BeyondTrust

Privileged Remote Access
SSL Certificates

TC:3/4/2024

Table of Contents

SSL Certificates and BeyondTrust Privileged Remote Access

Before BeyondTrust can provide your custom software package, your B Series Appliance must have a valid SSL certificate installed. When properly installed, an SSL certificate validates the identity of your BeyondTrust site, and allows software such as web browsers and BeyondTrust clients to establish secure, encrypted connections.

Overview

To ensure full functionality of the BeyondTrust software and to avoid security risks, a valid SSL certificate signed by a third-party certificate authority (CA) must be installed.

> ***Note:*** *Without an SSL certificate that matches your BeyondTrust site's hostname, your users will experience security errors. If your site uses the factory default or a self-signed certificate, users attempting to access your BeyondTrust site will receive an error message warning them that your site is untrusted, and some software clients will not function at all.*

Installing the new certificate in BeyondTrust automatically links a private key to the new certificate, making the B Series Appliance ready to decrypt traffic from remote clients such as access consoles and web browsers. The private key and its certificate can be transferred between servers (e.g., from an IIS server to a B Series Appliance), but if it is ever lost, decryption will be impossible, the B Series Appliance will be unable to validate its integrity, and the certificate will have to be replaced.

BeyondTrust software clients which require the heightened security of a CA-signed certificate include:

- iOS and Android access consoles
- Linux software clients (access consoles, endpoint clients)

BeyondTrust does not require any special type of certificate, and allows both commercial or public certificate authority and internal CA servers. Accepted certificates include:

- Wildcard certificates
- Subject alternative name (SAN) certificates
- Unified Communications (UC) certificates
- Extended Validation (EV) certificates
- Other standard certificates

BeyondTrust also provides support for requesting a Let's Encrypt certificate directly from the B Series Appliance. Let's Encrypt issues signed certificates that are valid for 90 days at a time, and can automatically renew themselves indefinitely.

Temporary, self-signed certificates can also be used for testing or installations. Using a self-signed certificate in a production environment does not provide the security of a CA-signed certificate, and users attempting to access your BeyondTrust site will receive an error message warning them that your site is untrusted.

> *For more information, please see the following:*
>
> - *SSL certificate at https://en.wikipedia.org/wiki/Public_key_certificate*
> - *"Create a Certificate Signed by a Certificate Authority for Your BeyondTrust Appliance B Series" on page 7*.
> - *"Create a Self-Signed Certificate for Your BeyondTrust Appliance B Series" on page 4*

Create a Self-Signed Certificate for Your BeyondTrust Appliance B Series

A self-signed certificate can be used on a temporary basis for testing or installing a BeyondTrust Appliance B Series. Self-signed certificates do not provide the security or features of a certificate from a public certificate authority (CA). A CA-signed certificate is recommended for long-term or production environments.

Self-signed certificates are created in the BeyondTrust **/appliance** web interface. Once created, the BeyondTrust software must be updated by BeyondTrust Technical Support.

For more information, please see "Create a Certificate Signed by a Certificate Authority for Your BeyondTrust Appliance B Series" on page 7.

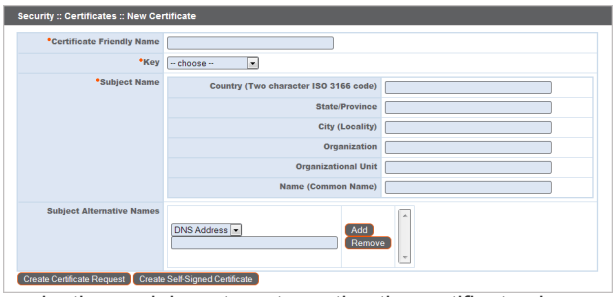
Create the Certificate

***Note:** Customers with a cloud site environment cannot create a self-signed certificate.*

Certificates consist of a **friendly name**, **key**, **subject name**, and one or more **subject alternative names**. You must enter this information in the BeyondTrust /appliance web interface to create a self-signed certificate.

1. Log into the /appliance web interface of your B Series Appliance and go to **Security > Certificates**.

2. Provide the following information to create your self-signed certificate:



- **Certificate Friendly Name**: A descriptive title used to identify your certificate request on the B Series Appliance **Security > Certificates** page. Examples could include your primary DNS name or the current month and year.
- **Key**: Select a key size from the dropdown. 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. If using a certificate authority, verify which key strengths they support.
- **Subject Name**: These fields consist of the contact information for the organization and department creating the certificate along with the name of the certificate.
    - **Country**: The two-character ISO 3166 country code for your organization. If you are unsure of your country code, please visit www.iso.org/iso-3166-country-codes.html.
    - **State/Province**: The full state or province name of your organization, if applicable.
    - **City (Locality)**: The city of your organization.
    - **Organization**: Your organization or company name.
    - **Organizational Unit**: The group or department within the organization managing the certificate and/or the BeyondTrust deployment for the organization.
    - **Name (Common Name)**: A human-readable title for your certificate. This name must be unique to differentiate the certificate from others on the network, which could include the public internet. It is not recommended that you use your DNS name as the common name.

- **Subject Alternative Names**: A list of the fully qualified domain names for each DNS A-record which resolves to your B Series Appliance (e.g., access.example.com). After entering each subject alternative name (SAN), click the **Add** button.

  A SAN lets you protect multiple hostnames with a single SSL certificate. A DNS address could be a fully qualified domain name, such as access.example.com, or it could be a wildcard domain name, such as *.example.com. A wildcard domain name covers multiple subdomains, such as access.example.com, remote.example.com, and so forth. If you are going to use multiple hostnames for your site that are not covered by a wildcard certificate, be sure to define those as additional SANs.

> ***Note:*** *If you entered the fully qualified domain name as your subject's common name, you must re-enter this as the first SAN entry. If you wish to use IP addresses instead of DNS names, contact BeyondTrust Technical Support first.*

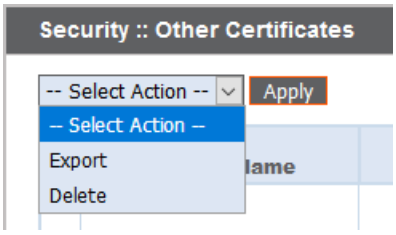
> ***Note:*** *If you plan to use multiple B Series Appliances in an Atlas setup, it is recommended that you use a wildcard certificate that covers both your BeyondTrust site hostname and each traffic node hostname. If you do not use a wildcard certificate, adding traffic nodes that use different certificates will require a rebuild of the BeyondTrust software.*

3. Click **Create Self-Signed Certificate** and wait for the page to refresh. The new certificate should now appear in the **Security :: Certificates** section.

