BeyondTrust

Privileged Remote Access
SSL Certificates

TC:5/14/2019

Table of Contents

SSL Certificates and BeyondTrust Privileged Remote Access

In this guide, you will learn about the role of SSL certificates in BeyondTrust — why they are needed and how to use them.

Before BeyondTrust can provide your custom software package, your BeyondTrust Appliance must have a valid SSL certificate installed that matches the hostname you have selected for your BeyondTrust site.

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.

What is SSL?

SSL (Secure Socket Layer) is a security protocol that uses encryption to ensure the secure transfer of data over the internet. An SSL certificate is a small digital file that contains a public key and private key pair, along with a "subject," which is the identity of the certificate owner. These keys work in a way that allows for the creation of a secure, encrypted connection between both parties. For example, in order for a browser and a server to establish a secure connection, an SSL certificate is needed. Essentially, an SSL certificate works as certified, digital proof of your online identity.

If your SSL certificate does not match your BeyondTrust site's hostname, your users will experience security errors. The proper way to resolve this is to get an SSL certificate signed by a third-party certificate authority (CA).

As a temporary measure, you can create a self-signed certificate, but this will not resolve all of the errors that come with not having a CA-signed certificate. If your site uses the factory default certificate or even if it uses a self-signed certificate, users attempting to access your BeyondTrust site will receive an error message warning them that your site is untrusted. Furthermore, without a CA-signed certificate, some software clients will not function at all. BeyondTrust software clients which absolutely require the heightened security of a CA-signed certificate include:

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

What is a Certificate Authority?

The CA or Issuing Authority issues multiple certificates in a certificate chain, proving that your site's certificate was issued by the CA. This proof is validated using a public and private key pair. The public key, available to all of your site visitors, must validate the private key in order to verify the authenticity of the certificate chain. The certificate chain typically consists of 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.

To have full functionality of the BeyondTrust software and to avoid security risks, it is very important that you obtain a valid CA-signed SSL certificate as soon as possible.

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 customers to obtain a certificate from a select list of certificate authorities.

BeyondTrust does not require any special type of certificate. BeyondTrust does accept wildcard certificates, subject alternative name (SAN) certificates, Unified Communications (UC) certificates, Extended Validation (EV) certificates, and so forth, as well as standard certificates.

BeyondTrust also provides support for requesting a Let's Encrypt certificate directly from the appliance. (missing or bad snippet)

The sections in this guide explain how to request and upload a certificate for the first time, how to replicate a certificate on additional BeyondTrust Appliances, how to renew an expired certificate, and how to replace a certificate with one from another certificate authority.

How do I obtain a CA-signed SSL certificate?

To obtain a valid CA-signed SSL certificate, create and submit a certificate signing request (CSR) as discussed in Create a Certificate Signed by a Certificate Authority for Your PRA Appliance . The CSR contains the public key portion of your BeyondTrust Appliance's key pair and the distinguished name of your appliance.

Once the CSR has been created, the appliance generates and saves a unique private key. You must then submit the CSR to a CA without the private key. The CA validates the identity of your site and returns a signed certificate to you, which you must install on your BeyondTrust Appliance.

Installing the new certificate in BeyondTrust automatically links the private key to the new certificate, making the 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 BeyondTrust Appliance), but if it is ever lost, decryption will be impossible, the appliance will be unable to validate its integrity, and the certificate will have to be replaced.

Never send the private key over the internet, and always secure it with a strong password.

Create a Self-Signed Certificate for Your PRA Appliance

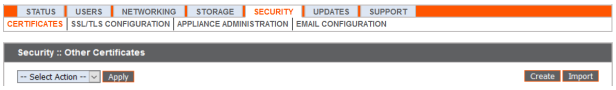
A self-signed certificate may be necessary on a temporary basis for testing or installing a BeyondTrust Appliance. For long-term use, a certificate from a public certificate authority (CA) should be used instead (see "Create a Certificate Signed by a Certificate Authority for Your PRA Appliance" on page 9). Self-signed certificates are created in the BeyondTrust /appliance web interface. Once created, the BeyondTrust software should be updated.

Create the Certificate

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

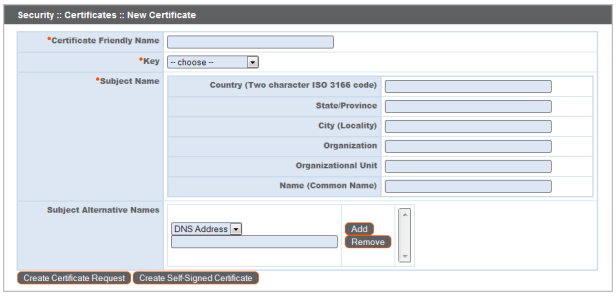
Certificates consist of a **friendly name**, **key**, **subject name**, and one or more **subject alternative names**. You must enter this information in the BeyondTrust /appliance web interface to create a self-signed certificate.

