Privileged Remote Access Appliance Hardware Installation
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Remote Access Appliance Setup Task List</td>
<td>3</td>
</tr>
<tr>
<td>Secure Remote Access Appliance Prerequisites</td>
<td>4</td>
</tr>
<tr>
<td>Secure Remote Access Appliance Installation</td>
<td>6</td>
</tr>
<tr>
<td>Power On the Secure Remote Access Appliance</td>
<td>6</td>
</tr>
<tr>
<td>Initial Network Configuration During Secure Remote Access Appliance Setup</td>
<td>7</td>
</tr>
<tr>
<td>SSL Certificate Requirement for the Secure Remote Access Appliance</td>
<td>11</td>
</tr>
<tr>
<td>Send Secure Remote Access Appliance Information to BeyondTrust Technical Support</td>
<td>13</td>
</tr>
<tr>
<td>Check for Updates to Install BeyondTrust PRA Software</td>
<td>14</td>
</tr>
<tr>
<td>Open Source Software Acknowledgments</td>
<td>15</td>
</tr>
</tbody>
</table>
Secure Remote Access Appliance Setup Task List

This task list is a quick reference for the steps necessary to get your Secure Remote Access Appliance set up. Full details can be found further on in this guide. Use this list as a checklist of the essential steps.

1. Configure a DNS A-record for the fully qualified domain name (FQDN) of your new site (e.g., access.example.com).
   - If your appliance will be located in your DMZ or internal network, then an internal A-record pointing to the internal IP address of the appliance is needed.
   - If you wish to support external customers, then a Public DNS A-record also needs to be registered for the external IP address of the appliance.
   - For BeyondTrust network deployment scenarios, please see The Secure Remote Access Appliance in the Network at www.beyondtrust.com/docs/deployment/dmz.

2. Install the Secure Remote Access Appliance according to “Secure Remote Access Appliance Prerequisites” on page 4.

3. Obtain an SSL certificate that matches your FQDN DNS (e.g., access.example.com).
   - For full details, please see the SSL Certificate Guide at www.beyondtrust.com/docs/privileged-remote-access/how-to/sslcertificates.
   - Import the certificate chain to your appliance and assign it to the IP address of the appliance.
   - Export the root portion of the certificate chain (with matching Issued To and Issued By values) without private key information, and save the root certificate for the next step.

4. Email the following three items to BeyondTrust Technical Support:
   - The FQDN DNS hostname of the appliance from Step 1.
   - The root SSL certificate segment exported in Step 3c.
   - A screenshot of the /appliance > Status > Basics page.

5. Install the new software license package which BeyondTrust Technical Support will send after you complete Steps 1-4.
   - You will be notified by email when you should install the software license package using the Check for Updates utility.
   - Once installed, navigate to the /login administrative interface (e.g., https://access.example.com/login).
   - Use the default admin credentials admin and password to log in for the first time.
Secure Remote Access Appliance Prerequisites

This guide walks you through the initial setup and configuration of your Secure Remote Access Appliance. Should you need any assistance, please contact BeyondTrust Technical Support at www.beyondtrust.com/support.

Prerequisites

Before starting, it is important to know that until the Secure Remote Access Appliance's prerequisites have been met, you will neither be able to reach your appliance directly by its IP address or hostname nor be able to check for updates or use it to provide privileged access. The Secure Remote Access Appliance requires the following at a minimum:

- Two available power outlets
- A high-speed network connection
- A network router or switch
- A unique, static IP address for the Secure Remote Access Appliance
- A private DNS A-record resolving to the static IP of your appliance. A public A-record and public IP will also be required if external clients will need access to the appliance.
- An SSL web server certificate + intermediate SSL certificate(s), and SSL root. OR, 1 Self-Signed certificate.

For more information, please see the SSL Certificates and BeyondTrust Guide.

- The BeyondTrust software licensing package

While these meet the minimum requirements, more advanced configurations may require additional items. For example:

- BeyondTrust mobile clients require an SSL root and intermediate SSL certificate(s).
- Access from external public networks require a public DNS A-record.
- Access from multiple DNS A-records require either multiple web server certificates and/or SAN or wildcard certificate(s).
- Isolating client traffic from multiple networks requires multiple static IP addresses.
- Automatic updating and advanced BeyondTrust technical support require outbound access to the public internet from the Secure Remote Access Appliance over TCP port 443.