Update the BeyondTrust Appliance B Series

To ensure the reliability of your client software, BeyondTrust Technical Support builds a copy of your certificate into your software. When you create a new certificate, you must send BeyondTrust Technical Support a copy of your certificate and also a screenshot of your **Status > Basics** page to identify the B Series Appliance being updated.

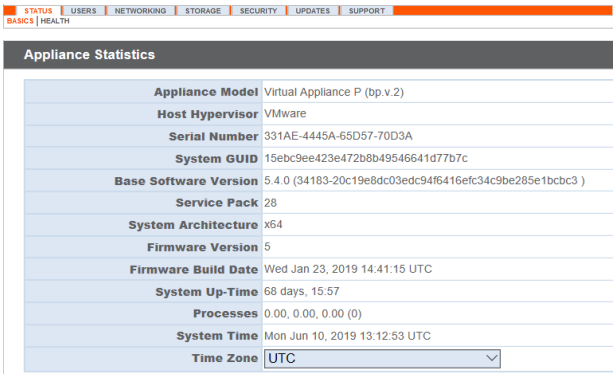
1. Go to **/appliance > Security > Certificates** and export a copy of your new certificate.
   a. Check the box next to the new certificate in the **Security :: Certificates** table.
   b. From the **Select Action** dropdown menu above the table, select **Export**. Then click **Apply**.
   c. Uncheck **Include Private Key**, click **Export**, and save the file to a convenient location.



IMPORTANT!

*Do NOT send your private key file (which ends in **.p12**) to BeyondTrust Technical Support. When exporting your certificate, you have the option to **Include Private Key**. If a certificate is being exported to be sent to BeyondTrust Technical Support, you should **NOT** check **Include Private Key**. This key is private because it allows the owner to authenticate your B Series Appliance's identity. Ensure that the private key and its passphrase are kept in a secure, well-documented location on your private network. If this key is ever exposed to the public (via email, for instance), the security of your B Series Appliance is compromised. Never export your private key when requesting software updates from BeyondTrust. A certificate without the private key usually exports as a file with the **.cer**, **.crt**, **.pem**, or **.p7b** extension. These files are safe to send by email and to share publicly. Exporting certificates does not remove them from the B Series Appliance.*

2. Go to **/appliance > Status > Basics** and take a screenshot of the page.
3. Add the saved screenshot and the exported certificate to a .zip archive.
4. Compose an email to BeyondTrust Technical Support requesting a software update. Attach the .zip archive containing the certificate and screenshot. If you have an open incident with Support, include your incident number in the email. Send the email.
5. Once BeyondTrust Technical Support has built your new software package, they will email you instructions for how to install it. Update your software following the emailed instructions.

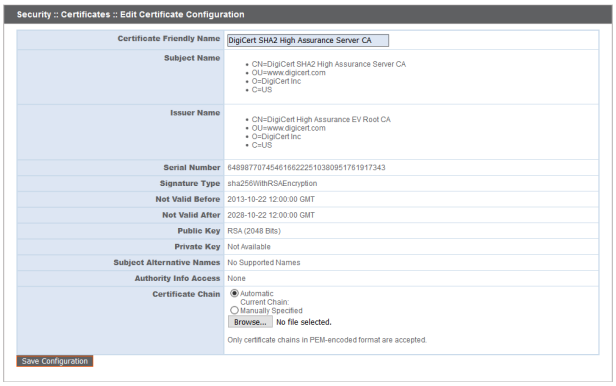


After these steps are complete, it is advisable to wait 24-48 hours before proceeding further. This allows time for your BeyondTrust client software (especially Jump Clients) to update themselves with the new certificate which BeyondTrust Technical Support included in your recent software update.

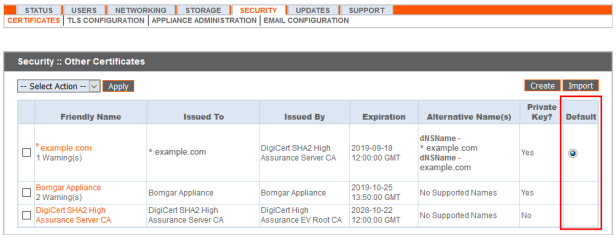
SSL Certificate Auto-Selection

BeyondTrust uses Server Name Indication (SNI), an extension to the TLS networking protocol, to allow any SSL certificate stored on the B Series Appliance to be served to any client. Because most TLS clients send SNI information at the start of the handshaking process, this enables the B Series Appliance to determine which SSL certificate to send back to a client that requests a connection.

You may choose a default certificate to serve to clients who do not send SNI information with their request, or to clients who do send SNI information, but which does not match anything in the B Series Appliance database.



1. Go to **/appliance > Security > Certificates**.
2. In the Default column, select the radio button for the certificate you wish to make default.



Once your certificate is installed and your appliance is updated, the B Series Appliance should be operational and ready for testing.

> *For information on long-term or production deployment, see "Create a Certificate Signed by a Certificate Authority for Your BeyondTrust Appliance B Series" on page 7.*

Create a Certificate Signed by a Certificate Authority for Your BeyondTrust Appliance B Series

To ensure full functionality of the BeyondTrust software and to avoid security risks, a valid SSL certificate signed by a certificate authority (CA) must be installed. A certificate authority acts to store, sign, and issue SSL certificates, allowing clients to establish secure, encrypted connections to your BeyondTrust site.

> ***Note:*** *While a CA-signed certificate is the best way to secure your site, a self-signed certificate or an internally-signed certificate will allow temporary access for testing or deployment. For more information, please see "Create a Self-Signed Certificate for Your BeyondTrust Appliance B Series" on page 4.*

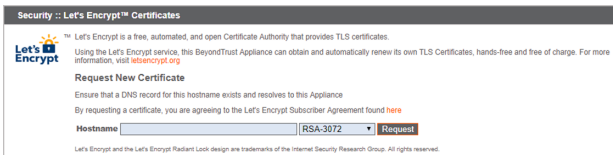
To obtain a certificate signed by a certificate authority, you must first create a certificate signing request (CSR) from the **/appliance** interface of your B Series Appliance, and then submit the request data to a certificate authority. Once the signed certificate is obtained, the BeyondTrust software might need to be updated by the BeyondTrust Technical Support team.

Obtain a Free TLS Certificate from 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

certificates for failover B Series Appliance pairs.

For more information, please see letsencrypt.org.