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



> ***Note:*** *You will see a "BeyondTrust Appliance" certificate listed. This is a standard certificate which ships with all BeyondTrust appliances. Both the certificate and its warning should be ignored.*

2. In the Security :: Other Certificates section, click **Create**.
3. Create a descriptive title for **Certificate Friendly Name**. Examples could include your primary DNS name or the current month and year. This name helps you identify your certificate request on your BeyondTrust Appliance **Security > Certificates** page.
4. Choose a key size from the **Key** dropdown. Verify with your certificate authority which key strengths they support. Larger key sizes normally require more processing overhead and may not be supported by older systems. However, smaller key sizes are likely to become obsolete or insecure sooner than larger ones.



5. The **Subject Name** consists of the contact information for the organization and department creating the certificate along with the name of the certificate.
    a. Enter your organization's two-character **Country** code. If you are unsure of your country code, please visit www.iso.org/iso-3166-country-codes.html.
    b. Enter your **State/Province** name if applicable. Enter the full state name.
    c. Enter your **City (Locality)**.
    d. In **Organization**, provide the name of your company.
    e. **Organizational Unit** is normally the group or department within the organization managing the certificate and/or the BeyondTrust deployment for the organization.
    f. For **Name (Common Name)**, enter a title for your certificate. In many cases, this should be simply a human-readable label. It is not recommended that you use your DNS name as the common name. This name must be unique to differentiate the certificate from others on the network. Be aware that this network could include the public internet.

6. In **Subject Alternative Names**, list the fully qualified domain name for each DNS A-record which resolves to your BeyondTrust 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.*

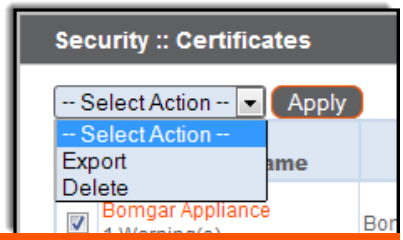
> ***Note:*** *If you plan to use multiple BeyondTrust Appliances in an Atlas setup, it is recommended that you use a wildcard certificate that covers both your BeyondTrust site hostname and each traffic node hostname. If you do not use a wildcard certificate, adding traffic nodes that use different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

7. 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

To insure the reliability of your client software, BeyondTrust Technical Support builds a copy of your certificate into your software. Therefore, when you create a new certificate, you must send to BeyondTrust Technical Support a copy of your certificate and also a screenshot of your **Status > Basics** page to identify the appliance being updated.

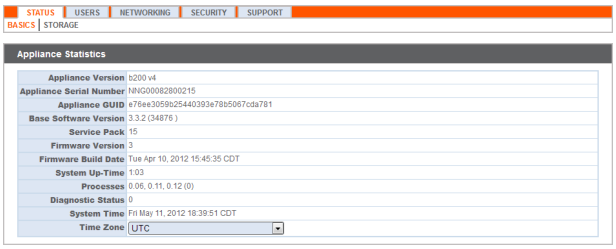
1. Go to **/appliance > Security > Certificates** and export a copy of your new certificate.
   a. Check the box next to the new certificate in the **Security :: Certificates** table.
   b. From the **Select Action** dropdown menu above the table, select **Export**. Then click **Apply**.
   c. Uncheck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



IMPORTANT!

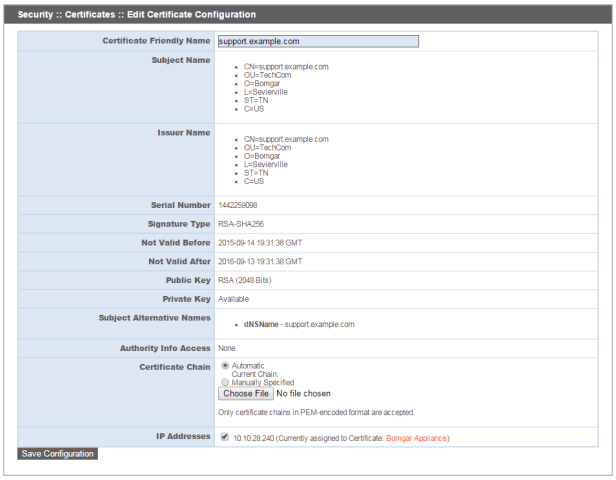
*Do NOT send your private key file (which ends in **.p12**) to BeyondTrust Technical Support. When exporting your certificate, you have the option to **Include Private Key**. If a certificate is being exported to be sent to BeyondTrust Technical Support, you should NOT check **Include Private Key**. This key is private because it allows the owner to authenticate your BeyondTrust 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 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 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.

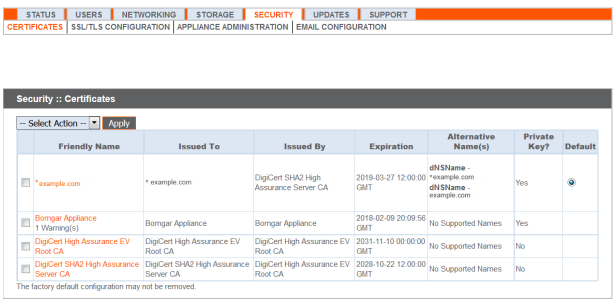


SSL Certificate Auto-Selection

Through the utilization of Server Name Indication (SNI), an extension to the TLS networking protocol, any SSL certificate stored on the appliance is a candidate to be served to any client. Because most TLS clients send Server Name Indication (SNI) information at the start of the handshaking process, this enables the 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 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 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.

