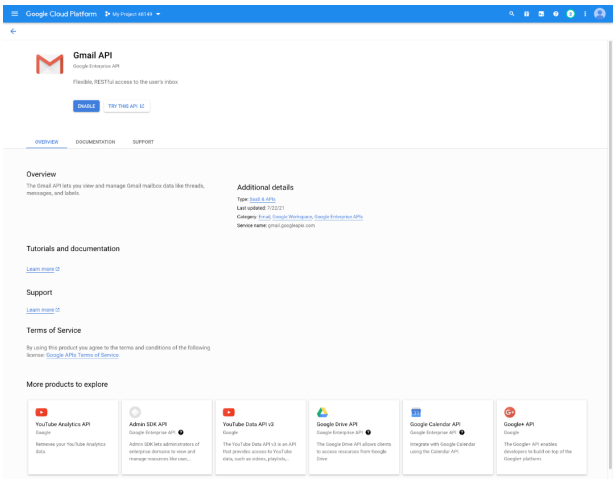


9. Search or browse for the **Gmail API** in the library, and click it.

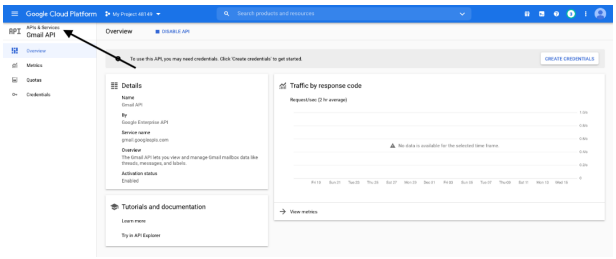


©2003-2023 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

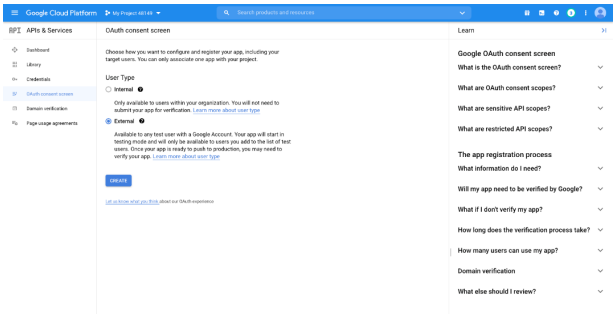
10. The **Gmail API** appears on its own page. Click **ENABLE**.



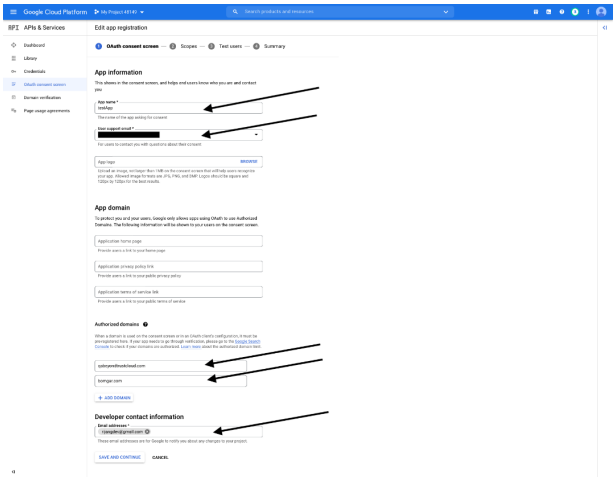
11. The **Gmail API Overview** page appears. Click **APIs & services** in the upper left.
12. The **APIs and services** page appears again. Click **OAuth consent screen** in the left menu.



13. Select the **User Type**. Internal allows only users from within the organization, but requires a Google Workspace account.
14. Click **CREATE**.