Create a Certificate Signing Request

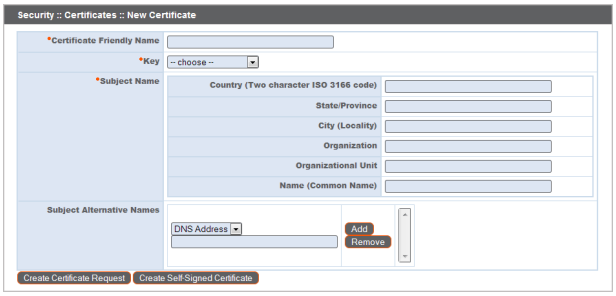
When using a CA issuer other than Let's Encrypt, a certificate signing request, or CSR, must first be created. The data associated with the CSR contains the details about your organization and BeyondTrust site, which is then submitted to your certificate authority. The CA can then publicly certify your organization and B Series Appliance.

Certificates consist of a **friendly name**, **key**, **subject name**, and one or more **subject alternative names**. You must enter this information in the BeyondTrust /appliance web interface to create a certificate signing request.

1. Log into the /appliance web interface of your B Series Appliance and go to **Security > Certificates**.

2. Provide the following information to create your self-signed certificate:

- **Certificate Friendly Name**: A descriptive title used to identify your certificate request on the B Series Appliance **Security > Certificates** page. Examples could include your primary DNS name or the current month and year.
- **Key**: Select a key size from the dropdown. 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. If using a certificate authority, verify which key strengths they support.



3. **Subject Name**: These fields consist of the contact information for the organization and department creating the certificate along with the name of the certificate.

    - **Country**: The two-character ISO 3166 country code for your organization. If you are unsure of your country code, please visit www.iso.org/iso-3166-country-codes.html.
    - **State/Province**: The full state or province name of your organization, if applicable.
    - **City (Locality)**: The city of your organization.
    - **Organization**: Your organization or company name.
    - **Organizational Unit**: The group or department within the organization managing the certificate and/or the BeyondTrust deployment for the organization.
    - **Name (Common Name)**: A human-readable title for your certificate. This name must be unique to differentiate the certificate from others on the network, which could include the public internet. It is not recommended that you use your DNS name as the common name. However, some certificate authorities may require that you do use your fully qualified DNS name for backward compatibility. Contact your certificate authority for details.

- **Subject Alternative Names**: A list of the fully qualified domain names for each DNS A-record which resolves to your B Series Appliance (e.g., access.example.com). After entering each subject alternative name (SAN), click the **Add** button.

  A SAN lets you protect multiple hostnames with a single SSL certificate. A DNS address could be a fully qualified domain name, such as access.example.com, or it could be a wildcard domain name, such as *.example.com. A wildcard domain name covers multiple subdomains, such as access.example.com, remote.example.com, and so forth. If you are going to use multiple hostnames for your site that are not covered by a wildcard certificate, be sure to define those as additional SANs.

> ***Note:*** *If you entered the fully qualified domain name as your subject's common name, you must re-enter this as the first SAN entry. If you wish to use IP addresses instead of DNS names, contact BeyondTrust Technical Support first.*

> ***Note:*** *If you plan to use multiple B Series Appliances in an Atlas setup, it is recommended that you use a wildcard certificate that covers both your BeyondTrust site hostname and each traffic node hostname. If you do not use a wildcard certificate, adding traffic nodes that use different certificates will require a rebuild of the BeyondTrust software.*

4. Click **Create Certificate Request** and wait for the page to refresh.
5. The certificate request should now appear in the **Certificate Requests** section.

Submit the Certificate Signing Request

Once the certificate signing request has been created, you must submit it to a certificate authority for certification. You can obtain an SSL certificate from a commercial or public certificate authority or from an internal CA server if your organization uses one. BeyondTrust does not require or recommend any specific certificate authority, but common providers include:

- Sectigo (www.sectigo.com/) - Sectigo is the one of the largest issuers of SSL certificates.
- Digicert (www.digicert.com) - Digicert is a US-based certificate authority that has been in business for over two decades.
- GeoTrust, Inc. (www.geotrust.com) - GeoTrust is the world's second largest digital certificate provider.
- GoDaddy SSL (www.godaddy.com/web-security/ssl-certificate) - GoDaddy is the world's largest domain name registrar, and their SSL certificates are widely used.

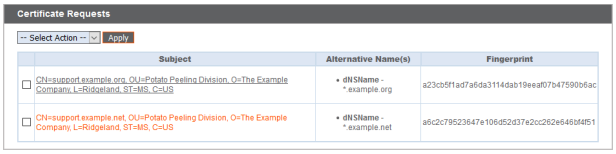
Once you have selected a certificate authority, you must purchase a certificate from them.

BeyondTrust does not require any special type of certificate, and allows both commercial or public certificate authority and internal CA servers. Accepted certificates include:

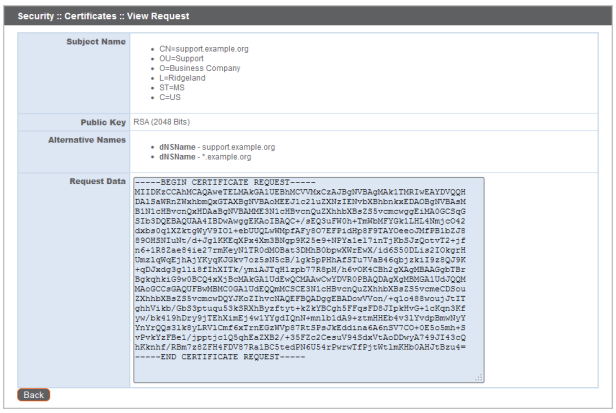
- Wildcard certificates
- Subject alternative name (SAN) certificates
- Unified Communications (UC) certificates
- Extended Validation (EV) certificates
- Other standard certificates

During or after the purchase, you will be prompted to upload or copy/paste your request data. The certificate authority should give you instructions for doing so. To retrieve your request data from BeyondTrust, take these steps:

1. When prompted to submit the request information, log into the /appliance interface of your B Series Appliance. Go to **Security > Certificates**.
2. In the **Certificate Requests** section, click the subject of your certificate request.



3. Select and copy the **Request Data**, and then submit this information to your certificate authority. Some certificate authorities require you to specify the type of server the certificate is for. If this is a required field, submit that the server is Apache-compatible. If given more than one Apache type as options, select Apache/ModSSL or Apache (Linux).