Create a Certificate Signed by a Certificate Authority for Your PRA Appliance

To have full functionality of the BeyondTrust software and to avoid security risks, it is very important that as soon as possible, you obtain a valid SSL certificate signed by a certificate authority (CA). While a CA-signed certificate is the best way to secure your site, you may need a self-signed certificate or an internally-signed certificate (see "Create a Self-Signed Certificate for Your PRA Appliance" on page 5).

To obtain a certificate signed by a certificate authority, you must first create a certificate signing request (CSR) from the /appliance interface of your BeyondTrust Appliance. You will then submit the request data to a certificate authority. Once the signed certificate is obtained, the BeyondTrust software should be updated.

In addition to the CA certificate request feature, BeyondTrust includes functionality for obtaining and automatically renewing its own TLS certificates from the open Certificate Authority Let's Encrypt.

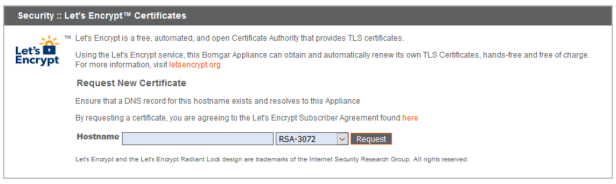
Obtain a Free TLS Certificate from Let's Encrypt

Let's Encrypt issues signed certificates which are valid for 90 days, yet have the capability of automatically renewing themselves indefinitely. In order to request a Let's Encrypt certificate, or to renew one in the future, you must meet the following requirements:

- The DNS for the hostname you are requesting must resolve to the appliance.
- The appliance must be able to reach Let's Encrypt on TCP 443.
- Let's Encrypt must be able to reach the appliance on TCP 80.

For more information, please see letsencrypt.org.

To implement a Let's Encrypt certificate, In the **Security :: Let's Encrypt™ Certificates** section:



- Enter the fully qualified domain name (FQDN) of the appliance in the **Hostname** field.
- Use the dropdown to choose the certificate key type.
- Click **Request**.

As long as the above requirements are met, this results in a certificate that will automatically renew every 90 days once the validity check with Let's Encrypt has completed.

Note: *The 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 appliance sends daily admin email alerts (if email notifications are enabled). The status will show the certificate in an error state.*

IMPORTANT!

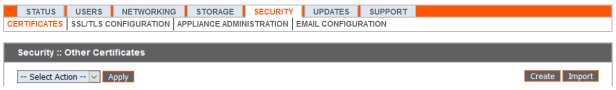
Because DNS can apply only to one appliance at a time, and because an appliance must be assigned the DNS hostname for which it makes a certificate request or renewal request, we recommend that you avoid use of Let's Encrypt certificates for failover appliance pairs.

Create a Certificate Signing Request

When using a CA issuer other than Let's Encrypt, the first step is to create the CSR. The request data associated with the CSR contains the details about your organization and BeyondTrust site. This request data is submitted to your certificate authority for them to publicly certify your organization and BeyondTrust Appliance.

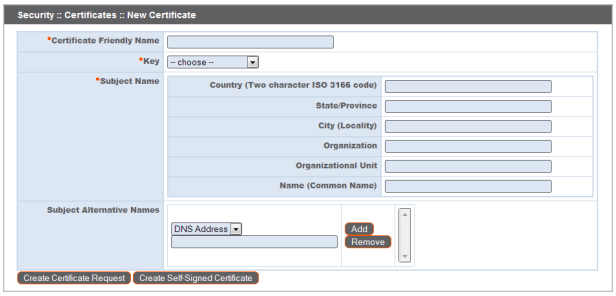
Certificates consist of a **friendly name**, **key**, **subject name**, and one or more **subject alternative names**. You must enter this information in the BeyondTrust /appliance web interface to create a certificate signing request.

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



> ***Note:*** *You will see a "BeyondTrust Appliance" certificate listed. This is a standard certificate which ships with all BeyondTrust appliances. Both the certificate and its warning should be ignored.*

2. In the Security :: Other Certificates section, click **Create**.
3. Create a descriptive title for **Certificate Friendly Name**. Examples could include your primary DNS name or the current month and year. This name helps you identify your certificate request on your BeyondTrust Appliance **Security > Certificates** page.
4. Choose a key size from the **Key** dropdown. Verify with your certificate authority which key strengths they support. Larger key sizes normally require more processing overhead and may not be supported by older systems. However, smaller key sizes are likely to become obsolete or insecure sooner than larger ones.