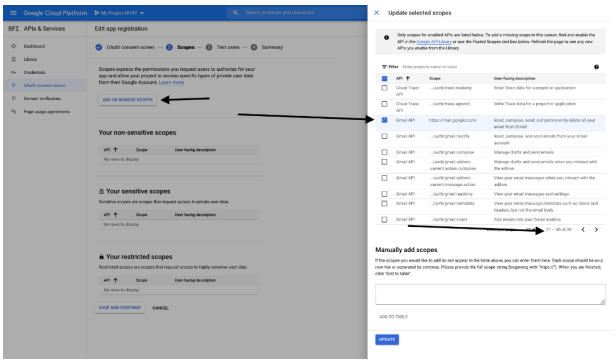


15. Enter the **App name**.
16. Enter a **User support email** address. This may default to the address you are using to create the project.
17. Enter a logo for the app, if desired. The **App domain** section is also optional.
18. Add the **Authorized domains**. For BeyondTrust test appliances, these 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**.



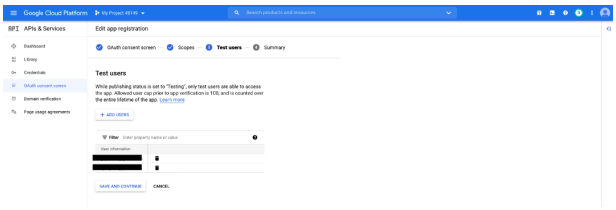
©2003-2023 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

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.

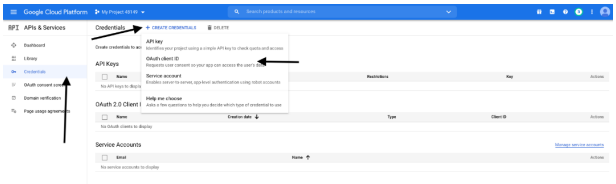


> ***Note:*** *The API does not appear if it has not been enabled.*

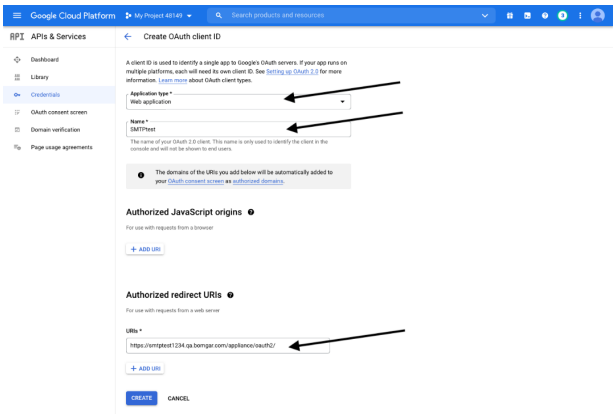
23. Click **UPDATE**. The **Update selected scopes** window closes.
24. Click **SAVE AND CONTINUE**.



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**.

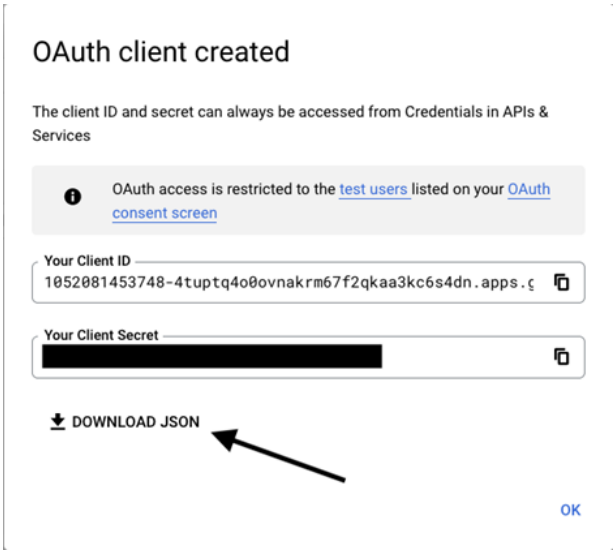


31. On the create credentials page, select **Web application** for the **Application type**. Additional fields appear when this is selected.
32. Enter a name for the application.
33. Scroll down to **Authorised redirect URIs** and click **ADD URI**.
34. Enter the **Authorization Redirect URI** obtained from the BeyondTrust appliance at the start of this process.
35. Click **CREATE**.



©2003-2023 BeyondTrust Corporation. 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.