Import the Certificate

Once the certificate authority has the request data, they will review, sign, and return the certificate to you, often with root and/or intermediate certificate files. All these together constitute your certificate chain, which proves your certificate was issued by the CA. The certificate chain typically includes three types of certificate:

- Root Certificate – The certificate that identifies the certificate authority.
- Intermediate Root Certificates – Certificates digitally signed and issued by an Intermediate CA, also called a *Signing CA* or *Subordinate CA*.
- Identity Certificate – A certificate that links a public key value to a real-world entity such as a person, a computer, or a web server.

All of these certificate files must be imported to your B Series Appliance before it will be completely operational.

1. Download all of the certificate files in your certificate chain to a secure location. This location should be accessible from the same computer used to access the /appliance interface. Sometimes the CA's certificate download interface prompts for a server type. If prompted to select a server type, select Apache. If given more than one Apache type as options, select Apache/ModSSL

   The certificate chain will be sent in one of multiple certificate file formats. The following certificate formats are acceptable:

   - DER-encoded X.509 certificate (.cer, .der, .crt)
   - PEM-wrapped DER-encoded X.509 certificate (.pem, .crt, .b64)
   - DER-encoded PKCS #7 certificates (.p7, .p7b, .p7c)

Note: *Many certificate authorities do not send the root certificate of your certificate chain. BeyondTrust requires this root certificate to function properly. If no links were provided to obtain the root certificate, contact your CA for assistance, or find the correct root certificate in your CA's online root certificate repository. Some major repositories include:*

- *Sectigo > Technical Documents > Root Certificates (www.sectigo.com/resource-library/sectigo-root-intermediate-certificate-files)*
- *DigiCert Trusted Root Authority Certificates (www.digicert.com/digicert-root-certificates.htm)*
- *GeoTrust Root Certificates (https://www.digicert.com/kb/digicert-root-certificates.htm)*
- *GoDaddy > Repository (certs.godaddy.com/repository)*

On most systems, it is also possible to open the certificate file and check the certificate chain manually. Follow the recommendations for your operating system to identify the root certificate from a provided certificate chain.

2. Once you have downloaded all the certificate files for your certificate chain, you must import these files to your B Series Appliance:
   - Log into the /appliance interface of your BeyondTrust Appliance B Series. Go to **Security > Certificates**
   - In the **Security :: Other Certificates** section, click the **Import** button.
   - Browse to your certificate file and click **Upload**. Then upload the intermediate certificate files and root certificate file used by the CA.

Your signed certificate should now appear in the **Security :: Other Certificates** section. If the new certificate shows a warning beneath its name, this typically means the intermediate and/or root certificates from the CA have not been imported. The components of the certificate chain can be identified as follows:

- The BeyondTrust server certificate has an **Issued To** field and/or an **Alternative Name(s)** field matching the B Series Appliance's URL (e.g., access.example.com).
- Intermediate certificates have different **Issued To** and **Issued By** fields, neither of which is a URL.
- The root certificate has identical values for the **Issued To** and **Issued By** fields, neither of which is a URL.

If any of these are missing, contact your certificate authority and/or follow the instructions given above in this guide to locate, download, and import the missing certificates.

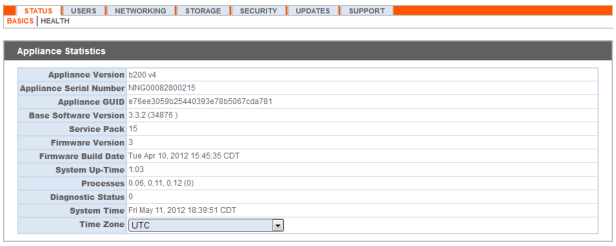
Update the BeyondTrust Appliance B Series

BeyondTrust software automatically trusts certificates issued by certificate authorities in your operating system's native CA trust store. If you obtain a self-signed certificate, or a certificate issued by an authority not trusted on all platforms, BeyondTrust Technical Support must build a copy of your certificate into your software. To update your appliance, send BeyondTrust Technical Support a copy of the new SSL certificate, as well as a screenshot of your **Status > Basics** page to identify the B Series Appliance being updated.

IMPORTANT!

*Do NOT send your private key file (which ends in **.p12**) to BeyondTrust Technical Support. This key is private because it allows the owner to authenticate your B Series Appliance's identity. Ensure that the private key and its passphrase are kept in a secure, well-documented location on your private network. If this key is ever exposed to the public (via email, for instance), the security of your B Series Appliance is compromised.*

1. Go to **/appliance > Status > Basics** and take a screenshot of the page.
2. Add the saved screenshot and the all of the SSL certificates files for your certificate chain to a .zip archive. Do NOT include any private key files (e.g., **.p12**, **.pfx**, or **.key** files).
3. Compose an email to BeyondTrust Technical Support requesting a software update. Attach the .zip archive containing the certificate files and screenshot. If you have an open incident with Support, include your incident number in the email. Send the email.



4. Once BeyondTrust Technical Support has built your new software package, they will email you instructions for how to install it. Update your software following the emailed instructions.

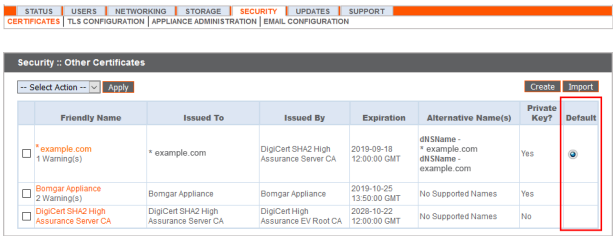
After these steps are complete, it is advisable to wait 24-48 hours before proceeding further. This allows time for your BeyondTrust client software (especially Jump Clients) to update themselves with the new certificate which BeyondTrust Technical Support included in your recent software update.

SSL Certificate Auto-Selection

BeyondTrust uses Server Name Indication (SNI), an extension to the TLS networking protocol, to allow any SSL certificate stored on the B Series Appliance to be served to any client. Because most TLS clients send SNI information at the start of the handshaking process, this enables the B Series Appliance to determine which SSL certificate to send back to a client that requests a connection.

You may choose a default certificate to serve to clients who do not send SNI information with their request, or to clients who do send SNI information, but which does not match anything in the B Series Appliance database.

1. Go to **/appliance > Security > Certificates**.
2. In the Default column, select the radio button for the certificate you wish to make default.



At this point, the B Series Appliance should be fully operational and ready for production. To learn more about how to manage and use BeyondTrust, please refer to www.beyondtrust.com/docs.