5. The **Subject Name** consists of the contact information for the organization and department creating the certificate along with the name of the certificate.
    a. Enter your organization's two-character **Country** code. If you are unsure of your country code, please visit www.iso.org/iso-3166-country-codes.html.
    b. Enter your **State/Province** name if applicable. Enter the full state name, as some certificate authorities will not accept a state abbreviation.
    c. Enter your **City (Locality)**.
    d. In **Organization**, provide the name of your company.
    e. **Organizational Unit** is normally the group or department within the organization managing the certificate and/or the BeyondTrust deployment for the organization.
    f. For **Name (Common Name)**, enter a title for your certificate. In many cases, this should be simply a human-readable label. 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. This name must be unique to differentiate the certificate from others on the network. Be aware that this network could include the public internet.
6. In **Subject Alternative Names**, list the fully qualified domain name for each DNS A-record which resolves to your BeyondTrust 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 BeyondTrust 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.*

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

Submit the Certificate Signing Request

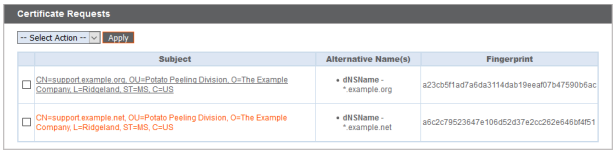
Once the certificate signing request has been created, you must submit it to a certificate authority for certification. You can obtain an SSL certificate from a commercial or public certificate authority or from an internal CA server if your organization uses one. BeyondTrust does not require or recommend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

- Comodo (www.comodo.com) - As of 24 February 2015, Comodo is the largest issuer of SSL certificates.
- Digicert (www.digicert.com) - Digicert is a US-based certificate authority that has been in business for over a decade.
- 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.
- Symantec SSL (www.websecurity.symantec.com/ssl-certificate) - 97 of the world's 100 largest financial institutions and 75 percent of the 500 biggest e-commerce sites in North America use SSL certificates from Symantec.

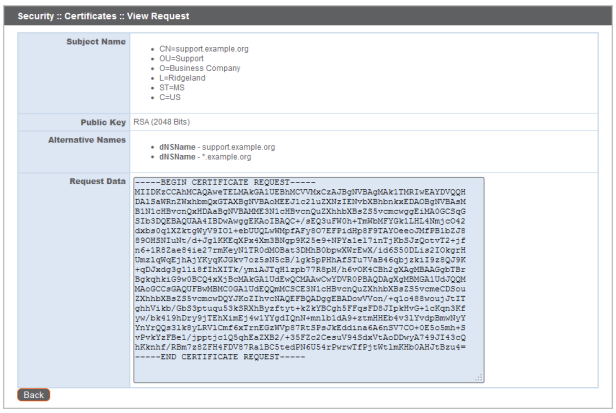
Once you have selected a certificate authority, you must purchase a certificate from them. BeyondTrust does not require any special type of certificate. BeyondTrust accepts wildcard certificates, subject alternative name (SAN) certificates, unified communications (UC) certificates, extended validation (EV) certificates, and so forth, as well as 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 BeyondTrust 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 it and sign it. After the certificate authority has signed the certificate, they will send it back to you, often with the root and/or intermediate certificate files. All these together constitute your certificate chain. The CA or Issuing Authority issues multiple certificates in a certificate chain, proving that your site's certificate was issued by the CA. This proof is validated using a public and private key pair. The public key, available to all of your site visitors, must validate the private key in order to verify the authenticity of the certificate chain. The certificate chain typically consists of 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 BeyondTrust Appliance before it will be completely operational. 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)

You must 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.

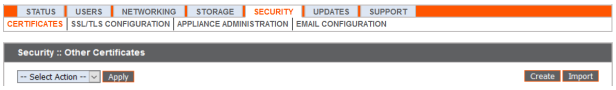
Many certificate authorities do not send the root certificate of your certificate chain. BeyondTrust requires this root certificate to function properly. If no links were provided to obtain the root certificate, then it is suggested that the CA be contacted for assistance. If this is impractical for any reason, it should be possible to find the correct root certificate in your CA's online root certificate repository. Some of the major repositories are these:

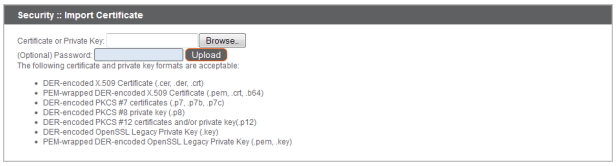
- Comodo > Repository > Root Certificates (www.comodo.com/about/comodo-agreements.php)
- DigiCert Trusted Root Authority Certificates (www.digicert.com/digicert-root-certificates.htm)
- GeoTrust Root Certificates (www.geotrust.com/resources/root-certificates)
- GoDaddy > Repository (certs.godaddy.com/repository)
- Symantec > Licensing and Use of Root Certificates (www.symantec.com/theme/roots)

To identify which root is appropriate for your certificate chain, you should contact your certificate authority. However, it is also possible on most systems to open your certificate file on the local system and check the certificate chain from there. For instance, in Windows 7, the certificate chain is shown under the **Certification Path** tab of the certificate file, and the root certificate is listed at the top. Opening the root certificate here normally allows you to identify the approprate root on the CA's online repository.

Once you have downloaded all the certificate files for your certificate chain, you must import these files to your BeyondTrust Appliance.

1. Log into the /appliance interface of your BeyondTrust Appliance. Go to **Security > Certificates**.
2. In the **Security :: Other Certificates** section, click the **Import** button.
3. 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 BeyondTrust 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.