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.



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.

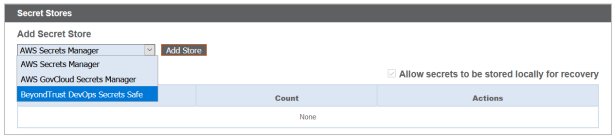
©2003-2023 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

47. To test the configuration:
    - Add an **Admin Contact Email**.
    - Check **Send a test email**.
    - Click **Save Changes**.

©2003-2023 BeyondTrust Corporation. 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.

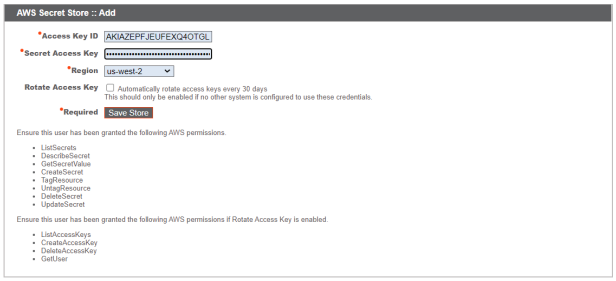
Secret Store: Store and Access Secrets

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.*

For the list of endpoints, please see AWS Secrets Manager endpoints and quotas at 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.

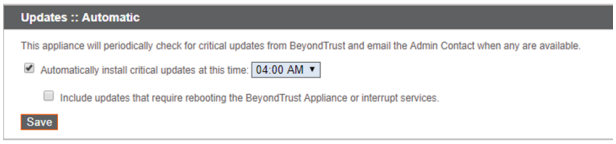
©2003-2023 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

Note: *If you delete the last remote store, a message displays indicating secrets will be moved locally.*

©2003-2023 BeyondTrust Corporation. 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.

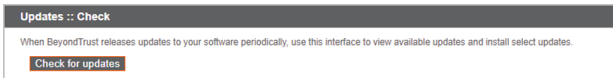
Updates: Check for Update Availability and Install Software on Privileged Remote Access

The B Series Appliance periodically checks for critical updates and emails the admin contact person when updates are available. You can select if you want the updates to install automatically and use the dropdown menu to select a time for the installation.



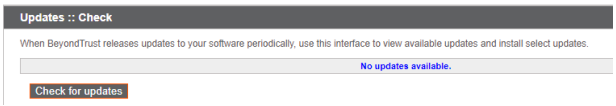
Updates requiring a B Series Appliance reboot or the interruption of services are excluded from the automatic update process unless you check the box to include them.

BeyondTrust continues to notify you of the latest builds as they become available . Whenever you receive notification that new update packages have been built for your B Series Appliance, clicking the **Check for Updates** button locates the packages and makes them available for you to install.

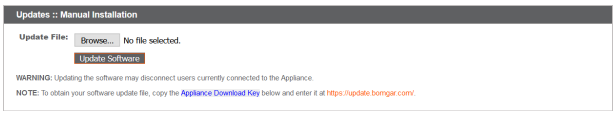


If multiple software packages have been built for your B Series Appliance, each one is listed separately in the list of available updates. Your new software is automatically downloaded and installed when you click the appropriate **Install This Update** button.

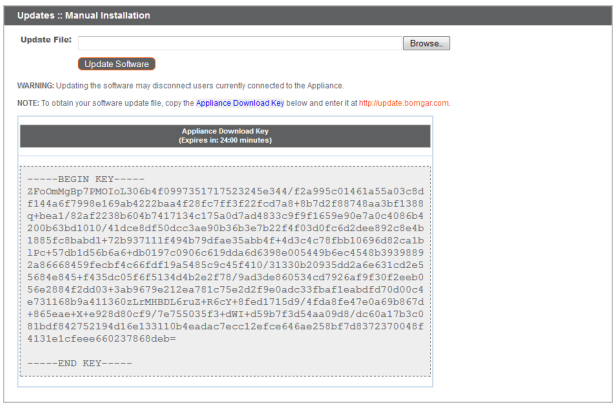
If no update packages or patches are available for your B Series Appliance, a message stating *No updates available* is displayed. If an update is available but an error occurred when distributing the update to your B Series Appliance, an additional message is displayed, such as, *An error occurred building your update. Please visit* www.beyondtrust.com/support *for more information.*