Copy the SSL Certificate to Privileged Remote Access Failover and Atlas B Series Appliances

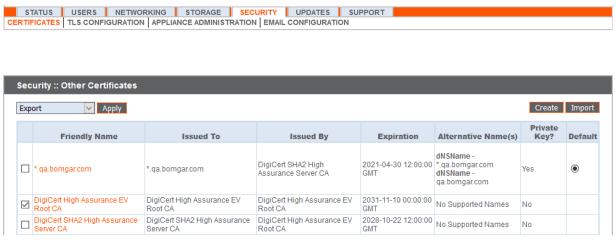
BeyondTrust allows you to use additional B Series Appliances for failover or for load balancing. If you intend to use additional B Series Appliances in your setup, it is important that each additional B Series Appliance is properly secured by an SSL certificate.

In a failover setup, the primary and backup B Series Appliances must have identical SSL certificates for the backup B Series Appliance to connect to the main BeyondTrust site hostname. The CA-signed certificate must support each B Series Appliance's unique hostname, as well as the main BeyondTrust site hostname. This certificate can then be replicated on both the primary and the backup B Series Appliances.

If using an Atlas setup, it is recommended that you use a wildcard certificate that covers both your BeyondTrust site name and each traffic node hostname. If you do not use a wildcard certificate, then adding traffic nodes that use different certificates may require a rebuild of the BeyondTrust software. Therefore, you should create a CA-signed wildcard certificate that supports all of the hostnames used in your Atlas setup. Replicate this certificate on each of your Atlas clustered B Series Appliances.

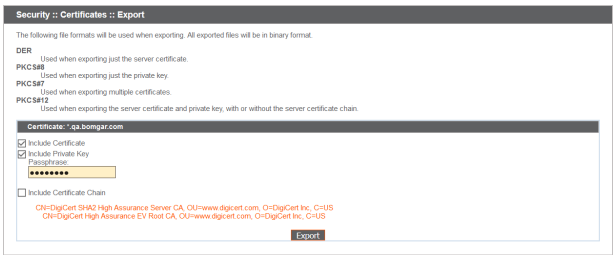
Export the Certificate

1. On the primary B Series Appliance, log into the /appliance interface. Go to **Security > Certificates**.
2. In the **Security :: Certificates** section, check the box beside the certificate that is assigned to the active IP address. Then, from the dropdown menu at the top of this section, select **Export**.



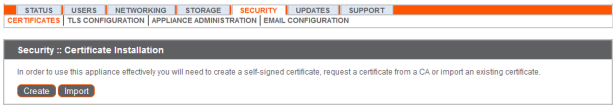
> ***Note:*** *Exporting certificates does not remove them from the B Series Appliance.*

3. On the **Security :: Certificates :: Export** page, check the options to include the certificate, the private key, and the certificate chain. It is strongly recommended that you set a passphrase for the private key.

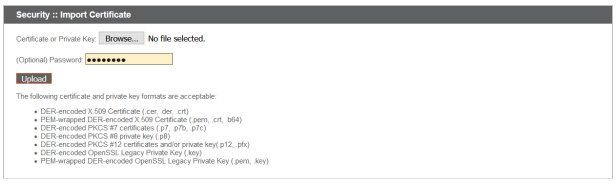


Import the Certificate

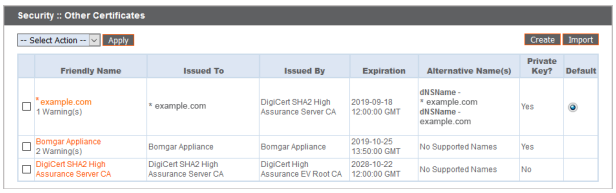
1. On the backup B Series Appliance, log into the /appliance interface. Go to **Security > Certificates**.
2. In the **Security :: Other Certificates** section, click the **Import** button.



3. Browse to the certificate file you just exported from the primary B Series Appliance. If a passphrase was assigned to the file, enter it in the **Password** field. Then click **Upload**.



4. The imported certificate chain should now appear in the **Security :: Other Certificates** section.
5. Repeat the import process for each additional clustered B Series Appliance.



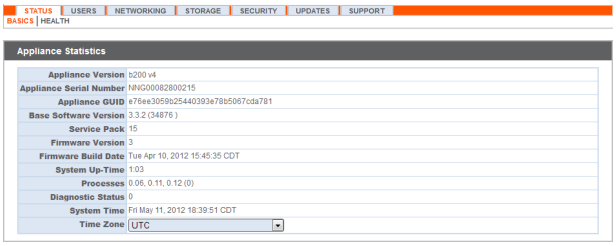
Update the BeyondTrust Appliance B Series

BeyondTrust software automatically trusts certificates issued by certificate authorities in your operating system's native CA trust store. If you obtain a self-signed certificate, or a certificate issued by an authority not trusted on all platforms, BeyondTrust Technical Support must build a copy of your certificate into your software. To update your appliance, send BeyondTrust Technical Support a copy of the new SSL certificate, as well as a screenshot of your **Status > Basics** page to identify the B Series Appliance being updated.

IMPORTANT!

*Do NOT send your private key file (which ends in **.p12**) to BeyondTrust Technical Support. This key is private because it allows the owner to authenticate your B Series Appliance's identity. Ensure that the private key and its passphrase are kept in a secure, well-documented location on your private network. If this key is ever exposed to the public (via email, for instance), the security of your B Series Appliance is compromised.*

1. Go to **/appliance > Status > Basics** and take a screenshot of the page.
2. Add the saved screenshot and the all of the SSL certificates files for your certificate chain to a .zip archive. Do NOT include any private key files (e.g., **.p12**, **.pfx**, or **.key** files).
3. Compose an email to BeyondTrust Technical Support requesting a software update. Attach the .zip archive containing the certificate files and screenshot. If you have an open incident with Support, include your incident number in the email. Send the email.



4. Once BeyondTrust Technical Support has built your new software package, they will email you instructions for how to install it. Update your software following the emailed instructions.
5. Repeat the update process for each additional clustered B Series Appliance.

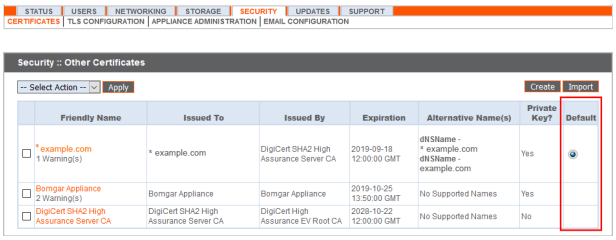
After these steps are complete, it is advisable to wait 24-48 hours before proceeding further. This allows time for your BeyondTrust client software (especially Jump Clients) to update themselves with the new certificate which BeyondTrust Technical Support included in your recent software update.