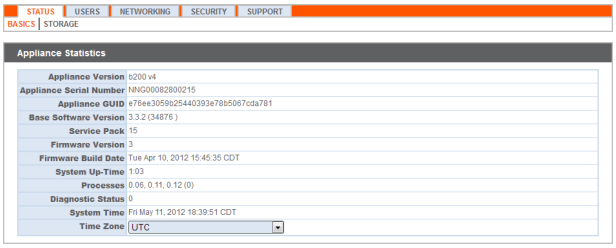
Update the BeyondTrust Appliance

To insure the reliability of your client software, BeyondTrust Technical Support builds your root certificate into your software. Therefore, any time you import a new root certificate to your BeyondTrust Appliance, you must send to BeyondTrust Technical Support a copy of the new SSL certificate and also a screenshot of your **Status > Basics** page to identify the 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 BeyondTrust 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 appliance is compromised.*

4. Go to **/appliance > Status > Basics** and take a screenshot of the page.
5. 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).
6. 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.



7. 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.

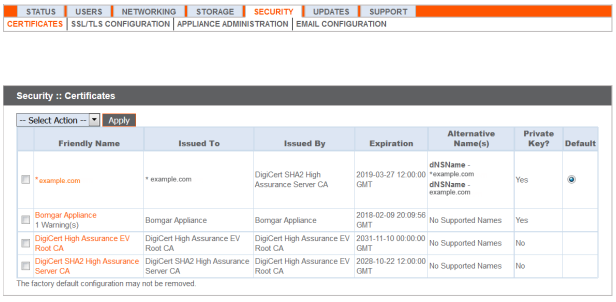
After these steps are complete, it is advisable to wait 24-48 hours before proceeding further. This allows time for your BeyondTrust client software (especially Jump Clients) to update themselves with the new certificate which BeyondTrust Technical Support included in your recent software update.

SSL Certificate Auto-Selection

Through the utilization of Server Name Indication (SNI), an extension to the TLS networking protocol, any SSL certificate stored on the appliance is a candidate to be served to any client. Because most TLS clients send Server Name Indication (SNI) information at the start of the handshaking process, this enables the 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 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 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 Appliances

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

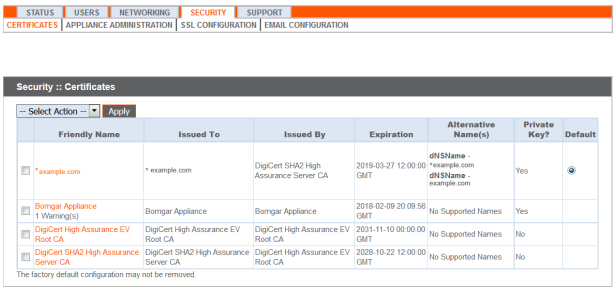
In a failover setup, the primary and backup appliances must have identical SSL certificates for failover to be successful. Otherwise, in the event of failover, the backup appliance will be unable to connect to any BeyondTrust software clients. Therefore, you should create a CA-signed certificate that supports each appliance's unique hostname as well as your main BeyondTrust site hostname. Replicate this certificate on both the primary and the backup appliances.

Additionally, if you plan to use 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 appliances.

To replicate an SSL certificate, follow the instructions below:

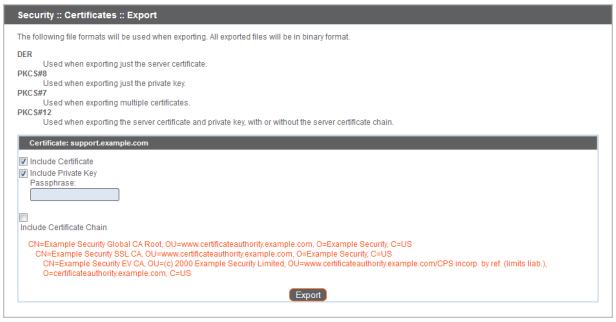
Export the Certificate

1. On the primary 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 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.

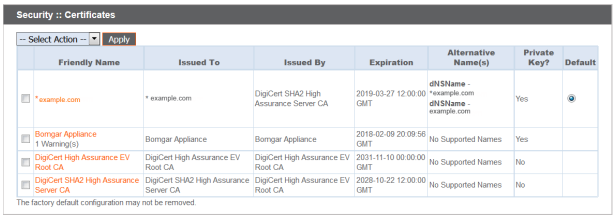


Import the Certificate

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

3. Browse to the certificate file you just exported from the primary 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 :: Certificates** section.
5. Repeat the import process for each additional clustered appliance.



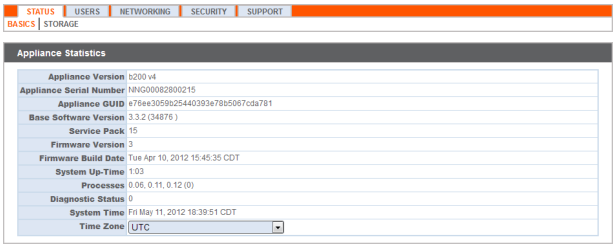
Update the BeyondTrust Appliance

To insure the reliability of your client software, BeyondTrust Technical Support builds your root certificate into your software. Therefore, any time you import a new root certificate to your BeyondTrust Appliance, you must send to BeyondTrust Technical Support a copy of the new SSL certificate and also a screenshot of your **Status > Basics** page to identify the 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 BeyondTrust 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 appliance is compromised.*

6. Go to **/appliance > Status > Basics** and take a screenshot of the page.
7. 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).
8. 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.