**IMPORTANT!**

No client software (e.g., access consoles, Jump Clients, Jumpoints, etc.) can be downloaded, installed, or used until BeyondTrust Technical Support builds a software licensing package for your appliance and you install it per the instructions provided by Support. Because this license package is encoded with the DNS A-record of the appliance as well as its SSL certificate, these must be in place before the license package can be completed.
Getting Started

Several steps should be taken before the BeyondTrust hardware is delivered and installed:

1. Allocate the necessary rack space for the appliance. Ensure the space has the necessary power and network access.
2. Reserve a static IP address for the appliance on the network. Refer to the following guides in order to reserve the correct IP address(es):
   - Secure Remote Access Appliance in the Network - www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/dmz
3. Configure a DNS A-record for the fully qualified domain name (FQDN) of your new site (e.g., access.example.com).

   **Note:** A private DNS A-record resolving to the static IP address of the appliance will always be necessary. A public A-record and public IP will also be required if clients on public, external networks will need access to the appliance.

Although your appliance can function anywhere in your network with internet access, you will need to decide where in your network you plan to install the appliance prior to this step. If you are going to access systems outside of your network, BeyondTrust recommends placing your appliance in a DMZ or outside of your internal firewall. See the table below for more details. For assistance with your firewall configuration, please contact the manufacturer of your firewall software.

   **Note:** If you must move the appliance to another location to connect it to the internet, you will need to power down before you unplug it from its power source. If you can log into the /appliance administrative interface, go to the **Status > Basics** page and click **Shut Down This Appliance**. Manual shut down is possible if you press and release the power button one time. Wait 60 seconds for the appliance to power down before unplugging the Secure Remote Access Appliance from the power source. When you reconnect the appliance at the new location, you will need to power up again.

---

<table>
<thead>
<tr>
<th>Network Location</th>
<th>Advantages/Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outside your firewall</td>
<td>Does not require that ports 80 and 443 be open inbound for TCP traffic on your firewall. Simplifies the setup process significantly because both the representative and customer clients are built to resolve to a specific DNS; if your registered DNS resolves to a public IP address directly assigned to your appliance, no additional setup is required by you to initiate a session.</td>
</tr>
<tr>
<td>DMZ</td>
<td>May require additional setup depending on your router or routers.</td>
</tr>
<tr>
<td>Inside your firewall</td>
<td>Requires port forwarding on your firewall and possibly additional setup of your NAT routing and internal DNS.</td>
</tr>
</tbody>
</table>
Secure Remote Access Appliance Installation


Power On the Secure Remote Access Appliance

1. Plug the power cables for the Secure Remote Access Appliance into a safe power source. Depending on the type of appliance, you may have two power cables. The appliance’s power supplies will automatically switch between 120v and 240v, as needed.

2. Using one of the patch cables provided, connect your computer to NIC1 or NIC2 on the rear of the Secure Remote Access Appliance. You can use either crossover or straight-through cables. If using DHCP, plug the provided straight-through cable into the network directly, and the appliance automatically receives a new IP address.

   **Note:** BeyondTrust supports placing both NICs on the same network for the purpose of NIC Teaming. Likewise, NICs can be placed on separate network subnets for segmented traffic routing. However, if placing NICs on the same network for the purpose of NIC Teaming, configure only one of the NICs. If both NICs have IP addresses from the same subnet, unexpected behavior will result. When multiple IP addresses are required for a single subnet, the proper solution is to assign all the IP address to one NIC.

3. Press and release the power button on the front of the appliance. The power LED immediately to the right of the reset button will illuminate, and the HDD activity LED (immediately to the right of the power LED) will begin to flash. Initialization of the Secure Remote Access Appliance will complete in about 60 seconds.

   **Note:** The NIC1 and NIC2 LEDs may illuminate and show activity even when the appliance is not powered on; therefore, it is important to check the power and HDD LEDs to confirm that the appliance is on.
Initial Network Configuration During Secure Remote Access Appliance Setup

Before deploying the Secure Remote Access Appliance on your network, you must set up its network configuration. This is done by accessing the Secure Remote Access Appliance administrative interface from a web browser on your computer. The steps below will walk you through this process. Your process may vary depending upon your operating system.

DHCP Instructions

If the network location you have selected for your appliance has DHCP enabled, the appliance receives an IP address from the network and can be immediately accessed via that IP address at https://<ipaddress>/appliance. You can find this IP address via the console on the video port.

Use the default username and password to log in.

Default Username: admin
Default Password: password

Upon initial login, you are prompted to change your appliance administration password.

Note: If using DHCP, you can skip the Local Area Connection Instructions section and go to the /appliance Configuration section.
Local Area Connection Instructions

1. After performing the external setup of your Secure Remote Access Appliance, go to the Local Area Connection on your computer and click Properties.

2. Highlight Internet Protocol Version 4 (IPv4) and click the Properties button.

3. Enter 169.254.1.5 as your IP address and 255.255.0.0 as the subnet mask. Be sure the Gateway and DNS fields are blank.
4. Launch a web browser and enter the address https://169.254.1.1/appliance/login.ns in the URL address field. If this fails, try alternately substituting ".2", ".3" and ".4" for the last decimal in the address above. Load each of these addresses separately until one responds. Enter the default username and password and click Login.