SSL Certificate Auto-Selection

BeyondTrust uses Server Name Indication (SNI), an extension to the TLS networking protocol, to allow any SSL certificate stored on the B Series Appliance to be served to any client. Because most TLS clients send SNI information at the start of the handshaking process, this enables the B Series Appliance to determine which SSL certificate to send back to a client that requests a connection.

You may choose a default certificate to serve to clients who do not send SNI information with their request, or to clients who do send SNI information, but which does not match anything in the B Series Appliance database.

1. Go to **/appliance > Security > Certificates**.
2. In the Default column, select the radio button for the certificate you wish to make default.



Renew an Expired Certificate for the BeyondTrust Appliance B Series

If the SSL certificate of your B Series Appliance is about to expire, you must renew it following the instructions below. If you need to replace an existing certificate with one from another certificate authority, see "Replace an SSL Certificate on the BeyondTrust Appliance B Series" on page 18.

IMPORTANT!

Because the software on the B Series Appliance is built for your specific SSL certificate, please be proactive in contacting BeyondTrust Technical Support before your SSL certificate expires. This way, BeyondTrust Technical Support can build software to help migrate your connections.

The steps below will guide you through renewing a CA-signed certificate.

Purchase the Certificate Renewal

1. Contact the certificate authority that signed your existing certificate to request a renewal.

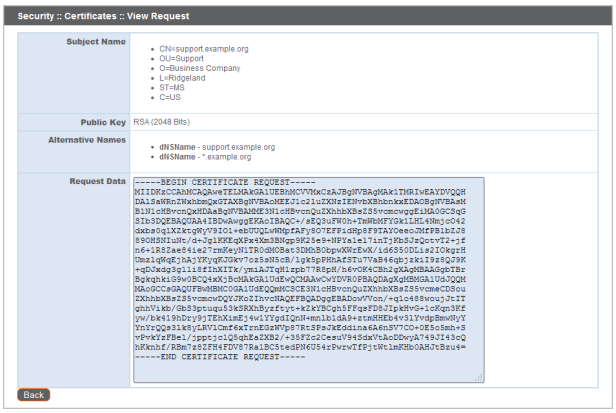
   When a certificate is renewed, the original certificate data is used. You do not need to create a new certificate request, and no new intermediate or root certificates need to be installed.

2. Many CAs keep the certificate request information on file. Others may require you to provide the original certificate request.

   If the CA requires a copy of the original certificate request, go to the **/appliance > Security > Certificates** page.

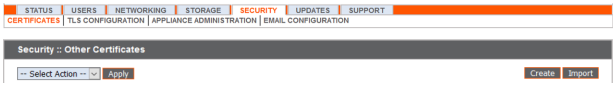
   a. In the **Security :: Certificate Requests** section, click the subject of the certificate request which matches the original certificate's data.

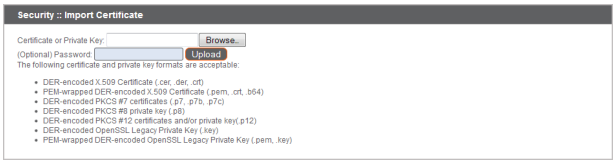
   b. Select and copy the **Request Data**, and then submit this information to your certificate authority.



Import the Certificate Files

1. Once the certificate authority has responded to the request with the new certificate files, download all of the files to a secure location. This location should be accessible from the same computer used to access the /appliance interface.
2. Log into the /appliance interface of your BeyondTrust Appliance B Series. Go to **Security > Certificates**.
3. In the **Security :: Other Certificates** section, click the **Import** button.
4. Browse to your new certificate file and click **Upload**.
5. Your renewed certificate should now appear in the **Security :: Certificates** section. This new certificate can be identified by its **Expiration**, since this will be a later date than the original certificate.



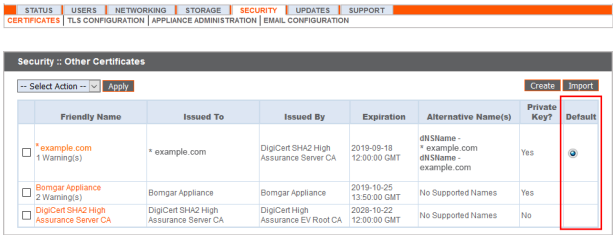


SSL Certificate Auto-Selection

BeyondTrust uses Server Name Indication (SNI), an extension to the TLS networking protocol, to allow any SSL certificate stored on the B Series Appliance to be served to any client. Because most TLS clients send SNI information at the start of the handshaking process, this enables the B Series Appliance to determine which SSL certificate to send back to a client that requests a connection.

You may choose a default certificate to serve to clients who do not send SNI information with their request, or to clients who do send SNI information, but which does not match anything in the B Series Appliance database.

1. Go to **/appliance > Security > Certificates**.
2. In the Default column, select the radio button for the certificate you wish to make default.



At this point, the B Series Appliance should be fully upgraded and operational with its new certificate. The old certificate may be removed and/or revoked as necessary.

Replace an SSL Certificate on the BeyondTrust Appliance B Series

BeyondTrust client software must be able to validate the SSL certificate of their B Series Appliance in order to establish secure connections. If your certificate authority must be changed for any reason, your B Series Appliance must be updated with a new product software package from BeyondTrust Technical Support provisioned with your new CA-signed certificate. If the CA is changed without preparing the clients beforehand, it is possible to permanently lose connectivity to the clients due to failed SSL validation.

Follow the instructions in this section to perform any of the following:

- Replace a CA-signed certificate from one certificate authority with a CA-signed certificate from another.
- Replace a self-signed certificate with a CA-signed certificate.
- Replace one type of CA-signed certificate with another type of CA-signed certificate from the same certificate authority.

For information on how too renew an existing CA-signed certificate from the same CA, please see "Renew an Expired Certificate for the BeyondTrust Appliance B Series" on page 16

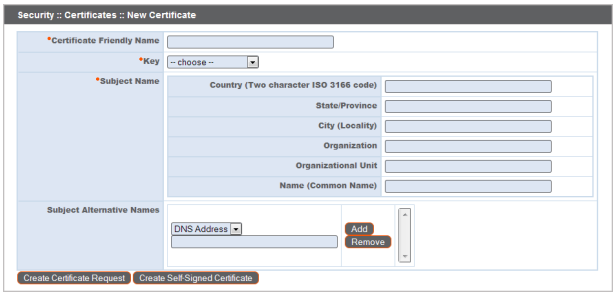
Create a Certificate Signing Request

When using a CA issuer other than Let's Encrypt, a certificate signing request, or CSR, must first be created. The data associated with the CSR contains the details about your organization and BeyondTrust site, which is then submitted to your certificate authority. The CA can then publicly certify your organization and B Series Appliance.