9. 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.
10. Repeat the update process for each additional clustered appliance.

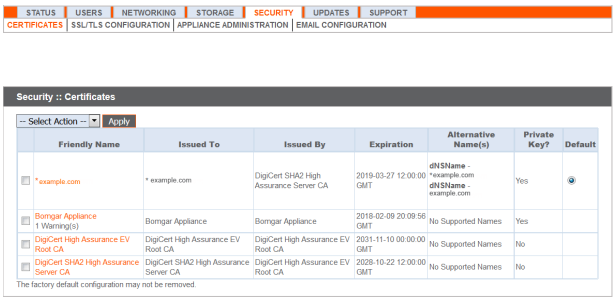
After these steps are complete, it is advisable to wait 24-48 hours before proceeding further. This allows time for your BeyondTrust client software (especially Jump Clients) to update themselves with the new certificate which BeyondTrust Technical Support included in your recent software update.

SSL Certificate Auto-Selection

Through the utilization of Server Name Indication (SNI), an extension to the TLS networking protocol, any SSL certificate stored on the appliance is a candidate to be served to any client. Because most TLS clients send Server Name Indication (SNI) information at the start of the handshaking process, this enables the 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 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 Privileged Remote Access Appliance

If the SSL certificate of your BeyondTrust 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 Privileged Remote Access Appliance" on page 20.

IMPORTANT!

Because the software on the BeyondTrust 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

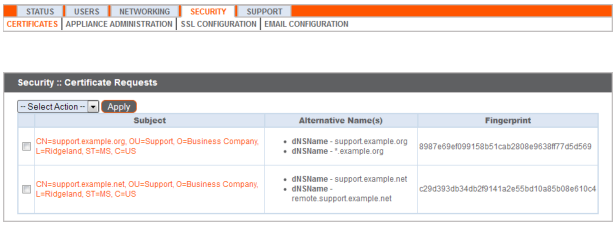
1. Contact the certificate authority that signed the certificate to request a renewal.

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

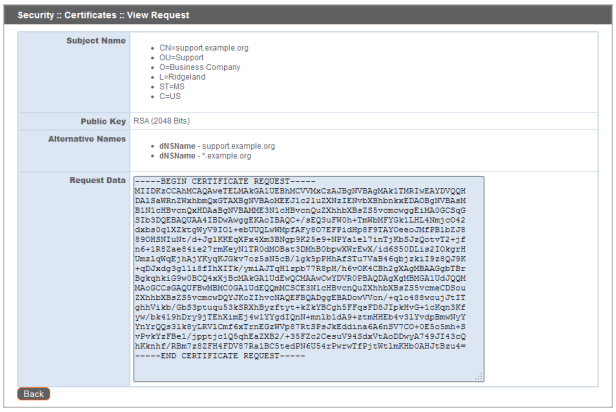
2. Many CAs keep the certificate request information on file. Others may require you to provide the original certificate request.

   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.

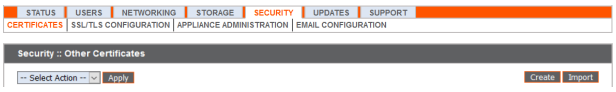


   b. Select and copy the **Request Data**, and then submit this information to your certificate authority.



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.
1. Log into the /appliance interface of your BeyondTrust Appliance. Go to **Security > Certificates**.
2. In the **Security :: Other Certificates** section, click the **Import** button.
3. Browse to your new certificate file and click **Upload**.
4. 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.

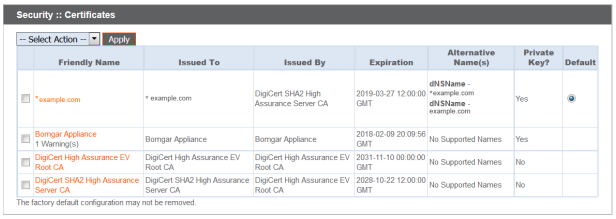


SSL Certificate Auto-Selection

Through the utilization of Server Name Indication (SNI), an extension to the TLS networking protocol, any SSL certificate stored on the appliance is a candidate to be served to any client. Because most TLS clients send Server Name Indication (SNI) information at the start of the handshaking process, this enables the 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 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 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 Privileged Remote Access Appliance

Follow the instructions in this section if you need to do one 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.

If you need to renew an existing CA-signed certificate from the same CA, see "Renew an Expired Certificate for the Privileged Remote Access Appliance" on page 18.