Default Username: admin

Default Password: password

Upon initial login, you are prompted to change your appliance administration password.

**Note:** The Secure Remote Access Appliance uses two administrative web interfaces, /appliance and /login, to isolate hardware administration from user management. The /appliance interface is used to configure network settings and upgrade BeyondTrust software. The /login interface is not available until after BeyondTrust Technical Support builds the necessary software licensing package and this package is installed through /appliance. Once installed, /login is used to manage users and workflows, deploy client software, report on access activity, create and use integrations, etc. See the BeyondTrust Privileged Remote Access Admin Interface at [www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin](http://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin).

/appliance Configuration

1. Once you are logged into the /appliance interface, you will see the Status > Basics page. This page includes information such as the serial number which BeyondTrust Technical Support requires to register the appliance with the BeyondTrust licensing servers. Take a screenshot of this page and send it to BeyondTrust Technical Support so that the Support team can register your appliance.

2. Next, go to Networking > IP Configuration. Under the NIC Configuration section, click Add New IP.
3. Enter the static IP address and subnet mask for your Secure Remote Access Appliance. Typically you should leave the default values for both fields. You can decide if this IP address will support session traffic, web traffic, or both. Then click **Save Changes**.

4. Under the **Global Network Configuration** section, set your default gateway. Enter your default Gateway and DNS server addresses. After entering the required information, click **Save Changes**.

**Note:** Valid DNS settings are required for failover and automatic updates to function properly.

For more about network configuration, see The Secure Remote Access Appliance in the Network at www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/dmz.
SSL Certificate Requirement for the Secure Remote Access Appliance

All BeyondTrust software communication occurs via secure, encrypted connections. These rely on the industry standard Secure Sockets Layer (SSL) technology and DNS address of the appliance. Secure Remote Access Appliances ship with a default certificate which secures all connections on all IP addresses. However, this will not satisfy the requirements of BeyondTrust’s client software, which runs more rigorous validation checks than standard web browsers. Therefore, before BeyondTrust can provide you with a fully operational software licensing package, your Secure Remote Access Appliance will need to have a valid SSL certificate installed that matches the DNS A-record you have registered for your appliance.

A valid SSL certificate can be either a certificate authority-signed (CA-signed) SSL certificate or a self-signed SSL certificate. CA-signed certificates are required to fully leverage all of BeyondTrust’s functionality (e.g., click-to-chat and mobile clients), but they require that a certificate signing request (CSR) be submitted to the CA. The CSR is an industry standard used by all network devices and software which use SSL. If a CSR/CA-signed certificate is used instead of a self-signed certificate, the CA-signed certificate must be downloaded from the CA’s web site (or certificate purchase email) and imported to the Secure Remote Access Appliance from the /appliance interface. 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.

For more information on creating and managing SSL certificates in BeyondTrust PRA, please see the following articles:

- Create a SSL Certificate Signed by a Certificate Authority for Your Secure Remote Access Appliance at www.beyondtrust.com/docs/privileged-remote-access/how-to/sslcertificates/create-ca-signed.htm
- Create a Self-Signed Certificate for Your Secure Remote Access Appliance at www.beyondtrust.com/docs/privileged-remote-access/how-to/sslcertificates/create-self-signed.htm
- Certificates: Create and Manage SSL Certificates at www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/web/security-certificates.htm.

For more information on how BeyondTrust uses SSL certificates as well as detailed configuration steps to request and install certificates in BeyondTrust, please see the SSL Certificates Guide at www.beyondtrust.com/docs/privileged-remote-access/how-to/sslcertificates.

The section Create an SSL Certificate describes the steps for initial configuration in detail. An overview of the process is given below.

1. Log into the BeyondTrust/appliance interface and create a certificate signing request (CSR) or self-signed certificate.

   **Note:** If the Secure Remote Access Appliance will be using a copy of the certificate from another Secure Remote Access Appliance or server, no CSR or self-signed certificate is necessary. Instead, export the certificate with its private key from the system on which it currently resides and import it to the Secure Remote Access Appliance. For detailed steps, see the section Replicate the SSL Certificate on Failover and Atlas Appliances in the SSL Certificates Guide.

2. Assign the new certificate to the IP address(es) of the Secure Remote Access Appliance.
3. Send BeyondTrust Technical Support a copy of the SSL root certificate and/or appliance DNS address.

**Note:** If a self-signed certificate is used, the certificate serves as its own root certificate, and therefore, the self-signed certificate should be sent to BeyondTrust Technical Support. If a CA-signed certificate is used, contact the CA for a copy of their root certificate. If you have trouble contacting the CA, articles to assist with obtaining your root certificate can be found at beyondtrustcorp.service-now.com/csm. In either case, BeyondTrust Technical Support will need to know the DNS address of the appliance. If your DNS address is public and the SSL certificate is already installed, Support can retrieve a copy of the root from the public DNS address; in this case, it is not necessary to manually send the root certificate.