It is not mandatory to use this **Check for Updates** feature. If your organization's security policy does not allow for automatic update functionality, you can manually check for updates. Click the **Appliance Download Key** link to generate a unique B Series Appliance key, and then, from a non-restricted system, submit that key to BeyondTrust's update server at https://btupdate.com. Download any available updates to a removable storage device and then transfer those updates to a system from which you can manage your B Series Appliance.



After downloading a software package, browse to the file from the **Manual Installation** section, and then click the **Update Software** button to complete the installation.



©2003-2023 BeyondTrust Corporation. 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.

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.

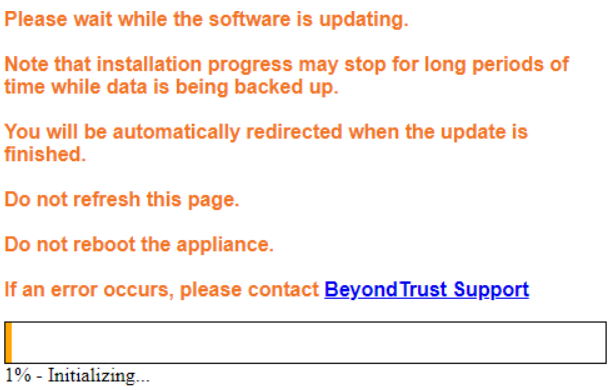
If you have any issues updating after accepting the EULA, please contact BeyondTrust Technical Support at www.beyondtrust.com/support.

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 users temporarily lose connection to any access sessions and the access 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 user connections.

Find current information about the latest BeyondTrust updates at https://www.beyondtrust.com/docs/release-notes/index.htm.

To view installed patches, under the **Updates** tab, select **Installed Patches**. The table shows all installed firmware patches and when they were installed.



©2003-2023 BeyondTrust Corporation. 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.

Support Utilities: Debug Network Problems

The **Utilities** section can be used for debugging network problems. If you are unable to establish a connection, these utilities may help to determine the reason:

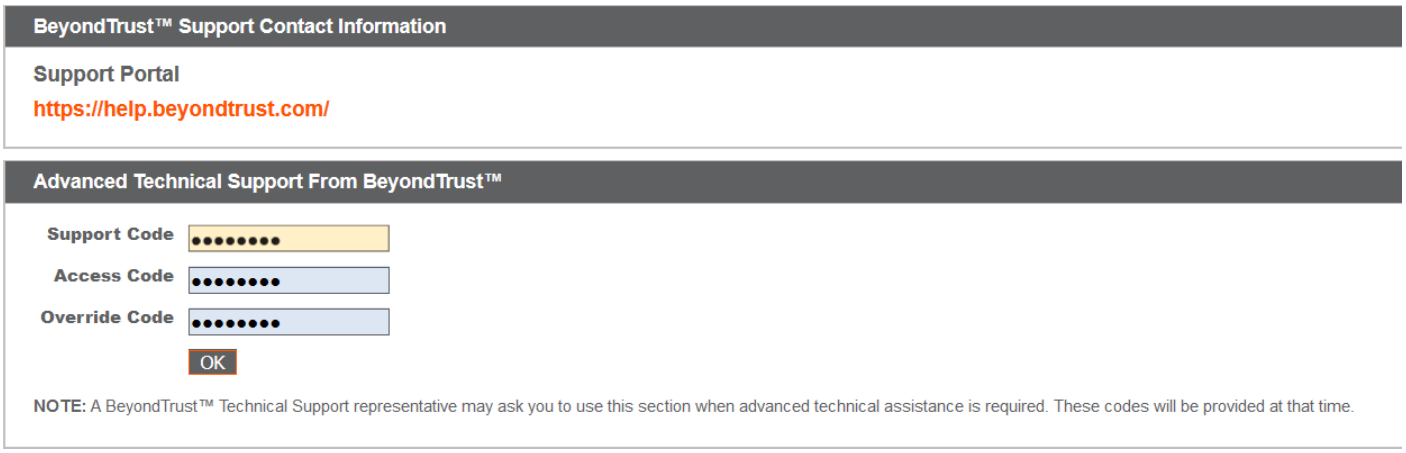
- Test your B Series Appliance's **DNS** resolution by performing a lookup of a hostname, or a reverse lookup of an IP address.
- **Ping** a hostname or IP address to test your B Series Appliance's network connectivity.
- Use the **Traceroute** to view the path that packets take on their journey from the B Series Appliance to any external system.
- Use the **TCP Connection Test** to check connectivity of a specific port on a target IP address or hostname.
- Use the **SSL/TLS Connection Test** to check connectivity to HTTPS or other TLS remote servers.