Certificates consist of a **friendly name**, **key**, **subject name**, and one or more **subject alternative names**. You must enter this information in the BeyondTrust /appliance web interface to create a certificate signing request.

1. Log into the /appliance web interface of your B Series Appliance and go to **Security > Certificates**.

2. Provide the following information to create your self-signed certificate:



- **Certificate Friendly Name**: A descriptive title used to identify your certificate request on the B Series Appliance **Security > Certificates** page. Examples could include your primary DNS name or the current month and year.
- **Key**: Select a key size from the dropdown. 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. If using a certificate authority, verify which key strengths they support.

3. **Subject Name**: These fields consist of the contact information for the organization and department creating the certificate along with the name of the certificate.
    - **Country**: The two-character ISO 3166 country code for your organization. If you are unsure of your country code, please visit www.iso.org/iso-3166-country-codes.html.
    - **State/Province**: The full state or province name of your organization, if applicable.
    - **City (Locality)**: The city of your organization.

- **Organization**: Your organization or company name.
- **Organizational Unit**: The group or department within the organization managing the certificate and/or the BeyondTrust deployment for the organization.
- **Name (Common Name)**: A human-readable title for your certificate. This name must be unique to differentiate the certificate from others on the network, which could include the public internet. It is not recommended that you use your DNS name as the common name. However, some certificate authorities may require that you do use your fully qualified DNS name for backward compatibility. Contact your certificate authority for details.

- **Subject Alternative Names**: A list of the fully qualified domain names for each DNS A-record which resolves to your B Series Appliance (e.g., access.example.com). After entering each subject alternative name (SAN), click the **Add** button.

  A SAN lets you protect multiple hostnames with a single SSL certificate. A DNS address could be a fully qualified domain name, such as access.example.com, or it could be a wildcard domain name, such as *.example.com. A wildcard domain name covers multiple subdomains, such as access.example.com, remote.example.com, and so forth. If you are going to use multiple hostnames for your site that are not covered by a wildcard certificate, be sure to define those as additional SANs.

Note: *If you entered the fully qualified domain name as your subject's common name, you must re-enter this as the first SAN entry. If you wish to use IP addresses instead of DNS names, contact BeyondTrust Technical Support first.*

Note: *If you plan to use multiple B Series Appliances in an Atlas setup, it is recommended that you use a wildcard certificate that covers both your BeyondTrust site hostname and each traffic node hostname. If you do not use a wildcard certificate, adding traffic nodes that use different certificates will require a rebuild of the BeyondTrust software.*

4. Click **Create Certificate Request** and wait for the page to refresh.
5. The certificate request should now appear in the **Certificate Requests** section.

Submit the Certificate Signing Request

Once the certificate signing request has been created, you must submit it to a certificate authority for certification. You can obtain an SSL certificate from a commercial or public certificate authority or from an internal CA server if your organization uses one. BeyondTrust does not require or recommend any specific certificate authority, but common providers include:

- Sectigo (www.sectigo.com/) - Sectigo is the one of the largest issuers of SSL certificates.
- Digicert (www.digicert.com) - Digicert is a US-based certificate authority that has been in business for over two decades.
- GeoTrust, Inc. (www.geotrust.com) - GeoTrust is the world's second largest digital certificate provider.
- GoDaddy SSL (www.godaddy.com/web-security/ssl-certificate) - GoDaddy is the world's largest domain name registrar, and their SSL certificates are widely used.

Once you have selected a certificate authority, you must purchase a certificate from them.

BeyondTrust does not require any special type of certificate, and allows both commercial or public certificate authority and internal CA servers. Accepted certificates include:

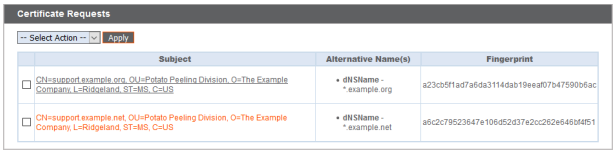
- Wildcard certificates
- Subject alternative name (SAN) certificates
- Unified Communications (UC) certificates

- Extended Validation (EV) certificates
- Other standard certificates

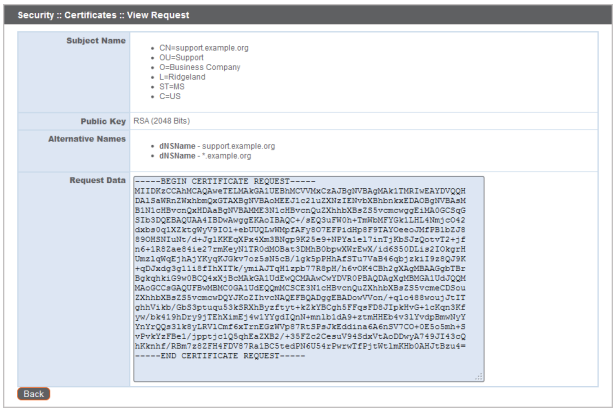
During or after the purchase, you will be prompted to upload or copy/paste your request data. The certificate authority should give you instructions for doing so. To retrieve your request data from BeyondTrust, take these steps:

1. When prompted to submit the request information, log into the /appliance interface of your B Series Appliance. Go to **Security > Certificates**.

2. In the **Certificate Requests** section, click the subject of your certificate request.



3. Select and copy the **Request Data**, and then submit this information to your certificate authority. Some certificate authorities require you to specify the type of server the certificate is for. If this is a required field, submit that the server is Apache-compatible. If given more than one Apache type as options, select Apache/ModSSL or Apache (Linux).



Import the Certificate

Once the certificate authority has the request data, they will review, sign, and return the certificate to you, often with root and/or intermediate certificate files. All these together constitute your certificate chain, which proves your certificate was issued by the CA. The certificate chain typically includes three types of certificate:

- Root Certificate – The certificate that identifies the certificate authority.
- Intermediate Root Certificates – Certificates digitally signed and issued by an Intermediate CA, also called a *Signing CA* or *Subordinate CA*.
- Identity Certificate – A certificate that links a public key value to a real-world entity such as a person, a computer, or a web server.