Once the above steps are complete, BeyondTrust Technical Support encodes the DNS hostname and SSL root certificate into a new software licensing package, sends it to the BeyondTrust licensing servers for building, and then sends you instructions to install the newly-built package once it is complete.
Send Secure Remote Access Appliance Information to BeyondTrust Technical Support

While building your software package, BeyondTrust Technical Support encodes your appliance’s DNS hostname and SSL root certificate into the software. Before BeyondTrust Technical Support can build your software, you must send them the items listed below.

1. DNS hostname (fully qualified domain name) of the appliance (e.g., access.example.com).
2. SSL root certificate or self-signed SSL certificate. This is obtained from the /appliance > Security > Certificates page. Export the certificate portion with matching Issued To and Issued By fields.
3. Screenshot of the /appliance > Status > Basics page.
Check for Updates to Install BeyondTrust PRA Software

Secure Remote Access Appliance updates are installed from the /appliance web interface on the Updates page. Each update must be built by BeyondTrust and is keyed to the serial number of the appliance for which it was built. For this reason, the appliance must be registered in order to check for updates.

1. Once BeyondTrust has built an update for your appliance, you will receive a notification email. Go to /appliance > Updates. Retrieve the update using either Updates :: Check > Check for Updates or Updates :: Manual Installation > Appliance Download Key.

   ![Note: The Check for Updates option can be used only if the appliance has outbound access over TCP port 443 to update.bomgar.com. Manual installation does not require this connection.]

2. Once the check is complete, all available updates matching the serial number of your appliance will be listed in the /appliance web interface. There are two types of updates:
   - Updates for /login licensing (always shown in the format of BeyondTrust-x.x.x)
   - Updates for /appliance Base Software (always shown in the format of Base Software x.x.x)

If no update packages or patches are available for your Secure Remote Access Appliance, a message stating "No updates available" is displayed. If an update is available but an error occurred when distributing the update to your appliance, an additional message is displayed, such as, "An error occurred building your update. Please visit [www.beyondtrust.com/support](http://www.beyondtrust.com/support) for more information."

Base Software includes features and fixes for /appliance as well as the prerequisite code required before installing license updates. Therefore, new licensing updates typically require you to install the prerequisite Base Software Update first. In this case, BeyondTrust's update interface will make note of the correct order in which to install updates. If you are still unsure, take a screenshot of your available updates and send the screenshot to BeyondTrust Technical Support for assistance.

![IMPORTANT!]

As a reminder, you must send BeyondTrust Technical Support the following items before Support can build your Base Software and/or software licensing updates:

1. DNS hostname (fully qualified domain name) of the appliance
2. SSL root certificate or self-signed SSL certificate
3. Screenshot of the /appliance > Status > Basics page

3. Once you have sent BeyondTrust Technical Support your hostname, SSL certificate, and screenshot, they will build the necessary updates and send you detailed installation instructions.

4. When installation is complete, the Secure Remote Access Appliance is ready to be used for privileged access. To validate your appliance's readiness, log into the /login interface by going to your appliance's URL followed by /login (e.g., access.example.com/login).

Default Username: admin
Default Password: **password**

5. Upon initial login, you will be prompted to change your password.

6. Once the initial login is complete, you can validate your software licensing configuration on the **Status > Information** page, add user accounts on **Users & Security > Users**, and download client software from **My Account**. Because BeyondTrust Privileged Remote Access is licensed by number of endpoints allowed, you can set up as many accounts as you need, each with unique usernames and passwords.

For security purposes, the administrative username and password used for the /appliance interface are distinct from those used for the /login interface and must be managed separately. Usernames and passwords for /login are valid for both the /login interface (where users and configuration are managed) and for access consoles (where sessions are run). The options available in both of these locations are dependent upon the permissions assigned by the /login administrator to each user's account.

For help getting started with the BeyondTrust client software, see the documentation located at [www.beyondtrust.com/docs](http://www.beyondtrust.com/docs). Appliance Guides and Privileged Remote Access Administrator Guides explain the various administrative options of your /appliance and /login web interfaces, and Access User Guides show you how to use the BeyondTrust client software.

**Open Source Software Acknowledgments**

For information on open source software copyrights and acknowledgments used in BeyondTrust hardware and software products, please see the [Attributions index](http://www.beyondtrust.com/docs/privileged-remote-access/updates/attribution) at [www.beyondtrust.com/docs/privileged-remote-access/updates/attributions](http://www.beyondtrust.com/docs/privileged-remote-access/updates/attributions).