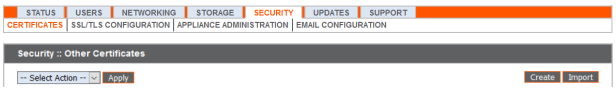
BeyondTrust client software must be able to validate the SSL certificate of their appliance in order to establish secure connections. To do this, they must trust the certificate authority of the appliance's server certificate. If this CA is changed without preparing the clients beforehand, then it is possible to permanently lose connectivity to the clients due to failed SSL validation. To avoid this, the BeyondTrust Appliance must be properly updated with product builds from BeyondTrust Technical Support and provisioned with the new CA-signed certificate.

Create a Certificate Signing Request

When using a CA issuer other than Let's Encrypt, the first step is to create the CSR. The request data associated with the CSR contains the details about your organization and BeyondTrust site. This request data is submitted to your certificate authority for them to publicly certify your organization and BeyondTrust Appliance.

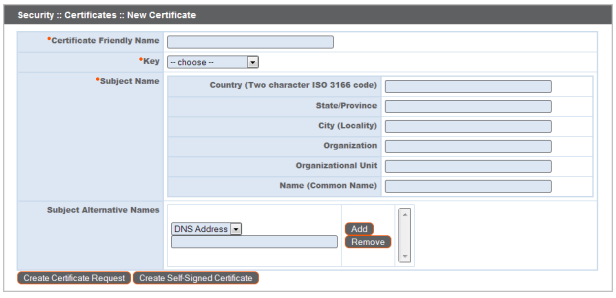
Certificates consist of a **friendly name**, **key**, **subject name**, and one or more **subject alternative names**. You must enter this information in the BeyondTrust /appliance web interface to create a certificate signing request.

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



> ***Note:*** *You will see a "BeyondTrust Appliance" certificate listed. This is a standard certificate which ships with all BeyondTrust appliances. Both the certificate and its warning should be ignored.*

2. In the Security :: Other Certificates section, click **Create**.
3. Create a descriptive title for **Certificate Friendly Name**. Examples could include your primary DNS name or the current month and year. This name helps you identify your certificate request on your BeyondTrust Appliance **Security > Certificates** page.
4. Choose a key size from the **Key** dropdown. Verify with your certificate authority which key strengths they support. Larger key sizes normally require more processing overhead and may not be supported by older systems. However, smaller key sizes are likely to become obsolete or insecure sooner than larger ones.



5. The **Subject Name** consists of the contact information for the organization and department creating the certificate along with the name of the certificate.

a. Enter your organization's two-character **Country** code. If you are unsure of your country code, please visit www.iso.org/iso-3166-country-codes.html.
b. Enter your **State/Province** name if applicable. Enter the full state name, as some certificate authorities will not accept a state abbreviation.
c. Enter your **City (Locality)**.
d. In **Organization**, provide the name of your company.
e. **Organizational Unit** is normally the group or department within the organization managing the certificate and/or the BeyondTrust deployment for the organization.
f. For **Name (Common Name)**, enter a title for your certificate. In many cases, this should be simply a human-readable label. 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. This name must be unique to differentiate the certificate from others on the network. Be aware that this network could include the public internet.

6. In **Subject Alternative Names**, list the fully qualified domain name for each DNS A-record which resolves to your BeyondTrust 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 BeyondTrust 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.*

7. Click **Create Certificate Request** and wait for the page to refresh.
8. 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 these are some of the most well known.

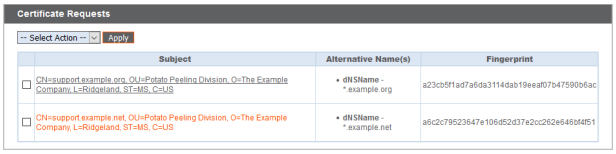
- Comodo (www.comodo.com) - As of 24 February 2015, Comodo is the largest issuer of SSL certificates.
- Digicert (www.digicert.com) - Digicert is a US-based certificate authority that has been in business for over a decade.
- GeoTrust, Inc. (www.geotrust.com) - GeoTrust is the world's second largest 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.
- Symantec SSL (www.websecurity.symantec.com/ssl-certificate) - 97 of the world's 100 largest financial institutions and 75 percent of the 500 biggest e-commerce sites in North America use SSL certificates from Symantec.

Once you have selected a certificate authority, you must purchase a certificate from them. BeyondTrust does not require any special type of certificate. BeyondTrust accepts wildcard certificates, subject alternative name (SAN) certificates, unified communications (UC) certificates, extended validation (EV) certificates, and so forth, as well as standard certificates.

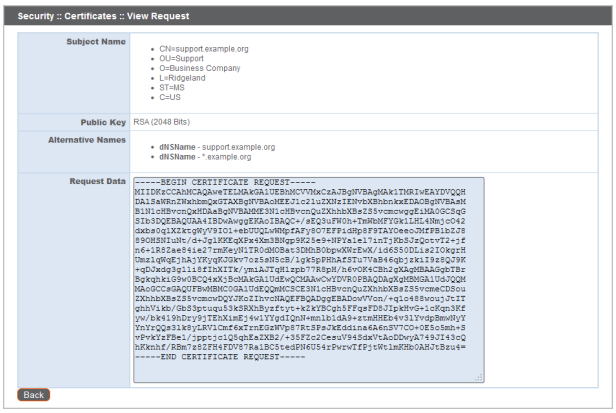
During or after the purchase, you will be prompted to upload or copy/paste your request data. The certificate authority should give you instructions for doing so. To retrieve your request data from BeyondTrust, take these steps:

1. When prompted to submit the request information, log into the /appliance interface of your BeyondTrust 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 it and sign it. After the certificate authority has signed the certificate, they will send it back to you, often with the root and/or intermediate certificate files. All these together constitute your certificate chain. The CA or Issuing Authority issues multiple certificates in a certificate chain, proving that your site's certificate was issued by the CA. This proof is validated using a public and private key pair. The public key, available to all of your site visitors, must validate the private key in order to verify the authenticity of the certificate chain. The certificate chain typically consists of 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 BeyondTrust Appliance before it will be completely operational. 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)

You must 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.

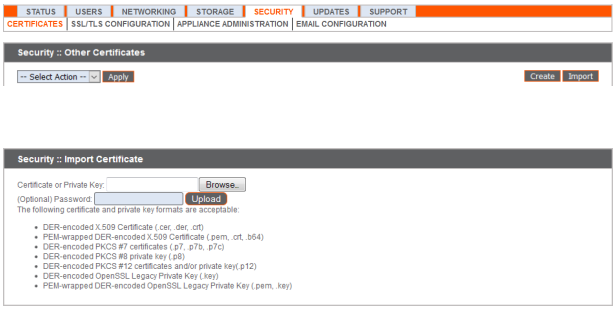
Many certificate authorities do not send the root certificate of your certificate chain. BeyondTrust requires this root certificate to function properly. If no links were provided to obtain the root certificate, then it is suggested that the CA be contacted for assistance. If this is impractical for any reason, it should be possible to find the correct root certificate in your CA's online root certificate repository. Some of the major repositories are these:

- Comodo > Repository > Root Certificates (www.comodo.com/about/comodo-agreements.php)
- DigiCert Trusted Root Authority Certificates (www.digicert.com/digicert-root-certificates.htm)
- GeoTrust Root Certificates (www.geotrust.com/resources/root-certificates)
- GoDaddy > Repository (certs.godaddy.com/repository)
- Symantec > Licensing and Use of Root Certificates (www.symantec.com/theme/roots)

To identify which root is appropriate for your certificate chain, you should contact your certificate authority. However, it is also possible on most systems to open your certificate file on the local system and check the certificate chain from there. For instance, in Windows 7, the certificate chain is shown under the **Certification Path** tab of the certificate file, and the root certificate is listed at the top. Opening the root certificate here normally allows you to identify the approprate root on the CA's online repository.

Once you have downloaded all the certificate files for your certificate chain, you must import these files to your BeyondTrust Appliance.

1. Log into the /appliance interface of your BeyondTrust Appliance. Go to **Security > Certificates**.
2. In the **Security :: Other Certificates** section, click the **Import** button.
3. 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 BeyondTrust 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.

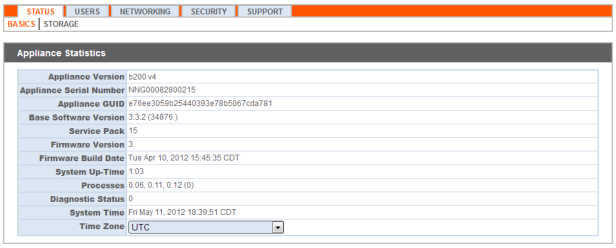
Update the BeyondTrust Appliance

To insure the reliability of your client software, BeyondTrust Technical Support builds your root certificate into your software. Therefore, any time you import a new root certificate to your BeyondTrust Appliance, you must send to BeyondTrust Technical Support a copy of the new SSL certificate and also a screenshot of your **Status > Basics** page to identify the 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 BeyondTrust 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 appliance is compromised.*

4. Go to **/appliance > Status > Basics** and take a screenshot of the page.
5. 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).
6. 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.



7. 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.

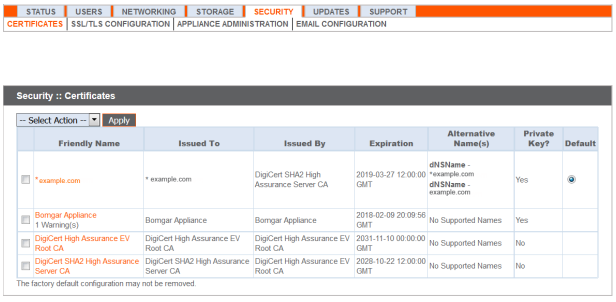
After these steps are complete, it is advisable to wait 24-48 hours before proceeding further. This allows time for your BeyondTrust client software (especially Jump Clients) to update themselves with the new certificate which BeyondTrust Technical Support included in your recent software update.

SSL Certificate Auto-Selection

Through the utilization of Server Name Indication (SNI), an extension to the TLS networking protocol, any SSL certificate stored on the appliance is a candidate to be served to any client. Because most TLS clients send Server Name Indication (SNI) information at the start of the handshaking process, this enables the 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 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 appliance should be fully upgraded and operational with its new certificate. The old certificate may be removed and/or revoked as necessary.