All of these certificate files must be imported to your B Series Appliance before it will be completely operational.

1. Download all of the certificate files in your certificate chain to a secure location. This location should be accessible from the same computer used to access the /appliance interface. Sometimes the CA's certificate download interface prompts for a server type. If prompted to select a server type, select Apache. If given more than one Apache type as options, select Apache/ModSSL

   The certificate chain will be sent in one of multiple certificate file formats. The following certificate formats are acceptable:

   - DER-encoded X.509 certificate (.cer, .der, .crt)

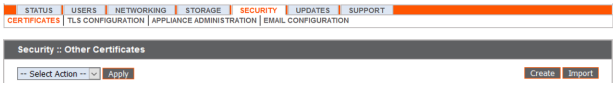
- PEM-wrapped DER-encoded X.509 certificate (.pem, .crt, .b64)
- DER-encoded PKCS #7 certificates (.p7, .p7b, .p7c)

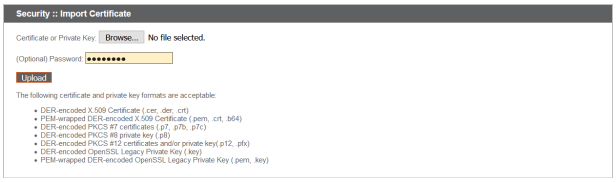
Note: *Many certificate authorities do not send the root certificate of your certificate chain. BeyondTrust requires this root certificate to function properly. If no links were provided to obtain the root certificate, contact your CA for assistance, or find the correct root certificate in your CA's online root certificate repository. Some major repositories include:*

- *Sectigo > Technical Documents > Root Certificates (www.sectigo.com/resource-library/sectigo-root-intermediate-certificate-files)*
- *DigiCert Trusted Root Authority Certificates (www.digicert.com/digicert-root-certificates.htm)*
- *GeoTrust Root Certificates (https://www.digicert.com/kb/digicert-root-certificates.htm)*
- *GoDaddy > Repository (certs.godaddy.com/repository)*

On most systems, it is also possible to open the certificate file and check the certificate chain manually. Follow the recommendations for your operating system to identify the root certificate from a provided certificate chain.

2. Once you have downloaded all the certificate files for your certificate chain, you must import these files to your B Series Appliance:
   - Log into the /appliance interface of your BeyondTrust Appliance B Series. Go to **Security > Certificates**
   - In the **Security :: Other Certificates** section, click the **Import** button.
   - Browse to your certificate file and click **Upload**. Then upload the intermediate certificate files and root certificate file used by the CA.





Your signed certificate should now appear in the **Security :: Other Certificates** section. If the new certificate shows a warning beneath its name, this typically means the intermediate and/or root certificates from the CA have not been imported. The components of the certificate chain can be identified as follows:

- The BeyondTrust server certificate has an **Issued To** field and/or an **Alternative Name(s)** field matching the B Series Appliance's URL (e.g., access.example.com).
- Intermediate certificates have different **Issued To** and **Issued By** fields, neither of which is a URL.
- The root certificate has identical values for the **Issued To** and **Issued By** fields, neither of which is a URL.

If any of these are missing, contact your certificate authority and/or follow the instructions given above in this guide to locate, download, and import the missing certificates.

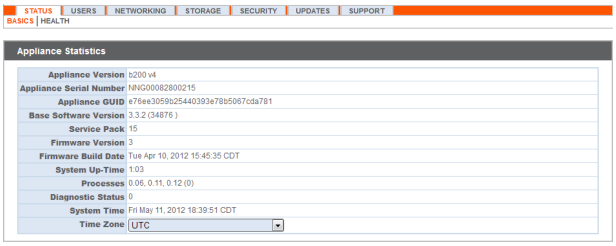
Update the BeyondTrust Appliance B Series

BeyondTrust software automatically trusts certificates issued by certificate authorities in your operating system's native CA trust store. If you obtain a self-signed certificate, or a certificate issued by an authority not trusted on all platforms, BeyondTrust Technical Support must build a copy of your certificate into your software. To update your appliance, send BeyondTrust Technical Support a copy of the new SSL certificate, as well as a screenshot of your **Status > Basics** page to identify the B Series Appliance being updated.

IMPORTANT!

*Do NOT send your private key file (which ends in **.p12**) to BeyondTrust Technical Support. This key is private because it allows the owner to authenticate your B Series Appliance's identity. Ensure that the private key and its passphrase are kept in a secure, well-documented location on your private network. If this key is ever exposed to the public (via email, for instance), the security of your B Series Appliance is compromised.*

1. Go to **/appliance > Status > Basics** and take a screenshot of the page.
2. Add the saved screenshot and the all of the SSL certificates files for your certificate chain to a .zip archive. Do NOT include any private key files (e.g., **.p12**, **.pfx**, or **.key** files).
3. Compose an email to BeyondTrust Technical Support requesting a software update. Attach the .zip archive containing the certificate files and screenshot. If you have an open incident with Support, include your incident number in the email. Send the email.
4. Once BeyondTrust Technical Support has built your new software package, they will email you instructions for how to install it. Update your software following the emailed instructions.



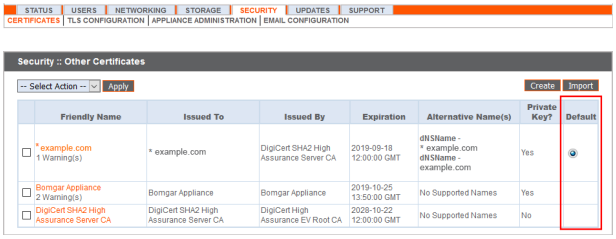
After these steps are complete, it is advisable to wait 24-48 hours before proceeding further. This allows time for your BeyondTrust client software (especially Jump Clients) to update themselves with the new certificate which BeyondTrust Technical Support included in your recent software update.

SSL Certificate Auto-Selection

BeyondTrust uses Server Name Indication (SNI), an extension to the TLS networking protocol, to allow any SSL certificate stored on the B Series Appliance to be served to any client. Because most TLS clients send SNI information at the start of the handshaking process, this enables the B Series Appliance to determine which SSL certificate to send back to a client that requests a connection.

You may choose a default certificate to serve to clients who do not send SNI information with their request, or to clients who do send SNI information, but which does not match anything in the B Series Appliance database.

1. Go to **/appliance > Security > Certificates**.
2. In the Default column, select the radio button for the certificate you wish to make default.



At this point, the B Series Appliance should be fully upgraded and operational with its new certificate. The old certificate may be removed and/or revoked as necessary.