©2003-2023 BeyondTrust Corporation. 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.

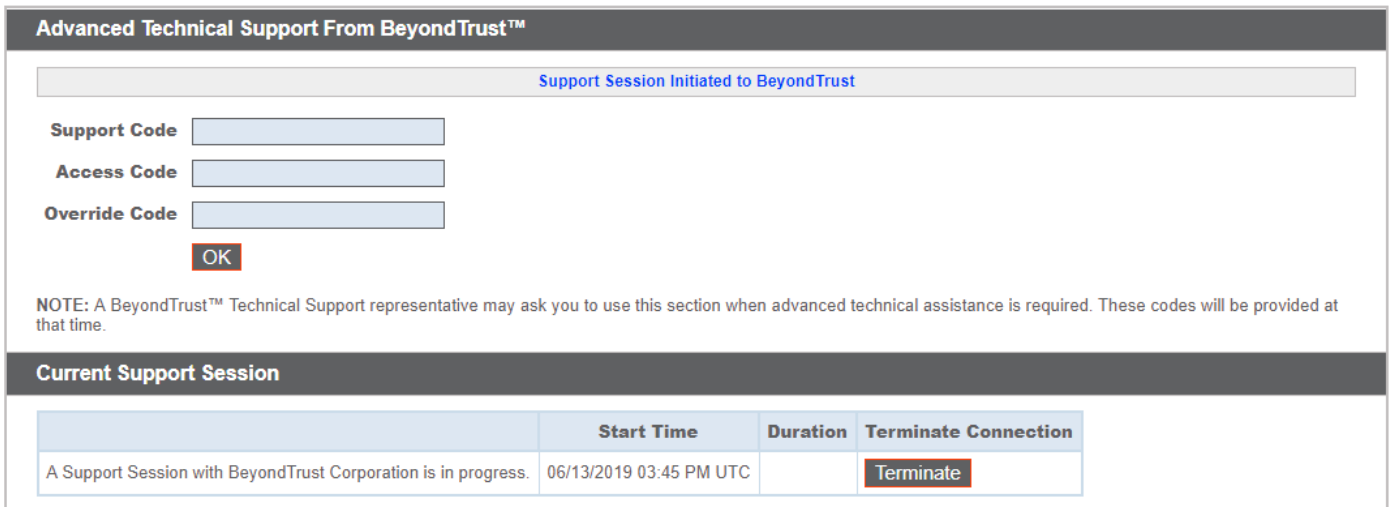
©2003-2023 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

Advanced Support: Contact BeyondTrust Technical Support

The **Advanced Support** section gives you contact information for your BeyondTrust Technical Support team and allows an appliance-initiated support tunnel back to BeyondTrust Technical Support, enabling quick resolution of complex issues.



If the **A Support Session with BeyondTrust Corporation in progress** section is visible, BeyondTrust Technical Support has an active session taking place with your B Series Appliance. The **Duration** column indicates how long BeyondTrust Technical Support has been in session with your B Series Appliance. To stop the session, click **Terminate**, and the tunnel between your B Series Appliance and BeyondTrust Technical Support closes.



©2003-2023 BeyondTrust Corporation. 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.